Strong Secrecy in Pairwise Key Agreement over a Generalized Multiple Access Channel

Somayeh Salimi, Matthieu Bloch, Frédéric Gabry, Mikael Skoglund, Panos Papadimitratos

Abstract

This paper considers the problem of pairwise key agreement without public communication between three users connected through a generalized multiple access channel (MAC). While two users control the channel inputs, all three users observe noisy outputs from the channel and each pair of users wishes to agree on a secret key hidden from the remaining user. We first develop a "pre-generated" key-agreement scheme based on secrecy codes for the generalized MAC, in which the channel is only used to distribute pre-generated secret keys. We then extend this scheme to include an additional layer of rate-limited secret-key generation by treating the observed channel outputs as induced sources. We characterize inner and outer bounds on the strong secret-key capacity region for both schemes. For a special case of the "pre-generated" scheme, we obtain an exact characterization. We also illustrate with some binary examples that exploiting the generalized nature of the generalized MAC may lead to significantly larger key-agreement rates.

I. Introduction

Key management and key distribution in modern communication networks are becoming increasingly challenging because of the dynamic and heterogenous nature of the networks. Among the proposed solutions to address these challenges, secret-key sharing at the physical layer offers a promising approach to complement traditional public-key and secret-key cryptographic techniques by obviating the need for pre-shared keys. The premise of secret-key sharing at the physical layer is to exploit the randomness in the medium as a resource to generate secret keys, which may then be exploited at the upper layers; one could, for instance, enhance confidentiality, authentication, and integrity of communications.

The canonical information-theoretic models of secret-key agreement have been introduced in [1], [2]. These models consider a situation in which two legitimate terminals, observing the outputs of a noisy source or connected through a noisy channel, attempt to generate a secret key by discussion over a public channel in the presence of

Somayeh Salimi, Mikael Skoglund and Panos Papadimitratos are with ACCESS Linnaeus Center, School of Electrical Engineering, KTH Royal Institute of Technology, Stockholm, Sweden, emails: somayen@kth.se, skoglund@kth.se, papadim@kth.se.

Matthieu Bloch is with School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta GA, USA, email: matthieu.bloch@ece.gatech.edu.

Frédéric Gabry is with the Mathematical and Algorithmic Sciences Lab at the Huawei France Research Center, Paris, France, email: frederic.gabry@huawei.com.

an eavesdropper. These models have since been extended in several directions to analyze situations involving more terminals, e.g., [3], [4], or requiring multiple pairs of keys to be generated, e.g., [5]- [12].

In this paper, we study a three-user model in which two users control the input of a generalized discrete memoryless multiple-access channel (GDMMAC) while all three users observe the outputs of the channel; each pair of users attempts to agree on a secret key concealed from the remaining user. This scenario models, for instance, a noisy environment with honest-but-curious users, in which two users communicate with a base station through the uplink and overhear each other's communications. Each user wishes to share a secret key with the base station hidden from the other user and simultaneously share a secret key with the other user hidden from the base station for their own private communications. Unlike the related work [12], we do not assume that a public channel is available; this allows us to capture some limitations of realistic systems in which communications are inherently rate-limited. In that regard, results and techniques to study secret-key agreement with rate-limited public communication [3] are particularly relevant to the present work. Our key-sharing scenario encompasses most previous works on secret-key agreement between three users; for instance, if we just consider key sharing between the two users controlling the channel inputs, our setting reduces to the problem of key sharing or secret message(s) transmission over two-way channels as in [13]- [16]. If we ignore key sharing between the two users controlling the channel inputs and only consider key sharing between each of these users and the third user simultaneously, our setting reduces to the problem of key sharing or secret message(s) transmission over multiple access channel as in [17].

Specifically, we investigate the performance of two distinct pairwise key sharing schemes. We first study a "pre-generated" key sharing scheme, in which each of the two active users randomly generates keys that are then encoded for secure transmission over the channel. This scheme does not exploit the generalized nature of the MAC, and merely relies on the use of wiretap codebooks combined with rate splitting. We derive inner and outer bounds on the secret-key capacity region (Theorem 1 and Theorem 2), and we identify a special case in which the bounds match (Corollary 1). We then study a "generalized scheme" in which the active terminals also exploit the observations from their noisy channel outputs to generate a key. This scheme extends the "pre-generated" key sharing scheme by combining rate-limited secret key generation with wiretap codebooks and rate splitting. We again establish inner and outer bounds on the secret-key capacity region (Theorem 3 and Theorem 4). We illustrate the performance of both schemes with examples of binary channels that are amenable to numerical calculations (Section III-C and Section IV-B). In particular, these examples show the potential performance gains brought by the extraction of secret keys from channel output observations. Another contribution of this work is to establish strong secrecy results, by leveraging and combining coding techniques for channel resolvability [18], [19] and channel intrinsic randomness [20]–[22]. It should be noted that "pre-generated" key sharing scheme was partially investigated in [23] with weak secrecy constraints.

The remainder of the paper is organized as follows. Section II formally introduces the general model of pairwise key agreement. Section III analyzes the "pre-generated" key-sharing scheme and characterizes its performance. The secret-key capacity region is fully characterized for a special case, and results are illustrated with two examples of binary generalized MAC. Section IV studies the performance of the generalized key-sharing scheme, which is again illustrated with examples. The technical details of most proofs are relegated in the appendices to streamline presentation.

II. Pairwise Secret Key Agreement Model

In this section, we introduce our model for pairwise secret key agreement. As illustrated in Fig. 1, we consider a memoryless generalized MAC $(\mathcal{X}_1, \mathcal{X}_2, P_{Y_1Y_2Y_3|X_1X_2}, \mathcal{Y}_1, \mathcal{Y}_2, \mathcal{Y}_3)$. User 1 and User 2 control the inputs X_1 and X_2, respectively, while Users 1, 2, and 3 observe the outputs Y_1, Y_2, Y_3. respectively. The objective is for each pair of users to share a secret key while keeping it concealed from the remaining user. Formally, a code for pairwise key agreement consists of the following.

- Two randomization sequences $\mathcal{V}_j$ for $j \in \{1, 2\}$, used as sources of local randomness for User 1 and User 2.
- Key sets $\mathcal{K}_{jl} = \{1, \cdots, 2^{nR_{jl}}\}$ for $j < l \in \{1, 2, 3\}$, in which the pairwise keys take values.
- Two sequences of encoding functions $f_j^{(i)} : \mathcal{V}_j \times \mathcal{Y}_j^{i-1} \to \mathcal{X}_j$ for $j \in \{1, 2\}$ and $i \in \{1, \cdots, n\}$ allowing User j, $j \in \{1, 2\}$, to generate channel input X_j^i at time instant i, as a function of a randomization sequence V_j and past observed channel outputs Y_j^{i-1}.
- Key generation functions g_l, $l \in \{1, 2, 3\}$ available at User l

$$g_1 : \mathcal{V}_1 \times \mathcal{Y}_1^n \to \mathcal{K}_{12} \times \mathcal{K}_{13} \tag{1}$$

$$g_2 : \mathcal{V}_2 \times \mathcal{Y}_2^n \to \mathcal{K}_{12} \times \mathcal{K}_{23} \tag{2}$$

$$g_3 : \mathcal{Y}_3^n \to \mathcal{K}_{13} \times \mathcal{K}_{23}. \tag{3}$$

  that allow Users j and l to generate K_{jl} and $\hat{K}_{jl}$, respectively, as the shared key between them for $j < l \in \{1, 2, 3\}$.

Definition 1: A secret-key rate triple (R_{12}, R_{13}, R_{23}) is achievable if for every $\varepsilon > 0$ and all sufficiently large n, we have:

$$\forall j < l \in \{1, 2, 3\} \quad \frac{1}{n} H(K_{jl}) = \frac{1}{n} \log |\mathcal{K}_{jl}| \geq R_{jl} - \epsilon \tag{4}$$

$$\forall j < l \in \{1, 2, 3\} \quad \Pr\{K_{jl} \neq \hat{K}_{jl}\} < \epsilon \tag{5}$$

$$I(K_{12}; Y_3^n) < \epsilon, \text{ and } \forall j \neq \bar{j} \in \{1, 2\} \quad I(K_{j3}; X_{\bar{j}}^n, Y_{\bar{j}}^n) < \epsilon \tag{6}$$

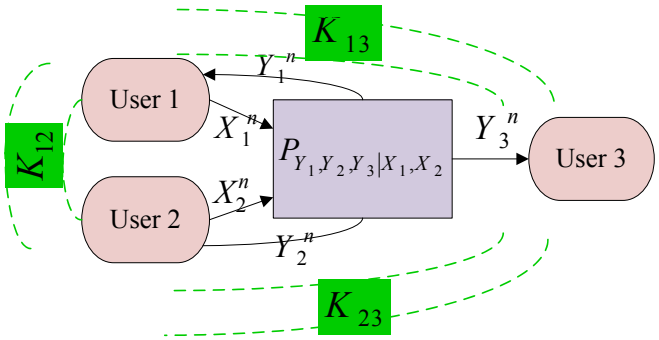


Fig. 1: Pairwise key sharing over GDMMAC

The set of all the achievable secret-key rate triples (R_{12}, R_{13}, R_{23}) is the secret-key capacity region.

Equation (4) means that the rates R_{12}, R_{13} and R_{23} are the rates of nearly uniform secret keys between Users 1 and 2, Users 1 and 3, and Users 2 and 3, respectively. Equation (5) means that each user can correctly estimate the related keys. Equation (6) means that each user effectively has no information about the other users' secret keys. The key rates in Definition 1 are strongly secure since only the total leakage information is bounded by ε. All the above keys take values in some finite sets.

III. The Pre-Generated Keys Scheme of Pairwise Secret Key Agreement over GDMMAC

In this section, we specialize the generic scheme of Section II to a simpler key-sharing scheme, in which the keys are "pre-generated". Specifically, the idea is to have User 1 and User 2 generate keys with their local randomness and then secretly transmit them to the other users without using the generalized feedback.

A. Principle of Pre-Generated Keys Scheme

As illustrated in Fig. 2, the pre-generated key sharing scheme consists of the following simplifications in the generic scheme.

- User 1 uses part of its common randomness to generate local keys $K_{12} \in \mathcal{K}_{12}$ and $K_{13} \in \mathcal{K}_{13}$ to share with Users 2 and 3, respectively. The remaining part is denoted $\widetilde{\mathcal{V}}_1$.
- User 2 uses part of its common randomness to generate local keys $K_{21} \in \mathcal{K}_{21}$ and $K_{23} \in \mathcal{K}_{23}$ to share with Users 1 and 3, respectively. The remaining part is denoted $\widetilde{\mathcal{V}}_2$.
- User 1's deterministic encoding and decoding functions are

$$f_1 : \widetilde{\mathcal{V}}_1 \times \mathcal{K}_{12} \times \mathcal{K}_{13} \to \mathcal{X}_1^n \quad \text{and} \quad g_1 : \mathcal{Y}_1^n \to \mathcal{K}_{21}.$$

- User 2's deterministic encoding and decoding functions are

$$f_2 : \widetilde{\mathcal{V}}_2 \times \mathcal{K}_{21} \times \mathcal{K}_{23} \to \mathcal{X}_3^n \quad \text{and} \quad g_2 : \mathcal{Y}_2^n \to \mathcal{K}_{12}.$$

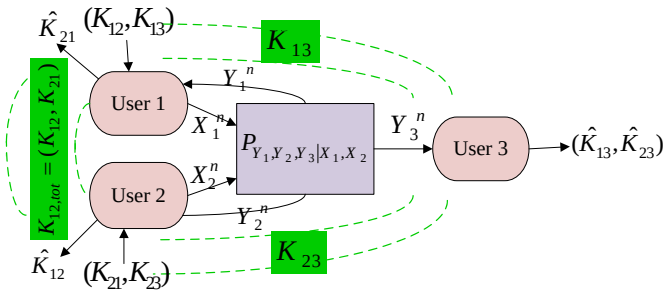


Fig. 2: Pairwise key sharing over GDMMAC using the pre-generated keys scheme

- User 3's deterministic decoding function is

$$g_3 : \mathcal{Y}_3^n \to \mathcal{K}_{13} \times \mathcal{K}_{23}$$

At the end of a transmission, the key pair $K_{12,tot} = (K_{12}, K_{21})$ is shared between User l and User 2, K_{13} is shared between User 1 and User 3, and K_{23} is shared between User 2 and User 3. Note that the shared key between Users 1 and 2 ($K_{12,tot}$) consists of two secret keys and hence, rate R_{12} defined in (4) is the total key rate. This specialization reduces the generic problem to the simpler problem of secret key distribution, and our analysis of this scheme only relies on the use of *wiretap codes*.

