KTH Information and
Communication Technology

Entanglement in quantum communication

Preparation and characterization of photonic qubits

DANIEL LJUNGGREN

Doctoral Thesis
Stockholm, Sweden 2006

Entanglement in quantum communication
Preparation and characterization of photonic qubits

Akademisk avhandling som med tillstånd av Kungl Tekniska högskolan framlägges till offentlig granskning för avläggande av teknologie doktorsexamen i fotonik torsdagen den 23 februari 2006 klockan 10.00 i Sal C1, Electrum, Kungliga Tekniska högskolan, Isafjordgatan 20-26, Kista.

TRITA-MVT Report 2006:1
ISSN 0348-4467
ISRN KTH/MVT/FR–06/1–SE
ISBN 91-7178-254-0

KTH School of Information and
Communication Technology
SE-164 40 Kista
SWEDEN

Typsatt med LaTeX 2_ε
Tryck: Universitetsservice US AB

Abstract

At the heart of quantum physics lies the principle of superposition, and at the heart of information theory lies the bit. Perhaps the most useful property of quantum systems is that they can be loaded with information bits, so-called *qubits*, that are indefinitely both `0` and `1` until a measurement is made. Another consequence is that several qubits can become *entangled*, which is manifested by the non-classical correlations between such quantum systems when measured in all possible bases. Within the rapidly progressing fields of quantum information and quantum communication these quantum effects are utilized to perform tasks such as quantum computing and quantum cryptography.

In this thesis we present experimental and theoretical work using single photon sources to prepare "flying" photonic qubits. We describe work using mainly quasi-phase-matched nonlinear crystals to generate beams of entangled photon pairs, that are either encoded in polarization at near-visible wavelengths, or in time at optical fiber telecommunication wavelengths (1550 nm). The optical fiber is the medium used for transporting the qubits over a long distance, and it is therefore essential to couple the photons well into the fibers. By focusing the beams optimally, we have investigated how this problem can meet the requirement of creating photons of a narrow frequency bandwidth and a high photon flux. Furthermore, we have generated truly single photons that are heralded by an electrical signal. As a result of modifying the statistics of such sources we have been able to show the effect of photon antibunching. In two separate works, we have implemented a quantum key distribution system based on faint laser pulses at the telecom wavelength of 1550 nm, as well as protocols based on entanglement for performing authentication of key distribution in quantum cryptography.

```
bvddddfcyg5e3w4efsjjholöop påyedegcdfc,l.bl t5b67vv888t8hb k.m
```

Codewords. A poem by Majken, 10 months.

happily interfering . . .

Jag har drömt att en liten, liten kvinna
skulle söva mig med visor, skulle smeka mig med skratt,
och när allt som jag byggt måste brinna,
skulle följa mig i elddopets natt.

Dan Andersson, *Jag har drömt...*

Preface

This thesis is the result of research work conducted in the group of Quantum Electronics and Quantum Optics at the Department of Microelectronics and Information Technology (KTH) between the years 2000 and 2005. The thesis consists of a short summary of the field in general, alternated with results and discussion of my own work in collaboration with others, which have originally been published or submitted for publication in research journals. These publications are listed on page xiii and appended at the end of the thesis, and form the core of the scientific results. Specific details omitted from the thesis are found in the reprinted publications. Details on the scientific contribution of the author is given on the cover page preceding each of the reprints. An overview of each chapter is found at the end of the introduction.

Thanks!

I shall seize the opportunity to thank some sources that have all provided a healthy amount of distraction from my work, in times when I needed to remember that science, too, shall not be taken any more serious than life ...

music,
the mountains,
snow,
the mind puzzling cubes,
play,
and many other meditative realities.

Probably all errors and misunderstandings in the text are mine. However, I wish to thank Gunnar Björk and Anders Karlsson for proofreading the manuscript. I also wish to thank them for providing me with exotic sweets, spirits (!), operators, photons, and, together with many other experts in the field, for all kinds of inspiration.

An expert, I've heard, is one who knows more and more about less and less, until he eventually knows everything about nothing ... I am learning.

Thanks to all the forefathers of physics who leaved us with something to work on.

Respect to those who enter the lab to support live physics!

Many thanks to past and present colleagues, especially Maria for the hard work.

Those I owe my most loving thanks know it already ... Sara and our little one.

Daniel,
December 2005

Contents

List of publications

Publications included in the thesis

A *Characterization of an asynchronous source of heralded single photons generated at a wavelength of 1550 nm*,
M. Tengner and **D. Ljunggren**, in preparation (2006).

B *Theory and experiment of entanglement in a quasi-phase-matched two-crystal source*,
D. Ljunggren, M. Tengner, P. Marsden, and M. Pelton, to be published in Phys. Rev. A (2006).

C *Optimal focusing for maximal collection of entangled narrow-band photon pairs into single-mode fibers*,
D. Ljunggren and M. Tengner, Phys. Rev. A **72**, 062301 (2005).

D *Bright, single-spatial-mode source of frequency non-degenerate, polarization-entangled photon pairs using periodically poled KTP*,
M. Pelton, P. Marsden, **D. Ljunggren**, M. Tengner, A. Karlsson, A. Fragemann, C. Canalias, and F. Laurell, Opt. Express. **12**, 3573 (2004).

E *Authority-based user authentication in quantum key distribution*,
D. Ljunggren, M. Bourennane and A. Karlsson, Phys. Rev. A **62**, 022305 (2000).

F *Experimental long wavelength quantum cryptography: from single-photon transmission to key extraction protocols*,
M. Bourennane, **D. Ljunggren**, A. Karlsson, P. Jonsson, A. Hening and J. Peña Císcar, J. Mod. Opt. **47**, 563-579 (2000).

Other selected publications and conference contributions

G *Twin-photon sources for quantum information applications*, A. Karlsson, **D. Ljunggren**, and M. Tengner, in Quantum Information Processing and Communication in Europe, Information Society Technologies FET, EU (2005).

H *A source of entangled photon-pairs: optimizing emission in two quasi-phase-matched crystals*, **D. Ljunggren**, M. Tengner, M. Pelton, and P. Marsden in Proceedings of QCMC04, eds. Barnett *et al.* AIP Conf. Proc. **734** (Edinburgh 2004).

J *Efficient single-mode generation of degenerate 1550 nm entanglement in type-II parametric downconversion*, **D. Ljunggren**, P. Marsden, M. Tengner, I. Ghiu, I. Vellekoop and A. Karlsson, CLEO/QELS, QTuB3, Baltimore, USA (2003).

K *Bright source of polarisation-entangled photons using periodically poled potassium titanyl phosphate (KTP)*, M. Pelton, P. Marsden, **D. Ljunggren**, M. Tengner, A. Karlsson, A. Fragemann, C. Canalias, and F. Laurell, CLEO/ QELS, QThPDB3, Baltimore, USA (2003).

L *Some properties of three-party entangled states and their application in quantum communication*, A. Karlsson, M. Bourennane, I. Ghiu, **D. Ljunggren**, and A. Månsson, Proceedings of Solvay Conference (2002).

M *Authority-based user authentication and quantum key distribution*, **D. Ljunggren**, M. Bourennane and A. Karlsson, Quantum Communication, Computing, and Measurement 3, eds. P. Tombesi and O. Hirota, 299-302 (Plenum, New York 2001).

N *Quantum communication and single-photon technologies*, A. Karlsson, M. Bourennane, **D. Ljunggren**, J. Peña Císcar, M. Mathes and A. Hening, ROMOPTO 2000: Sixth Conference on Optics (edited by V. I. Vlad), Proc. SPIE **4430**, 430-441 (2001).

P *User authentication in quantum cryptography based on two-particle entanglement*, **D. Ljunggren**, M. Bourennane, and A. Karlsson, oral talk at Swedish-Russian Workshop on Entangled Quantum Systems in St. Petersburg (2000).

Q *Quantum cryptography - from single-photon transmission, key extraction methods to novel quantum information protocols*, A. Karlsson, M. Bourennane, **D. Ljunggren**, P. Jonsson, A. Hening, J. Peña Císcar, M. Koashi and N. Imoto, IEEE Proceedings of the 1999 Congress on Evolutionary Computation **3**, 2247-2254 (Piscataway 1999).

R *Experiments on long wavelength (1550 nm) "plug and play" quantum cryptography systems*, M. Bourennane, F. Gibson, A. Karlsson, A. Hening, P. Jonsson, T. Tsegaye, **D. Ljunggren** and E. Sundberg, Opt. Express **4**, 383-387, (1999).

List of acronyms

EPR	Einstein-Podolsky-Rosen
LG	Laguerre-Gaussian
HG	Hermite-Gaussian
CNOT	Controlled NOT-operation
QKD	Quantum key distribution
BB84	[Bennett and Brassard, 1984]
B92	[Bennett, 1992]
QBER	Quantum bit error rate
SPDC	Spontaneous parametric downconversion
QPM	Quasi-phase-matching
PPKTP	Periodically poled KTP
KTP	$KTiOPO_4$
CHSH	Clauser-Horne-Shimony-Holt

Chapter 1

Introduction

In one respect, A. Einstein doubted quantum physics for the entire second part of his life. He had predicted that if quantum theory was right there would be an effect where two particles, in his case electrons, could show correlation in measurements at an infinite distance apart, even though each particle individually would show a random outcome in the same measurement. He called this implausible effect "a spooky action at a distance", and declared that clearly something is incomplete with quantum mechanics in its description of reality [Einstein, Podolsky, Rosen, 1935]. He never made peace with the idea, and neither did he live past the time of the first convincing experiments of the so-called EPR-effect, that indeed proved it just to be a natural consequence of quantum theory. The Nobel laureate in physics 2005, R. Glauber (who is among the inventors of quantum optics) recently participated in a round table discussion, Noble minds, where he touched upon this issue. He could safely declare that today we have an "EPR-industry". He was aiming at the lively fields of quantum information and quantum communication which has become the first to appreciate the power of so-called *entangled* pairs of particles. The graph in Figure 1.1 shows the evolution of sources of entangled photon pairs, which are frequently used today as a resource of entanglement. The y-axis shows the number of photon pairs that can be produced per second, and one can observe a tremendous growth in development over the past ten years as technology has made more and more efficient sources available. The first sources used emission from single atoms. It turned out to take over 30 years after the development of the laser until it became an key component in efficient entanglement generation. In a few years ($\sim$2025 by extrapolating the graph) we will probably create entangled photons with the same ease and high photon flux as a semiconductor laser-diode produce light today.

In quantum communication, entanglement is used as a resource to perform various tasks such as quantum teleportation, dense coding, and quantum cryptography. The latter has become the first commercial application based on full theory of quantum physics, and is currently hunting customers. The area is strongly multidisciplinary in the sense of merging ideas from both quantum physics, information

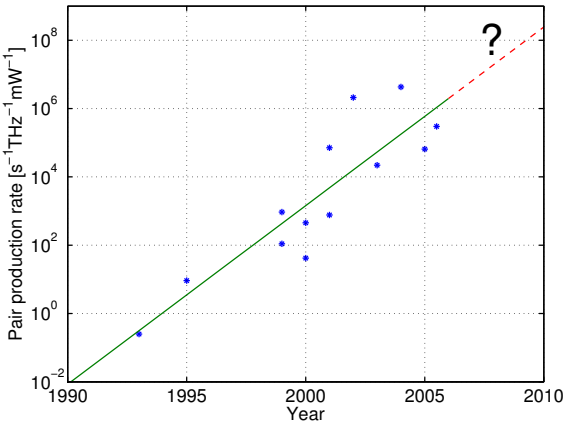

Figure 1.1: Historical and possible future trends of production rates of entangled photon pairs created in non-linear crystals. The exponential growth over time is mainly due to better crystal materials, longer crystals, more efficient fiber-coupling, or fiber-based generation. Data taken from Appendix A.

theory, cryptography, computer science, optics, atomic physics, etc., both experimentally and theoretically. In particular, quantum optics has become a very fruitful ground for direct tests and showcase of quantum theory, due its high pedagogical value and fairly simple implementations.

This thesis concerns the use of single photons to encode and decode quantum units of information called *qubits*. In Chapter 2 some fundamental concepts of quantum theory and quantum optics are given as a background and put into context with information theory and cryptography, together forming quantum information and quantum communication. Chapter 3 summarizes our work of generating single photon-pairs that are either entangled or used to generate single photons. The latter problem is treated in **Paper A**, and the former in **Paper D**. We also summarize **Paper B** which includes the latest results on a hybrid coded entanglement communication system that we are developing. In **Paper C** we attack the problem of how to efficiently collect the single photons into optical fibers, a problem which has received great attention over the last few years as a further way of increasing the quality of the sources, or perhaps due to the insight of how suitable fibers are for almost all optical manipulation and transportation of photonic qubits. This paper is also summarized in Chapter 3. To test the quality of entanglement and characterize the output emission of single photon sources there are standard tools developed which we have utilized in our work and which we provide a summary of in Chapter 4. Chapter 5 is devoted to a short review of the possible uses of entanglement and of the different implementations of quantum cryptography, as well as a summary of **Paper E** and **Paper F**. Chapter 6 concludes the thesis.

Chapter 2

Fundamental concepts

We shall in this chapter review some techniques that have been developed from quantum theory and optical communication to encode information at the single-photon level using the concept of a photonic qubit. We also summarize some fundamental results of quantum optics and beam propagation, and cover the manipulations of qubits in the language of quantum information. The role of superpositions, entanglement, and the principle of no-cloning in quantum communication and quantum cryptography is discussed. Rather complete introductory references would be Mandel and Wolf [1995]; Nielsen and Chuang [2000]; Tittel and Weihs [2001]; Gisin *et al.* [2002].

2.1 The photon as an information carrier

Waves and particles are the only known forms of energy that can carry information. This fact makes them two very fundamentally important entities. Even so, as we know today, information always needs to be represented by a physical system, or conversely: any physical system *is* information, which might be a more astonishing claim. Either way, the statements are simply a sign of wisdom, inspired by the thoughts of R. Landauer [1996]. Like him, many have now started to realize that information is not merely an abstract concept that is disconnected from the laws of physics. Rather, information is always embodied in some form of energy or another: everything we perceive is information — which should not be mistaken for that it carries any meaningful message. The above statements have become like a mantra for quantum information scientist, and the insight which we shall bring along when discussing light as an information carrier is that any encoding of quantum information is strongly affected by its medium.

The electromagnetic field as a medium has its clear advantages[1], it can easily reach very far distances, it travels at the fastest speed we are aware of, it has huge information carrying capacities, and it is fairly easy to manipulate. In 1895,

[1] As a comparison, at the other extreme we have a message in a bottle.

G. Marconi made the first attempt of taming the electromagnetic field as an information carrier using radio frequencies (MHz−GHz), discovered earlier by H. Hertz. Since then, we have managed to tame both sonar frequencies (kHz), optical frequencies (PHz), and X-rays (EHz). Already from the beginning, waves proved to be extremely successful in describing time-varying electrical fields in all possible contexts. Today, what is becoming more important also for communication, is that the field starts to behave particle-like for very low intensities and high frequencies. This idea was proposed by Planck in 1900 and used by Einstein in 1905 to explain the photoelectric effect. It would prove to be the birth of quantum theory. Earlier on, Maxwell's classical theories had been sufficient to explain the behavior of electromagnetic fields as waves, and already in 1865 he proposed that light is an electromagnetic wave. In the classical description many photons work together to form the electromagnetic field and acts therefore as a single wave. Information can be modulated onto the wave, or signal carrier, using the amplitude, frequency, polarization, or phase of the field; ideas which today defines the areas of radio-, microwave-, and optical communication. Combining the ideas from quantum theory [Peres, 1995] and optical communication [Agrawal, 1997], we shall in this chapter review some techniques that have been developed to encode information in a single photon.

Like all particles and waves, single photons obey the principle of *superposition*. But unlike classical objects and waves, the quantum version is special and a little bit more peculiar in the sense that it shows effects that are very different from what one can experience in everyday life. The quantum superposition principle, as it appears, is a consequence of the photon being *both* a wave and a particle. If we arrange for our detection system not to provide any information on the extent of the photon as a particle it will behave as a wave, and vice versa. Due to the indivisible nature of the photons, a single photon can only choose to give a click in a single detector at a time, and so therefore, in contrast to a classical wave showing interference and giving different intensities in two detectors, a photon must instead be attributed a probability to give a click in either detector. In this context, it has shown successful to ascribe quantum theory as a theory of predictions — a theory which is becoming more and more popularly looked at even as a theory of information; as soon as we have gathered information of the system we must update our description of it in terms of probabilities. In the above sense, superposition can be seen as a manifestation of Heisenberg's uncertainty principle, which in one form states that detection of a photon providing fairly exact knowledge on its time of arrival can only be done at the cost of not precisely knowing its frequency, or vice versa; noting that frequency is a characteristic property of waves. Thus, one way to look at the photon is to say that within its extent the photon is a wave, and outside it is a particle, that is, a waveparticle — be it either just a click in a detector or something real. From this semiclassical viewpoint, many effects of how single photons behave in for example interferometers can be understood using the particle picture to explain why *only one* detector will click, and the wave picture to predict via superpositions *which* detector will click. The combined effect cannot

be explained by the particle- or the wave picture alone. However, there is one quantum effect that is even more subtle and not explainable by the semiclassical picture, namely, the interference between two photons in a beamsplitter. We will come back to this device soon.

The quantum superposition property of the photon is used in the implementation of the qubit. As such, a single photon can carry maximumly one classical bit of information, pertaining to a yes (1) and no (0) outcome of a single measurement made on the qubit using two orthogonal projections. Regarding the photon as a qubit, it is probably the best and the worst implementation for a qubit at the same time. It interacts fairly weakly with the environment, which is good for propagation, and it is easy to manipulate its direction of propagation, and its polarization, etc. On the other hand, a photon is harder to make interact with other photons, because it is simply the mediating particle of the field between electrical charges composing atoms. If we would like photonic qubits to interact with other photonic qubits, to implement logical gate operations for example, the only way is therefore via atom-photon interaction — a non-linear coupling which is usually quite weak.

Despite the weak interactions in for example the optical fiber, light sent through it will be attenuated, or rather, in the case of a single photon, absorbed. The absorption-rate, or loss, has its minimum in optical fibers at the wavelength of 1550 nm. The loss is of course affected by the transmission distance, L, in the fiber, and will depend as $10^{-\alpha L/10}$, where α is $2-3$ dB/km for the first telecom window (800 nm), 0.35 dB/km for the second (1300 nm), and 0.20 dB/km for the third (1550 nm) (all values for single-mode fibers). The standard fiber is good as a photon carrier medium but far from perfect. There are mainly four effects that cause trouble. Depolarization effects are present in the form of *birefringence* and *polarization mode dispersion*; the former is due to different phase-velocities for two orthogonal polarizations and the latter is due to different group velocities. Both rotates the polarization randomly making it difficult to maintain information coded in polarization. The *geometric phase*, or Berry phase, will also rotate the state depending on the trajectory of the fiber. However, this is just a matter of a one-time agreement between the sender and receiver to apply some suitable anti-rotation within their reference frame if the fiber trajectory is stationary. Another problem is *chromatic dispersion* which will cause decoherence effects if the information is encoded in time, that is, phase.

A few long-distance quantum communication experiments at single photon level have been demonstrated in free-space as well. In straight point-to-point communication additional restrictions on the location of the sender and receiver apply, and consequently, a major interest lies in satellite-to-earth communication. Experimentally such links are outside the scope of the thesis. However, as we shall see, the ideas for authentication in quantum cryptography, **Paper E**, may be very useful in this context.

2.2 States, modes, and indistinguishability

In quantum physics, a state $|\psi\rangle$ is used to describe the physical *state* of the system, and in mathematical terms it is defined as a vector in a Hilbert space. If we choose a particular basis for our Hilbert space, the state can also be represented by a *wave-function* that assigns different complex weights c_n to each of the basis-vectors. A *pure* state is one which can be written as a single vector $|\psi\rangle$ in one particular basis, and a *mixed* state one which can only be expressed by a density matrix ρ as a sum of outer products of at least two pure states, $\rho = \sum_n p_n |\psi_n\rangle\langle\psi_n|$. In quantum physics the plus sign between two states, $|\psi\rangle = c_1|\psi_1\rangle + c_2|\psi_2\rangle$, is attributed a special significance by denoting the superposition of states. What is effectively added is quantum state amplitudes, c_n, corresponding to quantum probabilities, $c_n^* c_m$, that may be negative. It has the consequence that classical probabilities, $p_n = |c_n|^2$, are represented by the diagonal elements in a mixed density matrix.

What the Hilbert space actually does represent in physical terms are different *degrees of freedom* of the system. Such degrees of freedom can be the spatial coordinates (transverse spatial), temporal properties (longitudinal spatial), polarization, spin, or any other physical entity which we would like to use to describe the system.

To make a connection to the previous section, we could ask for the boundary where a wave acts as a particle, and a particle acts as a wave. The answer lies in the uncertainty relations, which for the temporal degree of freedom become

$$\Delta\nu\Delta t \geq 0.44, \tag{2.1}$$

for frequency and time with Gaussian forms. In analogy, for the one-dimensional spatial degree of freedom,

$$\Delta k_x \Delta x \geq 1, \tag{2.2}$$

where Δk_x is the uncertainty of the wavevector k_x in the x-direction, and Δx is the uncertainty in the position of a particle along x. Both of these equations will define the concept of temporal or spatial "modes" respectively. One can represent Eqn. (2.2) graphically by a two-dimensional surface as in Figure 2.1. In each basis, x and k_x, the wave-function describes the form of a slice cut through the surface. Together they define an area of uncertainty (volume in general). Now, a state is said to be in a *single-mode* if its wave-function is described by a real-valued Gaussian function in both dimensions, so that the uncertainty relation is obeyed in a strict sense, $\Delta k_x \Delta x = 1$. In other words, the area (volume) in that case defines the minimum resolution of the state of the system. Within the area the state is first-order coherent, that is, within it we are forbidden to make any further distinctions whatsoever between different values of the variables of positions, x, and propagation directions, k_x, of a particle, without affecting the other variable. Thus, the area defines the range of values of x and k_x which are fundamentally *indistinguishable*. Furthermore, two different systems, or particles, can be in different such "modes" that may or may not overlap. If two such systems, a and b, are components of a

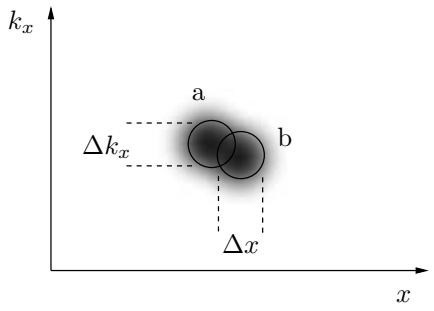

Figure 2.1: Areas of uncertainty defining the single-mode.

bigger system and the areas do not overlap they are *distinguishable*, and the bigger system is said to be *multimode*, $\Delta k_x \Delta x > 1$. These concepts will be very important later on for beam propagation, as we couple light into optical fibers. A fiber which guides only the fundamental single-mode is appropriate as a quantum channel as it will act as an isolated environment for the photon, in contrast to multimode fibers.

Turning to quantum optics, the concept of the photon as a particle enters from the quantization of the electromagnetic field of light. The electromagnetic field can be regarded as oscillating in a space restricted to the single-mode volume (also in free-space), setting boundary conditions for the energy of the field. Hence, as an effect, the energy becomes discretized, or quantized. The oscillation takes place between the two quadrature components P and Q of the real electrical field

$$E_{\text{real}}(t) = P\cos\omega t + Q\sin\omega t, \tag{2.3}$$

with the two components obeying the general principle of uncertainty. However, due to the quantization, the relation is much more conveniently expressed mathematically as a commutation rule using operators $\hat{P}$ and $\hat{Q}$ instead of the real fields. We have $[\hat{Q},\hat{P}] = \hat{Q}\hat{P} - \hat{P}\hat{Q} = 1$, symbolizing how $\hat{Q}\hat{P}$ and $\hat{P}\hat{Q}$ have different meanings in quantum theory. In other words, the nonzero factor is a result of the interplay between two non-commuting observables in two differently ordered sets of measurements. In general $\Delta\hat{Q}\Delta\hat{P} \geq \frac{1}{2}|\langle[\hat{Q},\hat{P}]\rangle|$ for any two non-commuting observables. Similarly $[\hat{a},\hat{a}^\dagger] = 1$, where $\hat{a} \sim E$ and $\hat{a}^\dagger \sim E^*$, loosely speaking. The quantization of the total energy $\hat{H}$ appears mathematically in form of an eigenequation,

$$\hat{H}|n\rangle = \hbar\omega n|n\rangle, \tag{2.4}$$

such that the field operations $\hat{a}|n\rangle = \sqrt{n}|n-1\rangle$ and $\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle$ alter the number of photons n occupying the single-mode oscillator in state $|n\rangle$. The total energy, $\hbar\omega n$, of n photons can thus attain only discrete values. Just like $E^*E = |E|^2$ represents the energy in a classical field, $\hat{n} = \hat{a}^\dagger\hat{a}$ represents the photon number.

Using the field operators, the energy becomes $\hat{H} = \hbar\omega(\hat{n}+1/2)$, where the constant term represents the vacuum energy for $n = 0$. This lowest energy is a consequence of the commutation relation introduced to represent the uncertainty principle in a single-mode oscillator. Thus, the uncertainty principle can now also be understood as a result of the field never coming to rest. The circle is closed. Finally, the instantaneous electrical field is given by

$$\hat{E}^{(+)}(t) = \hat{a}e^{-i\omega t} = (\hat{Q} + i\hat{P})e^{-i\omega t}, \tag{2.5}$$

which is used to describe the interactions in the crystals later on. There is also a special state, called the coherent state[2],

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \tag{2.6}$$

which has a minimum uncertainty in the photon number $\hat{n}$ and the complex field $\hat{a}$, and is an eigenstate to the field, $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$. It is the approximate state emitted by a laser, and is therefore often used as a source of single photons (although with limitations).

In a different language, each of the dynamical variables $\{x, k\}$, $\{\nu, t\}$, and operators $\{\hat{P}, \hat{Q}\}$ define a set of Fourier transform pairs. For example, k is the transform of x and vice versa, both representing the same information. The transform is simply an interconversion between two equally valid basis-sets; in this case describing two continuous variables of the spatial degree of freedom. If we instead choose a finite dimensional Hilbert-space, for example the polarization degree of freedom, the basis sets will be {H/V, D/A, R/L}, denoting the different polarizations. They are related by the discrete Fourier transform $|u_i\rangle = \sum_j |v_j\rangle\langle v_i|u_j\rangle$, which become extremely simple: $|\mathrm{D}\rangle = \frac{1}{\sqrt{2}}(|\mathrm{H}\rangle + |\mathrm{V}\rangle)$, $|\mathrm{L}\rangle = \frac{1}{\sqrt{2}}(|\mathrm{H}\rangle - i|\mathrm{V}\rangle)$, etc. The bases are said to be complementarity, or mutually unbiased, and is part of the same *urprincip* as uncertainty. For example, such bases are used to guarantee the security in quantum cryptography.

We will make some short notes on optical beam propagation, which can be treated by decomposing the light beam into a sum of plane waves $\boldsymbol{k}$. The normalized coordinates of each plane wave in an Cartesian system become $p = k_x/k$, $q = k_y/k$, and $m = k_z/k$, where k is the length of the vector $\boldsymbol{k}$, such that $\boldsymbol{k} = k(p\,\boldsymbol{e}_x + q\,\boldsymbol{e}_y + m\,\boldsymbol{e}_z)$. Along the z-axis the following approximation is useful: $m = \sqrt{1-(p^2+q^2)} \approx 1 - (p^2+q^2)/2$, where $p^2 + q^2 \leq 1$ represents a homogeneously propagating field, and $p^2 + q^2 > 1$ represents an inhomogeneous, damped field, which we pay no attention to here. Hence, the angular spectrum amplitude for a monochromatic Gaussian beam become

$$A(p,q) = \frac{kw_0}{\sqrt{2\pi}} e^{(kw_0)^2(p^2+q^2)/4}, \tag{2.7}$$

[2]Discovered by R. Glauber who received the Nobel prize last week (writing December 2005).

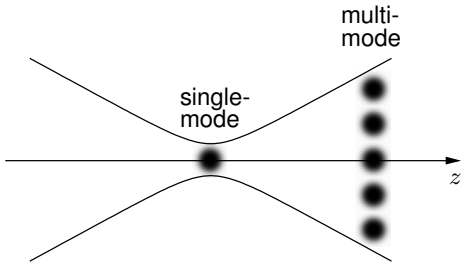

Figure 2.2: Gaussian beam propagation and the modes of uncertainty.

which is normalized to represent a constant power in the beam independent of the beam waist radius w_0. The angular spectrum can also be used to write the general state of the beam

$$|\mathcal{G}\rangle = \iint \mathrm{d}\theta \mathrm{d}\varphi \; A(\theta,\varphi) e^{-i\omega t} |\omega\rangle |\theta\rangle |\varphi\rangle, \tag{2.8}$$

in spherical coordinates ($p = \sin\theta\cos\varphi$, $q = \sin\theta\sin\varphi$, $m = \cos\theta$). The electrical field is found as the Fourier transform of the angular spectrum amplitude,

$$E(x,y,z) = \iint_{-\infty}^{\infty} A(p,q) e^{ik(px+qy+mz)} \mathrm{d}p \; \mathrm{d}q. \tag{2.9}$$

Figure Figure 2.2 shows the electrical field profile of a propagating Gaussian beam. The form of the angular spectrum and the electrical field is a real Gaussian function at the beam waist, related by their transforms and the single-mode condition $\Delta k \Delta x = 1$. At the far-field the state is multimode $\Delta k \Delta x > 1$. However, the state $|\mathcal{G}\rangle$ is pure everywhere. I believe that the following two conditions are generally valid for the relation between states and modes of uncertainty, pertaining to the same degree of freedom:

1. *It is a necessary but not sufficient condition for a single-mode to be a pure state:*

$$\textit{single-mode} \implies \textit{pure state}$$

2. *It is a necessary but not sufficient condition for a mixed state to be multimode:*

$$\textit{mixed state} \implies \textit{multimode}$$

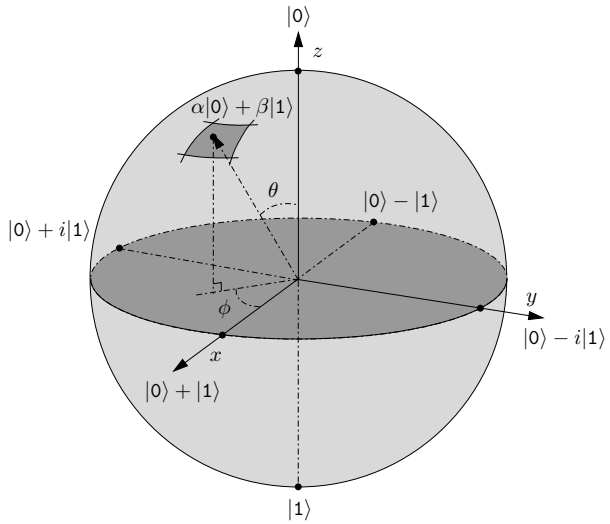

Figure 2.3: The qubit-sphere. Any two diagonally opposite states form an orthogonal basis to describe the qubit, and any two orthogonal lines through the origin define two mutually unbiased bases. Pure states lie on the outer shell and mixed states inside.

2.3 Qubit representations and operations

The qubit can carry at maximum one *bit* of classical information, but it is richer in the sense that it can describe superposition between two orthogonal states $|\mathtt{0}\rangle$ and $|\mathtt{1}\rangle$[3]. To define the quantum unit of information the name *qubit* was coined by Schumacher [1995]. The general pure state of a qubit system has the following form,

$$|\psi\rangle = \cos\frac{\theta}{2}|\mathtt{0}\rangle + e^{i\phi}\sin\frac{\theta}{2}|\mathtt{1}\rangle, \tag{2.10}$$

and can be visualized on the qubit-sphere, also called the Bloch-sphere, see Figure 2.3. The different axes represents the three mutually unbiased bases that exist for a two-dimensional Hilbert-space. In quantum communication (and computation) it is of special interest to look at systems of several qubits. When forming a system of two or more subsystems the qubits can also have correlations in the superpositions; they are said to be *entangled*. The general pure state for two entangled

[3]By the typewriter font we denote a logical value of the state of a system that can have many different physical representations.

systems A and B is

$$|\Phi\rangle = \alpha|0_A\rangle|0_B\rangle + \beta|0_A\rangle|1_B\rangle + \gamma|1_A\rangle|0_B\rangle + \delta|1_A\rangle|1_B\rangle, \tag{2.11}$$

which has the important property not to be *separable* into a product of states of the two subsystems, $|\vartheta_A\rangle \otimes |\vartheta_B\rangle$, for all states where $\alpha\delta \neq \beta\gamma$. We will come back to this special type of correlation soon. In the following text we will summarize the different realizations of qubits used in quantum communication, and for which the qubit-sphere is an equally valid illustration.

Polarization qubit

Perhaps the most illustrative and also most popular representation of a qubit is the polarization of the electrical field. The polarization can be H/V (horizontal/vertical), D/A (diagonal/ anti-diagonal), or R/L (right/left circular), forming three mutually unbiased bases. Each basis vector H and V etc. are orthogonal. R and L are found on the top and bottom of the qubit sphere, historically called the Poincaré-sphere in polarization optics. A simple qubit has the form $|\psi\rangle = \alpha|\mathrm{R}\rangle + \beta|\mathrm{L}\rangle = \alpha|0\rangle + \beta|1\rangle$. Polarization qubits are very simple to encode and decode using half-wave plates, quarter-wave plates, and polarizing beamsplitters, but are problematic to transport over fibers as we mentioned earlier. Due to the vast popularity of polarization coding in mainly free-space we will leave out any specific references. Polarization coding is used in **Paper A**, **Paper B**, and **Paper D**.

Phase qubit

The phase is the most commonly used representation for the qubit in faint-pulse quantum cryptography. The phase is naturally chosen to encode the information to overcome the problems using polarization in optical fibers. The phase-qubit is prepared and analyzed using interferometers and phase-modulators. The photon coherence length needs to be longer than the path-length mismatch between the different arms of the interferometers. This is the type of coding used for single qubits in the "plug and play" quantum cryptography scheme, and hence in **Paper F**. For the corresponding coding of entangled qubits please refer to the paragraph on continuous-time qubits.

Dual-rail qubit

As the name suggest the qubit is encoded in two spatially different modes, such that a single photon exists in a superposition of being in either mode, see Figure 2.4. Sometimes it is also called a bosonic qubit. The qubit is prepared by a semi-transparent mirror, or beamsplitter. The photon in each mode is attributed the value 0 or 1, according to the notation $|n_0 n_1\rangle$ where n denotes the number of photons in each arm (mode). Thus, the two modes define a single qubit system, which has the form $|\psi\rangle = \alpha|10\rangle + \beta e^{i\phi}|01\rangle = \alpha|0\rangle + \beta e^{i\phi}|1\rangle$. The qubit is decoded

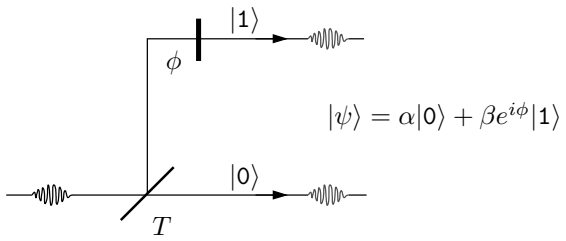

Figure 2.4: The dual-rail qubit. Variable transmission, $T = \alpha^2 = 1 - \beta^2$.

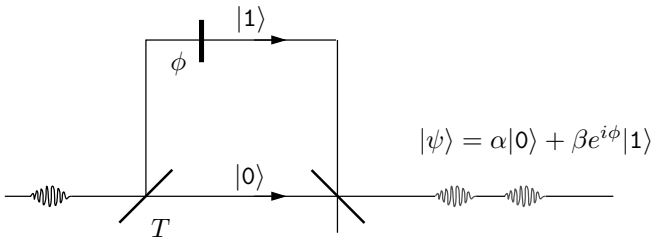

Figure 2.5: Discrete-time qubit. Variable transmission, $T = \alpha^2 = 1 - \beta^2$.

by a similar setup, which is reversed. The encoding is only practical for small-scale, short-distance implementations since both rails need the same environmentally induced noise on each of the modes, and has thus found its application in linear optical quantum computing [Knill *et al.*, 2001; O'Brien *et al.*, 2003].

Discrete-time qubit

If we instead let each spatial mode go into different but adjacent temporal modes (time-bins) roughly the same environment will act on both modes if the time-delay is not too long, see Figure 2.5. The scheme is used to send qubits robustly over optical fibers. The time-separation between the modes is larger than the coherence length of the photon itself. Denoting the different temporal modes with an superscript a simple qubit has the form $|\psi\rangle = \alpha|01\rangle^{t_1} + \beta e^{i\phi}|01\rangle^{t_2} = \alpha|0\rangle + \beta e^{i\phi}|1\rangle$. See further Section 3.4 where the decoder for this implementation is discussed. The principle is to interfere each of the modes again by reversing the encoding process. Thus, the phase relation will define the complementary basis. The implementation display a lot of similarities with Franson-type interferometry for two entangled states, see next paragraph. For references see Brendel *et al.* [1999]; Tittel *et al.* [2000] and **Paper B**.

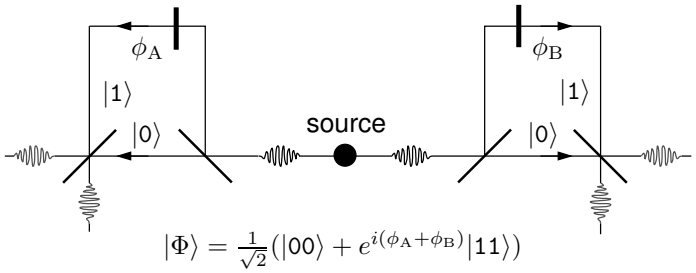

Figure 2.6: Continuous-time entangled qubits.

Continuous-time qubit

This type of coding is usually associated with entanglement between two systems, so called energy-time entanglement, and was first proposed by Franson [1989]. It consists of two unbalanced Mach-Zehnder interferometers similar to Figure 2.5, one for each system, see Figure 2.6. The coding uses the phase information to encode the information similar to phase-qubits. When detecting two energy-time correlated photons in precise coincidence, one cannot determine which way either of them took in the interferometers. Therefore, the two paths, long-long and short-short, will interfere (the long-short and short-long cases will not produce coincidences). Depending on the phase, the photons will come out in either port of the last beam-splitters, in correlation.

However, each of the two interferometers can also be seen separately as a encoder and a decoder for a single qubit. If looked at as being part of the detection system the unbalanced interferometer introduces an uncertainty in the time of arrival of the photons, or, in other words, effectively extends the photons' coherence length[4] to be as long as the path-difference between the arms. The state on each side will be in a coherent superposition between the lower $|0\rangle$ and upper arm $|1\rangle$, and realize a qubit. Depending on the phase, the photon will then choose way in the last interferometer and give a click in either detector. The entanglement in emission time and frequency of each photon will provide correlations between the two systems depending on the relative phase $\phi_A - \phi_B$. The encoding and decoding is implemented using phase-modulators. The scheme has been demonstrated in many implementations using a single basis [Kwiat *et al.*, 1993; Tittel *et al.*, 1998, 1999], and with two non-orthogonal bases for quantum cryptography [Ribordy *et al.*, 2001].

[4]The interferometer works here in the same way as the jitter of the detectors by extending the coherence length of the photons, see Section 3.5. For the entangled state it is necessary for the two-photon (i.e. the pump beam) coherence length to be longer than the path difference.

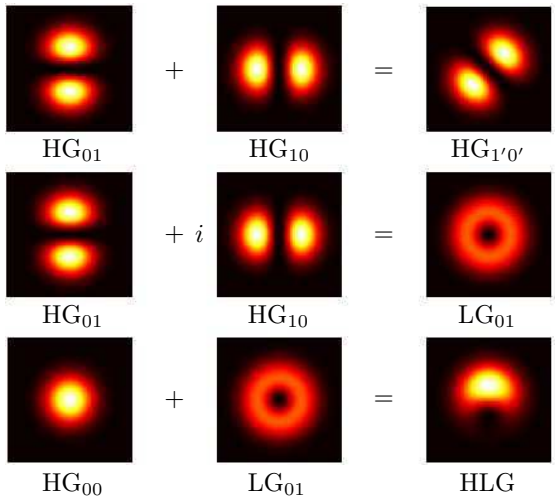

Figure 2.7: Spatial-mode qubit. Laguerre-Gaussian (LG) and Hermite-Gaussian (HG) modes. The vortex in the mode denoted HLG rotates around the optical axis as it propagates.

Spatial qubits

Spatial qubits can be obtained through the higher orders of transverse Hermite-Gaussian ($HG_{n,m}$) and Laguerre-Gaussian ($LG_{p,m}$) modes, which both contain an infinite set of orthogonal modes[5]. The mathematical structure of these modes, indexed by {n,m} and {p,m}, respectively, can be found in for example Siegman [1986]. The two sets differ in symmetry; the LG-modes have radial symmetry, while the HG-modes can always be decomposed into two orthogonal axes. How these sets of bases work to encode qubits should be clear from Figure 2.7. A superposition of two modes from either set will form another mode from either set like illustrated. For example, $|\mathrm{LG}_{01}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$, where $|0\rangle = |\mathrm{HG}_{01}\rangle$ and $|1\rangle = |\mathrm{HG}_{10}\rangle$, makes a qubit from a superposition of two HG-modes. The result is a mode of a single photon that exhibits orbital angular momentum, a so called donut mode. The fundamental modes HG_{00} and LG_{00} are identical to the zero:th order transverse electromagnetic mode TEM_{00}, that are all described by a real valued Gaussian function, Eqn. (2.7), and resembles closely the mode supported by the single-mode fibers. These modes also makes a suitable basis to represent the emission from spontaneous parametric down-conversion, hence our interest. The transformation between the modes can be realized by phase-holograms, working as an encoder via

[5]Not be confused with the spatial and temporal uncertainty modes discussed earlier, these modes are rather basis-vectors that constitute the different laser modes.

the mode-selection of a fiber. Example of such work is [Mair *et al.*, 2001; Leach *et al.*, 2002; Langford *et al.*, 2004]. The bases make a suitable way to encode higher-dimensional *qudits* of any dimension D.

Frequency qubit

The method of frequency-multiplexing has made a strong impact on classical communication, and in the case of a qubit it would imply the encoding of one frequency $|\omega_1\rangle$ as $|0\rangle$ and another frequency $|\omega_2\rangle$ as $|1\rangle$, where ω_1 and ω_2 are the sidebands of a center frequency ω_0. As we shall see later, photon-pairs generated by spontaneous parametric downconversion will have quantum correlations in frequency (entanglement), which makes it a suitable basis for qubits, or even qudits. The encoders and decoders would utilize phase modulators and wavelength-multiplexers for their implementation. Some work on this has been done [Sun *et al.*, 1995; Mérolla *et al.*, 1999].

Transformations

In analogy with tasks in classical computation and communication, where bits of information are processed via gates and circuits, a similar toolbox for operations on qubits in the language of quantum information has been developed. Such operations, or transformations, will correspond to rotations and/or reflections of the qubits in the qubit-sphere. The operations can either be single-qubit operations or multiqubit operations. The transformations we need to apply depend of course in each case on the qubit's physical implementation. We will here review the most important operations, ignoring any possible overall phase-factors.

The three Pauli matrices have a special significance when operated on single qubits like $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. They either invert the qubit, $X|\psi\rangle = \beta|0\rangle + \alpha|1\rangle$ (NOT-gate), flips the phase of the qubit, $Z|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$, or both, $Y|\psi\rangle = \beta|0\rangle - \alpha|1\rangle$, with the basis vectors represented as $|0\rangle = \left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$ and $|1\rangle = \left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]$. We list the operations here in matrix form together with the identity operator,

$$I = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}; \quad X = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}; \quad Y = \begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}; \quad Z = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}. \tag{2.12}$$

These four matrices together form a complete basis set for generating any 2×2 Hermitian matrix. The so called Hadamard transform H is a very important operation that takes a single vector $|0\rangle$ in some basis into a superposition $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ in the same basis. Another useful operation is the phase-gate S. They have the following matrix representations,

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}; \quad S = \begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}. \tag{2.13}$$

Even though not explicitly noted, these transforms are frequently used in our experimental work when analyzing qubits. For example, half-wave-plates and quarter-wave-plates rotates the qubit around the three axes, $R_X(b)$, $R_Y(c)$, $R_Z(d)$, for different angle settings $\phi = f(b, c, d)$ of the plates, corresponding to the three Pauli matrices. Any arbitrary transformation U can always be written as a combination of rotations of the qubit on the qubit-sphere, $U = e^{ia} R_Z(b) R_Y(c) R_Z(d)$, accordingly. It should also be noted that it is impossible to find a general transformation U that operates unambiguously on an unknown qubit. That is to say, we cannot create for example a universal bit-flip operation X that bit-flips every possible state on the qubit-sphere with complex coefficients. Such a transform would be non-unitary [Pati, 2002]. Thus, all operation on the qubit-sphere which we would like to use for computation has to be defined to work only for some partially known qubits that lie on a circle, for example the polar circle with only real coefficients. It is therefore important to decide upon a so called *computational basis* for the physical implementation. This is the basis which we would like to protect from decoherence in the communication system as we shall see later.

The most important two-qubit operation is the controlled-NOT function, referred to as CNOT. Conditioned on one of the qubit systems (the control qubit), the operation bit-flips the other (the target qubit). This gate is very important in order to explain the creation of entanglement in operational terms, as well as the analysis of entanglement, as it takes product states into non-separable states and vice versa. In matrix form it is represented by

$$U_{\text{CNOT}} = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{2.14}$$

We will soon return to this transformation in Section 2.4.

The beamsplitter

We will now pay some attention to a very useful and remarkable device: the beamsplitter. In all its simpleness, it has been an essential part of many new discoveries within quantum optics, especially in the investigations of higher-order correlation functions describing single-photon and two-photon interference effects [Hanbury Brown and Twiss, 1956a; Hong *et al.*, 1987]. In general, the beamsplitter is reciprocal and has four input ports and four output ports. As the name suggests it can be used to split the light of two input ports, a and b, into two output ports, a′ and b′, as is illustrated in Figure 2.8. For our purpose it suffice to simplify the analysis to 50/50% splitting. The device is used to interfere either one photon with itself or two or several photons with each other, and it is therefore a key component in preparing and analyzing discrete-time qubits. To understand the function of the beamsplitter we need to use the number state notation, which we already encountered: $|\psi_{\text{ab}}\rangle = |n_{\text{a}} n_{\text{b}}\rangle = \sqrt{1/n_{\text{a}}!}(\hat{a}^\dagger)^{n_{\text{a}}} \sqrt{1/n_{\text{b}}!}(\hat{b}^\dagger)^{n_{\text{b}}}|00\rangle$, where $n_{\text{a}}, n_{\text{b}}$ denotes the

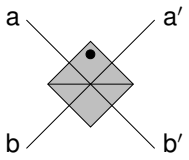

Figure 2.8: The beamsplitter.

number of photons in either port (mode) a or b. Since the number states belong to an infinite dimensional Hilbert space, we can hardly express the beamsplitter transformation as a matrix in general. Instead we can use Heisenberg's picture to describe how the creation operators evolve through the beamsplitter according to

$$\begin{aligned}\hat{a}^\dagger &= \frac{1}{\sqrt{2}}(i\cdot\hat{a}'^\dagger + \hat{b}'^\dagger),\\ \hat{b}^\dagger &= \frac{1}{\sqrt{2}}(\hat{a}'^\dagger + i\cdot\hat{b}'^\dagger).\end{aligned} \tag{2.15}$$

The imaginary number is due to the reflection, which makes a 90° retardation in phase, while transmission makes no change in phase. Table 2.1 summarizes the different types of interferences which can occur. Note especially the signature of two-photon interference (5) where two input photons never exits at different ports. This is a result of adding probability amplitudes, and is a distinguishing mark for how photons behave according to quantum theory, having no classical analog. The effect has been shown both with photon pairs [Hong *et al.*, 1987] and two independent photons [Santori *et al.*, 2002]. Furthermore, it is essential that the spatial and temporal modes of both ports overlap to see any interference effects, and that the polarizations are identical. This is the number-one concern experimentally, and therefore it is beneficial to use fiber optical based beamsplitter which are pre-aligned, solving at least the first of these three problems.

If we restrict ourself to a finite dimensional subset of the possible states of photon-numbers as given in the table, we can use the following basis set: $\{|10\rangle, |01\rangle, |20\rangle, |02\rangle, |11\rangle\}$ corresponding to vectors $\{(00001)^{\mathrm{T}}, \ldots, (10000)^{\mathrm{T}}\}$, with dimension $D = 5$. In this case, the action of the beamsplitter transform B on a general input state will give the correct output state $|\psi_{\mathrm{a'b'}}\rangle = B|\psi_{\mathrm{ab}}\rangle$ for

$$B = \frac{1}{\sqrt{2}}\begin{bmatrix} 0 & i & i & 0 & 0\\ i & -1/\sqrt{2} & 1/\sqrt{2} & 0 & 0\\ i & 1/\sqrt{2} & -1/\sqrt{2} & 0 & 0\\ 0 & 0 & 0 & i & 1\\ 0 & 0 & 0 & 1 & i \end{bmatrix}. \tag{2.16}$$

It is interesting to take note of the fact that the beamsplitter can for example

	$\lvert\psi_{\mathrm{ab}}\rangle$	$\overset{B}{\longleftrightarrow}$	$\lvert\psi_{\mathrm{a'b'}}\rangle$
1	$\frac{1}{\sqrt{2}}(\lvert 01\rangle + i\lvert 10\rangle)$		$i\lvert 01\rangle$
2	$\frac{1}{\sqrt{2}}(\lvert 01\rangle - i\lvert 10\rangle)$		$\lvert 10\rangle$
3	$\lvert 01\rangle$		$\frac{1}{\sqrt{2}}(i\lvert 01\rangle + \lvert 10\rangle)$
4	$\lvert 10\rangle$		$\frac{1}{\sqrt{2}}(\lvert 01\rangle + i\lvert 10\rangle)$
5	$\lvert 11\rangle$		$\frac{i}{\sqrt{2}}(\lvert 02\rangle + \lvert 20\rangle)$
6	$\frac{1}{\sqrt{2}}(\lvert 02\rangle - \lvert 20\rangle)$		$\frac{1}{\sqrt{2}}(\lvert 20\rangle - \lvert 02\rangle)$
7	$\lvert 20\rangle$		$-\frac{1}{2}\lvert 20\rangle + i\frac{1}{\sqrt{2}}\lvert 11\rangle + \frac{1}{2}\lvert 02\rangle$
8	$\lvert 02\rangle$		$\frac{1}{2}\lvert 20\rangle + i\frac{1}{\sqrt{2}}\lvert 11\rangle - \frac{1}{2}\lvert 02\rangle$
9	$\frac{1}{\sqrt{2}}(\lvert 02\rangle + \lvert 20\rangle)$		$i\lvert 11\rangle$

Table 2.1: The different types of interference effects in a beamsplitter.

act as a Hadamard transform. For the dual-rail qubit the lower-right part of the transform $B_{\mathrm{h}} = \left[\begin{smallmatrix} i & 1 \\ 1 & i \end{smallmatrix}\right]$ will have this function. Together with additional phase-shifts we get $SB_{\mathrm{h}}S = iH$.

Note also from the table, that if a product state is sent into the beamsplitter a non-separable state will in general exit (e.g. 3, 4, and 5). The two output modes will be entangled. As we shall see in Section 3.4 the beamsplitter can also be used to post-selectively create polarization entanglement. In the following section I will present ideas on how entanglement can be seen as the offspring of superpositions and classical correlations solely.

2.4 Entanglement demystified?

Ever since its discovery, entanglement has come to play a central role in many widely differing contexts dealing with quantum theory. It is not surprising since entanglement is a natural consequence for any multiparticle system described by quantum-like superpositions. Entanglement can in principle arise for any quantum system in which at least two subsystems can be identified and isolated. The two modes of the beamsplitter form exactly two such subsystems that can become entangled. In fact, the majority of states in our world are probably entangled, if we look at our overall environment as a system. A popular belief is that it is more of an exception for two subsystems to be separable than to be non-separable. In the following text we shall discuss how entanglement arise from the process of spontaneous parametric downconversion in a nonlinear crystal as a consequence of Nature not allowing clones to exist for quantum objects, and neither so superluminal communication [Peres, 2002]. We will not go into details about the process itself, but

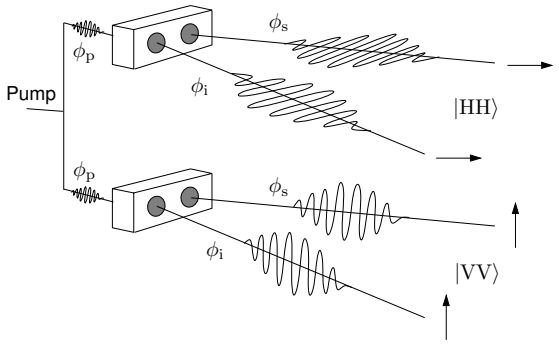

Figure 2.9: Illustration of creation of product states.

leave that to Chapter 3. The experiments we refer to are **Paper B** and **Paper D**, based on the idea to use two crystals to create polarization entanglement [Hardy, 1992; Kwiat *et al.*, 1999].

Consider first the following gedanken experiment, similar to the proposal by Herbert [1982]. The upper part of Figure 2.9 shows a single unpolarized photon (pump) give birth to two other photons (signal and idler) inside a box, with the pump photon itself becoming destroyed in the process. Ignore the content of the box. The two photons are created at some random time-instant with the same horizontal polarization $|HH\rangle$, both exactly in phase with the pump. Consider now the lower part, and the possibility that two vertical polarized photons $|VV\rangle$ are created, also in phase with the pump. The risk of two pairs to be created from either box at exactly the same time-instant is negligible. Now, as illustrated by Figure 2.10, we place both boxes just after each other (which are infinitely thin), so that we in principle cannot determine by any means from which box the photons come except by their polarization. Imagine so that we make a measurement behind the source to determine the polarization of the signal and idler photons. If we set the signal analyzer to measure $|D_s\rangle$, we understand from the principle of superposition that we will also measure $|D_i\rangle$ at the idler with a deterministic outcome since the photons are all in phase ("$|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$"). The anti-diagonal polarization $|A\rangle$ will never occur, but if we instead measure either $|H_s\rangle$ or $|V_s\rangle$ it is obvious that also $|H_i\rangle$ or $|V_i\rangle$, respectively, will be measured with a deterministic outcome, and never $|D_i\rangle$. This is because we can now determine (distinguish) from the result of the signal measurement if the photon was horizontal or vertical so that the superposition at the idler becomes destroyed. If this gedanken experiment worked one should observe that superluminal communication is possible: Depending on the type of measurement made on the signal side, either H/V-basis or D, it would immediately (with zero delay) affect the idler side to give either $|D_i\rangle$ and $|A_i\rangle$ randomly, or $|D_i\rangle$ deterministically, respectively, if always measured in the D/A-

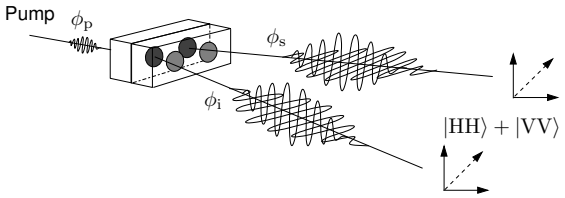

Figure 2.10: Illustration of how superposition between product states creates entanglement.

basis. In the statistical limit of many photon pairs sent, the signal side could send a message to the idler side by agreeing on encoding N random outcomes in a row as `0`, and N deterministic outcomes as `1`, with a high probability of success. In conclusion, what we would need to have created is the state $(|\mathrm{HH}\rangle + |\mathrm{VV}\rangle)/\sqrt{2}$, that when rotated to D/A-basis looks like $|\mathrm{DD}\rangle$ and not $(|\mathrm{DD}\rangle + |\mathrm{AA}\rangle)/\sqrt{2}$ for superluminal communication to be possible.

No-cloning

So, why is it not possible? We can see the pump as a polarized input state to a copying machine U that from the vacuum state $|\psi_0\rangle$ produce two polarized outputs, signal and idler: $U|V_\mathrm{p}\rangle|\psi_0\rangle = |V_\mathrm{s}\rangle|V_\mathrm{i}\rangle$ and $U|H_\mathrm{p}\rangle|\psi_0\rangle = |H_\mathrm{s}\rangle|H_\mathrm{i}\rangle$. For a perfect copy machine we would also expect $U|D_\mathrm{p}\rangle|\psi_0\rangle = |D_\mathrm{s}\rangle|D_\mathrm{i}\rangle$, hence providing superluminal communication indeed. This is not how the best quantum copy-machine work, and instead from linearity in quantum theory we get $U|D_\mathrm{p}\rangle|\psi_0\rangle = U(|H_\mathrm{p}\rangle + |V_\mathrm{p}\rangle)|\psi_0\rangle = |H_\mathrm{s}\rangle|H_\mathrm{i}\rangle + |V_\mathrm{s}\rangle|V_\mathrm{i}\rangle \neq |D_\mathrm{s}\rangle|D_\mathrm{i}\rangle$ which is (only) an entangled state. This proves that the process of spontaneous parametric downconversion (and any other process for that matter) is forbidden to act as a cloning machine. It is the fact that the process is *spontaneous* that prohibits it from being a cloning machine; instead, it seems that the entangled state is the closest we get to having two clones. In fact, we have just showed that we could perform superluminal communication if we had two identical clones, and therefore, we draw the conclusion that two clones cannot even exist, nor be created. Note how we distinguish two clones from two identically prepared quantum systems. No-cloning has been proven rigorously by Wootters and Zurek [1982]. For a comprehensive review, see Scarani *et al.* [2005]. No-cloning is a direct consequence of the uncertainty principle: If an unknown state could be cloned, then many copies of a state could be made so that each dynamical variable could be measured with an arbitrary precision and violate the uncertainty principle. Nevertheless, to compensate Nature has provided us with entanglement, which still have very useful properties that are exploited intensely today.

What prevents the downconversion process from being a cloning machine is that the the signal and idler are created randomly in phase with respect to each other,

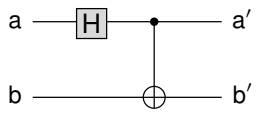

Figure 2.11: General Bell-state creation.

but, importantly, with their sum of phases still correlated with the phase of the pump. With this fact in mind, as each of the two possible processes $|\mathrm{HH}\rangle$ and $|\mathrm{VV}\rangle$ are both perfectly correlated individually, it is simply a natural consequence that also any of their superpositions exhibits correlations, but randomly what kind. As soon as a subsystem (signal) is detected in some particular state, we will know for sure from the phase correlation via the pump photon the state of the other subsystem (idler). As we can readily observe, classically correlated states in superposition is simply what we refer to as entanglement.

Quantum computation and communication

In classical circuit theory the controlled-not gate, or XOR, creates correlations between the two input bits. A target input bit value of `0` will come out with the same value as the control bit, `0` or `1`. What is unique for the corresponding quantum gate (CNOT) is that it also accepts superposition states, allowing to perform calculations on qubits. In quantum computation this effect can be used to create entanglement. Figure 2.11 shows a circuit to transform a product state into a non-separable entangled state, using a CNOT-gate and an additional Hadamard transform. The CNOT gate is said to realize a non-separable operation. It is an equivalent circuit for the process of spontaneous parametric downconversion, where the control qubit is the pump photon and the target qubit is the vacuum state. A CNOT does not realize a cloning device, but simply an entangling operation. The CNOT transform is non-separable operation in the sense that $U_{\mathrm{CNOT}} \neq U_{\mathrm{A}} \otimes U_{\mathrm{B}}$, due to its non-linearity, which is also an important property of spontaneous parametric downconversion. In essence, entanglement is a resource of non-linearity, and vice versa. However, as we shall discuss in Chapter 3 the non-linearity is in general a very weak effect in most physical systems, especially for photonic qubits through the Kerr-effect or spontaneous parametric downconversion. It was therefore a breakthrough when Knill *et al.* [2001] showed that it suffice with linear optics (single-photon states, beamsplitters, detector feedback etc.) to provide the same effect, and enable optical quantum computation via an optical CNOT [O'Brien *et al.*, 2003]. Linear optics quantum computing has turned into a lively area of research in strong need for single-photon sources and entanglement. As we will return to later, entanglement via linear optics can only be achieved probabilistically. We should also stress the importance of being able to efficiently implement the NOT-gate and the CNOT-gate,

as they form a universal set of gates for quantum computation, meaning that the two alone suffice to create any other type of logic.

There are four important maximally entangled states in the two-qubit space, called the Bell-states, which are created from a product state using the circuit in Figure 2.11,

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{2.17a}$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \tag{2.17b}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \tag{2.17c}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{2.17d}$$

What we have seen be due to the principle of no-cloning is that an entangled state is an entangled state also upon a rotation of both qubits into some other basis. All the four Bell-states have this property. The last state is special in that it is invariant upon a two-qubit rotation, that is, its form remain the same in any basis because of its anti-symmetry. Experimentally, either of these states can be created simply by rotating one of the qubits accordingly. However, the following results is important:

Fundamental law of quantum communication. *Using only local operations and classical communication, the total amount of entanglement between two separate qubits can never be increased.*

This is a general rule that distinguish entanglement as a resource of quantum correlations that can only be locally refueled. Another related results important to quantum communication is the fact that if we have a set of states that are only partially entangled, we can gain a subset of more entangled states from the first by the process of purification. This purification ideally needs the CNOT gate but can be implemented to work probabilistically via linear optics [Pan *et al.*, 2001, 2003], or via filtering [Kwiat *et al.*, 2001].

2.5 Information and cryptography

In cryptography it is essential with correlations. If two parties have a correlated string of bits at their hand that nobody else knows the values of, they can use this string to communicate any message absolutely secretly between each other. This is the so-called Vernam cipher, or one-time-pad [Vernam, 1926]. Let's say my bank has to provide me with my new VISA-code in binary form $V = \{1001001100111\}$(!) over plain text email, and that it happens that both I and the bank already share a number n of random bit-strings K_n which we exchanged a few years ago when I was

at the bank to authenticate myself and open my account. Hopefully the bank has kept the 3:rd bit-string $K_3 = \{1000100010001\}$ secret to be used now. By taking the XOR product $C = V \oplus K_3$ between all elements in the strings the bank can provide an encrypted string $C = \{0001101110110\}$ which looks as random as the random bit-string but is neither similar to K_3 nor to V. The information that C contains is distributed between K_3 and V; it is indeed tempting to think of K_3 and C as "classically entangled"! The bits in C are so meaningless to anyone that it could even be published in the newspaper, but only deciphered by someone knowing K_3 by evaluating $V = C \oplus K_3$. It is the only proven fully secret cipher system that exist, conditioned that the so-called *key* K_n is used only once [Shannon, 1949].

It is classically a hard problem to distribute such keys in a secure way. The asymmetrical cryptosystems (mainly RSA) were developed to solve these issues using separate keys for encryption and decryption, and on Internet today such systems are generally used to provide session keys for symmetrical cryptosystems as the digital encryption standard (DES) and advanced encryption standard (AES), which uses the same principle as the one-time-pad, but in a complex way and with much shorter keys [Stinson, 1995; Schneier, 1996]. All these cryptosystems rely on the mathematical (and unproven) assumption that factoring large numbers is hard. Indeed, the industry has to continuously keep up with the code-breakers and increase the used bit-lengths even with today's computer power. Perhaps even worse, Peter Shor's results [Shor, 1994] that quantum computers can solve factoring problems exponentially fast, have cast shadows over the whole field of cryptology, fearing that the quantum computer will eventually be implemented.

In order to appreciate quantum cryptography we should make the observation that the art of cryptography can be reduced to a problem of *key distribution* if the key can be generated fast enough and remain completely secret in the process. Actually, the better term for quantum cryptography is quantum key distribution (QKD). In Chapter 5 we will discuss different schemes of QKD that use either single qubits in the BB84 protocol [Bennett and Brassard, 1984] or entangled qubits [Ekert, 1991] to distribute raw-keys between two parties, Alice and Bob, protected from the malicious eavesdropper Eve.

The history of quantum cryptography goes back to 1970 when Stephen Wiesner prepared a manuscript on *Conjugate coding* [Wiesner, 1983]. His abstract provides an excellent description:

> *The uncertainty principle imposes restrictions on the capacity of certain types of communication channels. This paper will show that in compensation for this "quantum noise", quantum mechanics allows us novel forms of coding without analogue in communication channels adequately described by classical physics.*

Another way of putting the well-known principle to encode bits into two non-orthogonal, or mutually unbiased bases, is to say that the information a qubit can carry is set both at the preparation stage by Alice, and at the analyzer stage by Bob. Thus, the security lies in the fact that the data is not fully recorded into the

qubit until the final measurement. If Eve tries to make an measurement she will inevitably alter the correlations in the outcomes of Alice and Bob. For a beautiful review on quantum key distribution see Gisin *et al.* [2002].

Now, the business of QKD is not as simple as to simply use quantum channels to encode qubits and decode qubits. In fact, the bits to be transferred using QKD may not be guaranteed to be kept secret at all. The only guarantee, and which is a distinguishing mark for quantum theory, via the principle of no-cloning and complementarity, is that any eavesdropping attempt by Eve necessarily introduce *errors* in the key that Alice and Bob can discover, or rather, correct and compensate for via the two separate processes of *reconciliation* and *privacy amplification*. It is not only eavesdropping that creates errors, also natural sources cause errors, and therefore reconciliation over a classical channel is needed to correct the errors in the key [Brassard and Salvail, 1994]. However, neither this step can be performed without the risk of leaking some additional information to Eve. To ensure that the final key becomes fully known only to Alice and Bob, Bennett *et al.* [1995] devised a scheme to amplify the privacy of information. This theory relies heavily on the quantification of information that Claude Shannon formulated in his famous *The mathematical theory of communication* [Shannon, 1948]. There he defines entropy H from a mathematical viewpoint to quantify the information content in a string of bits $X = \{\mathtt{0}, \mathtt{1}\}^n$ that each occur with a probability $p_\mathtt{0}$ and $p_\mathtt{1} = 1 - p_\mathtt{0}$ (see also [Cover and Thomas, 1991]):

$$H(X) = -p_\mathtt{0} \log_2(p_\mathtt{0}) - p_\mathtt{1} \log_2(p_\mathtt{1}). \tag{2.18}$$

The information that Bob's string Y provide about Alice's string X is defined by the mutual information ($p_\mathtt{0} = p_\mathtt{1} = 1/2$ for a random key)

$$I(X;Y) = H(X) - H(X|Y) = 1 + e \log_2(e) + (1-e) \log_2(1-e), \tag{2.19}$$

where e is the introduced quantum bit error rate (QBER) of the channel. Given that a certain amount of information of the key has leaked to the eavesdropper, Alice and Bob can agree on randomizing the key they share using a special type of *hash-function*, which is assumed to be known to Eve. If Alice and Bob share more information $I(X;Y)$ about the key than Eve does $I(X;Z)$, this process will produce a smaller key about which Eve has an arbitrarily small amount of information. We have performed privacy amplification. The difficult part is to estimate how much information the eavesdropper has gained before this step; various eavesdropping analysis have been done by a number of people considering individual attacks on each of the qubits (using the optimal cloning machine), and coherent (collective) attacks. For the error correction part one can assume to use a method that works on the Shannon limit, giving away at most as much information as there are errors to correct.

To provide an estimate for the maximum QBER that can be tolerated, there is a beautiful result combining two theorems by Csiszár and Körner [1978] and Hall [1995], that also constitute a security proof of QKD. The first theorem states that a

key can only be established if Alice and Bob's mutual information $I(X;Y)$ is larger than Bob and Eve's mutual information $I(X;Z) < I(X;Y)$. The second theorem is an alternative formulation of the uncertainty principle, $I(X;Z) + I(X;Y) \leq 1$, which says that Bob's information is limited by the disturbance that Eve introduces by eavesdropping on a single qubit. Combining the two with Eqn. (2.19), we get the maximumly tolerated QBER, $e_{\max} = 11\%$. This result is valid for both non-entanglement based and entanglement based QKD. More realistic assumptions on eavesdropping attacks provide instead a limit of 15%. As a motivation for using higher-dimensional states, it can be noted that the tolerated error-rate increase for higher dimensions, using the maximally unbiased bases for each dimension to encode the qudits [Cerf *et al.*, 2002].

An important conclusion for security is that the QBER may be arbitrary large; regardless if errors are due to the eavesdropper or noise, the combined effect is simply a compression of the key. As long as the QBER is below some predetermined level, Alice and Bob are still able to end up with a non-vanishing number of bits that are secure up to a predetermined level. Therefore, it is essential to keep in mind that the performances of different implementations of QKD, like single qubits from faint-pulses, heralded sources, or entangled qubits in terms of empty pulses, multiphoton events, and low visibility of correlation, does not affect the security of the system, only the final bit-rate.

Chapter 3

Preparation of qubits

To prepare a qubit we need a quantized and coherent system consisting of two levels. Such a system can be realized using the energy levels of an atom, the spin of particles, or any other degree of freedom as we gave examples of in the previous chapter. When it comes to choice of realization of a single qubit for the application of quantum communication we must observe that different qubits are required to be physically separable from each other. Each qubit need to be coded in a physically separate systems[1] in order to carry any meaningful information that can be read in and out from the system and distributed between a sender and a receiver. Electromagnetic fields at optical frequencies provide a perfect ground for realizing such a freely propagating and quantized system through the concept of a single photon, using any of the photon's internal or external degrees of freedom to encode the qubits, as we have seen. As we shall briefly discuss here, a single photon can be prepared in several ways. In general, what is required by the photon in terms of performance in various quantum information tasks, is that the photon is prepared in a well-defined mode both spatially and temporally. By a well-defined *spatial mode* we mean that the photon is in a global sense not emitted from some source in an arbitrary direction, and from some arbitrary position, but rather into a single mode defined by the maximum precision allowed by quantum physics via the uncertainty relations. The remaining local uncertainty of the single-mode shall not be seen as an obstacle, but an asset. Such a spatial indistinguishability is of a fundamental kind that allows qubits to exist and for operations (interactions) between different systems (photons) to occur via interference which is only possible for systems occupying the same mode. Spatially well-defined modes are also important for efficient launching of photons into single-mode optical fibers which are utilized in long distance quantum communication. Moreover, the system also needs to be in a well-defined *temporal mode*, meaning that it can be determined whether a qubit is encoded into one or more single system at a time, or that two systems can be arranged to meet at specific time-instants limited only by the tem-

[1] In a quantum computer it is not equally important for the systems to be physically separable.

poral uncertainty of the system, which in terms of the single photon is limited by the coherence length.

Perhaps the simplest way to create a single photon is by the attenuation of a coherent state, which is approximately what is emitted from a laser. If we attenuate laser-light strongly enough, we will at some point reach the stage were the probability for more than a single photon to occupy a time-interval is arbitrary low. To motivate our worry for creating multiple photons we turn to an example discussed in Chapter 5, where it is noted that it is essential for security in quantum cryptography that a qubit is not encoded onto more than a single system, as an eavesdropper could otherwise get her hand on a copy. On the other hand, we would not like to attenuate the laser-light too strongly, as this would decrease the rate of the qubits and limit the communication speed. Considering these issues, a trade-off must be made. Suppose the average number of photons is $\overline{m}$ per time interval. We know that the photon number of a coherent state is Poisson distributed, and thus the probability of detecting n single-photons per time interval will be

$$P_n = \frac{e^{-\overline{m}}\overline{m}^n}{n!}, \tag{3.1}$$

which for $\overline{m} = 0.1$ gives $P_{n\geq 2} = 0.005$, $P_{n=1} = 0.09$, and $P_{n=0} = 0.9$ as an example. We can immediately see the consequences of using an attenuated continuous-wave laser as a source of single photons. It provides no information about when a photon is emitted. But even if we pulse the laser to provide synchronization signals the source will have a very high probability of sending empty pulses if we want to keep the two-photon events low. Nevertheless, there are some advantages of such a source. As we have no intermediate steps between the laser and the source output other than attenuation, the single-photons will inherit the spatial and temporal mode of the laser which can be chosen to be single-mode. Clearly, the source is very simple to set up and use. In **Paper F** we use this kind of source to prepare qubits.

Two promising competitors among sources of single-photons worth to mention are quantum dots or dye molecules. The advantages of quantum dots (and dye molecules) are that they provide very accurate timing information and have a very low probability of two or more photons being emitted. The single photon event is triggered by an external laser pulse, which sorts these type of sources into a class of single photons *on-demand*. The disadvantage is that the probability for a single photon to be emitted is also low, and that even fewer photons are sent into, or can be collected into, well-defined spatial modes.

In this thesis we will concentrate on a third type of source, namely photons that are emitted from the process of spontaneous parametric downconversion (SPDC), also called spontaneous parametric fluorescence which we have already discussed some in the previous chapter. In SPDC, photons come in pairs, and therefore we have a perfect way of creating a single photon accompanied by a synchronization pulse. By simply detecting one of the photons in a pair we can get an electrical signal that heralds the presence of the other. Sources of this type have come to be

called *heralded* single photon sources. One such is presented in **Paper A**. The pairs of photons can also be made entangled in any chosen degree of freedom, for example in polarization or in discrete-time. Such work has been presented in **Paper D** and **Paper B**, and is also reviewed in this chapter.

In **Paper C** we have investigated the mode-structure of SPDC, both spatially and temporally, with the aim to be able to efficiently collect the emission into optical single-mode fibers. We have looked into how the source can be optimized with respect to the focusing of the beams and the bandwidths of the filters, but also how to compensate for the mostly unavoidable effect of decoherence in either the source itself, or in the quantum channel, that is, the optical fiber.

Some suitable references for the following sections are Yariv [1989]; Siegman [1993a]; Mandel and Wolf [1995].

3.1 The emission from spontaneous parametric downconversion

The atomic dipoles in a dielectric medium will generally respond linearly to an incoming electromagnetic field by creating a dielectric polarization field. In some mediums this response is also weakly nonlinear, which was found already in the 60's to be very useful for optical frequency conversion. Before then, it had already been discovered and used in the microwave region. Usually the optical medium is a crystal, hence its name, nonlinear crystal.

The nonlinearity of the dielectric polarization makes it possible for an incoming single optical field of a certain frequency to be decomposed into several optical fields at other frequencies. The inverse process is also possible, where several incoming fields interact to generate a single output optical field at the sum- or difference frequencies. In this section will will concentrate on the former type of frequency conversion to create pairs of photons. The latter type can be used to detect infrared single photons at a visible frequency [Waldebäck, 2005].

