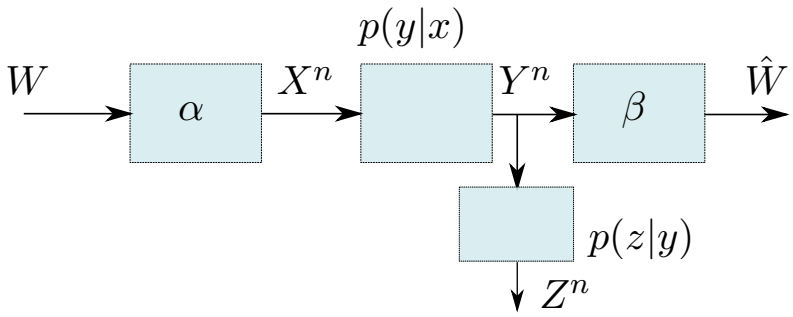
Quantum

Lecture 11

- The classical wiretap channel
- The quantum wiretap channel
- Quantum key distribution

The Classical Wiretap Channel

The degraded wiretap channel



Alice sends a uniformly distributed message $W \in \{1, \ldots, M\}$, coded as $X^n = \alpha(W)$

Bob receives Y^n and decodes $\hat{W} = \beta(Y^n)$

Eve receives Z^n over $p(z^n|x^n) = p(y^n|x^n)p(z^n|y^n)$

The channels are discrete and memoryless, with alphabets $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$

Error probability at Bob

$$P_e^{(n)} = \Pr(\hat{W} \neq W)$$

Normalized information leakage at Eve

$$\frac{1}{n} I(Z^n; W) = \frac{1}{n} \log M - \frac{1}{n} H(W|Z^n)$$

The pair R and Δ is jointly achievable if for any $\varepsilon > 0$ there is an N such that for all $n > N$

$$\frac{1}{n} \log M > R - \varepsilon, \quad P_e^{(n)} < \varepsilon, \quad \frac{1}{n} H(W|Z^n) > \Delta - \varepsilon$$

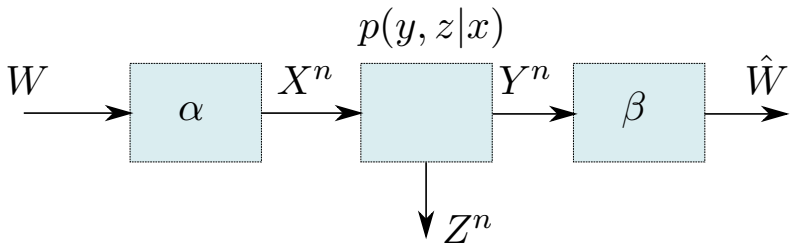
If R is achievable, the maximum possible Δ that is achievable is $\Delta = R$. The secrecy capacity is defined as

$$C_s = \max\{R : R \text{ achievable}, \Delta = R \text{ achievable}\}$$

It holds that

$$C_s = \max_{p(x)} (I(X;Y) - I(X;Z))$$

The general (non-degraded) wiretap channel



$$C_s = \max_{p(x,u)} (I(U;Y) - I(U;Z))$$

The Quantum Wiretap Channel

A quantum channel $\mathcal{R} : \mathcal{A} \to \mathcal{B} \otimes \mathcal{E}$

Assume we have a set of states $\{\rho_{i,j}\}$, $i \in \mathcal{I}_M$, $j \in \mathcal{I}_K$

Alice wishes to convey a uniform message $W \in \mathcal{I}_M = \{1, \ldots, M\}$. For $W = m$ she prepares the state

$$\rho_m = \frac{1}{K} \sum_{k=1}^{K} \rho_{m,k} \in \mathcal{A}^{\otimes n}$$

She then sends this state over n independent uses of $\mathcal{N} = \mathrm{Tr}_{\mathcal{E}}\mathcal{R}$, so that Bob receives $\mathcal{N}^{\otimes n}(\rho_m) \in \mathcal{B}^{\otimes n}$