B. Main Results

Our main results for the pre-generated key sharing scheme consist of inner and outer bounds on the secret-key capacity region. We first define the following rates:

$$\begin{aligned}
\mathbf{r_{12}} &= [I(S_{12}; X_2, Y_2) - I(S_{12}; Y_3, S_{13}, S_{23})]^+, \\
\mathbf{r_{21}} &= [I(S_{21}; X_1, Y_1) - I(S_{21}; Y_3, S_{13}, S_{23})]^+, \\
\mathbf{I_{12}} &= I(S_{12}; S_{21}|Y_3, S_{13}, S_{23}), \\
\mathbf{r_{13}} &= [I(S_{13}; Y_3|S_{23}) - I(S_{13}; X_2, Y_2, S_{12}|S_{23})]^+, \\
\mathbf{r_{23}} &= [I(S_{23}; Y_3|S_{13}) - I(S_{23}; X_1, Y_1, S_{21}|S_{13})]^+, \\
\mathbf{I_3} &= I(S_{13}; S_{23}|Y_3)
\end{aligned} \tag{7}$$

in which $[x]^+ = \max(x, 0)$.

Theorem 1: In the pre-generated keys scheme, all rate triples in the closure of the convex hull of the set of rate

triples (R_{12}, R_{13}, R_{23}) that satisfy the following conditions are achievable:

$$R_{12} \geq 0, R_{13} \geq 0, R_{23} \geq 0,$$

$$R_{12} \leq \mathbf{r_{12}}+\mathbf{r_{21}} - \mathbf{I_{12}},$$

$$R_{13} \leq \mathbf{r_{13}},$$

$$R_{23} \leq \mathbf{r_{23}},$$

$$R_{13} + R_{23} \leq \mathbf{r_{13}}+\mathbf{r_{23}} - \mathbf{I_3},$$

for random variables taking values in finite sets and with joint distribution factorizing as:

$$p(s_{12},s_{13}, s_{21},s_{23},x_1,x_2,y_1,y_2,y_3) = p(s_{12})p(s_{13})p(s_{21})p(s_{23})p(x_1|s_{12},s_{13})p(x_2|s_{21},s_{23})p(y_1,y_2,y_3|x_1,x_2).$$

The proof of Theorem 1 is actually a special case of the proof of Theorem 3, which may be found in Appendix A. We only provide here a high-level description of the scheme achieving the rate region, which is essentially a combination of wiretap codebooks and rate splitting. The channel model is split into two broadcast channels with confidential messages; one from User 1 to Users 2 and 3 and the other from User 2 to Users 1 and 3, where in each broadcast channel, the receivers are eavesdroppers of each other's key. The rates $\mathbf{r_{12}}$ and $\mathbf{r_{13}}$ correspond to the well known rates of secure communication between Users 1 and 2 and Users 1 and 3, respectively. Similarly, $\mathbf{r_{21}}$ and $\mathbf{r_{23}}$ are the rates of secure communication between Users 2 and 1 and, Users 2 and 3, respectively. The bound on the total key rate between Users 1 and 2 is the sum of the bounds $\mathbf{r_{12}}$ and $\mathbf{r_{21}}$ minus a penalty term $\mathbf{I_{12}}$, which results from the required independence of the transmitted keys. Similarly, the sum rate of the keys to User 3 is the sum rate $\mathbf{r_{13}}+\mathbf{r_{23}}$ penalized by $\mathbf{I_3}$.

Remark 1: If we ignore key sharing between Users 1 and 2, our result reduces to the secrecy rate region of the generalized multiple access channel with confidential messages [17, Corollary 1] by substituting $S_{12} = S_{21} = \emptyset$ in Theorem 1. Similarly, if we ignore key sharing between Users 1 and 3 as well as Users 2 and 3, our result reduces to secret-key sharing in the two-way channel with an external eavesdropper [16, Corollary 1] by substituting $S_{13} = S_{23} = \emptyset$ in Theorem 1.

Theorem 2: In the pre-generated keys scheme, if a key rate triple is achievable, then it belongs to the set of all rate triples (R_{12}, R_{13}, R_{23}) that satisfy:

$$0 \leq R_{12} \leq I(X_1;Y_2|X_2,Y_3)+I(X_2;Y_1|X_1,Y_3)+I(Y_1;Y_2|X_1, X_2,Y_3)+I(X_1;Y_3|X_2,U) - I(X_1;Y_3|U),$$

$$0 \leq R_{13} \leq I(X_1;Y_3|X_2,Y_2),$$

$$0 \leq R_{23} \leq I(X_2;Y_3|X_1,Y_1),$$

for random variables $U, X_1, X_2, Y_1, Y_2, Y_3$, all taking values in finite sets, such that $U-(X_1,X_2)-(Y_1,Y_2,Y_3)$ forms a Markov chain.

Proof: See Appendix D. ■

C. Special Case and Examples

We now investigate a special case of the model in which the inner and outer bounds in Theorems 1 and 2 match, hence providing a complete characterization of the secret-key capacity region.

Corollary 1: When the GDMMAC inputs and outputs form Markov chains as $X_1-(X_2,Y_2)-Y_3-Y_1$ and $X_1-Y_3-X_2$, the secret-key capacity region is

$$\left\{(R_1,R_2):\begin{array}{c} 0\le R_{12}\le I(X_1;Y_2|X_2Y_3),\\ R_{13}=0,\\ 0\le R_{23}\le I(X_2;Y_3|X_1,Y_1)\end{array}\right\} \tag{8}$$

Proof: The achievability can be inferred from Theorem 1 by substituting $S_{12}=X_1, S_{13}=\emptyset, S_{21}=\emptyset, S_{23}=X_2$ and using the Markov chains in the statement of Corollary 1. The converse follows from Theorem 2 since

$$\begin{aligned} I(X_1;Y_2|X_2,Y_3)+I(X_2;Y_1|X_1,Y_3)+I(Y_1;Y_2|X_1,X_2,Y_3)+I(X_1;Y_3|X_2,U)-I(X_1;Y_3|U)& \\ \overset{(a)}{=} I(X_1;Y_2|X_2,Y_3)+I(X_1;Y_3|X_2,U)-I(X_1;Y_3|U),& \\ \overset{(b)}{=} I(X_1;Y_2|X_2,Y_3)+H(X_1|X_2,U)-H(X_1|U,Y_3)-I(X_1;Y_3|U),& \\ \le I(X_1;Y_2|X_2,Y_3),& \end{aligned}$$

and

$$I(X_1;Y_3|X_2,Y_2)\overset{(c)}{=}0.$$

In the above equations (a) and (c) follow from the Markov chain $X_1-(X_2,Y_2)-Y_3-Y_1$ while (b) follows from the Markov chain $X_1-Y_3-X_2$. ■

We now introduce an example in which the Markov chains of Corollary 1 hold. The following lemma turns out to be useful.

Lemma 1: In the pre-generated keys scheme, if two GDMMACs have the same marginal channel transition probability distributions $p(y_1|x_1,x_2)$, $p(y_2|x_1,x_2)$ and $p(y_3|x_1,x_2)$, then they have the same secret-key capacity region.

Since in the pre-generated keys scheme, the channel outputs are not involved in the encoding, Lemma 1 can be proved using the same approach as in [17, Lemma 1].

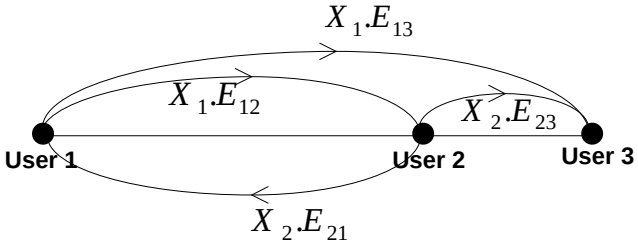


Fig. 3: Erasure Example 1

Example 1: Consider a GDMMAC with inputs alphabet $\{-1, 1\}$ where erased versions of the inputs are received by the users according to Fig. 3 as:

$$Y_1 = X_2 \times E_{21}, \quad Y_2 = X_1 \times E_{12}, \quad Y_3 = (X_1 \times E_{13}, X_2 \times E_{23}),$$

in which E_{ij} takes values in $\{0, 1\}$ with distribution $\Pr(E_{ij} = 0) = p_{ij}$. Operation $\times$ has the usual meaning of multiplication and the random variables $(X_1, X_2, E_{12}, E_{21}, E_{13}, E_{23})$ are independent of each other. In this example, we assume that the channels between Users 1 and 2 are symmetric and hence $p_{12} = p_{21}$ and furthermore $p_{13} \geq p_{12} \geq p_{23}$. Since $p_{13} \geq p_{12}$, User 1 can only share secret key with User 2 and hence, in Theorem 1, we set $S_{13} = \emptyset$ and $S_{12} = X_1$ where X_1 is uniformly distributed over $\{-1, 1\}$. On the other hand, since $p_{12} \geq p_{23}$, User 2 dedicates the whole channel input to share a secret key with User 3 by substituting $S_{21} = \emptyset$ and $S_{23} = X_2$ where X_2 is uniformly distributed over $\{-1, 1\}$. By substituting the auxiliary random variables in Theorem 1 as described above, we obtain the following achievable secret-key rate region:

$$\left\{ (R_1, R_2) : \begin{array}{l} 0 \leq R_{12} \leq p_{13} - p_{12}, \\ R_{13} = 0, \\ 0 \leq R_{23} \leq p_{12} - p_{23}. \end{array} \right\} \tag{9}$$

We now use Lemma 1 to show that the rate region in (10) is the capacity region. Consider a new GDMMAC with channel outputs y_1, y_2', y_3' at Users 1, 2 and 3, respectively, where

$$Y_1 = X_2 \times E_{21}, \quad Y_2' = X_1 \times E_{12}', \quad Y_3' = (X_1 \times E_{13}, X_2 \times E_{23}'),$$

in which E_{21} and E_{13} are the erasure random variables in Example 1 and E_{12}' and E_{23}' are erasure random variables with erasure probabilities p_{12} and p_{23}, respectively. E_{21} and E_{13} are correlated with E_{12}' and E_{23}' according to Fig. 4. It can be shown that the following relationships hold between the new channel outputs

$$Y_1 = X_2 \times E_{23}' \times E_x, \quad Y_2' = X_1 \times E_{12}', \quad Y_3' = (Y_2' \times E_y, X_2 \times E_{23}').$$

The new channel outputs satisfy the Markov chains of Corollary 1 (replacing Y_2 and Y_3 with Y_2' and Y_3'). Therefore,

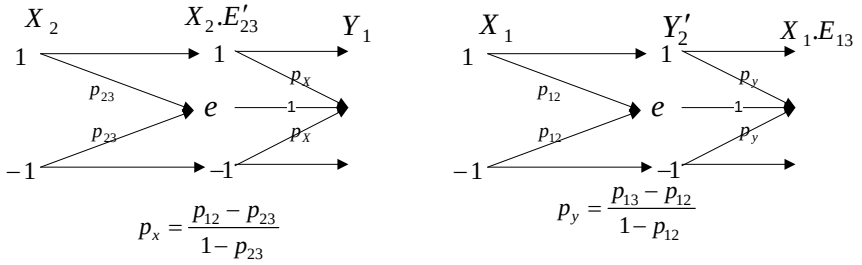


Fig. 4: New erasure channel outputs relationships in Example 1

the secret-key capacity region of the new channel is

$$\left\{ (R_1, R_2): \begin{array}{l} 0 \le R_{12} \le p_{13} - p_{12}, \\ R_{13} = 0, \\ 0 \le R_{23} \le p_{12} - p_{23}. \end{array} \right\} \tag{10}$$

Since Y'_2 and Y'_3 have the same marginal distributions as y_2 and y_3, respectively, according to Lemma 1, the original channel has the same secret-key capacity region as the new channel and hence, the secret-key capacity region in (10) is the capacity region.