Via the strength of the so-called susceptibility χ, which is a tensor, all types of conversions can be described by the nonlinear dielectric polarization

$$P = \epsilon_0 \chi^{(1)} E + \epsilon_0 \chi^{(2)} E^2 + \cdots , \tag{3.2}$$

created by the incoming field, E, which, for two input fields, is given by

$$E = E_1 \sin \omega_1 t + E_2 \sin \omega_2 t. \tag{3.3}$$

Expansion of P using Eqn. (3.3) in Eqn. (3.2) gives,

$$\begin{aligned} P = {} & \epsilon_0 \chi^{(1)} (E_1 \sin \omega_1 t + E_2 \sin \omega_2 t) \\ & + \frac{1}{2} \epsilon_0 \chi^{(2)} [E_1^2 (1 - \cos 2\omega_1 t) + E_2^2 (1 - \cos 2\omega_2 t) \\ & \quad + 2E_1 E_2 (\cos(\omega_1 - \omega_2)t - \cos(\omega_1 + \omega_2)t)]. \end{aligned} \tag{3.4}$$

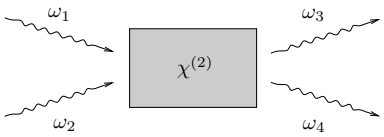

Figure 3.1: Frequency conversion in a nonlinear crystal.

As we can observe from equation Eqn. (3.4) there are harmonics, difference-, and sum-frequencies in the nonlinear term $\chi^{(2)}$: $2\omega_1$, $2\omega_2$, $\omega_1 - \omega_2$, or $\omega_1 + \omega_2$, which correspond to the frequencies of the output fields ω_3 and ω_4, see Figure 3.1. As seen, there are several possible combinations that produce different frequencies. Second harmonic generation (SHG) of a field at $2\omega_\mathrm{p}$ from a single input field at ω_p is a particularly simple case where $\omega_1 = \omega_2 = \omega_\mathrm{p}$ gives $P_\mathrm{SHG} = 2\epsilon_0\chi^{(2)}E_\mathrm{p}^2\cos 2\omega_\mathrm{p}t$, neglecting the linear and constant terms. Another case is called sum-frequency generation (SFG) for which $\omega_1 = \omega_\mathrm{p}$ and $\omega_2 = \omega_\mathrm{s}$ gives $P_\mathrm{SFG} = \frac{1}{2}\epsilon_0\chi^{(2)}[E_\mathrm{p}^2\cos 2\omega_\mathrm{p}t + E_\mathrm{s}^2\cos 2\omega_\mathrm{s}t + 2E_\mathrm{p}E_\mathrm{s}(\cos(\omega_\mathrm{p}-\omega_\mathrm{s})t - \cos(\omega_\mathrm{p}+\omega_\mathrm{s})t)]$, where we have $\omega_\mathrm{p} + \omega_\mathrm{s} = \omega_3$. Spontaneous parametric downconversion, which we will focus on here, can be described by setting $\omega_1 = \omega_\mathrm{p}$ and $\omega_2 = \omega_\mathrm{vac}$, using the vacuum (in very loose terms since vacuum does not really have a frequency). We get $P_\mathrm{SPDC} = \frac{1}{2}\epsilon_0\chi^{(2)}[E_\mathrm{p}^2\cos 2\omega_\mathrm{p}t + E_\mathrm{vac}^2\cos 2\omega_\mathrm{vac}t + 2E_\mathrm{p}E_\mathrm{vac}(\cos(\omega_\mathrm{p}-\omega_\mathrm{vac})t - \cos(\omega_\mathrm{p}+\omega_\mathrm{vac})t)]$. Any of the last two terms give the output $\omega_\mathrm{p} = \omega_\mathrm{s} + \omega_\mathrm{i}$, where the two output fields for historical reasons are called signal, $\omega_\mathrm{s} = \pm\omega_\mathrm{vac}$, and idler, ω_i, and the input field is called pump, ω_p. If we do not include the vacuum field in Eqn. (3.3) for SPDC we readily observe that the dielectric polarization fail to produce other frequencies, and so, even without knowledge of quantum theory we get a hint of that a fourth fluctuating field is actually needed to describe the process. The vacuum also explains why the process is spontaneous. The process is called parametric generation (PG) if the crystal is placed inside a cavity such that the signal is feedback. Another related process commonly used is parametric amplification (PA), which avoids any problems associated with vacuum by feeding ω_2 using ω_s, such that $\omega_3 = \omega_1 - \omega_2$. All the latter type of processes are a kind of difference frequency generation (DFG). When ω_s is a weak seeding field we attain a gain in the medium and the process is no longer spontaneous, but stimulated.

It is natural to ask under what conditions each of these processes occur. The answer is that all processes will occur as long as they obey the energy conservation $\omega_1 + \omega_2 = \omega_3 + \omega_4$. But, a problem that generally arise in dispersive mediums, is that the photon fields created will drift apart as they propagate through the crystal. For SPDC ($\omega_\mathrm{p} \to \omega_\mathrm{s} + \omega_\mathrm{i}$) this means that the signal and idler fields created at one place in the crystal will interfere destructively with fields created at another place, so that no conversion takes place. We thus need the fields to *phase-match*, which can be arranged if they have the same refractive index such that the wavevectors

add up, $\boldsymbol{k}_\mathrm{p} = \boldsymbol{k}_\mathrm{s} + \boldsymbol{k}_\mathrm{i}$. In a birefringent crystal the refractive index varies with the frequency and the direction of polarization. Thus it can happen for some specific propagation directions that each of the three fields travel at a speed (phase velocity) that makes the phases match up along the whole length of the crystal. This is called *birefringent* phase-matching. The direction changes with the frequency of the fields, which is why the emission reminds of a rainbow. The inverse process, $\omega_\mathrm{s} + \omega_\mathrm{i} \rightarrow \omega_\mathrm{p}$, is now also phase-matched but will not become significant until the signal and idler fields have grown strong enough, which will happen only after a very long distance in the crystal is reached. The needed distance is shorter for strong pump powers. These effects are all illustrated in Figure 3.2, showing the photon flux as function of distance.

The conversion efficiency in the forward direction

We shall shortly show how the graph in Figure 3.2 was generated using the coupled mode equations that governs the nonlinear interaction. Let us begin by assuming that there exist a total field energy function that relates to the dielectric polarization as

$$P = \nabla_E \, U(E), \tag{3.5}$$

where P is the same as in Eqn. (3.4). The nonlinear interaction Hamiltonian becomes

$$\hat{H}_P(t) = \int_V U(E) \, \mathrm{d}^3 r = \int_V \chi^{(2)} \hat{E}_\mathrm{p}^{(+)} \hat{E}_\mathrm{s}^{(-)} \hat{E}_\mathrm{i}^{(-)} \mathrm{d}^3 r \; + \mathrm{H.c.}, \tag{3.6}$$

where the three interacting electrical fields propagating along the z-axis are given in a quantized form using the annihilation and creation operators,

$$\hat{E}_\mathrm{p}^{(+)} = \hat{a}_\mathrm{p}(t) e^{i(k_\mathrm{p} z - \omega_\mathrm{p} t)}, \tag{3.7a}$$

$$\hat{E}_\mathrm{s}^{(-)} = \hat{a}_\mathrm{s}^\dagger(t) e^{-i(k_\mathrm{s} z - \omega_\mathrm{s} t)}, \tag{3.7b}$$

$$\hat{E}_\mathrm{i}^{(-)} = \hat{a}_\mathrm{i}^\dagger(t) e^{-i(k_\mathrm{i} z - \omega_\mathrm{i} t)}. \tag{3.7c}$$

By neglecting the annihilation terms for the signal and idler, as well as the creation term for the pump, we implicitly make an assumption of the validity of the slowly varying envelope approximation (SVEA), already at this stage. Without to affect the final results we shall also in the following derivation ignore the fact that the fields are annihilated and created with a random phase. The Hamiltonian becomes

$$\hat{H}_P(t) = \chi^{(2)} \int_{-\infty}^{\infty} \delta(z - z') e^{-i\Delta k z} \mathrm{d}z \; \hat{a}_\mathrm{p} \hat{a}_\mathrm{s}^\dagger \hat{a}_\mathrm{i}^\dagger \underbrace{e^{-i(\omega_\mathrm{p} - \omega_\mathrm{s} - \omega_\mathrm{i})t}}_{0} + \mathrm{H.c.}, \tag{3.8}$$

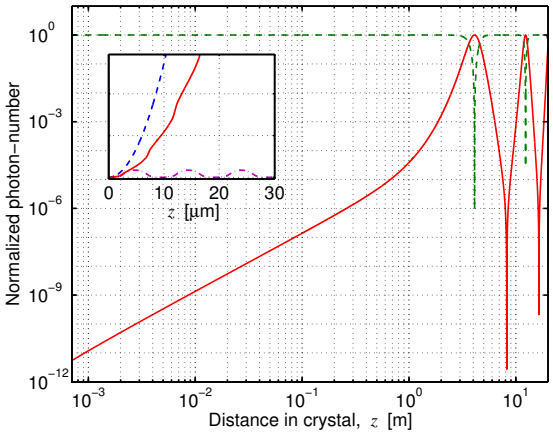

Figure 3.2: The average and normalized photon number of the emission from spontaneous parametric downconversion versus the distance of propagation in the nonlinear crystal. To the right can be seen the effect of the inverse process where the signal and idler (solid line) converts back into the pump (dashed line). The efficiency with which downconversion takes place for realistic crystal lengths ($\sim$ mm) is very small, about 10^{-10}. The inset shows the growth of photon number for perfect phase-matching, $\Delta k = 0$ (dashed line), quasi-phase-matching (solid line) and no phase-matching at all, $\Delta k \gg 0$ (dashed-dotted line).

where we have assumed perfect frequency matching, $\omega_{\rm p} = \omega_{\rm s} + \omega_{\rm i}$. The total Hamiltonian consists of the energy in all of the fields plus the energy in the dielectric polarization,

$$\hat{H}(t) = \sum_m \hbar\omega_m(\hat{a}_m^\dagger \hat{a}_m + \frac{1}{2}) + \hat{H}_P(t) + \text{H.c.} \tag{3.9}$$

Heisenberg's equation of motion will describe how the field operators evolve,

$$\frac{\mathrm{d}\hat{A}}{\mathrm{d}t} = -\frac{i}{\hbar}[\hat{A}, \hat{H}], \tag{3.10}$$

where $\hat{A} = \hat{a}_{\rm s}e^{-i\omega_{\rm s}t}$, $\hat{A} = \hat{a}_{\rm i}e^{-i\omega_{\rm i}t}$, and $\hat{A} = \hat{a}_{\rm p}^\dagger e^{i\omega_{\rm p}}$, each one put into Eqn. (3.10) leads to the coupled mode equations:

$$\frac{\mathrm{d}\hat{a}_{\rm s}}{\mathrm{d}t} = -i\frac{g}{2}\hat{a}_{\rm i}^\dagger \hat{a}_{\rm p}, \tag{3.11a}$$

$$\frac{\mathrm{d}\hat{a}_{\rm i}}{\mathrm{d}t} = -i\frac{g}{2}\hat{a}_{\rm s}^\dagger \hat{a}_{\rm p}, \tag{3.11b}$$

$$\frac{\mathrm{d}\hat{a}_{\rm p}}{\mathrm{d}t} = -i\frac{g^*}{2}\hat{a}_{\rm s}\hat{a}_{\rm i}, \tag{3.11c}$$

where $g = \chi^{(2)} e^{-i\Delta k z'}$, and $\Delta k = k_\mathrm{p} - k_\mathrm{s} - k_\mathrm{i}$. Let further $t = z'/c$, such that z' can be used for the horizontal axis in the graph. We have used the commutation relation $[\hat{a}_m, \hat{a}_n] = [\hat{a}_m^\dagger, \hat{a}_n^\dagger] = 0$, and $[\hat{a}_m, \hat{a}_n^\dagger] = \delta_{m,n}$. The first two equations of Eqn. (3.11) represents the down-conversion process, and the last equation represents the inverse conversion process, allowing for a depletion of the pump. The flux of photon pairs will be given by the average of the photon number operator $\hat{n}_m = \hat{a}_m^\dagger \hat{a}_m$, as

$$\bar{n}_m = \langle 0, 0, n_\mathrm{p} | \hat{n}_m | 0, 0, n_\mathrm{p} \rangle. \tag{3.12}$$

The average photon number is plotted in Figure 3.2 as a function of distance in the crystal for a perfect phase-matching condition, $\Delta k = 0$. The vertical axis is normalized to the initial photon number of the pump, thereby also representing the efficiency by which one pump-photon is converted into one signal and one idler photon. We also observe from Eqn. (3.12) that the photon-flux grows with the pump-power. In the absolute forward direction of propagation ($\Delta k = 0$) Figure 3.2 suggests that the photon-flux P is proportional to L^2. The situation gets more complicated for the total flux as we need to then integrate over all $\Delta k \geq 0$. In contrast to the textbook knowledge presented thus far, much less is understood for the behavior of the photon-flux for emission coupled into optical fibers. This is part of our original work, which we will return to in Section 3.6.

Types of phase-matching

In the foregoing discussion we have ignored the polarizations of the fields. However, the nonlinearity $\chi^{(2)}$ is a tensor that describes the strength in different polarization directions. The nonlinearity of a uniaxial crystals is rotationally invariant around the optic axis, which is defined by the two polarization components called ordinary, o, and extraordinary, e, polarization. The ordinary component is in a plane perpendicular to the optic axis, and the extraordinary component is in a plane parallel to the optic axis. As described by the tensor, different combinations of polarization directions of the pump and the emission lead to different strengths in nonlinearity. And because the refractive indices are polarization and frequency dependent, it will also change the phase-matching conditions, giving different kinds of rainbow patterns in the emission. Two such combinations that both gives high non-linearity are classified as type-I and type-II phase-matching processes. The first type of process can be described as $e_\mathrm{p} \rightarrow o_\mathrm{s} + o_\mathrm{i}$, where the pump is extraordinary and both the signal and idler are ordinary. The second process can be described as $e_\mathrm{p} \rightarrow e_\mathrm{s} + o_\mathrm{i}$, in which the signal and idler have different polarizations. Figure 3.3 shows these two types of processes, where each circle represents a different wavelength of the emission within a relatively small bandwidth. Some wavelengths are output as cones and others as spots, usually in a non-colinear fashion, which means that the propagation directions of the beams deviate from the direction of the pump beam. Still, it is very advantageous in many cases that all three beams propagate colinearly. In type-I phase-matching this is achieved for the wavelengths of signal and idler that

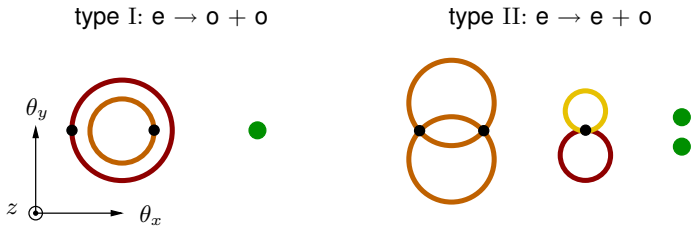

Figure 3.3: Types of phase-matching in a single crystal configuration. The emission is described by the x and y components of the polar angle θ, see Figure 3.5.

are emitted in the absolute forward direction. The two beams can have different wavelengths and become spot-like. In type-II phase-matching spot-like beams can only be achieved non-colinearly because of the different polarizations of the beams [Vellekoop, 2002]; thus, colinear emission is instead found in the intersection of two cones. In general, a colinear geometry allows easier alignment and spot-like beams allows efficient coupling into single-mode fibers, which makes both desirable. Before ending this discussion we should note that the particular wavelengths which are emitted in a particular geometry change with the incident angle of the pump beam with respect to the optic axis of the crystal, and also by the temperature of the crystal.

As an example, Figure 3.4 shows an experimentally obtained profile of the emission in type-II phase-matching in a β-BaB_2O_4 crystal (BBO). The different images are taken by an infrared CCD camera in an experiment with 2×1550 nm photons, described in Section 3.4. Each image correspond to different angles of incidence, using the same frequency filter. Notice the spot-like emission in the rightmost image. Some other types of uniaxial crystals used in birefringent phase-matching include potassium dihydrogen phosphate, KH_2PO_4 (KDP) and potassium niobate, $KNbO_3$.

Quasi-phase-matching

The work in **Paper A** through **Paper D** use instead the technique of *quasi-phase-matching* (QPM) to achieve colinear emission. The principle behind QPM is most easily understood by taking a few steps back and observe what makes a process *not* phase-matched; namely, the fact that the signal, idler and pump drift out-off phase after some distance in the crystal due to unmatched refractive indices and therefore interfere destructively. If we reverse the nonlinearity, that is, invert the dielectric dipoles in the crystal after some distance in the crystal, the signal and idler can be made to drift in-phase again. This process has to be repeated periodically in order for the photon-flux to grow continuously. The behavior of such a growing photon

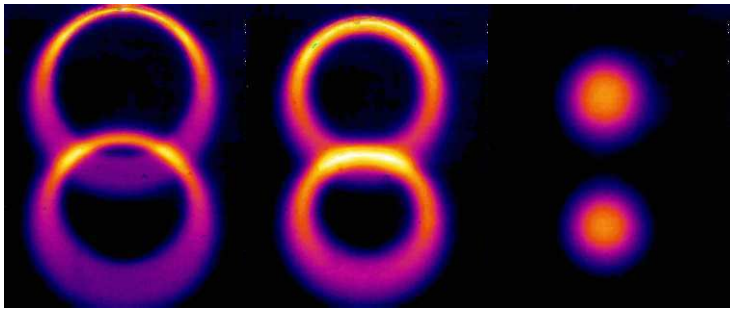

Figure 3.4: The electrical field distribution of the emission in type-II spontaneous parametric downconversion. The images were obtained with an InGaAs-CCD camera placed a few centimeters behind the nonlinear crystal in the experimental setup showed in Figure 3.19. The frequency filter bandwidth was 10 nm FWHM (full-width half maximum).

flux is found in the inset of Figure 3.2. The poling is achieved by applying voltage pulses across the crystal in a pattern that is determined by a photoresist placed on top of an unpoled crystal. Via the electro-optic effect, the poling is monitored by observing changes to the polarization of an external laser beam passing through the sample [Karlsson *et al.*, 1999]. For periodically poled materials, the spatial variation of the non-linear index, $\chi^{(2)}$, is in the order of a few μm in length, and has relatively sharp boundaries for a squared grating pattern. This periodic structure will enter mathematically as a quasi k-vector in the non-linear index, $\boldsymbol{K} = 2\pi/\Lambda\ \boldsymbol{e}_z$, where Λ is the grating period. For future use we will express $\chi^{(2)}$ expanded by its Fourier-series components

$$\chi^{(2)} = \chi_2\ f(\boldsymbol{r}) = \chi_2 \sum_{m=0}^{\infty} f_m e^{-im\boldsymbol{K}\cdot\boldsymbol{r}}, \tag{3.13}$$

and then do a sinusoidal approximation using the first term only,

$$\chi^{(2)} = \chi_2\ f_1 e^{-i\boldsymbol{K}\cdot\boldsymbol{r}}. \tag{3.14}$$

The condition for quasi-phase-matching becomes $\boldsymbol{k}_\mathrm{p} = \boldsymbol{k}_\mathrm{s} + \boldsymbol{k}_\mathrm{i} + \boldsymbol{K}$. The great advantage with QPM is that we can design specifically what wavelengths should phase-match colinearly by changing the period of the poling Λ. The disadvantage is that the photon-flux does not grow as fast as in perfect phase-matching, however, this is generally not a problem since QPM can be made to access other elements of the non-linearity tensor, that are much stronger. The crystal used in the work of this thesis is made from potassium titanyl phosphate which has the chemical formula $KTiOPO_4$, abbreviated KTP (PPKTP when being periodically poled). The

KTP material, which is transparent in the region 350 μm to 3 μm, is a typical example of a biaxial crystal in which there are three crystal axes needing to be specified, X, Y, and Z, see Figure 3.5. We will refer to these axes for the beam polarizations. The process that is phase-matched in our work is $Z_{\rm p} \rightarrow Z_{\rm i} + Z_{\rm s}$. Another crystal material popularly used in poled structure is lithium niobate, $LiNbO_3$, in short PPLN. Quasi-phase-matched materials have a shorter history than birefringent phase-matched materials because of the stronger technological challenges in manufacturing, however, the knowhow has rapidly advanced over the last years. PPLN has been on the market for some time now, and PPKTP has just become a commercial product. For the use in quantum communication it is still relatively few research groups, apart from us, that have investigated their potential for photon-pair generation, especially KTP [Kuklewicz *et al.*, 2004]. The KTP crystals we are using were made in-house at KTH by the group of F. Laurell [Fragemann, 2005].

It is interesting to take note of the problem of photorefractive damage which may occur at high powers or very strong focusing of the pump beam. It can be explained by the photorefractive effect, which is an effect where the strong pump intensity knocks out electrons from the valence band of the atoms in the bright areas in the crystal where the pump-beam propagates. The electrons become free to move around and will create a net-drift toward the dark regions in the crystal. The electrons build up a field with the holes that are left behind, which changes the dielectric polarization and, in turn, the refractive index. The crystal will thus not phase-match correctly and no output is seen. KTP has been shown to have relatively high resistance to the effect of photorefractive damage, and accordingly, we have not observed this effect for our pump-powers. The effect decreases with temperature, which makes another reason for heating the crystal apart from the adjustment of exact phase-matching.

Angular and frequency spectrum

Up to here, we have discussed several things: what types of processes that occur in birefringent and quasi-phase-matching, the growth of photon-flux with crystal length, and the general emission characteristics for each type of process. We will now analyze the characteristics of the emission a little more carefully, following **Paper C**. The main problem considered in this paper is how well the emission of quasi-phase-matched SPDC can be coupled into single-mode optical fibers. The problem is important in quantum communication, where one wants as many of the photon pairs as possible collected by the fibers. The obstacle against simply increasing the pump power to compensate for low collection efficiency, is that low collection efficiency itself limits the joint probability of getting both photon pairs into the fibers, which makes the source less efficient in heralding the presence of a single photon, or in creating entanglement. The solution to this problem is to couple identical modes of the signal and the idler into the fibers, leading to a problem of optimization. The obvious parameter to optimize with respect to maximum collection efficiency, is the focusing condition of the pump mode and the

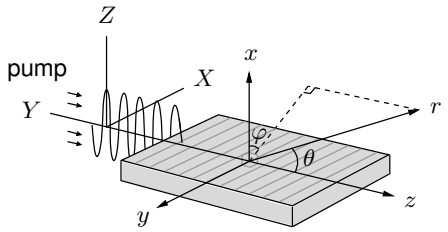

Figure 3.5: The coordinate system used in the analysis of the emission of signal and idler photons from a periodically poled crystal. The crystal's axes X, Y, and Z are used as a reference for the polarization of the incoming and outgoing optical fields.

fiber-matched modes. This was realized already before Boyd and Kleinman [1968], who thoroughly investigated the effects of focusing in parametric generation. In terms of SPDC as used for quantum information applications, the problem has been addressed by several other groups [Monken *et al.*, 1998; Pittman *et al.*, 1996; Aichele *et al.*, 2002; Kurtsiefer *et al.*, 2001; Bovino *et al.*, 2003; Dragan, 2004; Castelletto *et al.*, 2004]. To simplify the analysis, it is a standard method to apply a short crystal approximation, which means that the crystal is considered sufficiently short for the pump beam to be a plane wave for a particular focusing, leaving only the transverse form of the field in the calculations. Recently, however, it has been a growing interest for using long crystals as they are expected to generate more photons (see further Section 3.6). Hence, several groups have tried to determine the behavior of the emission using the same model as for short crystals, thereby needing to justify the validity of the approximation in ambiguous ways. Instead, we have employed a full analysis similar to Boyd and Kleinman, and as expected, our results show a similar geometrical behavior as theirs, in contrast to the other work. We will soon return to this problem in Section 3.2.

To that end, we need a way of describing the structure of the emission, preferably in terms of the angular and frequency spectrum. In order to determine the evolution of the state, commonly referred to as the two-photon amplitude, or bi-photon amplitude, we will use Schrödinger's picture instead of Heisenberg's, together with the interaction Hamiltonian. The procedure will lead to a final density matrix describing the state of the signal, the idler, or both. Throughout the derivations all three interacting electrical fields are decomposed into plane waves, which can naturally represent the focusing of a Gaussian beam. We also take into account the temporal information via the frequency dependencies of the k-vectors and the filter amplitudes $A(\omega)$. To describe the angular part of the spectrum, we will use the internal polar angle θ and the azimuthal angle φ, for each the signal and idler, using the spherical coordinate system shown in Figure 3.5. The following derivation simply sketches the procedure. For further details please refer to **Paper C**.

The evolution of the number state vector is given by

$$|\psi\rangle = \exp\left[-i\frac{1}{\hbar}\int_{t_0}^{t_0+T} \mathrm{d}t\ \hat{H}_P(t)\right]|\psi_{00}\rangle$$
$$\approx \left(\mathbb{1} + \frac{1}{i\hbar}\int_{t_0}^{t_0+T} \mathrm{d}t\ \hat{H}_P(t)\right)|\psi_{00}\rangle, \tag{3.15}$$

where $|\psi_{00}\rangle$ is the state at time t_0, T is the time of interaction, and $\hat{H}_P(t)$ is the Hamiltonian given by Eqn. (3.6). The three interacting electrical fields including spatial and temporal information can be written

$$E_{\mathrm{p}}^{(+)} = \sum_{\boldsymbol{s}_{\mathrm{p}}} A_{\mathrm{p}}(\boldsymbol{s}_{\mathrm{p}}) e^{i(k_{\mathrm{p}}\boldsymbol{s}_{\mathrm{p}}\cdot\boldsymbol{r}-\omega_{\mathrm{p}}t+\phi_{\mathrm{p}})}, \tag{3.16a}$$

$$\hat{E}_{\mathrm{s}}^{(-)} = \int \mathrm{d}\phi_{\mathrm{s}} \int \mathrm{d}\omega_{\mathrm{s}} A(\omega_{\mathrm{s}}) \sum_{\boldsymbol{s}_{\mathrm{s}}} e^{-i(k_{\mathrm{s}}\boldsymbol{s}_{\mathrm{s}}\cdot\boldsymbol{r}-\omega_{\mathrm{s}}t+\phi_{\mathrm{s}})} \hat{a}_{\mathrm{s}}^{\dagger}(\omega_{\mathrm{s}}, \boldsymbol{s}_{\mathrm{s}}), \tag{3.16b}$$

$$\hat{E}_{\mathrm{i}}^{(-)} = \int \mathrm{d}\phi_{\mathrm{i}} \int \mathrm{d}\omega_{\mathrm{i}} A(\omega_{\mathrm{i}}) \sum_{\boldsymbol{s}_{\mathrm{i}}} e^{-i(k_{\mathrm{i}}\boldsymbol{s}_{\mathrm{i}}\cdot\boldsymbol{r}-\omega_{\mathrm{i}}t+\phi_{\mathrm{i}})} \hat{a}_{\mathrm{i}}^{\dagger}(\omega_{\mathrm{i}}, \boldsymbol{s}_{\mathrm{i}}). \tag{3.16c}$$

From Eqn. (3.15) the number state becomes

$$|\psi\rangle = |\psi_{00}\rangle + G_2 \hat{a}_{\mathrm{s}}^{\dagger}\hat{a}_{\mathrm{i}}^{\dagger}|\psi_{00}\rangle = |\psi_{00}\rangle + G_2|\psi_{11}\rangle, \tag{3.17}$$

where G_2 is the unnormalized amplitude for the two-photon number state obtained by inserting Eqn. (3.14) into Eqn. (3.6) and then Eqn. (3.6) into Eqn. (3.15),

$$G_2 = \langle\psi_{11}|\psi\rangle = \frac{1}{i\hbar}\int_0^T \mathrm{d}t \int_V \mathrm{d}^3 r\ \chi_2\ f_1 e^{-i\boldsymbol{K}\cdot\boldsymbol{r}} E_{\mathrm{p}}^{(+)} E_{\mathrm{s}}^{(-)} E_{\mathrm{i}}^{(-)}. \tag{3.18}$$

Using Eqn. (3.16) the number state amplitude Eqn. (3.18) can be simplified as

$$G_2 = \iint \mathrm{d}\omega_{\mathrm{s}} \mathrm{d}\omega_{\mathrm{i}} \sum_{\boldsymbol{s}_{\mathrm{s}}} \sum_{\boldsymbol{s}_{\mathrm{i}}} S(\omega_{\mathrm{s}}, \omega_{\mathrm{i}}, \boldsymbol{s}_{\mathrm{s}}, \boldsymbol{s}_{\mathrm{i}}). \tag{3.19}$$

Our goal now is to arrive at an expression for the amplitude S as it also enters in the state of frequency and angular spectrum of the form

$$|\psi_{\omega,\boldsymbol{s}}\rangle = \iint \mathrm{d}\omega_{\mathrm{s}} \mathrm{d}\omega_{\mathrm{i}} \sum_{\boldsymbol{s}_{\mathrm{s}}} \sum_{\boldsymbol{s}_{\mathrm{i}}} S(\omega_{\mathrm{s}}, \omega_{\mathrm{i}}, \boldsymbol{s}_{\mathrm{s}}, \boldsymbol{s}_{\mathrm{i}}) |\omega_{\mathrm{s}}\rangle|\omega_{\mathrm{i}}\rangle|\boldsymbol{s}_{\mathrm{s}}\rangle|\boldsymbol{s}_{\mathrm{i}}\rangle. \tag{3.20}$$

The so called two-photon amplitude S can be simplified as

$$S(\omega_{\mathrm{s}}, \omega_{\mathrm{i}}, \theta_{\mathrm{s}}, \theta_{\mathrm{i}}, \Delta\varphi) = \chi_2\ f_1 A(\omega_{\mathrm{s}}) A(\omega_{\mathrm{i}}) A_{\mathrm{p}}(\theta'_{\mathrm{p}}, \varphi'_{\mathrm{p}})$$
$$\times\ L\ \mathrm{sinc}\left[\frac{L}{2}\Delta k'_z\right] \frac{4\pi^2}{i\hbar}\delta(\omega_{\mathrm{s}} + \omega_{\mathrm{i}} - \omega_{\mathrm{p}}), \tag{3.21}$$

where

$$\Delta k_z' = k_\mathrm{s}\cos\theta_\mathrm{s} + k_\mathrm{i}\cos\theta_\mathrm{i} - k_\mathrm{p}^Z\sqrt{1-(P^2+Q^2)} + K, \tag{3.22}$$

$$\theta_\mathrm{p}' = \arcsin\sqrt{P^2+Q^2} = \arccos\sqrt{1-(P^2+Q^2)}, \tag{3.23}$$

and

$$P^2+Q^2 = \frac{k_\mathrm{s}^2\sin^2\theta_\mathrm{s} + k_\mathrm{i}^2\sin^2\theta_\mathrm{i} + 2k_\mathrm{s}k_\mathrm{i}\sin\theta_\mathrm{s}\sin\theta_\mathrm{i}\cos(\Delta\varphi)}{(k_\mathrm{p}^Z)^2}. \tag{3.24}$$

In the last equation we have introduced $\Delta\varphi = \varphi_\mathrm{s} - \varphi_\mathrm{i}$, manifesting rotationally symmetric output emission. In closing, we note from Eqn. (3.20) and Eqn. (3.21) that the two output photons, signal and idler, are entangled in both frequency and in direction of propagation.

Emission modes

We are now ready to study the modes of the emission using the two-photon amplitude that was previously derived. As an aside, we saw in Chapter 2 that Hermite-Gaussian and Laguerre-Gaussian modes both represent a convenient, and complete, basis set to encode qubits, or qudits. Some superpositions of two or more modes taken from any of the two sets will be modes that also belong to one of the sets. In principle, any such pure mode can be chosen to be coupled into a single-mode fiber, for example using phase-holograms, and thus realize a qudit of any dimension. None of the work described in this thesis have utilized such qubits yet. Instead, as a first step our primary interest has been to find out how much of the emission can be made to radiate in the fundamental Gaussian single mode, which is the mode most closely supported by single-mode fibers. It is probably fair to say that the refractive indices along the X and Y axis are approximately the same so that the emission is rotationally symmetric around the axis of propagation. Rotational symmetry is a property of Laguerre-Gaussian modes; therefore, such modes easily come to mind as a suitable basis to describe the output emission. However, for our purpose it will turn out to be even simpler to use another set of modes, namely the eigenmodes, which are found by a diagonalization of the state density matrix. In the next subsection, we will optimize the emission is such a way that the collective amount of overlap between each of the eigenmodes with the fundamental Gaussian mode is as large as possible, and in Chapter 4 we will return to these emission modes in an effort to experimentally characterize the output using the M^2 factor. All work is described in detail in **Paper C**.

We discretize the problem to cast it in a form suitable for numeric computation, by choosing N_θ discrete plane-wave modes as a computational basis of the polar angle. The two-photon state can be formulated as

$$|\psi_\mathrm{si}^{\Delta\varphi,\epsilon}\rangle = \sum_{m,n=1}^{N_\theta} S(\epsilon,\theta_\mathrm{s}^{(m)},\theta_\mathrm{i}^{(n)},\Delta\varphi)|\theta_\mathrm{s}^{(m)}\rangle\otimes|\theta_\mathrm{i}^{(n)}\rangle, \tag{3.25}$$

where the state implicitly depends on $\Delta\varphi$, and ϵ, given as two parameters. The two-photon density matrix can be readily formed as

$$\rho_{\mathrm{si}}^{\Delta\varphi,\epsilon} = |\psi_{\mathrm{si}}^{\Delta\varphi,\epsilon}\rangle\langle\psi_{\mathrm{si}}^{\Delta\varphi,\epsilon}|. \tag{3.26}$$

We shall remove all other degrees of freedom except the idler polar angle, and in the following we therefore take a partial trace over the signal in the polar angle degree of freedom to get the reduced density matrix for the idler,

$$\rho_{\mathrm{i}}^{\Delta\varphi,\epsilon} = \mathrm{Tr}_{\mathrm{s}}(\rho_{\mathrm{si}}^{\Delta\varphi,\epsilon}) = \sum_{n}^{N_\theta} \langle\theta_s^{(n)}|\rho_{\mathrm{si}}^{\Delta\varphi,\epsilon}|\theta_s^{(n)}\rangle. \tag{3.27}$$

The dependence on $\Delta\varphi$ is also removed following the standard trace-operation, which is here equivalent to a sum over density matrices,

$$\rho_{\mathrm{i}}^{\epsilon} = \mathrm{Tr}_{\Delta\varphi}(\rho_{\mathrm{i}}^{\Delta\varphi,\epsilon}) = \sum_{m}^{N_\varphi} \rho_{\mathrm{i}}^{\Delta\varphi_m,\epsilon}, \tag{3.28}$$

and by repeating the procedure in the same way with respect to frequency, we thus arrive at a final ρ_i describing the state of the idler,

$$\rho_{\mathrm{i}} = \mathrm{Tr}_{\epsilon}(\rho_{\mathrm{i}}^{\epsilon}) = \sum_{n}^{N_\epsilon} \rho_{\mathrm{i}}^{\epsilon_n}. \tag{3.29}$$

Both of these two last operations were appropriate as a consequence of the entanglement between signal and idler photons. The entanglement leads to an incoherent mixture of density matrices for each photon separately, which mathematically is equivalent to a sum of density matrices in the degree of freedom to be traced away.

The final density matrix is mixed in general, which means that it describes multimode emission, and not single-mode emission. As a density matrix is diagonalized it becomes decomposed into a sum of its coherent parts, that is, single-modes. By diagonalizing Eqn. (3.29), we therefore get a representation of the multimode emission in terms of an incoherent sum of orthogonal single-modes, weighted by their real eigenvalues. The procedure can be quantified in the following way; the reduced density matrix is first diagonalized by $\boldsymbol{T}^{-1}\rho\boldsymbol{T} = \boldsymbol{D}$, such that $\boldsymbol{T} = (|\zeta_1\rangle, |\zeta_2\rangle, \ldots, |\zeta_{N_\theta}\rangle)$ has the eigenvectors in the columns, and $\boldsymbol{D}$ has the eigenvalues λ_n in its diagonal elements. The result is a density matrix that can be represented as a sum of pure states,

$$\rho = \sum_{n=1}^{N_\theta} \lambda_n |\zeta_n\rangle\langle\zeta_n|, \tag{3.30}$$

where N_θ is the Hilbert-space dimension. The finite set, $|\zeta_n\rangle$, now forms the sought basis, which we would like to view in terms of the form of its basis-vectors. Let us

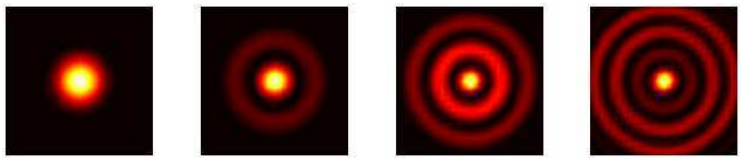

Figure 3.6: The electrical field eigenmodes of the emission generated numerically from a particular case of quasi-phase-matching at optimal focusing. The weights (eigenvalues) of each field mode are; $\lambda_0 = 0.9531$, $\lambda_1 = 0.0332$, $\lambda_2 = 0.0105$, $\lambda_3 = 0.0018$, which suggests that this emission is mostly in a single mode, in fact close to the fundamental Gaussian mode.

therefore introduce a discrete representation of these basis-kets: $\zeta_n[\theta]$, where θ is the polar angle, such that $a_{xy}[\theta] = \sum_n \lambda_n |\zeta_n[\theta]|^2$ becomes the two-dimensional angular spectral form taken as the absolute square of the modes, and $u_{xy}[\theta] = \sum_n \lambda_n |E_n[\theta]|^2$ the form of the two-dimensional electrical field, where the field amplitude $E_n[\theta]$ is the Fourier-transform of $\zeta_n[\theta]$. In rectangular components ($\theta^2 = \theta_x^2 + \theta_y^2$), the form of each field-mode becomes

$$u_n[\theta_x, \theta_y] = \lambda_n \left| E_n \left[\sqrt{\theta_x^2 + \theta_y^2} \right] \right|^2 . \tag{3.31}$$

In Figure 3.6 is shown a case of the normalized forms of the four lowest order electrical field modes, $u_n[\theta_x, \theta_y]$, as determined by Eqn. (3.31). The fundamental eigenmode, E_0, is very close to the fundamental Laguerre-Gaussian mode, as one can suspect by looking at the leftmost image.

3.2 Coupling into optical fibers

As previously stated, an important concern in quantum communication and in quantum computation using linear optics, is to prepare single photons in well-defined modes. For many applications it is necessary to collect the photons into fiber optical transmission links. The single-mode fiber defines precisely such a well-defined mode, and makes via spatial indistinguishability a perfect ground for many experiments involving interference, as most long-distance communication schemes do. We have also talked about the importance of preparing the two-photon state such that both photons of a pair will have a high probability of entering the fibers. To characterize sources of photon pairs based on SPDC and quasi-phase-matching we will make use of three parameters: single coupling, conditional coincidence, and pair coupling. In due order, the single coupling represents the fractional amount of photons collected by each fiber independent of the other. The conditional coincidence represents the fractional amount of photons, corresponding to one part of

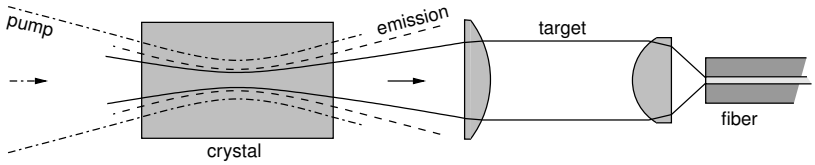

Figure 3.7: A principle sketch of fiber coupling, showing the pump beam, the crystal emission, the fiber's target-mode, and the single-mode fiber itself. The refraction at the crystal edges is neglected in the drawing.

the pairs, that are collected into its fiber conditioned upon the fact that the partner photon also entered its fiber. It is useful in the characterization of heralded single photon sources. Finally, the pair coupling represents the fractional amount of pairs for which both photons enters its own respective fiber. The last parameter finds its use in characterizing sources of entangled photon pairs. All three parameters can be optimized with respect to the focusing of the pump beam and the *fiber-matched modes*, as has been done in **Paper C**. By the latter we mean the mode of the fibers as seen from the crystal, that is to say, the form of the mode that can be traced back from the fiber to the crystal at the same time not worrying about any optics in-between that may serve to perform the actual transformation. A sketch of the principal arrangement for fiber coupling is shown in Figure 3.7. As we will soon show by determining the waist of the emission, the magnification of the optical focusing system from the fiber-tip to the crystal center needs to be in the order of unity. The single-mode fiber waist radius is a few μm and its true mode is described by a Bessel function $J_0(\alpha)$, which is defined as the solution to $\frac{1}{2\pi}\int_0^{2\pi}\exp\left(i\alpha\cos\varphi\right)\mathrm{d}\varphi$. Luckily, to simplify things somewhat, it can be approximated very well by the fundamental Gaussian mode, TEM_{00}, which is here given in the angular spectrum form,

$$|G_{00}\rangle = \frac{k^Z w_{00}}{\sqrt{2\pi}} e^{(k^Z w_{00})^2 \sin^2(\theta)/4}\ |\theta\rangle, \tag{3.32}$$

where w_{00} is the waist radius of the fiber-matched mode, and k^Z is the k-vector inside the crystal for light polarized along the Z-axis. We shall also assume the pump beam to be in the fundamental Gaussian single-mode.

Mathematically, the *single coupling efficiency* is simply the result of the standard trace operation, $\gamma = \mathrm{Tr}(|G_{00}\rangle\langle G_{00}|\rho)$, but an equally valid definition is obtained through the eigenmodes of the angular spectrum,

$$\gamma = \sum_{n=1}^{N_\theta} \lambda_n |\langle\zeta_n|G_{00}\rangle|^2, \tag{3.33}$$

where $|\zeta_n\rangle$ is given by the density matrix, ρ_s or ρ_i, as defined by Eqn. (3.30), resulting in γ_s or γ_i for the signal and idler, respectively. Eqn. (3.33) can readily be interpreted as taking the overlap between the fiber-mode and each of the eigenmodes, weighted by its eigenvalue and summed over to get the collective overlap, which will then represents the total single coupling efficiency.

The analysis above clearly takes care about the spatial degrees of freedom in terms of the angular spectrum. However, implicitly included is also temporal filtering, which enters through the frequency dependence of the k-vectors and the filter shape amplitude in Eqn. (3.21). In this respect, there is one issue worth noting that relates the filter bandwidth to the coupling efficiency, namely the observation that the emission from SPDC is spread over a wide frequency spectrum, while the interference filters used are relatively narrow-band. In that sense, there is not much meaning for any of the coupling measures to include photons which never have a chance to pass through the frequency filter. What we would like for the coupling parameters to measure, is the fractional amount of photons that enters the fibers among those that are also temporally filtered. For example, for any fixed filter bandwidth and no spatial filtering, which is almost the case for a multimode fiber, any measure of the coupling should be perfect, that is, unity. Alternatively, *without* interference filter, we could instead choose to define the coupling parameters in relation to the bandwidth of the fiber's own frequency filtering at optimal focusing, which is determined for each length of the crystal. As we have showed in **Paper C**, the fiber itself also effectively filter in frequency via its spatial filtering. This is because there is a connection between the direction of the wavevectors and their frequency. We will return to this problem in Section 3.6.

Before we continue with the problem of optimization, and its main results, we shall also in more detail define what we call *conditional coincidence*, $\mu_{i|s}$, which is useful for the characterization of heralded single photon sources. In words, the conditional coincidence is defined as the probability to find one photon of a pair in its fiber given that the partner photon has entered the fiber. In the following example, we will hence condition the idler photon upon detection of a signal photon, in accordance with our heralded photon source. The signal photon entering the fiber can be described mathematically by the following measurement operator,

$$M_\mathrm{s} = |G_{00}^{(\mathrm{s})}\rangle\langle G_{00}^{(\mathrm{s})}|. \tag{3.34}$$

Starting from Eqn. (3.26), we will first remove the frequency and azimuthal degrees of freedom, leading to the two-photon density matrix, $\rho_\mathrm{si} = \mathrm{Tr}_{\Delta\varphi,\epsilon}(\rho_\mathrm{si}^{\Delta\varphi,\epsilon})$. We can then perform the measurement accordingly and get the conditional two-photon state,

$$\rho_{\mathrm{si|s}} = \frac{M_\mathrm{s}\otimes\mathbb{1}_\mathrm{i}\rho_\mathrm{si}M_\mathrm{s}\otimes\mathbb{1}_\mathrm{i}}{\mathrm{Tr}(M_\mathrm{s}\otimes\mathbb{1}_\mathrm{i}\rho_\mathrm{si}M_\mathrm{s}\otimes\mathbb{1}_\mathrm{i})}. \tag{3.35}$$

We continue by taking the partial trace over the signal to get the conditional state of the idler, $\rho_{\mathrm{i|s}} = \mathrm{Tr}_s(\rho_{\mathrm{si|s}})$. The conditional coincidence can now be defined in a

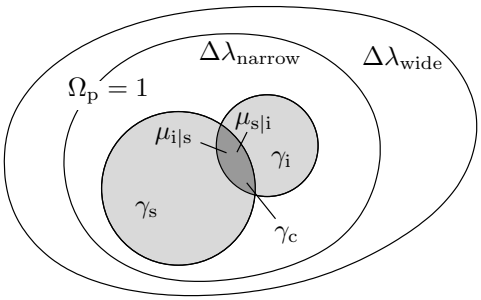

Figure 3.8: The figure shows a Venn diagram that is used to illustrate the single coupling efficiencies γ_{s} and γ_{i}, pair coupling γ_{c}, and conditional coincidences $\mu_{\text{s|i}}$ and $\mu_{\text{i|s}}$ as a fractional number representing the area of a set of elements. Each element represents a pair of photons generated by the crystal within the bandwidth of the detector filter $\Delta\lambda$, that can be either wide or narrow.

similar way as the single coupling,

$$\mu_{\text{i|s}} = \sum_{n=1}^{N_\theta} \lambda_n |\langle \zeta_n | G_{00}^{(\text{i})} \rangle|^2, \tag{3.36}$$

except this time, $|\zeta_n\rangle$ is given by the diagonalization of $\rho_{\text{i|s}}$.

Finally, we have the pair coupling, which is defined as the probability to find both photons of a pair in the respective fibers. The pair coupling is most simply derived in terms of the single and conditional coupling applying Bayes's rule,

$$\gamma_{\text{c}} = \mu_{\text{i|s}}\gamma_{\text{s}} = \mu_{\text{s|i}}\gamma_{\text{i}}. \tag{3.37}$$

Analytically simple, but more computationally more demanding[2], is to define the conditional coupling as $\gamma_c = \text{Tr}(M_{\text{s}} \otimes M_{\text{i}} \rho_{\text{si}})$, where M_{i} is given similar to Eqn. (3.34).

A graphical illustration of coupling

In **Paper C** and **Paper B** we also introduced a graphical way to illustrate the problem of photon collection. It is based on the concept of Venn diagrams, reproduced in Figure 3.8. The figure shows the different types of coupling efficiencies represented as sets of elements, where each element of a set represents a photon pair generated by the crystals in some spatial mode. That is, the collection of all

[2]It is quite cumbersome to do the numerical calculations since we need the whole description of the two-photon state, ρ_{si}, which is very large for the needed resolution. For $\gamma_{\text{s,i}}$ and $\mu_{\text{i|s}}$, only the reduced density matrix in one of the subsystems, $\rho_{\text{s,i}}$ or $\rho_{\text{i|s}}$, is needed.

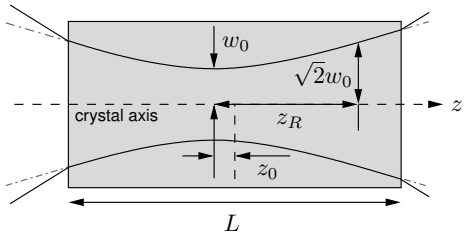

Figure 3.9: The geometry of focusing. The focusing parameter of the pump mode or fiber-matched modes is defined as $\xi = L/z_R$, where L is the length of the crystal and z_R is the Rayleigh-range.

elements within each set defines the pairs that are coupled into the fiber for some specific focusing condition in such a way that the coupling efficiency corresponds to the total area of the set. The elements contained in a specific set represent photon pairs that are coupled into a fiber taken from the universal set of pairs, $\Omega_{\rm p}$, which contains all pairs generated by the crystal within the bandwidth of the detector filter $\Delta\lambda$. The set $\Omega_{\rm p}$ is normalized to unity and represents perfect coupling of all pairs into the fiber. The union of the two sets represent photon pairs that both are coupled into the fibers.

It is also in place to discuss the procedure of optimization of the focusing before the numerical results. For this purpose, Figure 3.9 shows a sketch of the geometry of a Gaussian beam propagating through the crystal. The beam profile defines the general parameters involved in focusing of a beam apart from the wavelength; namely the beam waist radius, w_0, and the beam waist location, z_0. These parameters characterize both the pump's mode and the signal's and idler's fiber-matched modes, which can all of course all have different waists. To quantify the focusing we have used the following dimensionless parameter,

$$\xi = \frac{L}{z_R}, \tag{3.38}$$

where L is the length of the crystal and z_R is the Rayleigh-range of the pump, signal, or idler. (It was first introduced in this context by Boyd and Kleinman [1968], but in a slightly different form than here.) The maximum achievable coupling efficiencies are determined by the optimization of Eqn. (3.33) or Eqn. (3.36) with respect to the focusing parameter[3] for the pump $\xi_{\rm p}$, signal $\xi_{\rm s}$, and idler $\xi_{\rm i}$, respectively,

$$\gamma^{\rm opt} = \max_{\xi_{\rm s,i}} \ \gamma(\xi_{\rm p}, \xi_{\rm s,i}), \tag{3.39}$$

and similarly,

$$\mu^{\rm opt} = \max_{\xi_{\rm s,i}} \ \mu(\xi_{\rm p}, \xi_{\rm s,i}), \tag{3.40}$$

where in both cases,

$$\xi^{\mathrm{opt}} = \underset{\xi_{\mathrm{s,i}}}{\arg\max}\ \mu(\xi_{\mathrm{p}}, \xi_{\mathrm{s,i}}). \tag{3.41}$$

In connection, we should note that all the three coupling parameters assume perfect temporal correlation (i.e. time-matched conditional gating) and perfect frequency correlation (i.e. matched filters), so that the optimization only covers the spatial degrees of freedom. Returning shortly to the geometrical picture with this object, the consequence is that the pair coupling γ_{c}, in general, is completely disconnected with the single coupling, γ_{s} and γ_{i}, because the latter two do not represent uncorrelated events. To be more precise, and complicate the use of the diagram somewhat, we point out the fact that each element represents a pair that consist of two parts, each belonging to different subsystems that are not addable in a strict sense. Nevertheless, the picture using the Venn-diagram is still valid for many types of sources, and is helpful for purpose of illustrations and thinking. As should be clear from Figure 3.8, $\gamma_{\mathrm{c}} \neq \gamma_{\mathrm{s}}\gamma_{\mathrm{i}}$ in general, which stands in contrast to the not too uncommon assumptions used in the literature to estimate photon-rates. The diagram supports the intuitive feeling obtained by most experimentalists tweaking the system for maximum coincidence rates, namely, that it is not necessarily best to optimize each arm individually to get the largest coincidence rate, but rather, to simultaneously optimize both arms.

The main results for the single coupling of the idler, γ_{i}, is shown in Figure 3.10 for different focusing conditions of the pump beam and the idler's fiber-matched mode. The graph was generated from a numerical simulation that had to run for about two days on a standard personal computer[4]. The calculation was set to simulate a non-degenerate phase-matching condition, supporting the wavelength combination of 532 nm, 810 nm, and 1550 nm for the pump, signal, and idler, respectively, in a periodically poled $KTiOPO_4$ crystal. For each sample in the plot, the idler fiber focusing was optimized using Eqn. (3.39), to find the maximum coupling $\gamma_{\mathrm{i}}^{\mathrm{opt}}$. As observed, the same maximum coupling value can be attained for any length of the crystal by setting the pump-beam waist radius accordingly. The straight lines indicate that the optimal focusing parameters of the pump, ξ_{p}, and the idler fiber focusing, $\xi_{\mathrm{i}}^{\mathrm{opt}}$, are both constants, which means that the geometry of the beam profile in relation to different crystal lengths should stay fixed at optimal focusing. The maximum efficiency is about 95% for $\xi_{\mathrm{p}} = 0.9$ and $\xi_{\mathrm{i}}^{\mathrm{opt}} = 2.4$. Interestingly, we observe that as long as the fiber focusing is matched to the pump focusing, for any given length of the crystal, the coupling efficiency will reach $> 45\%$ irrespectively of the pump focusing, which is illustrated by the minimum value of γ_{i} in Figure 3.10. This fact may very well explain the relatively high efficiencies nevertheless achieved in many fiber-based SPDC-setups for which the

[3] Details on how ξ relates to the emission modes, $|\zeta_n\rangle$, via w_0 and z_0 can be obtained in **Paper C**.

[4] Pentium4, 1.8GHz, 256Mb

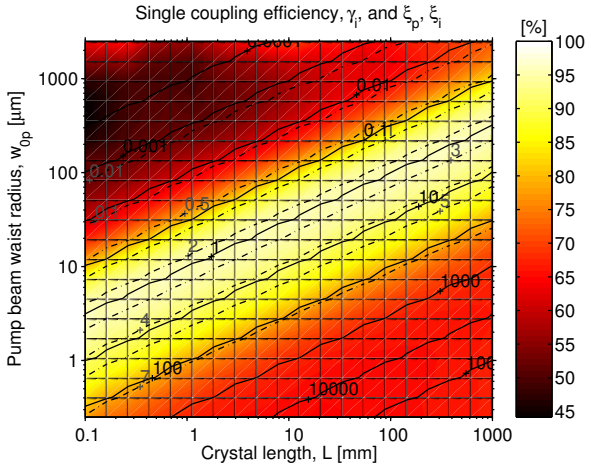

Figure 3.10: The single coupling efficiency of the idler, γ_i^{opt}, for a narrow filter bandwidth, $\Delta\lambda_{narrow}$, showing that about 95% of the photons are possible to collect into single-mode fiber at optimal pump focusing, $\xi_p \approx 1$ (solid lines), and idler focusing, $\xi_i^{opt} \approx 2$ (dash-dotted lines), when emitted from a PPKTP crystal. The numbers in the graph indicate the value of ξ for each line.

experimentalist have perhaps not worried about changing the pump's focusing, but solely the fiber coupling. However, the graph shows the importance of also optimizing the pump in order to "squeeze all the juice" from the crystal.

When and why is the emission single-mode?

In essence, the general result of optimal focusing can be stated as maintaining a fixed geometrical relation between the crystal length and the beam modes. Not surprising, there is also an intuitive understanding behind the result, which was not really presented in **Paper C**. Before we make an attempt to present it, a comment on the effects of frequency filtering shall be of help: As is apparent from the two-photon state, Eqn. (3.21), the angular spectrum of the emission is described by a sinc-function term. Considering a focused pump beam and a finite filter, there will be many such sinc-functions describing the emission, one for each plane wave component and one for each frequency component. The sinc-functions pertaining to frequency will add up incoherently in a complicated manner and hide our following reasoning, which has its goal to illustrate when and why the emission becomes multimode or single-mode without looking to frequency. Therefore, to that end, the frequency part shall effectively be ignored by looking only at a single frequency component (i.e. an infinitely narrow filter). The graph in Figure 3.10 was also generated using an infinitely narrow filter as we did not want to show the effects of

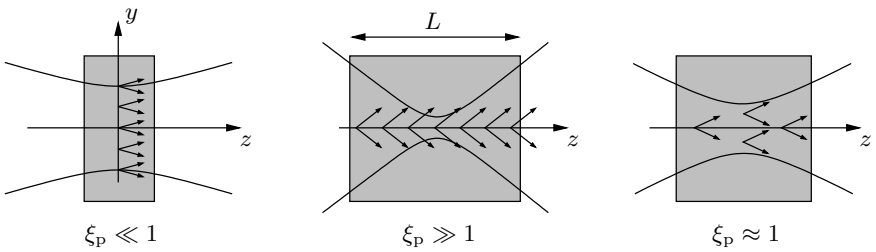

Figure 3.11: Transverse multimode, longitudinal multimode, and single-mode emission for different focusing conditions of the pump, ξ_p. The arrows represent the emission and the profile represents the pump beam, ignoring refraction at the crystal ends.

a finite filter bandwidth; namely that the coupling efficiency then decreases beyond a given length of the crystal. The effects of filtering are instead studied in Section 3.6 in terms of the photon flux.

Recall from the reasoning in Chapter 2, that a zeroth order Gaussian shaped angular spectrum mode defines a spatially coherent single-mode volume, transversely and longitudinally. Imagine then the artificial case where the angular spread of the emission, and thus its "volume", is described by a single sinc-function. Because the sinc-function closely resembles a real Gaussian function at some point, it will also closely define a single-mode at that point. This single-mode can be transformed to overlap nearly perfectly with the fundamental single-mode of the fiber using only simple optical components, and consequently, represents an ideal coupling situation.

In a real situation, having a *focused* pump beam, imagine instead a collection of several such sinc-functions (still describing the angular spread of the emission) that originate from many plane waves, and which have their propagation direction and transverse location defined by the phase-matching conditions. We find three extremes: For very weak focusing (essentially a single plane wave of the pump), the emission is described by many sinc-functions pointing in the same direction, but located along the transverse direction in the crystal. Hardly any of them overlap, and thereby they collectively define transverse multimode emission, leading to bad coupling efficiency. Refer to the leftmost picture of Figure 3.11, for $\xi_p \ll 1$.

Another case is that of strong focusing, where the many different sinc-functions points in all different directions, depending on the spread of the plane waves of the pump, but are located in the same transverse position. As the many differently directed sinc-functions are overlaid with each-other they collectively define longitudinal multimode emission, which neither couples well into a fiber. Refer to the middle picture of Figure 3.11, for $\xi_p \gg 1$.

Clearly, multimode emission will occur for both extremes of focusing, weak as strong. Luckily, as we have shown, there is a certain focusing which defines

optimum, $\xi_{\mathrm{p}} = 1$. At this intermediate spread of plane pump waves, all the different sinc-functions will overlap nearly perfect in the sense that they are pointing more or less in the same direction, and they are more or less emanating from the same spot. It turns out that the emission is well described by a single sinc-function, which implies good coupling efficiency according to the argumentation above. Thus, the emission is first-order coherent to a high degree, or in other words, in a pure state with a Gaussian shaped angular wave-function. Refer to the rightmost picture of Figure 3.11, for $\xi_{\mathrm{p}} \approx 1$.

Regarding the conditional coupling efficiency, $\mu_{\mathrm{i|s}}$, (that is, the probability of collecting the idler photon, given that its partner signal photon is in the fiber) the results show it is mainly set by the corresponding single coupling efficiency, γ_{i}, under the condition that the pump is focused optimally. As showed, γ_{i} approaches unity as the focusing of the idler is adjusted towards its optimal, implying that $\mu_{\mathrm{i|s}}$ also approaches unity. The result is the same when interchanging the roles of signal and idler. In terms of modes, the conclusion is that both the signal and idler will be emitted into the same single-mode at optimal focusing, in fact, to a large part the fundamental single-mode. If the pump is *not* focused optimally, the result is less clear. However, in our example, a high value of $\mu_{\mathrm{i|s}}$ can, in general, still be attained at some specific idler focusing, as long as the signal focusing is matched to the pump focusing. As we point out in **Paper C**, it is important to note that the numerical results in our example are valid only for a frequency filter at the signal side, and none on the idler. If two Gaussian shaped matched filters are used on each side, the maximum conditional coupling efficiency, and also the pair coupling, will be limited to $1/\sqrt{2} = 71\%$ as a result of the overlap of two equal Gaussian probability distributions.

Other conclusions about the pair coupling efficiency, γ_{c}, follows from the graph in Figure 3.12. Readily, we observe that a value close to 100 % can only be attained when both the signal and the idler are optimally focused. By the help of the Venn-diagram we can also observe that the pair coupling is bounded from above according to $\gamma_{\mathrm{c}} \leq \min(\gamma_{\mathrm{s}}, \gamma_{\mathrm{i}})$, which means that it is imperative that also the pump-focusing is optimal to attain a high γ_{c}.

With that, we will leave the theory for a while, and instead summarize the experimental work done towards realizations of sources of heralded photon pairs, and entangled qubits.

3.3 Heralded qubits

Previously we have dealt with the problem of spatially defining a single-photon originating from SPDC. There is also the problem of temporal definition, which will be the topic of this section.

As said earlier, sources of single-photons are fundamentally important in all areas of quantum information dealing with photonics. The different types of sources that are available all have different properties like repetition rate, single-photon

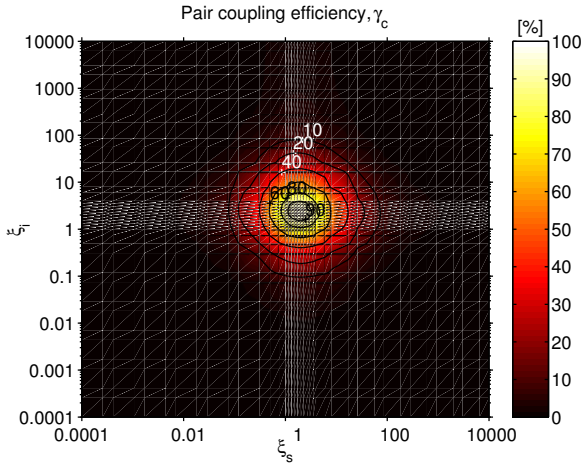

Figure 3.12: The pair coupling $\gamma_c = \mu_{i|s}\gamma_s$ at a pump focusing of $\xi_p = 1.3$, which is a trade-off between what is optimal for the pump in the case of signal and idler single coupling, respectively. The maximum γ_c is about 97%, at optimal focusing $\xi_{s,i} \approx 2.0$, using a narrow signal filter, $\Delta\lambda_{narrow}$, and no idler filter.

probability, and emission frequency. In **Paper A** we report on a source of single-photons based on emission of photon pairs in SPDC. Similar work include Mason *et al.* [2002]; Fasel *et al.* [2004a]; Alibart *et al.* [2005]. The idea can be simply stated as having one of the single-photons of a pair announced its presence by the detection event of its partner. The name "heralded" originates from the fact that the single-photons are not created on demand with a synchronous pulse, but rather, that they are asynchronously signaled for their presence by an external pulse. Asynchronous here means that the time-interval between different pulses is unspecified from pulse to pulse — a fact that may very well limit the usefulness of such sources, but ideas for storing photons in controlled fiber-loops have been suggested to overcome the problem [Pittman *et al.*, 2002]. First some background:

We have already mentioned the problems associated with attenuated coherent laser light as a generator of single-photons, such as the high probability of empty pulses resulting from the Poisson distribution in photon number. In some work on single-photon generation, it has been suggested to use a short-pulsed laser and SPDC to get synchronous pulses containing single photons [U'Ren *et al.*, 2004; Pittman *et al.*, 2004]. Once a photon is detected in the signal, one knows for sure there is a photon in the idler and thereby one can avoid empty pulses to a high degree. However, short pulses generally makes the emission coherent within the whole length of the pulse, so that stimulated emission will be dominant. Stimulated emission has a photon number distribution similar to thermal light and therefore

bunching effects are present. Bunching means that photons tend not to come alone, but several at a time. Such a property is unwanted, especially for the application of quantum key distribution, and therefore pulsed lasers are not ideal to use either. In essence, thermal distribution in photon number for pulsed lasers arise if: (i) the crystal length is too long (which makes the coherence length longer), (ii) the filter is too narrow, or (iii) the pulse length is too short. The theory of parametric amplification has been treated thoroughly in this context by Mollow and Glauber [1967].

Along those arguments we would instead like to choose a relatively long coherence length of the pump (representing, in a way, really long pulses), like is the case for a continuous wave (CW) laser. Even for relatively narrow frequency filtering of the emission, the coherence length of the emission will be much smaller than the gate-period of the detector. In such a case we have an incoherent collection of a large number of coherent "sources", each thermally distributed in photon number, but collectively giving Poisson distribution. The distribution will be Poissonian if we have (i) sufficiently short crystals, (ii) sufficiently wide filters, and (iii) sufficiently long gate-period. For realistic numbers this will most often be the case.

Now, as suggested, we would like to apply conditional (heralded) gating to such a source. It is shown in **Paper A** that by heralded gating we can modify the statistics (distribution of photon number) even further, to show either bunching, Poissonian, or *antibunching* depending on the size of the time-interval we choose to look at. Antibunching is a purely quantum physical phenomena, which, as its name suggests, is the opposite of bunching. Antibunching means that the single-photons tend to come alone, and not just after or just before another one, considering sufficiently small time-intervals. Obviously, for our purposes this is a desired effect. (Single photons from dye molecules, or quantum dots, exhibits this feature naturally, in contrast to the artificial effect created here by post-selection of sub-statistics.) The size of the needed time-interval to reach antibunching is set by the detector gate-period under the condition it is longer than the coherence time of the photons, and depends on the overall photon rate as shall be clear from the discussion following Eqn. (3.52).

Two things need to be noted. First, the asynchronousness in the time-intervals are due to the random nature of photon number distribution in the emission of SPDC. As the photon pairs from the crystal are Poisson distributed, the same distribution will thus be provided in the heralding detection events. Second, we still have the probability of getting empty pulses if the partner does not make it into its fiber, but as we have shown previously it is primarily an experimental challenge to increase the coupling efficiency and the transmission rate, and not a fundamental problem. In contrast, for attenuated weak coherent pulses the problem of empty pulses is fundamental. In order to appreciate the description of our heralded source and its benchmark numbers, we need to understand some of the theory behind, which is surprisingly rich with probabilities.

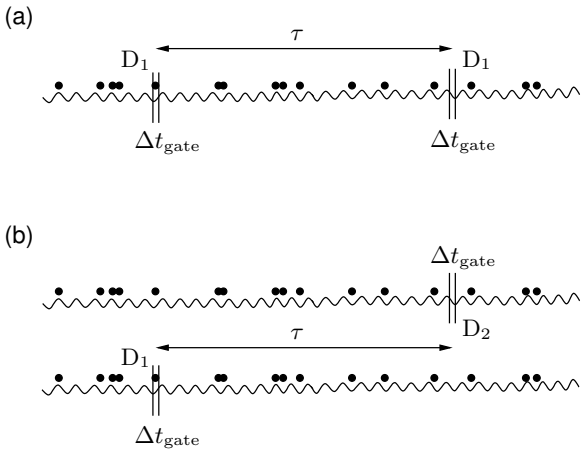

Figure 3.13: (a) Autocorrelation of an optical field, and (b) cross-correlation between two optical fields, both at field levels where the detectors D_1 and D_2 registers single photon counts within the gate-period, Δt_{gate}.

Photon correlations

The properties of any state of light can be described by correlation functions, and so can the statistics of photon counts. Such a function measures the degree to which a field is correlated with itself, or with another field, and can, for example, be found by putting a detector in front of an optical field and register intensity for different time-delays τ. In the context here, there are mainly two correlations to worry about. First, the normalized second-order autocorrelation function $g_{\text{a}}^{(2)}(\tau)$, illustrated by Figure 3.13a, that use a single detector to measure the correlation of the field. Secondly, the normalized second-order cross-correlation function $g_{\text{c}}^{(2)}(\tau)$, illustrated by Figure 3.13b, that use two detectors to measure the correlation between two fields. Hanbury-Brown and Twiss made pioneering experiments [Hanbury Brown and Twiss, 1956c,a,b] in which they showed intensity correlation in starlight between two different spatially separated observers. They proved that indeed bunching occurs for starlight, being a thermal source. The experiment was similar to the scheme showed in Figure 3.14, that splits light from one source into two different detectors. The autocorrelation function of the incoming light can be derived from the measured cross-correlation between the two detectors, compare Figure 3.14 with Figure 3.13. The true and continuous autocorrelation function is found in the limit of infinitely small detector integration times (gate-periods), $\Delta t_{\text{gate}} \to 0$. The graph in Figure 3.14 shows the case of thermal (solid line) and Poissonian (dashed line) distributions, that are allowed by the semi-classical de-

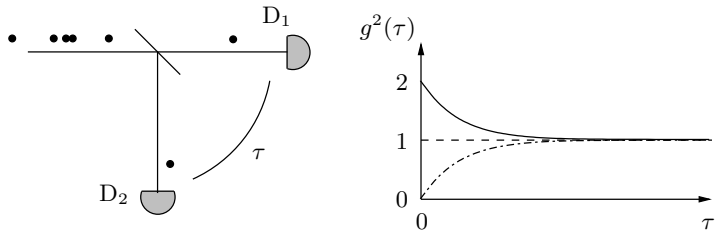

Figure 3.14: The setup shows Hanbury-Brown and Twiss's experiment to measure correlation statistics of an optical light field (at the single photon level), and the graph sketches the correlation function for thermal light showing bunching (solid line), uncorrelated light showing Poisson distribution (dashed line), and non-classical light showing antibunching (dash-dotted line).

scription of light.

In the semi-classical picture, still dealing with continuous fields, the second-order autocorrelation function [Mandel and Wolf, 1995] is given by

$$g^{(2)}(t_1, t_2) = \frac{\langle I(t_1)I(t_2)\rangle}{\langle I(t_1)\rangle\langle I(t_2)\rangle}, \tag{3.42}$$

where $I(t)$ is the field intensity at some time t, and $\langle I(t)\rangle$ denotes the ensemble average of a random process $I(t)$. Rearrangement gives

$$\langle I(t_1)I(t_2)\rangle = \langle I(t_1)\rangle\langle I(t_2)\rangle g^{(2)}(t_1, t_2), \tag{3.43}$$

or

$$\langle I(t_1)I(t_2)\rangle = \langle I(t_1)\rangle\langle I(t_2)\rangle(1 + |\gamma(t_1, t_2)|^2), \tag{3.44}$$

where $\gamma(t_1, t_2) = \frac{\langle E^*(t_1)E(t_2)\rangle}{[\langle I(t_1)\rangle]^{1/2}[\langle I(t_2)\rangle]^{1/2}}$ is the first-order degree of coherence of the electrical field E between times t_1 and t_2, which we have already denoted $\tau = t_2 - t_1$ as most processes we are dealing with here are stationary and does not depend on the absolute time. Because γ relates to $g^{(2)}$ by an absolute sign, it means that $g^{(2)}$ can not yet describe correlation outside the semi-classical sense, being above unity,

$$g^{(2)}(\tau) = 1 + |\gamma(\tau)|^2, \qquad 0 \leq \gamma(\tau) \leq 1. \tag{3.45}$$

Poisson distributed light is completely random and without correlations, therefore $\gamma(\tau) = 0$ for all τ as shown by the plot of $g^{(2)}(\tau)$ (dashed line) in Figure 3.14. For thermal light, instead, we have correlation for $\tau \to 0$, i.e. $\gamma(0) = 1$, as showed by the solid line in the same graph. As $\tau \to \infty$, any light in the semi-classical

description is completely uncorrelated. Hitherto, the second-order correlation has been possible to express in terms of a first-order correlation.

To explain antibunching, which occurs for an heralded source, we need to modify Eqn. (3.45) as

$$g^{(2)}(\tau) = 1 + \lambda(\tau), \qquad -1 \leq \lambda(\tau) \leq 1. \tag{3.46}$$

Antibunching can be seen as a truly quantum effects, being the result of negative probabilities and described by the new correlation function $\lambda(\tau)$ that can also attain negative values. From Eqn. (3.44) and Eqn. (3.46) we get $\lambda(\tau) = \frac{\langle I(t_1)I(t_2)\rangle}{\langle I(t_1)\rangle\langle I(t_2)\rangle}$ which is an irreducible second-order correlation function. This is somehow the inverse effect of the two-photon interference in a beamsplitter where two photons become bunched, manifesting their bosonic nature.

In the spirit of quantumness, we shall abandon the intensity of a fields in place of photon counts, which are best described in terms of probabilities of detector clicks. The previous definition of the autocorrelation function Eqn. (3.42) needs to be modified,

$$g^{(2)}(t_1, t_2) = \frac{2P_{m\geq 2}(t_1, t_2)}{P_{m\geq 1}(t_1)P_{m\geq 1}(t_2)}, \tag{3.47}$$

where $P_{m\geq k}$ is the probability to find k or more photons within the detector gate-period. The factor 2 in Eqn. (3.47) comes from the fact that the probabilities are normalized to attain the maximum value of unity, which is not the case for intensities. We can simplify Eqn. (3.47) as

$$g^{(2)}(\tau) = \frac{2P_{m\geq 2}(\tau)}{P^2_{m\geq 1}(\tau)}. \tag{3.48}$$

In a heralded source, one of the channels (the idler) will be triggered by a detection event of the other channel (the signal). Refer to Figure 3.13b and picture the lower field as the signal and the upper as the idler. The tiny dots symbolize photons. It is clear that as $\tau \to 0$ the probability for a photon in the idler will be large conditioned on a photon in the signal, and that the probability of an empty gate is very small, or even zero, if the probability that the idler photon makes it from the source to the detector is unity. If also the gate-period, Δt_{gate}, is short, the probability of two or more photon within that gate is small. We are thus interested in the autocorrelation function of the idler for $\tau = 0$, which becomes

$$g^{(2)}(0) = \frac{2P_{m\geq 2}}{P^2_{m\geq 1}}. \tag{3.49}$$

We would now like to characterize our source using this quantity, which is zero for perfect antibunching. Hence, we need to know the probabilities $P_{m\geq 2}$ and $P_{m\geq 1}$, which can be determined by the measured rates of photons in the fibers. As the

process is ergodic we can measure time averages instead of ensemble averages to find $P_{m\geq k}$. Note that by $P_{m\geq 2}$ in Eqn. (3.49) we do not care if we herald a truly correlated pair, or an accidental, which can happen for lower than unity coupling efficiencies and transmission factors into the fibers. It is shown in **Paper A** that

$$g^{(2)}(0) \approx 2[1 - e^{-\Delta t_{\rm gate}(\frac{R_{\rm i}R_{\rm s}}{R_{\rm c}} - R_0)}], \tag{3.50}$$

is a fair approximation for small products between the average rate $\bar{R} = R_{\rm i}R_{\rm s}/R_{\rm c}$ and the gate-period $\Delta t_{\rm gate}$, where $R_{\rm i}$ is the singles photon rate per second in the idler fiber, $R_{\rm s}$ is the rate in the signal fiber, and $R_{\rm c}$ is the number of correlated pairs per second in both fibers. Using the relations between the rates and coupling parameters,

$$R_{\rm i} = \delta_{\rm i}\gamma_{\rm i}R_{\rm p}, \tag{3.51a}$$
$$R_{\rm s} = \delta_{\rm s}\gamma_{\rm s}R_{\rm p}, \tag{3.51b}$$
$$R_{\rm c} = \delta_{\rm i}\delta_{\rm s}\gamma_{\rm c}R_{\rm p}, \tag{3.51c}$$

where $R_{\rm p}$ is the rate of pairs per second in free space, $\delta_{\rm s}$ and $\delta_{\rm i}$ are the transmission factors of the signal and idler respectively, together with some approximation, we are led to

$$g^{(2)}(0) \approx 2\Delta t_{\rm gate}\left(\frac{\gamma_{\rm i}\gamma_{\rm s}}{\gamma_{\rm c}}R_{\rm p} - R_0\right), \tag{3.52}$$

where R_0 is the rate of the signal detected *and* idler gated photon pairs. Again the formula is valid only for not too large gate-periods and rates. Various conclusions can be drawn; it is advantageous to maximize $\gamma_{\rm c}$ at the same time keeping $\gamma_{\rm i}$ and $\gamma_{\rm s}$ small [note: $\gamma_{\rm c} \leq \min(\gamma_{\rm i}, \gamma_{\rm s})$]. Furthermore, it is noted that $g^{(2)}(0)$ can always be made arbitrary small at the expense of the rate $R_{\rm p}$, by effectively lowering the pump power. As expected, it is also clear that $\Delta t_{\rm gate}$ should be as small as possible to achieve strong antibunching. The upper value for antibunching can be determined by the point where the light becomes Poisson distributed, $\Delta t_{\rm Poisson} = b/\bar{R}$, where $b \approx 0.5$ for coupling efficiencies and transmission factors close to unity. For example, with $\bar{R} = 10 \times 10^6$ [s^{-1}] this implies gate-periods not longer than 50 ns. For longer gate-periods the source will produce bunched photons. The value of $g^{(2)}(0)$, together with the heralding rate $R_{\rm s}$, and the conditional probability

$$\mu_{\rm i|s}^{\rm heralded} \approx 1 - \left(1 - \frac{R_{\rm c}}{R_{\rm s}}\right)e^{-\Delta t_{\rm gate}(R_{\rm i} - \frac{R_{\rm c}}{R_{\rm s}}R_0)}, \tag{3.53}$$

will benchmark the source in terms of its ability to produce exactly a single photon for every heralded event. Note that we do not need to do a full Hanbury-Brown and Twiss experiment in order to find $g^{(2)}(0)$, which is less straight forward for gated detectors [Fasel *et al.*, 2004a], all the necessary parameters are obtained by simple singles and coincidence rate measurements. The only assumption made is that the source produce single photons that are Poisson distributed in time, motivated by a gate-period much longer than the coherence time of the downconverted photons.