Eve receives $\sigma_m = \mathcal{M}^{\otimes n}(\rho_m)$ through n uses of $\mathcal{M} = \mathrm{Tr}_{\mathcal{B}}\mathcal{R}$

Let $\sigma = M^{-1} \sum_m \sigma_m$

The pair (R, Δ) is achievable, if there exists a coding scheme such that for any $\varepsilon > 0$ there is an N such that for $n > N$

$$\frac{1}{n} \log M > R - \varepsilon, \quad V(\sigma_m, \sigma) < \Delta, \ m \in \mathcal{I}_M$$

The secrecy capacity is

$$C_{\mathsf{s}} = \max\{R : (R, \Delta) \text{ achievable for any } \Delta > 0\}$$

The private information of a channel $\mathcal{R} : \mathcal{A} \to \mathcal{B} \otimes \mathcal{E}$ is

$$\begin{aligned} \mathcal{P}(\mathcal{N}) &= \max(S(\rho_B) + S(\rho_{XE}) - S(\rho_E) - S(\rho_{XB})) \\ &= \max(S(\rho_X; \rho_B) - S(\rho_X; \rho_E)) \end{aligned}$$

over $\{p(x), \rho_x\}$ in the classical–quantum states

$$\rho_{XA} = \sum_x p(x) |e(x)\rangle\langle e(x)| \otimes \rho_x \in \mathcal{X} \otimes \mathcal{A}$$

$$\rho_{XB} = \sum_x p(x) |e(x)\rangle\langle e(x)| \otimes \mathcal{N}(\rho_x) \in \mathcal{X} \otimes \mathcal{B}$$

$$\rho_{XE} = \sum_x p(x) |e(x)\rangle\langle e(x)| \otimes \mathcal{M}(\rho_x) \in \mathcal{X} \otimes \mathcal{E}$$

with $\mathcal{N} = \mathrm{Tr}_{\mathcal{E}} \mathcal{R}, \ \mathcal{M} = \mathrm{Tr}_{\mathcal{B}} \mathcal{R}, \ \rho_B = \mathrm{Tr}_{\mathcal{X}} \rho_{XB}, \ \rho_E = \mathrm{Tr}_{\mathcal{X}} \rho_{XE}$

Coding theorem for the quantum wiretap channel

$$C_s = \lim_{n\to\infty} \frac{1}{n}\mathcal{P}(\mathcal{R}^{\otimes n})$$

Fanne's inequality: For any densities ρ and σ in d dimensions for which $V(\rho,\sigma) < \varepsilon$ it holds that

$$|S(\rho) - S(\sigma)| \leq 4\varepsilon \log d + 2h(2\varepsilon)$$

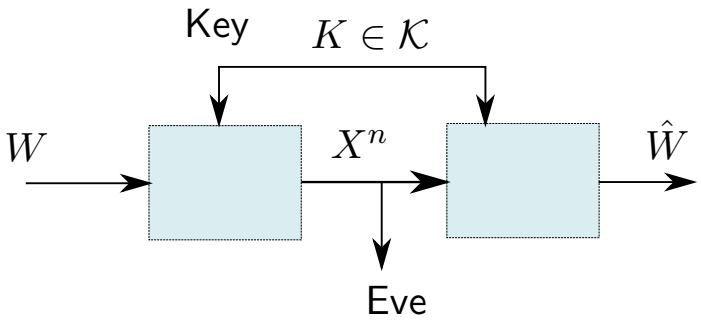
where $h(x) = -x\log x - (1-x)\log(1-x)$

Can be used to prove that

$$V(\sigma_m, \sigma) \to 0 \Rightarrow n^{-1} I(W;\hat{W}) \to 0$$

where $\hat{W}$ is any information about W that Eve can extract from $\mathcal{E}$ $\Rightarrow$ the classical result is essentially a special case of the quantum

The Shannon Cipher System



Perfect secrecy: $H(W|X^n) = H(W)$

Necessary: $H(K) \geq H(W)$

Sufficient: $H(K) = H(W) \Rightarrow$ extract $\log|\mathcal{K}|$ bits and add to W
the one-time pad, or Vernam cipher