Example 2: Consider a binary GDMMAC where the relationships between the channel inputs and outputs are according to:

$$Y_i = X_1 + X_2 + Z_i \qquad i = 1, 2, 3,$$

in which Z_i is a binary random variable with distribution $\Pr(Z_i = 1) = p_i$. Operation $+$ is the binary summation and the random variables $(X_1, X_2, Z_1, Z_2, Z_3)$ are independent of each other. We assume that $0 \le p_2 \le p_3 \le p_1 \le 0.5$. The other cases can be similarly considered. At first glance, it may seem that because of $p_2 \le p_3$, the best strategy for User 1 is to set $S_{12} = X_1, S_{13} = \emptyset$ where X_1 is uniformly distributed over $\{0, 1\}$. This is the best strategy for User 1 to maximize his secret key rate R_{12}, but it would result in $R_{23} = 0$ since X_1 is uniformly distributed over $\{0, 1\}$ and hence $I(S_{23}; Y_3) = 0$. Based on this argument, we assume that X_1 is a binary random variable with parameter α where $0 \le \alpha \le 0.5$. On the other hand, if User 2 sets $S_{21} = \emptyset, S_{23} = X_2$ with X_2 uniformly distributed over $\{0, 1\}$, the maximum rate of R_{23} will be achievable, however it decreases R_{12} since User 3 decodes X_2 and the leakage rate $I(S_{12}; Y_3, S_{23})$ in the expression of R_{12} will increase. Hence, we assume S_{23} be a binary random variable connected to X_2 by another binary symmetric channel with parameter β, as in Fig. 5 where $0 \le \beta \le 0.5$. By substituting the auxiliary random variables in Theorem 1 as described, the following rate region is achievable:

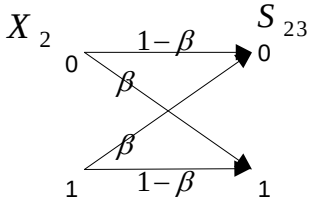


Fig. 5: Auxiliary random variable S_{23} in Example 2

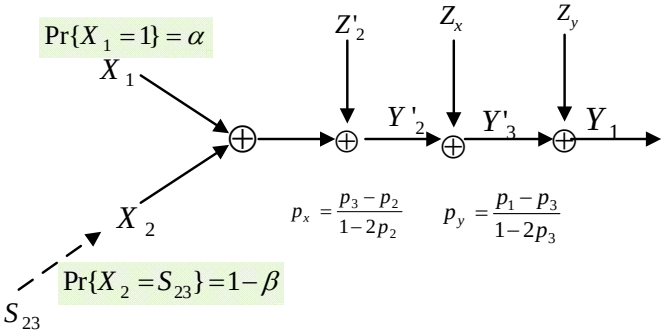


Fig. 6: New channel outputs relationships in Example 2

$$
\begin{aligned}
&R_{12} \leq h(\alpha * p_2) + h(\beta * p_3) - h(\alpha * \beta * p_3) - h(p_2),\\
&R_{13} = 0,\\
&R_{23} \leq h(\beta * p_1) - h(\beta * \alpha * p_3)
\end{aligned} \tag{11}
$$

for all values of $0 \leq \alpha, \beta \leq 0.5$, where

$$\alpha * \beta \triangleq \alpha(1-\beta) + \beta(1-\alpha) \tag{12}$$

$$h(p) \triangleq -p \log p - (1-p)\log(1-p) \tag{13}$$

To derive the outer bound on the secret-key capacity region, we use Lemma 1 as in Example 1 to introduce stochastic degradedness. Since $0 \leq p_2 \leq p_3 \leq p_1 \leq 0.5$, we define a new channel with the same marginal distributions as in Example 2 where:

$$
\begin{aligned}
&Y_2' = X_1 + X_2 + Z_2',\\
&Y_3' = X_1 + X_2 + Z_2' + Z_x,\\
&Y_1 = X_1 + X_2 + Z_2' + Z_x + Z_y = X_1 + X_2 + Z_1,
\end{aligned}
$$

in which Z_2' has the same distribution as Z_2 and Z_x and Z_y are binary random variables with distributions $\Pr(Z_x = 1) = p_x, \Pr(Z_y = 1) = p_y$ where p_x and p_y are defined as in Fig. 6. The random variables (Z_2', Z_x, Z_y) are independent of each other.

The Markov chain $(X_1, X_2) - Y_2' - Y_3' - Y_1$ holds between the new channel inputs and outputs and the following region is an outer bound on the secret-key capacity region of the new channel:

$$R_{12} \leq 1 - h(p_2), \qquad R_{13} = 0, \qquad R_{23} \leq h(p_1) - h(p_3) \tag{14}$$

where the upper bounds on R_{13} and R_{23} are directly inferred from Theorem 2 by considering the Markov chain $(X_1, X_2) - Y_2' - Y_3' - Y_1$. To deduce the upper bound on R_{12}, using Theorem 2, we have:

$$\begin{aligned}
R_{12} &\leq I(X_1;Y_2'|X_2,Y_3') + I(X_2;Y_1|X_1,Y_3') + I(Y_1;Y_2'|X_1,X_2,Y_3') + I(X_1;Y_3'|X_2,U) - I(X_1;Y_3'|U) \\
&\overset{(a)}{=} I(X_1;Y_2'|X_2,Y_3') + I(X_1;Y_3'|X_2,U) - I(X_1;Y_3'|U) \\
&\leq I(X_1;Y_2'|X_2,Y_3') + I(X_1;Y_3'|X_2,U) \\
&\overset{(b)}{=} I(X_1;Y_2'|X_2,Y_3') + H(Y_3'|X_2,U) - H(Y_3'|X_1,X_2) \\
&\leq I(X_1;Y_2'|X_2,Y_3') + I(X_1;Y_3'|X_2) \\
&= I(X_1;Y_2',Y_3'|X_2) \\
&\overset{(c)}{=} I(X_1;Y_2'|X_2)
\end{aligned}$$

where (a) and (c) are deduced from the Markov chain $(X_1, X_2) - Y_2' - Y_3' - Y_1$ and (b) from the distribution of U. Since the new channel and the original channel have the same marginal distributions, then the outer bound in (14) holds for the original channel.

The rate region (R_{23}, R_{12}) in (11) along with the outer bound in (14) are shown in Fig. 7 for different values of p_1, p_2 and p_3. In addition, the rate region in (11) is compared with the rate region obtained from the time sharing between Users 1 and 2.

IV. The Generalized Scheme of Pairwise Secret Key Agreement over GDMMAC

We now analyze the "generalized key sharing" scheme, in which the channel outputs allowed by the generalized feedback are used as induced sources for key generation. In contrast to the pre-generated keys scheme in Section III, the channel outputs at Users 1 and 2 are used as inputs to the encoders and hence, the channel inputs are stochastic functions of not only the pre-generated keys but also the previous channel outputs. The encoding and decoding functions refer to those introduced in Section II. In the generalized scheme, key sharing is achieved in two stages so that the final key K_{ij} shared between User i and User j for $i < j \in \{1, 2, 3\}$ is composed of two sub-keys; a randomly pre-generated key randomly produced by User i and another key generated as a stochastic function of the received channel output Y_i^n at user i. This procedure is performed over multiple blocks of n channel uses, and the detailed achievable scheme is given in the following subsection.

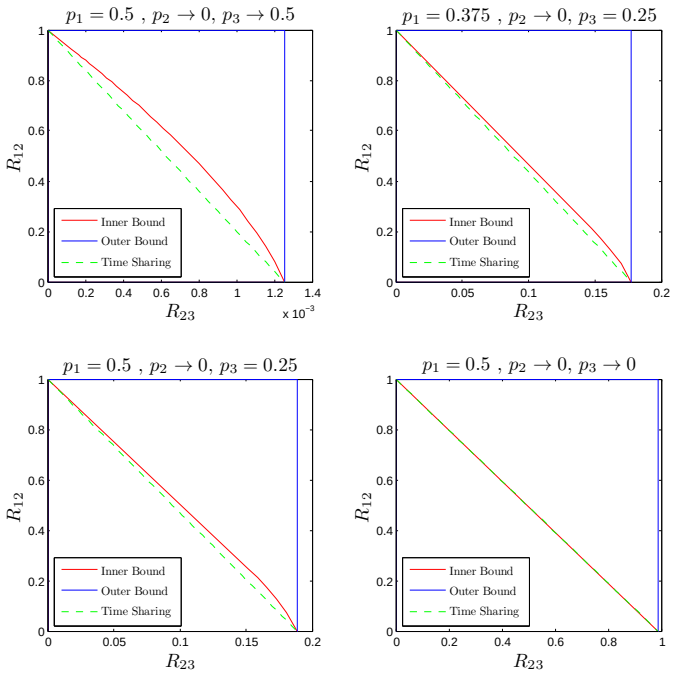


Fig. 7: Comparison of the bounds for different values of p_1, p_2 and p_3 in Example 2

A. Main Results

We first define the following rates:

$$\mathbf{r_{12,p}} = [I(S_{12}; X_2, Y_2) - I(S_{12}; Y_3, S_{13}, S_{23}, T_{13}, T_{23})]^+,$$

$$\mathbf{r_{21,p}} = [I(S_{21}; X_1, Y_1) - I(S_{21}; Y_3, S_{13}, S_{23}, T_{13}, T_{23})]^+,$$

$$\mathbf{I_{12,p}} = I(S_{12}; S_{21}|Y_3, S_{13}, S_{23}, T_{13}, T_{23}),$$

$$\mathbf{r_{13,p}} = [I(S_{13}; Y_3|S_{23}) - I(S_{13}; X_2, Y_2, S_{12}, T_{12}|S_{23})]^+,$$

$$\mathbf{r_{23,p}} = [I(S_{23}; Y_3|S_{13}) - I(S_{23}; X_1, Y_1, S_{21}, T_{21}|S_{13})]^+,$$

$$\mathbf{I_{3,p}} = I(S_{13}; S_{23}|Y_3)$$

$$\mathbf{r_{12,s}} = [I(T_{12}; X_2, Y_2|S_{12}, S_{21}) - I(T_{12}; Y_3, S_{13}, S_{23}, T_{13}, T_{23}|S_{12}, S_{21})]^+,$$

$$\mathbf{r_{21,s}} = [I(T_{21}; X_1, Y_1|S_{12}, S_{21}) - I(T_{21}; Y_3, S_{13}, S_{23}, T_{13}, T_{23}|S_{12}, S_{21})]^+,$$

$$\mathbf{I_{12,s}} = I(T_{12}; T_{21}|Y_3, S_{13}, S_{23}, T_{13}, T_{23}, S_{12}, S_{21}),$$

$$\mathbf{r_{13,s}} = [I(T_{13}; Y_3|S_{13}, S_{23}, T_{23}) - I(T_{13}; X_2, Y_2, S_{12}, T_{12}|S_{13}, S_{23}, T_{23})]^+,$$

$$\mathbf{r_{23,s}} = [I(T_{23}; Y_3|S_{13}, S_{23}, T_{13}) - I(T_{23}; X_1, Y_1, S_{21}, T_{21}|S_{13}, S_{23}, T_{13})]^+,$$

$$\mathbf{I_{3,s}} = I(T_{13}; T_{23}|Y_3, S_{13}, S_{23}) \tag{15}$$

Theorem 3: In the generalized scheme, all rate triples in the closure of the convex hull of the set of rate triples (R_{12}, R_{13}, R_{23}) that satisfy the following conditions are achievable:

$$
\begin{aligned}
&R_{12} \geq 0, R_{13} \geq 0, R_{23} \geq 0,\\
&R_{12} \leq [\mathbf{r_{12,p}} + \mathbf{r_{21,p}} - \mathbf{I_{12,p}}]^+ + [\mathbf{r_{12,s}} + \mathbf{r_{21,s}} - \mathbf{I_{12,s}}]^+,\\
&R_{13} \leq \mathbf{r_{13,p}} + \mathbf{r_{13,s}},\\
&R_{23} \leq \mathbf{r_{23,p}} + \mathbf{r_{23,s}},\\
&R_{13} + R_{23} \leq [\mathbf{r_{13,p}}+\mathbf{r_{23,p}} - \mathbf{I_{3,p}}]^+ + [\mathbf{r_{13,s}}+\mathbf{r_{23,s}} - \mathbf{I_{3,s}}]^+,
\end{aligned}
$$

for random variables taking values in finite sets and with joint distribution factorizing as:

$$
\begin{aligned}
&p(s_{12},s_{13},s_{21},s_{23},t_{12},t_{13},t_{21},t_{23},x_1,x_2,y_1,y_2,y_3) = p(s_{12})p(s_{13})p(s_{21})p(s_{23})p(x_1|s_{12},s_{13})p(x_2|s_{21},s_{23})\\
&p(y_1,y_2,y_3|x_1,x_2)p(t_{12}|x_1,y_1,s_{12})p(t_{13}|x_1,y_1,s_{13})p(t_{21}|x_2,y_2,s_{21})p(t_{23}|x_2,y_2,s_{23}) \qquad (16)
\end{aligned}
$$

and subject to the constraints:

$$
\begin{aligned}
&I(T_{12}; X_1, Y_1|X_2, Y_2, S_{12}, S_{21}) \leq I(S_{12}; X_2, Y_2),\\
&I(T_{13}; X_1, Y_1|Y_3, S_{13}, S_{23}, T_{23}) \leq I(S_{13}; Y_3|S_{23}),\\
&I(T_{21}; X_2, Y_2|X_1, Y_1, S_{12}, S_{21}) \leq I(S_{21}; X_1, Y_1),\\
&I(T_{23}; X_2, Y_2|Y_3, S_{13}, S_{23}, T_{13}) \leq I(S_{23}; Y_3|S_{13}),\\
&I(T_{13}, T_{23}; X_1, Y_1, X_2, Y_2|Y_3, S_{13}, S_{23}) \leq I(S_{13}, S_{23}; Y_3) \qquad (17)
\end{aligned}
$$