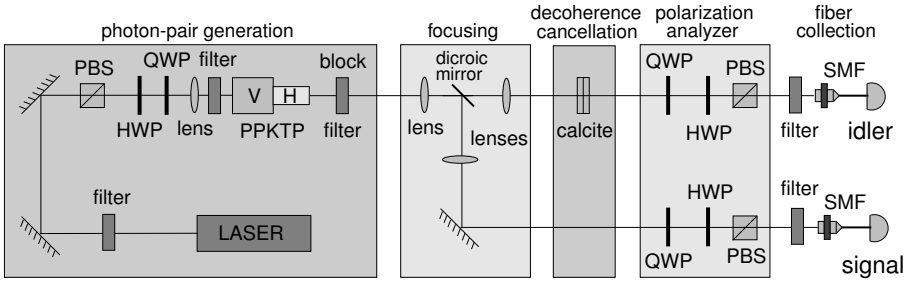

Figure 3.15: Experimental setup of the source that produce both heralded single photons and entangled photon pairs. For the heralded photons experiment only one of the crystals is needed. To characterize the entanglement from two crystals the polarization analyzers made by the rightmost quarter-wave-plates (QWP), half-wave-plates (HWP), and polarizing beamsplitters (PBS) are used. In both experiments the photons are collected by single-mode fibers (SMF).

A single-photon experiment

In this subsection I will shortly present the results of the experiment and the work done towards a single photon source implementation. I will bring some experimental issues to your attention that were not discussed in **Paper A**. The following discussion applies equally well to the experiments in **Paper B** to **Paper D**.

Figure 3.15 shows a schematic diagram of the experimental setup. The first two parts, photon pair generation and focusing, and the last part, fiber collection, are sufficient for explaining the source of heralded photons. Also, only one of the two crystals in the picture is needed. The first part consists of a spatial and temporal single mode continuous wave laser to pump the crystal. Its line-width is 0.00001 nm, corresponding to a coherence length > 100 meters. The mode is "cleaned up" in polarization and frequency using various filters and polarizing beam splitters. The laser itself is frequency doubled (Nd:YAG) from 1064 nm to produce 532 nm, and is internally pumped at 700-800 nm by solid-state laser diode. Thus, it is clear why we need to do some extra filtering to erase the last residues of these wavelengths. As the light levels are extremely low after the crystal ($\sim 10 \times 10^6$ photon pairs per second or ~ 1 pW), in a classical sense, one can understand why even a tiny fraction of unwanted light, although being several magnitudes smaller than the laser light ($\sim 1 \times 10^{16}$ photon pairs per second or ~ 5 mW), can disturb the measurements. The light exits horizontally after the polarization beam splitter and is further controlled by a half-wave-plate. Its purpose will become clear later. The lens is used to focus the pump beam onto the crystal in accordance with our predictions for producing emission in as much a single mode as possible. For the purpose of precision and greater tolerance in misalignment we use achromatic

doublet lenses. One disadvantage with such lenses, compared to ordinary lenses, is that the gluing layer used to keep the two lenses together will fluoresce when exposed to intense light. Therefore, we needed to place an extra shortpass filter (Schott glass) just before the crystal. We also found that the linear polarization of the pump was made elliptical by either the lens or the crystal, by measuring the emission. One possible explanation is that the dispersion of the lens is made non-centrosymmetric by an uneven thickness of the glue. In any case, the quarter-wave-plate is set to undo the effect. When aligned to phase-match, the crystal emits photons with the same polarization as the incoming light, i.e. horizontally in this case. After the crystal, the pump light is blocked and reduced several order of magnitudes in intensity by a long-pass filter. This component will have to define the end of the pair generation part.

To look for the emission at the initial stage we used a CCD camera to monitor any light coming in the colinear direction from the crystal. For the infrared part (idler at 1550 nm) we used an InGaAs CCD IR-detector, and for the near-infrared part (signal at 810 nm) we used a standard surveillance camera with a Si-based CCD. In practice, there are many reasons to why the light is not found at a first shot. First, assuming correct poling period of the crystal, its temperature needs to be accurate in order to phase-match at the wavelength within the rather precise bandwidths of the interference filters that sits in front of the camera to remove stray light. Second, the emission needs to be focused somewhat onto the CCD to be intense enough, and third, fluorescence again, which we found to be biggest problem. Moving the infrared camera around the setup we could find many sources of infrared light that may interfere with the downconverted light. In addition to hitting the lenses, the strong pump beam or remnants of it also hits the filters and creates fluorescence. (It is a very delicate problem to choose the right combination of filters that does the job of removing all of the pump, at the same time transmitting nearly perfect the downconverted light, which is several orders of magnitudes smaller than the pump.) There is also a lot of heat radiation from the oven which also falls into this category. Fluorescence is particularly devastating in our configuration and we find at least two reasonable explanations. First, the wavelength of the idler coincides to a large part with the main spectrum of the fluorescence, and secondly, in colinear geometries the camera or the fiber-focusing needs to be directed towards the crystal in line with every other component in the setup that may fluoresce. In contrast, in non-colinear geometries the downconversion deviates from the pump, which allows the camera or the fiber-focusing to be directed to the crystal at an angle, seeing no components along the path which are hit by the pump. In the next chapter we discuss further how the emission was characterized.

In the focusing part we made an arrangement with several lenses to achieve the desired collimation of the signal and idler beam. As described in Section 3.2, the focal length of the lenses have to be chosen so that the fiber-mode is matched with the single-mode part of the emission. In this version of the experiment we needed a double-lens configuration to increase the distance[5] between the lens system and the crystal. A dichroic mirror separates the signal from the idler into two different

$\bar{m}^{\text{poisson}}$	R_{s} [s^{-1}]	R_{i} [s^{-1}]	R_{c} [s^{-1}]	$P_{m=0}$	$\mu_{\text{i}\|\text{s}}^{\text{heralded}}$	$P_{m\geq 2}$	$g^{(2)}(0)$
-	100×10^3	97×10^3	27×10^3	0.73	0.27	0.00022	0.0060
-	147×10^3	306×10^3	71×10^3	0.52	0.48	0.00129	0.0110
0.02	-	-	-	0.98	0.02	0.00020	-
0.70	-	-	-	0.50	0.35	0.15600	-

Table 3.1: Rates, single-photon probability, and autocorrelation for the heralded source of single-photons for a pump power of 540 μW for the first row, 1.2 mW for the second, and idler gate-period of 10 ns. The last two rows show the values obtained with a weak coherent laser pulse, attenuated to a mean photon number $\bar{m}^{\text{poisson}}$.

paths. In front of the fiber couplers there are filters placed to block any remaining pump light, to remove unwanted stray light, and set the bandwidth. For alignment of the whole system the standard trick is to use backwards propagating light, hence, we connected a laser to the farther end of the fiber and aligned by adjusting the beam to pass through the same irises as the pump beam (but in opposite direction). It should be noted that the source is very alignment friendly, thanks to the colinear geometry.

To the fibers we connected single photon counters that provide an electrical output-signal upon detection of a photon. The signal photons (810 nm) are detected by a commercially available Si-based avalanche photo-diode (APD) module, and the infrared idler-photons are detected by an home-made APD-module. Concerning the home-made module, see Bourennane *et al.* [2001]. To reduce the dark-counts (noise), the home-made module is gated for a time Δt_{gate}, usually between 1 to 10 ns, at the time when the photons are expected to arrive. The exact time is decided by the signal detector, all in accordance with the previous discussion of the principle of a heralded source.

Table 3.1 summarizes the achieved rates and benchmark numbers. The first and second row are the results of the heralded source, and the last two are the results of a source based on weak coherent laser pulses, attenuated to different average photon numbers per pulse, $\bar{m}^{\text{poisson}}$, to resemble the heralded source. The first and the third row have similar probabilities for more than one photon, $P_{m\geq 2}$, within a pulse. But clearly, the heralded source has a smaller probability for empty pulses, $P_{m=0}$, and a much higher probability for pulses being filled with single photons, $\mu_{\text{i}|\text{s}}^{\text{heralded}}$. Conversely, if the single photon and empty pulse probabilities are set about the same (second and fourth row), then the probability for more than one photon is 100 times smaller in the heralded source, showing its advantage over weak coherent pulses. For further details please refer to **Paper A**.

[5] We are currently working on a version which have only one single lens in each arm, made possible using a longer crystal with weaker focusing.

I will end with a few words saying that a single-photon prepared in this way can of course also be prepared as a qubit. Using a single crystal the photon comes out in a particular known polarization which can be rotated into any other by active polarization switching using half-wave-plates. It could also be prepared as a discrete-time qubit, or a dual rail qubit, or any other representation, by suitable transformations as we saw in Chapter 2.

A final comment will naturally lead us over to the next section, namely, that for many useful purposes we can use the fact that the photon pairs are correlated in polarization. If one is horizontal, the other one is horizontal, leading to the idea to encode the idler by applying operations to the signal. For a qubit this implies that both polarizations need to be created by the crystal.

3.4 Entangled qubits

In Chapter 2 we have already discussed in length the quantum physical principle of superposition which leads to entanglement between two subsystems. Such quantum specific correlation that entanglement gives rise to can easily[6] be created by extending our source of heralded photons. The idea that we use was originally proposed by Hardy [1992], and implemented by Kwiat *et al.* [1999]. The idea starts with the observation that for two subsystems to become entangled, they need to be indistinguishable in all other degrees of freedom than the one which we would like to get entangled. For our system it is natural that the two subsystems are the signal and idler beams. They are easily separated by their wavelength information for a nondegenarate wavelength combination. The degree of freedom which is closest at hand to entangle is polarization, which is done by placing two crystals next each other, see Figure 3.16. The first crystal creates, for example, vertical (V) emission

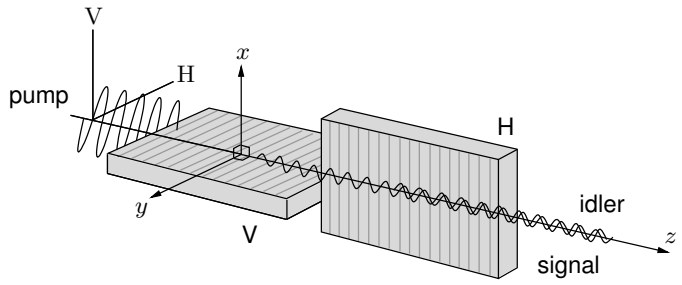

Figure 3.16: A two-crystals source that creates direct entanglement.

and the second horizontal (H) emission if the pump polarization is rotated to an angle in-between horizontal and vertical, i.e. 45°. If both of these two processes are made indistinguishable, as determined by the detector system, we will have a su-

perposition between H and V in each arm. The superposition will also contain joint correlations, as explained earlier, creating a state composed of the two subsystems that can be written in the following way,

$$|\Phi_0\rangle = \frac{1}{\sqrt{2}}(|\mathrm{H_s}\rangle|\mathrm{H_i}\rangle + |\mathrm{V_s}\rangle|\mathrm{V_i}\rangle). \tag{3.54}$$

The needed spatial indistinguishability is assured by the spatial single-mode that defines the fibers. Because of the way the spatial degree and the temporal degrees are related through the phase-matching conditions, the fibers will also perform frequency filtering. Helped by the limited timing-jitter of the detectors, the indistinguishability in frequency is thus assured.

Direct and post-selected entanglement

Sources of photon pairs that are entangled in either polarization, frequency, momentum, or time, come today in a variety of flavors, that all can be sorted into two main categories: *directly created* and *post-selectively created*. The source we started to present here belong to the first category, meaning that as soon as the photons exits the crystals they are directly entangled, without any need for selection of any subset containing only some of the pairs. The original proposal used two thin type-I phase-matched crystals, that each produce non-colinear cone-like emission. When placing the crystals so that the cones overlap spatially, the polarization entanglement will be found in any two opposite corners of the cones (or rings), representing the two spatially separated subsystems. To date, the most popular method to create polarization entanglement is via type-II phase-matching [Kwiat *et al.*, 1995]. As we have described in a previous section, the output from a single crystal in type-II phase-matching will consist of two non-overlapping but intersecting cones (see Figure 3.3). In each cone the photons are of a different polarization that the other, and since they are always generated in pairs, if one photon is H, the other one is V. By spatial selection, for example a single-mode fiber or an iris, we can make the photons in the intersection indistinguishable from each-other in any other degree of freedom than polarization. Hence, they become entangled in polarization.

To the second category falls such sources that relies on the post-selection of a subset of pairs of photons that are not entangled, but type-II correlated. For example, by sending the product state $|\mathrm{H_s V_i}\rangle = |\mathrm{H_a V_b}\rangle$ to the two input ports, a and b , of a beamsplitter, like the one depicted in Figure 2.8, and post-selecting only the events where the preceding detectors find one photon in each output arm,

$$|\Psi\rangle = \frac{1}{2}(|\mathrm{H_a}\rangle|\mathrm{V_a}\rangle + |\mathrm{H_a}\rangle|\mathrm{V_b}\rangle + |\mathrm{V_a}\rangle|\mathrm{H_b}\rangle + |\mathrm{V_b}\rangle|\mathrm{V_b}\rangle), \tag{3.55}$$

we will effectively create another of the Bell-states, similar to Eqn. (3.54),

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\mathrm{H_a}\rangle|\mathrm{V_b}\rangle + |\mathrm{V_a}\rangle|\mathrm{H_b}\rangle). \tag{3.56}$$

[6] In theory, not in practice!

The events where both photons exits on the same ports are effectively ignored if we look only to coincidence at the detectors. Such entangled states are obviously much easier to create as they do not require any interaction in the form of the non-linearity present in a crystal, but simply the generation of photon pairs combined on a beamsplitter. Nevertheless, the method has its uses since many schemes allows the selection of two-photon events where only half of the photons become entangled. We have also implemented a second source that falls into this category.

Before continuing, I would shortly like to emphasize on the beautiful connection between the post-selective generation of entanglement and non-deterministic Bell-state analysis. As we saw in Chapter 2, the process of creating entanglement can also be viewed through the function of a CNOT gate — a process in which product states are converted to non-separable (entangled) states fully deterministic. In that sense, SPDC can be seen as a (although very low) probabilistic CNOT. The reverse process is Bell-state analysis, which, obviously, requires higher probability of success than what is given by the inverse process of SPDC, and as explained further in Chapter 4, most straight forward is to use beamsplitters in the same way as described above to achieve $\sim 50\%$ success probability. The two processes are structurally identical, but each others reverse.

Let us go back to Figure 3.15 for a moment, noting that we are more or less finished describing the first part of photon pair generation. In connection to the focusing and fiber coupling parts one thing worth to mention concerns the use of the two crystals to create two orthogonal polarizations: For good entanglement in the fibers it is essential that both polarization are equally efficient coupled into the fibers. It is best illustrated by returning to the Venn-diagram; however, we shall not dig into that problem here, but instead refer to **Paper B** which includes a discussion similar to the one in relation to Figure 3.8.

There are two parts in Figure 3.15 that are yet to be dealt with. First, there is the serious problem of canceling decoherence, which will be treated in Section 3.5. In short, the crystals introduce chromatic dispersion which gives rise to temporal distinguishability between the different polarizations. The effect needs to be efficiently canceled to be able to create entanglement. Second, there are the standard polarization analyzing optics part used in detecting polarization entanglement, which is covered in Chapter 4. Instead, we jump to a discussion on how to apply the source within the context of quantum communication.

A scheme for quantum communication

Figure 3.17 shows a schematic diagram of an implementation of hybrid-coded entanglement, which is explained in detail in **Paper B**. Hybrid-coded means that qubits are encoded in polarization on one channel (signal) and discrete-time on the other (idler). As we emphasized earlier, the polarization dispersion in standard optical fibers is a major problem for sending polarization information down a fiber. Especially for quantum superpositions, which are unique to qubits, this type of decoherence will completely destroy the information as the distance increases.

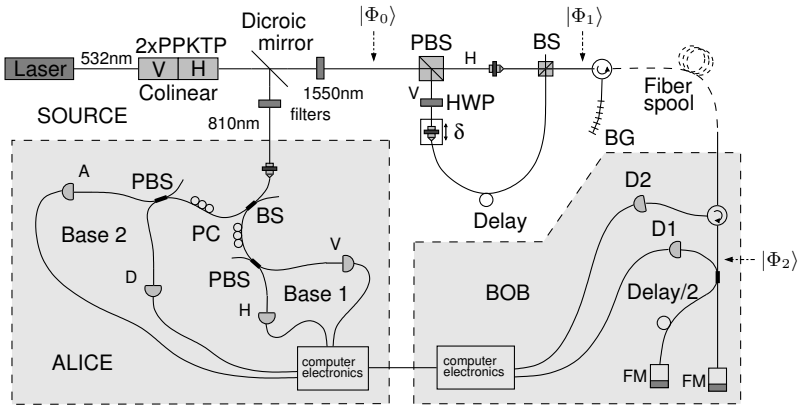

Figure 3.17: Quantum communication scheme utilizing directly created hybrid-coded entangled qubits. BS: beamsplitter; PBS: polarizing beamsplitter; HWP: half-wave-plate; BG: Bragg grating; FM: Faraday mirror.

Therefore, we need some other representation for qubits to be sent over long distance. In the above scheme the polarization encoded photons are converted into discrete-time representation. But only on the idler side (Bob). There is no fundamental reason to why two different subsystem should need the same representation for their entanglement to remain. Moreover, it is suitable to keep the polarization encoding on the signal side (Alice) if these photon are not to be transfered over any distance, as it makes the detection configuration simple. Alice's side is equipped with a single fiber to collect the emission, together with polarizing beamsplitters, polarization controllers, and an ordinary beamsplitter. The ordinary beamsplitter selects between the two non-orthogonal bases, V/H and D/A, that are required for quantum key distribution.

On Bob's side there is one preparing interferometer and one analyzing interferometer for the discrete-time qubits. Both are unbalanced, meaning that the path length of one arm is longer than the other. Instead, both interferometers have equal path-differences between each's arms. We shall see how this leads to three different time-slots, where a single qubit (photon) can take either the long-long path, the short-short path, the long-short, or the short-long path. The last two alternatives will interfere and work as a complementary basis to time, such that specifically one of the two detectors on Bob's side will click — which one depending only on the phase relation. Mathematically, we shall show how the time information at Bob's side is correlated with polarization information at Alice's. We start with the state given by Eqn. (3.54), before the preparing interferometer (see Figure 3.17). The

entangled state just after the preparing interferometer then becomes

$$\begin{aligned}|\Phi_1\rangle &= \frac{1}{\sqrt{2}}(|\mathrm{H_A}\rangle|\mathrm{S_B}\rangle + |\mathrm{V_A}\rangle|\mathrm{L_B}\rangle) \\ &= \frac{1}{\sqrt{2}}(|\mathrm{H_A}\rangle|10_\mathrm{B}\rangle^{t_0} + |\mathrm{V_A}\rangle|10_\mathrm{B}\rangle^{t_1}),\end{aligned} \tag{3.57}$$

where $|\mathrm{S_B}\rangle$ denotes that the photon took the short arm and $|\mathrm{L_B}\rangle$ the long. On the second line we have used the notation from Chapter 2, $|n_\mathrm{a}n_\mathrm{b}\rangle^t$, to describe the state in terms of photon number in the two modes of the input ports of the fiber-based analyzer beamsplitter (n_a photons in port a, and n_b in port b), at two different time-slot t_0 and t_1. At the output of the beamsplitter the photon, upon return from the Faraday mirror, is divided up into three time-slots, with the output ports connected to the two detectors D_1 and D_2. The state is now

$$\begin{aligned}|\Phi_2\rangle = \frac{1}{2}[&i|\mathrm{H_A}\rangle(|01_\mathrm{B}\rangle^{t_0} + i|10_\mathrm{B}\rangle^{t_0}) \\ &+ i(|\mathrm{H_A}\rangle + |\mathrm{V_A}\rangle)|01_\mathrm{B}\rangle^{t_1} \\ &+ (|\mathrm{H_A}\rangle - |\mathrm{V_A}\rangle)|10_\mathrm{B}\rangle^{t_1} \\ &+ |\mathrm{V_A}\rangle(i|01_\mathrm{B}\rangle^{t_2} + |10_\mathrm{B}\rangle^{t_2})],\end{aligned} \tag{3.58}$$

which is also illustrated graphically by Figure 3.18. From Eqn. (3.58) and the

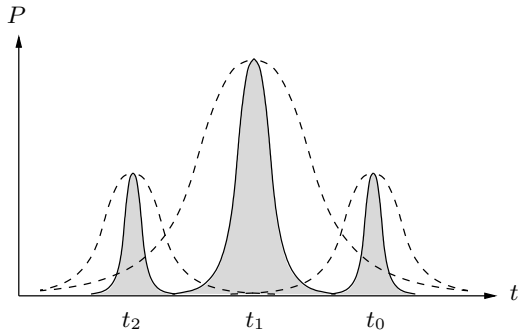

Figure 3.18: The output of the analyzing interferometer for discrete-time qubits. The probability for a photon to fall within the center peak is 1/2 and each of the satellites 1/4. The dashed lines illustrate the problem of pulse-broadening due to chromatic dispersion in the fibers, as described in Section 3.5.

figure we can observe that the entanglement between Alice and Bob is manifested in such a way that if an H photon is detected by Alice, Bob will find a click in either detector D_1 or D_2 at time-slot t_0 (the right satellite peak). If a V photon is

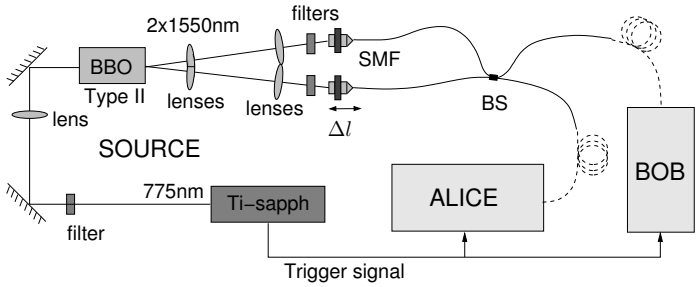

Figure 3.19: Experimental setup showing post-selective creation of polarization entangled photon pairs behind a beamsplitter. The crystal is phase-matched for type-II and emits orthogonally polarized photons both at the wavelength 1550 nm. The pump produce 200 fs long pulses at a repetition rate of 82 MHz, and electrical sync-pulses are used to gate the detectors. The lenses function as telescopes to control the focusing of the spot-like emission into the single-mode fibers.

detected by Alice, Bob will find his photon in time-slot t_2 (the left satellite peak). If Alice instead happens to measure in the diagonal basis, $\mathrm{D} = \mathrm{H} + \mathrm{V}$ and $\mathrm{A} = \mathrm{H} - \mathrm{V}$, Bob will always detect a photon in time-slot t_1 (the center peak) in detector D_1 if D was detected, and in detector D_2 for A.

The idea of hybrid-coding also addresses a problem that is inherent to plain time-coding, namely, the substantial experimental challenge of needing several interferometers aligned against each other. For example, in discrete-time coding using pulsed lasers [Brendel *et al.*, 1999; Tittel *et al.*, 2000], there are three different interferometers that all need to be mutually aligned, one before the crystal, one at Alice and one at Bob. Here, there is only one that needs to be aligned with the other. To simplify the alignment further, the preparing interferometer is half free-space and half fiber-optical, as opposed to the analyzing interferometer which is all fiber-optical. Making use of the free-space half, one can easily adjust the path-length difference of one interferometer to match that of the other interferometer, which both also need to be temperature stabilized.

Before embarking upon the problem of dispersion in the fibers and the crystals, which has important relations to the bandwidth and crystal length, we will finish off this section by showing an experiment on type-II parametric down-conversion in a single-crystal configuration.

Pulsed qubits at the telecom wavelength

Figure 3.19 shows the setup. The crystal is cut for birefringent phase-matching and creates two degenerate photons at 1550 nm from a single one at 775 nm. The two output photons are orthogonally polarized, and by sending them to a beamsplitter

we can post-select polarization entanglement in the coincidences, by possibly first converting them into discrete-time representation for long distance transfer. The experiment has been reported in **Paper J**, using a 12 mm long BBO crystal that was pumped by a femtosecond pulsed Ti-sapphire laser. One motivation for having both photons at the infrared wavelength of 1550 nm, is for the source to be used as part of a telecom quantum repeater, working at the most transparent wavelength of the optical fiber. A quantum repeater relies on the principle of entanglement swapping, which has been realized working at the less transparent wavelength combination of 1310 nm and 1550 nm [de Riedmatten *et al.*, 2005]. For the intended application it is suitable to have pulsed pairs of photons propagating along two different optical fiber channels, each in different directions.

The idea was first to use a relatively long crystal to achieve high photon-rates in a beam-like (or spot-like) manner as described in the beginning of this chapter. Our plan was that it would provide us with a well-defined beam close to the fundamental single-mode of the fiber, providing good coupling. However, the results were not as good as hoped for, probably due to a combination of strong walk-off effects of the beams in the crystals, and temporal dispersion induced by the short pump pulse [Grice and Walmsley, 1997]. The images viewed in Figure 3.4 are the results of placing the infrared CCD camera in front of the beam-path. Rings and spots are emitted depending on the alignment of the crystal; however, not even the spot-like emission turned out to produce as many photons in the fibers as was expected. It turned out that the problem was the strong focusing, which had been set according to ambiguous predictions. Later, we showed that for too strong focusing in long crystals at type-II phase-matching, the beams become non-symmetric and multi-mode, as explained by Vellekoop [2002]. This has been observed independently by Lee *et al.* [2005].

Nonetheless, we repeated the famous and pioneering two-photon interference experiment *à la* Hong, Ou, and Mandel, [Hong *et al.*, 1987], to prove that the crystal is emitting pairs of signal and idler photons that are both temporally coherent and spatially indistinguishable once launched into single-mode fibers. The result is shown in Figure 3.20. It is a purely quantum physical effect that two photons impinging onto separate ports of a beamsplitter will always come out together, randomly at either of the two output ports, as showed already in Table 2.1. Therefore, it is sufficient to measure the coincidence rate behind a beamsplitter as a function delay between the signal and idler as shown by the graph, to prove that we have a true two-photon state. The effect has no classical explanation.

3.5 Decoherence mechanisms

There are two effects of decoherence present in the system presented in Figure 3.15 and Figure 3.17, that need to be controlled. First, there is a special kind of polarization and chromatic dispersion introduced by the crystals, which is due to the wavelength non-degeneracy of the signal and idler, that leads to decoherence. It has

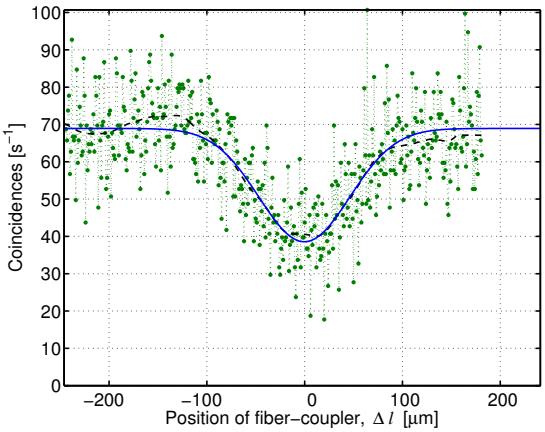

Figure 3.20: Graph of coincidence rate versus optical delay in an Hong-Ou-Mandel experiment. The visibility is 30% after subtraction of background counts, for a singles rate of 7000 s^{-1} in the idler, and 14000 s^{-1} in the signal, gated at 1MHz. The bandwidth of the interference filters were 10 nm FWHM (full-width half maximum), corresponding to 106 μm in coherence length. Dotted line: raw-data. Dashed line: raw-data sent through a digital lowpass FIR-filter (finite impulse response) of order 51 at a cut-off frequency of 1% of the data sample-rate. Solid line: Gaussian fit to raw-data.

been explained well in detail in **Paper B**. Second, there is the standard chromatic dispersion in the optical fibers, which leads to pulse broadening. The problem of controlling decoherence is one of the most important issues in modern quantum optics and quantum information, and for this purpose I will try to provide a short explanation for it within the scope of the thesis.

Simply put, decoherence can be explained as an effect that destroys (or rather relocates) the superpositions inherent to a quantum system. As a consequence, it affects quantum systems such as qubits, that need coherence within its computational basis to remain as pure states. In formal terms, the process of decoherence will couple the degree of freedom in which a qubit is encoded to some other degrees of freedom that do *not* ensure indistinguishability, but rather introduces *distinguishability*. (Recall that indistinguishability is a necessary condition for a superposition to exist in a system.) This works in the sense that our system becomes entangled with some additional degree of freedom that the detection apparatus ignores, or becomes part of, to effectively erase the superpositions (coherence). Decoherence can also be understood in terms of closed and open quantum systems. While a closed quantum system undergoes a closed (unitary) evolution and does not interact with any other systems, an open quantum system is one which interacts

with other systems (for example, the environment) in such a way that it becomes a subsystem (the qubit) in the context of a greater system (qubit + environment). The coherence of the smaller system has spread out into a bigger system. Here, we will consider the effect of decoherence as a process that reduces the superpositions with respect to a specific orthonormal basis, creating mixed states.

All quantum systems are open quantum systems even though the interaction with the environment may be very small, like is usually the case for the photonic qubit. To give a counter example showing a stronger kind of interaction, consider the following discussion on the temporal single-mode resolution of a detector which will help explain how the frequency work as an environment, to which our qubits will couple and become mixtures for the particular kind of decoherence processes that we are interested in: Looking only to coincidences between two photon pairs created by a spontaneous parametric downconversion, the coherence time Δt and thus the precision to which the photons simultaneously arrive at two perfect detectors, will in principle be given by the bandwidth, $\Delta\nu$, of the interference filters in front of the detectors according to $\Delta t = 0.44/\Delta\nu$ (for a Gaussian spectrum). (In our case the pump has a very narrow spectrum and very long coherence time leading also to small frequency uncertainty and long coherence time in the emission.) Now, in order to verify the above relation and measure the coherence time directly by coincidence detection similar to the experiment of Hanbury-Brown and Twiss, the detectors necessarily need a timing-jitter much smaller than the coherence time[7]. However, filter bandwidths used in practice are relatively large > 0.1 nm, in wavelengths, which makes the timing-jitter ($\Delta t_{\text{jitter}} \approx 350$ ps) orders of magnitudes larger than the corresponding true coherence time. This effectively means that the detector itself sets a minimum resolution for the wavelength, $\Delta\lambda_{\text{res}} = 0.44\lambda^2/c\Delta t_{\text{jitter}}$, such that the coherence time of the photons detected in coincidence are practically longer, set by the timing-jitter. In other words, and here comes the point; as the detector in principle can determine the photon's frequency components in a fine resolution, it means that the frequency components should all be added incoherently within the filter bandwidth. The incoherent nature is here a distinguishing mark for distinguishability. It is mathematically equivalent to saying that the detector *traces* over the frequency, i.e. the temporal degree of freedom. The number of temporal modes we trace over are set by the relation between the timing-jitter and the filter. (An ideal detector with perfect zero jitter defines a temporal single-mode with the filter and cannot distinguish between any frequency components and performs no trace). In retrospect, it should be clear from the above reasoning why it can be devastating for a qubit to be encoded into some degree of freedom that couples to frequency.

Let us now consider the type of decoherence that can occur in a birefringent crystal, for which the H and V polarizations makes an orthonormal basis

[7] In Hong, Ou, Mandel's experiment, a measurement of the timing-jitter instead of coherence time is avoided by an all-optical coincidence measurement, using the two-photon interference effect to measure "simultaneousness".

to encode the qubit. For well-defined superpositions between H and V to exist, $|\varphi^\nu\rangle = \frac{1}{\sqrt{2}}(|\mathrm{H}\rangle + e^{i\phi^\nu}|\mathrm{V}\rangle)$, it is necessary for the phase-relation ϕ^ν to be constant, as opposed to random, for all frequencies ν included in the description of the state. In a birefringent crystal the refractive index varies with polarization and frequency, meaning that a qubit passing such a medium will acquire a different phase-shift[8] for each of its frequency components. Hence, the phase has coupled to the frequency degree of freedom, which effectively is ignored by the detector system that measures an incoherent sum of superpositions $\sum_\nu |\varphi^\nu\rangle\langle\varphi^\nu|$, killing the superposition.

In our two-crystals source the phase-shifts taking place are very large due to the large non-degeneracy in frequency between the two entangled subsystems, signal and idler, that it even leads to *time-lags* between the different photon wave-packets. As explained in a different way in **Paper B**, we therefore have the effect of "time-lags coupled to the frequency", efficiently killing entanglement. Note that very narrow filtering should, and does, bring back coherence and thus the entanglement. As we have also showed in the same paper, the entanglement can be regained by inserting an extra piece of crystal that reverses all time-shifts, called decoherence cancellation in Figure 3.15.

The kind of decoherence that occurs in optical fibers can be attributed to the phase (and even more strongly to polarization) coupled to the frequency in the same way as described above. In connection to the discrete-time coding and Figure 3.18, the effect is that the photon wave-packets (defined by their coherence length) become broadened as they propagate through the fiber. This dispersion is significant for the wavelength of 1550 nm, and has its minimum at 1310 nm, leading to decreased resolvability of the different time-slots in the discrete-time analyzer. Again, it is possible to reverse the phase-shifts, and thus cancel the broadening introduced by the system. For fiber systems, devices such as Bragg gratings serve this purpose.

As noted, these decoherence effects diminish as the bandwidth decrease. Therefore, we have found it interesting to understand how we can make the crystal itself produce narrower bandwidth photons to match the detectors' timing-jitter, without reducing the flux of photons. This is the topic of the following section.

3.6 Photon-flux and bandwidth in optical fibers

Theoretically, we have shown in **Paper C** how the photon-flux both in free-space and in single-mode fiber depends on the length of the crystal and on the chosen filter bandwidth. The results are derived for a very general case of quasi-phase-matching in a bulk crystal, taking into account the results of optimal focusing. We also showed how the frequency bandwidth of the emission coupled into a single-mode fiber at optimal focusing relates to the crystal length. At the moment we are unsure

[8] Some entangled systems, called decoherence free subsystems (DFSS), e.g. the Bell-state $|\Psi^-\rangle$, are immune to these phase-shifts if the decoherence is identical on both subsystems, as their correlations of entanglement are invariant under rotation (different phase-shifts).

if the result are general enough to encompass also birefringent phase-matching. We see no immediate reasons to why it should not, although the statement is spoken against by results of others [Lee *et al.*, 2004]. Below follows a brief summary of the results, that are based on both physical arguments and computer simulations using the analysis from the beginning of this chapter.

The bandwidth of the light in a single-mode fiber at optimal focusing of both the pump and the fiber-modes, using no separate frequency filter, is given by

$$\Delta\lambda_{\mathrm{SM}} = B/L, \tag{3.59}$$

where B is a material specific constant that attains different values for the signal and idler depending on their amount of non-degeneracy. In our system showed by Figure 3.15 using PPKTP, the value for the signal (810 nm) is found to be $B_{\mathrm{s}} = 1.23 \times 10^{-11}$ [m^2] and idler (1550 nm) $B_{\mathrm{i}} = 4.50 \times 10^{-11}$ [m^2].

If a narrower filter $\Delta\lambda_{\mathrm{narrow}}$, than the single-mode bandwidth $\Delta\lambda_{\mathrm{SM}}$, is placed in front of the detection system the photon-flux P in both free-space and the fiber is

$$P \propto L\sqrt{L}\Delta\lambda_{\mathrm{narrow}}, \tag{3.60}$$

which readily is proportional to the bandwidth, and grows strongly with crystal length. Basically, Eqn. (3.60) is due to the product of three factors: (i) the intensity of light phase-matched in the forward direction, $\propto L$, (ii) the reduction of intensity of light weakly phase-matched in the non-forward directions, $\propto 1/\sqrt{L}$, and (iii) the concentration of power to the forward direction at optimal focusing of the pump in long crystals, $\propto L$. Now, if a filter wider than the single-mode bandwidth is placed in front of the fiber-coupling system, the photon-flux in the single-mode fiber is instead

$$P \propto L\sqrt{L}\Delta\lambda_{\mathrm{SM}} \propto \sqrt{L}, \tag{3.61}$$

for any filter $\Delta\lambda_{\mathrm{wide}} > \Delta\lambda_{\mathrm{SM}}$. The growth of photon-flux for different bandwidths can be found in Figure 11 in **Paper C**. Some of these results were also confirmed experimentally.

The obvious conclusion to draw is that both high photon-fluxes and a narrow bandwidths are achieved for long crystals, making it a natural choice if such properties are desired. As we already motivated in the previous section a narrow bandwidth is advantageous to limit the effects of decoherence. High photon-fluxes are not necessarily advantageous, as a high rate will increase the risk of accidental and false coincidences due to the Poisson distributed light, thereby reducing entanglement and/or increasing the probability for presence of more than a single photon in a heralded source. However, it is just a matter of reducing the pump power, and so the implication for long crystals is simply that we can use compact and cheap low-power laser-diodes to a greater extent.

To finish off this chapter I would like to put our work in context to others by referring to the Appendix A and a table which may be of interest mostly to the

specialists. The table shows a compilation of published results from many different groups working on sources of photon pairs and/or entanglement developed within the framework of quantum communication or quantum information. The detection rates and coupling parameters that we have achieved experimentally are reported in detail in **Paper A** and in **Paper C**. In the table we have included results of parameters that are commonly used to characterize the quality of entanglement, such as the visibility of the second-order correlation function and the violation of the CHSH-inequality parameter S. Such kind of measures will be discussed in the following chapter.

Chapter 4

Characterization of qubits

The state of a quantum system provides complete information on the possible outcomes of any future measurements made on the system. Ideally, we would like a source to produce qubits in a predetermined state, and it is therefore essential to be able to verify this experimentally by reconstructing the output state of the source in the form of a density matrix. It is impossible to make a reconstruction using a single qubit of an unknown state in a single measurement. Therefore, many identical member qubits of an ensemble are needed to be projected onto different basis states in a process called tomography. There are several ways in which we can characterize the qubits depending on their implementation. In the previous chapter and in **Paper C**, we searched theoretically for the state of the spatial modes for a polarization encoded photonic qubit, created by the process of spontaneous parametric downconversion. In **Paper C** we also compared that result with an experimental characterization. However, to experimentally determine the full state via tomography is difficult in the spatial degree of freedom, so instead we used the theory of optical beam propagation to quantify the emission. In contrast, for the polarization degree of freedom which contains the computational basis, the full density matrix is much easier to find. Such a measurement was performed in **Paper B** to characterize the entanglement. In due order of the sections, see further Siegman [1986]; Bouwmeester *et al.* [2000]; Altepeter *et al.* [2005a].

4.1 Mode-profiling

A complete spatial tomography would require taking images of the emission and record the transverse shape of the electrical field. However, in general, using a CCD camera only the intensity is monitored and not the phase of the field. If we look at the emission from the crystal as an optical beam, we can instead characterize it with a single parameter. The theory of optical beam propagation can be applied equally well at the level of single photons and constitute no fundamental obstacle; we need simply to use CCD sensors made for single photon detection. One way

to determine the quality of a laser beam is by measuring its longitudinal intensity profile. All light that is coherent enough to define a beam will at some point along its line of propagation necessarily have a waist, that is, a smallest radius. Only a beam described by the transverse fundamental Gaussian, TEM_{00}, with a purely real phase at its waist, will be in a coherent single-mode at the waist, all others will be multimode (see Figure 2.2). For example, the higher order Laguerre-Gaussian or Hermite-Gaussian modes are not diffraction limited and become multimode at the waist. The challenge of fiber coupling is to arrange for the optics to focus the beam such that its waist hits exactly at the end facet of the optical fiber. For a single-mode fiber it is thus necessary that the beam is in the fundamental Gaussian mode to achieve perfect coupling efficiency.

The transverse radius $w(z)$ of a Gaussian beam has the following form,

$$w(z) = w_0 \sqrt{1 + \left(\frac{z - z_0}{z_R} \right)^2}, \tag{4.1}$$

where w_0 is the beam waist radius at $z = z_0$, and z_R is the Rayleigh range defined by

$$z_R = \frac{\pi w_0^2}{M^2 \lambda}. \tag{4.2}$$

The parameter M^2 was introduced by Siegman [1993a,b] as a measure of how close a beam resembles the fundamental Gaussian mode. For the TEM_{00} mode $M^2 = 1$, and for all higher order modes $M^2 > 1$. It has become a standard beam quality measure in laser engineering. In theory, the only well-defined measure of the beam radius $w(z)$ that guarantees Eqn. (4.1) to hold for all types of transverse beam modes is $w(z) = 2\sigma(z)$, where $\sigma(z)$ is the standard deviation, or the second-order moment, of the transverse intensity profile, $I(y, z)$. Thus, the challenge of finding the M^2 factor is to determine $\sigma(z)$ for not too short distances z around the beam waist location z_0.

Theoretically, $\sigma(z)$ is indirectly provided by the discrete function $\zeta_n[\theta]$, which is the plane wave function representation of the angular spectrum $|\zeta_n\rangle$ of the different modes n of the emission, as derived in Eqn. (3.30). First, the electrical field is obtained by a discrete Hankel transform as

$$E_n(x, y, z) = \sum_{\theta} \lambda_n \zeta_n[\theta] \, e^{-ikz \cos\theta} J_0 \left(k \sqrt{x^2 + y^2} \theta \right), \tag{4.3}$$

where the basis functions $J_0(\alpha)$ are the standard Bessel functions of zeroth order. The intensity is given as an incoherent sum of all field-modes,

$$I(x, y, z) = \sum_{n=1}^{N_\theta} |E_n(x, y, z)|^2, \tag{4.4}$$

which leads to the transversely integrated intensity profile $I(y,z) = \sum_x I(x,y,z)$.

Experimentally, the transverse intensity profile is found by taking images of the beam along a number of point on the z-axis. The beam radius is then numerically extracted from the data. However, it turns out to be much more accurate to determine $\sigma(z)$ by fitting a Gaussian to the raw-data, rather than determining $\sigma(z)$ directly, as the noise will otherwise have a too strong impact on the result. Although beam quality measuring apparatus exist, they still use too low sensitivity CCD detectors for single photon applications. We found it to be a particularly skillful art to measure the M^2 factor correctly at single photon level with homemade alignment rails and software, especially at the infrared wavelength. To conclude, in **Paper C** there is an interesting theoretical plot that relates the single coupling efficiency to the M^2 factor, besides a plot of the experimental values obtained.

4.2 Bell-state analysis

The Bell-state analyzer is a key component in quantum communication systems. As the name suggests, it distinguishes between the four different types of two maximally entangled qubit pairs, the so-called Bell-states, Eqn. (2.17). In contrast to tomography, the Bell-state analyzer must work by making only a *single* measurement on a single sample of the entangled qubits. As a result, the measurement needs to be a joint projection of the qubits onto the Bell-basis. The circuit that performs such a measurement is depicted in Figure 4.1, and transforms entangled states into product states. It uses a CNOT gate and a Hadamard transform in the reverse direction of the circuit that creates Bell-states from product states in Figure 2.11.

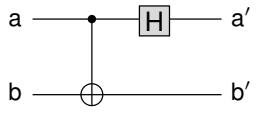

Figure 4.1: General Bell-state analyzer.

The realization of a CNOT for polarization qubits is not trivial however, as we discussed in Section 3.4. Via the nonlinear interaction in a crystal, only a very low efficiency of about 10^{-10} can be achieved for the CNOT function [Kim *et al.*, 2001]. In addition, it has been shown that a maximum 1/2 of the states can be distinguished deterministically when limited solely to linear optics [Calsamiglia and Lütkenhaus, 2001]. Such a scheme uses the interference effects in the beamsplitter [Hong *et al.*, 1987] by post-selecting events where the beamsplitter acts as "half a CNOT", according to Table 2.1. The simplest linear optical Bell-state analyzer sorts the outcomes into 3 classes: $|\Phi^+\rangle$, $|\Phi^-\rangle$, and $|\Psi^\pm\rangle$, which correspond to gathering

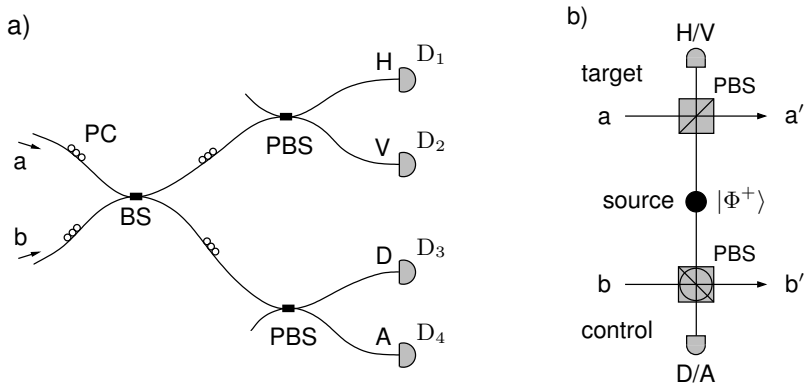

Figure 4.2: a) Linear optical fiber-based Bell-state analyzer for polarization qubits. BS: beamsplitter; PBS: polarizing beam splitter; PC: polarization controller. b) Linear optical CNOT for polarization qubits. The lower polarizing beamsplitter is rotated to the complementary basis.

$\log_2(3) = 1.59$ bits of information out of 2 possible bits. Figure 4.2a shows a fiber optical realization of such an analyzer.

Surprisingly, it has been shown that if we allow the gate to work only partly, that is indeterministically, it is possible to implement a CNOT that can be used to distinguish all of the four Bell-states by exploiting the nonlinearity of measurements, using only single photon sources and feedback information from single photon detection [Knill *et al.*, 2001]. A signal will announce when the gate has succeeded, and the gate can thus be seen as a heralded operation similar to heralded single photon sources. The gate succeeds typically with a probability of 1/16 and has very complex structure using dual-rail qubits. Nevertheless, the same team showed that the probability approaches unity, $(1 - \frac{1}{n})$, in the limit of a large number, n, of used single photon sources and detectors. A simpler scheme for polarization qubits was proposed by Koashi *et al.* [2001], using an additional entangled state and two single photons, working with a probability 1/4 but destroying the output photons in case of failure. An even simpler proposal uses only a single extra entangled state and works 1/4 of the time [Pittman *et al.*, 2001; Gasparoni *et al.*, 2004], see Figure 4.2b. Based on the same implementation, Walther and Zeilinger [2005] recently demonstrated a Bell-state analyzer that can distinguish all of the four Bell-states with a probability of 1/16 in passive operation, and 1/4 with active polarization control of the output.

The search for good working CNOT gates and Bell-state analyzers is currently a big experimental challenge of utmost importance for pushing the fields of optical quantum computing and quantum communication forward.

4.3 Entanglement tests and tomography

The first test of entanglement was proposed in a seminal paper by Bell [1964], in an effort to settle the debate whether or not the EPR-effect [Einstein *et al.*, 1935] could be explained by a limitation of access to classical information, so called "hidden variables". He derived an inequality that must hold for all local realistic models explaining the outcomes of a sequence of correlation measurements, and showed that entanglement indeed violates this inequality. Experimentally Bell's prediction was not confirmed until much later as technology had progressed [Aspect *et al.*, 1982].

Consider three local properties of some objects, for example, the true or false for each person in a group of people to be characterized by the following descriptions, a: sings in the shower; b: is of the opinion that Metallica just makes an awful lot of noise; or c: is a fan of fermented herring. Let $n(a, b)$ denote the number of persons that confess to both statements a and b. Bell's original inequality then states that for any fixed ensemble of people

$$n(a, \text{Not } c) \leq n(a, \text{Not } b) + n(b, \text{Not } c). \tag{4.5}$$

The condition holds for any type of correlations between a, b, and c for each object individually and between each object, as described by classical probability distributions. Similarly, the properties can also represent the yes and no outcomes of measurements X, Y, and Z of a polarization encoded qubit. However, due to complementarity, we cannot measure all of the three directions of the polarization qubit simultaneously. Therefore, and as another effect of negative probability amplitudes, two entangled qubits can actually violate Eqn. (4.5), unlike the personal tastes of two persons.

There are several refined versions of Bell's inequality available, of which the generalized CHSH-inequality has become perhaps the most frequently used [Clauser *et al.*, 1969]. The CHSH-inequality parameter S can be written in terms of the interference visibility V of the second-order correlation functions

$$R_{i,j} = \frac{1}{2}[1 + ijV_{i,j}\cos(4\phi_\mathrm{s} + 4\phi_\mathrm{i})], \tag{4.6}$$

obtained by rotating the half-wave plates (ϕ_s and ϕ_i) of the polarization state analyzer part in Figure 3.15 and observing coincident detections in the signal and idler arms. For $V_{i,j} = 1$ the correlations are perfect in each of the four combinations $i, j = \{\mathrm{H}, \mathrm{V}\}$ of the output arms that pertains to the two polarizing beamsplitters. Refer to **Paper B** for further details. For a classical state, $S \leq 2$, and for a maximally entangled state with unit visibility, $S = 2\sqrt{2}$. If the states decoheres equally in all bases a violation implies a visibility larger than 71%. However, when the states decoheres only in the computational basis, as in our case, it suffices with a visibility of 41% in that basis to prove that we have entanglement.

In recent years, several measures of entanglement have been suggested or adapted, like for example entanglement of formation [Wootters, 1998], entanglement witness

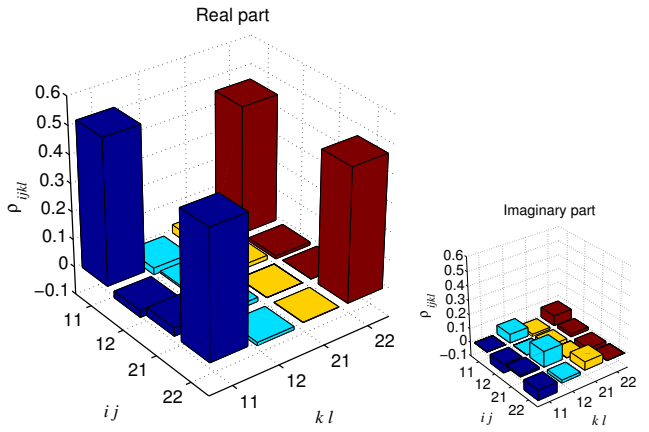

Figure 4.3: Experimentally determined density matrix obtained by quantum state tomography on a polarization entangled state (1 = vertical and 2 = horizontal).

[Lewenstein *et al.*, 2000] and entanglement fidelity [Nielsen and Chuang, 2000]. They all differ in their ability to experimentally detect entanglement accurately enough in as few number of measurements as possible. However, all tests and measures share with the CHSH-inequality the feature to be derivable from the density matrix. Therefore, full tomography of the state is considered to be the most exhaustive way of characterizing the state to which subsequently any measure of entanglement can be applied [Altepeter *et al.*, 2005c]. The only obstacle is the rather large number of measurements needed. For two polarization qubits of dimension $N = 2^2$, a total of 16 local measurements are needed if we are restricted to one detector for each qubit (in principle one measurement for each element in the density matrix), and totally 9 local measurements using four detectors. If we also have access to non-local measurements of the type used in the Bell-analyzer only 5 measurements are needed; in general $M = N + 1$. In order to minimize the errors in the estimation of the density matrix, each measurement should not gather any information already contained in other measurements, which means that the measurement bases should be mutually unbiased.

Following the tomography procedure of James *et al.* [2001], we have made laboratory software that automatically recreates the density matrix $\boldsymbol{\rho}_{\text{expt}}$. Figure 4.3 shows the result of one such tomographic estimation for the output of the first experiment in Section 3.4. Clearly, the state closely resembles the target state of the source, $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|\mathrm{H_s}\rangle|\mathrm{H_i}\rangle + |\mathrm{V_s}\rangle|\mathrm{V_i}\rangle)$, and has the fidelity $F = \langle\Phi^+|\boldsymbol{\rho}_{\text{expt}}|\Phi^+\rangle = 0.95$, which should be compared to $F = 1$ for a maximally entangled state. Further details of our results can be found in **Paper B**, or in the table of Appendix A.

Chapter 5

Quantum communication systems

So, what is entanglement useful for? It has been found that entangled qubits can be useful as a resource for accomplishing tasks that are not possible with classical bits. It may sound obvious that tasks involving transferring and manipulation of quantum states cannot be achieved classically. However, also purely classical tasks are possible to improve on using entangled states, in some cases because entangled qubits involve a phase term in the superposition that can be used to carry additional information, and in some cases due to the no-cloning principle. Interestingly enough, once distributed, entanglement can be seen as a quantum channel which needs no physical medium to transport information. In this chapter we make a short and incomplete review of how qubits are used in quantum communication. Good references are Nielsen and Chuang [2000] and Bouwmeester *et al.* [2000].

5.1 Entanglement as a resource

The phenomena which perhaps has attracted the most attention is *quantum teleportation*. Figure 5.1a shows the basic principle of transferring a partially unknown state of a photon from one place to another without the photon itself passing the intervening space, but using up the resource of entanglement. Let's say two parties, A and B, share an entangled state since long time ago, and that Alice now wants to send a quantum state $|\psi\rangle$ to Bob. She can then perform a Bell-state measurement between her photon of the entangled pair, and the photon who's state she would like to transmit, using a CNOT gate and a Hadamard transform like described in the previous chapter. Both her photons are destroyed in the process. As a result, the photon on Bob's side is now in one of four possible states, $|\psi\rangle$, $X|\psi\rangle$, $Y|\psi\rangle$, or $Z|\psi\rangle$, depending on the outcome of Alice's measurement. If Alice sends her outcome (two bits of information) to Bob, he can rotate his state accordingly to get exactly $|\psi\rangle$. This is called teleportation, however, it is not exactly the kind of teleportation as in Star Trek because it does not transfer the particle itself, nor any human. If anything, it is quantum state teleportation. Nevertheless, to appreciate the phenomena

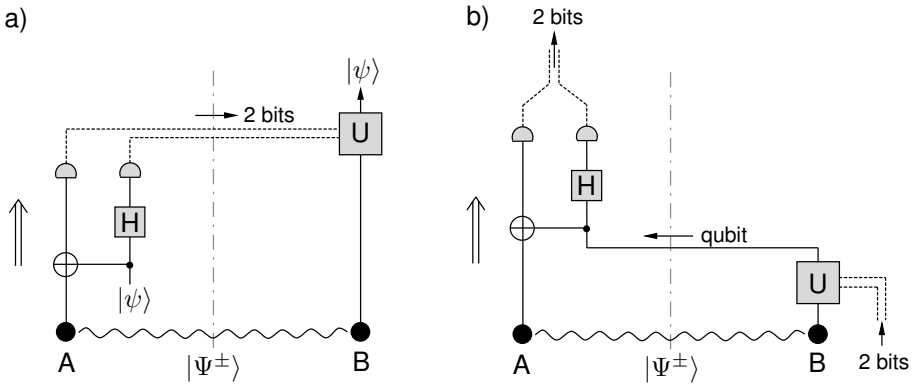

Figure 5.1: a) Teleportation protocol. b) Dense coding protocol.

one should think about what possibly constitutes matter or energy; namely information. For example, an atom is not different from any other atom of the same kind except for the state it happens to be in. If we can read off the information of the state of a particle on one place, thereby changing its state, and then read the same information into a different particle on another place, we have effectively recreated the "same" particle. Note that indistinguishability is a key ingredient is each step of the protocol for the particle to become identical. Teleportation was discovered by Bennett *et al.* [1993] and first realized experimentally by Bouwmeester *et al.* [1997] using photons. Since then, many similar experiments have been performed on other realizations of qubits, improving the implementation of the Bell-state analyzer or extending the distance [Marcikic *et al.*, 2003; Ursin *et al.*, 2004]. One can also note that if the entangled state used in the teleportation is applied with a unitary transform (that is a gate-operation) the teleported state will exit with the same transform applied to it, effectively realizing a *gate-teleportation* [Gottesman and Chuang, 1999], which can be used for quantum computation.

A very similar type of experiment is *entanglement swapping*, where the photon to be teleported is also itself entangled with another photon, such that after the Bell-state measurement the two remaining photons are entangled even though they never interacted [Pan *et al.*, 1998; de Riedmatten *et al.*, 2005]. Such a scheme may be useful as part of a *quantum state repeater*, which contains the basic idea to extend the distance over which a qubit may be sent, mainly due to absorption in the optical fiber.

By observing that the four different Bell-states give four different outcomes in a perfect Bell-state analyzer, we can also get the idea that a single photon entangled with another one can actually carry two bits of information (a single qubit contains only one bit) [Bennett and Wiesner, 1992; Mattle *et al.*, 1996]. This is called *dense*

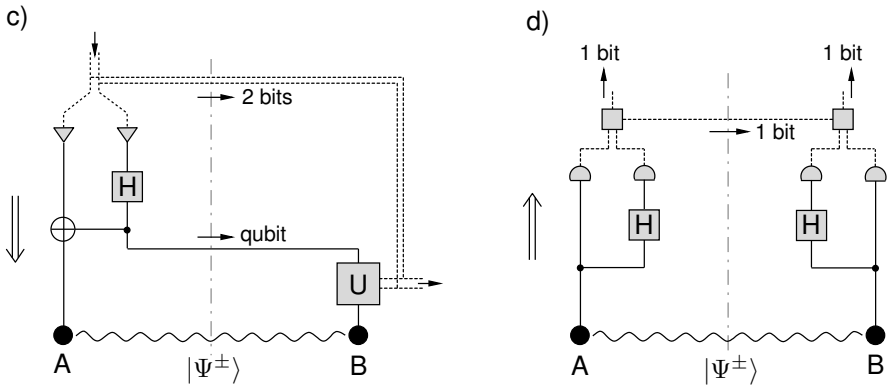

Figure 5.2: c) Entanglement distribution protocol. d) Quantum key distribution protocol.

coding and is depicted in Figure 5.1b. It is basically the reverse of teleportation. Alice starts off with the entangled state $|\Phi^+\rangle$, and sends only *one* of her both photons to Bob, which then applies a unitary transformation I, X, Y, or Z to the photon corresponding to the classical bit-values `00`, `01`, `10`, and `11`, thereby rotating the joint state to one of the four states $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, or $|\Psi^-\rangle$. As the particle is sent back to Alice is carries two bits of information that can be read off in a Bell-state analyzer. Thus, one bit is encoded in the qubit state value and the other bit in the phase between the qubit-states, according to Eqn. (2.17).

By the same token, we can also distribute any of the Bell-states by sending a single qubit and two bits of information telling which of the Bell-states are sent, or for Bob to decide which state to transform to as in Figure 5.2c. For completeness and illustration, the principle of quantum key distribution (QKD) based on entanglement can also be illustrated in circuit form, see Figure 5.2d. The single bit which is communicated contains information regarding the basis which Alice chose to encode her qubit in. As both Alice and Bob know the exact state of the entangled photon pairs they will end up with two deterministically correlated bits, assuming perfect conditions.

5.2 Quantum key distribution with entanglement

Quantum cryptography based on measuring Bell-inequalities in two complementary bases was proposed by Ekert [1991], and has been implemented in a variety of forms since then. The idea is that any attempt of eavesdropping inevitably leads to a violation of Bell's inequality which Alice and Bob can detect. In terms of security, the violation the inequality is at equal footing with the errors that are introduced in

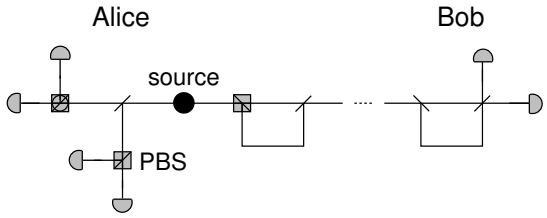

Figure 5.3: Quantum key distribution system using the hybrid-coded entanglement presented in **Paper B**. On Alice's side is a source of polarization entangled photon pairs. PBS: polarizing beamsplitter.

single-qubit quantum cryptography. The implementations of entanglement-based quantum key distribution is not as mature as weak-pulse QKD due to somewhat more demanding experiments. However, several proof of principle experiments have been performed, for example: polarization encoding in fibers [Jennewein *et al.*, 2000; Poppe *et al.*, 2004] and free-space [Naik *et al.*, 2000], or discrete-time [Tittel *et al.*, 2000], with the early references limited to meter-range distances. These schemes share the property of having both photons at the same wavelengths (either ∼700 nm, or 1310 nm). The advantage of using the shorter wavelength is that very efficient single photon detectors are available. However, for fiber-transmission, short wavelengths are highly attenuated, and therefore the wavelengths of 1310 nm or 1550 nm are preferred. Furthermore, degenerate wavelengths are advantageous only if the source is to be placed in the middle between sender and receiver. However, such a placement of the source is not needed for direct (non-relayed) QKD. The first experiment combining a short wavelength for efficient detection, and a long wavelength for low attenuation in fibers, was done by Ribordy *et al.* [2001] using continuous-time entanglement. The setup was asymmetric in the sense that the source of entangled pairs was located at Alice. The system generated non-degenerate wavelengths of 810 nm and 1550 nm utilizing both efficient detection at Alice, and the lowest possible attenuation for long-distance fiber transmission to Bob. With this experiment they managed to reach 8.5 km, and an even longer distance transmission of 30 km has also recently been reported [Fasel *et al.*, 2004b], using dispersion compensation methods.

For our scheme we took note of the non-degenerate configuration, but also proposed to use a hybrid-coded scheme that mixes polarization and discrete-time coding. The scheme is presented in **Paper B** and is currently being finalized experimentally. Since our source produce polarization entangled qubits, and only Bob's qubits need to be time-encoded to avoid polarization dispersion in fibers, Alice's qubit will remain polarization-coded. See Figure 5.3. As explained in Chapter 3, Alice and Bob end up with correlations between different polarization settings and time-slots detections, respectively, which will not violate Bell's inequality as soon

as the error-rate is too high. Note the nice feature of the random selection of non-orthogonal basis-set as arranged by the beamsplitters. Thus, there is no need for any active selection as with weak-pulse QKD, which is the topic of the next section.

5.3 Quantum key distribution without entanglement

Quantum key distribution all started with the very first experiment by Bennett *et al.* [1992] showing the principle of the BB84 protocol [Bennett and Brassard, 1984]. Since then, much more user-friendly and compact setups have been developed, for example resulting in two commercial companies to date.

Awaiting better sources, the current implementations use weak-coherent laser pulses as a source of "single" photons, with all the disadvantages that come along, like empty pulses and non-negligible probability of multi-photon pulses. Still, the first experiment to reach a long distance in fibers and observe single photon interference was performed by Townsend *et al.* [1993], and later refined by Townsend [1994]. Just as with Muller *et al.* [1996] using polarization, and Hughes *et al.* [2000] using phase, these schemes are based on *one-way* transmission of photons from Alice to Bob. For the phase-type of encoding, which is suitable for fiber-transmission, Alice creates a single photon which she encode in phase by sending it through an Mach-Zehnder interferometer equipped with a variable phase-shift. The phase qubit is sent to Bob who decodes the qubit using an exactly equal interferometer placed in front of a single photon detector. For the B92 protocol [Bennett, 1992], only two different values of the phases need to be controlled, representing two non-orthogonal basis-vectors. A problem with this scheme is that both interferometers need to be mutually aligned and stabilized, which makes the system rather sensitive and in need for active control. Nevertheless, a 122 km experiment has recently been performed [Gobby *et al.*, 2004].

Taking note of the problems, another scheme was suggested based on *two-way* transmission [Muller *et al.*, 1997]. By replacing Alice's interferometers with a Faraday mirror, one can ensure that the photon sent out by Bob comes back to his interferometer in the same polarization as it went, despite strong birefringence. Thereby, the same interferometer can be used twice and one avoids the stabilization problem, see Figure 5.4. It works in the following way: The source produce a strong coherent laser pulse which is split into two different pulses in the interferometer. Both of these pulses propagate in the fiber and are reflected back to Bob by a Faraday mirror[1]. Alice first applies a phase shift to one of the pulses, and because the pulse now carries information in one of two complementary bases, it is necessary before the back propagation to attenuate the pulse down to single photon level. Once back in the interferometer, Bob also applies a phase-shift, and depending on the phase-difference the photon gives a click in either detector. One can see the transmission line as a very long Mach-Zehnder interferometer, and

[1] A device that flips the polarization upon reflection; in the qubit-sphere it takes a state to its opposite diagonal corner, see Figure 2.3.

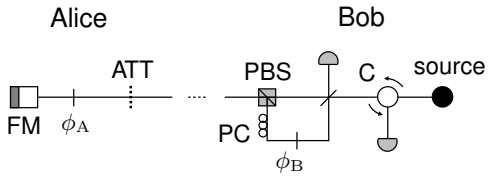

Figure 5.4: Quantum key distribution system using weak coherent pulses *à la* "plug & play". The implementation of the B92 protocol as presented in **Paper F** used only one detector. FM: Faraday mirror; ATT: attenuator; PC: polarization controller; PBS: polarizing beamsplitter; C: circulator.

due to its remarkable stability, it can be said to be auto-compensating. Hence, the system is sometimes referred to as "plug & play". With small modifications, this system has been implemented by many groups, along with the originators who succeeded with a long-distance experiment of 67 km at 1310 nm using the BB84 protocol [Stucki *et al.*, 2002]. The first implementation at the telecommunication wavelength 1550 nm was reported by our group in **Paper R** and **Paper F**, using the B92 protocol and a predecessor to the setup in Figure 5.4, using basically an ordinary beamsplitter instead of the polarizing beamsplitter and only one of the detectors.

To avoid empty pulses, future system will preferably use heralded single photons from photon pairs like the one developed in for example **Paper A**, together with the plug & play scheme. This would possibly also allow for random basis selection.

5.4 Authentication

The problems of cryptology does not stop with key distribution; neither does it stop with one-time-pad encryption. Among several other problems, Alice and Bob need to know they are talking to each other, and not to anyone else. In either classical or quantum cryptography, an eavesdropper Eve can act as an impersonator by pretending she is Alice to Bob, and vice versa. This is a so called (wo)man-in-the-middle attack, which gives rise to the need for the users of the crypto-system to authenticate each others identities. Yet, when the principle of QKD is demonstrated it is usually not questioned why the quantum channel should not be connected between locations other than the intended. Moreover, it is often silently assumed that the classical public side-channel, which is used to agree on the signal states, error correction, and privacy amplification, is not possible to tamper with. To guarantee these conditions, a classical solution is to perform authentication using hash functions and rely on computation assumptions for security [Wegman and Carter, 1981]. Likewise, in the context of quantum cryptography it was early observed that an initial secret is needed to be shared by Alice and Bob [Bennett *et al.*, 1992], and

later it was observed that the initial secret (classical bits) can be used to select the basis of qubit encoding in quantum key distribution [Crépeau and Salvail, 1995]. In such a case, QKD is regarded to as a quantum key growing system, whereby part of the new key is used for authentication in a later run [Dusek *et al.*, 1999]. Altogether, this use of QKD is unavoidable in a practical scenario where one needs to be sure about to where the communication cable is connected.

In a real world scenario, however, it is not practical that Alice and Bob need some initial secret to share. Rather, they would both like to commit to some trusted third party via which they can mutually authenticate (like the government issuing passports or the certification authorities issuing digital ID:s on Internet). Using such an arbitrated third party, we have in **Paper E** investigated how quantum methods similar as in QKD can help. Entanglement is showed to be beneficial. It is argued that the requirements for the channel connecting Alice and Bob can be relaxed, while the channel Alice-authority-Bob need still be non-tamperable. As mentioned early in the thesis, this is a perfect application for satellite-to-earth communication, where the trusted party is "inaccessibly" located in an orbiting satellite.

Finally, it is interesting to note that while the above problem concerned the protection of classical bits using quantum bits, the opposite problem of protecting quantum bits using classical bits have also received some attention recently. It has been shown that in such a case the one-time-pad can actually be reused [Oppenheim and Horodecki, 2005], in contrast to the cardinal rule of cryptology stating the opposite. It has been shown that qubit authentication protocols can always be implemented by small modifications to QKD [Gottesman, 2003], due to the fact that qubits are naturally protected by the no-cloning principle.

In summary, it is my hope to have illustrated in this chapter how the great power of quantum protocols can complement, and sometimes even beat, classical ones in solving both classical and quantum tasks.

Chapter 6

Conclusions and future developments

Regarding single photon sources, we have shown the importance of being able to control the photons in both the temporal and spatial domains. In order to be capable of interfering photons with each other for various tasks, such as logical gate operations and communications, the individual photons must be exactly alike, and not even in principle distinguishable. They need to have the same frequency, coherence length, direction of propagation, arrival time, frequency bandwidth, and polarization, etc. In addition, a single photon source should not emit more, nor less, than a single photon, preferably on demand. Using continuous pump light to produce pairs of photons by the process of spontaneous parametric downconversion in nonlinear crystals, we have shown that heralded single photon sources have some advantages over pulsed pump light, producing in principle less multiphoton events. Such a source was presented in **Paper A**. This is one of the first few realizations of a source of single-photons at a telecom wavelength. An interesting extension of our source of heralded single photons is a multiplexed configuration, where several sources contribute to produce higher number states, that is, two, three, or higher number of photons on demand. This is a long term goal for performing tests in quantum optics, and now also for doing quantum computation.

As the technology for manufacturing quasi-phase-matched crystal materials have progressed, periodically poles materials like PPKTP have become available for very efficient generation of photon pairs, as a complement to birefringently phase matched materials. Among other things, quasi-phase-matching allows a greater freedom in the choice of wavelengths. A wavelength combination that is particularly useful is 600-800 nm and 1310 or 1550 nm for the two photons of a pair. The former range is suitable for efficient detection in Si-based single photon detectors, or for addressing single atoms, and the latter represent the two most transparent wavelengths of the optical fiber. For these reasons we have for the first time in **Paper D** and **Paper B** reported on a single-pass two-crystals source of directly entangled

photon pairs using quasi-phase-matched crystals, that utilize the wavelength pair 810 nm and 1550 nm to be compatible with long-distance communication.

Furthermore, the single-mode optical fiber makes a perfect ground for interference experiments, as the spatial indistinguishability of the photons is naturally guaranteed. In this respect, and as a motivation for communication, it is important to efficiently collect the fragile photons into the fibers. In **Paper C** we showed how one can optimize the focusing of the pump beam and the fiber collection optics to achieve nearly perfect coupling into fibers, using bulk periodically poled crystals. To our knowledge, this is the first thorough investigation of focusing-techniques for optimizing the fiber-coupling in QPM materials. Supported by Boyd and Kleinman [1968], we think the results are general enough to cover also birefringent phase-matching, but our results seem not to agree with others' previous analysis on the topic for that case. Naturally, wave-guided structures seem beneficial to use to increase the coupling, as the mode of the waveguide can be constructed to match exactly that of the fiber. Indeed, some groups have reported very high photon fluxes. However, with our results at hand, we find it interesting to further understand if a wave-guided source is still preferable over a bulk crystal when both types are comparable in mode-quality, considering the more involved alignment of a waveguide. In addition, the effects of focusing in the pulsed regime in quasi-phase-matching is yet to be investigated. Our preliminary finding is that the emission becomes multimode if one does not compensate for the narrow pump pulse by using a long crystal.

Another issue is the photon flux and the bandwidth of the photons. The development of photon pair sources over the last few years have come quite far in terms of flux, and with respect to multiphoton probabilities per gate-period for a source producing Poisson distributed emission, it has nearly come to reach an upper limit. Rather, what is interesting to achieve is a higher conversion efficiency, possibly by using longer crystals and higher nonlinear index materials, so that the needed pump-power can be reduced and allow for more compact sources. Smooth transition to long crystals is another benefit of quasi-phase-matched materials, as they allow colinear propagation. The other essential need in quantum communication is to produce photons of a narrow bandwidth to avoid pulse broadening ($\sim$ GHz). Narrow filtering is usually not an option because it radically reduces the flux. However, longer crystals will produce narrower bandwidth at the same time as the photon flux is increased, as we showed in **Paper C**. This is valid also when the emission is coupled into fibers, as long as the focusing stays optimal. An even narrower bandwidth is needed to address atoms ($\sim$ MHz), which does not seem unforeseeable. It can be said that we have found no other similar work in the context of QPM.