A shared key can also be used to improve the secrecy capacity of the wiretap channel, $C_s \to C_s + H(K)$

Quantum Key Distribution

Assume Alice and Bob implement a protocol to share a secret key, encoded as a quantum state

Quantum fact 1: Eve cannot clone the key,
the no-cloning theorem

Quantum fact 2: Eve will always disturb the key,
telling non-orthogonal states apart is not possible without disturbing at least one of them

The Bennet–Brassard '84 (BB84) protocol

Alice generates two uniform and independent classical bits, $x \in \{0,1\}$ and $y \in \{0,1\}$. She wishes to share x with Bob

Alice encodes $xy \to |\psi\rangle \to \rho = |\psi\rangle\langle\psi|$ as

$$00 \to |0\rangle,\ \ 10 \to |1\rangle,\ \ 01 \to |+\rangle,\ \ 11 \to |-\rangle$$

where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$

Bob receives $\mathcal{E}(\rho)$, over a channel that includes Eve's possible interaction

Bob generates a uniform bit $z \in \{0,1\}$, and measures in the $\{|0\rangle, |1\rangle\}$ basis if $z = 0$, or the $\{|\pm 1\rangle\}$ basis if $z = 1$

Alice publicly reveals her bit y

Bob keeps his decoded bit if he finds that $z = y$

Repeat n times

The bits Bob keep can be in error due to the channel and/or Eve's interference

Alice and Bob can agree to publicly compare a fraction δn, $\delta \in (0, 1)$, of the conveyed bits

If their bits disagree in more than τ positions, they abort

Otherwise, they decide to trust the remaining $(1 - \delta)n$ bits

Alice and Bob can use an error-correcting code to improve the quality of the remaining bits

Eve will interfere with about 50% of the bits she decides to look at $\Rightarrow$ for $n \gg 1$ and a high enough δ, Alice and Bob will detect the presence of Eve with high probability

The Bennet '92 (B92) protocol

Alice generates a uniform bit $x \in \{0, 1\}$

If $x = 0$ she sends $|0\rangle$, if $x = 1$ she sends $|+\rangle$

Bob generates a uniform bit $y \in \{0, 1\}$, and measures in $\{|0\rangle, |1\rangle\}$ if $y = 0$, and in $\{|\pm\rangle\}$ if $y = 1$

The result of Bob's measurement is $z \in \{0, 1\}$ ($|0\rangle \to 0$, $|+\rangle \to 0$)

Bob publicly announces the value of z

Alice and Bob repeat many times, and they keep their bits (x, y) only in the cases $z = 1$, since
$x = y \Rightarrow z = 0, \quad y = x + 1 \Rightarrow z$ uniform in $\{0, 1\}$

Each bit in the resulting key is x for Alice, and $y + 1$ for Bob

The EPR protocol

Assume Alice and Bob share n independent copies of the EPR pair

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Using the Bell-CHSH operator $\sigma_1 \otimes (\sigma_1 + \sigma_2) + \sigma_2 \otimes (\sigma_2 - \sigma_1)$, Alice and Bob publicly share the results of their measurements, for a subset of their independent copies

If they find that the Bell inequality is violated in most cases, they conclude that the remaining joint states are (still) entangled, and have therefore not been systematically tampered with $\Rightarrow$ can be trusted to be used for generating a common key

Let $\rho = |\psi\rangle\langle\psi|$, then Alice and Bob share $\rho^n = \rho^{\otimes n}$

Noise and/or Eve's tampering $\Rightarrow$ new state σ^n

If $F(\rho^n, \sigma^n) > 1 - 2^{-s}$ then

$$S(\sigma) < (2n + s + \frac{1}{\ln 2})2^{-s} + O(2^{-2s})$$

The Holevo bound $\Rightarrow$ mutual information leaking to Eve $\leq S(\sigma)$

Thus, if Alice and Bob (by testing Bell's inequality, or by other means) can conclude a lower bound for $F(\rho^n, \sigma^n)$, then they know an upper bound on the information leaking to Eve