The proof of Theorem 3 is given in Appendix A. Note that each individual rate bound consists of two parts: a primary rate (denoted by subscript "p") and a secondary rate (denoted by subscript "s"). This split reflect the two-step key generation process behind the achievability proof. The primary rates are associated with the pre-generated keys randomly generated and sent by Users 1 and 2 through the channel, as in Theorem 1. The secondary rates are generated by Users 1 and 2 after receiving the channel outputs, which are exploited as induced sources to generate additional keys. Intuitively, the form of the bound for R_{12} originates from the two-way channel between Users 1 and 2 in which User 3 acts as an external eavesdropper. Similarly, the form of the bounds for R_{13} and R_{23} stems from the generalized MAC from Users 1 and 2 to User 3, in which Users 1 and 2 eavesdrop each other. For the secondary keys, a combination of secret sharing codebooks and superposition coding is used at Users 1 and 2 as well as random binning based on Probability Mass Function (PMF) approximation arguments [25]. Finally, note that the constraints in (17) reflect the absence of public channel, sot that all the required information to reconstruct

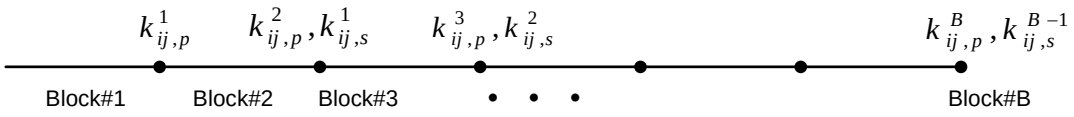


Fig. 8: Key sharing scheme associated with Theorem 3

the secondary keys should be sent through noisy channels.

This procedure is performed over multiple blocks. At each block, by n uses of the channel, each of Users 1 and 2 encodes pre-generated keys (primary keys) plus the secondary keys induced from the channel outputs received at the end of the previous block. In Theorem 3, S_{ij} and T_{ij} are the auxiliary random variables relevant to the primary and secondary keys $K_{ij,p}$ and $K_{ij,s}$, respectively, which are generated by User i to be shared with User j where $i \in \{1,2\}$, $j \in \{1,2,3\}$ and $i \neq j$.

A simple illustration of the encoding is shown in Fig. 8. The primary key $k^1_{ij,p}$ is randomly generated to be shared between Users i and j in the first block of n channel uses. At the end of the first block, by receiving the corresponding outputs, the secondary key of the first block $k^1_{ij,s}$ is generated as a stochastic function of the received outputs to be shared between Users i and j. The required information of the secondary key is sent through n channel uses in the second block along with the required information of the second block primary key, i.e., $k^2_{ij,p}$ which is generated randomly and independently of the first block secondary key. The constraints in (17) reflect this fact. In this scheme, the secondary key $k^1_{ij,s}$ is decoded and shared between Users i and j at the end of the second block in addition to the primary key of the second block $k^2_{ij,p}$. The same procedure is performed B blocks. Assuming $r_{ij,p}$ and $r_{ij,s}$ be the rates of the primary and secondary keys, respectively, the total rate of the shared key between Users i and j at the end of block B is:

$$\bar{R}_{ij} = \frac{nBr_{ij,p} + n(B-1)r_{ij,s}}{nB}$$

which is approximately equal to $r_{ij,p} + r_{ij,s}$ if B is large enough.

Remark 2: The auxiliary random variables S_{12} and S_{13} (resp. S_{21} and S_{23}) could be made dependent in (16). If this were the case, additional constraints should be added to (17) according to Marton's bound for the broadcast channel from User 1 to Users 2 and 3 (resp. from User 2 to Users 1 and 3). For the sake of simplicity, we assume that S_{12} and S_{13} (resp. S_{21} and S_{23}) are independent.

Remark 3: If we cancel the secondary keys generation by setting $T_{12} = T_{13} = T_{21} = T_{23} = \emptyset$ in Theorem 3, then the rate region reduces to the one in Theorem 1.

Theorem 4: In the generalized scheme, if a key rate triple is achievable, then it belongs to the set of all rate

triples (R_{12}, R_{13}, R_{23}) that satisfy:

$$0 \leq R_{12} \leq I(X_1;Y_2|X_2,Y_3)+I(X_2;Y_1|X_1,Y_3)+I(Y_1;Y_2|X_1,X_2,Y_3)+I(X_1;Y_3|X_2,U)-I(X_1;Y_3|U),$$
$$0 \leq R_{13} \leq I(X_1, Y_1; Y_3|X_2, Y_2),$$
$$0 \leq R_{23} \leq I(X_2, Y_2; Y_3|X_1, Y_1),$$

for random variables $U, X_1, X_2, Y_1, Y_2, Y_3$, all taking values in finite sets, such that $U - (X_1, X_2) - (Y_1, Y_2, Y_3)$ forms a Markov chain.

Proof: See Appendix E. ■

B. A Binary Example

In this section, we discuss a binary example to illustrate the benefits of the generalized scheme. To clarify the effect of involving the channel outputs in the pairwise key sharing, we modify Example 2 in such a way that the binary noises received over the channel are correlated and hence, given the channel inputs, the channel outputs can be considered as correlated sources.

Example 3: Consider a binary GDMMAC where the relationships between the channel inputs and outputs are according to:

$$Y_1 = X_1 + X_2 + Z_1 + Z_2 + Z_3,$$
$$Y_2 = X_1 + X_2 + Z_2,$$
$$Y_3 = X_1 + X_2 + Z_2 + Z_3,$$

in which Z_1, Z_2 and Z_3 are binary random variables with distributions $\Pr(Z_i = 1) = p_i$ where $0 < p_i \leq 0.5$ for $i = 1, 2, 3$. Operation $+$ is binary summation and the random variables $(X_1, X_2, Z_1, Z_2, Z_3)$ are independent of each other. In this example, there is a physical degradedness in the channel and the Markov chain $(X_1, X_2) - Y_2 - Y_3 - Y_1$ holds between the channel inputs and outputs. Since the received noises over the channel are not independent, the channel outputs have the role of correlated sources to produce the secondary keys. In particular, because of the Markov chain $Y_2 - Y_3 - Y_1$ between the channel outputs, Users 1 and 2 can, respectively, share secondary keys $K_{13,s}$ and $K_{23,s}$ with User 3 but they cannot share any secondary key with each other, i.e., $K_{12,s} = K_{21,s} = \emptyset$. Since the required information of secondary key $K_{13,s}$ should be sent through the channel form User 1 to User 3, we can not set $S_{13} = \emptyset$ as in Example 2. We change the auxiliary random variables of the pre-generated keys scheme in Example 2 such that $X_1 = S_{12} + S_{13}$ where $\Pr(S_{12} = 1) = \alpha$ and $\Pr(S_{13} = 1) = \alpha'$. The auxiliary random variables S_{21} and S_{23} are substituted the same as in Example 2, i.e., $S_{21} = \emptyset$ and $\Pr\{S_{23} = X_2\} = 1 - \beta$,

where $X_2 = Ber(0.5)$.

For the secondary key generation, Users 1 and 2, respectively, consider auxiliary random variables T_{13} and T_{23} to share secret keys with User 3 and set $T_{12} = T_{21} = \emptyset$ since they can not share a secondary key between themselves due to Markov chain $Y_2 - Y_3 - Y_1$. According to the constraints in (17), noisy versions of the channel outputs at Users 1 and 2 are considered as auxiliary random variables of the secondary keys, i.e., $T_{13} = Y_1 + Z_1', T_{23} = Y_2 + Z_2'$ where Z_1' and Z_2' are independently binary noises such that $\Pr(Z_1' = 1) = \alpha''$ and $\Pr(Z_2' = 1) = \beta'$. By substituting the auxiliary random variables in Theorem 3 as described, the following key rate region is achievable:

$$\begin{aligned}
&R_{12} \leq [h_x - h_y - h(\alpha' * p_2) + h(\alpha * \alpha' * p_2)]^+, \\
&R_{13} \leq h(p_1 * p_3 * \alpha'') - h(p_1 * \alpha''), \\
&R_{23} \leq [h(\beta * p_1 * p_2 * p_3) - h(\alpha * \beta * p_2 * p_3)]^+ + \\
&\qquad [h_z - h_y + h(\alpha * \beta * p_2 * p_3) - h(\beta * p_1 * p_2 * p_3)]^+
\end{aligned} \tag{18}$$

subject to:

$$\begin{aligned}
&h(\alpha'' * p_1) - h(\alpha'') \leq h(\alpha * \alpha' * \beta * p_2 * p_3) - h(\alpha * \beta * p_2 * p_3), \\
&h(\alpha'' * p_1) - h(\alpha'') + h_y - h(\beta') \leq 1,
\end{aligned}$$

where h_x,h_y and h_z are defined as:

$$\begin{aligned}
&h_x = f(\beta * p_2, p_3, \beta'), \\
&h_y = f(\alpha * \beta * p_2, p_3, \beta'), \\
&h_z = f(\beta * p_2, p_1 * p_3, \beta'), \\
&f(a,b,c) = -(abc + \bar{a}\bar{b}\bar{c}) \log(abc + \bar{a}\bar{b}\bar{c}) \\
&-(a\bar{b}c + \bar{a}b\bar{c}) \log(a\bar{b}c + \bar{a}b\bar{c}) \\
&-(ab\bar{c} + \bar{a}\bar{b}c) \log(ab\bar{c} + \bar{a}\bar{b}c) \\
&-(a\bar{b}\bar{c} + \bar{a}bc) \log(a\bar{b}\bar{c} + \bar{a}bc),
\end{aligned}$$

for all values of $0 \leq \alpha, \alpha', \alpha'', \beta, \beta', \leq 0.5$.

In the above equations $\overline{p} = 1 - p$ and, operations $*$ and $h(.)$ are defined the same as in (12) and (13).