Concerning the source's ability to produce entanglement, we have reported results in **Paper B** using two crystals to generate photons of two orthogonal polarizations. The output state is entangled in polarization, but due to that polarization is typically randomized along an optical fiber, we cast the polarization in the form of time encoding instead. One problem we came across was chromatic dispersion

in the crystals, due to the strongly non-degenerate wavelengths in a two-crystal configuration. The effect could be canceled by an extra piece of crystal. Our investigation on this special type of chromatic dispersion is the first we can find in the literature. Due to imperfections of the compensation the dispersion naturally leads to a small but noticeable residual degradation in the quality of entanglement. It would be preferable if Nature itself could take care of that process using decoherence free subspaces. Such states could be created by another type of phase matching process, $Z \rightarrow Z + X$, but if the dispersion effect is weak enough to be canceled that way, is something which we have yet to find out.

A few other words could be said about the future development of sources of entanglement in general. Many sources today still use very powerful and bulky lasers to pump the crystals, in some cases because it's the only type of laser that can deliver very short and high energy pulses, but in many cases also because wavelengths around 700-800 nm are aimed at for the photon pairs. However, blue laser diodes at 400 nm of sufficient power and mode-quality are becoming available, which means that polarization entanglement around 800 nm can be efficiently created in much more portable systems than before. It is also interesting to take note on progress of making intra-cavity parametric down-conversion inside laser diodes for the generation of photon pairs [Rossi *et al.*, 2004]. Such a structure would create entangled photons with much the same ease as a laser work.

Turning to applications, it is a near-term goal for our source of non-degenerate hybrid encoded entangled photon pairs in **Paper B** to be used in its current form for a demonstration of long-distance quantum key distribution. Using ideas from the quantum cryptography system developed in **Paper F**, which was the world's first demonstration of "plug and play" QKD at the 1550 nm telecom wavelength, it is also interesting to think of a variant to the scheme. Instead of Bob measuring his photon with an interferometer, the idea would be to directly reflect back his time-coded qubit using a Faraday mirror similar to the "plug and play" system, effectively realizing a long but very stable interferometer with Alice's side. Alice keep polarization coding on her qubit. In a coding scheme that reminds of dense coding, Bob, upon receiving his qubit of the pair, will change the phase of the qubit according to four possible phase-shifts. As the photonic qubit comes back to Alice, it carries two bits of information in two non-orthogonal bases, which then automatically is reconverted to polarization coding in the same device which transformed polarization to time in the first place. The entanglement of both qubits are then analyzed by Alice, who also checks for any eavesdropping, all in polarization. The nice feature of the scheme would be the combination of time-coding, entanglement, and a single self-stabilizing interferometer. The obvious disadvantage is that Bob's single photon needs to travel twice over the fiber.

At present, the maximum distance for doing quantum communication is less than 100 km because of the exponential decrease in bit rate with increasing distance. To reach longer distances quantum repeaters will inevitable be needed. One can reduce the probability of losing a photon, and hence limit the impact of detector dark-counts, and quantum bit error rates that sets the maximum secure distance,

by dividing the distance into smaller pieces of segments. A quantum repeater will in turn require the implementation of error correction, quantum interfaces, entanglement purification, and quantum memories — individual parts which today form a major experimental challenge on a 10 year time scale. In all parts, entanglement plays a fundamental role. A quantum repeater consists of many quantum relays, each measuring the relative correlations between two entangled states, and recreating new entangled states. Our ideas in **Paper E** for using a trusted third player and entanglement for authentication, could very well be used in this context for the implementation of a quantum repeater, where the relay station works as an authoritative site. In a quantum relay, a quantum memory is an essential component when two relays need to wait for each other until both hold entanglement. Some proposals for memories include Rubidium atoms, which respond to photons of a wavelength of typically 800 nm, making our non-degenerate source suitable as an interface to the 1550 nm photons that travel over the fibers. A quantum repeater require many different kinds of implementations of quantum systems to come together in a joint structure, making it a very challenging piece of work, as if the individual parts were not enough challenging. Nevertheless, its a very active field of research.

It is not an understatement to say that working with single photons to distribute information is a highly inefficient business. The efficiency with which we can detect a single photon is fairly low, $10-60\%$, the loss in optical fibers after 15 km is 50%, the flux of qubits is at most a few hundred kHz, the probability for a logical quantum gate to succeed is typically $6-25\%$, the bit rate in quantum cryptography systems is at best a few hundred bits per second, and the quantum bit error rate about $1-10\%$. These numbers should be compared to classical communication systems that are now working in terabit per second, with typical error probabilities of 10^{-12}, and CMOS-gate failure probabilities of 10^{-8} in ordinary processors. Nevertheless, as we have seen, the quantum world can offer is something entirely different from the classical, which makes such a comparison less interesting.

As anyone can observe, technology of the 20th century was dominated by the discovery of electromagnetism in the 19th century. Having recently entered a new millennium, we all witnessed the birth of information technology as a result of Shannon's information theory some 60 years ago. Logically, what can only be expected of the 21st century is that the discoveries of quantum theory and information theory of the 20th century merges and leaves footprints. In addition, it should be noted that similar to Moore's law in the semiconductor industry, the ever increasing bit rate in optical communication will inevitable lead to the single photon level. As the power per bit has to get lower to crank up the speed, and avoid overheating the systems, we will eventually reach the quantum domain at some point. At this point, presumably the quantum industry[1] is ready to take over.

[1]Regarding the future of quantum communication in political terms, it is quite clear that governments, like for example the EU, thinks it's becoming an important technology worth investments. In a global effort towards "Development of a Global Network for Secure Communication based on Quantum Cryptography" the EU is spending 11 million Euro in 4 years.

Appendix A

A comparison of photon sources

The table on the next page shows a detailed comparison of sources of photon-pairs based on results reported in the literature. All but one of the sources utilize nonlinear crystals to generate either entangled or unentangled photons-pairs. The meaning of some of the parameters are discussed in Section 3.6 and 4.3. Some numbers have been rederived using available data in order to make a fair comparison. We regret any errors that may have occurred in the process. Additional information regarding the content in the columns follows:

phasematching	wavelengths of the pump, signal and idler, and type of entanglement
crystal	type and length of nonlinear crystal
spatial mode	SM: single-mode fiber; MM: multimode fiber; and free-space
detec. sing.	r_s: detected rate of singles (signal)
detec. coin.	r_c: detected rate of coincidences
true corr.	R_c: rate of correlated pairs in either the fiber or in free-space, compensated for the detection efficiency
detected coin./sing.	$r_\mathrm{c}/r_\mathrm{s}$: fraction of detected correlated pairs to singles ($\mu = r_c/r_s\eta_i$ for heralded sources)
visibility	V: visibility of second-order correlation (entanglement)
prod. rate	$R_\mathrm{c}^\mathrm{prod}$: number of true correlated pairs per second, THz bandwidth of emission, and pump power in mW
CHSH-violation	S: degree of violation of the CHSH-inequality [Clauser *et al.*, 1969] ($S \leq 2.82$)
speed of CHSH-viol.	the number of standard deviations σ_S by which S is violated per $\sqrt{\mathrm{s}}$

group/publication	**phasematching** [nm]	**crystal** [mm]	**laser/ power** [mW]	**detectors** (det. eff.)	**spatial mode**	**filters** FWHM [nm]	**detec. sing.** r_s [s^{-1}]	**detec. coin.** r_c [s^{-1}]	**true corr.** R_c [s^{-1}]	**detected coin./ sing.** r_c/r_s	**visibility** [%]	**prod. rate** [s^{-1} THz^{-1} mW^{-1}]	**CHSH-violation** (time to measure $R_{\pm\pm}$)	**speed of CHSH-viol.** [$s^{-1/2}$]
Aspect, Grangier, and Roger, Phys. Rev. Lett. **49**, 91 (1982)	551 and 423 Polarization	Calcium-40 atoms	-	Photomult.	-	-	10000	40	-	0.004	-		2.679 ± 0.015 (500 sec.)	3.1
Kiess, Shih, Sergienko, and Alley, Phys. Rev. Lett. **71**, 3893 (1993)	351.1 → 702 + 702 Post-selected Type-II	BBO 0.5 mm	150 ?	Si APD ($\eta \approx 60\%$?)		1 nm		8.3	23			0.25		
Tapster, Rarity, Owens, Phys. Rev. Lett. **73**, 1923 (1994)	501.7 → 820 + 1300 Post-selected? Type-II?	$LiIO_3$ 20 mm	Ar^+	Si APD $\eta \approx 60\%$? Ge APD ($\eta \approx 10\%$?)	SM 4.3km	9.5 nm RG850	80000	1500	25000 ?	0.02 ($\mu = 20\%$)	86.9		2.458 ± 0.015 (6 sec.)	13
Kwiat, Mattle, Weinfurter, Zeilinger, Sergienko, and Shih, Phys. Rev. Lett. **75**, 4337 (1995)	351.1 → 702 + 702 Direct Polarization Type-II	BBO 3 mm	Ar^+ 150	Si APD ($\eta \approx 60\%$?)	Free space	5 nm		1500	4200 ?		97.8	9.2	2.649 ± 0.006 (18.75 sec.)	18
Tittel, Brendel, Gisin, and Zbinden, Phys. Rev. A **59**, 4150 (1999)	655 → 1310 + 1310 Post-selected Energy-time Type-I	$KNbO_3$ Diode 10	 Ge APD ($\eta \approx 5\%$)	SM? 9.3km, 8.1km	70 nm	34000– 39000	186–286	114000	≈0.007 ($\mu \approx 14\%$)	95.5	932	2.700 ± 0.028 (30 sec.)	8.4
Kwiat, Waks, White, Appelbaum, and Eberhard, Phys. Rev. A **60**, R773 (1999)	351.1 → 702 + 702 Direct Polarization Type-I	2×BBO $8 \times 8 \times 0.59$	Ar^+ 150 60	Si APD ($\eta \approx 65\%$)	Free space	 5 nm 10 nm	3500	175 21000 10000	 50000 24000	0.05 ($\mu = 7\%$)	 99.6	 110 65	 2.701 ± 0.003 (10 sec.)	 50
Jennewein, Simon, Weihs, Weinfurter, and Zeilinger, Phys. Rev. Lett. **84**, 4729 (2000)	351 → 702 + 702 Direct Polarization Type-II	BBO	Ar^+ 350	Si APD ($\eta \approx 35\%$?)	SM or MM? 0.5km		35000	1700	14000 ?	0.05 ($\mu = 14\%$)				
Tittel, Brendel, Zbinden, and Gisin, Phys. Rev. Lett. **84**, 4737 (2000)	655 → 1310 + 1310 Post-selected Time-bin Type-I	$KNbO_3$ $4 \times 3 \times 12$	Diode Pulsed 80MHz 1.0	Ge APD ($\eta \approx 5\%$)	SM?	$\Delta l = 20\mu m$ → 86 nm	4000– 7000	17	6800	0.004 ($\mu = 8\%$)	92.2	452	2.610 ± 0.050 (50 sec.)	1.8
Kim, Kulik, and Shih, Phys. Rev. A **62**, 011802 (2000)	400 → 800 + 800 Post-selected Polarization Type-I	2×BBO 3.4 mm	Ti:Sapp Pulsed 80fs 82MHz	Si APD ($\eta \approx 60\%$?)	Free space	40 nm		400			90			
Ribordy, Brendel, Gauthier, Gisin, and Zbinden, Phys. Rev. A **63** 012309 (2001)	532 → 810 + 1550 Direct Energy-time Type-I	$KNbO_3$ $3 \times 4 \times 10$	Nd:YAG 100	Si APD ($\eta = 60\%$?) InGaAs ($\eta = 8.5\%$)	SM	no filter → 5 nm @810 nm	1100000 Si	(65450) 500 (entangled)	(1300000) 9700	(0.06) ($\mu = 70\%$)	 91.8	(5500, unentangled!) 42	 2.600 ± 0.045 (2 sec.)	 9.4
Kurtsiefer, Oberparleiter, and Weinfurter, Phys. Rev. A **64**, 023802 (2001)	351.1 → 702 + 702 Direct Polarization Type-II	BBO 2 mm	Ar^+ 465 400	Si APD ($\eta = 60\%$?)	SM	4.6 nm	 1300000 420000	 360800 90000	 1000000 ? 250000 ?	 0.28 0.21 ($\mu < 47\%$)	 H,V 98.2 D,A 96.3	 768 223	 2.698 ± 0.003	 148
Banaszek, U'Ren, and Walmsley, Opt. Lett. **26**, 1367 (2001)	418 → 848 + 824 QPM	PPKTP 1 mm Waveguide	Ti:Sapp Pulsed 22μW	Si APD ($\eta = 60\%$?)	Free space + fibertip	6 nm	8150	1400	3900 ?	0.17 ($\mu = 28\%$)		(71000, unentangled!)		
Tanzilli, De Riedmatten, Tittel, Zbinden, Baldi, De Micheli, Ostrowsky, and Gisin, Electronics Lett. **37**, 26 (2001)	657 → 1314 + 1314 QPM	PPLN 32 mm Waveguide	Laser-diode CW 5.2μW	Ge APD ($\eta \approx 10\%$)	SM	30 nm	177000	1550	155000	0.009 ($\mu = 9\%$)		(5700000, unentangled!)		
Tanzilli, Tittel, De Riedmatten, Zbinden, Baldi, De Micheli, Ostrowsky, and Gisin, Eur. Phys. J. D **18**, 155 (2002)	657 → 1314 + 1314 Energy-time Time-bin QPM	PPLN 32 mm Waveguide	Diode Pulsed 400ps 80MHz 5μW	Ge APD ($\eta \approx 10\%$)	SM	40 nm		 750 90	 75000 9000		97.0 84.0	2100000	2.744 ± 0.04	14

group/publication	**phasematching** [nm]	**crystal** [mm]	**laser/ power** [mW]	**detectors** (det. eff.)	**spatial mode**	**filters** FWHM [nm]	**detec. sing.** r_s [s^{-1}]	**detec. coin.** r_c [s^{-1}]	**true corr.** R_c [s^{-1}]	**detected coin./ sing.** r_c/r_s	**visibi-lity** [%]	**prod. rate** [s^{-1} THz^{-1} mW^{-1}]	**CHSH-violation** (time to measure $R_{\pm\pm}$)	**speed of CHSH-viol.** [$s^{-1/2}$]
Bitton, Grice, Moreau, and Zhang, Phys. Rev. A **65**, 063805 (2002)	395 → 790 + 790 Direct Polarization Type-II	2×BBO 1 mm	Ti:Sapp Pulsed 76MHz 200	Si APD ($\eta = 60\%$?)	Free space			4000			73			
Nambu, Usami, Tsuda, Matsumoto, and Nakamura, Phys. Rev. A **66**, 033816 (2002)	266 → 532 + 532 Direct Polarization Type-I	2×BBO 0.13 mm	Ti:Sapp Pulsed 100fs 82MHz 150	Photomult. ($\eta = 40\%$)	Free space	8 nm 40 nm		450 2700	2800 17000		92.0 90.0	2.2 1	2.602 ± 0.020 2.546 ± 0.009	9 20
Mason, Albota, König, and Wong, Optics Letters **27**, 2115 (2002)	532 → 808 + 1559 Type-I	PPLN 20 mm	Nd:YAG ? 1-2	Si APD ($\eta = 54\%$) InGaAs ($\eta = 20\%$)	MM SM	1.26 nm	7560000 30000 10000 gate	600 200	5500	0.02 ($\mu = 10\%$)		(35000, unentangled!)		
Fiorentino, Messin, Kuklewicz, Wong, and Shapiro, Phys. Rev. A **69** 041801, (2004)	399 → 797 + 797 Direct Polarization Type-II	2×PPKTP (2 ways) 10 mm	Ti:Sapp CW 0.7	Si APD ($\eta = 60\%$)	Free space	3 nm	47000	8000	22000	0.18 ($\mu = 30\%$)	90.0	22000	2.599 ± 0.004 (15 sec.?)	38
Trojek, Schmid, Bourennane, and Weinfurter, Optics Express **12**, 276 (2004)	402.6 → 805 + 805 Direct Polarization Type-II	BB0 2 mm	Diode 24	Si APD ($\eta = 36\%$)	SM	6 nm	27000	5200	40000	0.19 ($\mu = 50\%$)	H,V 98.3 D,A 94.3	600	2.732 ± 0.017 (5 sec)	37
Fasel, Gisin, Ribordy, and Zbinden, Eur. Phys. J. D **30**, pp. 143-148 (2004)	532 → 814 + 1536 Direct Energy-time Type-I	$KNbO_3$ $3 \times 4 \times 10$	Nd:YAG 100	Si APD InGaAs ($\eta = 10\%$)	SM 30km	2/6.9 1.45/5.2 (814 nm/ 1536 nm)	79000 Si 36000 Si	3900 1800	39500 18000	0.05 0.05 (μ=50%)	89.0 92.0	436 199		
Li, Voss, Sharping, and Kumar, Phys. Rev. Lett. **94**, 053601 (2005)	1547 + 1525 Polarization Type-I	NFSI (non-linear fiber)	MIRA-OPO Pulsed 75MHz 0.39	InGaAs ($\eta_1 = 25\%$) ($\eta_2 = 20\%$)	SM	0.6 nm	4000 3000 (588kHz gate)	50 20	127000 50800	0.01 0.007 ($\mu < 5\%$)	93	4300000 1700000	2.750 ± 0.077	2.4
Altepeter, Jeffrey, and Kwiat, Optics Exp. **13**, 8951 (2005)	351 → 702 + 702 Direct Polarization Type-I	BBO 2×0.6 mm	280	Si APD ($\eta = 65\%$)	Free space	25 nm $T = 84\%$		1000000	3350000			555	2.726 ± 0.002	513
D. Ljunggren, P. Marsden, M. Tengner, I. Ghiu, I. Vellekoop and A. Karlsson, **Paper J** (2003)	775 → 1550 + 1550 Postselected Polarization Type-II	BBO 12 mm	Ti:Sapp 200 fs 82 GHz 100	InGaAs ($\eta = 18\%$)	SM	10/10	7000 (1 MHz gate)	70	2200	0.01		17 1400 (82	MHz gate)	
D. Ljunggren, M. Tengner, P. Marsden, and M. Pelton, **Paper B** (2005)	532 → 810 + 1550 Direct Polarization QPM	2×PPKTP 4.5 mm	Nd:YAG 4.5	Si APD ($\eta = 60\%$) InGaAs ($\eta = 18\%$)	SM	2/10 (810/ 1550 nm)	100000	2100 (10 ns gate)	19600	0.02 (μ=11%) (σ=32%)	H,V 99.6 D,A 94.2	4600	2.679 ± 0.004 (10 sec.)	56
M. Tengner and D. Ljunggren, **Paper A** (2005)	532 → 810 + 1550 Direct Polarization QPM	2×PPKTP 4.5 mm	Nd:YAG 1.2	Si APD ($\eta = 60\%$) InGaAs ($\eta = 18\%$)	SM	2 (810 nm)	88000	7200 (10 ns gate)	71000	0.08 (μ=48%) (σ=77%)		65000		

Bibliography

Agrawal, G. P. (1997), *Fiber-optic communication systems*, John Wiley and Sons, New York.

Aichele, T., A. I. Lvovsky, and S. Schiller (2002), *Optical mode characterization of single photons prepared by means of conditional measurements on a biphoton state*, Eur. Phys. J. D **18**, 237.

Alibart, O., D. B. Ostrowsky, P. Baldi, and S. Tanzilli (2005), *High-performance guided-wave asynchronous heralded single-photon source*, Opt. Lett. **30**(12), 1539.

Altepeter, J. B., E. R. Jeffrey, and P. G. Kwiat (2005a), *Advances in atomic, molecular, and optical physics*, Vol. 52, Chapt. Photonic State Tomography, Elsevier.

Altepeter, J. B., E. R. Jeffrey, and P. G. Kwiat (2005b), *Phase-compensated ultra-bright source of entangled photons*, Opt. Express. **13**(22), 8951.

Altepeter, J. B., E. R. Jeffrey, P. G. Kwiat, S. Tanzilli, N. Gisin, and A. Acin (2005c), *Experimental Methods for Detecting Entanglement*, Phys. Rev. Lett. **95**(3), 033601.

Aspect, A., P. Grangier, and G. Roger (1982), *Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities*, Phys. Rev. Lett. **49**(2), 91.

Banaszek, K., A. B. U'Ren, and I. A. Walmsley (2001), *Generation of correlated photons in controlled spatial modes by down-conversion in nonlinear waveguides*, Opt. Lett. **26**, 1367.

Bell, J. S. (1964), *On the Einstein-Podolski-Rosen Paradox*, Physics (Long Island City, N.Y.) **1**, 195.

Bennett, C. H. (1992), *Quantum cryptography using any two nonorthogonal states*, Phys. Rev. Lett. **68**, 3121.

Bennett, C. H., F. Bessette, G. Brassard, L. Salvail, and J. Smolin (1992), *Experimental quantum cryptography*, J. Cryptol. **5**(1), 3.

Bennett, C. H. and G. Brassard (1984), *Quantum Cryptography: Public Key Distribution and Coin Tossing*, in *Proc. of IEEE: Int. Conference on Computers, Systems and Signal Processing*, pp 175–179, Bangalore, India.

Bennett, C. H., G. Brassard, C. Crepeau, and U. M. Maurer (1995), *Generalized privacy amplification*, IEEE Trans. Inform. Theor. **41**(6), 1915.

Bennett, C. H., G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters (1993), *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Phys. Rev. Lett. **70**(13), 1895.

Bennett, C. H. and S. J. Wiesner (1992), *Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states*, Phys. Rev. Lett. **69**(20), 2881.

Bitton, G., W. P. Grice, J. Moreau, and L. Zhang (2002), *Cascaded ultrabright source of polarization-entangled photons*, Phys. Rev. A **65**(6), 063805.

Bourennane, M., A. Karlsson, J. P. Ciscar, and M. Mathes (2001), *Single-photon counters in the telecom wavelength region of 1550 nm for quantum information processing*, J. Mod. Opt. **48**(13), 1983.

Bouwmeester, D., A. Ekert, and A. Zeilinger (eds.) (2000), *The physics of quantum information*, Springer-Verlag, Berlin, Heidelberg.

Bouwmeester, D., J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger (1997), *Experimental quantum teleportation*, Nature **390**, 575.

Bovino, F. A., P. Varisco, A. M. Colla, G. Castagnoli, G. D. Giuseppe, and A. V. Sergienko (2003), *Effective Fiber-Coupling of Entangled Photons for Quantum Communication*, Opt. Commun. **227**, 343.

Boyd, G. D. and D. A. Kleinman (1968), *Parametric interaction of focused Gaussian light beams*, J. Appl. Phys. **39**, 3597.

Brassard, G. and L. Salvail (1994), *Secret Key Reconciliation by Public Discussion*, in T. Helleseth (ed.), *Advances in Cryptology — EUROCRYPT '93*, Vol. 765, pp 410–423, Springer-Verlag.

Brendel, J., N. Gisin, W. Tittel, and H. Zbinden (1999), *Pulsed Energy-Time Entangled Twin-Photon Source for Quantum Communication*, Phys. Rev. Lett. **82**, 2594.

Calsamiglia, J. and N. Lütkenhaus (2001), *Maximum efficiency of a linear-optical Bell-state analyzer*, Appl. Phys. B **72**, 61.

Castelletto, S., I. P. Degiovanni, A. Migdall, and M. Ware (2004), *On the measurement of two-photon single-mode coupling efficiency in parametric downconversion photon sources*, New J. Phys. **6**, 87.

Cerf, N. J., M. Bourennane, A. Karlsson, and N. Gisin (2002), *Security of Quantum Key Distribution Using d-Level Systems*, Phys. Rev. Lett. **88**(12), 127902.

Clauser, J. F., M. A. Horne, A. Shimony, and R. A. Holt (1969), *Proposed Experiment to Test Local Hidden-Variable Theories*, Phys. Rev. Lett. **23**, 880.

Cover, T. M. and J. A. Thomas (1991), *Elements of information theory*, John Wiley and Sons, New York.

Crépeau, C. and L. Salvail (1995), *Quantum Oblivious Mutual Identification*, in *Advances in Cryptology: Proceedings of Eurocrypt '95*, pp 133–146, Springer-Verlag.

Csiszár, I. and J. Körner (1978), *Broadcast channels with confidential messages*, IEEE Trans. Inform. Theor. **24**(3), 339.

de Riedmatten, H., I. Marcikic, J. A. W. van Houwelingen, W. Tittel, H. Zbinden, and N. Gisin (2005), *Long-distance entanglement swapping with photons from separated sources*, Phys. Rev. A **71**(5), 050302.

Dragan, A. (2004), *Efficient fiber coupling of down-conversion photon pairs*, Phys. Rev. A **70**(5), 053814.

Dusek, M., O. Haderka, M. Hendrych, and R. Myska (1999), *Quantum identification system*, Phys. Rev. A **60**(1), 149.

Einstein, A., B. Podolsky, and N. Rosen (1935), *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, Phys. Rev. **47**(10), 777.

Ekert, A. K. (1991), *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. **67**, 661.

Fasel, S., O. Alibart, S. Tanzilli, P. Baldi, A. Beveratos, N. Gisin, and H. Zbinden (2004a), *High-quality asynchronous heralded single-photon source at telecom wavelength*, New J. Phys. **6**, 163.

Fasel, S., N. Gisin, G. Ribordy, and H. Zbinden (2004b), *Quantum key distribution over 30 km of standard fiber using energy-time entangled photon pairs: a comparison of two chromatic dispersion reduction methods*, Eur. Phys. J. D **30**, 143.

Fiorentino, M., G. Messin, C. E. Kuklewicz, F. N. C. Wong, and J. H. Shapiro (2004), *Generation of ultrabright tunable polarization entanglement without spatial, spectral, or temporal constraints*, Phys. Rev. A **69**, 041801(R).

Fragemann, A. (2005), *Optical parametric amplification with periodically poled $KTiOPO_4$, Ph.D. thesis*, Royal Institute of Technology, Stockholm.

Franson, J. D. (1989), *Bell inequality for position and time*, Phys. Rev. Lett. **62**, 2205.

Gasparoni, S., J.-W. Pan, P. Walther, T. Rudolph, and A. Zeilinger (2004), *Realization of a Photonic Controlled-NOT Gate Sufficient for Quantum Computation*, Phys. Rev. Lett. **93**(2), 020504.

Gisin, N., G. Ribordy, W. Tittel, and H. Zbinden (2002), *Quantum cryptography*, Rev. Mod. Phys. **74**, 145.

Gobby, C., Z. L. Yuan, and A. J. Shields (2004), *Quantum key distribution over 122 km of standard telecom fiber*, Applied Physics Letters **84**(19), 3762.

Gottesman, D. (2003), *Uncloneable Encryption*, Quant. Inf. Comput. **3**, 581.

Gottesman, D. and I. L. Chuang (1999), *Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations*, Nature **402**, 390.

Grice, W. P. and I. A. Walmsley (1997), *Spectral information and distinguishability in type-II down-conversion with a broadband pump*, Phys. Rev. A **56**, 1627.

Hall, M. J. W. (1995), *Information Exclusion Principle for Complementary Observables*, Phys. Rev. Lett. **74**(17), 3307.

Hanbury Brown, R. and R. Q. Twiss (1956a), *Correlation between photons in two coherent beams of light*, Nature **177**, 27.

Hanbury Brown, R. and R. Q. Twiss (1956b), *The question of correlation between photons in coherent light rays*, Nature **178**, 1447.

Hanbury Brown, R. and R. Q. Twiss (1956c), *Test of new type of stellar interferometer on Sirius*, Nature **178**(4541), 1046.

Hardy, L. (1992), *Source of photons with correlated polarisations and correlated directions*, Phys. Lett. A **161**(4), 326.

Herbert, N. (1982), *FLASH-a superluminal communicator based upon a new kind of quantum measurement*, Foundations of Physics **12**(12), 1171.

Hong, C. K., Z. Y. Ou, and L. Mandel (1987), *Measurement of subpicosecond time intervals between two photons by interference*, Phys. Rev. Lett. **59**, 2044.

Hughes, R., G. Morgan, and C. Peterson (2000), *Quantum key distribution over a 48 km optical fibre network*, J. Mod. Opt. **47**(2-3), 533.

James, D. F. V., P. G. Kwiat, W. J. Munro, and A. G. White (2001), *Measurement of qubits*, Phys. Rev. A **64**, 052312.

Jennewein, T., C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger (2000), *Quantum Cryptography with Entangled Photons*, Phys. Rev. Lett. **84**, 4729.

Karlsson, H., F. Laurell, and L. K. Cheng (1999), *Periodic poling of $RbTiOPO_4$ for quasi-phase matched blue light generation*, Appl. Phys. Lett. **74**(11), 1519.

Kiess, T. E., Y. H. Shih, A. V. Sergienko, and C. O. Alley (1993), *Einstein-Podolsky-Rosen-Bohm experiment using pairs of light quanta produced by type-II parametric down-conversion*, Phys. Rev. Lett. **71**, 3893.

Kim, Y. H., S. P. Kulik, and Y. Shih (2000), *High-intensity pulsed source of space-time and polarization double-entangled photon pairs*, Phys. Rev. A **62**, 011802(R).

Kim, Y.-H., S. P. Kulik, and Y. Shih (2001), *Quantum Teleportation of a Polarization State with a Complete Bell State Measurement*, Phys. Rev. Lett. **86**(7), 1370.

Knill, E., R. Laflamme, and G. J. Milburn (2001), *A scheme for efficient quantum computation with linear optics*, Nature **409**, 46.

Koashi, M., T. Yamamoto, and N. Imoto (2001), *Probabilistic manipulation of entangled photons*, Phys. Rev. A **63**(3), 030301.

König, F., E. J. Mason, F. N. C. Wong, and M. A. Albota (2005), *Efficient and spectrally bright source of polarization-entangled photons*, Phys. Rev. A **71**(3), 033805.

Kuklewicz, C. E., M. Fiorentino, G. Messin, F. N. C. Wong, and J. H. Shapiro (2004), *High-flux source of polarization-entangled photons from a perodically-poled $KTiOPO_4$ parametric down-converter*, Phys. Rev. A **69**, 013807.

Kurtsiefer, C., M. Oberparleiter, and H. Weinfurter (2001), *High-efficiency entangled photon pair collection in type-II parametric fluorescence*, Phys. Rev. A **64**, 023802.

Kwiat, P. G., S. B.-L. abd André Stefanov, and N. Gisin (2001), *Experimental entanglement distillation and 'hidden' non-locality*, Nature **409**, 1014.

Kwiat, P. G., K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih (1995), *New High-Intensity Source of Polarization-Entangled Photon Pairs*, Phys. Rev. Lett. **75**, 4337.

Kwiat, P. G., A. M. Steinberg, and R. Y. Chiao (1993), *High-visibility interference in a Bell-inequality experiment for energy and time*, Phys. Rev. A **47**(4), R2472.

Kwiat, P. G., E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard (1999), *Ultrabright source of polarization-entangled photons*, Phys. Rev. A **60**, R773.

Landauer, R. (1996), *The physical nature of information*, Phys. Lett. A **217**(4), 188.

Langford, N. K., R. B. Dalton, M. D. Harvey, J. L. O'Brien, G. J. Pryde, A. Gilchrist, S. D. Bartlett, and A. G. White (2004), *Measuring Entangled Qutrits and Their Use for Quantum Bit Commitment*, Phys. Rev. Lett. **93**(5), 053601.

Leach, J., M. J. Padgett, S. M. Barnett, S. Franke-Arnold, and J. Courtial (2002), *Measuring the Orbital Angular Momentum of a Single Photon*, Phys. Rev. Lett. **88**(25), 257901.

Lee, P. S. K., M. P. van Exter, and J. Woerdman (2004), *Increased polarization-entangled photon flux via thinner crystals*, Phys. Rev. A **70**, 043818.

Lee, P. S. K., M. P. van Exter, and J. P. Woerdman (2005), *How focused pumping affects type-II spontaneous parametric down-conversion*, Phys. Rev. A **72**(3), 033803.

Lewenstein, M., B. Kraus, J. I. Cirac, and P. Horodecki (2000), *Optimization of entanglement witnesses*, Phys. Rev. A **62**(5), 052310.

Li, X., P. L. Voss, J. E. Sharping, and P. Kumar (2005), *Optical-Fiber Source of Polarization-Entangled Photons in the 1550 nm Telecom Band*, Phys. Rev. Lett. **94**(5), 053601.

Mair, A., A. Vaziri, G. Weihs, and A. Zeilinger (2001), *Entanglement of the orbital angular momentum states of photons*, Nature **412**, 313.

Mandel, L. and E. Wolf (1995), *Optical Coherence and Quantum Optics*, Cambridge University Press, Cambridge, UK.

Marcikic, I., H. de Riedmatten, H. Z. W. Tittel, and N. Gisin (2003), *Long-distance teleportation of qubits at telecommunication wavelengths*, Nature **421**, 509.

Mason, E. J., M. A. Albota, F. Knig, and F. N. C. Wong (2002), *Efficient generation of tunable photon pairs at 0.8 and 1.6 um*, Opt. Lett. **27**(23), 2115.

Mattle, K., H. Weinfurter, P. G. Kwiat, , and A. Zeilinger (1996), *Dense Coding in Experimental Quantum Communication*, Phys. Rev. Lett. **76**(25), 4656.

Mollow, B. R. and R. J. Glauber (1967), *Quantum Theory of Parametric Amplification. I*, Phys. Rev. **160**(5), 1076.

Monken, C. H., P. H. S. Ribeiro, and S. Pádua (1998), *Optimizing the photon pair collection efficiency: A step toward a loophole-free Bell's inequalities experiment*, Phys. Rev. A **57**(4), R2267.

Mérolla, J.-M., Y. Mazurenko, J.-P. Goedgebuer, and W. T. Rhodes (1999), *Single-Photon Interference in Sidebands of Phase-Modulated Light for Quantum Cryptography*, Phys. Rev. Lett. **82**(8), 1656.

Muller, A., T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin (1997), *"Plug and play" systems for quantum cryptography*, Appl. Phys. Lett. **70**(7), 793.

Muller, A., H. Zbinden, and N. Gisin (1996), *Quantum cryptography over 23 km in installed under-lake telecom fibre*, Europhys. Lett. **33**(5), 335.

Naik, D. S., C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat (2000), *Entangled state quantum cryptography: Eavesdropping on the Ekert protocol*, Phys. Rev. Lett. **84**, 4733.

Nambu, Y., K. Usami, Y. Tsuda, K. Matsumoto, and K. Nakamura (2002), *Generation of polarization-entangled photon pairs in a cascade of two type-I crystals pumped by femtosecond pulses*, Phys. Rev. A **66**(3), 033816.

Nielsen, M. A. and I. L. Chuang (2000), *Quantum computation and quantum information*, Cambridge University Press, Cambridge.

O'Brien, J. L., G. J. Pryde, A. G. White, T. C. Ralph, and D. Branning (2003), *Demonstration of an all-optical quantum controlled-NOT gate*, Nature **426**, 264.

Oppenheim, J. and M. Horodecki (2005), *How to reuse a one-time pad and other notes on authentication, encryption, and protection of quantum information*, Phys. Rev. A **72**(4), 042309.

Pan, J., D. Bouwmeester, H. Weinfurter, and A. Zeilinger (1998), *Experimental Entanglement Swapping: Entangling Photons That Never Interacted*, Phys. Rev. Lett. **80**, 3891.

Pan, J.-W., S. Gasparoni, R. Ursin, G. Weihs, and A. Zeilinger (2003), *Experimental entanglement purification of arbitrary unknown states*, Nature **423**, 417.

Pan, J.-W., C. Simon, Časlav Brukner, and A. Zeilinger (2001), *Entanglement purification for quantum communication*, Nature **410**, 1067.

Pati, A. K. (2002), *General impossible operations in quantum information*, Phys. Rev. A **66**(6), 062319.

Peres, A. (1995), *Quantum Theory: Concepts and Methods*, Kluwer Academic Publishers.

Peres, A. (2002), *How the no-cloning theorem got its name*, arXiv.org:quant-ph/0205076.

Pittman, T. B., B. C. Jacobs, and J. D. Franson (2001), *Probabilistic quantum logic operations using polarizing beam splitters*, Phys. Rev. A **64**(6), 062311.

Pittman, T. B., B. C. Jacobs, and J. D. Franson (2002), *Single photons on pseudo-demand from stored parametric down-conversion*, Phys. Rev. A **66**(4), 042303.

Pittman, T. B., B. C. Jacobs, and J. D. Franson (2004), *Heralding single photons from pulsed parametric down-conversion*, Opt. Commun. **246**, 545.

Pittman, T. B., D. V. Strekalov, D. N. Klyshko, M. H. Rubin, A. V. Sergienko, and Y. H. Shih (1996), *Two-photon geometric optics*, Phys. Rev. A **53**(4), 2804.

Poppe, A., A. Fedrizzi, R. Ursin, H. R. Böhm, T. Lörunser, O. Maurhardt, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger (2004), *Practical quantum key distribution with polarization entangled photons*, Opt. Express. **12**(16), 3865.

Ribordy, G., J. Brendel, J. D. Gauthier, N. Gisin, and H. Zbinden (2001), *Long-distance entanglement-based quantum key distribution*, Phys. Rev. A **63**, 012309.

Rossi, A. D., V. Ortiz, M. Calligaro, B. Vinter, J. Nagle, S. Ducci, and V. Berger (2004), *A third-order-mode laser diode for quantum communication*, Semicond. Sci. Technol **19**(10), L99.

Santori, C., D. Fattal, J. Vukovi, G. S. Solomon, and Y. Yamamoto (2002), *Indistinguishable photons from a single-photon device*, Nature **419**, 594.

Scarani, V., S. Iblisdir, N. Gisin, and A. Acin (2005), *Quantum cloning*, Rev. Mod. Phys. **77**(4), 1225.

Schneier, B. (1996), *Applied Cryptography*, J. Wiley, New York.

Schumacher, B. (1995), *Quantum coding*, Phys. Rev. A **51**(4), 2738.

Shannon, C. E. (1948), *A mathematical theory of communication*, Bell Syst. Tech. J. **27**, 379.

Shannon, C. E. (1949), *Communication theory of secrecy systems*, Bell Syst. Tech. J. **28**(4), 656.

Shor, P. W. (1994), *Algorithms for quantum computation: discrete logarithms and factoring*, in *Proc. of 35th IEEE FOCS*, pp 124–134, IEEE Press, Los Alamitos, CA.

Siegman, A. E. (1986), *Lasers*, University Science Books, Sausalito.

Siegman, A. E. (1993a), *Defining, measuring, and optimizing laser beam quality*, Laser Resonators and Coherent Optics: Modeling, Technology, and Applications **1868**(1), 2.

Siegman, A. E. (1993b), *Output Beam Propagation and Beam Quality from a Multimode Stable-Cavity Laser*, IEEE J. Quantum Electron. **29**(4), 1212.

Stinson, D. R. (1995), *Cryptography, Theory and Practice*, CRC press, New York.

Stucki, D., N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden (2002), *Quantum key distribution over 67 km with a plug&play system*, New J. Phys. **4**, 41.1.

Sun, P., Y. Mazurenko, and Y. Fainman (1995), *Long-distance frequency-division interferometer for communication and quantum cryptography*, Opt. Lett. **20**, 1062.

Tanzilli, S., H. D. Riedmatten, W. Tittel, H. Zbinden, P. Baldi, M. D. Micheli, D. Ostrowsky, and N. Gisin (2001), *Highly efficient photon-pair source using periodically poled lithium niobate waveguide*, Elec. Lett. **37**(1), 26.

Tanzilli, S., W. Tittel, H. D. Riedmatten, H. Zbinden, P. Baldi, M. D. Micheli, D. Ostrowsky, and N. Gisin (2002), *PPLN waveguide for quantum communication*, Eur. Phys. J. D **18**, 155.

Tapster, P. R., J. G. Rarity, and P. C. M. Owens (1994), *Violation of Bell's Inequality over 4 km of Optical Fiber*, Phys. Rev. Lett. **73**, 1923.

Tittel, W., J. Brendel, B. Gisin, T. Herzog, H. Zbinden, and N. Gisin (1998), *Experimental demonstration of quantum correlations over more than 10 km*, Phys. Rev. A **57**, 3229.

Tittel, W., J. Brendel, N. Gisin, and H. Zbinden (1999), *Long-distance Bell-type tests using energy-time entangled photons*, Phys. Rev. A **59**, 4150.

Tittel, W., J. Brendel, H. Zbinden, and N. Gisin (2000), *Quantum Cryptography Using Entangled Photons in Energy-Time Bell States*, Phys. Rev. Lett. **84**, 4737.

Tittel, W. and G. Weihs (2001), *Photonic entanglement for fundamental tests and quantum communication*, Quant. Inf. Comput. **1**(2), 3.

Townsend, P. (1994), *Secure key distribution system based on quantum cryptography*, Elec. Lett. **30**(10), 809.

Townsend, P. D., J. G. Rarity, and P. R. Tapster (1993), *Single photon interference in 10 km long optical fibreinterferometer*, Elec. Lett. **29**(7), 634.

Trojek, P., M. B. Ch. Schmid, and H. Weinfurter (2004), *Compact source of polarization-entangled photon pairs*, Phys. Rev. Lett. **12**(2), 276.

U'Ren, A. B., C. Silberhorn, K. Banaszek, and I. A. Walmsley (2004), *Efficient Conditional Preparation of High-Fidelity Single Photon States for Fiber-Optic Quantum Networks*, Phys. Rev. Lett. **93**(9), 093601.

Ursin, R., T. Jennewein, M. Aspelmeyer, R. Kaltenbaek, M. Lindenthal, P. Walther, and A. Zeilinger (2004), *Quantum teleportation across the Danube*, Nature **430**, 849.

Vellekoop, I. (2002), *Type-II downconversion in BBO crystal: Optimizing SPDC emission for fiber coupling*, *Master's thesis*, Royal Institute of Technology, IMIT, Kista, Sweden.

Vernam, G. S. (1926), *Cipher printing telegraph systems for secret wire and radio*, J. Amer. Inst. Elect. Eng. **55**, 109.

Waldebäck, J. (2005), *Single-photon detection at 1550 nm via frequency up-conversion*, *Master's thesis*, Royal Institute of Technology, IMIT, Kista, Sweden.

Walther, P. and A. Zeilinger (2005), *Experimental realization of a photonic Bell-state analyzer*, Phys. Rev. A **72**(1), 010302.

Wegman, M. N. and J. L. Carter (1981), *New hash functions and their use in authentication and set equality*, J. of Comp. and System Sc. **22**, 265.

Wiesner, S. (1983), *Conjugate coding*, Sigact News **15**(1), 78 .

Wootters, W. K. (1998), *Entanglement of Formation of an Arbitrary State of Two Qubits*, Phys. Rev. Lett. **80**, 2245.

Wootters, W. K. and W. H. Zurek (1982), *A single quantum cannot be cloned*, Nature **299**, 802.

Yariv, A. (1989), *Quantum electronics, Third edition*, John Wiley and Sons, New York.

Paper A

Characterization of an asynchronous source of heralded single photons generated at a wavelength of 1550 nm

M. Tengner and D. Ljunggren

in preparation (2006)

Contributions by the author: The candidate initiated the study of single photon generation from the perspective of heralded events. The preliminary theory was done by the candidate, and was further extended together with M. Tengner in a joint work. The first author prepared the paper based on joint writing and collected experimental data.

Characterization of an asynchronous source of heralded single photons generated at a wavelength of 1550 nm

Maria Tengner* and Daniel Ljunggren
Department of Microelectronics and Applied Physics,
Royal Institute of Technology, KTH, Electrum 229, SE-164 40 Kista, Sweden
(Dated: January 21, 2006)

We report on an asynchronous source of heralded single photons based on spontaneous parametric downconversion in a periodically poled, bulk $KTiOPO_4$ crystal. The source generates light with highly non-degenerate wavelengths of 810 nm and 1550 nm, where the 810 nm photons are used to announce the presence of the 1550 nm ones inside a single-mode optical fiber. We make a thorough analysis of how factors such as gate-period, photon rates, coupling efficiencies, and system losses affect the performance of the source. For our setup we find the probability of having a 1550 nm photon present at the output of the single-mode fiber, as announced by the 810 nm photon, to be 48%. The probability of multiphoton events is strongly suppressed compared to a poissonian light source giving highly sub-Poisson photon statistics.

PACS numbers: 03.67.Hk, 42.50.Ar, 42.50.Dv, 42.65.Lm

I. INTRODUCTION

Sources of single photons have become fundamentally important in all areas of quantum information processing dealing with photonic qubits, for example linear optics quantum computing and quantum communication. Consequently, many types of single photon sources have been developed, like molecule or atom emission [1, 2], nitrogen vacancies in diamond [3, 4], quantum dots [5, 6], etc., all having different properties like repetition rate, single-photon probability, and emission frequency. A promising alternative is so-called heralded single-photon sources (HSPS) [7–12], where photon pairs produced by spontaneous parametric downconversion (SPDC) are used to prepare conditional single photons [13]. One special property of single-photon sources, essential to most applications, is that the single photons are prepared in a well defined mode both temporally and spatially. In contrast to most other sources, HSPS have shown to successfully meet the latter requirement by optimizing the coupling into single-mode fibers [14–16]. However, it still leaves room for improvements on the statistics of the photon distributions in time, referred to as the temporal mode. Moreover, HSPS also provide a great flexibility in the choice of frequency for the single photons.

The basic idea of HSPS can be simply stated as having the detection event of one of the single-photons of a pair announcing the presence of its partner. The name "heralded" originates from the fact that the single-photons are not created on demand but rather announced by an external electric signal. In the realization presented here, this signal is not synchronous due to the use of a continuous wave (CW) pump laser for the SPDC process, therefore the source is called asynchronous.

*Corresponding author. Electronic address: mariate@imit.kth.se; URL: http://www.quantum.se

HSPS have been successfully implemented using a short-pulsed pump laser to get synchronous pulses containing single photons. Hereby one can avoid empty pulses to a high degree, a problem when using attenuated pulsed lasers as single-photon sources. In essence, the temporal statistics of the photons is controlled by utilizing apriori information. However, as long as the coherence time of the emission, Δt_c, is longer than the duration of the pump pulse, a single process of stimulated emission will take place [17] giving a thermal photon number distribution for the source [18]. This causes *bunching* effects, meaning that more than one photon is present. Such a property is unwanted and therefore pulsed pump lasers are not ideal to use. Along these arguments, the alternative is to use a CW laser as pump with a relatively long coherence length. In this case, as long as Δt_c is much shorter than the gate-period of the detector, there will be an incoherent collection of a large number of coherent SPDC processes present, each thermally distributed in photon number, but collectively giving a Poisson distribution [17, 19].

In this paper, we will show how it is advantageous in these respects to use CW light over pulsed light to herald the presence of single photons. By making temporal selection through conditional (heralded) gating to photon pairs output from a continuously pumped SPDC process, we can modify the photon number statistics even further than with pulsed light. By determining the autocorrelation $g^{(2)}(0)$ we can show either bunching, poissonian, or *antibunching* behavior depending on the chosen gate-period of the detector. In addition to lowering the probability of empty gates, the probability for higher photon numbers occupying a gate, can now also be decreased by using a shorter gate-period, as opposed to with pulsed light.

Following this analysis, we report the results of a source of heralded single-photons created by a quasi-phase-matched nonlinear crystal made of periodically poled $KTiOPO_4$ (PPKTP). The heralded photons have

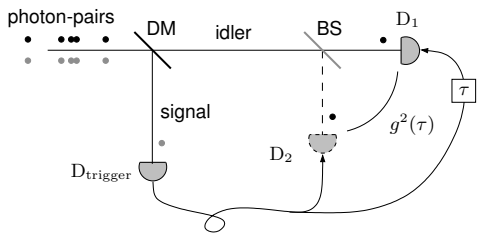

FIG. 1: Outline of a heralded single photon source. The autocorrelation function $g^{(2)}(\tau)$ can be measured using a Hanbury-Brown and Twiss detection scheme using two detectors, or $g^{(2)}(0)$ can be measured by a single detector when assuming a Poisson distribution in photon flux. DM: dichroic mirror; BS: beamsplitter.

a wavelength of 1550 nm, which makes them suitable for transmission in optical telecommunication fibers. To characterize the source we use the second-order autocorrelation function, which we derive formulas for in terms of singles rates, coincidence rates, and coupling parameters, assuming that the original photon distribution is poissonian. In this way we are able to determine the autocorrelation function at zero time-delay without needing to perform a Hanbury-Brown and Twiss correlation experiment [20], which is a non-straight forward task for a heralded and gated source [8].

The paper is organized as follows. In Sec. II we take a theoretical viewpoint and investigate the prospects for generating heralded single photons using the photon-pairs created by a CW laser in a nonlinear crystal. In Sec. III we describe the principal setup of the source and define the coupling parameters. We also show how these parameters are connected to the detected and derived photon rates. Section IV discusses the autocorrelation function and other measures to quantify the source in terms of system parameters. The result of the experiment is presented in Sec. V, and we round off with some conclusions and discussion in Sec. VI.

II. THEORY

The basic principle of the source is depicted in Fig. 1. Using different wavelengths of the trigger photon and the heralded photon the two are separated by a dichroic mirror. The trigger photon (signal) hits a detector and sends a signal to open the detector for the heralded photon (idler). Even for an ideal system, there will be a finite probability for more than a single photon to arrive within the gate-period of the detector—a behavior which can be characterized by the second-order autocorrelation function $g^{(2)}(t_1, t_2)$. (In this section we assume perfect detectors). The function can be found by a Hanbury-Brown and Twiss experiment [20] measuring the second-order cross correlation function using two detectors behind a beamsplitter, see Fig. 1. The true and continuous autocorrelation function is found in the limit of infinitely short detector gate-periods, $\Delta t_{\rm gate} \to 0$, for different time-delays $\tau = t_1 - t_2$, assuming stationary light. In terms of probabilities of photon counts, the autocorrelation function is given by

$$g^{(2)}(\tau) = \frac{2P_{m\geq 2}(\tau)}{P^2_{m\geq 1}(\tau)}. \qquad (1)$$

where $P_{m\geq k}$ is the probability to find k or more photons within the detector gate-period. The factor 2 in Eq. (1) origins from the fact that the probabilities are normalized to attain the maximum value of unity, which is not the case for $g^{(2)}(\tau)$ written in the standard form using the intensity of the light. (As the process we are dealing with is ergodic we are allowed to measure time averages instead of ensemble averages to find $g^{(2)}(\tau)$).

Using a single detector, D_1, it is clear that as $\tau \to 0$, the probability for a photon in the idler will be large conditioned on a photon in the signal, and that the probability of an empty gate is very small, or even zero, if the probability that the idler photon makes it from the source to the detector is unity. If also the gate-period, $\Delta t_{\rm gate}$, is made short, the probability of two or more photon within that gate becomes small as a result of the Poisson distribution in the number of photon arriving (as opposed to the case using a pulsed pump laser with thermal distribution). Hence, by gating in the temporal mode we hereby sub-select events to effectively change the original statistics. To quantify, we are thus interested in the autocorrelation function of the idler for $\tau = 0$,

$$g^{(2)}(0) = \frac{2P_{m\geq 2}}{P^2_{m\geq 1}}. \qquad (2)$$

It is a well known fact that for $g^{(2)}(0) < 1$ and $g^{(2)}(\tau \neq 0) > g^{(2)}(0)$ we have antibunching, hence sub-Poisson statistics, and for $g^{(2)}(0) > 1$ and $g^{(2)}(\tau \neq 0) < g^{(2)}(0)$ we have bunching, hence super-Poisson statistics.

We would like to characterize our source using this quantity, which is zero for perfect antibunching. Thus, we need to know the probabilities $P_{m\geq 2}$ and $P_{m\geq 1}$, which can be determined by assuming that the original distribution is Poisson (a valid assumption as long as $\Delta t_c \ll \Delta t_{\rm gate}$), and by measuring the mean accidental photon number per gate-period, $b = \Delta t_{\rm gate}\bar{R}$, where $\bar{R}$ is the singles rate of photons in counts per second. The probability for at least k photons to be present in the gate is given by

$$P_{m\geq k} = 1 - (1 - P^{\rm cor}P^{\rm acc}_{n\geq k-1})(1 - P^{\rm acc}_{n\geq k})) \qquad (3)$$

where $P^{\rm cor}$ is the probability that the "true" twin photon is present, and $P^{\rm acc}_{n\geq k}$ is the probability that k accidental photons are present. The former probability is unity for

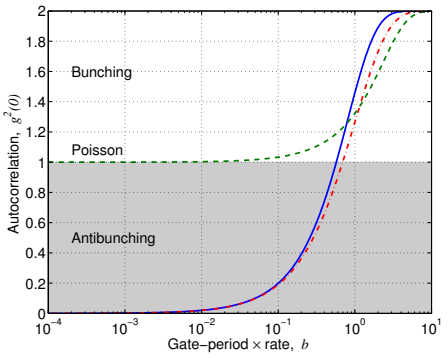

FIG. 2: (Color online) The value of the second-order autocorrelation function $g^2(\tau)$ at $\tau = 0$, showing the effects of antibunching or bunching depending on the detector gate-period and average photon rate for heralded single photons (solid blue line), where $b = \Delta t_{\rm gate}\bar{R}$ and $P^{\rm cor} = 1$. The dashed green line represents the statistics achieved for a poissonian source gated at random. The dash-dotted red line shows an approximation to the solid line for small b, using Eq. (5).

a perfect system, and the latter probability is given by

$$P^{\rm acc}_{n\geq k} = 1 - \sum_{j=0}^{k-1} \frac{e^{-b}b^j}{j!} \tag{4}$$

Note that in Eq. (2) we do not care if we herald a truly correlated pair, or an accidental, which can happen for lower than unity coupling efficiencies and transmission factors into the fibers. In Fig. 2 we have plotted Eq. (2) for different values of b. It is clear that the sub-selected statistics can show either antibunching or bunching. The statistics is poissonian for an intermediate value $b = 0.57$ for $P^{\rm cor} = 1$, and $b = 0.42$ for $P^{\rm cor} = 0.5$, given as two examples. Sufficiently large values of b will always give bunched light in the sense that there will always be more than one photon present within the gate-period. For two uncorrelated events that are each Poisson distributed, the $g^{(2)}(0)$ value follows instead the dashed line implying that such a source remains poissonian for short gate-periods or low photon flux, as opposed to a HSPS. Similarly, a thermal distribution due to pulsed light will remain super-poissonian. The expression for $g^{(2)}(0)$ for a CW pumped HSPS becomes a little unhandy, but can be approximated by

$$g^{(2)}(0) \approx 2[1 - e^{-b}], \tag{5}$$

which is valid for small b as shown by the dash-dotted line in the graph. For an ideal single photon source, the overall mean photon number $\langle n\rangle = b + P^{\rm cor}$, equals unity, which means that $b = 0$ and $P^{\rm cor} = 1$. In addition, the variance $\langle \Delta n^2\rangle$ of the mean photon number should be zero, as quantified by $g^{(2)}(0) = 1 + \frac{\langle \Delta n^2\rangle - \langle n\rangle}{\langle n\rangle^2}$.

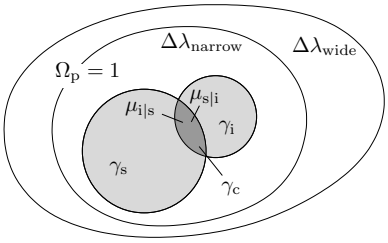

FIG. 3: A Venn diagram illustrating the single coupling efficiencies $\gamma_{\rm s}$ and $\gamma_{\rm i}$, pair coupling $\gamma_{\rm c}$ and conditional coincidences $\mu_{\rm s|i}$ and $\mu_{\rm i|s}$. The total amount of pairs within the filter bandwidth $\Delta\lambda$ is denoted $\Omega_{\rm p}$ and is normalized to unity.

Moreover, the probability for getting exactly n photons within the gate can also be expressed by the above probabilities as

$$P(n) = P_{m\geq 1} - \sum_{k=1}^{n-1} P(k) - P_{m\geq n+1}. \tag{6}$$

The probability $P(1)$ equals the parameter $\mu^{\rm her}$ commonly used to characterize sources of single photons, i.e. the probability that exactly single photon is heralded (ignoring if its a twin or an accidental for a non-perfect system).

III. COUPLING EFFICIENCIES AND PHOTON RATES

There are several different coupling efficiencies of interest in photon-pair sources. In this section we will define them and discuss their mutual relations in detail. For a schematic illustration of the different quantities see Fig. 3. All the coupling efficiencies are related to the bandwidth $\Delta\lambda$ of the light. The motivation for this is that the emission from SPDC has in general a very wide bandwidth that is preferably filtered before detection, either by bandpass filters $\Delta\lambda_{\rm BP}$ or by the spectral filtering performed by the single-mode fibers $\Delta\lambda_{\rm SM}$, such that $\Delta\lambda \leq \min(\Delta\lambda_{\rm BP}, \Delta\lambda_{\rm SM})$. The single-mode filtering is an effect of the correlation between each wavevector's spatial direction and frequency as determined by the phase-matching in the SPDC process. By normalizing to the bandwidth of interest we solely investigate how well photons within that bandwidth are collected into the fibers. Hence, as a natural consequence, with no spatial filtering the "coupling" is perfect, as e.g. in the case of a free-space detector or a multimode fiber (essentially), with a frequency filter in front.

With this in mind we denote the total number of photon-pairs generated within a given bandwidth $\Delta\lambda$, with $\Omega_{\rm p}$ and normalize it to 1. This set will of course

differ in size in the sense of absolute numbers of photon pairs, depending on the bandwidth of the chosen filter. The *single coupling efficiencies* for the signal, $\gamma_{\rm s}$, and idler, $\gamma_{\rm i}$, are the fraction of Ω_p that is coupled into the single-mode fibers, i.e. the probability to have a photon in the fiber which was emitted within the filter bandwidth $\Delta\lambda$. A high single coupling efficiency give a high photon rate, but do not guarantee a good quality heralded single-photon source. For that, a high *pair coupling efficiency* $\gamma_{\rm c}$, and high *conditional coincidences* $\mu_{\rm s|i}$ and $\mu_{\rm i|s}$ are required. The pair coupling efficiency states the amount of pairs where both photons are coupled into the two fibers, i.e. how large an overlap there is between the sets $\gamma_{\rm s}$ and $\gamma_{\rm i}$ in Fig. 3. It is important to note that in general $\gamma_{\rm c} \neq \gamma_{\rm s}\gamma_{\rm i}$, and instead of only optimizing the single coupling efficiencies it is crucial to maximize the overlap, i.e. to strive to couple the matching modes of the signal and idler into the fibers, in order to obtain a high pair coupling efficiency [15]. The conditional coincidence is the probability to have a photon in the fiber given that the partner photon of the pair is in its fiber.

All of these coupling efficiencies can be determined from the measured photon rates and parameters of the experimental setup such as losses and detector efficiencies. Referring to Fig. 4 we denote the total generated photon pair rate within the given bandwidth $\Delta\lambda$ just after the crystal $R_{\rm p}$. The photon rates inside the single-mode fibers are $R_{\rm s}$ and $R_{\rm i}$ for the signal and idler respectively. They are related to the single coupling efficiencies by

$$\gamma_{\rm s} = \frac{R_{\rm s}}{\zeta\delta_{\rm s}R_{\rm p}}, \qquad \gamma_{\rm i} = \frac{R_{\rm i}}{\delta_{\rm i}R_{\rm p}}, \tag{7}$$

where $\delta_{\rm s}$ and $\delta_{\rm i}$ are the total transmission factors for the signal and idler, stretching from the crystal to the detectors including all components such as filter transmission and reflection losses. Thus, $\delta_{\rm s} = \delta_{\rm i} = 1$ corresponds to an ideal system with no losses present other than from the fiber coupling. By weighting the coupling efficiencies by the transmission we obtain measures that solely describe how well the coupling into the fibers is performed. The factor $\zeta \leq 1$ compensates for the possible unmatched bandwidths of the interference filters of the signal and idler. When $\zeta = 1$ the filter bandwidths match (the relation between signal and idler for our choice of wavelengths is $\Delta\lambda_{\rm i}\zeta \approx 3.66 \times \Delta\lambda_{\rm s}$) while $\zeta < 1$ represents a narrower filter used for the signal than for the idler.

At the end of the fibers we have single photon detectors with quantum efficiencies $\eta_{\rm s}$ and $\eta_{\rm i}$. The signal detector measure the single photon rate $r_{\rm s}$. These detections serve as the heralding signal to the other detector, however it is routed via a delay/pulse generator which in turn provide the gate-pulse for the idler detector. We call the gate-pulse rate the heralding rate, denoted R_0. This signal announces the presence of the heralded single photon. In principle R_0 should equal $r_{\rm s}$ but in practice R_0 is lower because of the dead-time of the delay/pulse generator. The pulse gates the idler detector for a time

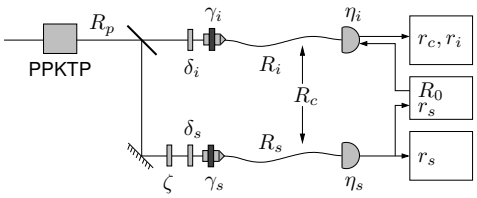

FIG. 4: Schematics of the experimental setup showing photon rates and relevant parameters. $R_{\rm p}$: rate of generated pairs; $\gamma_{\rm s}$ and $\gamma_{\rm i}$: single coupling efficiencies for signal and idler; $\delta_{\rm s}$ and $\delta_{\rm i}$: total transmissions from crystal to detectors; $R_{\rm s}$ and $R_{\rm i}$: total photon rates inside the fibers; ζ: compensating factor for unmatched filters between signal and idler; $R_{\rm c}$: rate of correlated pairs in the fibers; $\eta_{\rm s}$ and $\eta_{\rm i}$: detector efficiencies; $r_{\rm s}$: detected photon rate for the signal; R_0: heralding rate from delay generator; $r_{\rm c}$: detected coincidence rate; $r_{\rm i}$: rate of accidental coincidences.

$\Delta t_{\rm gate}$ during which the idler photon is expected to arrive at the detector. From the idler detector we then obtain the measured heralded coincidence photon rate $r_{\rm c}$. We also measure the accidental rate $r_{\rm i}$ at the idler detector, i.e. the single photon rate at random gating, to provide the mean accidental photon number in the Poisson distribution used later on. Also dark count rates $r_{\rm s}^{\rm d}$ and $r_{\rm i}^{\rm d}$ are measured for the two detectors, while after-pulsing effects are removed by an electrical hold-off circuit (10 μs).

In order to determine $R_{\rm p}$ the photon rate $r_{\rm p}$ for the signal is measured using a multi-mode fiber. $R_{\rm p}$ is then found as

$$R_{\rm p} = \frac{r_{\rm p}\alpha_{\rm p}^{\rm corr} - r_{\rm s}^{\rm d}}{\eta_{\rm s}\zeta\delta_{\rm s}}, \tag{8}$$

where $\alpha_{\rm p}^{\rm corr}$ is the correction factor at rate $r_{\rm p}$ for the signal detector, compensating the detected rate for the poissonian distribution of the arrivals of the photons. The photon rate for the signal inside the single-mode fiber, $R_{\rm s}$, is obtained in a similar way

$$R_{\rm s} = \frac{r_{\rm s}\alpha_{\rm s}^{\rm corr} - r_{\rm s}^{\rm d}}{\eta_{\rm s}}. \tag{9}$$

The idler fiber photon rate, $R_{\rm i}$, is calculated from the measured rate of accidental coincidences $r_{\rm i}$, i.e. the rate when the idler detector is randomly gated, using $r_{\rm i} = R_0 P_{\rm click}^{\rm acc}$, where

$$P_{\rm click}^{\rm acc} = 1 - (1 - P_{\rm light})(1 - P_{\rm dark}), \tag{10}$$

is the probability of a detector-click during one gate caused by light or dark count probabilities. Assuming a Poisson photon statistics within the gate, justified by a gate-period $\Delta t_{\rm gate}$ much larger than the coherence time $\Delta t_{\rm c}$ of the downconverted light, we have $P_{\rm light} = 1 - \exp\left(-\eta_{\rm i}\Delta t_{\rm gate}R_{\rm i}\right)$ and $P_{\rm dark} = \Delta t_{\rm gate} r_{\rm i}^{\rm d}/R_0$,

leading to

$$R_{\rm i} = \frac{1}{\eta_{\rm i}\Delta t_{\rm gate}} \ln\left(\frac{1-r_{\rm i}^{\rm d}/R_0}{1-r_{\rm i}/R_0}\right). \quad (11)$$

The pair coupling efficiency $\gamma_{\rm c}$ is defined via the rate of correlated pairs inside the fibers $R_{\rm c}$. This rate describes the amount of $R_{\rm p}$ where both the photons of a pair have coupled into their respective fiber, giving

$$\gamma_{\rm c} = \frac{R_{\rm c}}{\zeta\delta_{\rm s}\delta_{\rm i}R_{\rm p}}. \quad (12)$$

The correlated pair rate $R_{\rm c}$ is determined from the measured coincidence count rate $r_{\rm c} = R_0 P_{\rm click}^{\rm cor}$, where

$$P_{\rm click}^{\rm cor} = 1-(1-P_{\rm light}^{\rm cor})(1-P_{\rm dark})(1-P_{\rm light}^{\rm acc}), \quad (13)$$

once again is the probability of a detector-click during one gate, with $P_{\rm light}^{\rm cor} = \eta_{\rm i}R_{\rm c}/R_{\rm s}$ as the probability to detect the "true" twin photon, and $P_{\rm light}^{\rm acc} = 1-\exp\left[-\eta_{\rm i}\Delta t_{\rm gate}(R_{\rm i}-R_{\rm c}R_0/R_{\rm s})\right]$ as the probability to detect an accidental photon. The last minus term in the exponential exclude those events which are counted as true coincidences. In terms of photon rates we obtain an implicit expression for $R_{\rm c}$,

$$\frac{r_{\rm c}}{R_0} = 1-\left(1-\eta_{\rm i}\frac{R_{\rm c}}{R_{\rm s}}\right)\left(1-\frac{r_{\rm i}^{\rm d}}{R_0}\right)e^{-\eta_{\rm i}\Delta t_{\rm gate}(R_{\rm i}-R_{\rm c}R_0/R_{\rm s})}, \quad (14)$$

which can be solved numerically.

Having determined all the photon rates, we can calculate the different coupling efficiencies from Eq. (7), Eq. (12), and

$$\mu_{\rm i|s} = \frac{R_{\rm c}}{R_{\rm s}}, \qquad \mu_{\rm s|i} = \frac{R_{\rm c}}{R_{\rm i}}, \quad (15)$$

altogether describing how well optimized the fiber coupling is actually done in the experiment. Note that the conditional coincidences in Eq. (15) are the probabilities of having the "true" twin photon present, a property important when using downconversion sources to create entanglement. For a HSPS however, the significant quantity is $\mu^{\rm her} = P(1)$; the probability to herald exactly one photon, determined by Eq. (6). This procedure to determine rates and coupling efficiencies is not only relevant for heralded single-photon sources, but is applicable to other fiber-coupled downconversion sources as well [15, 21].

IV. HERALDED SINGLE- AND MULTI-PHOTON PROBABILITIES

As discussed in Sec. II, the characterizing quantities for a heralded single-photon source are the probabilities of the photon statistics. We will in this section relate these probabilities to the various photon rates and coupling efficiencies presented in Sec. III.

To obtain the $g^{(2)}(0)$-value for the source we need to determine the probabilities $P_{m\geq 1}$ and $P_{m\geq 2}$ according to Eq. (2). Expressed in terms of photon rates these probabilities are found to be

$$P_{m\geq 1} = 1-\left(1-\frac{R_{\rm c}}{R_{\rm s}}\right)e^{-b}, \quad (16)$$

$$P_{m\geq 2} = 1-\left(1-\frac{R_{\rm c}}{R_{\rm s}}\left(1-e^{-b}\right)\right)(1+b)\,e^{-b}, \quad (17)$$

where $b = \Delta t_{\rm gate}(R_{\rm i}-R_{\rm c}R_0/R_{\rm s})$. Inserting this into the expression for $g^{(2)}(0)$, Eq. (2), we obtain

$$g^{(2)}(0) = \frac{2\left[1-\left(1-\frac{R_{\rm c}}{R_{\rm s}}\left(1-e^{-b}\right)\right)(1+b)\,e^{-b}\right]}{\left[1-\left(1-\frac{R_{\rm c}}{R_{\rm s}}\right)e^{-b}\right]^2}. \quad (18)$$

A good approximation for small b is as seen in Fig. 2

$$g^{(2)}(0) \approx 2(1-e^{-bR_{\rm s}/R_{\rm c}}) \approx \frac{2bR_{\rm s}}{R_{\rm c}}, \quad (19)$$

for a non-ideal source with $P^{\rm cor} = R_{\rm c}/R_{\rm s}$, in contrast to Eq. (5), for which $P^{\rm cor} = 1$. Rewriting $g^{(2)}(0)$ using the coupling efficiencies in Eq. (7) and Eq. (12) we get

$$g^{(2)}(0) \approx 2\Delta t_{\rm gate}\left(\frac{\gamma_{\rm s}\gamma_{\rm i}}{\gamma_{\rm c}}R_{\rm p}-R_0\right). \quad (20)$$

For a ideal antibunched source $g^{(2)}(0) = 0$, so we want the value as small as possible. As seen from Eq. (20), $g^{(2)}(0)$ can always be made smaller by decreasing the number of generated photon pairs $R_{\rm p}$, i.e. by simply by lowering the pump power. However, for a single photon source to be useful for applications, high photon rates are in general desirable, so this does not seem like a sensible way to improve the performance of the source. We also conclude that a decrease of the single coupling efficiencies, $\gamma_{\rm s}$ and $\gamma_{\rm i}$, and an increase of the pair coupling, $\gamma_{\rm c}$, both lower $g^{(2)}(0)$. Since $\gamma_{\rm c} = \min(\gamma_{\rm s},\gamma_{\rm i})$ the optimal is to have all three equal, but also as small as possible. Again however, this leads to undesirably low photon rates. Decreasing the gate-period $\Delta t_{\rm gate}$ is also a possibility, and this seems like a more natural way to enhance the performance, since it essentially does not affect the photon rates. Yet, $\Delta t_{\rm gate}$ must still be kept much longer than the coherence time of the downconverted photons in order to maintain the Poisson photon statistics.

Using Eq. (6), Eq. (16) and Eq. (17) we find the expression for $\mu^{\rm her} = P(1)$ to be

$$\mu^{\rm her} = \left(1-\frac{R_{\rm c}}{R_{\rm s}}\right)be^{-b} + \frac{R_{\rm c}}{R_{\rm s}}(1+b)e^{-2b}. \quad (21)$$

V. EXPERIMENTAL RESULTS

The experimental setup of the source is shown in Fig. 5. A CW laser at a wavelength of 532 nm pumps a 4.5 mm

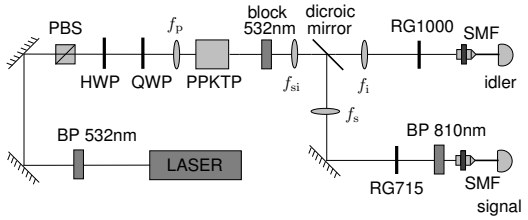

FIG. 5: The experimental setup of the heralded single photon source. PBS: polarizing beam splitter; HWP: half wave plate, QWP: quarter wave plate; BP: band pass filter; SMF: single-mode fiber.

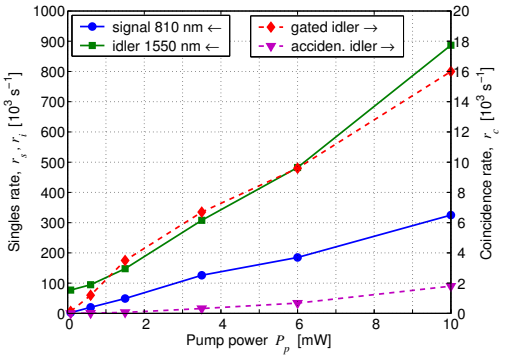

FIG. 6: (Color online) The singles rate of signal and idler, both in free-running mode (left axis). The idler's rate in counts per second is derived from randomly gated mode, with a gate-period $\Delta t_{\rm gate} = 10$ ns, at a rate R_0. The right axis shows the total gated coincidence rate $r_{\rm c}$ and the derived accidental coincidence rate $r_{\rm a}$.

long periodically poled potassium titanyl phosphate (PPKTP) bulk crystal. The crystal is poled with a period of 9.6 μm to assure collinear phase-matching for a signal and idler at 810 nm and 1550 nm, respectively. The pump's polarization is controlled by a polarizing beam splitter, a half wave plate, and a quarter wave plate, before focusing the light onto the crystal with an achromatic doublet ($f_{\rm p} = 50$ mm). Directly after the crystal the pump light is blocked by a bandstop filter. The signal and idler emission is refocused by an achromatic doublet ($f_{\rm si} = 30$ mm) before split by a dichroic mirror, then collimated by two additional lenses ($f_{\rm s} = 60$ mm, $f_{\rm i} = 40$ mm), and finally focused into single-mode fiber by aspherical lenses ($f = 11$ mm) following predictions in [15]. In front of the signal fiber-coupler a Schott-RG715 filter is placed to block any remaining pump light, together with an interference filter at 2 nm (FWHM). For the idler it suffice a Schott-RG1000 filter to block the last residue of the pump, giving an estimated single-mode bandwidth of 15 nm (FWHM) for the accidental photons and 7 nm (FWHM) for the coincidence photons. The detectors used are a Si-based APD (PerkinElmer SPCM-AQR-14) for the 810 nm light with a quantum efficiency $\eta_s = 60\%$, and a homemade InGaAs-APD (Epitaxx) module for the 1550 nm light with $\eta_i = 18\%$. The detection of a 810 nm photon triggers the digital delay generator (DG535 from SRS), which, in turn, generates a gate-pulse for the 1550 nm detector.

We measured the singles- and coincidence photon rates for different pump powers by varying the power using neutral density filters. As expected, both singles, coincidences, and accidental counts increase with the pump power, see Fig. 6. The pump power 1.2 mW was chosen for the subsequent measurements. Histograms of the coincidence rate for different delays of the gate-signal can be seen in Fig. 7. The gate delay was moved within a 12 ns window for the two cases of gate-periods, $\Delta t_{\rm gate}$, of 2 ns and 4 ns. We can observe that the coincidences are well localized in time for both cases. The total number of coincidences are lower for the 2 ns gate-period than for the 4 ns gate-period due to the limited rise time of the gate-pulse, and a lower excess gate voltage for shorter gate-periods, causing a drop in the detector quantum efficiency.