If we substitute $S_{13} = T_{13} = T_{23} = \emptyset$ in Example 3 or equivalently $\alpha'' = \beta' = 0.5$ and $\alpha' = 0$ in rate region

(18), then the rate region of the pre-generated keys scheme is deduced as:

$$\begin{aligned} R_{12} &\leq [h(\beta * p_2 * p_3) - h(\alpha\beta * p_2 * p_3) - h(\alpha' * p_2) + h(\alpha * \alpha' * p_2)]^+, \\ R_{13} &= 0, \\ R_{23} &\leq [h(\beta * p_1 * p_2 * p_3) - h(\alpha * \beta * p_2 * p_3)]^+. \end{aligned} \tag{19}$$

The following region is an outer bound of the secret-key capacity region for the generalized scheme in Example 3:

$$\begin{aligned} R_{12} &\leq 1 - h(p_2), \\ R_{13} &\leq h(p_1 * p_3) - h(p_1), \\ R_{23} &\leq h(p_1 * p_3) - h(p_3) \end{aligned} \tag{20}$$

which is directly deduced from Theorem 4 since we have:

$$\begin{aligned} R_{12} &\leq I(X_1;Y_2|X_2,Y_3) + I(X_2;Y_1|X_1,Y_3) + I(Y_1;Y_2|X_1,X_2,Y_3) + I(X_1;Y_3|X_2,U) - I(X_1;Y_3|U), \\ &\overset{(a)}{=} I(X_1;Y_2|X_2,Y_3) + I(X_1;Y_3|X_2,U) - I(X_1;Y_3|U) \\ &\leq I(X_1;Y_2|X_2,Y_3) + I(X_1;Y_3|X_2,U), \\ &= I(X_1;Y_2|X_2,Y_3) + H(Y_3|X_2,U) - H(Y_3|X_1,X_2,U) \\ &\leq I(X_1;Y_2|X_2,Y_3) + H(Y_3|X_2) - H(Y_3|X_1,X_2,U), \\ &\overset{(b)}{=} I(X_1;Y_2|X_2,Y_3) + H(Y_3|X_2) - H(Y_3|X_1,X_2), \\ &= I(X_1;Y_2|X_2,Y_3) + I(X_1;Y_3|X_2) = I(X_1;Y_2,Y_3|X_2), \\ &\overset{(c)}{=} I(X_1;Y_2|X_2) \leq 1 - h(p_2), \end{aligned}$$

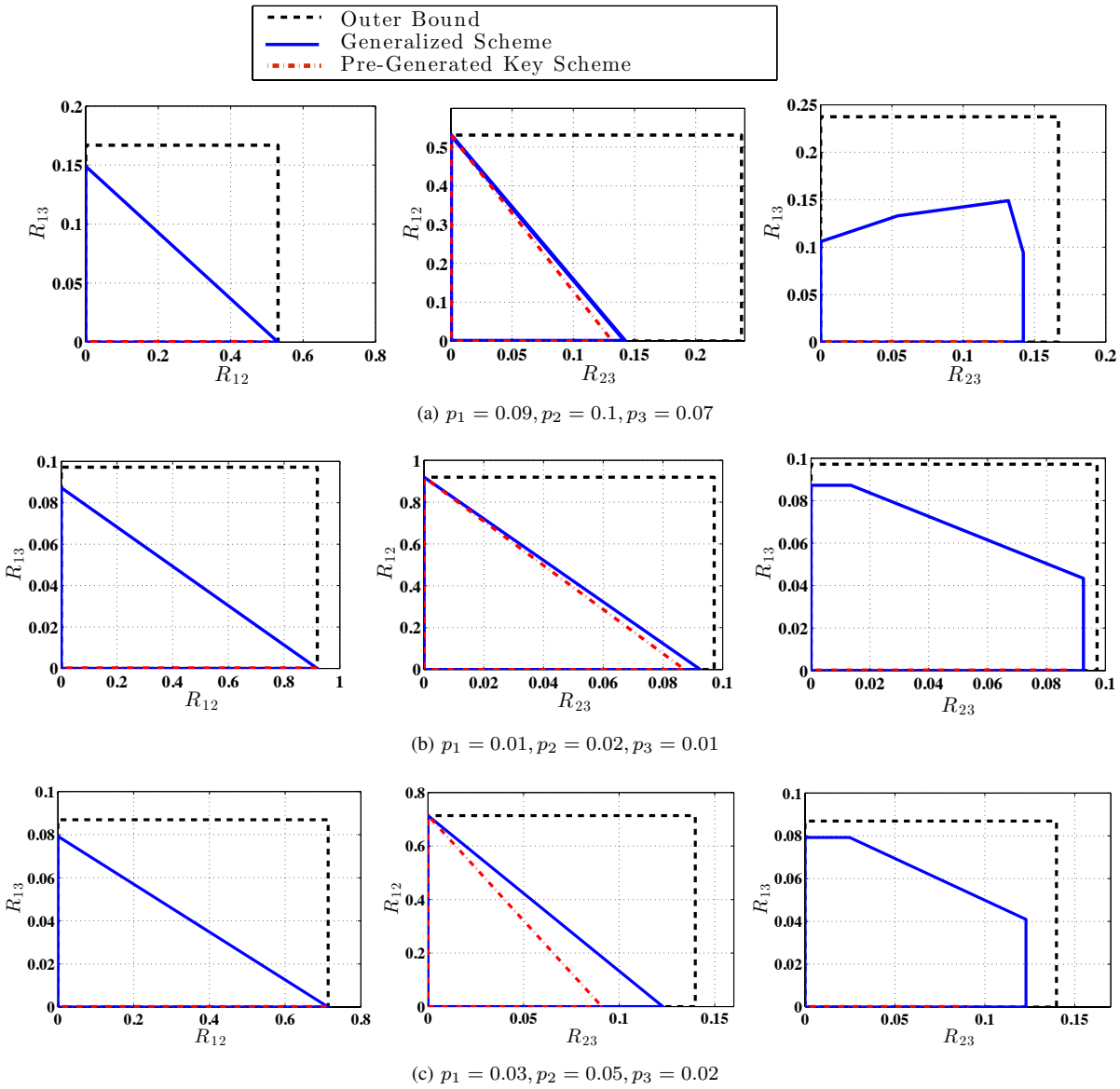
$$\begin{aligned} R_{23} \leq I(X_2,Y_2;Y_3|X_1,Y_1) &= H(Y_3|X_1,Y_1) - H(Y_3|X_1,Y_1,X_2,Y_2) \\ &= H(X_2+Z_2+Z_3|X_2+Z_1+Z_2+Z_3) - H(Z_2+Z_3|Z_2,Z_1+Z_2+Z_3) \\ &= H(X_2+Z_2+Z_3|X_2+Z_1+Z_2+Z_3) - H(Z_3|Z_1+Z_3) \\ &\leq h(p_1) - H(Z_3|Z_1+Z_3) = h(p_1 * p_3) - h(p_3). \end{aligned}$$

and

$$R_{13} \leq I(X_1,Y_1;Y_3|X_2,Y_2) \overset{(d)}{=} I(Y_1;Y_3|Y_2) = h(p_1 * p_3) - h(p_1).$$

In the above equations, (a), (c) and (d) are inferred from the Markov chain $(X_1, X_2) - Y_2 - Y_3 - Y_1$ and (b) is deduced from the distribution of U.

The key rate regions of the pre-generated keys and the generalized schemes in (19) and (18) along with the outer bound in (20) are compared in Fig. 9 for different values of the noises. In order to clarify the regions, we projected each 3-D region into three 2-D regions. It is seen that the generalized scheme strictly has a better performance compared to the pre-generated keys scheme. By using the pre-generated keys scheme, we can only achieve two non-zero secret-key rates while using the generalized scheme, we attain all three non-zero rates and obtain rate regions which are significantly larger compared to the former scheme.



(a) $p_1 = 0.09, p_2 = 0.1, p_3 = 0.07$

(b) $p_1 = 0.01, p_2 = 0.02, p_3 = 0.01$

(c) $p_1 = 0.03, p_2 = 0.05, p_3 = 0.02$

Fig. 9: Comparison of the two schemes and the outer bound for Binary Example 3

APPENDIX A
PROOF OF THE INNER BOUND IN THEOREM 3 (INCLUDING PROOF OF THEOREM 1)

We fix the distribution of all random variables involved in the coding scheme as defined Theorem 3. Key sharing is performed over B blocks, each comprised of n uses of the channel. In what follows, we describe the code construction, the associated encoding and decoding, and the security analysis, in the i-th block. The boldface random variable $\mathbf{X}$ (resp. $\mathbf{x}$) denotes n repetitions of random variable X, i.e., X^n (resp. its realization x). $\mathbf{X}^i$ (resp. $\mathbf{x}^i$) denotes $X^{in}_{(i-1)n+1}$ (resp. $x^{in}_{(i-1)n+1}$), i.e, n successive repetitions of random variable X associated with block i (resp. its successive realizations). $\mathbf{X}^{i:j}$ denotes $X^{jn}_{(i-1)n+1}$ and correspondingly, $\mathbf{x}^{i:j}$ denotes $n(j-i+1)$ realizations of X from block i to j.

Code Construction

User j independently generates $2^{n(r_{jl,p}+r'_{jl,p})}$ codewords $\mathbf{s}_{jl}$, for $j<l\in\{1,2,3\}$ according to the i.i.d. distribution $\prod_{i=1}^{n} p(s_{jl,i})$ which are labeled as:

$$\mathbf{s}_{jl}(k_{jl,p},k'_{jl,p}),k_{jl,p}\in\mathcal{K}_{jl,p}=\{1,...,2^{nr_{jl,p}}\},k'_{jl,p}\in\mathcal{K}'_{jl,p}=\{1,...,2^{nr'_{jl,p}}\}.$$

Each sequence $\mathbf{s}_{jl}$ can be determined if the indices $(k_{jl,p},k'_{jl,p})$ are known. The index $k_{jl,p}$ represents the pre-generated key to be shared between Users j and l while $k'_{jl,p}$ is a randomization index drawn from the local randomness.

Moreover, User j chooses sequences $\mathbf{t}_{jl}$ according to i.i.d. distribution $\prod_{i=1}^{n} p(t_{jl,i})$ and, it randomly and independently bins all sequences $\mathbf{t}_{jl}$ as follows:

- index $\phi_{jl}(\mathbf{t}_{jl})$ is uniformly generated over $[1,2^{nr_{jl}}]$. We set $k_{jl,s}=\phi(\mathbf{t}_{jl})$ as the secondary key to be shared between Users j and l.
- index $\psi_{jl}(\mathbf{t}_{jl})$ is uniformly generated over $[1,2^{nr'_{jl}}]$. We set $k'_{jl,s}=\psi(\mathbf{t}_{jl})$ as the index sent to User l such that it can reconstruct $\mathbf{T}_{jl}$.
- index $\theta_{jl}(\mathbf{t}_{jl})$ is uniformly generated over $[1,2^{nr''_{jl}}]$. We set $k''_{jl,s}=\theta(\mathbf{t}_{jl})$ as the index also used by User l to reconstruct $\mathbf{t}_{jl}$. We assume that a specific index $k''_{jl,s}$ is publicly shared between Users j and l ahead of time.

Note that, unlike traditional source models for key generation, there is no public channel over which to transmit the index $k'_{jl,s}$. To transmit the index over the noisy channel, we will have to explicitly define how to encode it into a codeword $\mathbf{s}_{jl}$. To this end, for $j\in\{1,2\}$, $l\in\{1,2,3\}$, $j\neq l$, we define functions

$$f_{jl}:\tilde{\mathcal{S}}_{jl}\rightarrow\mathcal{K}'_{jl,s},$$

where $\tilde{\mathcal{S}}_{jl}$ is the set of $2^{n(r_{jl,p}+r'_{jl,p})}$ indices pairs $(k_{jl,p},k'_{jl,p})$. Each f_{jl} is a random partitioning of $\tilde{\mathcal{S}}_{jl}$ into $2^{nr'_{jl,s}}$

equal-sized parts. Elements of part i are labeled as $(\tilde{\mathcal{S}}_{jl})_i$. We implicitly assume that the following condition holds

$$r'_{jl,s} < (r_{jl,p} + r'_{jl,p}) \tag{21}$$

Later on, It will be seen that this assumption holds because of the rate constraints (17) in Theorem 3.

Encoding in block i

At the beginning of block i, we assume that $k_{jl,s}^{''i-1}$ is chosen uniformly at random from its corresponding set and is publicly shared between Users j and l. We will later show that under specific conditions, the users can agree on specific values of $k_{jl,s}^{''i-1}$ ahead of time so that this assumption can be dropped. Sequences $\mathbf{y}_1^{1:i-1}, \mathbf{x}_1^{1:i-1}, \mathbf{s}_{12}^{1:i-1}, \mathbf{s}_{13}^{1:i-1}, \mathbf{t}_{12}^{1:i-2}, \mathbf{t}_{13}^{1:i-2}$ are available at User 1, who can also decode sequences $\mathbf{s}_{21}^{1:i-1}\mathbf{t}_{21}^{1:i-2}$.

User 1 then generates sequence $\mathbf{t}_{12}^{i-1}$ according to distribution $P_{\mathbf{T}_{12}|\mathbf{Y}_1\mathbf{X}_1\mathbf{S}_{12}K''_{12,s}}$, and sequence $\mathbf{t}_{13}^{i-1}$ according to distribution $P_{\mathbf{T}_{13}|\mathbf{Y}_1\mathbf{X}_1\mathbf{S}_{13}K''_{13,s}}$. Similarly, User 2 generates sequences $\mathbf{t}_{21}^{i-1}$ and $\mathbf{t}_{23}^{i-1}$. Subsequently, User j computes the secondary key of block $i-1$ for sharing with User l as $k_{jl,s}^{i-1} = \phi_{jl}(\mathbf{t}_{jl}^{i-1})$ and the index to be sent to User l to reconstruct $\mathbf{t}_{jl}^{i-1}$ as $k_{jl,s}^{'i-1} = \psi_{jl}(\mathbf{t}_{jl}^{i-1})$. As stated earlier $k_{jl,s}^{''i-1} = \theta_{jl}(\mathbf{t}_{jl}^{i-1})$ is already shared between Users j and l.

User j encodes $k_{jl,s}^{'i-1}$ in such a way that he finds the respective part $(\tilde{\mathcal{S}}_{jl})_{k_{jl,s}^{'i-1}}$ according to partitioning function f_{jl}, and then it randomly chooses a pair $(k_{jl,p}, k'_{jl,p})$ from $(\tilde{\mathcal{S}}_{jl})_{k_{jl,s}^{'i-1}}$. For the selected $(k_{jl,p}, k'_{jl,p})$, User j picks up sequence $\mathbf{s}_{jl}^i(k_{jl,p}, k'_{jl,p})$. Then, User j selects the respective index $k_{jl,p}$ of $\mathbf{s}_{jl}^i$ as the primary key of block i for sharing with User l, i.e., $k_{jl,p}^i$. In this way, Users 1 and 2 choose $(\mathbf{s}_{12}^i, \mathbf{s}_{13}^i)$ and $(\mathbf{s}_{21}^i, \mathbf{s}_{23}^i)$, respectively. The channel inputs of block i are sent over the GDMMAC according to the distributions $p(x_1|s_{12}, s_{13})$ and $p(x_2|s_{21}, s_{23})$ by Users 1 and 2, respectively, through n channel uses.

Decoding of block i

We let $\mathcal{T}_{\epsilon'}^n(P_X)$ denote the set of $\epsilon'-$strongly typical sequences x^n with respect to distribution $p(x)$. At the end of block i, Users 1, 2 and 3 receive $\mathbf{y}_1^i, \mathbf{y}_2^i$ and $\mathbf{y}_3^i$ through the channel, respectively. With access to $(\mathbf{x}_1^i, \mathbf{y}_1^i)$, User 1 declares an error unless there exists a unique $\mathbf{s}_{21}^i(k_{21,p}^i, k_{21,p}^{'i})$ such that $(\mathbf{x}_1^i, \mathbf{y}_1^i, \mathbf{s}_{21}^i) \in \mathcal{T}_{\epsilon_1}^n(P_{X_1,Y_1,S_{21}})$. User 2 acts in the symmetric way and decodes $\mathbf{s}_{12}^i$. With access to $\mathbf{y}_3^i$, User 3 declares an error unless there exists a unique pair $(\mathbf{s}_{13}^i(k_{13,p}^i, k_{13,p}^{'i}), \mathbf{s}_{23}^i(k_{23,p}^i, k_{23,p}^{'i}))$ such that $(\mathbf{y}_3^i, \mathbf{s}_{13}^i, \mathbf{s}_{23}^i) \in \mathcal{T}_{\epsilon_1}^n(P_{Y_3,S_{13},S_{23}})$.

After decoding the primary keys of block i, users decode the secondary keys of block $i-1$. In particular, using function f_{21}, User 1 finds mapping $(\tilde{\mathcal{S}}_{21})_{q_{21}}$ of the pair indices $(k_{21,p}^i, k_{21,p}^{'i})$ related to the decoded $\mathbf{s}_{21}^i$ and sets $k_{21,s}^{'i-1} = q_{21}$. Furthermore, as we assumed at the beginning of the encoding step, index $k_{21,s}^{''i-1}$ is available at User 1. With access to indices $k_{21,s}^{'i-1}$ and $k_{21,s}^{''i-1}$, and the sequences $(\mathbf{x}_1^{i-1}, \mathbf{y}_1^{i-1}, \mathbf{s}_{12}^{i-1}, \mathbf{s}_{21}^{i-1})$, User 1 decodes sequence $\mathbf{t}_{21}^{i-1}$ if $(\mathbf{t}_{21}^{i-1}(k_{21,s}^{i-1}, k_{21,s}^{'i-1}, k_{21,s}^{''i-1}), \mathbf{x}_1^{i-1}, \mathbf{y}_1^{i-1}, \mathbf{s}_{12}^{i-1}, \mathbf{s}_{21}^{i-1}) \in \mathcal{T}_{\epsilon_2}^n(P_{T_{21},X_1,Y_1|S_{12},S_{21}})$, when such $\mathbf{t}_{21}^{i-1}$ exists and is unique.

Otherwise, it declares an error. User 2 exploits mapping f_{12} to find $k_{12,s}^{'i-1}$ and decodes $\mathbf{t}_{12}^{i-1}$ in the symmetric way. User 3 uses mappings f_{13} and f_{23} to find $k_{13,s}^{'i-1}$ and $k_{23,s}^{'i-1}$. With access to the indices $k_{13,s}^{'i-1}, k_{23,s}^{'i-1}$, and the shared indices $k_{13,s}^{''i-1}, k_{23,s}^{''i-1}$ and the sequences $(\mathbf{y}_3^{i-1}, \mathbf{s}_{13}^{i-1}, \mathbf{s}_{23}^{i-1})$, User 3 decodes sequence pair $(\mathbf{t}_{13}^{i-1}, \mathbf{t}_{23}^{i-1})$ if $(\mathbf{t}_{13}^{i-1}(k_{13,s}^{i-1}, k_{13,s}^{'i-1}, k_{13,s}^{''i-1}), \mathbf{t}_{23}^{i-1}(k_{23,s}^{i-1}, k_{23,s}^{'i-1}, k_{23,s}^{''i-1}), \mathbf{y}_3^{i-1}, \mathbf{s}_{13}^{i-1}, \mathbf{s}_{23}^{i-1}) \in \mathcal{T}_{\epsilon_2}^n(P_{T_{13},T_{23},Y_3|S_{13},S_{23}})$, when such pair $(\mathbf{t}_{13}^{i-1}, \mathbf{t}_{23}^{i-1})$ exists and is unique. Otherwise, it declares an error.

Reliability analysis

If we set:

$$r_{12,p} + r'_{12,p} < I(S_{12}; X_2, Y_2) \tag{22}$$

$$r_{21,p} + r'_{21,p} < I(S_{21}; X_1, Y_1) \tag{23}$$

$$r_{13,p} + r'_{13,p} < I(S_{13}; Y_3|S_{23}) \tag{24}$$

$$r_{23,p} + r'_{23,p} < I(S_{23}; Y_3|S_{13}) \tag{25}$$

$$r_{13,p} + r'_{13,p} + r_{23,p} + r'_{23,p} < I(S_{13}, S_{23}; Y_3) \tag{26}$$

and if we choose $\epsilon_1 = \frac{\epsilon}{16B}$, it can be shown with standard arguments that the average of the primary decoding error probabilities $P_{ej,p}^{(n)}$ at User j are bounded by

$$E(P_{e1,p}^{(n)}) \leq 2\epsilon_1 = \frac{\epsilon}{8B} \tag{27}$$

$$E(P_{e2,p}^{(n)}) \leq 2\epsilon_1 = \frac{\epsilon}{8B} \tag{28}$$

$$E(P_{e3,p}^{(n)}) \leq 4\epsilon_1 = \frac{\epsilon}{4B} \tag{29}$$

for n sufficiently large. In (27)-(29), expectation is taken over the randomly generated code and all the binning functions where the error probabilities are conditioned to them. Notice that (22)-(23) reflect the point-to-point nature of the channel between Users 1 and 2, while (24)-(26) reflect the multiple access nature of the channel to User 3.

The analysis of the error probability for the secondary keys requires slightly more care. Note that the induced probability distribution by the encoding scheme is:

$$\begin{aligned}
&\tilde{P}_{K_{12,s}K'_{12,s}K''_{12,s}K_{13,s}K'_{13,s}K''_{13,s}K_{21,s}K'_{21,s}K''_{21,s}K_{23,s}K'_{23,s}K''_{23,s}\mathbf{T}_{12}\mathbf{T}_{13}\mathbf{T}_{21}\mathbf{T}_{23}\mathbf{X}_1\mathbf{X}_2\mathbf{Y}_1\mathbf{Y}_2\mathbf{Y}_3\mathbf{S}_{12}\mathbf{S}_{13}\mathbf{S}_{21}\mathbf{S}_{23}} = \\
&P_{K_{12,s}|\mathbf{T}_{12}}P_{K'_{12,s}|\mathbf{T}_{12}}P_{K''_{12,s}}P_{K_{13,s}|\mathbf{T}_{13}}P_{K'_{13,s}|\mathbf{T}_{13}}P_{K''_{13,s}}P_{K_{21,s}|\mathbf{T}_{21}}P_{K'_{21,s}|\mathbf{T}_{21}}P_{K''_{21,s}}P_{K_{23,s}|\mathbf{T}_{23}}P_{K'_{23,s}|\mathbf{T}_{23}}P_{K''_{23,s}}\times \\
&P_{\mathbf{T}_{12}|\mathbf{X}_1\mathbf{Y}_1\mathbf{S}_{12}K''_{12,s}}P_{\mathbf{T}_{13}|\mathbf{X}_1\mathbf{Y}_1\mathbf{S}_{13}K''_{13,s}}P_{\mathbf{T}_{21}|\mathbf{X}_2\mathbf{Y}_2\mathbf{S}_{21}K''_{21,s}}P_{\mathbf{T}_{23}|\mathbf{X}_2\mathbf{Y}_2\mathbf{S}_{23}K''_{23,s}}P_{\mathbf{X}_1\mathbf{X}_2\mathbf{Y}_1\mathbf{Y}_2\mathbf{Y}_3\mathbf{S}_{12}\mathbf{S}_{13}\mathbf{S}_{21}\mathbf{S}_{23}}
\end{aligned} \tag{30}$$

We will show that this distribution is nearly indistinguishable from the distribution

$$P_{K_{12,s}K'_{12,s}K''_{12,s}K_{13,s}K'_{13,s}K''_{13,s}K_{21,s}K'_{21,s}K''_{21,s}K_{23,s}K'_{23,s}K''_{23,s}\mathbf{T}_{12}\mathbf{T}_{13}\mathbf{T}_{21}\mathbf{T}_{23}\mathbf{X}_1\mathbf{X}_2\mathbf{Y}_1\mathbf{Y}_2\mathbf{Y}_3\mathbf{S}_{12}\mathbf{S}_{13}\mathbf{S}_{21}\mathbf{S}_{23}} =$$
$$P_{K_{12,s}|\mathbf{T}_{12}}P_{K'_{12,s}|\mathbf{T}_{12}}P_{K''_{12,s}|\mathbf{T}_{12}}P_{K_{13,s}|\mathbf{T}_{13}}P_{K'_{13,s}|\mathbf{T}_{13}}P_{K''_{13,s}|\mathbf{T}_{13}}P_{K_{21,s}|\mathbf{T}_{21}}P_{K'_{21,s}|\mathbf{T}_{21}}P_{K''_{21,s}|\mathbf{T}_{21}}P_{K_{23,s}|\mathbf{T}_{23}}\times$$
$$P_{K'_{23,s}|\mathbf{T}_{23}}P_{K''_{23,s}|\mathbf{T}_{23}}P_{\mathbf{T}_{12}|\mathbf{X}_1\mathbf{Y}_1\mathbf{S}_{12}}P_{\mathbf{T}_{13}|\mathbf{X}_1\mathbf{Y}_1\mathbf{S}_{13}}P_{\mathbf{T}_{21}|\mathbf{X}_2\mathbf{Y}_2\mathbf{S}_{21}}P_{\mathbf{T}_{23}|\mathbf{X}_2\mathbf{Y}_2\mathbf{S}_{23}}P_{\mathbf{X}_1\mathbf{X}_2\mathbf{Y}_1\mathbf{Y}_2\mathbf{Y}_3\mathbf{S}_{12}\mathbf{S}_{13}\mathbf{S}_{21}\mathbf{S}_{23}} \quad (31)$$