We have optimized the fiber coupling with the goal of obtaining an as high conditional coincidence as possible, which did not correspond to the highest possible single coupling efficiencies. The resulting detected single counts rate for the signal was $r_{\rm p} = 218 \times 10^3$ s^{-1} with the multi-mode fiber, and $r_{\rm s} = 88 \times 10^3$ s^{-1} with the single-mode fiber. The latter rate resulted in a gate-rate $R_0 = 81 \times 10^3$ s^{-1}, and a detected coincidence rate $r_{\rm c} = 7200$ s^{-1} for a gate-period $\Delta t_{\rm gate} = 10$ ns. Accidental coincidences, i.e. coincidences measured with random gating, was $r_{\rm i} = 130$ s^{-1}. The dark count for the signal detector was $r_{\rm s}^{\rm d} = 90$ s^{-1} and for the idler detector $r_{\rm i}^{\rm d} = 40$ s^{-1} at gate-rate R_0. The overall transmission factors in the signal and idler arm were $\delta_{\rm s} = 54\%$ and $\delta_{\rm i} = 63\%$, as determined by sending strong laser light at the corresponding frequency through the setup and

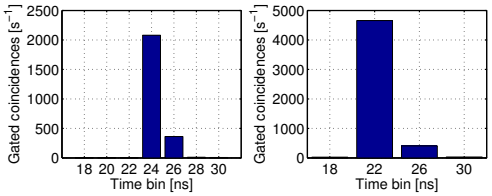

FIG. 7: The rate of gated coincidences, $r_{\rm c}$ for different delays of the gate-signal at a gate-rate $R_0 = 65 \times 10^3$ s^{-1}. The gate-period, $\Delta t_{\rm gate}$, was in the left histogram 2 ns and in the right 4 ns.

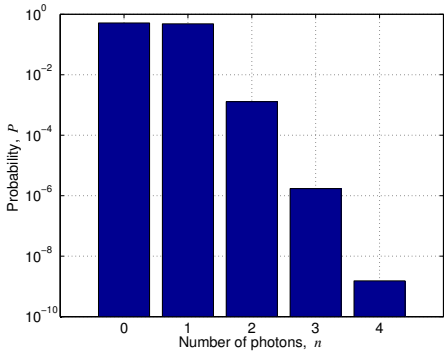

FIG. 8: The probability distribution, $P(n)$, of the idler photon number, n, as a result of gating the idler conditioned upon detection of a signal photon. The numbers are the results of an experiment at a pump power, $P_{\rm p} = 1.2$ mW, average photon-rate $\bar{R} = 1270 \times 10^3$ s^{-1}, and gate-rate $R_0 = 81 \times 10^3$ s^{-1}.

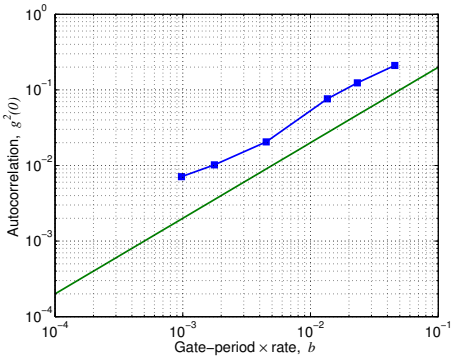

FIG. 9: The autocorrelation $g^{(2)}(0)$ as a function of $b = \Delta t(R_{\rm i} - R_{\rm c}R_0/R_{\rm s})$ with $\Delta t_{\rm gate} = 10$ ns. The upper line shows the experimental data where b has been varied by changing the pump power (0.08, 0.6, 1.5, 3.5, 6, and 10 mW). The lower line is the theoretical curve with $P^{\rm cor} = 1$.

measuring the loss. The 2 nm interference filter for the signal and no interference filter for the idler give $\zeta = 0.5$. With these measured photon rates and setup parameters the actual photon rates were calculated using the expressions in Sec. III, obtaining a generated photon-pair rate $R_{\rm p} = 1340 \times 10^3$ s^{-1}, photon rates inside the single-mode fibers $R_{\rm s} = 147 \times 10^3$ s^{-1}, and $R_{\rm i} = 615 \times 10^3$ s^{-1}, and correlated pair rate inside the fibers $R_{\rm c} = 71 \times 10^3$ s^{-1}. This resulted in single coupling efficiencies $\gamma_{\rm s} = 40\%$ and $\gamma_{\rm i} = 71\%$, pair coupling efficiency $\gamma_{\rm c} = 31\%$, and conditional coincidences $\mu_{\rm i|s} = 48\%$ and $\mu_{\rm s|i} = 12\%$.

With the calculated photon rates the heralded photon statistics was determined, see Fig. 8. The probability to have zero photons present within the gate-period was $P(0) = 0.514$, and the probability to have exactly one photon present was $\mu^{\rm her} = P(1) = 0.483$. The probabilities for higher number of photons drop off rapidly, with $P_{m\geq 1} = 0.486$, and $P_{m\geq 2} = 0.0028$, giving $g^{(2)}(0) = 0.0235$. For the different pump powers in Fig. 6, $g^{(2)}(0)$ was also calculated, showing to grow linearly with pump power via the b parameter, see Fig. 9, all in agreement with Eq. (20).

VI. CONCLUSIONS AND DISCUSSION

In this article we have made an analysis of an asynchronous heralded single-photon source in terms of photon rates, gate-periods, coupling efficiencies etc. We have determined the photon number statistics and found it to be highly sub-poissonian. We have also calculated the autocorrelation $g^{(2)}(\tau = 0)$, and concluded that it is not a fully satisfactory measure for HSPS, since it can for example be improved by simply lowering the overall photon rate as also noted by [8]. However, in a different aspect, we have noted that the autocorrelation at $\tau = 0$ is proportional to the variance of the mean photon number for a source both with or without losses, turning $g^{(2)}(0)$ into a rather good measure if related to the mean *accidental* photon number b.

If one compare synchronous and asynchronous HSPS, i.e. sources with pulsed and CW pump lasers, regarding photon number statistics, there are some distinct differences. For a short-pulsed source, the SPDC process can be seen as a single coherent process that creates photon pairs spread in creation-time not more than the duration of the pump-pulse $\Delta t_{\rm p}$, giving a thermal photon number statistics for the heralded photons as long as the coherence time $\Delta t_{\rm c} > \Delta t$. This situation is rather easily achieved by short-pulsed lasers and narrow bandpass filters for the emission, alternatively, with long down-conversion crystals to increases the coherence length. If $\Delta t_{\rm c} < \Delta t_{\rm p}$ but $\Delta t_{\rm c} > \Delta t_{\rm gate}$ we still have the same situation, but now with the gate-period as the limiting factor, selecting photons originating from a single process. However, this situation is rather unrealistic using pulsed lasers, since it requires $\Delta t_{\rm gate} \ll \Delta t_{\rm p}$. If instead $\Delta t_{\rm c} \ll \Delta t_{\rm p}$ and $\Delta t_{\rm gate}$, there will be a large collection of processes, all individually with a thermal distribution, but collectively giving a Poisson distribution.

For a CW source all the different single SPDC processes can in principle be arbitrarily spread over time. In such a case the gate-period in relation to the coherence time sets the type of distribution in photon number statistics. Still, for $\Delta t_{\rm c} > \Delta t_{\rm gate}$ the photons within the gate can be seen as originating from a single SPDC process, hence with a thermal photon number statistics. However, for $\Delta t_{\rm c} \ll \Delta t_{\rm gate}$ we have a large collection of processes collectively providing a Poisson distribution.

By sub-selecting temporal modes (events) by conditional gating, using a CW pump, the photon number distribution can be further altered to show sub-Poisson statistics, effectively decreasing both the probability of a falsely heralded single photon, and suppressing the probability of multi-photon events. In our experiment there is still a probability of false announcements of 52%, but in contrast to attenuated coherent pulses it is primarily of an experimental challenge to lower the fraction of such events by increasing the coupling efficiencies or the transmission factors, and not a fundamental problem.

VII. ACKNOWLEDGMENTS

We would like to thank Anders Karlsson and Gunnar Björk for fruitful discussions, A. Fragemann, C. Canalias and F. Laurell for providing us with the crystals, and J. Waldebäck for his help with electronics. Financial support by the European Commission through the integrated project SECOQC (Contract No. IST-2003-506813) and by the Swedish Foundation for Strategic Research (SSF) is acknowledged.

[1] F. D. Martini, G. D. Giuseppe, and M. Marrocco, Phys. Rev. Lett. **76**, 900 (1996).
[2] B. Lounis and W. E. Moerner, Nature **407**, 491 (2000).
[3] C. Kurtsiefer, S. Mayer, P. Zarda, and H. Weinfurter, Phys. Rev. Lett. **85**, 290 (2000).
[4] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat, and P. Grangier, Phys. Rev. Lett. **89**, 187901 (2002).
[5] M. Pelton, C. Santori, J. Vuckovic, B. Zhang, G. S. Solomon, J. Plant, and Y. Yamamoto, Phys. Rev. Lett. **89**, 233602 (2002).
[6] V. Zwiller, P. Jonsson, H. Blom, S. Jeppesen, M.-E. Pistol, L. Samuelson, A. A. Katznelson, E. Y. Kotelnikov, V. Evtikhiev, and G. Björk, Phys. Rev. A **66**, 053814 (2002).
[7] T. B. Pittman, B. C. Jacobs, and J. D. Franson, Opt. Commun. **246**, 545 (2005).
[8] S. Fasel, O. Alibart, S. Tanzilli, P. Baldi, A. Beveratos, N. Gisin, and H. Zbinden, New J. Phys. **6**, 163 (2004).
[9] S. Takeuchi, R. Okamoto, and K. Sasaki, Appl. Opt. **43**, 5708 (2004).
[10] O. Alibart, D. B. Ostrowsky, P. Baldi, and S. Tanzilli, Opt. Lett. **30**, 1539 (2005).
[11] A. B. U'Ren, C. Silberhorn, J. L. Ball, K. Banaszek, and I. A. Walmsley, Phys. Rev. A **72**, 021802 (2005).
[12] E. J. Mason, M. A. Albota, F. König, and F. N. C. Wong, Opt. Lett. **27**, 2115 (2002).
[13] C. K. Hong and L. Mandel, Phys. Rev. Lett. **56**, 58 (1986).
[14] C. Kurtsiefer, M. Oberparleiter, and H. Weinfurter, Phys. Rev. A **64**, 023802 (2001).
[15] D. Ljunggren and M. Tengner, Phys. Rev. A **72**, 062301 (2005).
[16] S. Castelletto, I. P. Degiovanni, V. Schettini, and A. Migdall, Opt. Express. **13**, 6709 (2005).
[17] H. de Riedmatten, V. Scarani, I. Marcikic, A. Acín, W. Tittel, H. Zbinden, and N. Gisin, J. Mod. Opt. **51**, 1637 (2004).
[18] B. R. Mollow and R. J. Glauber, Phys. Rev. **160**, 1076 (1967).
[19] S. Mori, J. Söderholm, and S. I. Naoto Namekata (2005), arXiv.org:quant-ph/0509186.
[20] R. Hanbury Brown and R. Q. Twiss, Nature **177**, 27 (1956).
[21] D. Ljunggren, M. Tengner, P. Marsden, and M. Pelton, (to be published) (2006).

Paper B

Theory and experiment of entanglement in a quasi-phase-matched two-crystal source

D. Ljunggren, M. Tengner, P. Marsden, and M. Pelton

to be published in Phys. Rev. A (2006)

Contributions by the author: The candidate proposed to carry out a deeper study on the generation of entanglement in order to increase the quality of the source, and initiated further work. The candidate developed the theory together with M. Tengner, and wrote the paper. The co-authors took part of the problem and the experiment at an initial stage. The main experimental work was carried out by the first two authors.

Theory and experiment of entanglement in a quasi-phase-matched two-crystal source

Daniel Ljunggren,* Maria Tengner, Philip Marsden,† and Matthew Pelton‡
Department of Microelectronics and Information Technology,
The Royal Institute of Technology, KTH, Electrum 229, SE-164 40 Kista, Sweden
(Dated: October 8, 2005)

We report new results regarding a source of polarization entangled photon-pairs created by the process of spontaneous parametric downconversion in two orthogonally oriented, periodically poled, bulk $KTiOPO_4$ crystals (PPKTP). The source emits light colinearly at the non-degenerate wavelengths of 810 nm and 1550 nm, and is optimized for single-mode optical fiber collection and long-distance quantum communication. The configuration favors long crystals, which promote a high photon-pair production rate at a narrow bandwidth, together with a high pair-probability in fibers. The quality of entanglement is limited by chromatic dispersion, which we analyze by determining the output state. We find that such a decoherence effect is strongly material dependent, providing for long crystals an upper bound on the visibility of the coincidence fringes of 41% for $KTiOPO_4$, and zero for $LiNbO_3$. The best obtained raw visibility, when canceling decoherence with an extra piece of crystal, was $91 \pm 0.2\%$, including background counts. We confirm by a violation of the CHSH-inequality ($S = 2.679 \pm 0.004$ at 55 $s^{-1/2}$ standard deviations) and by complete quantum state tomography that the fibers carry high-quality entangled pairs at a maximum rate of 55×10^3 $s^{-1}THz^{-1}mW^{-1}$.

PACS numbers: 03.67.Mn, 03.67.Hk, 42.50.Dv, 42.65.Lm

I. INTRODUCTION

A nonlinear medium exposed to an optical field will occasionally emit several other photons. The phenomenon is known as spontaneous parametric downconversion (SPDC), and is frequently utilized for the production of photon-pairs. Such a pair can also become entangled in a certain degree of freedom if indistinguishability is ensured in all the remaining degrees of freedom. Many successful examples of direct creation of entangled photon-pairs [1–3], post-selected entangled pairs [4–6], and in-fiber generated pairs [7–9] can be given, already serving as an indispensable tool for quantum communication.

The source reported here uses two orthogonally oriented crystals, each emitting pairs of photons of a different polarization than the other. The different pairs are made indistinguishable, in our case by single-mode fibers, and therefore the individual photons of a single pair become directly entangled in polarization — an idea originally proposed by Hardy [10] and realized in modified form by Kwiat *et al.* [11]. One problem with the original realization is that the crystals cannot be made too long, since the non-colinearity makes the two emission-cones non-overlapping. Another problem is that the crystals used generally emit into many spatial modes, which is not suitable for fiber-coupling. Using periodically poled crystals via quasi-phase matching [12–14], it has been shown that colinear emission can be achieved very close to a single mode [15] (even in non-waveguiding structures), providing much greater overlap in the emission. Such a configuration also allows non-degenerate wavelengths to be generated.

Some desirable properties of photon-pair sources to be used for quantum communication include: i) a high probability of photon-pairs to be collected into optical fibers; ii) a minimum number of false coincidences; iii) wavelength combinations that either suit efficient detection, match atomic transitions, or are well transmitted over long distances; iv) a narrow bandwidth that limits the effects of fiber dispersion ($\sim$ GHz) [16] or can address atoms ($\sim$ MHz); v) a long coherence length that limits the need for precise interferometry; vi) small jitter in arrival-time of photons; vii) perfect correlations in all bases; and, ideally, viii) the source being compact enough to be put in a box, carried out of the lab, and be used, e.g., for quantum key distribution (QKD). Furthermore, for maximum security in QKD a strong requirement is to have neither more nor less than a single photon per gate pulse. In this respect, photon-pair sources have been shown to be good candidates compared to weak coherent pulses, potentially fulfilling properties i) and ii). Equally imperative for security in Ekert's scheme [17] is property vii), which expresses the wish for high visibility of entanglement in the presence of background detection, which implies the need to minimize dark counts and false coincidence counts.

In this work, we extend our previous results [18] regarding a PPKTP-based two-crystal source and try to address some of the anticipated features above. By emitting at non-degenerate wavelengths, the source exploits the highly efficient Si-based single-photon counters available in the near-infrared region and the low attenuation in fibers at telecom wavelengths. The shorter wavelength also matches the transmission bands of alkaline atoms,

*Corresponding author. Electronic address: daniellj@kth.se; URL: http://www.quantum.se
†Current address: Department of Physics, University of Toronto, Toronto M5S 1A7, Canada
‡Current address: Department of Physics, University of Chicago, Chicago, IL 60637, USA

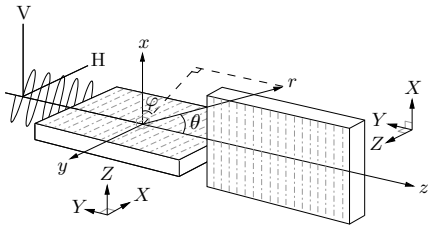

FIG. 1: The source consists of two PPKTP crystals placed one after the other; the first creates a vertically (V) and the second a horizontally (H) polarized field. The laboratory coordinate system is drawn, as well as the crystal axes, X, Y, and Z, which refer to the polarization of the incoming and outgoing electromagnetic fields.

which makes the source suitable as part of a quantum memory [19, 20]. For our crystal configuration, we show how effects like chromatic dispersion enter the picture as problems to be dealt with. The source has been optimized for coupling into single-mode fibers following Ref. [15], where one can also find motivations for using long crystals to achieve a narrow bandwidth. An early example of a non-degenerate source is Ref. [21], using energy-time entanglement. One reason for utilizing energy-time entanglement is to overcome the strong decoherence mechanism of polarization-states over fibers, and, for the same reason, we propose a scheme that combines time-multiplexed encoding on the telecom wavelength side [22] with polarization on the near-infrared side, altogether realizing a sort of hybrid-coded entanglement.

The article is organized as follows. In section II, we describe the main characteristics of the source. In section III, we derive the quantum state emitted by the two crystals in terms of frequency and polarization degrees of freedom, based on the quantum state of a single crystal derived in the Appendix. Following that, in section IV, we briefly show how to compensate for the effect of chromatic dispersion in the crystals, so as to assure indistinguishability, and, in section V, we present our experimental results showing the quality of the source, including results on quantum state tomography. In section VI, we discuss the future directions of a hybrid-coded source, and we end with a summary in section VII.

II. A SOURCE OF POLARIZATION ENTANGLEMENT

The source is depicted in Fig. 1, and consists of two orthogonally aligned bulk crystals placed one after the other. They each have the dimensions $3 \times 4.5 \times 1$ mm (X, Y, Z), of which the second dimension defines the length, $L = 4.5$ mm. The crystals are made of potassium titanyl phosphate, $KTiOPO_4$, and are periodical poled with the period $\Lambda = 9.6$ μm, chosen such that we have phase-matching for the signal at a wavelength of 810 nm, and the idler at 1550 nm, for a temperature $T = 111$ °C determined by the Sellmeier equations of KTP [23, 24]. The crystals are pumped by monochromatic and continuous wave laser light (p) at a wavelength of 532 nm, which is propagating in a Gaussian TEM_{00} mode along the z-axis, producing a signal (s) and idler (i) field in the same direction and with the same polarization as the Z-component of the pump field ($Z_\mathrm{p} Z_\mathrm{s} Z_\mathrm{i}$). Fig. 1 defines the laboratory axes and the crystals' optical axes X, Y, and Z, oriented as shown. Both crystals will generate down-converted light if the pump polarization is oriented at 45° to the horizontal (H) and vertical (V) axes. Following [15], we have optimized the focusing of the pump and the fiber-matched modes using the parameter $\xi = L/z_R$, where L is the length of the crystal and z_R is the Rayleigh range, such that a maximum amount of the emission that is generated is collectible into single-mode fibers. The optimal values for our configuration are $\xi_\mathrm{p} = 1.3$, $\xi_\mathrm{s} = 2.0$, and $\xi_\mathrm{i} = 2.3$, respectively.

The use of single-mode fibers to collect the light will erase all spatial information that reveals from which crystal the photons came, except for the polarization degree of freedom. Therefore, each of the beams will interfere in the diagonal basis and get entangled in polarization. (Note that the spatial information is partly correlated with frequency via the phase-matching condition, and that indistinguishability could also be achieved via frequency filtering.) The resulting state is the Bell-state,

$$|\Phi^\varphi\rangle = \frac{1}{\sqrt{2}} \left(|\mathrm{V}\rangle_\mathrm{s} |\mathrm{V}\rangle_\mathrm{i} + e^{i\varphi} |\mathrm{H}\rangle_\mathrm{s} |\mathrm{H}\rangle_\mathrm{i} \right), \qquad (1)$$

with a relative phase φ that we can control. As in most cases, it is required that the probability of creating more than a single pair within a time determined by the coherence time of the photons, or the detector gate-time, whichever is longer, is negligible, and for moderate pump-powers and relatively short gate-times or wide bandwidths, this probability is very small, but not vanishing. Assuming a Poissonian distribution, the probability becomes $P_{n\geq 2} = 1 - (1+m)e^{-m}$, where $m = \Delta t_\mathrm{g} \beta P_\mathrm{p} \lambda_\mathrm{p} / hc$ is the mean photon number in a single random gating. For a typical detector gate-time $\Delta t_\mathrm{g} = 5$ ns, pump-power $P_\mathrm{p} = 540$ μW, and conversion efficiency $\beta = 3 \times 10^{-10}$ we get $m = 2 \times 10^{-3}$ and $P_{n\geq 2} = 2 \times 10^{-6}$.

Fig. 2 will serve as an illustration of the problem of optimizing the focus of the pump-mode, and the fiber-matched modes with respect to *two* crystals. As a compromise, the pump-beam is focused at the interface between the crystals, in the anticipation that the profile of the generated emission exactly trails the profile of the pump-beam. However, numerical simulations with the software developed in [15] show that the waist of the emission will be shifted towards the center of each crystal, so that neither the vertically nor the horizontally polarized photons will couple perfectly into the fiber simulta-

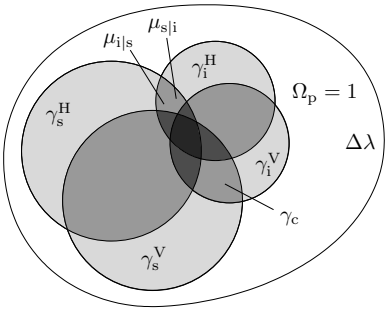

FIG. 2: The figure shows a Venn diagram, which is used to illustrate the single coupling efficiencies γ_{s} and γ_{i}, pair coupling γ_{c}, and conditional coincidences $\mu_{\mathrm{s|i}}$ and $\mu_{\mathrm{i|s}}$ as a fractional number representing the area of a set. The elements contained in a specific set represent photon pairs that are coupled into a fiber taken from the universal set of pairs, Ω_{p}, which contains all pairs generated from the crystals (V or H) within the bandwidth of the detector filter $\Delta\lambda$. The set Ω_{p} is normalized to unity and represents perfect coupling. Maximum overlap of all sets is needed to generate the best entanglement in the fiber, which is represented by the darkest shaded area in the diagram (the union of all sets).

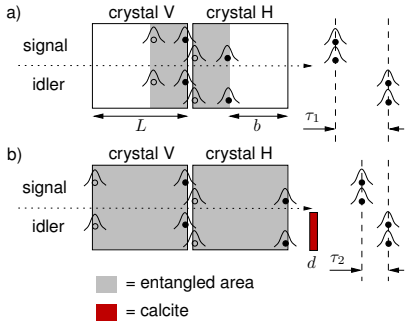

FIG. 3: Color online. The figure illustrates the effects of chromatic dispersion resulting from the strong non-degeneracy of the signal and idler photons, with group refractive indices $n_{\mathrm{g,s}}$ and $n_{\mathrm{g,i}}$. a) A pair created at the end-facet of the V-crystal (black dots) will non-interactively pass through the H-crystal, after which the signal and idler wavepackets become separated by a time $\tau_1 = (n^X_{\mathrm{g,s}} - n^X_{\mathrm{g,i}})L/c$ before hitting the detectors. As seen from the detectors' viewpoint, for the same pair to instead have been created in the H-crystal (black dots), its wavepackets would necessarily need to have separated by the same amount, given by $\tau_1' = (n^Z_{\mathrm{g,s}} - n^Z_{\mathrm{g,i}})b/c$, in order to interfere with (i.e. overlap with, or be indistinguishable from) the first case. (The superscripts refers to different polarization-axes.) Any pair created within the gray area (between black and white dots), are separated by a time $\tau \geq \tau_1 = \tau_1'$, and will always find a corresponding position in the orthogonal crystal to interfere with, according to the detectors; however, all the pairs from the white area of either crystal will be *distinguishable* in time from any pair of the other crystal, i.e. the wavepackets are non-overlapping due to different dispersions, and contribute therefore to a mixed output state. b) If we put a birefringent plate of thickness d in one of the arms, the time-separation for a pair created at the end-facet of the V-crystal is reduced to $\tau_2 = (n^X_{\mathrm{g,s}} - n^X_{\mathrm{g,i}})L/c + (1 - n^e_{\mathrm{g,c}})d/c < \tau_1$, for which some d equals the time-separation of an interfering position at the *end-facet* of the H-crystal, $\tau_2 = -(1 - n^o_{\mathrm{g,c}})d/c$. Consequently, all H and V-pairs now show "self-interference", and a pure output state is created. Note that two pairs created within the coherence time of the pump (which needs to be longer than L) are always coherent, ignoring dispersion.

neously. The figure shows the different types of coupling efficiencies represented as sets in a Venn-diagram, where each element of a set represents a photon pair generated by the crystals in some spatial mode. That is, the collection of all elements within each set defines which pairs are coupled into the fiber for some specific focusing condition, in such a way that the coupling efficiency corresponds to the total area of the set. The problem can be described in two parts: first, the need to overlap the matching modes of the signal and idler, represented by the coupling efficiencies γ_{s} and γ_{i}, for each polarization separately (i.e. by optimizing the pair coupling $\gamma_{\mathrm{c}} = \mu_{\mathrm{i|s}}\gamma_{\mathrm{s}}$, via the conditional coincidence $\mu_{\mathrm{i|s}}$), and second, the need to overlap the vertically, γ^{V}, and the horizontally, γ^{H}, polarized photons for both the signal and idler. It is only in the intersection of all sets where entanglement exits, and any detection of photons outside of this set will limit the visibility in the $\pm 45°$-basis (denoted here D/A-basis) by contributing to a mixed state. This picture is valid for many types of sources, and we believe that the coupling efficiencies in many cases in the literature are estimated in an incorrect way, as it is important to note that $\gamma_{\mathrm{c}} \neq \gamma_{\mathrm{s}}\gamma_{\mathrm{i}}$ (especially in non-degenerate regimes). By this short discussion (see [25] for a comprehensive discussion), we hope to have illustrated that it is not necessarily best to optimize each arm individually to find the greatest coincidences, but rather, to simultaneously optimize both arms.

As we have mentioned, the different polarizations need to interfere, and therefore a major concern is that they are not distinguishable by time information, noting the limited extent of the photon wave-packets. For long crystals, the photon pairs will separate by chromatic dispersion, due to the very different group velocities between the strongly non-degenerate signal and idler. This will occur to a degree that is different for pairs created in the first crystal than for pairs created in the second, because the pairs from the first crystal also need to pass through the second. The differences in group velocities between signal and idler are not the same for light polarized along the Z-axis and the X-axis, implying that not all pairs, created along the length of either crystal, will find any (possibly) generated pairs to interfere with from

the other crystal. Some photon-pairs will therefore be distinguishable by temporal information. See Fig. 3 for an illustration. We would like to point out that, while this chromatic two-photon dispersion effect is reminiscent of the "two-photon dispersion" effects discussed in [1] or [26], it does not have the same origin, although the current effect can also be compensated for by an extra piece of crystal. The chromatic effect comes as an disadvantage when placing the crystals adjacent to each other, and could in principle be avoided by an "interferometric" solution [6, 12], in which the pump beam splits into two separate arms, impinges onto each of the crystals, or onto a single crystal but in opposite directions, and recombines on a beam-splitter. Still, we believe the current solution requires fewer optics, is easier to align, and can be made more compact.

The previous discussion gave a limited, although intuitive, understanding of the origin of a mixed state, but, as we will show in the next section, a mathematical derivation will give additional insights into how the effect of decoherence is affected by the group velocities.

III. THE TWO-CRYSTAL TWO-PHOTON QUANTUM STATE

In this section, we derive the output state from the two-crystal source in terms of the frequency and polarization degrees of freedom $|\boldsymbol{\epsilon}\rangle\otimes|\boldsymbol{\chi}_{i,j}\rangle$, where $i,j=\{1=\text{"V"},2=\text{"H"}\}$ denotes the polarizations. Emission from each of the crystals, V and H, will thus be represented by $|\boldsymbol{\chi}_{11}\rangle$ and $|\boldsymbol{\chi}_{22}\rangle$, respectively, according to Eq. (A.15) of the Appendix and Fig. 1. As just described, the vertical light will be subject to dispersion upon its passing through the second crystal. We will formulate this mathematically by introducing a unitary transform acting on the states. The eigenequation which describes the transformation U_L on the state of the first crystal, when it passes through the second crystal, is

$$\begin{aligned} U_L|\boldsymbol{\chi}_{11}\rangle &= e^{i(k_{\rm s}L+k_{\rm i}L)}|\boldsymbol{\chi}_{11}\rangle \\ &= e^{i(n_{\rm s}^X\omega_{0\rm s}+n_{\rm i}^X\omega_{0\rm i}+(n_{\rm g,s}^X-n_{\rm g,i}^X)\epsilon)L/c}|\boldsymbol{\chi}_{11}\rangle, \end{aligned} \tag{2}$$

where the length of the crystal, L, enters the phase term, together with the frequency ϵ. With reference to the Appendix, and Eq. (A.15), we can then express the output state of each crystal as

$$\begin{aligned} |\Psi_{11}\rangle &= \frac{1}{B}\int \mathrm{d}\epsilon\, U_L U(\epsilon)\,|\boldsymbol{\epsilon}\rangle\otimes|\boldsymbol{\chi}_{11}\rangle, \\ |\Psi_{22}\rangle &= \frac{1}{B}\int \mathrm{d}\epsilon\, U(\epsilon)\, e^{in_{\rm p}^X\omega_{\rm p}L/c}\,|\boldsymbol{\epsilon}\rangle\otimes|\boldsymbol{\chi}_{22}\rangle, \end{aligned} \tag{3}$$

where an extra phase-term has been added to the pump field in the second crystal due to the pump field passing through the first crystal, $U(\epsilon)$ is the state amplitude, and B is a normalization constant. The sum of these two kets will give us the combined two-crystal two-photon state,

$$\begin{aligned} |\Psi^\epsilon\rangle &= |\Psi_{11}\rangle + |\Psi_{22}\rangle \\ &= \frac{1}{B}\int \mathrm{d}\epsilon\,\Big[U_L U(\epsilon)|\boldsymbol{\epsilon}\rangle\otimes|\boldsymbol{\chi}_{11}\rangle \\ &\qquad + U(\epsilon)e^{in_{\rm p}^X\omega_{\rm p}L/c}|\boldsymbol{\epsilon}\rangle\otimes|\boldsymbol{\chi}_{22}\rangle\Big] \\ &= \frac{1}{B}\int \mathrm{d}\epsilon\sum_{i,j=1}^{2} c_{ij}V_{ij}(\epsilon)\,|\boldsymbol{\epsilon}\rangle\otimes|\boldsymbol{\chi}_{ij}\rangle, \end{aligned} \tag{4}$$

where we have introduced $V_{11}(\epsilon)=\frac{1}{B}U_L U(\epsilon)$, $V_{22}(\epsilon)=\frac{1}{B}U(\epsilon)e^{in_{\rm p}^X\omega_{\rm p}L/c}$, and the coefficients $c_{ij}=1/\sqrt{2}$ for $i=j$, and $c_{ij}=0$ for $i\neq j$, normalized such that $|c_{11}|^2+|c_{22}|^2=1$.

We can now form the two-photon density matrix

$$\begin{aligned} \boldsymbol{\rho}^\epsilon &= |\Psi^\epsilon\rangle\langle\Psi^{\tilde\epsilon}| \\ &= \frac{1}{B^2}\iint \mathrm{d}\epsilon\,\mathrm{d}\tilde\epsilon\sum_{i,j,k,l=1}^{2} c_{ij}c_{kl}^*V_{ij}(\epsilon)V_{kl}^*(\tilde\epsilon)\,|\boldsymbol{\epsilon}\rangle\langle\tilde{\boldsymbol{\epsilon}}|\otimes|\boldsymbol{\chi}_{ij}\rangle\langle\boldsymbol{\chi}_{kl}|, \end{aligned} \tag{5}$$

from which we would like to remove the frequency information. For that, we need to note that we could, in principle, measure the frequency of the photons at a resolution much smaller than the bandwidths of the filters. The resolution is given by a wavelength bandwidth $\Delta\lambda_{\rm res}$, which is set by the timing-jitter $\Delta t_{\rm jitter}$ of the detectors. For the light passing the filters to remain transform-limited upon detection the detectors necessarily need a timing-jitter much smaller than the coherence time. However, filter bandwidths used in practice are relatively large > 0.1 nm, in wavelengths, which makes the timing-jitter ($\Delta t_{\rm jitter}\approx 350$ ps) orders of magnitudes larger than the corresponding true coherence time. This effectively means that the detector itself sets a minimum resolution for the wavelength, $\Delta\lambda_{\rm res}=\lambda^2/c\Delta t_{\rm jitter}<23$ pm, such that the coherence time of the photons detected in coincidence are practically longer, set by the timing-jitter. In other words, as the detector in principle can determine the photon's frequency components in a fine resolution, it means that the frequency components should all be added incoherently within the filter bandwidth. Therefore, it is appropriate to take the partial trace over the frequency mode:

$$\begin{aligned} \boldsymbol{\rho} &= \mathrm{Tr}_\epsilon[\,|\boldsymbol{\epsilon}'\rangle\langle\boldsymbol{\epsilon}'|\,\boldsymbol{\rho}^\epsilon] = \int_{-\infty}^{\infty}\mathrm{d}\boldsymbol{\epsilon}'\langle\boldsymbol{\epsilon}'|\boldsymbol{\rho}^\epsilon|\boldsymbol{\epsilon}'\rangle \\ &= \frac{1}{B^2}\sum_{i,j,k,l=1}^{2} c_{ij}c_{kl}^*\int \mathrm{d}\epsilon' V_{ij}(\epsilon')V_{kl}^*(\epsilon')\,|\boldsymbol{\chi}_{ij}\rangle\langle\boldsymbol{\chi}_{kl}|. \end{aligned} \tag{6}$$

Let ρ_{ijkl} denote the elements of the density matrix, of

which the only non-zero ones become

$$\begin{aligned}\rho_{1122} &= c_{11}c_{22}^{*}\frac{1}{B^2}\int \mathrm{d}\epsilon' U_L U(\epsilon')\, U^{*}(\epsilon') e^{-in_{\mathrm{p}}^{X}\omega_{\mathrm{p}}L/c} \\ &= \frac{1}{2}\frac{\chi_2^2 f_1^2 E_0^2 L^2}{\hbar^2 B^2} \\ &\quad\times \int \mathrm{d}\epsilon' \,|A_{\mathrm{s}}(\epsilon')|^2 |A_{\mathrm{i}}(\epsilon')|^2 \\ &\quad\times e^{-in_{\mathrm{p}}^{X}\omega_{\mathrm{p}}L/c}\, e^{i(n_{\mathrm{s}}^{X}\omega_{0\mathrm{s}} + n_{\mathrm{i}}^{X}\omega_{0\mathrm{i}} + (n_{\mathrm{g,s}}^{X} - n_{\mathrm{g,i}}^{X})\epsilon')L/c} \\ &\quad\times \mathrm{sinc}^2\left[\frac{L\epsilon'}{2c}(n_{\mathrm{g,s}}^{Z} - n_{\mathrm{g,i}}^{Z})\right] \\ &= \rho_{2211}^{*} \end{aligned} \tag{7}$$

and

$$\rho_{1111} = \rho_{2222} = \frac{1}{2}. \tag{8}$$

The off-diagonal element, which describes the degree of coherence in the entangled state, can be further simplified and identified as a Fourier transform:

$$\begin{aligned}\rho_{1122} &= \frac{1}{2}\, e^{-in_{\mathrm{p}}^{X}\omega_{\mathrm{p}}L/c}\, e^{i(n_{\mathrm{s}}^{X}\omega_{0\mathrm{s}} + n_{\mathrm{i}}^{X}\omega_{0\mathrm{i}})L/c} \\ &\quad\times \int \mathrm{d}\epsilon'\, g(\epsilon')\, e^{i\tau_X \epsilon'}\, \mathrm{sinc}^2(\frac{\tau_Z}{2}\epsilon'), \end{aligned} \tag{9}$$

where

$$\begin{aligned} g(\epsilon') &= \frac{\chi_2^2 f_1^2 E_0^2 L^2}{\hbar^2 B^2}|A_{\mathrm{s}}(\epsilon')|^2 |A_{\mathrm{i}}(\epsilon')|^2, \\ \tau_X &= (n_{\mathrm{g,s}}^{X} - n_{\mathrm{g,i}}^{X})L/c, \\ \tau_Z &= (n_{\mathrm{g,s}}^{Z} - n_{\mathrm{g,i}}^{Z})L/c. \end{aligned} \tag{10}$$

In Fig. 4, we have plotted the result of Eq. (9) versus the length of the crystals using different crystal materials to generate 810 and 1550 nm. We observe that the dispersion in long, periodically poled $LiNbO_3$ (PPLN) crystal materials completely suppresses the ρ_{1122} term, and thereby the entanglement. For PPKTP this is not the case, and if we search for ρ_{1122} in the limit of an infinitely long crystal we find that

$$\lim_{L\to\infty} |\rho_{1122}| = \begin{cases} 1 - \frac{\tau_X}{\tau_Z} & \text{if} \quad \tau_X < \tau_Z \\ 0 & \text{if} \quad \tau_X \geq \tau_Z, \end{cases} \tag{11}$$

which, for PPKTP leads to $\rho_{1122} = 0.203$, implying still a visibility of entanglement (i.e. of the second-order interference fringes) of 40.6%. The different results stem from the material-specific relation between τ_X and τ_Z. If the material is more strongly dispersive for polarizations along the Z-axis than the X-axis, then the off-diagonal term will be bounded below by a non-vanishing value; otherwise, the off-diagonal term will approach zero. As expected, we found that all numbers increase as we go closer to having degenerate wavelength pairs. We also note that the bandwidth of the frequency filter affects the shape of the curve; a narrower bandwidth increases the extent of the temporal coherence and provides a greater overlap between wave-packets, leading to an arbitrarily increased ρ_{1122}. Emission that is optimally coupled into single-mode fibers will automatically be filtered also in frequency, since the frequency is correlated to spatial information via the phase-matching conditions [15], and for long PPKTP crystals, in such a case, the minimum value of ρ_{1122} equals 0.266 ($V = 53.2\%$).

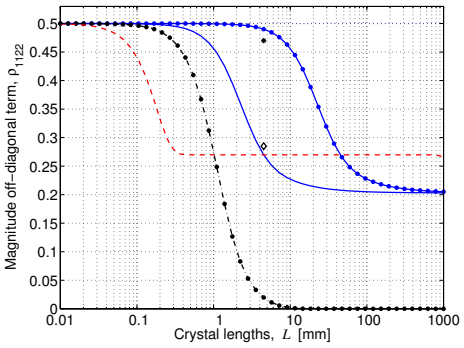

FIG. 4: Color online. The off-diagonal term, Eq. (9), of the generated density matrix plotted versus crystal length, which corresponds to the visibility of entanglement via the relation $V = 2\rho_{1122}$. Solid line: PPKTP-crystal with 10 nm idler filter. Dots over solid line: PPKTP with 1 nm idler filter. Dash-dotted line: PPLN or PPMgOLN with 10 nm idler filter. Dashed line: PPKTP at optimal fiber coupling using the idler fiber's own filtering. Diamond: experimental value for $L = 4.5$ mm using PPKTP and with a 10 nm idler filter. Solid point: experimental value for $L = 4.5$ mm using PPKTP and with a dispersion canceling calcite plate of thickness $d = 0.86$ mm.

IV. DECOHERENCE CANCELLATION

We will now briefly show how the pure state, $|\Phi^{\varphi}\rangle$ in Eq. (1), can be fully regained, for generation in long crystals, by inserting a highly birefringent crystal plate into one of the arms. The eigenequations for each polarization state propagating through such a crystal plate become

$$\begin{aligned} U_C|\boldsymbol{\chi}_{1j}\rangle &= e^{ik_{\mathrm{c}}d}|\boldsymbol{\chi}_{1j}\rangle \\ &= e^{i(n_{\mathrm{c}}^{o}\omega_{0\mathrm{i}} - n_{\mathrm{g,c}}^{o}\epsilon)d/c}|\boldsymbol{\chi}_{1j}\rangle, \\ U_C|\boldsymbol{\chi}_{2j}\rangle &= e^{ik_{\mathrm{c}}d}|\boldsymbol{\chi}_{2j}\rangle \\ &= e^{i(n_{\mathrm{c}}^{e}\omega_{0\mathrm{i}} - n_{\mathrm{g,c}}^{e}\epsilon)d/c}|\boldsymbol{\chi}_{2j}\rangle, \end{aligned} \tag{12}$$

with the density matrix after the plate becoming

$$\boldsymbol{\rho}^{\epsilon}(d) = U_C \boldsymbol{\rho}^{\epsilon} U_C^{\dagger}. \tag{13}$$

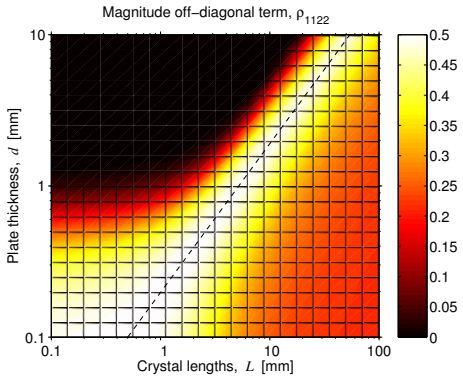

FIG. 5: Color online. The off-diagonal term, Eq. (14), plotted versus the crystal lengths, L, and the thickness, d, of a dispersion-canceling calcite plate, using PPKTP with a 10 nm idler filter. The dashed line represents perfect cancellation.

Repeating Eqns. (5) to (9), we arrive at

$$\rho_{1122} = \frac{1}{2}\, e^{-in_{\rm p}^X \omega_{\rm p} L/c}\, e^{i(n_{\rm s}^X \omega_{0\rm s} + n_{\rm i}^X \omega_{0\rm i})L/c} \times e^{i(n_{\rm c}^o \omega_{0\rm i} - n_{\rm c}^e \omega_{0\rm i})d/c} \times \int \mathrm{d}\epsilon'\, g(\epsilon')\, e^{i(\tau_X - \kappa)\epsilon'}\, \mathrm{sinc}^2(\frac{\tau_Z}{2}\epsilon'), \qquad (14)$$

where $g(\epsilon'), \tau_X$, and τ_Z is defined by Eq. (10), and where

$$\kappa = (n_{\rm g,c}^o - n_{\rm g,c}^e)d/c. \qquad (15)$$

Now, if d is chosen such that $\kappa = \tau_X$, it means that we have perfectly canceled the decoherence and retrieved a pure state. Hence,

$$\rho_{1122} = \rho_{2211}^* = \rho_{1111} = \rho_{2222} = \frac{1}{2}. \qquad (16)$$

Note that, by adjusting d and tilting the plate (affecting φ) our source can prepare any arbitrary mixed state of the kind $\boldsymbol{\rho} = V|\boldsymbol{\Phi}^\varphi\rangle\langle\boldsymbol{\Phi}^\varphi| + (1-V)\boldsymbol{\rho}_m$, where $\boldsymbol{\rho}_m = \frac{1}{2}(|\boldsymbol{\chi}_{11}\rangle\langle\boldsymbol{\chi}_{11}| + |\boldsymbol{\chi}_{22}\rangle\langle\boldsymbol{\chi}_{22}|)$, and V is the visibility. Fig. 5 shows a plot of ρ_{1122} versus L and d.

V. EXPERIMENTAL RESULTS

The experimental setup used when characterizing the source's output state is shown in Fig. 6. As a pump, we use a frequency-doubled Nd:YAG laser emitting approximately 60 mW in the TEM_{00} mode at 532 nm, which can be variably attenuated. Its M^2 factor was measured to be 1.06. This factor is commonly used to quantify the quality of laser beams, and can be determined by measuring the longitudinal profile of the beam [27]. A value of unity states that the beam is in the fundamental Gaussian single-mode. For all other modes $M^2 > 1$.

After a band-pass filter (BP532) that removes any remaining infrared light, we "clean up" the polarization using a polarizing beam-splitter (PBS). The polarization is controlled by a half-wave plate (HWP) and a quarter-wave plate (QWP) in front of the crystal. The pump beam is focused onto the crystal using an achromatic doublet lens ($f_{\rm p} = 50$ mm), which introduces a minimal amount of aberrations, so as not to destroy the low M^2–value. The QWP is set to undo any polarization ellipticisation effects caused by the lens, and fluorescence caused by the same lens is removed by a Schott-KG5 filter (SP).

The next components are the two PPKTP crystals, which are heated in an oven to a temperature $T \approx 100$ °C. After the crystals, we block the pump light with a 532 nm band-stop filter, and the signal and idler emission is focused by achromatic doublet lenses. To separate the 810 nm and 1550 nm emission, we use a dichroic mirror made for a 45° angle of incidence. The first lens ($f_{\rm si} = 30$ mm) is common to both signal and idler, and its task is to refocus the beams somewhere near the dichroic mirror. The next two lenses ($f_{\rm s} = 60$ mm and $f_{\rm i} = 40$ mm) collimate each beam, which are then focused into the fiber tips (with the mode field diameters being $\mathrm{MFD}_{810} = 5.5$ μm and $\mathrm{MFD}_{1550} = 10.4$ μm) using aspherical lenses with $f = 11$ mm. Next, we use quarter-wave plates (QWP), half-wave plates (HWP), and polarizing beam-splitters (PBS) in each arm to analyze the state. In the idler arm, we also place the tiltable cancellation plate, which is made of calcite. In front of the fiber couplers, we have first Schott-RG715/RG1000 filters to block any remaining pump light, and then interference filters (BP) of 2 nm and 10 nm bandwidth at the 810 nm and 1550 nm side respectively. The detectors used are a Si-based APD (PerkinElmer SPCM-AQR-14) for 810 nm with a quantum efficiency $\eta_{\rm s} = 60\%$ and a home-made InGaAs-APD (Epitaxx) module for 1550 nm with $\eta_{\rm i} = 18\%$, gated with 5 ns pulses. To avoid afterpulsing effects, the InGaAs-APD is used together with a hold-off circuit (10 μs) for all of the measurements. The pulses were generated using a digital delay generator (DG535)

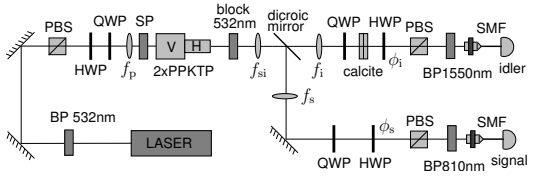

FIG. 6: Experimental setup used to measure the density matrix. PBS: polarizing beam-splitter, HWP: half-wave plate, QWP: quarter-wave plate, SP: short-pass filter, BP: band-pass filter, SMF: single-mode fiber.

TABLE I: Three runs at different alignments and pump powers, showing the coupling efficiencies, photon rates in fibers, conversion efficiency, and the production rate of the system.

P_p [mW]	γ_s	γ_i	γ_c	$\mu_{\mathrm{i}\vert\mathrm{s}}$	σ	R_s [s^{-1}]	R_i [s^{-1}]	R_p [s^{-1}]	R_c [s^{-1}]	β	$R_\mathrm{c}^\mathrm{prod}$ [$\mathrm{s}^{-1}\mathrm{THz}^{-1}\mathrm{mW}^{-1}$]
60	0.32	0.79	0.11	0.12	0.34	2.32×10^6	2.39×10^6	8.61×10^6	274×10^3	5×10^{-11}	5.0×10^3
4.5	0.32	0.56	0.10	0.11	0.32	167×10^3	121×10^3	617×10^3	19×10^3	5×10^{-11}	4.6×10^3
0.54	0.46	0.38	0.22	0.27	0.57	100×10^3	195×10^3	450×10^3	27×10^3	3×10^{-10}	55×10^3

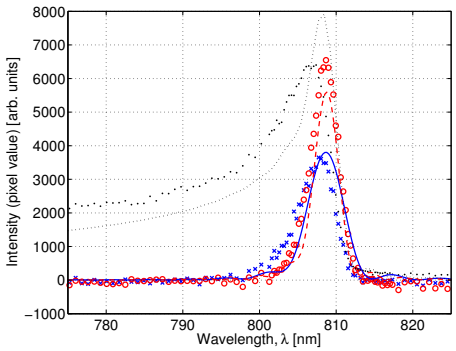

FIG. 7: Color online. Spectrogram of signal emission inside single-mode fibers without interference filters. The crosses ($\Delta\lambda_\mathrm{s}$ = 6 nm) and circles ($\Delta\lambda_\mathrm{s}$ = 4 nm) represent experimental data for the H and the V crystal, respectively, to be compared to theoretical predictions for a 2 nm (solid line) and a 3 nm (dashed line) long crystal. Also shown is the downconversion spectrum in free space, experimentally (dots) and in theory (dotted line), demonstrating the fiber's own filtering.

from SRS, with a maximal repetition rate of 1 MHz, and a trigger dead time of 1 μs.

We have used a spectrograph (SpectraPro 500i, ARC) to measure the bandwidth of the signal emission using a single-mode fiber without any filter; see Fig. 7. The bandwidth was found to be 4 nm for the V-crystal and 6 nm for the H-crystal. The results in [15] suggests that the effective lengths of the crystals being poled must then be 3 mm and 2 mm, respectively, but also that the 2 mm crystal should give $\approx$ 55% of the photon-rate of the 3 mm one. Experimental agreement is good, as we saw the H-crystal giving half the rate of the V-crystal. When measuring, we refocused the fiber coupling for each crystal to find maximum counts, while keeping the pump polarization exactly at 45°. As described in connection to Fig. 2, the best tradeoff when collecting from both crystals simultaneously is to set the focus of the pump mode and the fiber-matched modes at the intersecting faces. Experimentally, however, in order to produce as pure a Bell-state as possible, we needed to balance the rate of each crystal, which we did by shifting the fiber-matched focus a bit closer to the H-crystal and by turning the pump-polarization slightly towards H. (The focus point was moved by turning the focusing knob on the fiber coupler.) In this way we allowed lower coupling efficiencies than the maximum attainable. Recalling the definition of the focusing parameter ξ from Section II and [15], the focusing conditions achieved with available lenses were: $\xi_\mathrm{p} = 2.1$ for the pump mode, $\xi_\mathrm{s} = 3.2$ for the signal's fiber-matched mode, and $\xi_\mathrm{i} = 2.5$ for the idler's.

With this configuration, we obtained the results showed in Table I. In each column of the table, γ_s represents the signal's single coupling efficiency, γ_i the idler's, γ_c the pair coupling efficiency, $\mu_{\mathrm{i}\vert\mathrm{s}}$ the conditional coincidence, and σ the correlation efficiency, which corresponds directly to $\mu_{\mathrm{i}\vert\mathrm{s}}$ but includes a compensation for the transmission of the 1550 nm filter, $\delta_\mathrm{i} = 0.35$, and the transmission of the 810 nm filter, $\delta_\mathrm{s} = 0.85$. The singles photon-rate in the signal fiber, R_s, and the idler R_i, were both derived from detected raw counts, taking into account the detection efficiencies. The total generated rate R_p of pairs before fiber coupling was estimated from detected counts using a multimode fiber. The pair rate in the fibers, R_c, was deduced from the above efficiencies and the detected raw coincidence rate, with accidental counts subtracted by assuming that R_i originates from a Poissonian distribution at random gating [25]. The following relations between the coupling efficiencies and the rates were used: $R_\mathrm{i} = \delta_\mathrm{i}\gamma_\mathrm{i}R_\mathrm{p}$, $R_\mathrm{s} = \delta_\mathrm{s}\gamma_\mathrm{s}R_\mathrm{p}$, and $R_\mathrm{c} = \delta_\mathrm{i}\delta_\mathrm{s}\gamma_\mathrm{c}R_\mathrm{p}$.

The conversion efficiency β is the fraction of pump photons converted into signal and idler pairs, leading to a pair production rate $R_\mathrm{c}^\mathrm{prod}$, which equals 5×10^3 $\mathrm{s}^{-1}\mathrm{THz}^{-1}\mathrm{mW}^{-1}$ at the pump power $P_\mathrm{p} = 60$ mW and with the idler detector gated at 585 kHz. (The production rate is the pair rate normalized to the wavelength bandwidth in THz and the pump power in mW.) The second row of Table I shows similar results for a lower pump power and an idler gate rate of 91 kHz. We also took measurements without any interference filter at the idler side (but still with a 2 nm filter at the signal), with the results shown in the third row of Table I, for $P_\mathrm{p} = 540$ μW and with a gate-rate of 57 kHz. The results are improved, not because of the lower power, but because of a simultaneous optimization of the arms in order to maximize γ_c. The table shows how γ_i decreases in the process. The correlation efficiency σ now includes the estimated transmission-loss of the optics at the idler side, and a correction factor for the unequal filtering between signal and idler (the idler fiber itself provides a frequency filtering of $\Delta\lambda_\mathrm{i} = 14.7$ nm). The best conditional coincidence is $\mu_{\mathrm{i}\vert\mathrm{s}} = 0.27$, and the conversion efficiency, $\beta = 3\times10^{-10}$, was possibly improved by aligning to a more homoge-

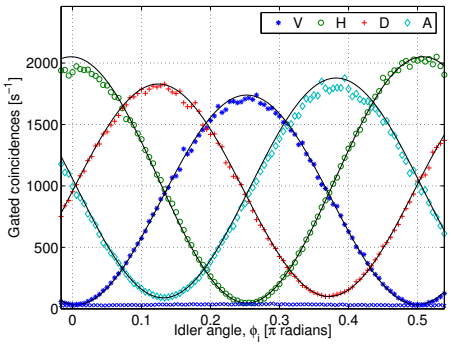

FIG. 8: Color online. The plot shows the raw visibility curves obtained at a pump power $P_{\rm p} = 4.5$ mW, gate-rate 91 kHz, without subtraction of background counts (including accidentals) shown at the bottom. Each curve correspond to a different polarization setting of the signal arm, $\phi_{\rm s}^{\rm V} = -3\pi/16$, $\phi_{\rm s}^{\rm H} = \pi/16$, $\phi_{\rm s}^{\rm D} = -\pi/16$, and $\phi_{\rm s}^{\rm A} = 3\pi/16$, as indicated the inset. Fitting of the collected data gives $V_{\rm H} = 99.6 \pm 0.2\%$, $V_{\rm V} = 99.2 \pm 0.2\%$, $V_{\rm D} = 92.7 \pm 0.2\%$, and $V_{\rm A} = 94.2 \pm 0.2\%$. When background counts were not subtracted, we obtained the visibilities $V_{\rm H} = 95.6 \pm 0.2\%$, $V_{\rm V} = 96.2 \pm 0.2\%$, $V_{\rm D} = 89.6 \pm 0.2\%$, and $V_{\rm A} = 90.9 \pm 0.2\%$.

neously poled area of the crystals. We believe that the pair production rate, 55×10^3 s^{-1}THz^{-1}mW^{-1}, is one of the highest yet reported for polarization entangled photon pairs generated in crystals and launched into single-mode fibers. Frequency filtering at a narrow bandwidth of 50 GHz would imply 3×10^3 s^{-1}mW^{-1} of pairs in the fibers. Besides, for narrow filtering, the photon flux has been shown [15] to be $\propto L\sqrt{L}$, and so, by using longer crystals ($L = 50$ mm) we could still reach 20 s^{-1}mW^{-1} at a 10 MHz bandwidth, which is the bandwidth regime of e.g. Rb-atom based quantum memories. As a comparison, we have derived numbers using data available for some other experiments, among which the best include Fiorentino *et al.* [12], who seem to have 22×10^3 s^{-1}THz^{-1}mW^{-1} of pairs being generated by two 10 mm long crystals into free-space; König *et al.* [20], who claim to have 300×10^3 s^{-1}THz^{-1}mW^{-1} pairs from two 20 mm long crystals into fibers; and Li *et al.* [9], who seem to have an exceptional value of 4.3×10^6 s^{-1}THz^{-1}mW^{-1} pairs generated directly inside a non-linear fiber.

Fig. 8 shows the visibility curves obtained, with and without subtraction of background counts, including false coincidences. Note that the number of "accidental" coincidences increases with the pump power, as the probability of more than a single pair to arrive within the gate-time of the detector increases, as shown in section II.

We have also measured a violation of the CHSH-inequality [28] by taking measurements of the coincidence-rate functions

$$R_{i,j} = \frac{1}{2}[1 + ijV_{i,j}\cos(4\phi_{\rm s} + 4\phi_{\rm i})], \tag{17}$$

where $i, j = \pm 1$ denotes the four combinations of measurable output-arms of the two PBS:s in the signal and idler, $V_{i,j}$ is the corresponding visibility, and $\phi_{\rm s}$, $\phi_{\rm i}$, are the angles of the HWPs. The correlation function becomes

$$\begin{aligned} E(\phi_{\rm s}, \phi_{\rm i}) &= \frac{R_{1,1} - R_{1,-1} - R_{-1,1} + R_{-1,-1}}{R_{1,1} + R_{1,-1} + R_{-1,1} + R_{-1,-1}} \\ &= V\cos(4\phi_{\rm s} + 4\phi_{\rm i}), \end{aligned} \tag{18}$$

where $V = V_{1,1}$, assuming fully equal rate functions, so that we can rely on measurements taken at only one of the output arms. Entanglement is present iff the CHSH-inequality is violated,

$$S = E(\phi_{\rm s}^1, \phi_{\rm i}^1) + E(\phi_{\rm s}^1, \phi_{\rm i}^2) + |E(\phi_{\rm s}^2, \phi_{\rm i}^1) - E(\phi_{\rm s}^2, \phi_{\rm i}^2)| \leq 2, \tag{19}$$

where the correlation function is to be measured at the following pair of angles: $\phi_{\rm s}^1 = -\pi/16, \phi_{\rm i}^1 = 0$ and $\phi_{\rm s}^2 = \pi/16, \phi_{\rm i}^2 = \pi/8$. The parameter S can reach the maximum value of $2\sqrt{2}$, corresponding to 100% visibility, and it is well known that the average visibility needs to be $> 71\%$ to violate the inequality, if the state is subject to equal decoherence in all bases. In our case, the state decoheres in the H/V-basis, while maintaining nearly perfect visibility for the H and V settings. Let $\phi_{\rm s}^1$ represent the H/V-basis, and $\phi_{\rm s}^2$ the D/A-basis. Furthermore, let $V_{\rm H,V}$ and $V_{\rm D,A}$ represent the visibilities in each respective basis. We get

$$\begin{aligned} S &= V_{\rm H,V}\cos(-\frac{\pi}{4} + 0) + V_{\rm H,V}\cos(-\frac{\pi}{4} + \frac{\pi}{2}) + \\ &\quad \left|V_{\rm D,A}\cos(\frac{\pi}{4} + 0) - V_{\rm D,A}\cos(\frac{\pi}{4} + \frac{\pi}{2})\right| \\ &= \sqrt{2}(V_{\rm H,V} + V_{\rm D,A}), \end{aligned} \tag{20}$$

which shows that, for $V_{\rm H,V} = 100\%$, the requirement is $V_{\rm D,A} > 41\%$ for a violation of Eq. (19).

A direct measurement of S at the above angles yields $S = 2.679 \pm 0.004$ at a pump power $P_{\rm p} = 60$ mW, after subtraction of accidental counts (gate-rate was 585 kHz). The CHSH-inequality was violated by 177 standard deviations in 10 s, or $56\sigma_S$ s$^{-1/2}$. To our knowledge, this is one of the highest reported to date; only Kurtsiefer *et al.* [3] exceeds this rate, with $148\sigma_S$ s$^{-1/2}$. Other examples of good results can be found in [11] ($50\sigma_S$ s$^{-1/2}$) and in [12] ($38\sigma_S$ s$^{-1/2}$). We have re-derived these numbers using available data, in the hopes of having created directly comparable normalized numbers. The derivation was made as follows. Assuming no fluctuation of the rate other than that originating from Poissonian-distributed single-photon detections, the standard deviation of the coincidence rate $R_{i,j}$ becomes $\sigma_R = \sqrt{R_{\rm max}/2}/\sqrt{T_R}$, where $R_{\rm max}$ is the peak coincidence rate, $\sqrt{R_{\rm max}/2}$ is the

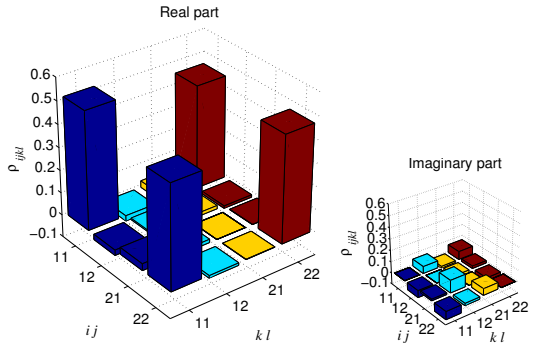

FIG. 9: Color online. Experimentally determined density matrix, $\boldsymbol{\rho}_{\rm expt}$, (real and imaginary parts) obtained by quantum state tomography on the generated polarization entangled state (1 = "V" and 2 = "H"). (Pump power, $P_{\rm p} = 60$ mW).

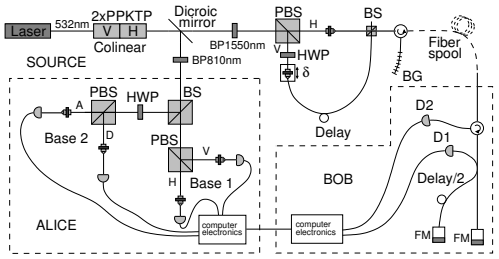

FIG. 10: Scheme to create hybrid-coded entanglement. BS: beam splitter, PBS: polarizing beam splitter, HWP: half-wave plate, BP: band-pass filter, BG: Bragg grating, FM: Faraday mirror.

standard deviation of the average photon-rate, T_R is the integration-time in seconds, and the central limit theorem is used to sum over time. According to Eq. (18), the standard deviation of the correlation function becomes $\sigma_E = \sqrt{4}\sigma_R/2R_{\rm max}$, and by Eq. (19) we have $\sigma_S = \sqrt{4}\sigma_E = 2/\sqrt{2R_{\rm max}T_R}$, such that $S = S_m \pm \sigma_S$, where S_m is the measured value over T_R seconds. Thus, the normalized "speed of CHSH violation" becomes

$$x = \frac{S_m - 2}{\sigma_S\sqrt{T_R}} = \frac{(S_m-2)\sqrt{2R_{\rm max}}}{2} \quad [{\rm s}^{-1/2}], \qquad (21)$$

which only depends on the maximum rate and the measured value of S. If the accidental counts are not subtracted from the coincidence counts, we instead measure the value $S = 2.6283 \pm 0.0102$ ($P_{\rm p} = 4.5$ mW), with the CHSH-inequality being violated by $19\sigma_S$ s$^{-1/2}$, showing that we truly have a high degree of entanglement launched into the fibers. This is important in entanglement-based quantum key distribution (QKD) systems that do not allow a subtraction of the background. Rather, any accidentals will increase the quantum bit error rate (QBER) and reduce the final bit rate, equivalently degrading the system performance.

Following Ref. [29], we have made a complete tomography of the state, with the resulting density matrix becoming

$$\boldsymbol{\rho}_{\rm expt} = \begin{bmatrix} 0.5197 & -0.0237 & 0.0300 & 0.4573 \\ -0.0237 & 0.0069 & 0.0146 & -0.0114 \\ 0.0300 & 0.0146 & 0 & 0.0010 \\ 0.4573 & -0.0114 & 0.0010 & 0.4734 \end{bmatrix} + i \begin{bmatrix} 0 & 0.0628 & -0.0150 & 0.0720 \\ -0.0628 & 0 & -0.1107 & 0.0206 \\ 0.0150 & 0.1107 & 0 & -0.0581 \\ -0.0720 & -0.0206 & 0.0581 & 0 \end{bmatrix}, \qquad (22)$$

which is also plotted in Fig. 9. Recall that the off-diagonal element, $\rho_{1122} = 0.457$, corresponds approximately to the visibility in the D/A-basis, $V \approx 2\rho_{1122} = 0.915$, which is indeed close to the measured visibilities. When applying the density matrix to Wootters's entanglement of formation measure [30], we get the value $E = 0.56$. The entanglement of formation equals unity for a pure Bell-state, as do the fidelity, $F = \langle \boldsymbol{\Phi}^{\varphi} | \boldsymbol{\rho}_{\rm expt} | \boldsymbol{\Phi}^{\varphi} \rangle$, which is found to be 0.95 for the generated state.

VI. FUTURE DIRECTIONS: A HYBRID-CODED ENTANGLEMENT SOURCE

In order to motivate the usefulness of the source, we provide in Fig. 10 a complete setup for quantum communication (e.g. QKD). The scheme, which is under implementation, uses long crystals (2×50 mm) in order to achieve a bandwidth of < 80 GHz, which means higher production rates and less dispersion in combination with a telecom Bragg grating as dispersion compensator. For long crystals, the optimal focusing is weaker, which leads to a more compact source with fewer collimating lenses placed at closer distances to each other. Furthermore, improvement of the conditional coincidences as well as the size of the source can be achieved by minimizing the number of components, each of which contribute to loss.

In Bob's arm, the polarization information is converted into time information in order to avoid the polarization dispersion in standard telecom fibers. (For a thorough review on photonic qubits, please refer to [31].) A polarizing beam splitter sits in an unbalanced Mach-Zehnder interferometer, directing vertical photons into the long arm and horizontal into the short. The vertical photons are rotated to horizontal before the photons in both arms are recombined on a fiber-based beam-splitter and sent to a Bragg grating. The result is a time encoded qubit with all polarization information erased. (To our knowledge, there is no way to erase this information passively without having to accept 50% losses in the unused arm of the beam-splitter, which is an disadvantage,

but could also be turned to an advantage by introducing a third party Charlie.) The resulting state becomes $|\Phi'\rangle = 1/\sqrt{2}\left(|\mathrm{V}\rangle_\mathrm{s}|\mathrm{L}\rangle_\mathrm{i} + e^{i\varphi}|\mathrm{H}\rangle_\mathrm{s}|\mathrm{S}\rangle_\mathrm{i}\right)$, where L denotes the long arm and S the short arm. On Bob's analyzer side, there is an unbalanced all-fiber Michelson interferometer with a single beam-splitter to decode the qubits. The interferometer uses Faraday mirrors, which reflect the light in such a way that the polarization is exactly orthogonal when the photons arrive a second time at the beam-splitter to interfere, and thereby avoids the need for polarization controllers [32]. The phase information of the qubit defines a complementary basis to time, and for that information to remain, the path length difference between the short and the long arm needs to be exactly matched to that of the preparing interferometer, requiring both interferometers to be temperature stabilized. However, longer coherence length of the emitted photons (an effect of narrow bandwidth) will effectively relax these requirements. One advantage of the above solution is that the preparing interferometer has translatable fiber couplers inside the interferometer, which simplifies their mutual alignment. Also, we avoid the possibly difficult alignment of three interferometers, as Alice adheres to polarization coding. Another important condition for the qubits to remain coherent is that the delay between two consecutive pulses is short enough (≈ 5 ns) that they experience the same phase shift due to vibrations and temperature fluctuations when traveling over the fiber. On Alice's side, the analyzer realizes a standard polarization decoder. Note that the H/V or D/A-basis is randomly chosen by the first beam-splitter, just as at Bob's side, which implies that there is no need for any active devices. Note also that there exists the possibility to delay the outputs of each detector arm on Alice side and combine into different time-slots for detection with a single detector, instead of four, which may reduce the need for space.

VII. SUMMARY

In this article, we have presented work on a two-crystal source that uses PPKTP for the production of polarization-entangled photon-pairs in a single spatial mode, leading to efficient fiber coupling. The source is suitable for schemes that combine polarization and time coding. We have shown how distinguishability between photon-pairs is introduced for this type of colinear source, due to a special kind of chromatic two-photon dispersion. We have derived and analyzed the output state of SPDC for this case, with the goal to cancel the decoherence and regain a pure state using an extra piece of birefringent crystal. We have determined the quality of entanglement for the reported setup using various measures, including the method of quantum state tomography, and we draw the conclusion that this is one of the brightest sources available for polarization entanglement in terms of Bell-inequality violation and production rates.

Acknowledgments

The authors would like to thank A. Karlsson and G. Björk for their valuable comments and suggestions throughout the work, M. Andersson and J. Tidström for useful discussions, A. Fragemann, C. Canalias, and F. Laurell for providing us with crystals, and J. Waldebäck for his help with electronics. Financial support is gratefully acknowledged from the European Commission through the integrated project SECOQC (Contract No. IST-2003-506813), and from the Swedish Foundation for Strategic Research (SSF).

APPENDIX: THE TWO-PHOTON FREQUENCY AND POLARIZATION QUANTUM STATE

In this Appendix, we derive the quantum state of a single crystal in terms of frequency and polarization degrees of freedom, using the interaction picture of SPDC [33].

The evolution of the number state vector is given by

$$|\psi\rangle = \exp\left[\frac{1}{i\hbar}\int_T^{t_0+T} \mathrm{d}t\hat{H}(t)\right]|\psi_{00}\rangle \approx \left(\mathbb{1} + \frac{1}{i\hbar}\int_T^{t_0+T}\mathrm{d}t\hat{H}(t)\right)|\psi_{00}\rangle, \tag{A.1}$$

where $|\psi_{00}\rangle$ is the number state at time t_0 and $\hat{H}(t)$ is the interaction Hamiltonian,

$$\hat{H}(t) = \int_{-L/2}^{L/2}\mathrm{d}z\int_{-\infty}^{\infty}\mathrm{d}y\int_{-\infty}^{\infty}\mathrm{d}x\,\chi^{(2)}\hat{E}_\mathrm{p}^{(+)}\hat{E}_\mathrm{s}^{(-)}\hat{E}_\mathrm{i}^{(-)} + \mathrm{H.c.}, \tag{A.2}$$

displayed in a Cartesian coordinate system, $\boldsymbol{r} = x\boldsymbol{e}_x + y\boldsymbol{e}_y + z\boldsymbol{e}_z$. There are three interacting fields in the crystal's volume, ignoring all higher-order terms ($n \geq 3$) of the non-linearity $\chi^{(n)}$. All three fields have the same polarization (ZZZ):

$$E_\mathrm{p}^{(+)} = E_0\, e^{-i(k_{0\mathrm{p}}\boldsymbol{s}_\mathrm{p}\cdot\boldsymbol{r}-\omega_\mathrm{p}t+\phi_\mathrm{p})} \tag{A.3}$$

$$\hat{E}_\mathrm{s}^{(-)} = \int\mathrm{d}\phi_\mathrm{s}\int\mathrm{d}\omega_\mathrm{s}A_\mathrm{s}(\omega_\mathrm{s})\sum_{\boldsymbol{s}_\mathrm{s}} e^{i(k_\mathrm{s}\boldsymbol{s}_\mathrm{s}\cdot\boldsymbol{r}-\omega_\mathrm{s}t+\phi_\mathrm{s})}\hat{a}_\mathrm{s}^\dagger(\omega_\mathrm{s},\boldsymbol{s}_\mathrm{s}) \tag{A.4}$$

$$\hat{E}_\mathrm{i}^{(-)} = \int\mathrm{d}\phi_\mathrm{i}\int\mathrm{d}\omega_\mathrm{i}A_\mathrm{i}(\omega_\mathrm{i})\sum_{\boldsymbol{s}_\mathrm{i}} e^{i(k_\mathrm{i}\boldsymbol{s}_\mathrm{i}\cdot\boldsymbol{r}-\omega_\mathrm{i}t+\phi_\mathrm{i})}\hat{a}_\mathrm{i}^\dagger(\omega_\mathrm{i},\boldsymbol{s}_\mathrm{i}), \tag{A.5}$$

where the pump field is classical and monochromatic so that we can replace $\hat{E}_\mathrm{p}^{(+)}$ by $E_\mathrm{p}^{(+)}$. The plus sign denotes conjugation, i.e annihilation (+) or creation (-) of the state. We have also introduced the notation $\boldsymbol{k} = k\boldsymbol{s}$,

where $\boldsymbol{s} = p\boldsymbol{e}_x + q\boldsymbol{e}_y + m\boldsymbol{e}_z$, is the unit length vector of $\boldsymbol{k}$ with components in each of the three dimensions [34], as defined by the coordinate system in Fig. 1. The pump field is a plane wave propagating in the z-direction, $\boldsymbol{s}_\mathrm{p} = \boldsymbol{e}_z$. For signal and idler, we sum over both frequency and angular modes, where $\hat{a}(\omega, \boldsymbol{s})$ is the field operator, and $A(\omega)$ is the frequency amplitude of a Gaussian-shaped detector filter having the bandwidth $\Delta\lambda$ (FWHM) and center wavelength λ_c (all wavelengths in vacuum). Via the relation $\omega = 2\pi c n_\lambda/\lambda$, its form is given by

$$A(\omega;\lambda) = e^{-2\log(2)(\lambda-\lambda_c)^2/\Delta\lambda^2}. \tag{A.6}$$

Each signal and idler photon is created with a random phase, ϕ_s and ϕ_i, respectively, which we need to sum over. The phase of the pump, ϕ_p, is constant and arbitrary.

For periodically poled materials, the spatial variation of the nonlinear index $\chi^{(2)}$ has sharp boundaries, but we will simplify and make a sinusoidal approximation using the first term of an Fourier-series expansion of $\chi^{(2)}$:

$$\chi^{(2)} = \chi_2 \sum_{m=0}^{\infty} f_m e^{-im\boldsymbol{K}\cdot\boldsymbol{r}} \approx \chi_2\, f_1 e^{-i\boldsymbol{K}\cdot\boldsymbol{r}}, \tag{A.7}$$

where $\boldsymbol{K} = K\boldsymbol{e}_z = 2\pi/\Lambda\, \boldsymbol{e}_z$ and Λ is the grating period.

The Hamiltonian now takes the form

$$\begin{aligned}\hat{H}(t) = \chi_2\, f_1 E_0 &\int \mathrm{d}\phi_\mathrm{s} \int \mathrm{d}\phi_\mathrm{i} \int \mathrm{d}\omega_\mathrm{s} \int \mathrm{d}\omega_\mathrm{i} \\ &\times A_\mathrm{s}(\omega_\mathrm{s}) A_\mathrm{i}(\omega_\mathrm{i}) \\ &\times \sum_{\boldsymbol{s}_\mathrm{s}} \sum_{\boldsymbol{s}_\mathrm{i}} \hat{a}_\mathrm{s}^\dagger(\omega_\mathrm{s}, \boldsymbol{s}_\mathrm{s}) \hat{a}_\mathrm{i}^\dagger(\omega_\mathrm{i}, \boldsymbol{s}_\mathrm{i}) \\ &\times \int_{-L/2}^{L/2} \mathrm{d}z \int_{-\infty}^{\infty} \mathrm{d}y \int_{-\infty}^{\infty} \mathrm{d}x \\ &\times e^{-i[\Delta\boldsymbol{k}\cdot(x\boldsymbol{e}_x + y\boldsymbol{e}_y + z\boldsymbol{e}_z) - (\omega_\mathrm{s}+\omega_\mathrm{i}-\omega_\mathrm{p})t + \phi_\mathrm{s}+\phi_\mathrm{i}-\phi_\mathrm{p}]} \\ &+ \text{H.c.}, \end{aligned} \tag{A.8}$$

where the mismatch vector is

$$\begin{aligned}\Delta\boldsymbol{k} &= k_\mathrm{s}\boldsymbol{s}_\mathrm{s} + k_\mathrm{i}\boldsymbol{s}_\mathrm{i} - k_{0\mathrm{p}}\boldsymbol{s}_\mathrm{p} + \boldsymbol{K} \\ &= \Delta k_x \boldsymbol{e}_x + \Delta k_y \boldsymbol{e}_y + \Delta k_z \boldsymbol{e}_z. \end{aligned} \tag{A.9}$$

Following Eq. (A.1), we now let the Hamiltonian undergo time evolution. The mismatch vector is also divided up into its x, y, and z components using Eq. (A.9). Hence,

$$\begin{aligned}\frac{1}{i\hbar}\int \mathrm{d}t \hat{H}(t) = &\\ &\chi_2\, f_1 E_0 \int \mathrm{d}\omega_\mathrm{s} \int \mathrm{d}\omega_\mathrm{i}\, A_\mathrm{s}(\omega_\mathrm{s}) A_\mathrm{i}(\omega_\mathrm{i}) \\ &\times \sum_{\boldsymbol{s}_\mathrm{s}} \sum_{\boldsymbol{s}_\mathrm{i}} \hat{a}_\mathrm{s}^\dagger(\omega_\mathrm{s}, \boldsymbol{s}_\mathrm{s}) \hat{a}_\mathrm{i}^\dagger(\omega_\mathrm{i}, \boldsymbol{s}_\mathrm{i}) \\ &\times \int_{-L/2}^{L/2} \mathrm{d}z \int_{-\infty}^{\infty} \mathrm{d}y \int_{-\infty}^{\infty} \mathrm{d}x\, e^{-i[\Delta k_x x + \Delta k_y y + \Delta k_z z]} \\ &\times \frac{1}{i\hbar} \iint_0^{2\pi} \mathrm{d}\phi_\mathrm{s} \mathrm{d}\phi_\mathrm{i} \int_0^T \mathrm{d}t\, e^{-i[(\omega_\mathrm{s}+\omega_\mathrm{i}-\omega_\mathrm{p})t + \phi_\mathrm{s}+\phi_\mathrm{i}-\phi_\mathrm{p}]} \\ &- \text{H.c.}. \end{aligned} \tag{A.10}$$

The integration over the interaction volume, $\mathrm{d}x$, $\mathrm{d}y$, and $\mathrm{d}z$, can now be easily carried out. There are three spatial integrals, of which two are the Fourier transforms of unity ($\mathrm{d}x$ and $\mathrm{d}y$) and one is the transform of a box function ($\mathrm{d}z$). The transforms turn into two δ functions and a sinc function, respectively. The time integral also turns into a δ function of the three frequencies ω_s, ω_i, and ω_p. This is because we assume a monochromatic pump beam with infinite coherence length, which effectively leads to an infinite interaction time, $T \to \infty$, even for short crystals. Motivated by the rotational symmetry of the emitted modes, we also change to a spherical coordinate system (see Fig. 1), by replacing the summation over $\boldsymbol{s}$ with integrals over $\theta_\mathrm{s}, \theta_\mathrm{i}, \varphi_\mathrm{s}$ and φ_i. Furthermore, the only non-zero solution for the integration over the random phases, ϕ_s and ϕ_i, is for the phases to add up to a constant, yielding the relation $\phi_\mathrm{s} + \phi_\mathrm{i} = \phi_\mathrm{p} + C$. If we let $C = 0$ for simplicity, and drop some constants resulting from the integrations, we are led to

$$\begin{aligned}\frac{1}{i\hbar}\int \mathrm{d}t \hat{H}(t) = \frac{1}{i\hbar}\chi_2\, f_1 E_0 &\int \mathrm{d}\omega_\mathrm{s} \int \mathrm{d}\omega_\mathrm{i}\, A_\mathrm{s}(\omega_\mathrm{s}) A_\mathrm{i}(\omega_\mathrm{i}) \\ &\times \int_0^{\pi/2} \sin\theta_\mathrm{s}\, \mathrm{d}\theta_\mathrm{s} \int_0^{\pi/2} \sin\theta_\mathrm{i}\, \mathrm{d}\theta_\mathrm{i} \int_0^{2\pi} \mathrm{d}\varphi_\mathrm{s} \int_0^{2\pi} \mathrm{d}\varphi_\mathrm{i} \\ &\times \hat{a}_\mathrm{s}^\dagger(\omega_\mathrm{s}, \theta_\mathrm{s}, \varphi_\mathrm{s})\, \hat{a}_\mathrm{i}^\dagger(\omega_\mathrm{i}, \theta_\mathrm{i}, \varphi_\mathrm{i})\, \delta(\omega_\mathrm{s} + \omega_\mathrm{i} - \omega_\mathrm{p}) \\ &\times \delta(\Delta k_x)\, \delta(\Delta k_y)\, L\,\mathrm{sinc}\left[\frac{L}{2}\Delta k_z\right] \\ &- \text{H.c.}. \end{aligned} \tag{A.11}$$

At this stage, we observe that k_s and k_i each depend on ω_s and ω_i, respectively. Motivated by the δ-function in Eq. (A.11), we let $\omega_\mathrm{s} = \omega_{0\mathrm{s}} + \epsilon$ and $\omega_\mathrm{i} = \omega_{0\mathrm{i}} - \epsilon$, and make a series expansion of the k-vectors:

$$k_\mathrm{s} \approx k_{0\mathrm{s}} + \epsilon \frac{\mathrm{d}k_{0\mathrm{s}}}{\mathrm{d}\omega_{0\mathrm{s}}} = k_{0\mathrm{s}} + \epsilon \frac{1}{v_{\mathrm{g,s}}^Z} = k_{0\mathrm{s}} + \epsilon \frac{n_{\mathrm{g,s}}^Z}{c} \tag{A.12a}$$

$$k_\mathrm{i} \approx k_{0\mathrm{i}} - \epsilon \frac{\mathrm{d}k_{0\mathrm{i}}}{\mathrm{d}\omega_{0\mathrm{i}}} = k_{0\mathrm{i}} - \epsilon \frac{1}{v_{\mathrm{g,i}}^Z} = k_{0\mathrm{i}} - \epsilon \frac{n_{\mathrm{g,i}}^Z}{c}. \tag{A.12b}$$

In a spherical coordinate system, we have $p = \sin\theta\cos\varphi$, $q = \sin\theta\sin\varphi$, and $m = \cos\theta$, and so the phase-mismatch vector components become

$$\begin{aligned}\Delta k_x &= k_\mathrm{s}\sin\theta_\mathrm{s}\cos\varphi_\mathrm{s} + k_\mathrm{i}\sin\theta_\mathrm{i}\cos\varphi_\mathrm{i} \approx 0,\\ \Delta k_y &= k_\mathrm{s}\sin\theta_\mathrm{s}\sin\varphi_\mathrm{s} + k_\mathrm{i}\sin\theta_\mathrm{i}\sin\varphi_\mathrm{i} \approx 0,\\ \Delta k_z &= k_\mathrm{s}\cos\theta_\mathrm{s} + k_\mathrm{i}\cos\theta_\mathrm{i} - k_{0\mathrm{p}} + K\\ &\approx \frac{\epsilon}{c}(n^Z_{\mathrm{g,s}} - n^Z_{\mathrm{g,i}}),\end{aligned} \tag{A.13}$$

where we have done a first-order approximation of $\sin\theta$ and $\cos\theta$ for small angles, meaning that we consider only plane waves, and where the last component is simplified using the phase-matching condition for the forward direction, $k_{0\mathrm{s}} + k_{0\mathrm{i}} - k_{0\mathrm{p}} + K = 0$, together with Eq. (A.12). Thanks to Eq. (A.13), we can now trivially perform the integration over the spatial modes $\mathrm{d}\theta_\mathrm{s}, \mathrm{d}\theta_\mathrm{i}$ and $\mathrm{d}\varphi$, which finally leads to the following compact expression

$$\begin{aligned}\frac{1}{i\hbar}\int \mathrm{d}t\hat{H}(t) &= \frac{1}{i\hbar}\chi_2\, f_1 E_0\\ &\quad\times \int \mathrm{d}\epsilon\, A_\mathrm{s}(\epsilon)A_\mathrm{i}(\epsilon)\hat{a}^\dagger_\mathrm{s}(\epsilon)\hat{a}^\dagger_\mathrm{i}(\epsilon)\\ &\quad\times L\,\mathrm{sinc}\left[\frac{L\epsilon}{2c}(n^Z_{\mathrm{g,s}} - n^Z_{\mathrm{g,i}})\right]\\ &\quad - \text{H.c.}\\ &= \int \mathrm{d}\epsilon\, U(\epsilon)\,\hat{a}^\dagger_\mathrm{s}(\epsilon)\hat{a}^\dagger_\mathrm{i}(\epsilon) \;-\; \text{H.c.}.\end{aligned} \tag{A.14}$$

In summary, Eq. (A.1), via Eq. (A.14), has helped us find the frequency and polarization state generated in one crystal, which we will write in the form

$$|\Psi_{ZZ}\rangle = \frac{1}{B}\int \mathrm{d}\epsilon\, U(\epsilon)\,|\boldsymbol{\epsilon}\rangle \otimes |\boldsymbol{\chi}_{ZZ}\rangle, \tag{A.15}$$

where $U(\epsilon)$ is defined by Eq. (A.14), and where

$$B = \frac{\left(\int \mathrm{d}\epsilon |A_\mathrm{s}(\epsilon)A_\mathrm{i}(\epsilon)|^2\,\mathrm{sinc}^2[L\epsilon(n^Z_{\mathrm{g,s}} - n^Z_{\mathrm{g,i}})/2c]\right)^{1/2}}{\hbar(\chi_2\, f_1 E_0 L)^{-1}}, \tag{A.16}$$

is a normalization constant, such that $|\frac{1}{B}\int \mathrm{d}\epsilon\, U(\epsilon)|^2 = 1$. Here, $\boldsymbol{\epsilon}$ represents the frequency mode and $\boldsymbol{\chi}_{ZZ}$ represents the polarization mode along the Z-axis.

[1] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, Phys. Rev. Lett. **75**, 4337 (1995).
[2] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **84**, 4729 (2000).
[3] C. Kurtsiefer, M. Oberparleiter, and H. Weinfurter, Phys. Rev. A **64**, 023802 (2001).
[4] T. E. Kiess, Y. H. Shih, A. V. Sergienko, and C. O. Alley, Phys. Rev. Lett. **71**, 3893 (1993).
[5] W. Tittel, J. Brendel, N. Gisin, and H. Zbinden, Phys. Rev. A **59**, 4150 (1999).
[6] Y. H. Kim, S. P. Kulik, and Y. Shih, Phys. Rev. A **62**, 011802(R) (2000).
[7] H. Takesue and K. Inoue, Phys. Rev. A **70**, 031802(R) (2004).
[8] X. Li, P. L. Voss, J. Chen, J. E. Sharping, and P. Kumar, Opt. Lett. **30**, 1201 (2005).
[9] X. Li, P. L. Voss, J. E. Sharping, and P. Kumar, Phys. Rev. Lett. **94**, 053601 (pages 4) (2005).
[10] L. Hardy, Phys. Lett. A **161**, 326 (1992).
[11] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, Phys. Rev. A **60**, R773 (1999).
[12] M. Fiorentino, G. Messin, C. E. Kuklewicz, F. N. C. Wong, and J. H. Shapiro, Phys. Rev. A **69**, 041801(R) (2004).
[13] E. J. Mason, M. A. Albota, F. Knig, and F. N. C. Wong, Opt. Lett. **27**, 2115 (2002).
[14] S. Tanzilli, W. Tittel, H. D. Riedmatten, H. Zbinden, P. Baldi, M. D. Micheli, D. Ostrowsky, and N. Gisin, Eur. Phys. J. D **18**, 155 (2002).
[15] D. Ljunggren and M. Tengner, Phys. Rev. A **72**, 062301 (2005).
[16] M. Halder, S. Tanzilli, H. de Riedmatten, A. Beveratos, H. Zbinden, and N. Gisin, Phys. Rev. A **71**, 042335 (2005).
[17] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[18] M. Pelton, P. Marsden, D. Ljunggren, M. Tengner, A. Karlsson, A. Fragemann, C. Canalias, and F. Laurell, Opt. Express. **12**, 3573 (2004).
[19] S. Tanzilli, W. Tittel, M. Halder, O. Alibart, P. Baldi, N. Gisin, and H. Zbinden, Nature **437**, 116 (2005).
[20] F. König, E. J. Mason, F. N. C. Wong, and M. A. Albota, Phys. Rev. A **71**, 033805 (2005).
[21] G. Ribordy, J. Brendel, J. D. Gauthier, N. Gisin, and H. Zbinden, Phys. Rev. A **63**, 012309 (2001).
[22] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).
[23] T. Y. Fan, C. E. Huang, B. Q. Hu, R. C. Eckardt, Y. X. Fan, R. L. Byer, and R. S. Feigelson, Appl. Opt. **26**, 2390 (1987).
[24] K. Fradkin, A. Arie, A. Skliar, and G. Rosenman, Appl. Phys. Lett. **74**, 914 (1999).
[25] M. Tengner and D. Ljunggren, in preparation (2005).
[26] C. E. Kuklewicz, M. Fiorentino, G. Messin, F. N. C. Wong, and J. H. Shapiro, Phys. Rev. A **69**, 013807

(2004).
[27] A. E. Siegman, Laser Resonators and Coherent Optics: Modeling, Technology, and Applications **1868**, 2 (1993).
[28] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[29] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White, Phys. Rev. A **64**, 052312 (2001).
[30] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
[31] W. Tittel and G. Weihs, Quant. Inf. Comput. **1**, 3 (2001), arXiv.org:quant-ph/0107156.
[32] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **81**, 3563 (1998).
[33] D. N. Klyshko, *Photons and Nonlinear Optics* (Gordon and Breach Science Publishers, New York, 1988).
[34] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics* (Cambridge University Press, Cambridge, UK, 1995).

Paper C

Optimal focusing for maximal collection of entangled narrow-band photon pairs into single-mode fibers

D. Ljunggren and M. Tengner

Phys. Rev. A **72**, 062301 (2005)

Contributions by the author: The candidate proposed and initiated the study of the optimization of focusing. The authors jointly developed the theory and made the experiments. The numerical simulations was done by the candidate, who also wrote the paper.

Optimal focusing for maximal collection of entangled narrow-band photon pairs into single-mode fibers

Daniel Ljunggren* and Maria Tengner
Department of Microelectronics and Information Technology, The Royal Institute of Technology, KTH, Electrum 229, SE-164 40 Kista, Sweden
(Received 22 June 2005; published 2 December 2005)

We present a theoretical and experimental investigation of the emission characteristics and the flux of photon pairs generated by spontaneous parametric downconversion in quasi-phase matched bulk crystals for the use in quantum communication sources. We show that, by careful design, one can attain well defined modes close to the fundamental mode of optical fibers and obtain high coupling efficiencies also for bulk crystals, these being more easily aligned than crystal waveguides. We distinguish between singles coupling, γ_s and γ_i, conditional coincidence, $\mu_{i|s}$, and pair coupling, γ_c, and show how each of these parameters can be maximized by varying the focusing of the pump mode and the fiber-matched modes using standard optical elements. Specifically we analyze a periodically poled KTP-crystal pumped by a 532 nm laser creating photon pairs at 810 nm and 1550 nm. Numerical calculations lead to coupling efficiencies above 93% at optimal focusing, which is found by the geometrical relation L/z_R to be $\approx$1 to 2 for the pump mode and $\approx$2 to 3 for the fiber-modes, where L is the crystal length and z_R is the Rayleigh-range of the mode-profile. These results are independent on L. By showing that the single-mode bandwidth decreases $\propto 1/L$, we can therefore design the source to produce and couple narrow bandwidth photon pairs well into the fibers. Smaller bandwidth means both less chromatic dispersion for long propagation distances in fibers, and that telecom Bragg gratings can be utilized to compensate for broadened photon packets—a vital problem for time-multiplexed qubits. Longer crystals also yield an increase in fiber photon flux $\propto\sqrt{L}$, and so, assuming correct focusing, we can only see advantages using long crystals.

DOI: 10.1103/PhysRevA.72.062301 PACS number(s): 03.67.Mn, 03.67.Hk, 42.50.Dv, 42.65.Lm

I. INTRODUCTION

Spontaneous parametric downconversion (SPDC) accounts for the majority of entangled photon pairs being produced today. It can be described as a process in which the electromagnetic field of a single photon—traveling inside a dielectric material such as a birefringent crystal—interacts with the atoms by absorption and gives rise to a nonlinear response in the field of polarization, thereby leaving the possibility of two or more photons being re-emitted. The laws of conservation of energy and momentum, together with the randomness and indistinguishability in the process, also give rise to entanglement, a nonlocal correlation between the photons.

In quantum communication numerous experiments have been performed to date involving non-entangled or entangled photons being sent over long distances, e.g., sources of heralded single photons [1–3], quantum cryptography [4–6], and teleportation [7]. A typical such experiment involves launching each photon of a (entangled) pair into single-mode fibers and to deliver each one to a separate party for encoding or decoding. For successful distribution over long distances it is vital to have a high rate of pairs generated at the source, as the attenuation of the fiber is a strongly limiting factor even at the wavelength of 1550 nm for which the fiber is most transparent. Today, results with crystals of periodically poled materials have proved this viable even at moderate pump laser powers [8], and in some cases the problem has turned into a matter of limiting the pump power to avoid creating two pairs at the same time, as this will give false coincidences also when having low *single*-coupling efficiencies. Instead, what has gained importance is to have a high *pair*-coupling efficiency that increases the probability of both photons of a pair being present in the fibers once they have been created. Furthermore, the use of time-multiplexed schemes [9,10] have elicited the need of launching photons having very narrow frequency bandwidth and long coherence length in order to limit the effects of dispersion in the fibers, and to enable the use of interferometers. Rather than just filtering the emission at some desired width, as is commonly done, we will show that it is more efficient in terms of photon-rates to design the source so that the bandwidth is determined by the crystal length and fiber coupling alone.

It is the purpose of this article to calculate the maximum coupling efficiency achievable for photon pairs generated in crystals that are phase-matched for colinear emission in general, and for periodically poled $KTiOPO_4$ (PPKTP) crystals using non-degenerate quasi-phase matching (QPM) in particular. We look for the optimal condition for focusing of the pump onto the crystal and focusing of the emission onto the fiber-end (mode-matching) which maximizes either the single or the pair-coupling efficiency. The focusing is specified using the parameter $\xi=L/z_R$, adopted from [11] with a slight modification, where L is the length of the crystal and z_R is the Rayleigh range. We make no thin-crystal approximations, but take fully into account the focusing geometry of

*Corresponding author. Electronic address: daniellj@kth.se; URL: http://www.quantum.se

all three interacting fields: pump, signal, and idler, by decomposing all three fields into a complete set of orthogonal plane-wave modes. Other optimizable parameters of these beams include the direction of the beam axis and the location of the focus. Both are regarded fixed, the former being motivated by the colinear geometry of perfect quasi-phase matching, and the latter by the fact that focusing onto the center of the crystal shows to give highest efficiencies. (Support for the last claim is given in [12] for second harmonic generation.) We also regard the center frequency of the beams, the power of the pump, and the optical properties of the crystal as fixed parameters of the problem. We take into account the polychromatic character of the emission but assume a monochromatic pump (continuous-wave pump), and we investigate how the coupling efficiency depends on the length of the crystal and the bandwidth of the wavelength filter in front of the fiber, but also how the fiber coupling affects the bandwidth of the coupled photons and the achievable photon-rates. Our goal is to give a simple recipe for setting up a colinear source of entangled photon pairs that optimizes the focusing for the highest single and pair coupling efficiencies into single mode fibers, and that also determines a suitable crystal length for a desired bandwidth.

Shortly after the demonstration of parametric generation (PG) and second harmonic generation (SHG) in the 1960s, Boyd and Kleinman [11], and others, addressed the focusing in non-colinear geometries of type-I and showed the importance of optimization for achieving maximal conversion efficiency in optical parametric oscillators and frequency doublers. By using cavities to enhance the processes one can control the spatial mode of the pump, signal and idler to support only the fundamental TEM_{00} mode, and under this condition Boyd and Kleinman suggested that the general optimal focusing is to set the ξ-parameters of all fields the same ($\xi_p=\xi_s=\xi_i$). Later, Guha *et al.* [13] showed that having unequal parameters can improve the conversion even further and this is also supported by our results. The case of type-II SHG have also been studied [14], as well as sum- and difference frequency generation (SFG and DFG) [15], with similar results. These works were all treating the light as a classical field, having the signal beam acting as the relatively strong control-field that is being amplified by the much stronger pump-beam together with the creation of an idler. It is not unreasonable to expect that a different situation arises at the quantum level where both the signal and idler initially are in uncontrolled vacuum-states.

Spontaneous parametric downconversion commonly takes place in bulk crystal configurations where the signal and idler modes are not restricted by cavities. This will provide an additional degree of freedom. The pump is assumed to be TEM_{00}, but the emission will in general be spatially multimode. A central problem in this article is to find how much of the emission is in a transverse and longitudinal fundamental single-mode at different focusing conditions. For the transverse part, such a single-mode, being Gaussian shaped, is very close to the Bessel function of the first kind, $J_0(\alpha)$, which describes the shape of the fundamental fiber mode, and will therefore provide nearly perfect overlap. After determining the mode of the emission we also calculate the M^2 factor, commonly used as a measure of beam-quality, and compare it to experimentally obtained results.

To our knowledge, no analysis has been made to date that characterizes the colinear emission in quasi-phase-matched materials in the way presented here, i.e., making no assumptions about short crystals or weak focusing. It should be noted that the analytical calculations become difficult without these assumptions and so our goal have been to formulate the final expression in such a way that it can be evaluated numerically with relative ease, with only simple assumptions being made. Taking into account all the needed degrees of freedom—azimuthal and polar angular spectrum and frequency included—these numerical computations will become quite time-consuming on an ordinary personal computer, but still doable.

Various other attempts have been made in the past to characterize the one- and two-photon spatial optical modes generated by non-colinear birefringent phase-matching. However, most of them do not use single-mode fibers to collect photons; Monken *et al.* [16] and Pittman *et al.* [17] show how focusing of the pump with a lens can increase the coincidence counts using an analysis limited to thin crystals, and Aichele *et al.* [18] seek to match the spatio-temporal mode of a conditionally prepared photon to a classical wave by spectrally and spatially filtering the trigger, however, without considering focusing effects.

More recent work connected to ours is a number of papers that consider the coupling into single-mode fibers; Kurtsiefer *et al.* [19] provide, for thin crystals, a hands-on method of determining the mode of the emission using the relation between the emission-angle and the wavelength coming from the phase-matching conditions. For maximal overlap between the emission mode and the fiber-matched mode (target) they presume it is best to choose the waist of the pump-mode and fiber-matched mode equal. According to [11], and our results, this is not optimal in general. Bovino *et al.* [20] take on a more sophisticated approach as they carry out the biphoton-state calculation for a non-colinear source, which takes into account focusing, dispersion, and walk-off and arrives at a closed expression for the coincidence efficiency. Other work have been continued along the same lines [21]; our conclusion from examining the formulas herein being that high efficiency can always be achieved for any length of crystal by choosing the pump waist large enough and the fiber-matched waist small enough. This is in contrary to our results which show an optimal value of the focusing parameter ($1 \lesssim \xi \lesssim 3$). Furthermore, as shown both in this report and in [11], for a specific crystal type and wavelength configuration the value of ξ is found to be a fixed constant for all crystal lengths which makes the pump-beam waist w_0 relate to the length as $w_0 \propto \sqrt{L}$ (at optimal focusing), while the results of Refs. [20,21] appear to show a linear relationship. We are not sure whether these apparent differences are best explained by the different situations of a non-colinear and colinear source, pulsed vs. continuous-wave pump, or by otherwise different models or parameters in either case. It can be noted that our results seem to provide good agreement with experiments.

The particular source of photon pairs that spurred the work of this article is presented by Pelton *et al.* in Ref. [22]. The main idea is to create polarization-entangled photon

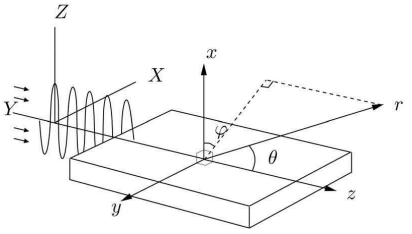

FIG. 1. The figure shows the periodically poled crystal with the laboratory coordinate system drawn. Also defined are the crystal's axes *X*, *Y*, and *Z*, referring to the polarization of the incoming and outgoing electromagnetic fields.

pairs at the non-degenerate wavelengths of 810 nm and 1550 nm from a pump-photon at 532 nm, using two orthogonally oriented [23], long, bulk KTP crystals. These crystals are periodically poled for quasi-phase matching which provides colinear emission suitable for coupling into single-mode fibers, but as told, also require some optimization for maximum throughput. Preliminary results can be found in [24]. Related work is found in [6,25,26].

The agenda of this article is as follows. Section II gives a mathematical background, starting in subsection II A with a review of the one and two-photon state of the emission derived in Appendix A. In Sec. II B we calculate the emitted modes, which are qualitatively measured using the beam quality parameter M^2. This is followed in subsection II C by a mathematical definition of the single-coupling, coincidence, and pair-coupling efficiencies. Section III presents the numerical results of the coupling (III A-III B), bandwidth (III C), and the M^2 factor (III D). Section IV covers the experimental setup and the experimental results, where a comparison is made to numerical predictions. Conclusions are found in Sec. V.

II. THEORETICAL DESCRIPTION

The aim of this section is to derive the formulas used for the numerical calculations of the emission modes, coupling efficiencies, and emission bandwidths for the emitted quantum state of the SPDC process, and also to give a physical meaning to these concepts in the role of single photon sources. We will optimize over the spatial parameters involved to find the highest quality modes and maximal coupling efficiencies attainable. The result is based on a calculation carried out in Appendix A involving the Hamiltonian that governs the interaction of spontaneous parametric down-conversion in quasi-phase-matched materials. The crystal is pumped by monochromatic and continuous wave laser light (p) of frequency ω_p, which is propagating in a Gaussian TEM_{00} mode along the *z*-axis, producing a signal (s) and idler (i) field in the same direction. Figure 1 defines the laboratory axes used; the *z*-axis being along the length *L* of the crystal, the *x*-axis along the height, and the *y*-axis along the width. The crystal is bi-axial, and the crystal axes *X*, *Y*, and *Z* are oriented as shown in the figure. We have chosen the poling period in the crystal to allow for copolarized ($Z_pZ_sZ_i$), colinear down-conversion, but the calculations are general enough to allow other polarization settings. The refractive indices, and thus the phase-matching, depends on the temperature of the crystal and is determined by the Sellmeier coefficients of PPKTP [27,28]. In general we are interested in phase-matching at non-degenerate wavelengths, and for such cases the shorter wavelength will be regarded as the signal and the longer wavelength as the idler.

Many references, following Klyshko [29], start with the coupled mode equations and look at the evolution of operators to find the two-photon state from SPDC in terms of a frequency and angular intensity distribution [30]. This is effectively the same as finding the diagonal elements of the second order moment density matrix which represent the incoherent part of the information of the state. This information is sufficient for determining the shape of the emission. However, it is not sufficient for determining the overlap between the emission and a single-mode fiber. In this case we need the "coherent" information available in the full density matrix. The approach we take in Appendix A and in the next subsection is to use the Schrödinger picture and look at evolution of the state to find the two-photon amplitude. In the following subsections we then diagonalize the corresponding density matrix into a sum of coherent parts (eigenmodes), and project each one onto the fiber-mode so that we can calculate the coupling efficiency as a sum of overlap coefficients. We also use this decomposition to calculate the electrical field and beam profile of the emission.

A. The emitted two-photon state

The two-photon amplitude describes the joint state of the signal and idler emission in terms of (internal) angular and frequency spectrum. Using spherical coordinates (see Fig. 1) the two-photon amplitude derived in Eq. (A28) becomes

$$S(\epsilon,\theta_s,\theta_i,\Delta\varphi) = \frac{4\pi^2\chi_2 f_1 L}{i\hbar}A^2(\epsilon) \times \frac{k_p^Z w_{0p}}{\sqrt{2\pi}} e^{-(k_p^Z w_{0p})^2[P^2+Q^2]/4}\mathrm{sinc}\left[\frac{L}{2}\Delta k_z'\right], \tag{1}$$

where, according to Eq. (A26)

$$\Delta k_z' = k_s\cos\theta_s + k_i\cos\theta_i - k_p^Z\sqrt{1-(P^2+Q^2)} + K, \tag{2}$$

and, according to Eq. (A25)

$$P^2+Q^2 = \frac{k_s^2\sin^2\theta_s + k_i^2\sin^2\theta_i + 2k_sk_i\sin\theta_s\sin\theta_i\cos(\Delta\varphi)}{(k_p^Z)^2}. \tag{3}$$

All three interacting fields have been decomposed into a complete set of orthogonal plane-wave modes, $\boldsymbol{k}(\theta,\varphi)$. The magnitudes of the *k*-vectors, k_s and k_i, are given by Eq. (A17), θ_s and θ_i are the internal polar angles of the plane waves of signal and idler respectively, $\Delta\varphi$ is the difference in angle between the azimuthal angles φ_s and φ_i, and ϵ is the

frequency (specified by a single parameter due to exact energy-matching). Furthermore, χ_2 is the nonlinear coefficient of the crystal, K is the grating constant of the poling, L is the length of the crystal, and w_{0p} is the pump-beam waist radius. $A(\epsilon)$ is the frequency amplitude of the detector filter having a bandwidth $\Delta\lambda$ (FWHM) and a center wavelength λ_c (all wavelengths in vacuum). Via the relation $\epsilon=2\pi c(n_\lambda/\lambda - n_{\lambda_c}/\lambda_c)$ its form, assuming a Gaussian shaped filter, is given by

$$A(\epsilon;\lambda) = e^{-2\log(2)(\lambda-\lambda_c)^2/\Delta\lambda^2}. \tag{4}$$

In a plane wave mode-decomposition, Eq. (1) represents the two-photon field (that is generated in the crystal by the pump field) in the form of a continuous angular spectrum in polar and azimuthal degrees of freedom. Together with the frequency, the full state is a tensor-product of four degrees of freedom. We will need to discretize the spectrum in order to represent it on a computer. As the size of the Hilbert space of the full ket-vector becomes very large for a large number of points in resolution, we need to limit its size to make the numerical calculations feasible. In the following, the two-photon state is therefore explicitly represented only by the polar angles of the signal, $|\theta_s\rangle$, and the idler, $|\theta_i\rangle$, written as kets, leaving the state implicitly dependent upon the two remaining degrees of freedom, $\Delta\varphi$ and ϵ. The purpose of this notation is to reflect the actual way that the state is numerically implemented as a one-dimensional array of θ (the density matrix is a two-dimensional array), with separate arrays being calculated for each discrete value $\Delta\varphi$ and ϵ. Choosing N_θ discrete plane-wave modes as a basis of the polar angle, the two-photon state can then be formulated as

$$|\psi_{si}^{\Delta\varphi,\epsilon}\rangle = \sum_{m,n=1}^{N_\theta} S(\epsilon,\theta_s^{(m)},\theta_i^{(n)},\Delta\varphi)|\theta_s^{(m)}\rangle \quad |\theta_i^{(n)}\rangle. \tag{5}$$

There are a few approximations that have been made during the calculation of S, apart from the paraxial approximation inherent in the standard form of the angular spectrum representation of the Gaussian pump field of Eq. (A19). These include (i) the assumption of a constant pump k-vector magnitude $k_p=k_p^Z$ in order to remove the implicit dependence of θ_p and φ_p in Eq. (A16), which thus leads to Eq. (3), (ii) the assumption of an infinite coherence length of the pump (cw), providing a δ-function over frequency so that we can describe the signal and idler by a single frequency ϵ, and (iii) the assumption of having the same refractive indices along the crystal's X and Y axis, such that the X-component of the k-vectors can be set to the same as that of Y. The last assumption also provides a motivation for the output of completely rotationally symmetric modes, and will greatly simplify the expressions and the numerical calculations as the azimuthal angle dependence, via φ_s and φ_i, is automatically removed from the two-photon amplitude. The two-photon density matrix is given by

$$\rho_{si}^{\Delta\varphi,\epsilon} = |\psi_{si}^{\Delta\varphi,\epsilon}\rangle\langle\psi_{si}^{\Delta\varphi,\epsilon}|, \tag{6}$$

which now contains four degrees of freedom; θ_s and θ_i being the two state parameters, and $\Delta\varphi$, ϵ being two other parameters which we will trace over later. Note that ρ_{si} is a description of the emission *inside* the crystal, not taking into account the refraction between crystal and air.

B. The emission modes and the beam quality, M^2

We are interested in the shape of the signal or idler beam profiles using free detection so that we can compare with images taken by a CCD camera. To do this comparison we need to have the beam described in terms of the electrical field, which is given as the Fourier transform of the angular spectrum (the density matrix). The electrical field, or intensity, then gives the beam profile which, in turn, determines the M^2 factor.

First, each signal or idler beam are made independent of the other beam by partially tracing over its partner. In the following we trace over the signal in the polar angle degree of freedom, and in doing so we get the reduced density matrix for the idler,

$$\rho_i^{\Delta\varphi,\epsilon} = \mathrm{Tr}_s(\rho_{si}^{\Delta\varphi,\epsilon}) = \sum_n^{N_\theta} \langle\theta_s^{(n)}|\rho_{si}^{\Delta\varphi,\epsilon}|\theta_s^{(n)}\rangle. \tag{7}$$

The remaining dependence on $\Delta\varphi$ can also be removed following the standard trace-operation, which is here equivalent to a sum over density matrices,

$$\rho_i^{\epsilon} = \mathrm{Tr}_{\Delta\varphi}(\rho_i^{\Delta\varphi,\epsilon}) = \sum_m^{N_\varphi} \rho_i^{\Delta\varphi_m,\epsilon}. \tag{8}$$

Additionally, as we could in principle measure the frequency of the photons at a resolution given by $\Delta\lambda_{res}=\lambda^2/c\Delta t_{gate}$ (set by the timing information of the detectors, >1 ns, to be <8 pm), which generally is much smaller than the bandwidths of the filters, we need to incoherently sum over the frequency ϵ in the same way, giving a final ρ_i describing the state of the idler,

$$\rho_i = \mathrm{Tr}_\epsilon(\rho_i^\epsilon) = \sum_n^{N_\epsilon} \rho_i^{\epsilon_n}. \tag{9}$$

1. Mode decomposition

We cannot, however, directly now apply a Fourier transform to the reduced density matrix ρ_i, as it is generally mixed. Instead, we shall diagonalize ρ_i to find its eigenvectors and eigenvalues. For such a Hermitian matrix all eigenvalues are real and the eigenvectors will form a complete orthonormal set. Thence, the set will represent a natural mode-decomposition of the emission, and consequently, each vector, or mode, will represent a coherent part of the emission. The sum of all modes weighted by its corresponding eigenvalue will determine the state. For each such mode, on the other hand, we can apply a Fourier transform and thus find the electrical field modes. The squared sum of all electrical field modes, again weighed by the corresponding eigenvalue, will then determine the total electrical field. We will quantify this to show our future notation; the reduced density matrix is first diagonalized by $\boldsymbol{T}^{-1}\rho\boldsymbol{T}=\boldsymbol{D}$, such that $\boldsymbol{T}=(|\zeta_1\rangle,|\zeta_2\rangle,\ldots,|\zeta_{N_\theta}\rangle)$ has the eigenvectors in the columns,

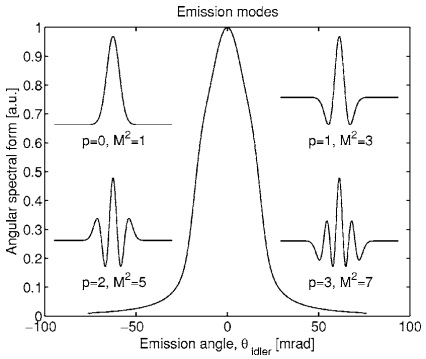

FIG. 2. The figure shows an example of the angular spectral form $u[\theta_y]$ of the emitted idler light att 1550 nm in a PPKTP crystal (central curve) which gives an M^2 factor less than 3 with a filter bandwidth $\Delta\lambda=10$ nm. The pump at 532 nm is focused close to optimal, $\xi_p=1.3$. The insets show the four lowest order LG_{p0} modes which are similar, but never the same as the natural eigenmodes of the emission, and illustrates how the M^2 factor in general grows with mode order.

and $\boldsymbol{D}$ has the eigenvalues λ_n in its diagonal elements. The result is a density matrix that can be represented as a sum of pure states,

$$\rho=\sum_{n=1}^{N_\theta}\lambda_n|\zeta_n\rangle\langle\zeta_n|, \tag{10}$$

where N_θ is the Hilbert-space dimension. Following this result, in Fig. 2 is plotted the one-dimensional angular spectral form $u[\theta_y]$, taken as an integration of the absolute square of the two-dimensional angular spectral amplitude $a_{xy}[\theta]$. We have $a_{xy}[\theta]=\Sigma_n\lambda_n\zeta_n[\theta]$, where $\zeta_n[\theta]$ is the discrete function representation of $|\zeta_n\rangle$, and $\theta^2=\theta_x^2+\theta_y^2$. Hence,

$$u[\theta_y]=\sum_{\theta_x}|a_{xy}[\sqrt{\theta_x^2+\theta_y^2}]|^2, \tag{11}$$

is the one-dimensional angular spectral form.

2. The field intensity

We can now transform the angular spectrum modes $|\zeta_n\rangle$, into electrical field modes E_n. As these modes are rotationally symmetric and depend on one parameter only, the electrical field is most suitably expressed through the Hankel transform. In writing the transform in the following form we make use of the fact that the vector $|\zeta_n\rangle$, again written as a discrete function, $\zeta_n[\theta,\varphi]=\zeta_n[\theta]$, is independent of φ. Thus,

$$E_n(x,y,z)=\sum_\theta\lambda_n\zeta_n[\theta]e^{-ikz\cos\theta}J_0(k\sqrt{x^2+y^2}\theta), \tag{12}$$

where the basis functions $J_0(\alpha)$ of the Hankel transform are the Bessel function of zero order and the solution to $(1/2\pi)\int_0^{2\pi}\exp(i\alpha\cos\varphi)d\varphi$. However, the one-dimensional fast Hankel transform (FHT), which would possibly provide very fast computations, is not widely implemented, at least not in an efficient form for use in Matlab or Mathematica and was not available to us at the time for the numerical calculations. Therefore, the next simplest transform at hand is the two-dimensional Fourier transform,

$$E_n(x,y,z)=\sum_\theta\sum_\varphi\lambda_n\zeta_n[\theta,\varphi]e^{-ikz\cos\theta}\times e^{kx\sin\theta\cos\varphi}e^{ky\sin\theta\sin\varphi}. \tag{13}$$

With still two dimensions being used, Eq. (13) can also be rewritten using the polar angle components θ_x and θ_y,

$$E_n(x,y,z)=\sum_{\theta_x}\sum_{\theta_y}\lambda_n\zeta_n[\sqrt{\theta_x^2+\theta_y^2}]e^{-ikz\cos(\sqrt{\theta_x^2+\theta_y^2})}\times e^{kx\sin\theta_x}e^{ky\sin\theta_y}, \tag{14}$$

where $\theta=\sqrt{\theta_x^2+\theta_y^2}$. In this form, which is the form we will use, Eq. (14) represents a standard single two-dimensional FFT. Note that this transform is, in general, not separable with respect to x and y into two, but simple, one-dimensional transforms. This is a characteristic of Laguerre-Gaussian modes and of the modes emitted by the crystal, in comparison to Hermite-Gaussian modes which are always separable.

The intensity is now given by incoherently summing all field-modes,

$$I(x,y,z)=\sum_{n=1}^{N_\theta}|E_n(x,y,z)|^2. \tag{15}$$

Finally, the transversely integrated intensity profile of the emitted beam is given by $I(y,z)=\Sigma_x I(x,y,z)$.

3. Gaussian beam fitting

The beam waist radius $w(z)$ can be found from the standard deviation $\sigma(z)$, or the second moment, of the intensity distribution $I(y,z)$, as $w(z)=2\sigma(z)$, see Ref. [31]. The standard deviation is known to provide the correct waist estimate for arbitrary multimode light as opposed to trying to make a curve-fit with various mode-shapes. Readily, $\sigma^2(z)=\Sigma_y(y-\bar{y}(z))^2I(y,z)$, where $\bar{y}(z)=\Sigma_y yI(y,z)$ is the expectation value with respect to the spatial position y in the intensity distribution. As said, we will use the beam quality factor M^2 to quantify the emission. This factor is determined through the Rayleigh range

$$z_R=\frac{\pi w_0^2}{M^2\lambda}, \tag{16}$$

entering the standard Gaussian beam formula

$$w_{\text{model}}(z)=w_0\sqrt{1+\left(\frac{z-z_0}{z_R}\right)^2}. \tag{17}$$

By varying the parameters w_0 and M^2 we can make a curve-fitting of the model profile $w_{\text{model}}(z)$ to the actual beam profile $w(z)$, such that the M^2-factor is determined. Eq. (16) states that the diffraction limited fundamental Gaussian mode TEM_{00} has a beam quality factor of $M^2=1$. As a comparison, this factor increases for general higher order Laguerre-Gaussian modes LG_{pm} [32], defined by the radial

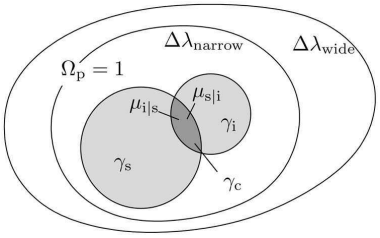

FIG. 3. The figure shows a Venn diagram. It illustrates the single coupling efficiencies γ_{s} and γ_{i}, pair coupling γ_{c}, and conditional coincidences $\mu_{\text{s|i}}$ and $\mu_{\text{i|s}}$, which are defined in the text. The total amount of pairs Ω_{p} generated within the bandwidth of the detector filter $\Delta\lambda$ is normalized to unity, and represents perfect coupling.

index p and the azimuthal mode index $m=0$, such that $M^2=3$ for $p=1$, $M^2=5$ for $p=2$, and $M^2=7$ for $p=3$ and so on, see Fig. 2.

C. Single coupling, coincidence, and pair coupling

To characterize the source and to optimize the coupling of the emission into optical fibers we shall make use of three parameters: single coupling, conditional coincidence, and pair coupling. However, before we define each of the three coupling parameters we shall briefly comment on the necessity to relate them to the detection window being used, i.e., the frequency bandwidth of the detector filter $\Delta\lambda$. The emission will always fluoresce in a wide spectrum, and in that sense there is no meaning to speak about a coupling efficiency for photons that cannot be seen through the window in any case. By making a simple normalization to the filter bandwidth, the coupling probability will consistently measure only how well photons of specific frequencies are spatially collected into the fibers. For example, for any fixed filter and no spatial filtering, as is almost the case with a multimode fiber, and certainly the case in free-space, the coupling is always perfect. Effectively, this normalization enters the calculations through the bandwidth in Eq. (4). Figure 3 helps to illustrate the different coupling parameters using a Venn diagram.

1. Single coupling

The *single-coupling* efficiencies γ_{s} and γ_{i} are readily defined as the probability to find a photon in the fiber which has been emitted within a certain filter bandwidth. The single-coupling efficiency is useful when maximizing the individual rate of photons present in the fibers. To calculate the probability we shall take the overlap of the emitted modes with the mode of the fiber as seen from the crystal, here called the *fiber-matched mode*. That is to say, the form of the mode that can be traced back to the crystal from the fiber tip, not worrying about crystal refraction or any other optics in between performing the actual transformation. Also, we do not consider any additional aperture limitations enforced, e.g., by irises.

The true mode of the fiber is described by a Bessel function. However, it can be approximated very well with a fundamental Gaussian which in normalized form is described by

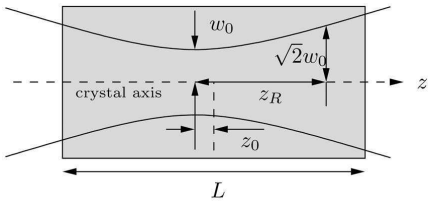

FIG. 4. The picture shows the geometry of focusing, with the Rayleigh-range z_R, the crystal length L, the beam waist radius w_0, and the focus offset z_0 being defined. The focusing parameter is defined as $\xi=L/z_R$.

$$|G_{00}\rangle = \frac{k^Z w_{00}}{\sqrt{2\pi}} e^{-ik^Z z_{00}\cos(\theta)-(k^Z w_{00})^2 \sin^2(\theta)/4} |\theta\rangle, \tag{18}$$

where w_{00} is the beam waist radius of the fiber-matched mode, TEM_{00}, as determined by the focusing system, and z_{00} is the location of the corresponding focus (which shall be at the center of the crystal $z_{00}=0$ for optimum coupling), see Fig. 4.

The single-coupling efficiency is trivially given by $\gamma = \text{Tr}(|G_{00}\rangle\langle G_{00}|\rho)$, but the numerical optimization converges slowly and badly using this form. For this reason we shall exploit the diagonalization and calculate the single coupling efficiency as the sum of the projection of each emitted mode $|\zeta_n\rangle$ onto the fiber-matched mode $|G_{00}\rangle$,

$$\gamma = \sum_{n=1}^{N_\theta} \lambda_n |\langle \zeta_n | G_{00}\rangle|^2, \tag{19}$$

where $|\zeta_n\rangle$ is given by the density matrix, ρ_{s} or ρ_{i}, as defined by Eq. (10), resulting in γ_{s} or γ_{i} respectively.

2. Optimization

The maximum achievable coupling efficiency is determined by an optimization of Eq. (19) with respect to the focusing conditions of either the pump mode, or the fiber-matched signal/idler mode, or both. To quantify the focusing we shall use the beam focusing parameter $\xi=L/z_R$, where L is the length of the crystal and z_R is the Rayleigh-range (note that we have $M^2=1$ for both the pump mode and the fiber-matched modes). See Fig. 4. The parameter is suitable as a dimensionless representation of the focusing geometry. (As will be shown further ahead, the results indeed show that the geometry is kept intact at optimal focusing, irrespectively of the length of the crystal, which corresponds to a fixed ξ^{opt}). In both Eq. (1) and Eq. (18) the parameter ξ enters through the beam waist radius of the pump mode $w_{0\text{p}}$ and the signal/idler fiber-matched mode w_{00}, according to $w_{0\text{p}}=\sqrt{L\lambda_{\text{p}}/\pi\xi_{\text{p}}}$, and $w_{00}=\sqrt{L\lambda_{\text{s,i}}/\pi\xi_{\text{s,i}}}$. We can formalize the optimization of the signal and idler fiber-matched modes as

$$\gamma^{\text{opt}} = \max_{\xi_{\text{s,i}}} \gamma(\xi_{\text{p}}, \xi_{\text{s,i}}), \tag{20a}$$

$$\xi^{\mathrm{opt}} = \arg\max_{\xi_{s,i}} \gamma(\xi_p, \xi_{s,i}), \tag{20b}$$

with γ given by Eq. (19).

3. Conditional coincidence

The *conditional coincidences*, $\mu_{s|i}$ and $\mu_{i|s}$ are useful for the characterization of heralded single photon sources, and are defined as the probability to find a photon in either the signal or the idler fiber given that the partner photon has entered its fiber, whether or not its detected. The conditional coincidence probability is found by first projecting the two-photon amplitude onto the one fiber, and then calculating the overlap with the other fiber in the same way as for single coupling. In this example we will search for $\mu_{i|s}$ and make a conditional measurement on the signal, defined by the following operator

$$M_s = |G_{00}^{(s)}\rangle\langle G_{00}^{(s)}|. \tag{21}$$

Due to the measurement, the derivation of ρ_i will be slightly different here, and we need to take a few steps back and reformulate the two-photon density matrix ρ_{si}^{ϵ} as a coherent sum of amplitudes with respect to $\Delta\varphi$, instead of as a incoherent trace operation in Eq. (8). The density matrix is now written

$$\rho_{si}^{\epsilon} = \sum_m \sum_l |\psi_{si}^{\Delta\varphi_m,\epsilon}\rangle\langle\psi_{si}^{\Delta\varphi_l,\epsilon}|. \tag{22}$$

Using the measurement operator M_s, the two-photon density matrix after the projection becomes

$$\rho_{si|s}^{\epsilon} = \frac{M_s \quad 1_i \rho_{si}^{\epsilon} M_s \quad 1_i}{\mathrm{Tr}(M_s \quad 1_i \rho_{si}^{\epsilon} M_s \quad 1_i)}. \tag{23}$$

The reduced density matrix is readily found by tracing over the partner, $\rho_{i|s}^{\epsilon} = \mathrm{Tr}_s(\rho_{si|s}^{\epsilon})$, which leaves only a trace over frequency, $\rho_{i|s} = \Sigma_n \rho_{i|s}^{\epsilon_n}$. The conditional coincidence is now defined in the same way as for single coupling; we can replace γ by $\mu_{i|s}$ in Eq. (19), still using Eq. (10) to find the eigenvalues λ_n and eigenmodes $|\zeta_n\rangle$ of $\rho_{i|s}$. We have,

$$\mu_{i|s} = \sum_{n=1}^{N_\theta} \lambda_n |\langle\zeta_n|G_{00}^{(i)}\rangle|^2, \tag{24}$$

where $|G_{00}^{(i)}\rangle$ is the fiber-matched mode of the idler. The parameter $\mu_{s|i}$ follows accordingly, as well as the formal optimization:

$$\mu^{\mathrm{opt}} = \max_{\xi_{s,i}} \mu(\xi_p, \xi_{s,i}), \tag{25a}$$

$$\xi^{\mathrm{opt}} = \arg\max_{\xi_{s,i}} \mu(\xi_p, \xi_{s,i}). \tag{25b}$$

4. Pair coupling

Finally, the *pair-coupling* efficiency γ_c is defined as the probability to find both photons of a pair in the respective fiber. This measure tells what fraction of the pairs enters the fibers compared to the total amount of pairs that are generated within the frequency bandwidth window. The pair-coupling can be derived from the single coupling and conditional coincidence using effectively Bayes's rule, see Fig. 3,

$$\gamma_c = \mu_{i|s}\gamma_s = \mu_{s|i}\gamma_i. \tag{26}$$

The alternative is to calculate the coupling via $\gamma_c = \mathrm{Tr}(M_s \quad M_i \rho_{si})$, but this requires the calculation of ρ_{si}, which is computationally more demanding. When computing $\mu_{i|s}$ and γ_s via Eq. (26), using Eq. (24) and Eq. (19), the ket is sufficient, because we can simplify the trace-operation of Eq. (7), and also the projection of Eq. (23), to work in ket-space before the trace over frequency; $\rho_i^{\epsilon} = \mathrm{Tr}_s(\rho_{si}^{\epsilon}) = \Sigma_{m,n,j} S_{m,j} S_{n,j}^* |\theta_i^{(m)}\rangle\langle\theta_i^{(n)}|$. We could also think of rewriting $\mathrm{Tr}(M_s \quad M_i \rho_{si})$ using two-photon kets in the same way, but as ρ_{si} generally becomes a mixture after tracing over frequency this is not an option. To compute γ_c before the frequency trace is also not an option numerically, as the trace over frequency involves a for-loop and optimization performed within it will reduce efficiency heavily.

The measure γ_c should be compared to $\eta \equiv \gamma_c / \sqrt{\gamma_s \gamma_i} = \sqrt{\mu_{s|i}\mu_{i|s}}$, which is basically γ_c normalized to γ_s and γ_i, that have been used by some authors [20,21]. The parameter η is useful as a type of measure of correlation that tells how well the focusing system has been set up to couple the modes of the idler emission to the same as those conditioned by the signal emission, or vice versa, depending on which of the two possess the smaller single-coupling efficiency. We intend to simply plot γ_c as this compares directly to γ_s and γ_i in terms of achievable photon rates; in principle, γ_c could be low while η is high.

III. NUMERICAL PREDICTIONS

All results in this section are for the case of a PPKTP crystal with the poling period $\Lambda = 2\pi/K = 9.6$ μm operating at perfect quasi-phase matching; the pump at 532 nm creates emission at 810 nm and 1550 nm in the absolute forward direction. The temperature $T = 111$ °C, which affects the k-vector magnitudes, is chosen such that $k_p = k_s + k_i + K$, see Ref. [22].

The numerical calculations are implemented in Matlab using Eq. (1)–(3). All refractive indices are determined by the Sellmeier equations [27,28], setting the wavelength and temperature dependence of the k-vector magnitudes. The resolution N_θ of the discrete angular spectral amplitude representation in the polar degree are a few hundred points and varies between 1–100 μradians, with the higher resolution for short crystals and strong focusing (wide-spread emission) and the lower resolution for long crystals and weak focusing (narrow emission). The needed azimuthal angle resolution N_φ is found to be $\gtrsim N_\theta/5$, and the frequency resolution N_ϵ varies between a few points for short crystals to a few hundred points for long crystals where the spectrally induced contribution to spatial multimode is larger. To spare the computer from unnecessary workload we observe that the two-photon density-matrix in Eq. (6) (scaling as N_θ^2 number of points in size) is always pure and can be fully represented by its amplitude vector alone (scaling as N_θ), for all of the calculations.

A. Single coupling

As said earlier, according to our definition the single-coupling efficiency depends on the emission bandwidth filter that is being used. This is because of the fact that many of the different frequencies created in the SPDC process will not couple into a single-mode fiber. Looking at a single frequency of the emission, the angular spectrum of the emission will be described by a single sinc-function for each of the plane waves of the pump, see Eq. (1). As will be argued in the next subsection, most of these sinc-functions will overlap nearly perfectly at optimal pump-focusing such that the emission is strongly spatially coherent and define almost a single-mode that will couple well into a single-mode fiber. If the pump-focusing is too weak it will create transverse multimode emission, as the many sinc-functions are then distributed along the transverse position of the pump beam and do not coincide. If the pump is instead focused too strongly the effect is the same, except that the multimode now originates from longitudinal position, also providing bad coupling. This is the general picture using the window of a single emission frequency.

If we look at a wide spectrum of the emission, each of the different frequencies can be seen as composed by a set of sinc-functions, each set in a different direction, and with every sinc in a set coming from one plane wave in the decomposition of the pump. For long crystals, when the width of the sinc-functions narrows down, the different sets of sinc-functions will no longer overlap. Within each set the sinc-functions are spatially well overlapping, thus defining a coherent single-mode, but as the sets do not overlap the emission will become spectrally multimode similar to above, also resulting in spatial multimode. This again provides poor coupling efficiencies. However, coupling into fibers automatically does some spatial filtering as it selects only the coherent part of the emission defining a single-mode, i.e., sinc-functions largely overlapping, and thereby it also does some frequency filtering. Altogether, this motivates why we have looked at only a single frequency of the emission for the results of the numerical calculations of the single coupling efficiencies shown in Figs. 5–7. We will refer to this case by saying that we have a "narrow enough" filter bandwidth, $\Delta\lambda_{\text{narrow}}$, which maintains a single-mode at optimal focusing of the pump and the signal and idler fibers, i.e. the bandwidth is narrow enough that the different sinc-sets, corresponding to different frequencies, within the bandwidth overlap (are coherent). Frequency filtering effects, as those just described, are left to the next section.

Figure 5 shows the single-coupling efficiency of the idler γ_i plotted against the crystal length L and the focusing of the pump-beam, via its waist w_{0p}. For each sample in the plot, the idler fiber focusing has been optimized using Eq. (20) to find the maximum coupling γ_i^{opt}. As seen, there is always the same maximal coupling to be found for any length of the crystal by changing the pump-beam waist radius accordingly. The straight lines show that the focusing parameters of both the pump ξ_p and the idler fiber focusing ξ_i^{opt} are constant, which means that the geometry of the beam profile and the crystal edges should stay fixed for different lengths of the crystal for optimal focusing. The said graph would look

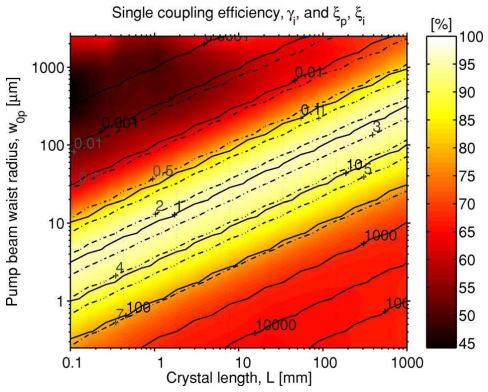

FIG. 5. (Color online) The single coupling of the idler γ_i^{opt}, plotted for a narrow enough filter bandwidth, $\Delta\lambda_{\text{narrow}}$, which shows that about 95% of the emission can be coupled into a single-mode fiber at optimal focusing. The solid line shows the pump-focusing parameter ξ_p, and the dashed-dotted lines show the focusing of the idler's fiber-matched mode ξ_i^{opt}. For each data sample the idler focusing has been optimized for maximum coupling using Eq. (20).

nearly the same for the signal emission, and, taking a different view of the results, Fig. 6 clearly shows the importance of choosing the right combination of focusing for the pump and for the fibers. Interestingly, we observe that as long as the fiber focusing is matched to the pump focusing, for any given length of the crystal, then the coupling efficiency will reach >45% irrespectively of the pump focusing. This fact may very well explain the relatively high efficiency nevertheless achived in many fiber-based SPDC-setups for which the experimentalist perhaps have not worried about changing the pump's focusing, but rather solely the fiber coupling.

Figure 7 shows both the signal and idler coupling in a graph that is parametrized by the pump focusing. In each case the optimal fiber focusing is found, and plotted along

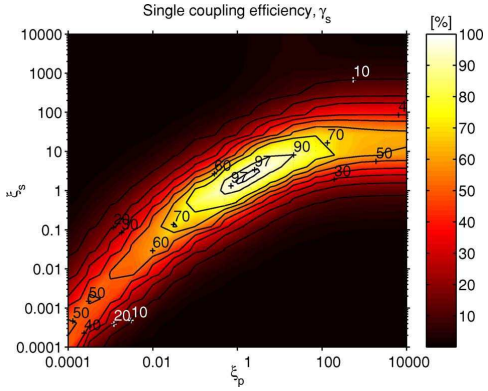

FIG. 6. (Color online) The single coupling of the signal γ_s, plotted for a narrow enough filter bandwidth, $\Delta\lambda_{\text{narrow}}$, which reaches a maximal 98% at optimal focusing, $\xi_p=1.7$ and $\xi_s=2.3$.

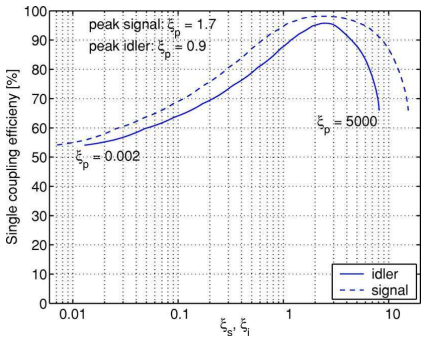

FIG. 7. (Color online) The single couplings, γ_i^{opt} and γ_s^{opt}, reaches a maximum at $\xi_p=0.9$ for the idler, and at $\xi_p=1.7$ for the signal, which corresponds to $\xi_i^{opt}=2.4$ and $\xi_s^{opt}=2.3$. The line representing the signal in this graph is essentially a plot of the ridge of the surface in Fig. 6.

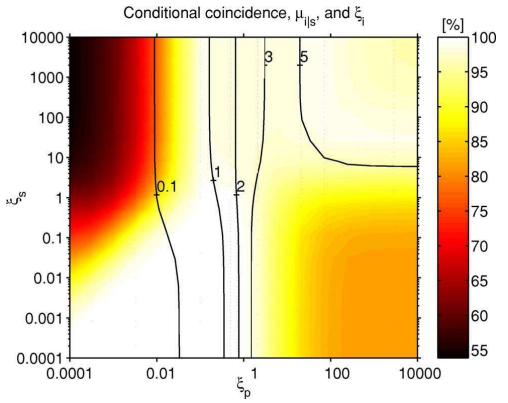

FIG. 8. (Color online) The conditional coincidence $\mu_{i|s}$, plotted versus the focusing of the pump ξ_p and the focusing of the signal's fiber-matched mode ξ_s. For each sample in the graph the focusing of the idler (ξ_i^{opt}=solid lines) is optimized to find the maximum $\mu_{i|s}^{opt}$ (up to 100%), using Eq. (25) with a narrow signal filter, $\Delta\lambda_{narrow}$, and no idler filter.

the horizontal axis. In this asymmetrical configuration it leads to a maximal $\gamma_s^{opt}=98\%$ when optimizing the focusing for the 810 nm emission ($\xi_p=1.7$ and $\xi_s^{opt}=2.3$), and $\gamma_i^{opt}=93\%$ for the 1550 nm emission ($\xi_p=0.9$ and $\xi_i^{opt}=2.4$). The optimal focusing of the pump depends on the amount of non-degeneracy for each of the wavelengths, e.g., for the degenerate case (1064 nm) the optimal focusing is $\xi_p=1.4$ and $\xi_{s,i}^{opt}=2.3$. It should be noted that, in general, the found optimal focusing parameters do not correspond to a match of the beam-waist sizes [19], but rather to an equal geometry. However, a matching of the waists are within the same order of magnitude comparable to using optimal focusing parameters.

B. Coincidence and pair coupling

For any focusing of the pump-beam, the fundamental modes of the signal and idler emission will be highly correlated, meaning that, e.g., a signal photon that enters its fiber will have its idler partner entering the other fiber, provided correct fiber focusing. At optimal focusing of the pump-beam, this correlation is always high if the partner beam is focused optimally, independent of the focusing of the beam that we condition upon. In other words, at optimal focusing of the pump-beam the conditional coincidence $\mu_{i|s}$, i.e., the probability of having the idler photon in the fiber given that the signal photon is in the fiber, will be mainly set only by its single coupling probability γ_i, which is always at a high value at optimal focusing due to the emission being mostly single-mode, see Fig. 8. In contrast, because of the multimode character of the emission at other pump-beam focusing settings than optimal, a high conditional coincidence can, in that case, only be attained near optimal focusing for both the signal and idler fibers. Each sample in the plot has been generated using Eq. (25) with a narrow filter, $\Delta\lambda_{narrow}$, at the signal side, as defined earlier, and without a filter at the idler side, when finding the maximum $\mu_{i|s}^{opt}$ that corresponds to optimal focusing of the idler, ξ_i^{opt}. As can be deduced from the graph, the conditional coincidence is always very high, reaching 100% for most weaker focusing conditions. When instead using an idler frequency filter that is matched to the signal filter, then $\mu_{i|s}$ will be bounded above by 71%, assuming Gaussian shaped filters on both sides. This limitation follows from the fact that while the signal photon of a given pair may very well be transmitted through its filter, the idler may not. Using Eq. (4), the maximum number can be easily derived from the normalized overlap integral $\int|A_s(\epsilon)|^2|A_i(\epsilon)|^2d\epsilon/\int|A_s(\epsilon)|^2d\epsilon=1/\sqrt{2}$, for which we note that the result is independent of the bandwidth.

Additional qualitative results on the optimal joint focusing can be found by turning to the pair coupling efficiency γ_c. As opposed to $\mu_{i|s}$, this measure relates to the total amount of pairs that is generated, and not only to those conditioned upon. As shown in Fig. 9, for optimal pump-beam focusing, there is a maximal value of about 97% for γ_c at $\xi_s=2.0$ and $\xi_i=2.3$. Note that, since the optimal pump-beam focusing varies for each of the beams for a non-degenerate wavelength case ($\xi_p=1.7$ for signal and $\xi_p=0.9$ for idler), we had to find a compromise using $\xi_p=1.3$. This graph is again plotted using a narrow filter at the signal and no filter at the idler. Equation (26) tells us that for matched filters, γ_c will also be limited to 71%, as long as $\gamma_s=1$ which is achievable with narrow filters. In general, both the conditional coincidence and the pair coupling decrease for wide bandwidths; $\mu_{i|s}$ in such case being bounded above by 100% and γ_c bounded above by the value of γ_s.

In terms of sources of heralded single photons, these results imply that almost perfect correlation can be achieved by careful focusing and by having no limiting interference filter on the triggered photon side; leaving such sources limited entirely by the transmission imperfections of lenses and filters, and by detector efficiencies.

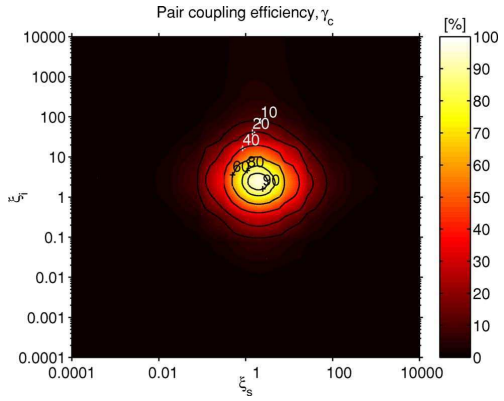

FIG. 9. (Color online) The pair coupling $\gamma_c=\mu_{i|s}\gamma_s$ at a pump focusing of $\xi_p=1.3$, which is trade-off between what is optimal for the signal ($\xi_p=1.7$) and the idler ($\xi_p=0.9$) individually. At optimal focusing, $\xi_s=2.0$ and $\xi_i=2.3$, the maximum γ_c is about 97%, using a narrow signal filter, $\Delta\lambda_{narrow}$, and no idler filter.

C. Photon-rate and bandwidth

In this subsection we will look at the achievable photon fluxes in free-space and in single-mode fibers and its dependence on the crystal length. As we will argue, and we have shown numerically, this dependence will in turn depend on the chosen frequency filter. Our arguments will follow a series of steps, where the later steps include the effects of spatial and spectral filtering. The final results are found in Fig. 10 and Fig. 11.

As a first step, imagine the pump beam to be a single plane wave that is perfectly phase-matched for a single frequency of the signal and the idler along the z-axis, called here the forward direction. In this case, by looking at the two-photon amplitude Eq. (1), we see that the height of the sinc-function, which describes the angular spectrum, is $\propto L$, corresponding to an L^2 dependence for the intensity (One should imagine two-dimensional, "Mexican-hat-like", sinc-functions). The width of the sinc will shrink $\propto 1/L$, such that the flux will increase $\propto L$. This argument is still valid considering the spatial transverse multimode emission created by such a plane wave pump, discussed earlier.

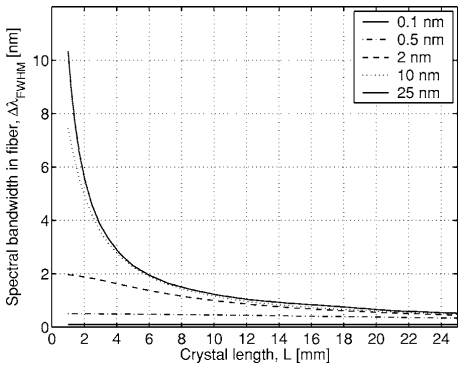

FIG. 10. The fiber coupled bandwidth is $\propto 1/L$ for a wide enough spectral filter $\Delta\lambda_{wide}$, see text, which can be said to be the case for the solid line of $\Delta\lambda=25$ nm for all crystal lengths defined by the plot. In the limit of no filter at all, the graph corresponds to the single-mode bandwidth $\Delta\lambda_{SM}$, see Eq. (28). The graph shows the result for the signal emission (810 nm) at optimal focusing conditions, $\xi_p=1.7$ and $\xi_s=2.4$, and the legend shows what filter bandwidth $\Delta\lambda$ was used for each line.

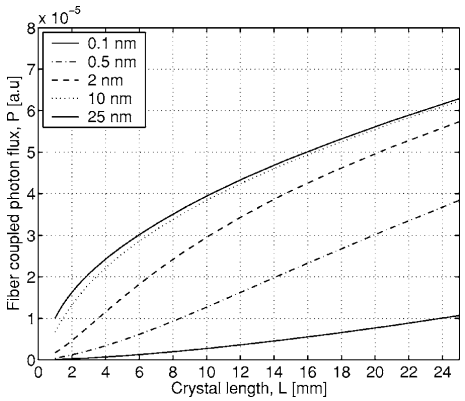

FIG. 11. The fiber photon flux is $\propto\sqrt{L}$ for a wide enough filter $\Delta\lambda_{wide}$, and $\propto L\sqrt{L}$ for a narrow enough filter $\Delta\lambda_{narrow}$. The filter is defined as narrow or wide in relation to the natural single-mode bandwidth $\Delta\lambda_{SM}$. For the solid line of $\Delta\lambda=25$ nm the case has been reached where $\Delta\lambda=\Delta\lambda_{wide}>\Delta\lambda_{SM}$. The graph shows the result for the signal emission (810 nm) at optimal focusing conditions, $\xi_p=1.7$ and $\xi_s=2.4$, and the legend shows what filter bandwidth $\Delta\lambda$ was used for each line.

As a second step, consider a focused pump being composed of many differently directed plane waves. In this case, still looking at the same single frequency emitted, each such plane wave will phase-match a little less strongly than the one in the absolute forward direction. We will have a collection of sinc-functions being added together, each originating from a different plane pump wave, and numerical calculations show that the combined total width, or envelope, of these sinc-functions will decrease for longer crystals, thus adding to the previous result a factor $1/\sqrt{L}$, with the flux now becoming $\propto\sqrt{L}$.

The third step includes the observation that the energy of the pump beam is concentrated to the plane wave in the forward direction for longer crystals at optimal focusing. Equation (1) shows that the intensity will be $\propto w_{0p}^2$, because, at optimal focusing we have $z_R=L/\xi_p$, where z_R is given by Eq. (16), and thus $w_{0p}^2\propto L$. The total flux is now $\propto L\sqrt{L}$.

As a last step we include filtering. In the previous steps we looked at a single frequency of the emission, which means that the bandwidth was narrow enough for the emission to be a single-mode (at optimal focusing). For narrow enough bandwidths we therefore get a flux

$$P \propto L\sqrt{L}\Delta\lambda_{\text{narrow}}, \tag{27}$$

which is valid both in free-space and in fiber. As an effect of the phase-matching conditions there will be a tight connection between the spectral and spatial modes, as we described in Sec. III A for frequency filtering. In terms of fiber-coupling this means that when the fiber spatially filters the emission it will also effectively do frequency filtering. The bandwidth of the signal emission (810 nm) coupled into single-mode fibers (using no separate frequency filter) is given by

$$\Delta\lambda_{\text{SM}} = B/L, \tag{28}$$

where the value $B=1.23\times10^{-11}$ [m^2] is found for PPKTP when both the pump and fiber are focused optimally, see Fig. 10. We will refer to this bandwidth as the single-mode bandwidth. It will also determine how narrow the bandwidth of a filter ($\Delta\lambda_{\text{narrow}}<\Delta\lambda_{\text{SM}}$) need to be for any given length of the crystal to be considered narrow. The photon flux in the fiber will be

$$P \propto L\sqrt{L}\Delta\lambda_{\text{SM}} = \sqrt{L}, \tag{29}$$

for any filter $\Delta\lambda>\Delta\lambda_{\text{SM}}$. In Fig. 11 we have plotted the flux for different filters, $\Delta\lambda_{\text{narrow}}<\Delta\lambda_{\text{SM}}<\Delta\lambda_{\text{wide}}$. For filter bandwidths that are "wide enough," $\Delta\lambda_{\text{wide}}$, the free-space emission will be multimode even at optimal pump focusing, and the free-space photon flux becomes

$$P \propto \sqrt{L}g(\Delta\lambda_{\text{wide}}), \tag{30}$$

where g is some unknown and non-trivial function determined by the properties of the crystal material via the Sellmeier equations.

These results clearly show that it is advantageous to have long crystals as the photon-rate will always monotonically increase even when coupling the emission into single-mode fibers. As an effect, we can keep the pump power low, promoting the use of a compact and cheap laser. This requires that we change the focusing of both the pump ξ_{p} and the fibers $\xi_{\text{s,i}}$ to the optimal for some length L. Additionally, longer crystals give narrower bandwidth, which is very advantageous in many applications of entangled photons. For example, in time-multiplexed schemes it is crucial that the photon packets keep their widths in the fibers and do not broaden due to chromatic dispersion, and the broadening can be limited by having a narrow bandwidth. Another way of reducing the effect of broadening is by introducing negative dispersion using an appropriatly designed fiber Bragg grating. In general these have to be custom manufactured for broad bandwidths, but for telecom bandwidths, 30–80 GHz, (in the C-band, between 1525–1562 nm) these are standard off-the-shelf items, and corresponds to wavelength bandwidths of about 0.25–0.65 nm at 1550 nm. We can see from Eq. (28) that 70–180 mm long crystals are needed, taking into account the conversion factor between signal and idler bandwidths $[\Delta\lambda_{\text{i}}=(\lambda_{0\text{i}}/\lambda_{0\text{p}}-1)^2\Delta\lambda_{\text{s}}\approx3.66\times\Delta\lambda_{\text{s}}]$. Narrow bandwidth can of course be obtained by the use of spectral filters, however, our results show that it is better in terms of photon-rates to use long crystals to achieve small bandwidths rather than to strongly filter the emission of a short crystal.

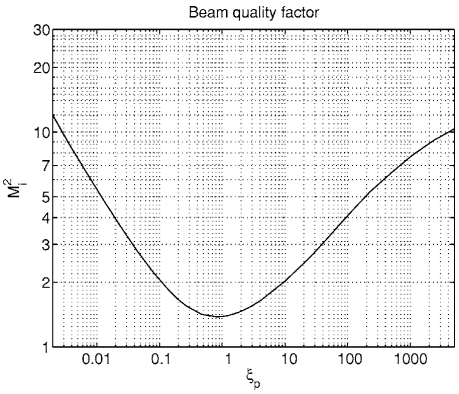

FIG. 12. The beam quality factor M^2 of the idler plotted against the pump beam focusing ξ_{p}. The smallest value, $M^2=1.4$, is found for $\xi_{\text{p}}=0.9$

(This is in contrast to what is claimed by Lee *et al.* in Ref. [33], for birefringent phase-matching and intersecting cones.) Furthermore, with narrow bandwidth follows also long coherence length of the photons which is highly desirable when working with interferometry as is commonly done when using time-multiplexing analyzers to code and decode qubits.