To this aim, we use the fact that index $k''_{jl,s}$ is generated at random by User j independently of the other available sequences for $j = 1, 2$. In particular, $K''_{12,s}$ is independent of $(\mathbf{Y}_1, \mathbf{X}_1, \mathbf{S}_{12})$ and $K''_{13,s}$ is independent of $(\mathbf{Y}_1, \mathbf{X}_1, \mathbf{S}_{13})$. Symmetrically, $K''_{21,s}$ is independent of $(\mathbf{Y}_2, \mathbf{X}_2, \mathbf{S}_{21})$ and $K''_{23,s}$ is independent of $(\mathbf{Y}_2, \mathbf{X}_2, \mathbf{S}_{23})$. It follows from standard results [25] that if

$$r''_{12,s} < H(T_{12}|Y_1, X_1, S_{12}) \quad (32)$$

$$r''_{13,s} < H(T_{13}|Y_1, X_1, S_{13}) \quad (33)$$

$$r''_{21,s} < H(T_{21}|Y_2, X_2, S_{21}) \quad (34)$$

$$r''_{23,s} < H(T_{23}|Y_2, X_2, S_{23}) \quad (35)$$

then there exist $\alpha_{12} > 0, \alpha_{13} > 0, \alpha_{21} > 0$ and $\alpha_{23} > 0$ such that:

$$E(D(P_{K''_{12,s}\mathbf{Y}_1\mathbf{X}_1\mathbf{S}_{12}} \parallel q_{K''_{12,s}}P_{\mathbf{Y}_1\mathbf{X}_1\mathbf{S}_{12}})) \leq 2^{-n\alpha_{12}} \quad (36)$$

$$E(D(P_{K''_{13,s}\mathbf{Y}_1\mathbf{X}_1\mathbf{S}_{13}} \parallel q_{K''_{13,s}}P_{\mathbf{Y}_1\mathbf{X}_1\mathbf{S}_{13}})) \leq 2^{-n\alpha_{13}} \quad (37)$$

$$E(D(P_{K''_{21,s}\mathbf{Y}_2\mathbf{X}_2\mathbf{S}_{21}} \parallel q_{K''_{21,s}}P_{\mathbf{Y}_2\mathbf{X}_2\mathbf{S}_{21}})) \leq 2^{-n\alpha_{21}} \quad (38)$$

$$E(D(P_{K''_{23,s}\mathbf{Y}_2\mathbf{X}_2\mathbf{S}_{23}} \parallel q_{K''_{23,s}}P_{\mathbf{Y}_2\mathbf{X}_2\mathbf{S}_{23}})) \leq 2^{-n\alpha_{23}} \quad (39)$$

in which q represents uniform distribution over the respective set. We now set:

$$\mathbf{O}_{12} = (\mathbf{X}_1, \mathbf{Y}_1, \mathbf{S}_{12}) \quad (40)$$

$$\mathbf{O}_{13} = (\mathbf{X}_1, \mathbf{Y}_1, \mathbf{S}_{13}) \quad (41)$$

$$\mathbf{O}_{21} = (\mathbf{X}_2, \mathbf{Y}_2, \mathbf{S}_{21}) \quad (42)$$

$$\mathbf{O}_{23} = (\mathbf{X}_2, \mathbf{Y}_2, \mathbf{S}_{23}) \quad (43)$$

$$\mathbf{O}_3 = \mathbf{Y}_3 \quad (44)$$

Then, we have

$$
\begin{aligned}
&D(P_{\mathbf{T}_{12}\mathbf{T}_{13}\mathbf{T}_{21}\mathbf{T}_{23}\mathbf{O}_{12}\mathbf{O}_{13}\mathbf{O}_{21}\mathbf{O}_{23}\mathbf{O}_3} \parallel \tilde{P}_{\mathbf{T}_{12}\mathbf{T}_{13}\mathbf{T}_{21}\mathbf{T}_{23}\mathbf{O}_{12}\mathbf{O}_{13}\mathbf{O}_{21}\mathbf{O}_{23}\mathbf{O}_3})\\
&\overset{(a)}{\leq} D(P_{K''_{12,s}K''_{13,s}K''_{21,s}K''_{23,s}\mathbf{T}_{12}\mathbf{T}_{13}\mathbf{T}_{21}\mathbf{T}_{23}\mathbf{O}_{12}\mathbf{O}_{13}\mathbf{O}_{21}\mathbf{O}_{23}\mathbf{O}_3} \parallel \tilde{P}_{K''_{12,s}K''_{13,s}K''_{21,s}K''_{23,s}\mathbf{T}_{12}\mathbf{T}_{13}\mathbf{T}_{21}\mathbf{T}_{23}\mathbf{O}_{12}\mathbf{O}_{13}\mathbf{O}_{21}\mathbf{O}_{23}\mathbf{O}_3})\\
&\overset{(b)}{=} D(P_{K''_{12,s}K''_{13,s}\mathbf{T}_{12}\mathbf{T}_{13}\mathbf{O}_{12}\mathbf{O}_{13}}\|\tilde{P}_{K''_{12,s}K''_{13,s}\mathbf{T}_{12}\mathbf{T}_{13}\mathbf{O}_{12}\mathbf{O}_{13}})+D(P_{K''_{21,s}K''_{23,s}\mathbf{T}_{21}\mathbf{T}_{23}\mathbf{O}_{21}\mathbf{O}_{23}}\|\tilde{P}_{K''_{21,s}K''_{23,s}\mathbf{T}_{21}\mathbf{T}_{23}\mathbf{O}_{21}\mathbf{O}_{23}})\\
&= \sum_{k''_{12,s}k''_{13,s}\mathbf{t}_{12}\mathbf{t}_{13}\mathbf{o}_{12}\mathbf{o}_{13}} P(k''_{12,s},k''_{13,s},\mathbf{t}_{12},\mathbf{t}_{13},\mathbf{o}_{12},\mathbf{o}_{13})\log_2\frac{P(k''_{12,s},k''_{13,s},\mathbf{t}_{12},\mathbf{t}_{13},\mathbf{o}_{12},\mathbf{o}_{13})}{\tilde{P}(k''_{12,s},k''_{13,s},\mathbf{t}_{12},\mathbf{t}_{13},\mathbf{o}_{12},\mathbf{o}_{13})}\\
&+ \sum_{k''_{21,s}k''_{23,s}\mathbf{t}_{21}\mathbf{t}_{23}\mathbf{o}_{21}\mathbf{o}_{23}} P(k''_{21,s},k''_{23,s},\mathbf{t}_{21},\mathbf{t}_{23},\mathbf{o}_{21},\mathbf{o}_{23})\log_2\frac{P(k''_{21,s},k''_{23,s},\mathbf{t}_{21},\mathbf{t}_{23},\mathbf{o}_{21},\mathbf{o}_{23})}{\tilde{P}(k''_{21,s},k''_{23,s},\mathbf{t}_{21},\mathbf{t}_{23},\mathbf{o}_{21},\mathbf{o}_{23})}\\
&= \sum_{k''_{12,s}k''_{13,s}\mathbf{t}_{12}\mathbf{t}_{13}\mathbf{o}_{12}\mathbf{o}_{13}} P(k''_{12,s},k''_{13,s},\mathbf{t}_{12},\mathbf{t}_{13},\mathbf{o}_{12},\mathbf{o}_{13})\log_2\frac{P(\mathbf{t}_{12},\mathbf{t}_{13}|k''_{12,s},k''_{13,s},\mathbf{o}_{12},\mathbf{o}_{13})P(k''_{12,s},k''_{13,s},\mathbf{o}_{12},\mathbf{o}_{13})}{P(\mathbf{t}_{12},\mathbf{t}_{13}|k''_{12,s},k''_{13,s},\mathbf{o}_{12},\mathbf{o}_{13})q_{k''_{12,s}}q_{k''_{13,s}}p(\mathbf{o}_{12},\mathbf{o}_{13})}\\
&+ \sum_{k''_{21,s}k''_{23,s}\mathbf{t}_{21}\mathbf{t}_{23}\mathbf{o}_{21}\mathbf{o}_{23}} P(k''_{21,s},k''_{23,s},\mathbf{t}_{21},\mathbf{t}_{23},\mathbf{o}_{21},\mathbf{o}_{23})\log_2\frac{P(\mathbf{t}_{21},\mathbf{t}_{23}|k''_{21,s},k''_{23,s},\mathbf{o}_{21},\mathbf{o}_{23})P(k''_{21,s},k''_{23,s},\mathbf{o}_{21},\mathbf{o}_{23})}{P(\mathbf{t}_{21},\mathbf{t}_{23}|k''_{21,s},k''_{23,s},\mathbf{o}_{21},\mathbf{o}_{23})q_{k''_{21,s}}q_{k''_{23,s}}p(\mathbf{o}_{21},\mathbf{o}_{23})}\\
&\overset{(c)}{=} \sum_{k''_{12,s}k''_{13,s}\mathbf{t}_{12}\mathbf{t}_{13}\mathbf{o}_{12}\mathbf{o}_{13}} P(k''_{12,s},k''_{13,s},\mathbf{t}_{12},\mathbf{t}_{13},\mathbf{o}_{12},\mathbf{o}_{13})\log_2\frac{P(k''_{12,s}|\mathbf{o}_{12})P(k''_{13,s}|\mathbf{o}_{13})p(\mathbf{o}_{12},\mathbf{o}_{13})}{q_{k''_{12,s}}q_{k''_{13,s}}p(\mathbf{o}_{12},\mathbf{o}_{13})}\\
&+ \sum_{k''_{21,s}k''_{23,s}\mathbf{t}_{21}\mathbf{t}_{23}\mathbf{o}_{21}\mathbf{o}_{23}} P(k''_{21,s},k''_{23,s},\mathbf{t}_{21},\mathbf{t}_{23},\mathbf{o}_{21},\mathbf{o}_{23})\log_2\frac{P(k''_{21,s}|\mathbf{o}_{21})P(k''_{23,s}|\mathbf{o}_{23})p(\mathbf{o}_{21},\mathbf{o}_{23})}{q_{k''_{21,s}}q_{k''_{23,s}}p(\mathbf{o}_{21},\mathbf{o}_{23})}\\
&= \sum_{k''_{12,s}k''_{13,s}\mathbf{t}_{12}\mathbf{t}_{13}\mathbf{o}_{12}\mathbf{o}_{13}} P(k''_{12,s},k''_{13,s},\mathbf{t}_{12},\mathbf{t}_{13},\mathbf{o}_{12},\mathbf{o}_{13})\log_2\frac{P(k''_{12,s}|\mathbf{o}_{12})P(k''_{13,s}|\mathbf{o}_{13})}{q_{k''_{12,s}}q_{k''_{13,s}}}\\
&+ \sum_{k''_{21,s}k''_{23,s}\mathbf{t}_{21}\mathbf{t}_{23}\mathbf{o}_{21}\mathbf{o}_{23}} P(k''_{21,s},k''_{23,s},\mathbf{t}_{21},\mathbf{t}_{23},\mathbf{o}_{21},\mathbf{o}_{23})\log_2\frac{P(k''_{21,s}|\mathbf{o}_{21})P(k''_{23,s}|\mathbf{o}_{23})}{q_{k''_{21,s}}q_{k''_{23,s}}}\\
&= \sum_{k''_{12,s}k''_{13,s}\mathbf{t}_{12}\mathbf{t}_{13}\mathbf{o}_{12}\mathbf{o}_{13}} P(k''_{12,s},k''_{13,s},\mathbf{t}_{12},\mathbf{t}_{13},\mathbf{o}_{12},\mathbf{o}_{13})(\log_2\frac{P(k''_{12,s}|\mathbf{o}_{12})}{q_{k''_{12,s}}}+\log_2\frac{P(k''_{13,s}|\mathbf{o}_{13})}{q_{k''_{13,s}}})\\
&+ \sum_{k''_{21,s}k''_{23,s}\mathbf{t}_{21}\mathbf{t}_{23}\mathbf{o}_{21}\mathbf{o}_{23}} P(k''_{21,s},k''_{23,s},\mathbf{t}_{21},\mathbf{t}_{23},\mathbf{o}_{21},\mathbf{o}_{23})(\log_2\frac{P(k''_{21,s}|\mathbf{o}_{21})}{q_{k''_{21,s}}}+\log_2\frac{P(k''_{23,s}|\mathbf{o}_{23})}{q_{k''_{23,s}}})\\
&= D(P_{K''_{12,s}\mathbf{O}_{12}}\|q_{K''_{12,s}}P_{\mathbf{O}_{12}})+D(P_{K''_{13,s}\mathbf{O}_{13}}\|q_{K''_{13,s}}P_{\mathbf{O}_{13}})+D(P_{K''_{21,s}\mathbf{O}_{21}}\|q_{K''_{21,s}}P_{\mathbf{O}_{21}})+D(P_{K''_{23,s}\mathbf{O}_{23}}\|q_{K''_{23,s}}P_{\mathbf{O}_{23}})\\
&\overset{(d)}{\leq} 2^{-n\alpha_{12}}+2^{-n\alpha_{13}}+2^{-n\alpha_{21}}+2^{-n\alpha_{23}}
\end{aligned}
\tag{45}
$$

where in the above equations, (a) follows from the relative entropy properties [27], (b) follows from the auxiliary random variables distributions in (30) and (31), (c) follows from distribution P in (31) that results in the following Markov chains:

$$K''_{12,s}-\mathbf{T}_{12}-\mathbf{O}_{12}-\mathbf{O}_{13}-\mathbf{T}_{13}-K''_{13,s}$$

$$K''_{21,s}-\mathbf{T}_{21}-\mathbf{O}_{21}-\mathbf{O}_{23}-\mathbf{T}_{23}-K''_{23,s}$$

and (d) is deduced from (36)-(39).