D. M^2 and coupling

In this subsection we will present the numerical predictions of the emission mode in terms of the beam quality factor M^2 for different focusing conditions. We will also elaborate on the connection between the beam quality factor and the coupling efficiency.

Figure 12 shows the beam quality factor M_{i}^2 plotted against the focusing of the pump for a narrow enough frequency bandwidth of the idler emission ($\Delta\lambda_{\text{narrow}}\ll\Delta\lambda_{\text{SM}}$). There is a clear optimal focusing, where the emission reaches close to single-mode, $M_{\text{i}}^2=1.4$, at a focusing of $\xi_{\text{p}}=0.9$. These results are valid for any length of the crystal, compare to Fig. 5. A low value of M^2 means that the light is close to a single-mode, and thus possible to couple well into a single-mode fiber. For bandwidths larger than the single-mode bandwidth $\Delta\lambda_{\text{wide}}\gg\Delta\lambda_{\text{SM}}$, the light will become spatially multimode and the coupling efficiency will decrease accordingly.

Figure 13 shows the relation between the coupling efficiency γ_i and the M_{i}^2, as the focusing ξ_{p} of the pump is varied. The correspondence is clear, and we can see that different M^2-values can provide the same coupling efficiency. This is so because the coupling efficiency is only determined by how much of the emission is in the fundamental mode. What determines the M^2 is the distribution of the light between the higher order modes, and this can differ from one case to another, even with the same amount contributing to the fundamental mode. In general, as we have said, too weak focusing will provide spatial transverse mul-

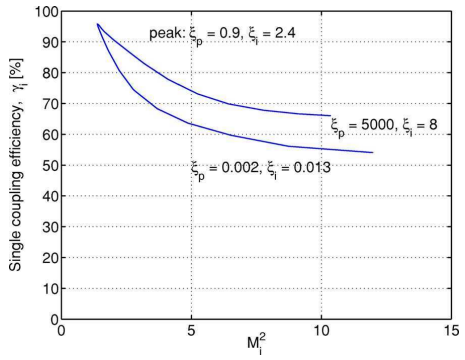

FIG. 13. (Color online) The single coupling γ_i versus the M^2 of the idler, using the same data as in Fig. 12 and Fig. 7. The graph is parametrized by the pump beam focusing and illustrate how a low M^2 is connected with a large γ_i.

timode, and too strong focusing will provide spatial longitudinal multimode. It can be deduced from Fig. 13 that longitudinal multimode, originating from too strong focusing, creates emission with relatively higher contribution to the fundamental mode for the same M^2 value.

IV. EXPERIMENTAL RESULTS

To verify some of the numerical results we compared with experiments. We have measured the beam quality factor, the bandwidth in the fiber, and the coupling efficiencies for different focusing conditions of the pump. The experimental setup is shown in Fig. 14. As a pump we use a frequency doubled YAG laser emitting approximately 60 mW in the TEM_{00} mode at 532 nm. Its M_p^2 value was measured to 1.06. After a band-pass filter (BP532), which removes any remaining infrared light, we "clean up" the polarization using a polarizing beam splitter (PBS). The polarization is controlled by a half wave plate (HWP) and a quarter wave plate (QWP) in front of the crystal. The pump-beam is focused onto the crystal using a achromatic doublet lens (f_p=50 mm) which introduces a minimal amount of aberrations not to destroy

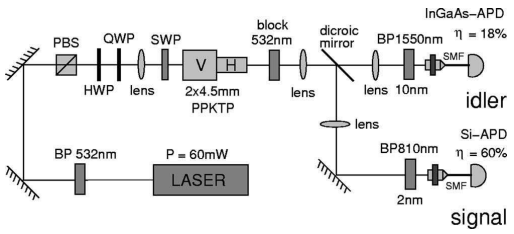

FIG. 14. The experimental setup used to create polarization entangled photon pairs, and to verify numerical results. PBS: polarizing beam splitter; HWP: half wave plate; QWP: quarter wave plate; SWP: short-pass filter; BP: band-pass filter; SMF: single-mode fiber; η: detection efficiency.

the low M^2 value. The QWP is set to undo any polarization elliptisation effects caused by the lens, and fluorescence caused by the same lens is removed by a Schott filter (KG5).

The next component is the crystal. This is a periodically poled, bulk 4.5 mm long KTP crystal, with a poling period of Λ=9.6 μm, which will colinearly create a signal at 810 nm and an idler at 1550 nm when heated in an oven to a temperature $T \approx 100°$. When the setup is used to create polarization entanglement, two crystals are present, one oriented for V and one for H, and the polarization of the pump is set to 45°. By coupling the emission from both crystals into single-mode fibers we cannot even in principle determine which crystal the photons came from, except by their polarization degree of freedom, and therefore the signal and idler will interfere in the diagonal basis and get entangled in polarization. This principle was first demonstrated by Kwiat *et al.* in Ref. [23]. Our first results was presented in Ref. [22], and the latest results, overcoming some problems of crystal dispersion and using optimal focusing, will be found in Ref. [34].

After the crystal, we block the pump light by a 532 nm band-stop filter, and the signal and idler emission is focused by achromatic doublet lenses. The rather small F-number ($F=f/D$, where f is the focal length and D is the beam diameter) of the emitted light ($F<40$ for f_p=50 mm and $F<9$ for f_p=12 mm) requires good quality lenses not to increase the M^2-factor. The lenses we use are all aberration free down to $F \approx 6-11$, and are also quite insensitive to an offset in the alignment of the optical axis.

To determine the coupling efficiencies and bandwidths, the complete setup of Fig. 14 was used. To separate the 810 nm and 1550 nm emission we used a dichroic mirror made for a 45° angle of incidence. The first lens (f_{si}=30 mm) is common to both signal and idler and its task is to refocus the beams somewhere near the dichroic mirror. The next two lenses (f_s=60 mm and f_i=40 mm) collimate each beam, and they are focused into the fiber-tips (with the mode field diameters being MFD_{810}=5.5 μm and MFD_{1550}=10.4 μm) using aspherical lenses with f=11 mm. In front of the fiber couplers we have first Schott filters (RG715) to block any remaining pump light, and then interference filters of 2 nm and 10 nm at the 810 nm and 1550 nm side respectively (BP). The detectors used were a Si-based APD (PerkinElmer SPCM-AQR-14) for 810 nm and a homemade $In_xGa_{1-x}As$-APD (Epitaxx) module for 1550 nm.

When determining the beam quality factor, M^2, we used only a single crystal oriented to create vertical (V) polarized light, and the complete setup of Fig. 14 was also not used. Instead, we focused the idler emission directly using a lens of focal length f_i=75 mm placed at a distance of 75 mm from the V-crystal to collimate the beam. At the additional distance of 470 mm we placed another lens with focal length f_i=150 mm that refocused the beam again, so that we could take measurements of the beam profile around its waist.

A. M^2 measurements, results

To obtain the results of Fig. 15 we first took images of the refocused idler beam in the x-y plane using an InGaAs-detector camera from Indigo Systems, model Alpha NIR.

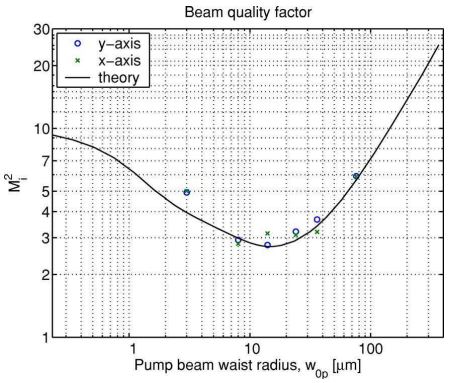

FIG. 15. (Color online) The experimentally observed beam quality factor, M_i^2, for the idler beam at different sizes of the pump beam waist radius w_{0p}. The lowest value of the M_i^2 is 2.8 at a 14 μm pump waist.

Several images were acquired for different positions along the z-axis around the waist, and we then integrated the resulting 2-dimensional surface over one axis to create an intensity profile for the remaining axis. Because of the detector noise we could not use the standard deviation method to find the beam radius, defined by the $1/e^2$ level. Instead we matched a Gaussian shaped function to the intensity profile to find the width. This is accurate enough for mode-shapes that are close to Gaussian, which is the case for low M^2 values. To limit the impact of the noise we applied a function that assigned greater weight to the center-values of the intensity profile. The widths of the beam for each z-axis position were then set together to find the beam profile of the emission, and its M^2 factor was determined by fitting to the standard Gaussian-beam function, Eq. (17). We now repeated the procedure for different focal lengths, f_p, of the pump lens: 12 mm, 30 mm, 50 mm, 75 mm, 100 mm, and 150 mm, each being placed at a distance that set the focus in the center of the crystal. The result, which is shown in Fig. 15, agrees fairly well with the numerical predictions. The shortest focal length lens, 12 mm, gave a somewhat higher M^2, which can be explained by the fact that this was the only singlet lens used, probably adding some aberrations, while the others where achromatic doublets. The lowest value, $M_i^2=2.8$, was found with the 50 mm lens giving a 14 μm pump waist radius w_{0p} inside the crystal, corresponding to $\xi_p=2$ for the 4.5 mm long V-crystal (for later reference we observe that $\xi_p=1.3$ for $L=3$ mm agrees a little bit better with numerical results). Note that the M^2 values are slightly higher here compared to Fig. 12. This can be explained by the nonperfect phase-matching in the experimental case, resulting from either too low crystal temperature, uncertainty in the true value of the poling period (possibly deviating somewhat from its specification), or both.

B. Coupling efficiencies, results

The experimental data for the coupling efficiencies were obtained with the source producing polarization-entanglement using two crystals. For this reason we expect the values to be a bit lower than predicted as we needed to focus the fiber-matched modes for both the H and the V crystal at the same time. We also have this problem with the pump beam, and we aimed at placing the focus at the intersecting faces of the two crystals for both the pump and the fiber. As already mentioned, the temperature of the crystal used in the experiment was set lower than required for absolute perfect phase matching at 810 nm and 1550 nm. This was because we observed higher photon fluxes at this setting. Contradictory as it may seem, the explanation is that the peak of the emission spectrum is not symmetrically centered around the above wavelengths, but rather towards $810-\alpha$ and $1550+\beta$, including a long tail representing the emission at larger angles. As our filters are centered for 810 nm and 1550 nm, the peaks of the emission can be moved to line up with these by changing the temperature, and thus the phase-matching, which will give somewhat higher fluxes although the coupling efficiencies will decrease according to our definitions. In addition to having a slightly wrong poling period these effects degrades the efficiencies, which we could verify numerically and which is supported by comparing Fig. 15 and Fig. 12. The obtained results for the single coupling efficiencies were $\gamma_s=32\%$ and $\gamma_i=79\%$, for the conditional coincidence $\mu_{i|s}=34\%$, and for the pair coupling $\gamma_c=11\%$, when focusing according to $\xi_p=2.1$, $\xi_s=3.2$, and $\xi_i=2.5$ (as decided by available lenses, and assuming $L=4.5$ mm). For these numbers we have compensated for the 35% transmission of the 1550 nm filter, and the 85% transmission of the 810 nm filter. The singles photon rate in the signal fiber was 2.3 Mcps (10^6 counts/sec) and in the idler fiber 2.4 Mcps. The total generated rate of photons before fiber coupling was estimated at 8.6 Mcps and the coincidence rate in the fibers was 274 kcps, (see Ref. [34]).

C. Bandwidth, results

We have used a spectrograph (SpectraPro 500i, ARC) to measure the bandwidth of the signal emission using the single-mode fiber without a filter. The bandwidth was 4 nm for the V-crystal and 6 nm for the H-crystal. Fig. 10 suggests that the effective length of the crystal being poled must be 3 mm and 2 mm respectively. Also, from Fig. 11, for the 2 nm filter, we can deduce that the 2 mm crystal should give roughly 55% of the photon rate of that of the 3 mm one. Experimental agreement is good, as we saw the H-crystal giving half the rate of the V-crystal (with no compensation done by balancing the fiber coupling or rotating the pump polarization). Referring again to Fig. 15 using the effective crystal length, the best pump beam focusing parameter is modified to $\xi_p=1.3$ for $L=3$ mm (V-crystal) which agrees roughly with the value of optimal focusing, $\xi_p=0.9$.

V. CONCLUDING DISCUSSION

In summary, precise focusing of the pump-beam and the fiber-matched modes can significantly increase the coupling and coincidence efficiencies of quasi-phase matched SPDC-sources, which is important for applications needing highly

correlated pairs of single photons to propagate in fibers. We have shown how the beam quality factor of the emission changes with the focusing of the pump. At optimal focusing the emission is mostly created in a spatial single-mode, which couples well into single-mode fibers, and by maintaining a fixed geometry of the beam profile in relation to different lengths of the crystal this stays true for all lengths. We have also shown how the photon flux depends on the crystal length for different frequency filters, the conclusion being that longer crystals produce more photons per unit time at a smaller bandwidth.

In all of the calculations we have assumed a monochromatic (CW) pump laser. Looking for a possible extension to pulsed operation we observe that the interaction time, T, in Eq. (A18) for a CW laser is set by the coherence time of the pump alone, and as T is infinite it transforms into a delta-function of frequency in Eq. (A20). Using pulsed light, the integral $\int_0^T \exp(-i\Delta\omega t)$ should be replaced by $\int_{-\infty}^{\infty} h(t)\exp(-i\Delta\omega t)$, where $h(t)$ is the convolution, $h(t)=h_C(t) \ \ h_L(t)$, between the form of the temporal wave-packet of the pump, $h_C(t)$, and the form of the crystal along the z-axis, $h_L(t)$. We observe that when $h_C(t)$ is narrow, like for pulsed operation, the transform of $h(t)$ will instead become a sinc-function, specifying an inexact energy-matching condition. Preliminary numerical calculations then show increased M^2-values and decreased coupling efficiencies. However, due to the characteristics of the convolution, it seems we can retain the good results of CW even for pulsed operation by using very long crystals, as this will bring back the delta-function at the limit of infinitely long crystals. For this discussion we have not yet worried about any dispersion effects that might come with long crystals and short pump pulses.

ACKNOWLEDGMENTS

We would like to thank G. Björk and A. Karlsson for their valuable comments and suggestions throughout the work, M. Pelton and P. Marsden for their initial work on the source, A. Fragemann, C. Canalias, and F. Laurell for providing us with crystals, and J. Waldebäck for his skills with electronics. This work was supported by the Swedish Foundation for Strategic Research (SSF) and by the European Commission through the integrated project SECOQC (Contract No. IST-2003-506813).

APPENDIX A: THE TWO-PHOTON FREQUENCY AND ANGULAR SPECTRAL AMPLITUDE

The evolution of the number state vector is given by

$$|\psi\rangle = \exp\left[-\frac{i}{\hbar}\int_{t_0}^{t_0+T} dt\hat{H}(t)\right]|\psi_{00}\rangle \approx \left(1+\frac{1}{i\hbar}\int_{t_0}^{t_0+T} dt\hat{H}(t)\right)|\psi_{00}\rangle, \tag{A1}$$

where $|\psi_{00}\rangle$ is the state at time t_0, T is the time of interaction, and $\hat{H}(t)$ is the Hamiltonian

$$\hat{H}(t) = \int_V \chi^{(2)}\hat{E}_{\mathrm{p}}^{(+)}\hat{E}_{\mathrm{s}}^{(-)}\hat{E}_{\mathrm{i}}^{(-)}d^3r + \mathrm{H.c.} \tag{A2}$$

There are three interacting fields in the crystal's volume V ignoring all higher-order terms ($n \geqslant 3$) of the nonlinearity $\chi^{(n)}$. All three fields have the same polarization (ZZZ):

$$E_{\mathrm{p}}^{(+)} = \sum_{\boldsymbol{s}_{\mathrm{p}}} A_{\mathrm{p}}(\boldsymbol{s}_{\mathrm{p}})e^{i(k_{\mathrm{p}}\boldsymbol{s}_{\mathrm{p}}\cdot\boldsymbol{r}-\omega_{\mathrm{p}}t+\phi_{\mathrm{p}})}, \tag{A3a}$$

$$\hat{E}_{\mathrm{s}}^{(-)} = \int d\phi_{\mathrm{s}}\int d\omega_{\mathrm{s}}A(\omega_{\mathrm{s}})\sum_{\boldsymbol{s}_{\mathrm{s}}} e^{-i(k_{\mathrm{s}}\boldsymbol{s}_{\mathrm{s}}\cdot\boldsymbol{r}-\omega_{\mathrm{s}}t+\phi_{\mathrm{s}})}\hat{a}_{\mathrm{s}}^{\dagger}(\omega_{\mathrm{s}},\boldsymbol{s}_{\mathrm{s}}), \tag{A3b}$$

$$\hat{E}_{\mathrm{i}}^{(-)} = \int d\phi_{\mathrm{i}}\int d\omega_{\mathrm{i}}A(\omega_{\mathrm{i}})\sum_{\boldsymbol{s}_{\mathrm{i}}} e^{-i(k_{\mathrm{i}}\boldsymbol{s}_{\mathrm{i}}\cdot\boldsymbol{r}-\omega_{\mathrm{i}}t+\phi_{\mathrm{i}})}\hat{a}_{\mathrm{i}}^{\dagger}(\omega_{\mathrm{i}},\boldsymbol{s}_{\mathrm{i}}). \tag{A3c}$$

The field of the pump is classical and monochromatic so that we can replace $\hat{E}_{\mathrm{p}}^{(+)}$ by $E_{\mathrm{p}}^{(+)}$. The plus-sign denotes conjugation, i.e., annihilation $(+)$ or creation $(-)$ of the state. In all the calculations we use the notation $\boldsymbol{k}=k\boldsymbol{s}$, where $\boldsymbol{s}$ is the unit length vector of $\boldsymbol{k}$. The angular amplitude spectrum $A_{\mathrm{p}}(\boldsymbol{s}_{\mathrm{p}})$ takes into account the focusing of the pump. For signal and idler, we sum over both frequency and angular modes, where $\hat{a}(\omega,\boldsymbol{s})$ is the field operator, and $A(\omega)$ is the frequency amplitude of a Gaussian shaped detector filter having the bandwidth $\Delta\lambda$ (FWHM) and center wavelength λ_c (all wavelengths in vacuum). Via the relation $\omega=2\pi cn_{\lambda}/\lambda$ its form is given by

$$A(\omega;\lambda) = e^{-2\,\log(2)(\lambda-\lambda_c)^2/\Delta\lambda^2}. \tag{A4}$$

Each signal and idler photon is created with a random phase, ϕ_{s} and ϕ_{i} respectively, which we also need to sum over. The only nonzero solution is completely correlated phases as will be shown later. The phase of the pump ϕ_{p} is constant but arbitrary.

For periodically poled materials, the nonlinearity $\chi^{(2)}$ has sharp boundaries, and later on in the calculations it will facilitate to make an expansion of $\chi^{(2)}$ into its Fourier-series components

$$\chi^{(2)} = \chi_2 f(\boldsymbol{r}) = \chi_2\sum_{m=0}^{\infty} f_m e^{-im\boldsymbol{K}\cdot\boldsymbol{r}}, \tag{A5}$$

and then do a sinusoidal approximation using the first term,

$$\chi^{(2)} = \chi_2 f_1 e^{-i\boldsymbol{K}\cdot\boldsymbol{r}}, \tag{A6}$$

where $\boldsymbol{K}=2\pi/\Lambda\boldsymbol{e}_z$, and Λ is the grating period. Appendix B treats the case of a $M+1$ term series expansion.

From Eq. (A1) the number state becomes

$$|\psi\rangle = |\psi_{00}\rangle + \int\int d\omega_s d\omega_i \sum_{\boldsymbol{s}_s}\sum_{\boldsymbol{s}_i} S(\omega_s,\omega_i,\boldsymbol{s}_s,\boldsymbol{s}_i)\hat{a}_s^\dagger \hat{a}_i^\dagger |\psi_{00}\rangle$$
$$= |\psi_{00}\rangle + G_2|\psi_{11}\rangle, \tag{A7}$$

where G_2 is the unnormalized amplitude for the two-photon number state,

$$G_2 = \langle\psi_{11}|\psi\rangle = \int\int d\omega_s d\omega_i \sum_{\boldsymbol{s}_s}\sum_{\boldsymbol{s}_i} S(\omega_s,\omega_i,\boldsymbol{s}_s,\boldsymbol{s}_i), \tag{A8}$$

such that for $t_0=0$,

$$\frac{1}{i\hbar}\int_0^T dt\, \hat{H}(t) = G_2\hat{a}_s^\dagger\hat{a}_i^\dagger - \text{H.c.} \tag{A9}$$

Our goal now is to arrive at an expression for the amplitude S which will also enter in the state of frequency and angular spectrum of the form

$$|\psi_{\omega,\boldsymbol{s}}\rangle = \int\int d\omega_s d\omega_i \sum_{\boldsymbol{s}_s}\sum_{\boldsymbol{s}_i} S(\omega_s,\omega_i,\boldsymbol{s}_s,\boldsymbol{s}_i)|\omega_s\rangle|\omega_i\rangle|\boldsymbol{s}_s\rangle|\boldsymbol{s}_i\rangle. \tag{A10}$$

We start by inserting Eq. (A6) into Eq. (A2) and then Eq. (A2) into Eq. (A9) which gives

$$G_2 = \frac{1}{i\hbar}\int_0^T dt \int_V d^3r\, \chi_2 f_1 e^{-i\boldsymbol{K}\cdot\boldsymbol{r}} E_p^{(+)} E_s^{(-)} E_i^{(-)}. \tag{A11}$$

By making a substitution of the fields in Eq. (A3) into Eq. (A11), and via identification using Eq. (A8) we find that

$$S(\omega_s,\omega_i,\boldsymbol{s}_s,\boldsymbol{s}_i) = \chi_2 f_1 A(\omega_s)A(\omega_i)\sum_{\boldsymbol{s}_p} A_p(\boldsymbol{s}_p)$$
$$\times \int_{-L/2}^{L/2} dz \int_{-\infty}^{\infty} dy \int_{-\infty}^{\infty} dx\, e^{-i\Delta\boldsymbol{k}\cdot(x\boldsymbol{e}_x+y\boldsymbol{e}_y+z\boldsymbol{e}_z)}$$
$$\times \frac{1}{i\hbar}\int_0^{2\pi}\int_0^{2\pi} d\phi_s d\phi_i \int_0^T dt$$
$$\times e^{-i[(\omega_s+\omega_i-\omega_p)t+\phi_s+\phi_i-\phi_p]}, \tag{A12}$$

where the volume integral has been expressed in a Cartesian coordinate system ($\boldsymbol{r}=x\boldsymbol{e}_x+y\boldsymbol{e}_y+z\boldsymbol{e}_z$, see Fig. 1),

$$\int_V d^3r = \int_{-L/2}^{L/2} dz \int_{-\infty}^{\infty} dy \int_{-\infty}^{\infty} dx. \tag{A13}$$

We have also introduced the phase mismatching vector

$$\Delta\boldsymbol{k} = k_s\boldsymbol{s}_s + k_i\boldsymbol{s}_i - k_p\boldsymbol{s}_p + \boldsymbol{K} \tag{A14a}$$

$$= \Delta k_x\boldsymbol{e}_x + \Delta k_y\boldsymbol{e}_y + \Delta k_z\boldsymbol{e}_z. \tag{A14b}$$

In a Cartesian coordinate system the normalized vectors $\boldsymbol{s}$ are represented by

$$\begin{aligned}\boldsymbol{s}_s &= p_s\boldsymbol{e}_x + q_s\boldsymbol{e}_y + m_s\boldsymbol{e}_z,\\ \boldsymbol{s}_i &= p_i\boldsymbol{e}_x + q_i\boldsymbol{e}_y + m_i\boldsymbol{e}_z,\\ \boldsymbol{s}_p &= p_p\boldsymbol{e}_x + q_p\boldsymbol{e}_y + m_p\boldsymbol{e}_z,\\ \boldsymbol{K} &= K\boldsymbol{e}_z,\end{aligned} \tag{A15}$$

where p, q, and m are the normalized components of $\boldsymbol{s}$ in each of the three dimensions [30].

Because of the rotational symmetry of the emitted modes, it is suitable to use a spherical coordinate system (θ,φ), for which $p=\sin\theta\cos\varphi$, $q=\sin\theta\sin\varphi$, and $m=\cos\theta$. The phase-mismatch vector components then become

$$\Delta k_x = k_s\sin\theta_s\cos\varphi_s + k_i\sin\theta_i\cos\varphi_i - k_p\sin\theta_p\cos\varphi_p,$$
$$\Delta k_y = k_s\sin\theta_s\sin\varphi_s + k_i\sin\theta_i\sin\varphi_i - k_p\sin\theta_p\sin\varphi_p,$$
$$\Delta k_z = k_s\cos\theta_s + k_i\cos\theta_i - k_p\cos\theta_p + K. \tag{A16}$$

Note that the magnitude of the signal and idler k-vectors implicitly depends on the polar angle θ according to

$$k_s(\theta_s) = 1/\sqrt{\left(\frac{\cos\theta_s}{k_s^Z}\right)^2 + \left(\frac{\sin\theta_s}{k_s^Y}\right)^2}, \tag{A17a}$$

$$k_i(\theta_i) = 1/\sqrt{\left(\frac{\cos\theta_i}{k_i^Z}\right)^2 + \left(\frac{\sin\theta_i}{k_i^Y}\right)^2}, \tag{A17b}$$

where k_s^Z, k_s^Y, k_i^Z, and k_i^Y are the constant magnitude of the k-vectors along the crystals Z- and Y-axis, respectively (k_p need to be constant and equal to k_p^Z as we will soon show). Generally, there is negligible difference in refractive indices between the crystal's X and Y axes which cancels the dependence on the azimuthal angle φ in the equations above. We therefore use the Y axis as the major axis being orthogonal to Z.

Using spherical coordinates exclusively leads to

$$S(\omega_s,\omega_i,\theta_s,\theta_i,\varphi_s,\varphi_i)$$
$$= \chi_2 f_1 A(\omega_s)A(\omega_i)\int_0^{\pi/2}\sin\theta_p d\theta_p \int_0^{2\pi} d\varphi_p A_p(\theta_p,\varphi_p)$$
$$\times \int_{-L/2}^{L/2} dz \int_{-\infty}^{\infty} dy \int_{-\infty}^{\infty} dx\, e^{-i[\Delta k_x x+\Delta k_y y+\Delta k_z z]}$$
$$\times \frac{1}{i\hbar}\int_0^{2\pi}\int_0^{2\pi} d\phi_s d\phi_i \int_0^T dt\, e^{-i[(\omega_s+\omega_i-\omega_p)t+\phi_s+\phi_i-\phi_p]}. \tag{A18}$$

The angular spectral amplitude A_p of the pump beam in Eq. (A18) is Gaussian shaped for a laser emitting in a TEM_{00} single mode, and in spherical coordinates it becomes [30]

$$A_p(\theta_p,\varphi_p) = \frac{k_p w_{0p}}{\sqrt{2\pi}} e^{-(k_p w_{0p})^2\sin^2\theta_p/4}, \tag{A19}$$

where the beam waist radius w_{0p} of the focused pump beam has entered the calculations. The function is normalized to

represent the same constant power available in the beam at different focusing conditions.

Now we will solve the integrals over space, time, and phase in Eq. (A18). In doing so we note that there are three spatial integrals of which two are the Fourier transforms of unity (dx and dy) and one is the transform of a box-function (dz). The transforms turn into two δ-functions and a sinc-function respectively. The time-integral also turns into a δ-function of the three frequencies ω_s, ω_i, and ω_p. This is because we have a monochromatic pump-beam with infinite coherence length, which effectively leads to an infinite interaction-time, $T\to\infty$, even for short crystals. The two integrals over the random phases ϕ_s and ϕ_i will make the amplitude S vanish completely if the phases are not fully correlated with each other. Therefore, the only non-zero solution is when the two phases add up to a constant. S can be complex-valued, thus yielding the relation $\phi_s+\phi_i=\phi_p+C$. If we let $C=0$ for simplicity, we are led to

$$S(\omega_s,\omega_i,\theta_s,\theta_i,\varphi_s,\varphi_i) = \chi_2 f_1 A(\omega_s)A(\omega_i)\int_0^{\pi/2}\sin\theta_p d\theta_p\int_0^{2\pi} d\varphi_p A_p(\theta_p,\varphi_p) \times \delta(\Delta k_x)\delta(\Delta k_y) L\,\mathrm{sinc}\left[\frac{L}{2}\Delta k_z\right]\frac{4\pi^2}{i\hbar}\delta(\omega_s+\omega_i-\omega_p). \tag{A20}$$

We now have two integrals over θ_p and φ_p with δ-functions over Δk_x and Δk_y which in turn depends on θ_p and φ_p according to Eq. (A16). The integrals can be canceled in a few steps by setting the equalities $\Delta k_x=0$ and $\Delta k_y=0$, and to that end we need to assume that k_p is constant for small angles θ_p, i.e., $k_p=k_p^Z$ which we believe is a fair approximation for pump-light that is not extremely focused. By extreme we mean beyond the validity of the paraxial approximation. The latter equality applied to Eq. (A16) gives

$$\varphi_p' = \arcsin\left(\frac{k_s\sin\theta_s\sin\varphi_s + k_i\sin\theta_i\sin\varphi_i}{k_p^Z\sin\theta_p'}\right). \tag{A21}$$

Equation (A21) together with the relation $\arcsin(x)=\arccos(\sqrt{1-x^2})$ now gives the following expression for $\Delta k_x=0$ of Eq. (A16) (with φ_p primed),

$$k_s\sin\theta_s\cos\varphi_s + k_i\sin\theta_i\cos\varphi_i - k_p^Z\sin\theta_p'\sqrt{1-\left(\frac{k_s\sin\theta_s\sin\varphi_s + k_i\sin\theta_i\sin\varphi_i}{k_p^Z\sin\theta_p'}\right)^2} = 0. \tag{A22}$$

If we now take the square of Eq. (A22) and solve for θ_p' we get

$$\theta_p' = \arcsin\sqrt{P^2+Q^2} = \arccos\sqrt{1-(P^2+Q^2)}, \tag{A23}$$

where

$$P = \frac{k_s\sin\theta_s\sin\varphi_s + k_i\sin\theta_i\sin\varphi_i}{k_p^Z}, \tag{A24a}$$

$$Q = \frac{k_s\sin\theta_s\cos\varphi_s + k_i\sin\theta_i\cos\varphi_i}{k_p^Z}. \tag{A24b}$$

Furthermore,

$$P^2+Q^2 = \frac{k_s^2\sin^2\theta_s + k_i^2\sin^2\theta_i + 2k_sk_i\sin\theta_s\sin\theta_i\cos(\Delta\varphi)}{(k_p^Z)^2}, \tag{A25}$$

where we are allowed to introduce $\Delta\varphi=\varphi_s-\varphi_i$. This is a result of the assumption of rotational symmetry and will lead to the final state being invariant to a common variation in the azimuthal angles for signal, φ_s, and idler, φ_i. As shown here, only the angle-difference is of importance. Using Eq. (A23) in the expression for Δk_z of Eq. (A16) we have

$$\Delta k_z' = k_s\cos\theta_s + k_i\cos\theta_i - k_p^Z\sqrt{1-(P^2+Q^2)} + K. \tag{A26}$$

At this stage the two integrals in Eq. (A20) have been canceled and the amplitude can be simplified as

$$S(\omega_s,\omega_i,\theta_s,\theta_i,\Delta\varphi) = \chi_2 f_1 A(\omega_s)A(\omega_i)A_p(\theta_p',\varphi_p') \times L\,\mathrm{sinc}\left[\frac{L}{2}\Delta k_z'\right]\frac{4\pi^2}{i\hbar}\delta(\omega_s+\omega_i-\omega_p). \tag{A27}$$

One further simplification includes the observation that the frequency δ-function can be reduced to unity by introducing a common frequency ϵ instead of ω_s and ω_i as defined by $\omega_s=\omega_{0s}+\epsilon$, $\omega_i=\omega_{0i}-\epsilon$, so that for two matched filters the form of the filter amplitude becomes squared. Using also Eq. (A23) together with Eq. (A19) the expression for the amplitude of the state of frequency and angular spectrum finally becomes

$$S(\epsilon,\theta_s,\theta_i,\Delta\varphi) = \frac{4\pi^2\chi_2 f_1 L}{i\hbar}A^2(\epsilon)\frac{k_p^Z w_{0p}}{\sqrt{2\pi}}e^{-(k_p^Z w_{0p})^2[P^2+Q^2]/4} \times \mathrm{sinc}\left[\frac{L}{2}(k_s\cos\theta_s + k_i\cos\theta_i - k_p^Z\sqrt{1-(P^2+Q^2)} + K)\right], \tag{A28}$$

where P^2+Q^2 is defined by Eq. (A25) and the k_s's and k_i's by Eq. (A17).

We now have a final expression for the two-photon amplitude

$$G_2 = \int d\epsilon\int\int\sin\theta_s d\theta_s\sin\theta_i d\theta_i\int d\Delta\varphi S(\epsilon,\theta_s,\theta_i,\Delta\varphi), \tag{A29}$$

which gives the two-photon state-vector in terms of frequency and angular spectrum in the form of Eq. (A10)

$$|\psi_{\epsilon,\theta,\Delta\varphi}\rangle = G_2|\epsilon\rangle|\theta_s\rangle|\theta_i\rangle|\Delta\varphi\rangle. \tag{A30}$$

APPENDIX B: SERIES EXPANSION OF $\chi^{(2)}$

The poling structure of periodically poled crystal has the approximate form of a square-function along the z-axis. In such a case, the $M+1$ term series expansion of $\chi^{(2)}$ become

$$\chi^{(2)} = \chi_2 f(\boldsymbol{r}) = \frac{4\chi_2}{\pi} \sum_{m=0}^{M} \frac{(-1)^m}{2m+1} e^{-i(2m+1)\boldsymbol{K}\cdot\boldsymbol{r}}, \tag{B1}$$

where $\boldsymbol{K}=2\pi/\Lambda \boldsymbol{e}_z$, and Λ is the grating period. In the following expression we have isolated the z-dependent part of Eq. (A18):

$$\chi_2 f_1 \int_{-L/2}^{L/2} dz\, e^{-i\Delta k_z z}. \tag{B2}$$

Now, putting the series expansion of $\chi^{(2)}$ into the calculations of Appendix A, the former expression should be replaced by

$$\frac{4\chi_2}{\pi} \int_{-L/2}^{L/2} dz \sum_{m=0}^{M} \frac{(-1)^m}{2m+1} e^{-i\Delta k_z^{(m)} z}, \tag{B3}$$

where

$$\Delta k_z^{(m)} = \Delta k_z' + 2mK. \tag{B4}$$

By reversing the order of the sum and the integral in Eq. (B3) we can identify a Fourier transform of box-function with an extra phase. The result of the transform is a sinc, providing thus

$$\frac{4\chi_2}{\pi} \sum_{m=0}^{M} \frac{(-1)^m}{2m+1} \mathrm{sinc}\left[\frac{L}{2}(\Delta k_z' + 2mK)\right], \tag{B5}$$

which is the final expression to replace the sinc-function in the state amplitude, Eq. (A28), having now $M+1$ terms to approximate the square-shaped poling structure. For $M=0$ the expression reduces to the sinusoidal approximation with $f_1=4/\pi$.

[1] S. Fasel, O. Alibart, S. Tanzilli, P. Baldi, A. Beveratos, N. Gisin, and H. Zbinden, New J. Phys. **6**, 163 (2004).
[2] T. B. Pittman, B. C. Jacobs, and J. D. Franson, Opt. Commun. **246**, 545 (2004).
[3] O. Alibart, D. B. Ostrowsky, and P. Baldi, Opt. Lett. **30**, 1539 (2005).
[4] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **84**, 4729 (2000).
[5] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, Phys. Rev. Lett. **84**, 4733 (2000).
[6] G. Ribordy, J. Brendel, J.-D. Gauthier, N. Gisin, and H. Zbinden, Phys. Rev. A **63**, 012309 (2000).
[7] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, and N. Gisin, Nature (London) **421**, 509 (2003).
[8] S. Tanzilli, W. Tittel, H. D. Riedmatten, H. Zbinden, P. Baldi, M. D. Micheli, D. Ostrowsky, and N. Gisin, Eur. Phys. J. D **18**, 155 (2002).
[9] W. Tittel, J. Brendel, N. Gisin, and H. Zbinden, Phys. Rev. A **59**, 4150 (1999).
[10] S. Fasel, N. Gisin, G. Ribordy, and H. Zbinden, Eur. Phys. J. D **30**, 143 (2004).
[11] G. D. Boyd and D. A. Kleinman, J. Appl. Phys. **39**, 3597 (1968).
[12] D. A. Kleinman and R. C. Miller, Phys. Rev. **148**, 302 (1966).
[13] S. Guha, F. Wu, and J. Falk, IEEE J. Quantum Electron. **18**, 907 (1982).
[14] J.-J. Zondy, Opt. Commun. **81**, 427 (1991).
[15] J.-J. Zondy, Opt. Commun. **149**, 181 (1998).
[16] C. H. Monken, P. H. Souto Ribeiro, and S. Pádua, Phys. Rev. A **57**, R2267 (1998).
[17] T. B. Pittman, D. V. Strekalov, D. N. Klyshko, M. H. Rubin, A. V. Sergienko, and Y. H. Shih, Phys. Rev. A **53**, 2804 (1996).
[18] T. Aichele, A. I. Lvovsky, and S. Schiller, Eur. Phys. J. D **18**, 237 (2002).
[19] C. Kurtsiefer, M. Oberparleiter, and H. Weinfurter, Phys. Rev. A **64**, 023802 (2001).
[20] F. A. Bovino, P. Varisco, A. M. Colla, G. Castagnoli, G. D. Giuseppe, and A. V. Sergienko, Opt. Commun. **227**, 343 (2003).
[21] S. Castelletto, I. P. Degiovanni, A. Migdall, and M. Ware, New J. Phys. **6**, 87 (2004).
[22] M. Pelton, P. Marsden, D. Ljunggren, M. Tengner, A. Karlsson, A. Fragemann, C. Canalias, and F. Laurell, Opt. Express **12**, 3573 (2004).
[23] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, Phys. Rev. A **60**, R773 (1999).
[24] D. Ljunggren, M. Tengner, M. Pelton, and P. Marsden, in *Quantum Communication, Measurement and Computing*, edited by S. M. Barnett *et al.*, AIP Conf. Proc. No. 734 (AIP, Melville, NY, 2004).
[25] C. E. Kuklewicz, M. Fiorentino, G. Messin, F. N. C. Wong, and J. H. Shapiro, Phys. Rev. A **69**, 013807 (2004).
[26] M. Fiorentino, G. Messin, C. E. Kuklewicz, F. N. C. Wong, and J. Shapiro, Phys. Rev. A **69**, 041801 (2004).
[27] T. Y. Fan, C. E. Huang, B. Q. Hu, R. C. Eckardt, Y. X. Fan, R. L. Byer, and R. S. Feigelson, Appl. Opt. **26**, 2390 (1987).
[28] K. Fradkin, A. Arie, A. Skliar, and G. Rosenman, Appl. Phys. Lett. **74**, 914 (1999).
[29] D. N. Klyshko, *Photons and Nonlinear Optics* (Gordon and Breach, New York, 1988).
[30] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics* (Cambridge University Press, Cambridge, UK, 1995).
[31] A. E. Siegman, IEEE J. Quantum Electron. **29**, 1212 (1993).
[32] A. E. Siegman, *Lasers* (University Science Books, Sausalito, 1986).
[33] P. S. K. Lee, M. P. van Exter, and J. P. Woerdman, Phys. Rev. A **70**, 043818 (2004).
[34] D. Ljunggren, M. Tengner, P. Marsden, and M. Pelton (to be published).

Paper D

Bright, single-spatial-mode source of frequency non-degenerate, polarization-entangled photon pairs using periodically poled KTP

M. Pelton, P. Marsden, D. Ljunggren, M. Tengner, A. Karlsson, A. Fragemann, C. Canalias, and F. Laurell

Opt. Express. **12**, 3573 (2004)

Contributions by the author: The candidate collected the final data after a major rebuild of the source together with P. Marsden and M. Tengner. The first author proposed the source and built the first version of the experimental setup. M. Pelton also wrote the paper, with contributions of preliminary results of **Paper C** made available by the candidate. The last three authors supplied the crystals.

Bright, single-spatial-mode source of frequency non-degenerate, polarization-entangled photon pairs using periodically poled KTP

Matthew Pelton, Philip Marsden, Daniel Ljunggren, Maria Tengner, Anders Karlsson

Department of Microelectronics and Information Technology, Royal Institute of Technology, Electrum 229, SE-164 40, Kista, Sweden

pelton@uchicago.edu

Anna Fragemann, Carlota Canalias, Fredrik Laurell

Department of Physics, Royal Institute of Technology, Roslagstullsbacken 22, SE-106 91, Stockholm, Sweden

Abstract: We use two perpendicular crystals of periodically-poled KTP to directly generate polarization-entangled photon pairs, the majority of which are emitted into a single Gaussian spatial mode. The signal and idler photons have wavelengths of 810 nm and 1550 nm, respectively, and the photon-pair generation rate is 1.2×10^7 sec^{-1} for a pump power of 62 mW. The apparatus is compact, flexible, and easily to use.

OCIS codes: (270.0270) Quantum optics; (270.4180) Multiphoton processes.

References and links

1. P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, "New high-intensity source of polarization-entangled photon pairs," Phys. Rev. Lett. **75**, 4337 – 4341 (1995).
2. P. G. Kwiat, E. Waks, A. G. White, I. Appelbaim, and P. H. Eberhard, "Ultrabright source of polarization-entangled photons," Phys. Rev. A **60**, R773 – 776 (1999).
3. S. Tanzilli, H. De Riedmatten, W. Tittel, H. Zbinden, P. Baldi, M. De Micheli, D. B. Ostrowski, and N. Gisin, "Highly efficient photon-pair source using periodically poled lithium niobate waveguide," Electron. Lett. **37**, 26 – 28 (2001).
4. K. Banaszek, A. B. U'Ren, and I. A. Walmsley, "Generation of correlated photons in controlled spatial modes by downconversion in nonlinear waveguides," Opt. Lett. **26**, 1367 – 1369 (2001).
5. C. E. Kuklewicz, M. Fiorentino, G. Messin, F. N. C. Wong, and J. H. Shapiro, "High-flux source of polarization-entangled photons from a periodically-poled $KTiOPO_4$ parametric down-converter," Phys. Rev. A **69**, 013807 (2004).
6. M. Fiorentino, G. Messin, C. E. Kuklewicz, F. N. C. Wong, and J. H. Shapiro, "Generation of ultrabright tunable polarization entanglement without spatial, spectral, or temporal constraints," Phys. Rev. A **69**, 041801 (2004).
7. G. Ribordy, J. Brendel, J.-D. Gautier, N. Gisin, and H. Zbinden, "Long-distance entanglement-based quantum key distribution," Phys. Rev. A. **63**, 012309 (2001).
8. E. J. Mason, M. A. Albota, F. König, and F. N. C. Wong, "Efficient generation of tunable photon pairs at 0.8 and 1.6 μm," Opt. Lett. **27**, 2115 – 2117 (2002).
9. Q. Chen and W. P. Risk, "Periodic poling of $KTiOPO_4$ using an applied electric field," Electron. Lett. **30**, 1516 – 1517 (1994).
10. H. Karlsson, F. Laurell, P. Henriksson, and G. Arvidsson, "Frequency doubling in periodically poled $RbTiOAsO_4$," Electron. Lett. **32**, 556 – 557 (1996).
11. H. Karlsson, F. Laurell, and L. K. Cheng, "Periodic poling of $RbTiOPO_4$ for quasi-phase matched blue light generation," Appl. Phys. Lett. **74**, 1519 (1999).

#4344 - $15.00 US Received 14 April 2004; revised 19 July 2004; accepted 21 July 2004

12. T.Y. Fan, C. E. Huang, B. Q. Hu, R. C. Eckardt, Y. X. Fan, R. L. Byer, and R. S. Feigelson, "Second harmonic generation and accurate index of refraction measurements in flux-grown $KTiOPO_4$," Appl. Opt. **26**, 2390 (1987).
13. K. Fradkin, A. Arie, A. Skliar, and G. Rosenman, "Tunable midinfrared source by difference frequency generation in bulk periodically poled $KTiOPO_4$," Appl. Phys. Lett. **74**, 914 – 916 (1999).
14. M. W. Sasnett, "Propagation of multimode laser beams: The M^2 factor," in *The Physics and Technology of Laser Resonators,* D. R. Hall and P. E. Jackson. eds. (New York: Adam Hilger, 1989), pp. 132 - 142.
15. D. Ljunggren, M. Tengner, P. Marsden, M. Pelton, and A. Karlsson, Department of Microelectronics and Information Technology, Royal Institute of Technology, Electrum 229, SE-164 40, Kista, Sweden, are preparing a manuscript to be called "Theory and experiment of entanglement in a quasi-phasematched two-crystal source."
16. M. Bourennane, A. Karlsson, J. Peña Císcar, and M. Mathes, "Single photon counters in the telecom wavelength region of 1550 nm for quantum information processing," J. Mod. Opt. **48**, 1983 – 1995 (2001).
17. C. Kurtseifer, M. Oberparleiter, and H. Weinfurter, "High-efficiency entangled photon pair collection in type-II parametric fluorscence," Phys. Rev. A **64**, 023802 (2001).
18. J. Volz, C. Kurtseifer, and H. Weinfurter, "Compact all-solid-state source of polarization-entangled photon pairs," Appl. Phys. Lett. **79**, 869 – 871 (2001).
19. D. Ljunggren and M. Tengner, Department of Microelectronics and Information Technology, Royal Institute of Technology, Electrum 229, SE-164 40, Kista, Sweden, are preparing a manuscript to be called "Entangled photon paris from two quasi-phasematched crystlas: Optimizing the emission for efficient fiber coupling."
20. A. G. White, D. F. V. James, W. J. Munro, and P. G. Kwiat, "Exploring Hilbert space: Accurate characterization of quantum information," Phys. Rev. A **65**, 012301 (2002).

Polarization-entangled photon pairs have been central to recent experiments in quantum information, including investigations of quantum cryptography, quantum teleportation, and preliminary results in linear-optical quantum computation. Perhaps the best-known scheme for generating such photon pairs involves spontaneous parametric downconversion with type-II birefringent phase matching, in which a pair of orthogonally-polarized photons are emitted into two intersecting cones [1]. However, in this case, only a small fraction of the generated photon pairs are entangled. On the other hand, all of the frequency-degenerate pairs are entangled in a scheme involving type-I phasematching in two separate crystals, allowing for significant improvement in the generation efficiency [2]. In this case, the optic axis of the first crystal is oriented horizontally, the optic axis of the second crystal is oriented vertically, and the pump is polarized at 45° with respect to each of the axes. There is thus an equal probability that two vertically polarized (V) photons will be generated in the first crystal or that two horizontally polarized (H) photons will be generated in the second crystal. These two possibilities are made indistinguishable by using thin crystals, so that the generated photons emerge in two overlapping cones. The conical emission is inconvenient, though, for coupling the emitted photons into optical fibers, while the need to use thin crystals limits the pair generation rate.

We have therefore developed a two-crystal source of entangled photons which uses quasi-phasematched (QPM) materials. QPM materials have previously been used for efficient generation of photon pairs without polarization entanglement [3, 4], and for probabilistic generation of polarization-entangled photon pairs by postselection [5]. In our scheme, by contrast, polarization-entangled photons are generated directly. Compared to schemes that involve pumping a single QPM crystal from opposite sides [6], the two-crystal scheme has the advantage of not requiring a stabilized interferometer.

The poling period of our crystals is chosen to allow for co-polarized (ZZZ), colinear downconversion. The colinear configuration means that the output modes of the photons created in the first and second crystals have nearly complete spatial overlap, regardless of crystal length. In other words, it is possible to use long crystals, thereby increasing the pair generation rate, without reducing the degree of entanglement. As well, the signal and idler beams have a large overlap with a simple Gaussian (TEM_{00}) mode, allowing for efficient coupling of the generated photons into single-mode optical fibers. Finally, since the entanglement is generated directly in the downconversion process, it is not necessary that the signal and idler be frequency degenerate. We have thus chosen the idler to have a wavelength of 1550 nm, corresponding to the

#4344 - $15.00 US Received 14 April 2004; revised 19 July 2004; accepted 21 July 2004

transmission-loss minimum in optical fibers, while choosing the signal to have a wavelength of 810 nm, allowing for efficient, low-noise photon counting using Si-based detectors [7]. Very nearly the same wavelength pair is also of interest for quantum teleportation systems in which the signal photon is used to load a Rb-based quantum memory [8].

Our nonlinear crystals are flux-grown, periodically poled potassium titanyl phosphate (PPKTP) [9, 10]. Each crystal is 5 mm long (in the X direction) and 0.5 mm high (in the Z direction). A photoresist grating with a 9.6 μm period is patterned on the top side of the unpoled crystal, and poling is achieved by applying voltage pulses across the crystal using liquid electrodes. The poling is monitored *via* the electro-optic effect, by observing polarization changes of a He-Ne laser beam passing through the sample in the X direction [11].

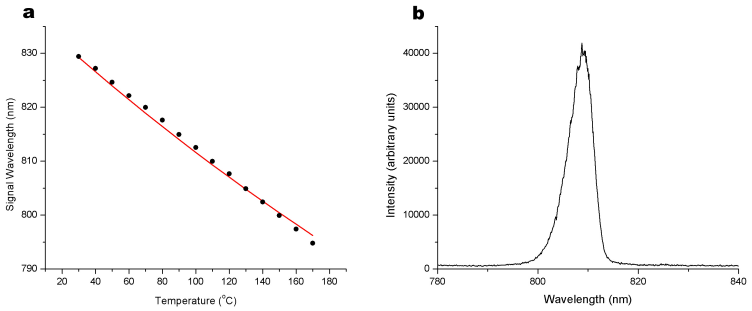

Fig. 1. (a) Wavelength of the signal photons, as a function of sample temperature. The points show the experimentally-measured values, while the solid line is the theoretical prediction. (b) Spectrum of the signal photons at a sample temperature of 109.3°C.

Since downconversion occurs with high efficiency in the PPKTP crystals, only a moderate pump power is needed. This is provided by a compact, diode-pumped, frequency-doubled Nd:YAG laser, which has a continuous-wave output at a wavelength of 532 nm. This source is small compared to the large-frame lasers generally used for downconversion (only $120 \times 50 \times 36$ mm), allowing the entire pair-generation system to be compact and inexpensive. Stray light is reduced by sending the pump beam through a bandpass (BP) filter. The two PPKTP crystals are mounted orthogonally on a temperature-controlled brass block.

Figure 1(a) shows the measured signal wavelength as a function of sample temperature. Also shown are the predicted wavelengths, calculated using published Sellmeier coefficients [12, 13]. Good agreement between theory and experiment is seen. The results show that a temperature of 109.3°C will give a signal wavelength of 810 nm, corresponding to an idler wavelength of 1550 nm. Figure 1(b) shows the signal spectrum at this temperature; it can be seen that the signal has a bandwidth of only 5 nm.

The idler beam was sent through a lens, and its profile was measured at various distances from the crystal using an InGaAs detector array. A sample profile is shown in Fig. 2(a); it can be seen that the profile has the symmetric, circular shape characteristic of a fundamental TEM_{00} mode. In order to make a more quantitative analysis, the measured profiles were integrated in the horizontal and vertical directions, and the integrated profiles were fitted to Gaussians in order to obtain beam diameters, shown in Fig. 2(b). The results were fitted to the standard formula for nearly Gaussian beam propagation [14], giving M^2 parameters of 2.4 ± 0.3 and 2.0 ± 0.2 in the horizontal and vertical directions, respectively. This indicates that the majority

#4344 - $15.00 US
Received 14 April 2004; revised 19 July 2004; accepted 21 July 2004

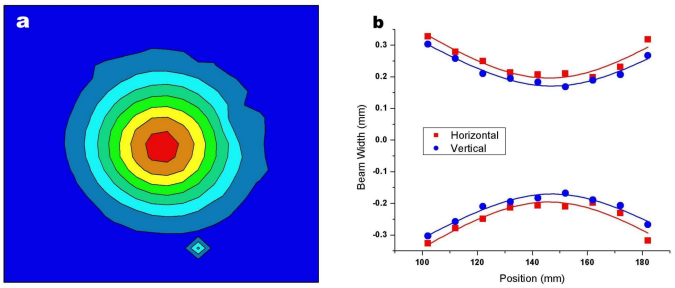

Fig. 2. (a) Sample contour plot of the idler beam. (b) Diameter of the idler beam at different distances from the nonlinear crystal (points: measured data, lines: fits).

of the beam is contained within a single Gaussian spatial mode. The slight difference between the two different directions may be due to ellipticity of the pump beam, or imperfect alignment of the lenses or the crystal axes relative to the pump beam.

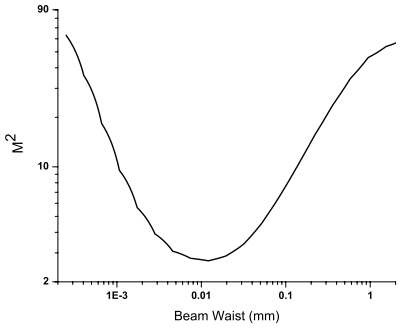

Fig. 3. Predicted M^2 values for the idler beam as a function of the pump beam waist.

Figure 3 shows theoretically estimated M^2 values for different pump beam waists [15]. These values were obtained by numerically integrating the nonlinear interaction Hamiltonian over the length of the crystal, thereby calculating the angular distribution of the photon-pair probability amplitude. This probability amplitude was used to calculate the idler density matrices. For each eigenvector of these density matrices, the spatial distribution of the electric field was determined; these spatial profiles were summed incoherently to give the total intensity distribution. These calculated profiles were then fitted in the same way as the experimental profiles in order to obtain M^2 values. Our experimental focussing condition corresponds to a beam waist of approximately 8 μm, giving a theoretical M^2 value of approximately 2.7. Considering the imprecisions involved in using Gaussians to fit more complex beam profiles, we have reasonable agreement between the theoretical prediction and our experimental results. Optimization of the pump focussing conditions should allow a lower M^2 value to be achieved, corresponding to an

#4344 - $15.00 US
Received 14 April 2004; revised 19 July 2004; accepted 21 July 2004

even larger overlap with the fundamental Gaussian mode.

Figure 4 shows a schematic of the apparatus used to generate and characterize the polarization-entangled photons. After the BP filter, the pump beam is sent through a polarizing beamsplitter (PBS) and a half-wave plate (HWP), which is rotated until the detection rates for horizontally- and vertically-polarized signal photons are the same. Following the crystals, the signal and idler beams are collimated, and are then separated using a dichroic beamsplitter.

At this point, the generated photon pairs are not yet highly entangled. Since the signal and idler have very different wavelengths, they will experience significantly different group velocities in the PPKTP. Two V photons generated in the first crystal will pass through a greater length of PPKTP than two H photons generated in the second crystal, and will thus be separated further from one another by the time they leave the material. This means that photons with different polarizations are distinguishable, destroying the entanglement. In order to recover the entanglement, it is necessary to delay the V photons relative to the H photons in only one of the beams (signal or idler), thereby eliminating the temporal separation between photons with different polarizations and erasing the distinguishing information. This delay is provided by two calcite crystals, each 1 mm thick, which we place in the idler arm. Following the calcite crystals is a quarter-wave plate, which adjusts the phase between the two polarizations.

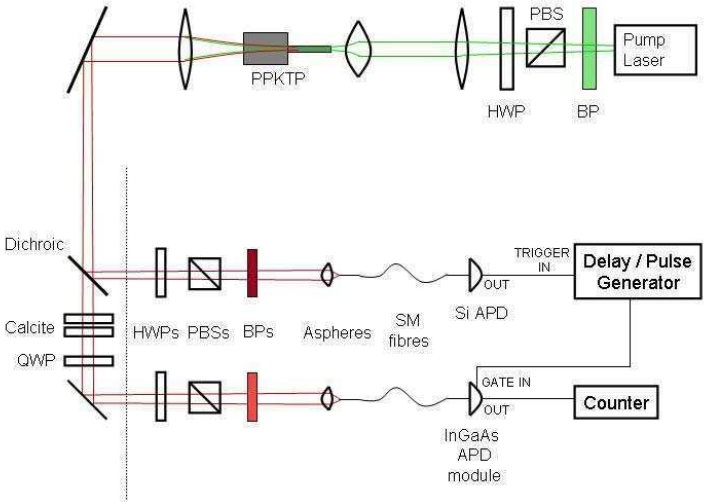

Fig. 4. Schematic of the experimental apparatus. PPKTP = periodically poled $KTiPO_4$, BP = bandpass filter; PBS = polarizing beamsplitter, HWP = half-wave plate, QWP = quarter-wave plate, SM = single-mode, APD = avalanche photodiode.

In order to evaluate the entanglement between the photons, we place a HWP followed by a PBS in each of the signal and idler arms. Pump laser light is removed by sending the signal and idler beams through BP filters with bandwidths of 10 nm. The beams are then coupled into single-mode optical fibers using aspheric lenses. Additional rejection of pump laser light is provided by chromatic aberrations in the focussing lenses, which ensure that only the desired

#4344 - $15.00 US
Received 14 April 2004; revised 19 July 2004; accepted 21 July 2004

wavelengths are focussed exactly onto the fiber tips. The fiber used for the idler photons is designed for single-mode operation at the telecommunications wavelength of 1550 nm, while the fiber used for the signal is designed for single-mode operation at 820 nm. The fiber for the idler photons leads to a home-built detector module incorporating an InGaAs / InP avalanche photodiode (APD) [16], while the fiber for the signal photons leads to a low-noise Si-based APD module. The output pulses from this detector are sent to a delay / pulse generator, which, in turn, sends gate pulses (4.0 V amplitude, 5 ns duration) to the InGaAs APD module. The delay is adjusted so that the gate pulses arrive at the InGaAs detector at the same time as the idler photons. This means that the InGaAs APD module detects coincidences (*i.e.*, signal and idler photons generated simultaneously by the source). We note that the delay / pulse generator cannot relay a second pulse if it arrives less than 1 μs after a first pulse, so that some of the output pulses from the Si APD module are lost; this effectively means a slight reduction in our overall detection efficiency.

To measure the polarization correlations between signal and idler photons, we set the HWP in the signal path to a particular angle and rotate the HWP in the idler path; for each setting, we measure a coincidence rate. This rate includes both "true" coincidences, corresponding to photons generated simultaneously in the PPKTP, and "accidental" coincidences, corresponding to photons generated at different times that happen to both arrive at the detector within the 5 ns detection time window. The accidental coincidence rate was measured, for each polarizer setting, by increasing the gate pulse delay by more than 5 ns, and was then subtracted from the total measured coincidence rate to obtain the rate of true coincidences.

Results are shown in Fig. 5; for these measurements, the incident pump power was 62 mW. There is a strong correlation between signal and idler polarizations, regardless of the measurement basis; this is the signature of entanglement. The fitted visibilities in the H, V, and 45° bases are $95.2 \pm 0.4\%$, $95.4 \pm 1.0\%$, and $79.7 \pm 0.6\%$, respectively. The visibilities in the H and V bases are probably limited by the fact that the crystals are not exactly perpendicular to one another. In future work, this will be corrected by mounting one of the samples on a rotation stage, so that its orientation can be optimized with respect to the other [15]. The reduced visibility in the 45° basis, on the other hand, is largely due to the fact that the calcite crystal thicknesses have not been optimized. The birefingence of these crystals is used to compensate for group-velocity differences between the signal and idler in the PPKTP crystals, as described above. The degree of compensation is determined by the amount of calcite material the idler photons pass through, which must be carefully adjusted in order to exactly cancel the differences in group delay and restore a high degree of entanglement [15]. The reduced visibility is also partially due to small differences between the two PPKTP crystals, possibly caused by inhomogeneities in poling period, refractive indices, and nonlinear coefficient. More uniform crystals can be obtained (albeit at a greater expense) using the hydrothermal growth technique. However, a more practical solution may be to test a number of imperfect crystals until two are found which have nearly identical nonlinear-optical properties; using these two crystals together will cancel out the effects of their imperfections.

The quantum efficiency of the InGaAs detector module was calibrated by measuring the count rates when sending in light from a fiber-coupled laser, attenuated by various degrees. After correcting the measured count rates for the Poissonian statistics of the input light, we calculated a quantum efficiency of 8%, including any losses in the optical fiber, as well as coupling losses between the fiber and detector. The quantum efficiency of the Si detector was similarly determined to be 57%. Using these detector efficiencies, we deduced the photon pair number in the single-mode optical fibers, shown on the right-hand axis of Fig. 5. We obtain approximately 3200 pairs/s in the fibers for every mW of pump power, better than any fiber-coupled source of polarization-entangled photons that we are aware of, regardless of wavelength [17, 18].

#4344 - $15.00 US Received 14 April 2004; revised 19 July 2004; accepted 21 July 2004

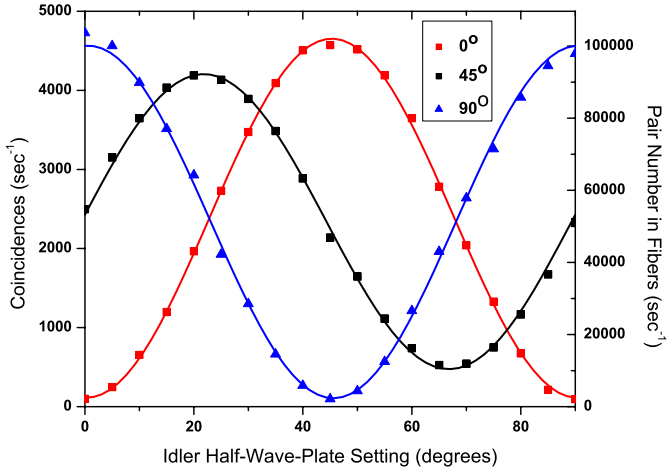

Fig. 5. Coincidence rate as a function of idler polarization, for three different settings of the signal polarization (points: measured data, lines: fits). Right-hand axis: inferred photon-pair number in the single-mode fibers.

We also calculated the overall photon detection efficiencies by comparing singles rates to coincidence rates. Photons are generated in pairs at a rate R. The number of signal and idler photons detected are $S_s = \eta_s R$ and $S_i = \eta_i R$, respectively, where η_s and η_i are the overall signal- and idler-photon detection efficiencies. The number of coincidences detected, on the other hand, is $C = \eta_s \eta_i R$, so the overall detection efficiencies can be simply determined by calculating the ratios $\eta_s = C/S_s$ and $\eta_i = C/S_i$. These total efficiencies are the products of the detector quantum efficiencies, described above, and the coupling efficiencies into the single-mode fibers; the coupling efficiencies can thus be determined by dividing the measured overall efficiencies by the calibrated detector efficiencies. Following this procedure, we determined coupling efficiencies of 21% and 7.5% for the signal and idler, respectively. This means that we have a total entangled-pair generation rate in a single spatial mode of approximately 1.2×10^7 sec^{-1}, comparable to the best reported rates for polarization-entangled photon pairs [6]. In this first experiment, we have not attempted to optimize coupling into the single-mode fibers. The relatively low coupling efficiencies we obtain are due to imperfect matching between the incoming signal and idler beams and the modes of the optical fibers; this matching is likely poorer for the idler beam, resulting in a lower coupling efficiency. By optimizing the focussing optics, it should be possible to obtain better mode matching and, therefore, significantly better fiber coupling [19].

In summary, we have demonstrated a new, efficient source of highly frequency-nondegenerate, polarization-entangled photon pairs using two crystals of periodically poled KTP, with the majority of the photons emitted into single spatial modes. The idler photons have a wavelength of 1550 nm, suitable for long-distance fiber transmission, while the signal

#4344 - $15.00 US
Received 14 April 2004; revised 19 July 2004; accepted 21 July 2004

photons have a wavelength of 810 nm, suitable for detection with high-quality Si-based photon counters. The downconversion efficiency is high, so that a relatively low-power pump laser can be used, thereby reducing the cost and size of the system. The design is highly flexible; for example, straightforward modifications would make it possible to generate any two-photon polarization state [20], while different pairs of signal and idler wavelengths could be generated simply by changing the crystal poling period (or temperature) and the pump wavelength. In this sense, our system should be able to serve as an all-purpose source of polarization-entangled photon pairs.

We would like to thank G. Björk for his helpful comments, and J. Waldebäck for his indispensable assistance with electronics. This work was supported by the Swedish Foundation for Strategic Research (SSF) and the European Commission through the IST 199-100 33 QuComm project.

#4344 - $15.00 US
Received 14 April 2004; revised 19 July 2004; accepted 21 July 2004

Paper E

Authority-based user authentication in quantum key distribution

D. Ljunggren, M. Bourennane and A. Karlsson

Phys. Rev. A **62**, 022305 (2000)

Contributions by the author: The idea was initially proposed by A. Karlsson, and further developed jointly by the authors. The candidate rewrote most of the paper based on an early manuscript prepared by the last author.

PHYSICAL REVIEW A, VOLUME 62, 022305

Authority-based user authentication in quantum key distribution

Daniel Ljunggren, Mohamed Bourennane, and Anders Karlsson*
Laboratory of Quantum Electronics and Quantum Optics, Department of Electronics, Royal Institute of Technology, Electrum 229, SE-164 40 Kista, Sweden

(Received 19 November 1999; published 13 July 2000)

We propose secure protocols for user authenticated quantum key distribution on jammable public channels between two parties, Alice and Bob. Via an arbitrator, Trent, these protocols provide data integrity and mutual identification of the messenger and recipient. The first three are based on single-photon generation and detection. The first and second require (initially) an unjammable channel between the arbitrator and each party. The third requires one broadcast from the arbitrator, disclosing what type of deterministic modification of the states sent through the quantum channel was done by him. The fourth and fifth protocols are based on two-particle entanglement with a preselection of nonorthogonal superpositions of Bell states. These two protocols also require one broadcast from the arbitrator disclosing the type of entangled state in each sending.

PACS number(s): 03.67.Dd, 03.67.Hk, 03.65.Bz

I. INTRODUCTION

Secure electronic communication, as provided by cryptography, is one of the cornerstones of the emerging information society. The following are among the basic tasks of cryptography: authentication of users, integrity of data, and privacy of data [1,2]. By *user authentication* (also called user identification) we mean the way in which a user's identity is proved (i.e., the origin of data); by *data integrity* (also called data authentication) we mean the way that data sent by the true user over any channel have not been modified or replaced; and by *privacy of data*, we mean the prevention of data from being intercepted by an unauthorized eavesdropper. The latter is warranted by encrypting the plain text into a cipher text, and for this we need a key that is to become shared by both parties involved, and this requires secure key distribution.

Classically, cryptography is divided into two classes, namely, private (symmetric) key cryptography and public (asymmetric) key cryptography. In the former class, two users (conventionally denoted Alice and Bob) must share a key to protect the privacy of data. To some extent this method can also be used to provide data integrity once the users have been authenticated, but not for user authentication directly since this requires an encryption key that has not yet been authenticated.

In the latter class, a user can provide all other users with a public key for encryption, while he/she keeps a private key for decryption. The decryption key cannot easily be found knowing only the encryption key. This class of cryptosystems easily solves the problem of *key distribution*, and can also be used to provide user authentication and data integrity, although it has the disadvantage of relying heavily on computational assumptions [1–4], making it vulnerable to threats of powered computing. It is often used together with private key cryptography, and serves in this case only the need for key distribution.

Quantum key distribution (QKD) has been proposed as a way to solve the problem of key distribution using fundamental properties of quantum mechanics to establish an unconditionally secret shared key [5–7]. See [8,9] for a flavor of experimental QKD and [10–12] for discussions on the security of QKD.

Before addressing the issue of authentication, we will define two types of channels present in QKD: the quantum channel and the public channel.

(1) The quantum channel serves the need to be private in the sense that the quantum channel may be eavesdropped on or tampered with by no more than what is permissible by quantum mechanics. This can be done passively by Eve, or actively by Mallory. The essence of QKD is to provide a method of encoding bits onto quantum states in such a way that any measure taken by an eavesdropper can be discovered by the legitimate users.

(2) The public channel is used by involved parties to exchange classical information, required for basis encoding, error correction, check of eavesdropping, and privacy amplification. It can be divided into two classes: jammable and unjammable. The unjammable channel provides data integrity that can be classically realized through authentication techniques using hash functions [3]. The security of these functions, though, also relies on computational assumptions. The jammable channel can be actively tampered with in such a way as to insert or modify messages.

A crucial assumption in QKD has been that the public channel is unjammable. Indeed, if Mallory controls the classical public channel as well as being able to monitor the quantum channel, QKD will inevitably fail. In such a scenario, Mallory can always do a ''man-in-the-middle'' attack and impersonate Alice or Bob. For instance, separate keys could be established for Alice and Bob, and thus provide unlimited access to their information.

To guarantee that this does not happen, user authentication comes into play. The fundamental problem of authentication is how to check for a shared secret under the guarantee that it will stay known only to Alice and Bob. For mutual authentication, of course, it is inevitable that they share some initial secret. If this is not the case, one classical method is to use a trusted third party who can verify that a certain key

*Electronic address: andkar@ele.kth.se

belongs to whomever it is supposed to—like in public key cryptography. User authentication based on quantum cryptography using any kind of public channel has previously been studied. Most protocols use unjammable channels and are so-called self-enforcing; i.e., no parties other than Alice and Bob are involved. However, a realistic QKD environment instead suggests that a jammable public channel between Alice and Bob should be considered. Moreover, contrary to self-enforcing protocols, we believe it is desirable that Alice and Bob need not share an initial secret. Due to this, and to prevent ''man-in-the-middle'' attacks, the introduction of a trusted authority, Trent, becomes inevitable also for QKD. The authentication between Alice and Bob will instead pass via Trent, who can verify (necessarily over unjammable channels) to each user the identity of the other. This is partly addressed in Ref. [21].

Unjammable channels like those between Alice-Trent and Bob-Trent can be guaranteed by ''personal'' authentication of such a kind that you make when you visit your bank to get your personal identification number code, together with classical authentication techniques, e.g., authentication codes [2]. In principle, if necessary, arbitrarily long authentication seeds can be exchanged for this purpose.

As a first indication that quantum authentication could be possible we consider the method of Crépeau and Salvail [13]. It provides a simple solution without Trent: if there is a shared secret string between the true Alice and Bob, then use the secret string for the selection of the polarization basis in the Bennett-Brassard 1984 (BB84) four-state quantum cryptoprotocol [5] and send a known code word over the channel. Having no *a priori* information regarding the basis choice, the eavesdropper will inevitably make errors in his or her detection. Independently, Huttner, Imoto, and Barnett proposed a very similar idea in Ref. [14], again using the basis encoding to test the correspondence between two strings. The problem, however, as stressed in [13], is that in the authentication process a dishonest party or an eavesdropper should not be able to extract any information about the initial secret, even through repeated attempts. In [13], no solution to this strict requirement was found, although it was proposed that a protocol could be built on quantum-oblivious transfer. Later, however, it was shown that quantum-bit commitment and quantum-oblivious transfer are not unconditionally secure [15,16].

Similar ideas along these lines, without Trent, have also been presented by Dusek *et al.* in [17]. They propose one classical and one QKD-based solution for user authentication. To address the problem in [13] regarding repeated attempts by an eavesdropper, the bits used for authentication are thrown away after each interleaved comparison of their secretly shared string. New secret bits are then refueled using QKD.

Another recent paper [18] discusses self-enforced authentication based on entanglement catalysis. In a first simple protocol, Alice and Bob share an ensemble of two-particle entangled quantum states. The initial secret in this case is Alice and Bob's unique knowledge of the particle states. To authenticate, Alice (Bob) sends over a number of states from her (his) ensemble and Bob (Alice) verifies that the states are the correct ones. In this process, a few of the initial states are consumed and thus the authentication secret is diminished. In an improved version of the protocol, the states initially shared by Alice and Bob are catalysis states [19]. Using these catalysis states as the shared secret only Alice and Bob will be able to make the correct local transformations [20,19] of another pair of states. The correctness of this transformation is verified between Alice and Bob and used as an authentication. What is interesting about this procedure is that the shared secret information, the catalysis states, is kept intact.

These protocols described above involve only Alice and Bob. Recently, Zeng and Zhang [21] studied the same basic idea as in [13] and [14]; however, their work was more in the context of user authenticated secret key distribution. Trent is introduced to generate the initial secret. In the protocol, Alice and Bob each have a two-particle entangled state [Einstein-Podolsky-Rosen (EPR) pairs] from which one particle each is sent to and measured by Trent. He uses the method of entanglement swapping [22] to generate a joint key to be used by Alice and Bob. Following this, the joint key should be used for user authentication in an EPR-type quantum cryptography [6] protocol with the basis choice made from the joint session key, similar to [13] and [14].

The main purpose of the present work is to address the issue of user authentication and data integrity by quantum methods. This also goes under the name of quantum authentication. As pointed out, in a realistic scenario we cannot justify self-enforcing protocols, and so therefore we feel the arbitrator unavoidable. With Trent's help, and with a jammable channel at Alice and Bob's disposal, we will provide means for Alice and Bob to agree upon a secret key using QKD. If we have a channel, or a combination of channels, that can provide us with data integrity, we can then use this to perform user authentication. Furthermore, we will show that the same objectives as in [21], using an arbitrator, can be achieved in a less complex fashion using either nonentanglement or entanglement-based protocols.

The paper is outlined as follows: In this introduction we gave a brief review of the recent work on quantum authentication. In Sec. II we will introduce and define the conditions for the third-party trusted authority, Trent. His role is to provide Alice and Bob with the seeding information that will increase security. In Sec. III, we present protocols for quantum key distribution based on conventional single-photon quantum cryptography, providing user authentication and data integrity. In Sec. IV, we present two simple entanglement-based quantum key distribution protocols, also with user authentication and data integrity. Finally, in Sec. V, our results are discussed and concluded.

II. THIRD-PARTY TRUSTED ARBITRATOR FOR QKD-BASED USER AUTHENTICATION

Obviously, it would be nice if quantum methods could provide self-enforcing protocols. However, even if this would call for some kind of ''asymmetric quantum key''

cryptography (which remains to be invented), we would unfortunately still need a trusted authority to authenticate the public quantum key. What we are concerned with here is to reflect upon whether quantum mechanics with its inherent properties (unitarity, entanglement) can yield any advantage over classical methods providing authentication via an arbitrator.

For protocols designed with Trent, like those proposed here and in Ref. [21], we believe we cannot provide Alice and Bob with a key that can be unconditionally kept in secret from Trent, as it is actually he/she who directs the entire authentication process. In other words, if Alice and Bob's mutual authentication is guaranteed only by their individual and non-necessarily correlated secret with Trent, Trent will also have full control over their communication (regardless of what channels are used) and can always do a ''man-in-the-middle'' attack if he so chooses. We conclude that, in principle, no restrictions can be imposed on Trent.

What we gain though, and what our last four protocols show, is that we can make it necessary for Trent to actively have to eavesdrop on the communication between Alice and Bob in order to get the key. Also, for the authentication that enables the authenticated direct channel to be opened up between Alice and Bob, we can allow the channels Alice-Trent and Trent-Bob to be open only once initially. Note that Trent can succeed in his eventual attempt of finding the key only during its setup and that Mallory can never. The protocols we propose are quite simple, and can clearly be improved, but we hope they are in enough detail to illustrate a few points that presumably have not been pointed out before.

Suppose the protocol followed by Trent has the following properties:

(A) Alice and Trent know the identity of each other, and they share at some instant an unjammable public channel.

(B) Bob and Trent know the identity of each other, and they share at some instant an unjammable public channel.

If the channels are available at all times, we again have an unjammable and direct public channel between Alice and Bob, and conventional quantum cryptography can be used. What we would like to do is to set restrictions on the joint availability of the channel with Trent. We will present five schemes, starting from very simple schemes and moving toward more complex ones, where with given restrictions, and some additional ones, one will be able to authenticate Alice and Bob, while at the same time provide a secret key for encryption. By giving these examples, we try to address the essential classical and quantum ingredients in the protocols.

III. NONENTANGLEMENT-BASED QKD WITH USER AUTHENTICATION

A. Nonentanglement QKD protocol (i)

The additional restriction we set on the channels between Alice and Trent and Bob and Trent for the next two protocols is (C) the public channel between Alice and Trent is open only once, as is also the channel between Bob and Trent, and there is on no occasion a channel that is directly open between Alice, Trent, and Bob. This condition, as formulated, is needed for the scheme presented next.

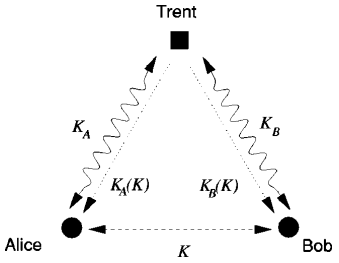

FIG. 1. Channel diagram for protocol (i). The wavy line shows the quantum channel, the dotted line shows the unjammable public channel, and the dashed line the encrypted channel. See text for details.

To set up the authentication between Alice and Bob, Trent does the following, as illustrated in Fig. 1:

(1) Trent sends Alice a long bit string encoded using the BB84 protocol (or another quantum key distribution protocol such as Ekert's protocol [6]) along with error correction and privacy amplification [5] to generate a secret key K_A. He then sends the ''session key'' K to Alice encrypted with the secret key K_A.

(2) Next, Trent sends the key K to Bob by the same method (using a different secret key K_B).

(3) Alice and Bob can send each other the secret message encrypted with the key K. It should be noted that in this trivial case, since Trent knows the key K, he can also listen to the encrypted communication. Furthermore, this protocol is obviously nothing other than a slight variation of the conventional quantum cryptographic protocol split up into two channels with Trent in the middle. Thus this protocol as such is not very interesting, but it serves as a prelude to the protocols that will follow.

B. Nonentanglement QKD protocol (ii)

The second protocol is also based on the scheme BB84 using either phase or polarization encoding. The basic idea of this protocol is to send an authentication string S to Alice and Bob, which is then sent from Alice to Bob interleaved with the other bits in the QKD protocol.

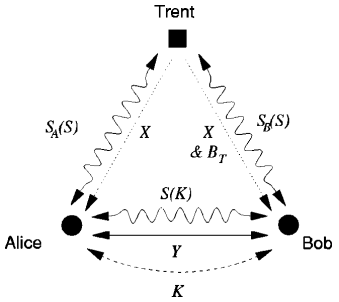

FIG. 2. Channel diagram for protocol (ii). The line types are defined as in Fig. 1, with the addition of the solid line showing the jammable public channel. See text for details.

The restriction we set on the channels between Alice and Trent and Bob and Trent is the same as in the previous example, i.e., (A–)C). The added feature in this protocol, and in the ones following, is that Trent does not directly possess the key K, but he has to actively eavesdrop on the information in Y to get it. On the contrary, Mallory can always be detected.

To set up the authentication between Alice and Bob, Trent does the following, as illustrated in Fig. 2:

(1) Trent sends Alice a long bit string encoded using the BB84 protocol with extra information X for error correction and privacy amplification. This will give Alice a bit string S_A of N bits, which is provably secure.

(2) Next, Trent sends an even longer bit sequence to Bob and establishes a secret bit string with Bob, S_B, again using the BB84 protocol with extra information X. From this string, Trent tells Bob a sequence $B_T=(b_1,b_2,\ldots,b_N)$, with the property that the bit sent to Bob at position b_i is exactly the same as the corresponding bit i in the string S_A established for Alice. Using this, Alice and Bob now share a common secret string $S=S_A=S_B$. Note that we rather not use S for the encryption itself, as Trent has direct knowledge of it. In practice we gain security if we can make Trent to actively have to eavesdrop on the information in Y to get the key. On the contrary, Mallory can always be detected.

(3) To use S for authentication, we partition S into blocks, $S=(S_1,S_2,\ldots,S_u,W,Z)$ where the length of $S_1,S_2,\ldots,S_u$ is $\log(M)$ bits (all log in base 2), M is the total number of bits sent for the key, and the length of W and Z is equal to u. We then let each block represent a position in the ensuing secret key transmission. The small chance that any $S_i=S_j$ for any i or j can be treated separately. Alternatively, we may divide M into separate blocks, with one S_i for each block. If so, the length of block S_i is $\log(M/u)$ bits.

(4) Now Alice and Bob establish a secret key K according to the BB84 protocol, sending a long bit string of M bits, however, interleaved at given bit slots S_i with a known outcome taken as the ith bit of W with polarizer settings from the ith bit of Z. This is similar to the hiding procedure used in [13]. With no *a priori* information on S, the photon sequence will then appear completely random for Mallory. In a simpler version, one could just use deterministic settings of the polarizers since Mallory will only get a few chances to extract the string.

(5) For Bob to authenticate Alice, he only checks that the outcome Y he receives corresponds to the correct ones he expects. This could be done using some coding procedure similar to that used in [13], or simply by checking the bit-error rate (BER) of the bits received. It should be noted that in practical cases where the transfer efficiency is low, the length of Y is much smaller than the length u of W.

(6) For Alice to authenticate Bob, she waits for Bob to send back over the public channel the result of Bob's measurement of Y together with the information of the timing slots indicating when he received each bit. The latter is needed when the transfer efficiency is below unity for Alice knowing which bit was received by Bob. If correct, she knows that Bob is the correct person receiving the secret key K. To succeed with eavesdropping, or impersonation, Mallory would have to succeed in evading detection. For the BB84 scheme using an intercept-and-resend strategy on all bits, Mallory will introduce a 25% BER [5]. Furthermore, he would have to guess which of the M bits constitutes W. The probability of succeeding in obtaining the authentication string correctly with no *a priori* information on S is $\Pr(S)=(3/4)^u\binom{u}{M}$, which is very small.

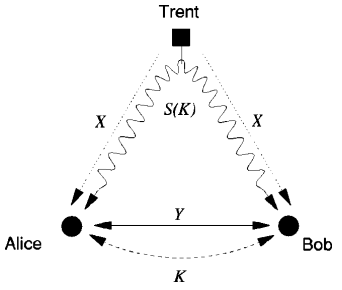

FIG. 3. Channel diagram for protocol (iii). The line types are defined as in the previous figures. In the quantum channel that goes between Alice and Bob (via Trent), Trent can only make changes in polarization. See text for details.

Another check of authentication is that Bob also knows that the sensible clear text he extracts must come from Alice, because if Mallory does not know K he cannot produce a cryptogram that when decrypted would produce anything readable.

C. Nonentanglement QKD protocol (iii)

Let us now present an even simpler protocol, which to some extent resembles [21] in that Trent determines the correlations between the bits sent by Alice and received by Bob. Let us modify assumptions (A) and (B) and (C) to the following: (A′) Trent can publicly (unjammably) broadcast to Alice and Bob the results of his actions. There also exists a jammable public channel between Alice and Bob.

The protocol is as follows, illustrated by Fig. 3:

(1) Alice sends Bob a string S of qubits encoded according to the BB84 protocol, i.e., for each bit sending either a $|z+\rangle$, $|z-\rangle$, $|x+\rangle$, or $|x-\rangle$ polarized photon.

(2) Trent sits midway between, and choose randomly between five sets (shifts qubits $|z+\rangle\rightarrow|z-\rangle$, $|z-\rangle\rightarrow|z+\rangle$, $|x+\rangle\rightarrow|x-\rangle$, $|x-\rangle\rightarrow|x+\rangle$ or does nothing). This is possible both in theory and in practice (using a polarization shifter). Note that Trent does not know what the bit value is, as he does not measure the polarizations, he only shifts them. If he had measured them, his actions would have been the same as those of an eavesdropper.

(3) Bob tells Alice a different set of bits, their position in the transmission, and the settings of the polarizers. This classical information is denoted Y in Fig. 3.

(4) Bob and Alice randomly alternate telling the settings of the polarizers for all the states received. This classical information is denoted Y in Fig. 3.

(5) Trent broadcasts (unjammably) to Alice and Bob whether or not he shifted the bits. Alternatively, we may

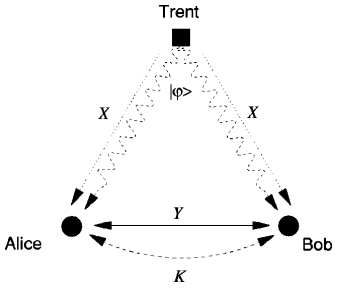

FIG. 4. Channel diagram for protocols (iv) and (v). The line types are defined as in the previous figures, with the addition of the entangled-state quantum channel illustrated with a wavy dashed line. See text for details.

suppose that the choice of states by Trent is secret information that the true Alice and Bob are given. This information is denoted *X* in Fig. 3.

(6) The above is done by first keeping only bits where the settings of the polarizers are correct.

If the data between Alice and Bob and the settings given from Trent agree, Bob and Alice have again authenticated each other via Trent. Let us stress the essential ingredient for authentication, namely, that Alice and Bob declare their bases and outcome for the test bits *before* Trent tells how the outcomes should be correlated. Note once again, that if Trent does not actively proceed with any eavesdropping on Alice and Bob's channel he will not know the authentication string, nor the key, *K*.

IV. ENTANGLEMENT-BASED QKD WITH USER AUTHENTICATION

Let us now show two protocols for authenticated key distribution based on entangled states. Whereas in [21], for each shared bit two entangled states are used, one for Alice and one for Bob, followed by an entanglement swapping measurement [22], in our protocol only one initial two-particle entangled state per shared bit is needed, which would make a substantial simplification in practice. In the present scheme, as illustrated in Fig. 4, Trent has a pool of entangled states. For each bit he wants to establish, he sends the first particle from the entangled state to Alice, and the other to Bob. Note that the present protocol uses some ideas from quantum secret sharing [27,28]. As in [21], using entanglement, Trent will only be required to broadcast extra information regarding which entangled states he sent in each case.

Before going into the protocols, let us reiterate some basic properties of entangled photon states. A two-photon entangled state, such as that generated from a type-II parametric down-conversion crystal [23], can be written as

$$|\psi\rangle=\frac{1}{\sqrt{2}}(|z+\rangle|z-\rangle+e^{i\alpha}|z-\rangle|z+\rangle), \tag{1}$$

where α is a birefringent phase shift of the crystal, and $|z+\rangle$ and $|z-\rangle$ denote the horizontal and vertical polarization eigenstates.

Using appropriate birefringent phase shifts and polarization conversions, one may easily convert the above state into any of the four Bell states;

$$|\phi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|z+\rangle|z+\rangle\pm|z-\rangle|z-\rangle), \tag{2}$$

$$|\psi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|z+\rangle|z-\rangle\pm|z-\rangle|z+\rangle). \tag{3}$$

Shifting between these states (actually among all four Bell states) has been demonstrated experimentally in Bell-state analysis [24]. (In the entanglement-based quantum cryptography scheme [6], however, one considers a passive version based on sending only one of the Bell states to Alice and Bob.)

Furthermore, let us define a new linear combination of Bell states as

$$|\Psi^{+}\rangle\equiv\frac{1}{\sqrt{2}}(|\phi^{-}\rangle+|\psi^{+}\rangle)=\frac{1}{\sqrt{2}}(|z+\rangle|x+\rangle+|z-\rangle|x-\rangle)$$

$$=\frac{1}{\sqrt{2}}(|x+\rangle|z+\rangle+|x-\rangle|z-\rangle), \tag{4}$$

$$|\Phi^{-}\rangle\equiv\frac{1}{\sqrt{2}}(|\phi^{-}\rangle-|\psi^{+}\rangle)=\frac{1}{\sqrt{2}}(|z+\rangle|x-\rangle-|z-\rangle|x+\rangle)$$

$$=\frac{1}{\sqrt{2}}(|x+\rangle|z-\rangle-|x-\rangle|z+\rangle). \tag{5}$$

Now the set of states $|\varphi\rangle\in\{|\psi^{+}\rangle,|\phi^{-}\rangle,|\Psi^{+}\rangle,|\Phi^{-}\rangle\}$ has the feature that $\langle\psi^{+}|\phi^{-}\rangle=\langle\Psi^{+}|\Phi^{-}\rangle=0$.

Furthermore, all states are not orthogonal, as $|\langle\psi^{+}|\Psi^{+}\rangle|^2=|\langle\psi^{+}|\Phi^{-}\rangle|^2=1/2$ and $|\langle\phi^{-}|\Psi^{+}\rangle|^2=|\langle\phi^{+}|\Phi^{-}\rangle|^2=1/2$. We will use this feature in the protocols below. The main idea is for Trent to pick states from a set of nonorthogonal base states and send them to Alice and Bob. Since the states are nonorthogonal, Mallory cannot intercept them and reliably measure their properties. A second feature we will use in the protocol is that Alice and Bob will first declare their information for authentication based on their respective measurements. After this, Trent will release which quantum state was sent, allowing Alice and Bob to cross check independently to see if the information released was correct. An impersonator like Mallory will not be able to release the correct information, and Alice and Bob will know that the public and/or quantum channel has been tampered with.

A. Four-state entanglement-based QKD with user authentication (iv)

Using two-particle quantum entanglement with Trent providing the states, we keep assumption (A′) on Trent. Let us

TABLE I. Correlation of measurement outcomes given that Trent has sent a certain two-particle entangled state.

Alice \ Bob	$z+$	$z-$	$x+$	$x-$
$z+$	ϕ^-	ψ^+	Ψ^+	Φ^-
$z-$	ψ^+	ϕ^-	Φ^-	Ψ^+
$x+$	Ψ^+	Φ^-	ψ^+	ϕ^-
$x-$	Φ^-	Ψ^+	ϕ^-	ψ^+

as starting states pick $|\phi^-\rangle$ and $|\psi^+\rangle$ as one base, and $|\Phi^-\rangle$ and $|\Psi^+\rangle$ as the other. The user authentication and key distribution scheme illustrated with Fig. 4 is as follows:

(1) Trent sends one of the entangled states $|\varphi\rangle \in \{|\psi^+\rangle, |\phi^-\rangle, |\Psi^+\rangle, |\Phi^-\rangle\}$, each with a probability of $\frac{1}{4}$. One photon from the entangled state is sent to Alice, and the other photon is sent to Bob. Alice and Bob measure the polarization of the incoming photon by switching randomly between the z base and the x base.

(2) Alice tells Bob a set of bits, their positions in the transmission, and the corresponding settings of the polarizers.

(3) Bob tells Alice a different set of bits, their positions in the transmission, and the corresponding settings of the polarizers.

(4) Bob and Alice randomly alternate telling the settings of the polarizers for all the states received.

(5) Trent broadcasts (unjammably) to Alice and Bob which of the entangled states he sent for all of the bits. Alternatively, we may suppose that the choice of states by Trent is secret information that the true Alice and Bob are given. This information is denoted by X.

(6) Alice and Bob sort their released data into four bins N_1 to N_4. In bin N_1, they place the states pertaining to if Trent sent a $|\psi^+\rangle$ state. In this case they know that their results should be anticorrelated in the z base and correlated in the x base. In bin N_2, they place the states pertaining to if Trent sent a $|\phi^-\rangle$ state. Their results should then be perfectly correlated when both are measured in the z base and anticorrelated when both are measured in the x base. In bin N_3 they place the results if Trent sent a $|\Psi^+\rangle$ state. In this case, if Bob and Alice measure in different bases, the results are correlated. Finally, in bin N_4, they place the results if Trent sent a $|\Phi^-\rangle$ state. For this state they know that the bits should be anticorrelated when Alice and Bob measure in different bases. All other cases they discard. In Table I we have summarized the correlation relations for different settings of Alice and Bob polarizers. This departure from correlation to anticorrelation gives Alice and Bob the unique signature from Trent, which allows them user authentication.

(7) Alice and Bob then check their bits according to the bins N_1 to N_4.

(8) The final step is to distribute the cryptokey K, which is done using the remaining secret bits from the bins N_1 to N_4 as before. This is done by first keeping only bits where the settings of the polarizers were the same. This exchanged information Y is shown in Fig. 4.

If the data between Alice and Bob and the settings given from Trent agree, Bob and Alice have again authenticated each other via Trent. Let us stress the two essential ingredients for authentication: first, the control of the sign of the correlation between the bits done by Trent, and second the fact that Alice and Bob declare their bases and outcome for the the test bits *before* Trent tells how the outcomes should be correlated. Note that, since we do the eavesdropping test using data from Trent, it is not necessary to use the encoding procedure in [6], where a test of the violation of a Bell inequality [26] is used to detect the eavesdropper. Consider the eavesdropper using a Bell analyzer to perform eavesdropping. If so, in half the cases he will make the right choice; in the other half he will not. On average, the eavesdropper will impair a 25% BER, as well as induce the same BER in the channel. To check the agreement with the data one may simply check that the BER is not above a critical value. Let us furthermore stress that, as Trent does not know the outcome of Alice and Bob's measurements, he knows neither the authentication string nor the secret key K established by Alice and Bob.

The data-sorting procedure used in the protocol is similar to the ''entangled entanglement'' studied by Krenn and Zeilinger [25] for three-particle entangled states (GHZ-states [29]), albeit here Trent does classical random selection of the states. One can also easily construct (on paper) a three-particle entangled version of the above protocol, in which the selection of the state sent by Trent is made purely random, contingent upon the outcome of the measurement of his particle from the three-particle entangled states.

B. Two-state entanglement-based QKD with user authentication (v)

Finally, let us show a simplified version of the four-state scheme, using only two nonorthogonal states. This scheme is in some respects, very similar to the two-state scheme Bennet 1992 (B92) [7]. In this case, Trent will again not know which is the authentication string, nor will he know the secret key bits.

The user authentication and key distribution scheme, as illustrated with Fig. 4, is as follows:

(1) Trent sends the entangled states $|\psi^+\rangle$ or $|\Psi^+\rangle$, each with the probability $\frac{1}{2}$ (remember these states are not orthogonal). Alice and Bob do measurements in the polarization by randomly switching between the z base and the x base.

(2) Alice tells Bob a set of bits, their position in the transmission, and the settings of the polarizers.

(3) Bob tells Alice a different set of bits, their position in the transmission, and the settings of the polarizers.

(4) Bob and Alice randomly alternate telling the settings of the polarizers for all the states received.

(5) Trent broadcasts which of the entangled states he sent for all of the bits.

(6) Alice and Bob sort their released data into two bins N_1 and N_2. In bin N_1, they place the states if Trent sent a $|\psi^+\rangle$ state. In this case they know that their results should be an-

ticorrelated in the z base and correlated in the x base. In bin N_2 they place the states if Trent sent $|\Psi^+\rangle$ state. In this case, if Bob and Alice measure in incompatible bases, the results are correlated.

(7) Alice and Bob then check their bits according to the bins N_1 and N_2.

(8) The final step is the distribution of the cryptokey itself, which is done using the remaining secret bits from the bins N_1 and N_2 as before. This is done by first keeping only bits where the settings of the polarizers were the same.

If the data between Alice and Bob and the settings given from Trent agree, Bob and Alice have again authenticated each other via Trent. If an eavesdropper listens in or is not in possession of any of the entangled states, he cannot reproduce the statistical correlations between the three persons. Furthermore, an eavesdropper cannot successfully (using a Bell-state measurement) distinguish the two states without ambiguity. If there are losses in the system, he may, however, succeed in eavesdropping as is the case for two-state quantum cryptography [7].

V. DISCUSSION

As for the general applicability of these schemes, they still assume the existence of an unjammable public channel at some instance (one way in some protocols, two ways in other). Alternatively, the protocols assume that some initial piece of secret information is available. Also with Trent this is inevitable. However, they do allow quantum key distribution on a jammable public channel between Alice and Bob, and they do increase the overall security by giving ''an extra handle'' in the correlations. We believe that the three main results–to send authentication information interleaved with the quantum key, to manipulate the Bell states used for the key generation, and to use a nonorthogonal state base similar to what is done in single-photon quantum cryptography—are all of interest for applications of user authentication in quantum cryptography. Entangled-state manipulation also has use in quantum secret sharing protocols [27,28]. An interesting question, that we just commented on briefly, is to what extent three-particle entangled states can be used for authentication, similar to the case of secret sharing [27]. As for the experimental feasibility of the above protocols, they would all be possible using present-day technology; optical Bell-state generation has been done by several groups, Bell-state manipulation has been demonstrated, and on the receiver side only single-photon detection will be required. Of course, the feasibility does not imply that the added technical complexity compared to attenuated coherent-state quantum cryptography using unjammable public channels will necessarily be justified.

ACKNOWLEDGMENTS

A. Karlsson would like to acknowledge Nobuyuki Imoto and Masato Koashi of NTT Basic Research Laboratories and Soken University for Graduate Studies, and Artur Ekert of Oxford University for useful discussions during the initial part of the work. This work was supported by the European IST FET QuComm project, the Swedish Natural Science Research Council (NFR), and the Swedish Technical Science Research Council (TFR).

[1] B. Schneier, *Applied Cryptography, Protocols, Algorithms and Source Code in C* (John Wiley and Sons, New York, 1996).
[2] D. R. Stinson, *Cryptography, Theory and Practice* (CRC, New York, 1995).
[3] M. N. Wegman and J. L. Carter, J. Comput. Syst. Sci. **22**, 265 (1981).
[4] A. Fiat and A. Shamir, in *Advances in Cryptology: Proceedings of Crypto 86*, edited by A. M. Odlyzko (Springer-Verlag, New York, 1987), pp. 186–194.
[5] C. H. Bennett, G. Brassard, and J. Smolin, J. Cryptology **5**, 3 (1992).
[6] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[7] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[8] H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin, and G. Ribordy, Appl. Phys. B: Lasers Opt. **67**, 743 (1998).
[9] M. Bourennane, D. Ljunggren, A. Karlsson, Per Jonsson, A. Hening, and J. P. Ciscar, J. Mod. Opt. **47**, 563 (2000).
[10] N. Lütkenhaus, Phys. Rev. A **54**, 97 (1996).
[11] N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999).
[12] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Los Alamos e-print quant-ph/9911054.
[13] C. Crépeau and L. Salvail in *Advances in Cryptology: Proceedings of Eurocrypt '95*, edited by L. C. Guillon and J. J. Quisquater (Springer-Verlag, New York, 1995), p. 133–14.
[14] B. Huttner, N. Imoto, and S. Barnett, J. Nonlinear Opt. Phys. Mater. **5**, 823 (1996).
[15] H. K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).
[16] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).
[17] M. Dusek, O. Haderka, M. Henrych, and R. Myska, Phys. Rev. A **60**, 149 (1999).
[18] H. Barnum, Los Alamos e-print quant-ph/9910072.
[19] D. Jonathan and M. Plenio, Phys. Rev. Lett. **83**, 3566 (1999).
[20] M. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).
[21] G. Zeng and W. Zhang, Phys. Rev. A **61**, 022303 (2000).
[22] J. W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998).
[23] P. G. Kwiat, K. Mattle, H. Weinfurther, and A. Zeilinger, Phys. Rev. Lett. **75**, 4337 (1995).
[24] M. Michler, K. Mattle, M. Eible, H. Weinfurther, and A. Zeilinger, Phys. Rev. A **53**, R1209 (1996).
[25] G. Krenn and A. Zeilinger, Phys. Rev. A **54**, 1793 (1996).
[26] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).
[27] M. Hillary, V. Buzek, and A. Bertaiume, Phys. Rev. A **59**, 1829 (1999).
[28] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
[29] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).

Paper F

Experimental long wavelength quantum cryptography: from single-photon transmission to key extraction protocols

M. Bourennane, D. Ljunggren, A. Karlsson, P. Jonsson, A. Hening and J. Peña Císcar

J. Mod. Opt. **47**, 563-579 (2000)

Contributions by the author: The candidate investigated the theory of error correction and privacy amplification and wrote all the software under the supervision of M. Bourennane and A. Karlsson. The candidate also took part in the experimental work, specifically single photon detection. The system experiment was conducted by the first author with background work done by the co-authors. The paper was prepared jointly by the first three authors.

JOURNAL OF MODERN OPTICS, 2000, VOL. 47, NO. 2/3, 563–579

Experimental long wavelength quantum cryptography: from single-photon transmission to key extraction protocols

MOHAMED BOURENNANE, DANIEL LJUNGGREN, ANDERS KARLSSON, PER JONSSON, ALEXANDRU HENING† and JUAN PENA CISCAR

Department of Electronics, Royal Institute of Technology (KTH), Electrum 229, 164 40 Kista, Sweden

(*Received 31 March 1999; revision received 7 July 1999*)

Abstract. We present experiments on long wavelength ($\lambda = 1.55\,\mu m$) 'plug and play' quantum cryptography systems. We discuss the performance of single-photon detectors at $\lambda = 1.55\,\mu m$. Furthermore, we address the full implementation of the quantum cryptography protocol, discussing in detail the implementation of protocols for error correction and privacy amplification needed to get a secure key. We illustrate the theory with examples from a full software simulation to show the performance of the complete protocol in terms of final secure key creation rate.

1. Introduction

The last decade has seen the birth of quantum information, which combines quantum mechanics with information technology in novel and fruitful ways. Of various theoretical proposals and experimental demonstrations, quantum cryptography for secret key distribution [1] is the most mature and closest to 'real world' applications. From the initial 'proof-of-principle' demonstration (in 1989) of secret-key transmission over 30 cm by researchers at IBM [1], the field has progressed very rapidly. At Los Alamos National Laboratory secret keys have been transmitted in optical fibres over distances of 48 km [2] and up to 1 km in free space [3]. BT labs have sent cryptographic keys in a $\lambda = 1.3/1.5\,\mu m$ field wavelength division multiplexing (WDM) system, sending the key at $\lambda = 1.3\,\mu m$ and the encrypted data at $\lambda = 1.5\,\mu m$ [4]. The University of Geneva has demonstrated a very stable 'plug and play' interferometric system on 23 km installed telecom fibre, see [5] and the improved automated system in [6]. The main obstacle today is noise in the avalanche photodiodes (APDs) used as single-photon detectors. At an optical wavelength of $0.85\,\mu m$ silicon APDs have a very good performance, but the losses in the optical fibre limits the transmission distance to a few kilometres. At $1.3\,\mu m$, both germanium and InGaAs/InP APDs have been extensively studied [7, 8]. Finally, at $1.55\,\mu m$, where the optical fibre losses are the lowest, several groups—among others the European ESPRIT project EQCSPOT (University of Geneva, DERA, Oxford, Innsbruck, Elsag Bailey), Telenor

† Permanent address: Institute of Atom Physics, Magurele, Romania.

Journal of Modern Optics ISSN 0950–0340 print/ISSN 1362–3044 online
http://www.tandf.co.uk/JNLS/mop.htm
http://www.taylorandfrancis.com/JNLS/mop.htm

(Norwegian PTT), University of Århus, and our group at KTH, Stockholm [9, 10]—are now studying quantum cryptography systems using indium gallium arsenide (InGaAs) APDs as single-photon counters.

In this paper, we will discuss our experimental work at KTH on the realization of a long wavelength ($\lambda = 1.55\,\mu m$) 'plug and play' quantum cryptography system as well as discuss the implementation of the protocols needed for the extraction of a final secure key. The paper is organized as follows: in section 2, we describe the 'plug and play' system, the performance of single-photon counting APDs and the system's results on quantum bit error rate. In section 3 we discuss in detail the classical communication protocols needed to supplement the quantum parts of the protocol, and describe software simulations of the complete protocol. Finally in section 4 we combine the results of sections 2 and 3 to predict what would be the final performance for the bit rate of the secure key.

2. Experimental long wavelength quantum cryptography

2.1. *A systems example*

Let us now describe our implementation [9, 10] of a $\lambda = 1.55\,\mu m$ 'plug-and-play' interferometric scheme for quantum cryptography [5], see figure 1. Our present system uses phase encoding of the B92 protocol [11], based on two non-orthogonal states. The Geneva group has also at $\lambda = 1.3\,\mu m$ implemented the 4-state BB84 protocol featuring improved security compared to the two-state protocol [6]. Phase encoding is often preferred over polarization encoding, because the interferometric phase of a photon is better preserved than the polarization in telecom fibres. The birefringence of fibres and the effect of the environment make polarization fluctuate more randomly.

The principle is to get interference at Bob between two weak pulses. Bob and Alice can change the phase of these pulses. If this interference is constructive, there is a click in the receiving photodetector; *thus Alice's and Bob's independent*

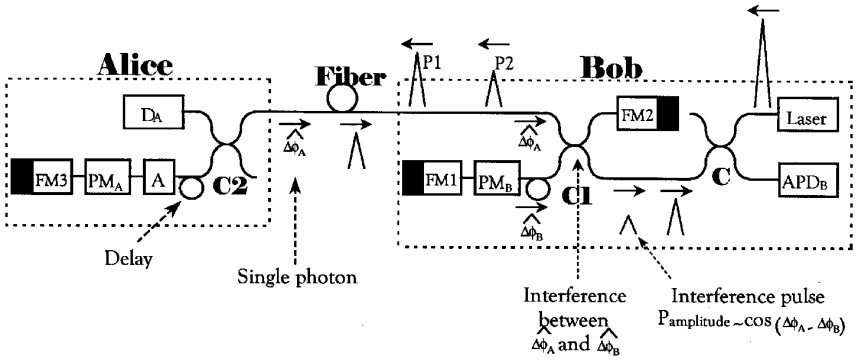

Figure 1. 'Plug and play' system (originally demonstrated by University Geneva in [5]) at the Department of Electronics, KTH, using phase encoding in the B92 scheme. The laser pulse from Bob is split into two pulses, one comes back from Alice modulated, and the other one is reflected at Bob and also modulated. Both pulses will interfere at Bob and can carry information about a digital 1 or a 0 in either one of the bases, by Alice's choice of modulation.

choices of the phase can carry information from Alice to Bob. These weak pulses typically will have an intensity of $\mu = 0.1$ photons per transmission, as the probability that two or more photons are sent will then be given approximately by $\mu^2/2$ (a laser exhibits a Poissonian distribution of the photons). With more than one photon per pulse, one can eavesdrop more easily [12, 13].

In figure 1, we show the implemented 'plug and play' quantum cryptography system set-up. By using Faraday mirrors, any birefringence in the interferometer is compensated and no alignment is needed. These main steps can describe the procedure of the encoding and transmission of the raw bits.

- Bob sends a pulse from the laser.
- At C1 (fibre coupler), the pulse is split into two pulses P1 and P2. The P1 pulse goes directly onto the fibre, while P2 goes first through Faraday mirrors FM1–FM2 and then into the fibre.
- When part of the P1 pulse (split in C2) reaches detector D_A (PIN), the detector triggers Alice's phase modulator PM_A, which encodes a phase to the P2 pulse.
- Both pulses are reflected at Faraday mirror FM3, and attenuated by attenuator A to the single photon level.
- When the pulses again reach C1, one part of the P1 pulse goes via FM2 Bob's phase modulator PM_B, where it acquires a phase shift.
- The P2 pulse, with a phase shift from Alice, interferes at the coupler C1 with the P1 pulse, with a phase shift of Bob.
- The interference will be constructive and destructive if the phase difference is 0 or π respectively.
- The cases of constructive interference causing also a count in Bob's detector are kept as valid data bits.

2.2. *Detector performance*

The single-photon detector used in the present work is a liquid nitrogen cooled indium gallium arsenide (InGaAs) APD operated in a gated mode, lifting the bias voltage above breakdown a few nanoseconds, when we expect a signal to arrive. In the 'plug and play' system this information is readily available since Bob both sends and receives the pulses. A passive quenching circuit with a 320 kΩ series resistance providing the DC bias was used. The gate voltage was added on top of the bias, and the signal was measured over a 50 Ω load resistance. Our best performance so far has been obtained with an InGaAs APD C306444EJT-07 manufactured by EG&G. However, other work [14], indicates that selected APDs from other manufactures also may give a similar performance. The APD was put in a Dewar together with a thermoheater on the circuit board, which we use to regulate the temperature to find an optimum operating range. In figure 2 we show the quantum efficiency η of the APD, and in figure 3, the noise-equivalent power ($\mathrm{NEP} = h\nu(2R)^{1/2}/\eta$), where $h\nu$ is the photon energy and R the dark count rate (counts s^{-1}) as a function of temperature respectively. As seen from figure 3, a good operating temperature is found around − 60°C. At this temperature, we operate the APD with an excess bias voltage of 3.5 V (from 0.5 V below the breakdown voltage of 41.5 V). This gives a quantum efficiency of 18% at 210 K and using a gate width of 5 ns, we obtain a dark count probability per pulse of $P_d = 2 \times 10^{-4}$ in the

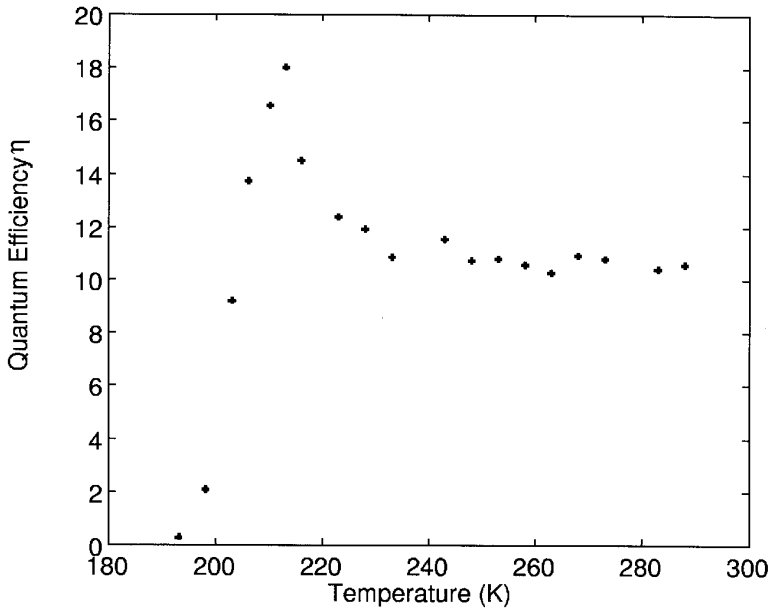

Figure 2. Quantum efficiency of the avalanche photodiode as a function of temperature. An excess voltage of 3.5 V above breakdown is used in the gating.

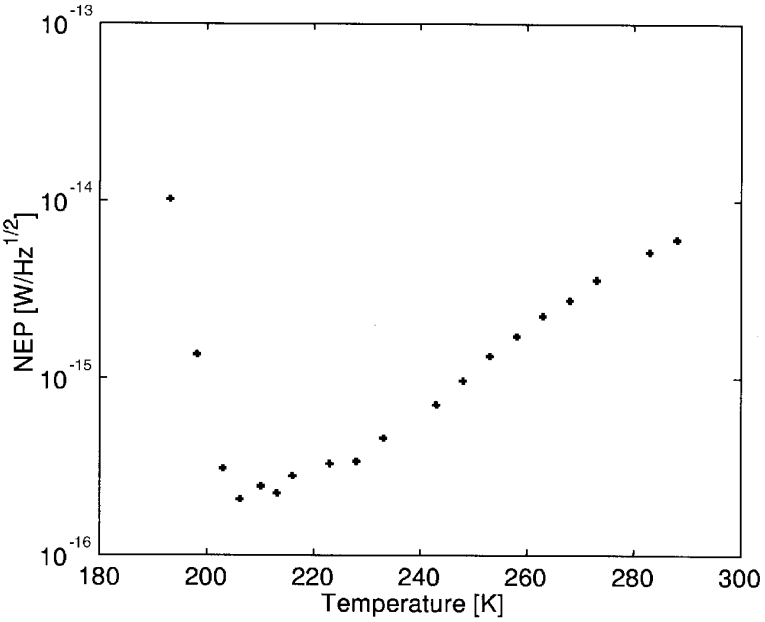

Figure 3. Noise-equivalent power (NEP), as a function of temperature for the InGaAs APD. An excess voltage of 3.5 V above breakdown is used in the gating.

counter. This is slightly higher compared to the results for selected Fujitsu APDs reported in [14], but our results for the quantum efficiency are higher.

2.3. *Systems results*

For a quantum cryptography system where the security is based on the ability of detecting an eavesdropper (Eve), one of the most critical parameters is the system noise. This is because we tactically have to assume that all errors are due to Eve, so that for the impaired quantum bit error rate (QBER) she has obtained maximum information. As will be shown below, the larger the systems noise, the more the key must be compressed in order to reach the final secure key of which Eve has arbitrarily low information. As also will be shown, beyond a certain error rate, it is not possible to obtain a fully secure key.

The collected rate of all errors e is called the quantum bit error rate. The name quantum bit error rate, instead of simply error rate, is chosen because it is only the error rate before error correction is applied. If η is the detector quantum efficiency, μ the average number of photons per pulse, α the channel (fibre) attenuation coefficient in dB km^{-1}, and L the transmission length in km, then the raw bit rate R_r for Bob is

$$R_r = \eta\mu 10^{-\alpha L/10} R_0, \tag{1}$$

where R_0 is the source bit rate on Alice's side. Note that in the 'plug-and-play' system, the signal is attenuated to the single-photon level (average photon per pulse μ) only after Alice has phase modulated the pulse.

However, the key distribution is limited not so much to the bit rate itself, but rather to the error rate, QBER, for which an upper bound exists above which not all errors can be corrected without decreasing the final bit rate to zero. Assuming quite realistically a non-perfect classical visibility V_c in the photon interference, the QBER is given by [10]

$$\text{QBER} = e = \frac{(1 - V_c)10^{-\alpha L/10}\eta\mu/2 + P_d}{2P_d + 10^{-\alpha L/10}\eta\mu}, \tag{2}$$

where α is the fibre loss in dB km^{-1} and L is the transmission distance in km; the other parameters were defined above. This result follows simply by applying Bayes' rule for the computation of the probabilities in terms of transmission rates.

In the systems experiment, a $\lambda = 1.55$ μm distributed feedback (DFB) laser was directly modulated to produce a 2 ns pulse with a repetition rate of $B = 1$ kHz. The pulses are sent from Bob along a spooled fibre before reaching the side of Alice where the pulses are attenuated to an average of $\mu = 0.1$ photon per pulse. In a separate measurement, using strong signals ($\mu \gg 1$), the classical fringe visibilities of 98, 96 and 90% were obtained for a propagation of 10, 30 and 40 km of spooled fibre, respectively. To experimentally infer what would be the total system QBER, i.e. the error rate before error correction, we measure in the single-photon regime the counts per second for constructive, I_{max}, and destructive interference, I_{min}. From Bayes' rule we obtain QBERs of $e = I_{min}/(I_{max} + I_{min})$ of 3%, 6% and 9% for a propagation distance of 10, 30 and 40 km respectively. This is below both the 11.5% limit and the 15% limit (the different limits are due to different assumptions on the eavesdropper's abilities), above which error correction and privacy amplification cannot be used easily [12, 13], see also below.

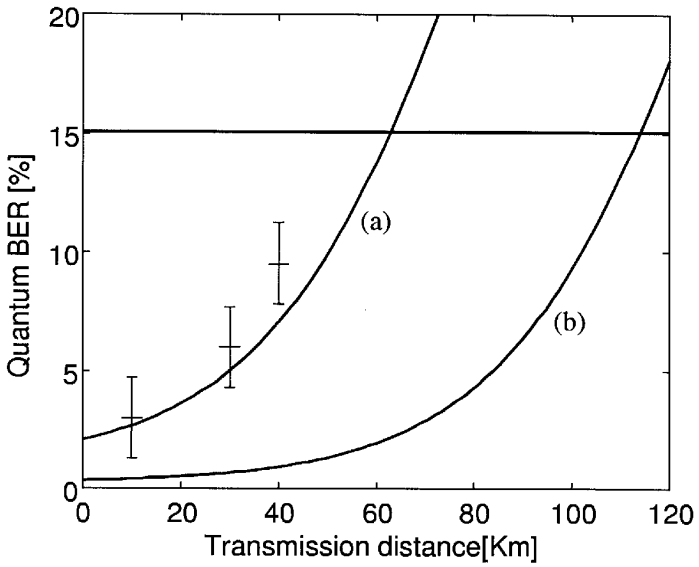

Figure 4. (*a*) QBER as a function of transmission distance. The marks with error bars are experimentally obtained results for 10, 20, 40 km transmission on spooled fibre. The dark count probability is 2×10^{-4}, the average photon number per pulse is 0.1, the quantum efficiency is 18%, the fibre loss is 0.2 dB km^{-1} and the visibility is 98%. (*b*) QBER for a dark count probability 2×10^{-5} and a visibility of 99.5% is plotted.

From the experimental results, and a theoretical expression for the QBER [10], we may extrapolate to find the longest transmission distance possible. In figure 3, we plot the QBER as a function of transmission distance, inserting also our experimental results. From this figure we see that using the present experimental parameters a 60 km transmission of a secure key would be feasible. Considering the quite large classical visibilities we already have, further improvements in visibility do not improve the transmission distance very much. The key parameter is rather the reduction of the dark counts (while keeping the quantum efficiency high enough). Assuming 0.2 dB km^{-1} losses, a ten-fold decrease in dark count rate (for constant quantum efficiency) translates into a 50 km increase in transmission distance. To decrease the dark counts one may use shorter gate widths, for instance by having an actively quenched APD, or use a time-to-amplitude converter. In curve (b) (figure 4) we show the predicted result for 99.5% classical visibility and a ten-fold decrease in dark count rate (but the same quantum efficiency), allowing for more than 100 km secure key distribution.

In the present experimental data we opted for a very low source rate of 1 kHz. This, however, is neither any fundamental nor any practical limit of the APD detector or the 'plug and play' system itself. Primarily two effects will limit the source rate. First, for the 'plug and play' system, as discussed in [6], one must avoid having too many pulses circulating in the transmission line. A second concern is the APD itself, in that after-pulsing due to trapped carriers may increase the dark counts if the gate pulses are too close in time [14]. Still, a 100 kHz to a 1 Mbit s^{-1} source rate system should be feasible and, as will be seen below, will be needed to realize a final key creation rate in the kbit s^{-1} regime.

3. Secret key extraction from raw data transmission

When Bob has received and decoded the transmitted information he will end up with a number of raw bits. Depending on the chosen coding scheme, a constant factor (on average) of bits will be lost at the demodulation, typically half of the bits. The remaining, so-called sifted bits will still contain errors that have to be corrected. There exists a minimum amount of bits that have to be sacrificed in order to accomplish error correction. Also, the corrected key is not perfectly secure and has to be compressed by privacy amplification to gain security. When the key is compressed, an additional number of bits need to be discarded. All these steps entail a reduction of the number of raw bits for the key extraction protocol.

3.1. *Information flow*

By key agreement we refer to the procedures by which a perfectly secret key is agreed upon between two parties. A key is perfectly secret if any eavesdropper has no other strategy than a random guess for each bit in the key. A block-diagram of a complete protocol for key distribution in quantum cryptography is shown in figure 5. The raw key (before sifting) is made up of bits obtained by Bob after demodulation of incoming photons. Two channels are needed in order to make a key agreement protocol complete.

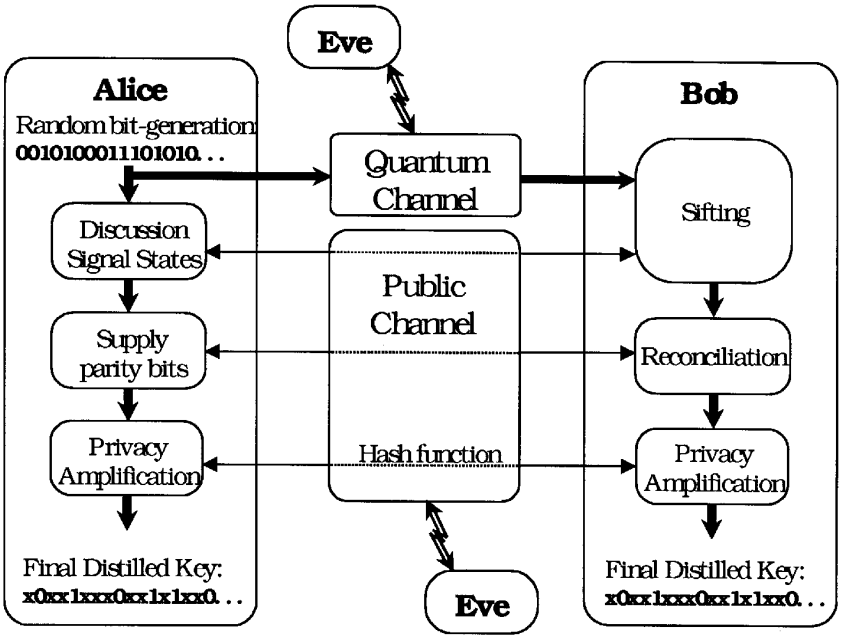

Figure 5. Diagram of the basic flow in the information process for quantum cryptography. Two channels: the private quantum channel and the public channel are shown. Several steps like sifting, error correction and privacy amplification are needed to distribute a final secure key between Alice and Bob.

- For transmission of the photons we have the private quantum channel (PQC), i.e. the optical fibre. This channel has no authenticity and imperfect privacy.
- Alice and Bob use the public channel (PC) to exchange classical information as part of the key agreement. This channel is assumed to have perfect authenticity, but no privacy. This means that Eve can only listen to the channel, but not change the information sent by it. The public channel transmits information with perfect fidelity.

The assumption that public messages cannot be corrupted by Eve is an important (and very reasonable) restriction, because otherwise it is clear that Eve could sit in between Alice and Bob and impersonate each of them to the other. If message authenticity cannot be enforced by the physical properties of the channel, it can be provided by a secure classical authentication scheme [15].

In order to control the experimental system set-up, as well as being able to simulate the quantum cryptography system, we need computer protocols. We have recently built up a software system to simulate all steps—from the sending of the random bit string over the fibre to the sifting, error correction, and privacy amplification—all according to the quantum cryptography scheme described earlier [16]. New results using this tool will be given below. We have two different kinds of software that communicate with each other and the experimental set-up. The first one has been fully implemented and, at the time of submission of the paper (March 1999), the second part was under implementation.

The purpose of the first software part (protocol software) is principally to make up a window user interface for both Alice and Bob were all necessary system parameters are set and the resulting key is presented. In the background, the program should utilize the protocols of reconciliation (error correction) and privacy amplification to extract the final secretly shared key. The code is written in Matlab, allowing easy simulations.

The objective for the second software part (controlling software) is to control the hardware of the experimental set-up; i.e. this part supplies the raw key for further processing in the protocol-software part. The program is written in LabVIEW. Note that in this first system we only use one computer hosting both Alice and Bob, but no communication between Alice's and Bob's software are allowed outside the strict rules of the protocol.

3.2. *Sifting*

As mentioned, according to the specific protocol, e.g. BB84 and B92, Bob and Alice will agree to use only the information sent together with those photons Bob measured in the correct basis. This selection is made by comparing the bases of Alice and Bob. This part of the protocol is called *sifting* and produces a sifted key out of the raw key. Due to the eventual presence of an eavesdropper and due to transmission and detection limitations, errors are introduced and have to be corrected by the protocol.

3.3. *Reconciliation*

Reconciliation is the process of correcting errors between Alice and Bob's version of the sifted key. There are several, more or less successful, methods to accomplish error correction efficiently. In classical noisy communication, there are

very well known error-correction codes that use redundancy in the signal to transmit error-free information. Perhaps the reason why classical coding does not seem so popular in quantum cryptography is that in some way the code words must be known to both sender and receiver, e.g. decided before transmission. Alice and Bob then have to share some initial information. Another problem is that a large fraction of bits is thrown away in the sifting part. This fraction (50%) is so large that other error-correction schemes become more efficient. In other cases coding can be implemented to work very efficiently.

During reconciliation, information is exchanged over the insecure public channel. We want to minimize the information that the eavesdropper Eve gains, and at the same time efficiently correct all errors in Bob's key, losing as small a fraction of bits as possible.

Unconditionally there is a minimum amount of information that has to be exchanged between Alice and Bob in order to correct all of Bob's bits. Either this information may be in the form of bits leaked to Eve, or by bits Alice and Bob have to agree to lose in the form of introduced redundancy or by discarded bits. We can calculate for this bound in information for a binary symmetric channel (BSC) like the private quantum channel (PQC). First, we review some information-theoretical definitions.

If Alice and Bob share n_s bits before reconciliation, this corresponds to knowledge of n_s bits of Shannon information. Let sender Alice's entropy of the whole string be denoted $H(A)$, where $A = \mathbf{X}^n$ is the string of bits sent by her, and where X is the random process defining either 1 or 0. The entropy of a discrete random variable X is defined by

$$H(X) = -\sum_{i=1}^{K} p_i \log_2 p_i, \tag{3}$$

where K is the length of the alphabet and p_i the probability of each symbol. For the binary case when $p_i = 1/2$ and $K = 2$ we have $H(X) = 1$ and $H(A) = n_s$.

Let S denote the knowledge picked up by any receiver (or observer) of the signal on the PQC. Hence, on the receiver's side (or somewhere along the channel) the observed normalized amount of entropy on Alice's sent signal given S, will be $H(X|S)$. If we introduce the probability of an error e on the channel, this conditional entropy follows from the result from a binary symmetric channel and can be written as

$$H(X|S) = h(e) = -e \log_2 e - (1-e) \log_2 (1-e). \tag{4}$$

Thus, given the observed knowledge S we can find the mutual information $I(X;S)$. This is the amount of information provided by S about variable X, i.e. the received information corresponding to the bits sent by Alice. Let us introduce the notation $I_{XY} = I(X;S=Y)$, where Y is the random variable of Bob. From the definition of Shannon information we then have

$$I_{XY} = I(X;Y) = H(X) - H(X|S=Y) = 1 + e \log_2 e + (1-e) \log_2 (1-e). \tag{5}$$

This is the normalized mutual Shannon information between Alice and the observer (preferably Bob) on the sifted key before error correction having an error rate e. Similarly, if $S = B$, where $B = \mathbf{Y}^n$ is Bob's received bit sequence, then we have the shared absolute information between Alice and Bob,

$I_{AB} = n_s I(A;S = B)$. In the same way, if $S = E$ represents the total knowledge picked up by Eve after eavesdropping (received bit string $E = \mathbf{Z}^n$) we have $I_E = n_s I(A;S = E)$. Eve's normalized information is denoted I_Z, where Z is Eve's random variable. The minimum number of exchanged (lost) bits then simply becomes [16]

$$n_{\min} = n_s(1 - I_{XY}) = n_s(-e \log_2 e - (1 - e) \log_2 (1 - e)). \quad (6)$$

In the following discussion, we refer to this limit as the Shannon limit. The objective now for different error-correction methods is to perform as close as possible to this limit. Generally more than $n_{\min}$ bits are lost during reconciliation.

The methods used for error correction in quantum cryptography [17–19] are all variations of a simple error correction method where one compares the parity (XOR) of a subset of both versions of the bit sequence. If the parities are not matching then you know an error occurred, and you proceed with a binary search on that subset with subsequent parity checks to find the error. Recently, in a MSc thesis project [16] we studied in detail a slightly improved version called 'cascade', first presented by Brassard and Salvail in [17]. The cascade method is designed for practical implementations and is not fully optimal. Yet, the capacity is very close to that of noisy channel coding, i.e. the bit loss is close to the value of $n_{\min}$.

The basic idea for cascade is to remember the error location for each error found in one pass, and use this when going back in all previous passes to correct even one more error (figure 6). For every error found a new error will be found and corrected. First we define a pass as the starting point of a new iteration that will

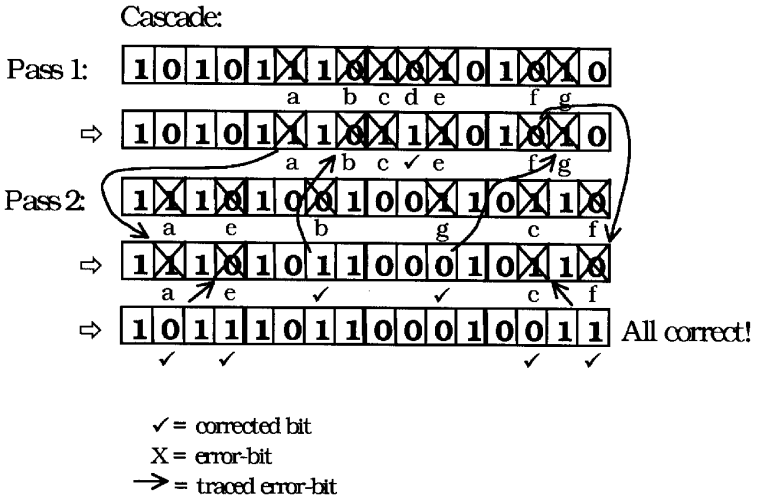

Figure 6. The cascade error correction by binary search and parity disclosure on a chosen sub-block of the key. Error *d* is the only one found and corrected by Binary (a binary search algorithm) in Pass 1. A random permutation of the key is then carried out, prior to entering Pass 2. In this stage two errors, *b* and *g* are found, but now looking for these corrected errors and their positions in the stage of Pass 1, we find two more errors, bit *a* and bit *f* to correct. We can run Binary on the first and the last block in the final stage to correct the last two errors, *e* and *c*.

randomly divide the key in a new set of blocks for further error search. Cascade works in several passes. So, in every pass, each time an error is found in a block, its corresponding error position will also be found in a block of a previous pass. This block was previously left (after binary search) with an even number of errors. Now as the actual error is corrected, this block has an odd number of errors. The binary search is applied on that block again, and one error in the other block can be corrected in the same way. This process is continued until no more errors are found for the pass. In this way pairs of errors are corrected and we can achieve a low bit loss close to the minimum required [16, 17].

3.4. *Estimating Eve's information*

Eve has several possible strategies at her disposal for eavesdropping, such as intercept/resent, beamsplit and quantum non-demolition (QND) attacks. Our objective is to get an upper bound on the expected average amount of information that Eve is in possession of after error- correction. The fraction I_Z is a function of the error rate introduced by Eve. In addition to the following text we refer the reader to [12, 13, 20–22] for more rigorous derivations of the bounds on I_Z as a function of the quantum bit error rate e.

Eve picks up information on both communication channels—in the quantum channel by eavesdropping the photons, and in the public channel by listening to the exchanged parity bits—and uses them to correct her version of the key.

It is hard to exactly estimate the knowledge that Eve might have harvested. However, we can calculate upper bounds on I_Z. We will consider two different simple approaches of eavesdropping, namely, intercept/resent and beamsplit. By straightforward calculations on the amount of normalized information I_Z leaked to Eve when she applies these methods, we arrive at the formula

$$I_Z \mu + 4e/2^{1/2} + 5[(\mu(1 - \mu) + (4 + 2(2^{1/2}))e)/n]^{1/2}, \tag{7}$$

where μ is the intensity of the photons. This expression was derived by Bennett *et al.* [1] in 1992.

However, more recently there have been estimations on I_Z performed more rigorously, with consideration of the many more possible ways of attack (but still restricted to the individual attacks like intercept/resent and beamsplit). For more details see a paper by Lütkenhaus [13]. The fraction of bits learned by Eve with this stringent estimation is

$$I_Z \begin{cases} \log_2(1 + 4e - 4e^2), & \text{for } e \leqslant 1/2, \\ 1, & \text{for } 1/2 \leqslant e. \end{cases} \tag{8}$$

Figure 7 shows a simulation of Eve's collected information using both these estimates together with the reconciliation-method cascade. As mentioned, the simulation is made by Alice generating a random bit string (here 4000 bits), which Bob receives with a given bit rate e. The complete reconciliation protocol is then followed by the software. Alice's and Bob's shared information I_{XY} is plotted as well as Eve's I_Z. In order to extract a final key with length $\geqslant 0$ we have for the early estimate [1] a theoretical maximum allowed error rate of 15% (figure 7). For the stringent estimate [13] the bound is 11.5% (these limits apply both for error

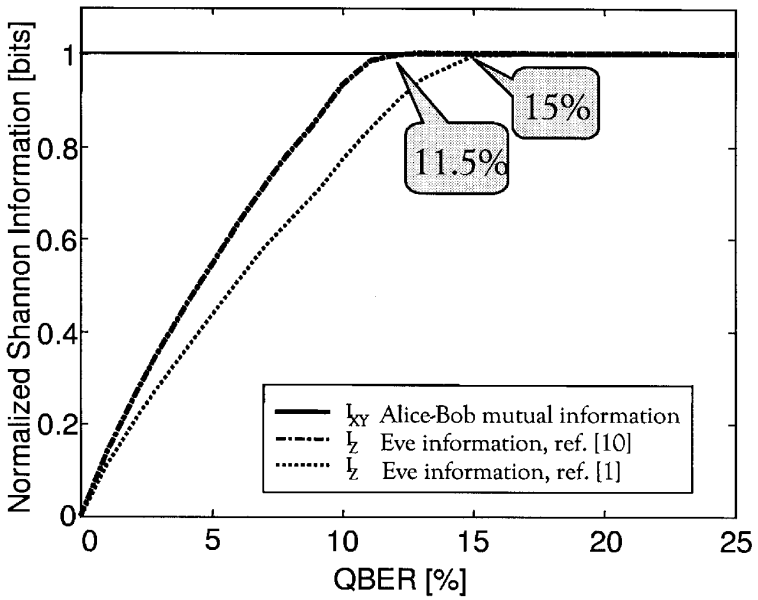

Figure 7. Cascade protocol simulation using the tool developed in [16]. The solid line shows Alice's and Bob's mutual information; it is constant because errors are corrected. Eve's knowledge is consequently increasing with respect to the error rate. At some point the curves meet, and there's no secret information that can be extracted from their key. Two limits, e_{lim}, are achieved, one for each estimate of Eve's information.

correction at the Shannon limit, $n_{\min}$). These plots (using our software simulation) verify the theoretical results obtained [17–19].

When studying figure 7 it is easy to realize that if I_Z becomes larger than I_{XY} further processing (privacy amplification, to be discussed below) cannot be used to decrease Eve's information on the key while still leaving bits for Alice and Bob to use as a key.

3.5. *Privacy amplification*

We now turn our interest to the next step, the privacy amplification, which is a technique to reduce Eve's information on the key to an arbitrarily low amount by compressing the key. Privacy amplification uses so-called universal hash functions, first introduced by Carter and Wegman (1979). Privacy amplification by public discussion was first introduced by Bennett and co-workers [18, 19], see also [23].

Suppose Alice and Bob share a n_e-bit long string A and B after error correction, while the eavesdropper learns at most $t < n_e$ bits of information (Eve's string is E). Note that we expect $t < n_s I_Z$. Alice and Bob now agree on a publicly chosen random compression function f, which Eve also knows. They calculate $f(A)$ respective of $f(B)$ (note that $A = B$), and then take $K = f(A = B)$ to be their new, now n_f-bit long ($n_f < n_e$), shared key after the privacy amplification. The basic idea of privacy amplification is to choose f from a set of hash functions, which randomly redistributes the bits. For a hash function the output bits are a chaotic

permutation of input bits, that is, a small input change will provide a large output change. Hence, if Eve knows the whole key except one bit, then the output will look completely random compared to the output where the input bits are the correct key. In other words, even if Eve knows $f(E)$, she will be left with an arbitrarily small knowledge of the final key $K = f(A = B)$. The amount of compression n_f/n_e depends on the amount of final security sought. The most important result from the theory of privacy amplification is that this final security level will depend only on the chosen value of an extra compression parameter s, called the security parameter, according to the formula [18]

$$I_E \frac{2^{-s}}{\ln 2}, \tag{9}$$

where I_E is Eve's final information. To reach the level of security where Eve knows at most one bit of the final key, the reconciled key has to be compressed only by the amount of information estimated to be in Eve's possession after reconciliation, i.e. $s = 0$. To reach a higher grade of security we have to choose $s > 0$. An arbitrary level of security can be reached by choosing s large enough. This will though provide a larger and less desired compression, i.e. a smaller final key. All this, of course, can be put in a rigorous mathematical basis, see [18, 19, 23].

Let us now estimate the fraction of bits lost in privacy amplification. For a given security parameter s, we are interested in the normalized transmission rate, R_{eff}, telling us how effective our protocol is in keeping bits from the initially received raw bits. For the method of discarding errors, the discard method, the effective bit rate is given by

$$R_{\text{eff}}^{\text{discard}} = (1 - r_s)(I_{XY} + h(e) - r_{\text{ec}}^{\text{discard}} - r_{\text{pa}}^{\text{discard}}(1 - r_{\text{ec}}^{\text{discard}})), \tag{10a}$$

and for the method of correcting errors, the cascade method

$$R_{\text{eff}}^{\text{cascade}} = (1 - r_s)(I_{XY} + h(e) - r_{\text{ec}}^{\text{cascade}} - r_{\text{pa}}^{\text{cascade}}), \tag{10b}$$

r_s is the fraction of bits abandoned in the sifting step

$$r_s = \tfrac{1}{2}, \tag{11}$$

$r_{\text{ec}}^{\text{discard}}$ is the fraction of bits lost in the error correction step [22],

$$r_{\text{ec}}^{\text{discard}} = \tfrac{7}{2}e - e \log_2 e, \tag{12a}$$

at Shannon limit $r_{\text{ec}}^{\text{discard}}$ is expressed as

$$r_{\text{ec}}^{\text{discard}} = h(e), \tag{12b}$$

for the cascade method all errors are corrected and therefore

$$r_{\text{ec}}^{\text{cascade}} = 0. \tag{12c}$$

$h(e)$ and I_{XY} are given by equations (4) and (5) respectively. r_{pa}^{i} (i = discard, cascade) is the fraction of the key to be compressed in the privacy amplification step. Note that for $s > 0$, we lose a fraction $r_{\text{pa}}^{i} = (t + s)/n_e$ of bits in this step, which for $s = 0$ from the theory becomes [13], or according to equation (8)

$$r_{\text{pa}}^{\text{discard}} = \log_2(1 + 4e - 4e^2), \quad \text{for } e < 1/2, \tag{13a}$$

for the cascade method is given by [16, 17]

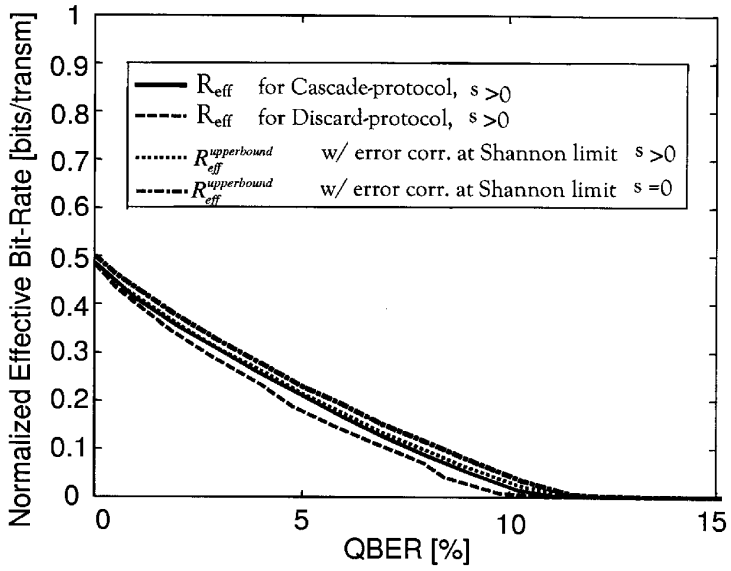

Figure 8. Using the stringent estimate of t, simulations using the software of [16], of the fractions of bits remaining after error correction and privacy amplification gives effective bit rates for discard and cascade protocol. As seen the cascade method works very close to the result for error correction at the theoretical Shannon limit.

$$r_{\mathrm{pa}}^{\mathrm{cascade}} = \log_2(1 + 4e - 4e^2) + 2 + \frac{1 - (1 - 2e)^{0.73}}{2} \log_2\left(\frac{0.73}{e}\right) + \left(0.73 - \frac{1 - (1 - 2e)^{0.73/e}}{2}\right) \log\left(\frac{0.73}{e}\right) \sum_{l=2}^{w} 2^{1-l}, \quad \text{for } e < 1/2, \tag{13 b}$$

and at the Shannon limit $r_{\mathrm{pa}}^{\mathrm{cascade}}$ is expressed as

$$r_{\mathrm{pa}}^{\mathrm{cascade}} = \log_2(1 + 4e - 4e^2) + h(e), \quad \text{for } e < 1/2. \tag{13 c}$$

In figure 8 the results are shown from our simulation tool developed in [16] of the complete key agreement protocol using as a hash function a simple XOR multiplication of the key with a random binary matrix of size $n_e \times n_f$ (n_e and n_f is before and after privacy amplification, respectively). This is an example of the class H_3 universal linear hash functions [17] that requires $n_e \times n_f$ size matrices of random 1:s and 0:s. There are several classes of hash functions to use. Universal hash functions, in general, require $n_e \times 2^{n_f}$ size matrices. Of course computations are made faster with the use of smaller matrices, and there are other classes of hash functions to accomplish this, but the class of linear functions used here are easy to implement. As seen from figure 8, the cascade method performs very close to the theoretical Shannon limit for error correction. Note, however, that a minimum fraction r_{pa} of bits are lost in the privacy amplification step. The larger the error rate, the more bits will be lost in the privacy amplification step, and for large error rates, this is a major reduction in effective transmission rate R_{eff}. From figure 8 we

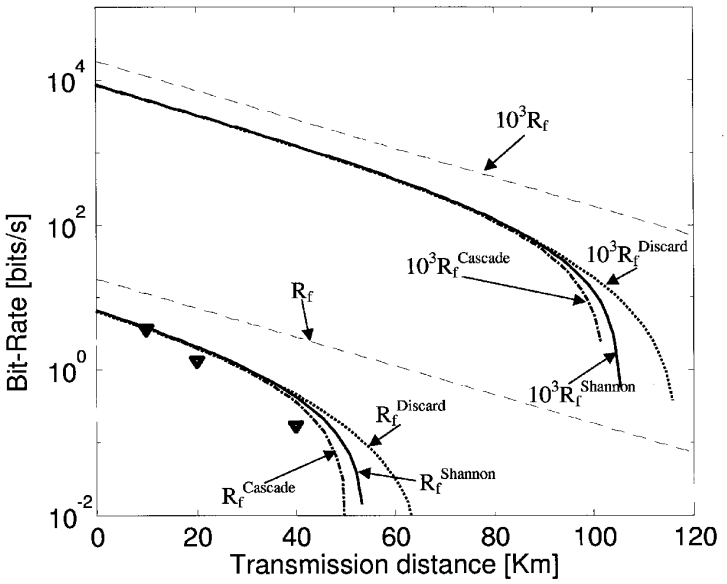

Figure 9. The predicted final key generation rate R_f from equation (14) for our system parameters as a function of the transmission distance L. The marks with error bars are experimentally obtained results presented in figure 4. Both the results for a raw source rate of $R_0 = 1\,\mathrm{kbit\,s^{-1}}$ and dark counts probability 2×10^{-4}, and for $R_0 = 1\,\mathrm{Mbit\,s^{-1}}$ dark count probability per pulse of 2×10^{-5} are shown.

also observe that it is essential to keep the system's bit error rate low, otherwise the transmission rate drops drastically.

4. Putting it all together

Let us now finally combine the experimental results of the quantum transmission with the simulation results from the software system. At the time of writing of the paper (March 1999), these results were separate, but we are currently working towards a systems demonstrator where the software will be using the real data from the transmission. Critical parameters for a quantum cryptography system will be the final key rate R_f given a security parameter, and the transmission distance L. A natural benchmark (similar to that used in conventional fibre optics) would be the capacity $C = R_f L$ (measured in $\mathrm{bit\,s^{-1}} \times \mathrm{km}$). However, the capacity will depend both on transmission distance and the key extraction protocol and will for instance, be a nonlinear function of the transmission distance.

The final key rate R_f can be obtained from the raw rate R_r (equation (1)), and the normalized effective rate R_{eff} (equations (10 *a*) and (10 *b*))

$$R_f = R_r R_{\mathrm{eff}} = \eta\mu 10^{-\alpha L/10} R_0 R_{\mathrm{eff}}. \tag{14}$$

The final key rate decreases due to sifting, error correction and privacy amplification.

In figure 9 we plot the predicted final rate R_f for our system parameters as a function of the transmission distance L. As mentioned, the cascade method performs very close to the Shannon limit of error correction, so we only show the latter in the graph. Note that, even for $L = 0$ and before error correction, the final key rate drops from the source rate by a factor $2/(\eta\mu)$ (about a factor 110 for our system). In figure 9 we show the results both for $R_0 = 1\,\mathrm{kbit\,s^{-1}}$ and dark counts probability 2×10^{-4}, for $R_0 = 1\,\mathrm{Mbit\,s^{-1}}$ dark count probability 2×10^{-5}. Clearly, a high bit-rate system is highly desirable. What should be stressed also is that this chart alone should not be used for the optimization of the system. For instance, it could be desirable to operate the system at a slightly higher quantum efficiency, and therefore higher error rate, say 5% instead of 1%[24]. What is then lost in the key extraction part, can be regained in the increased raw transmission rate. We believe these issues deserve further discussion.

5. Conclusions

In conclusion, we have demonstrated the feasibility of quantum cryptographic systems operating at 1550 nm. Some key results are that InGaAs APD can have sufficient performance to systems, albeit so far our 1550 nm system does not have the same performance as a 1300 nm system. An improvement in detector performance would be highly desirable, and seems reachable. Improving detection electronics, increasing the key rate, and using Peltier cooling of the detector could lead to practical a quantum cryptographic system at 1550 nm for telecom applications capable of 100 km transmission. We have also discussed in detail the key extraction protocol, and in the final section made predictions of the performance of a complete long wavelength quantum cryptography system.

Acknowledgments

We would like to thank J. G. Rarity of DERA Malvern, UK, G. Ribordy, H. Zbinden and N. Gisin of University of Geneva, Switzerland for very valuable technical comments on the experiments, and N. Lütkenhaus of Helsinki University, Finland for very useful discussions on cryptography protocols and eavesdropping issues. This work was supported by the Swedish Technical Science Research Council (TFR) and The Swedish Natural Science Research Council (NFR).

References

[1] Bennett, C. H, Bessette, F., Brassard, G., Salvail, L., and Smolin, J., 1992, *J. Cryptol.*, **5,** 3.
[2] Hughes, R. J., 1997, *Optics Photon. News*, **September,** 9.
[3] Buttler, W. T., Hughes, R. J., Kwiat, P. G., Lamoreaux, S. K., Luther, G., Morgan, G. L., Nordholt, J. E., Peterson, C. G., and Simmons, C. M., 1998, *Phys. Rev. Lett.*, **81**, 3283.
[4] Townsend, P. D., 1997, *Electron. Lett.*, **33,** 188.
[5] Muller, A., Hertzog, T., Huttner, B., Tittel, W., Zbinden, H., and Gisin, N., 1997, *Appl. Phys. Lett.*, **70,** 7.
[6] Ribordy, G., Gautier, J.-D., Gisin, N., Guinnard, O., and Zbinden, H., 1998, *Electron. Lett.*, **34,** 2116.

[7] OWENS, P. C. M., RARITY, J. G., TAPSTER, P. R., KNIGHT, D., and TOWNSEND, P. D., 1994, *Appl. Optics*, **33,** 6895.
[8] COVA, S., GHIONI, M., LACAITA, A., SAMORI, C., and ZAPPA, F., 1996, *Appl. Optics,* **35,** 1956.
[9] GIBSON, F., 1998, MSc thesis, Telia Research AB and Laboratory of Photonics and Microwave Engineering, Department of Electronics, KTH, Sweden.
[10] BOURENNANE, M., GIBSON, F., HENING, A., KARLSSON, A., JONSSON, P., TSEGAYE, T., LJUNGGREN, D., and SUNDBERG, E., 1999, *Optics Express*, **4,** 383.
[11] BENNETT, C. H., 1992, *Phys. Rev. Lett.*, **68,** 3121.
[12] LÜTKENHAUS, N., 1996, *Phys. Rev.* A, **54,** 97.
[13] LÜTKENHAUS, N., 1999, *Phys. Rev.* A, **59,** 3301.
[14] RIBORDNY, G., GAUTHIER, J. D., ZBIBDEN, H., and GISIN, N., 1998, *Appl. Optics*, **37,** 2272.
[15] STINSON, D., 1995, *Cryptography: Theory and Practice* (Boca Raton: CRC Press).
[16] LJUNGGREN, D., 1999, MSc thesis, Laboratory of Photonics and Microwave Engineering, Department of Electronics, KTH, Sweden.
[17] BRASSARD, G., and SALVAIL, L., 1994, *Adventures in Cryptology, Eurocrypt93, Lecture Notes in Computer Science,* Vol. 765 (New York: Springer-Verlag), p. 410.
[18] BENNETT, C. H., BRASSARD, G., and ROBERT, J.-M., 1988, *SIAM J. Comput.*, **17,** 210.
[19] BENNETT, C. H., BRASSARD, G., CREPEAU, C., and MAURER, U. M., 1995, *IEEE Trans. Info. Theory,* **41,** 1915.
[20] SLUTSKY, B., SUN, P-C., MAZURENKO, Y., RAO, R., and FAINMAN, Y., 1997, *J. mod. Optics,* **44,** 953.
[21] SLUTSKY, B., RAO, R., SUN, P-C., and FAINMAN, Y., 1998, *Phys. Rev.* A, **57,** 238.
[22] TANCEVSKI, L., SLUTSKY, B., RAO, R., and FAINMAN, S., 1997, *SPIE*, **3228,** 310.
[23] CASHIN, C., and MAURER, U. M., 1997, *J. Cryptol.*, **10,** 97.
[24] RIBORDY, G., ZBINDEN, H., and GISIN, N., private communication, 1998.

Life only demands from you the strength you possess.
Only one feat is possible - not to have run away.

Dag Hammarskjöld