Hence, the distance between the two probabilities P and $\tilde{P}$ is arbitrarily small. Consequently the decoding error probability of the secondary keys can be analyzed for the much simpler distribution P.

It follows from standard results of Slepian-Wolf coding [24] that if

$$r'_{12,s}+r''_{12,s} > H(T_{12}|X_2, Y_2, S_{12}, S_{21}) \tag{46}$$

$$r'_{21,s}+r''_{21,s} > H(T_{21}|X_1, Y_1, S_{12}, S_{21}) \tag{47}$$

$$r'_{13,s}+r''_{13,s} > H(T_{13}|Y_3, S_{13}, S_{23}, T_{23}) \tag{48}$$

$$r'_{23,s}+r''_{23,s} > H(T_{23}|Y_3, S_{13}, S_{23}, T_{13}) \tag{49}$$

$$r'_{13,s}+r''_{13,s}+r'_{23,s}+r''_{23,s} > H(T_{13}, T_{23}|Y_3, S_{13}, S_{23}) \tag{50}$$

and if we set $\epsilon_2 = \frac{\epsilon}{16B}$, then

$$E(P^{(n)}_{e1,s}) \leq 2\epsilon_2 = \frac{\epsilon}{8B} \tag{51}$$

$$E(P^{(n)}_{e2,s}) \leq 2\epsilon_2 = \frac{\epsilon}{8B} \tag{52}$$

$$E(P^{(n)}_{e3,s}) \leq 4\epsilon_2 = \frac{\epsilon}{4B} \tag{53}$$

for sufficiently large n.

Finally, we show that we can select a specific $k^{''*}_{21,s}$ ahead of time so that need not be transmitted. In fact by assuming C as the random variable representing randomly generated code and all binning functions, we have:

$$\begin{aligned}
&E(P^{(n)}_{e1,s}) = E_C(\Pr\{\mathbf{T}_{21} \neq g_1(\mathbf{O}_{12}, K'_{21,s}, K''_{21,s})|C\}) = \\
&E_C(\sum_{k''_{21,s}k'_{21,s}\mathbf{o}_{12}\mathbf{o}_{21}\mathbf{t}_{21}} \frac{1}{2^{nr''_{21,s}}} P_{K'_{21,s}|\mathbf{T}_{21}}(k'_{21,s}|\mathbf{t}_{21}) P_{\mathbf{T}_{21}|\mathbf{O}_{21}K''_{21,s}}(\mathbf{t}_{21}|\mathbf{o}_{21}, k''_{21,s}) P_{\mathbf{O}_{12}\mathbf{O}_{21}}(\mathbf{o}_{12}, \mathbf{o}_{21}) \mathbf{1}[\mathbf{t}_{21} \neq g_1(\mathbf{o}_{12}, k'_{21,s}, k''_{21,s})|C]) \\
&= E_{K''_{21,s}C}(\Pr\{\mathbf{T}_{21} \neq g_1(\mathbf{O}_{12}, K'_{21,s}, K''_{21,s})\}|K''_{21,s}, C) \leq \frac{\epsilon}{8B}
\end{aligned} \tag{54}$$

Hence, there exists $k^{''*}_{21,s}$ such that:

$$E(P^{(n)}_{e1,s}) = E_C(\Pr\{\mathbf{T}_{21} \neq g_1(\mathbf{O}_{12}, K'_{21,s}, k^{''*}_{21,s})|C\}) < \frac{3\epsilon}{8B} \tag{55}$$

Similarly, there exist $k^{''*}_{12,s}, k^{''*}_{13,s}$ and $k^{''*}_{23,s}$ such that:

$$E(P^{(n)}_{e2,s}) = E_C(\Pr\{\mathbf{T}_{12} \neq g_2(\mathbf{O}_{21}, K'_{12,s}, k^{''*}_{12,s})|C\}) < \frac{3\epsilon}{8B} \tag{56}$$

$$E(P^{(n)}_{e3,s}) = E_C(\Pr\{(\mathbf{T}_{13}, \mathbf{T}_{23}) \neq g_3(\mathbf{O}_3, K'_{13,s}, k^{''*}_{13,s}, K'_{23}, k^{''*}_{23,s})|C\}) < \frac{3\epsilon}{4B} \tag{57}$$

Repeating the above encoding and decoding procedures over B blocks, the total decoding error probability at

User $j \in \{1,2,3\}$ is bounded as

$$E(P_j^{(nB)}) \leq B(E(P_{ej,p}^{(n)}) + E(P_{ej,s}^{(n)})) \overset{(a)}{<} \epsilon,$$

where (a) is deduced from (27)-(29) and (55)-(57).

Remark 4: combining (46)-(50) and (32)-(35), we obtain:

$$r'_{12,s} > I(T_{12}; X_1, Y_1 | X_2, Y_2, S_{12}, S_{21}) \tag{58}$$

$$r'_{21,s} > I(T_{21}; X_2, Y_2 | X_1, Y_1, S_{12}, S_{21}) \tag{59}$$

$$r'_{13,s} > I(T_{13}; X_1, Y_1 | Y_3, S_{13}, S_{23}, T_{23}) \tag{60}$$

$$r'_{23,s} > I(T_{23}; X_2, Y_2 | Y_3, S_{13}, S_{23}, T_{13}) \tag{61}$$

$$r'_{13,s} + r'_{23,s} > I(T_{13}, T_{23}; X_1, Y_1, X_2, Y_2 | Y_3, S_{13}, S_{23}) \tag{62}$$

The necessary condition (21) in definition of the functions f_{12}, f_{13}, f_{21} and f_{23} holds according to the rate constraints (17) in Theorem 3 and equations (22)-(26) and (58)-(62).

Remark 5: In the code construction of the primary keys, we implicitly assumed that $I(S_{12}; X_2, Y_2) \geq I(S_{12}; Y_3, S_{13}, S_{23}, T_{13}, T_{23})$. In the case where $I(S_{12}; X_2, Y_2) < I(S_{12}; Y_3, S_{13}, S_{23}, T_{13}, T_{23})$, User 1 randomly maps $k'_{12,s}$ into a space with $2^{n(I(S_{12};X_2,Y_2)-\delta'(\epsilon))}$ elements and no primary key is chosen by User 1 to be shared with User 2 and the bound on the rate of the primary key between Users 1 and 2 is equal to $[I(S_{21}; X_1, Y_1) - I(S_{21}; Y_3, S_{13}, S_{23}, T_{13}, T_{23})]^+$ in (15). Similarly, we implicitly assumed that $I(S_{13}; Y_3 | S_{23}) \geq I(S_{13}; X_2, Y_2, S_{12}, T_{12} | S_{23})$. In the case where $I(S_{13}; Y_3 | S_{23}) < I(S_{13}; X_2, Y_2, S_{12}, T_{12} | S_{23})$, User 1 randomly maps $k'_{13,s}$ into a space with $2^{n(I(S_{13};Y_3|S_{23})-\delta''(\epsilon))}$ elements and no primary key is chosen by User 1 to be shared with User 3 and the bound on the sum rate of $r_{13,p}+r_{23,p}$ is equal to $[I(S_{23}; Y_3|S_{13}) - I(S_{23}; X_1, Y_1, S_{21}, T_{21}|S_{13})]^+$ in (15). The same is true for User 2's codebook.

Remark 6: In the code construction of the secondary keys, we assumed that $I(T_{12}; X_2, Y_2 | S_{12}, S_{21}) - I(T_{12}; Y_3, S_{13}, S_{23}, T_{13}, T_{23} | S_{12}, S_{21}) \geq 0$, respectively $I(T_{21}; X_1, Y_1 | S_{12}, S_{21}) - I(T_{21}; Y_3, S_{13}, S_{23}, t_{13}, t_{23} | S_{12}, S_{21}) \geq 0$. Otherwise, we set $T_{12} = \phi$, respectively $T_{21} = \phi$. The same is true in deriving $r_{13,s} + r_{23,s}$.

Security Analysis

We now analyze the security condition of Definition 1. Performing the described encoding and decoding procedures in B blocks, the first secrecy constraint in (6) specializes as

$$I((K_{12,p}, K_{21,p}, K_{12,s}, K_{21,s})^{1:B}; \mathbf{Y}_3^{1:B} | (K''_{12,s}, K''_{21,s})^{1:B}) < \epsilon \tag{63}$$

where $(K_{12,s}, K_{21,s})^B = \emptyset$. We have:

$$
\begin{aligned}
&I((K_{12,p}, K_{21,p}, K_{12,s}, K_{21,s})^{1:B}; \mathbf{Y}_3^{1:B} | (K''_{12,s}, K''_{21,s})^{1:B}) \\
&\leq I((K_{12,p}, K_{21,p}, K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^{1:B}; \mathbf{Y}_3^{1:B}) \\
&= \sum_{i=1}^{B} I((K_{12,p}, K_{21,p}, K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^{i}; \mathbf{Y}_3^{1:B} | (K_{12,p}, K_{21,p}, K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^{1:i-1}) \\
&\leq \sum_{i=1}^{B} I((K_{12,p}, K_{21,p}, K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^{i}; \mathbf{Y}_3^{1:B}, (K_{12,p}, K_{21,p}, K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^{1:i-1}) \qquad (64) \\
&= \sum_{i=1}^{B} [I((K_{12,p}, K_{21,p})^{i}; \mathbf{Y}_3^{1:B}, (K_{12,p}, K_{21,p}, K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^{1:i-1}) \\
&+ I((K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^{i}; \mathbf{Y}_3^{1:B}, (K_{12,p}, K_{21,p}, K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^{1:i-1} | (K_{12,p}, K_{21,p})^{i})] \\
&\leq \sum_{i=1}^{B} [\overbrace{I((K_{12,p}, K_{21,p})^{i}; \mathbf{Y}_3^{1:B}, (K_{12,p}, K_{21,p}, K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^{1:i-1})}^{A_i} \\
&+ \underbrace{I((K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^{i}; \mathbf{Y}_3^{1:B}, (K_{12,p}, K_{21,p}, K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^{1:i-1}, (K_{12,p}, K_{21,p})^{i})}_{B_i}]
\end{aligned}
$$

We analyze each of the above terms separately. Some Markov chains useful in the security analysis are given in (65)-(69). These Markov chains arise from the coding scheme.

$$(K_{12,p}, K_{21,p})^{i} - (K'_{12,s}, K'_{21,s}, K'_{13,s}, K'_{23,s})^{i-1} - (K_{12,p}, K_{21,p}, K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s}, \mathbf{Y}_3)^{1:i-1} \qquad (65)$$

$$(K_{12,p}, K_{21,p})^{i} - (K'_{12,s}, K'_{21,s}, K'_{13,s}, K'_{23,s})^{i} - (\mathbf{Y}_3)^{i+1:B} \qquad (66)$$

$$(K_{12,p}, K_{21,p})^{i} - (\mathbf{Y}_3, \mathbf{S}_{13}, \mathbf{S}_{23})^{i} - (K'_{12,s}, K'_{21,s}, K'_{13,s}, K'_{23,s})^{i-1} \qquad (67)$$

$$(K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^{i} - (\mathbf{S}_{12}, \mathbf{S}_{21}, \mathbf{S}_{13}, \mathbf{S}_{23})^{i} - (K_{12,p}, K_{21,p}, K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s}, \mathbf{Y}_3)^{1:i-1} \qquad (68)$$

$$(K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^{i} - (K'_{12,s}, K'_{21,s}, K'_{13,s}, K'_{23,s})^{i} - (\mathbf{Y}_3)^{i+1:B} \qquad (69)$$

For term A_i, we have:

$$
\begin{aligned}
&A_i = I((K_{12,p}, K_{21,p})^{i}; \mathbf{Y}_3^{1:B}, (K_{12,p}, K_{21,p}, K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^{1:i-1}) \\
&\leq I((K_{12,p}, K_{21,p})^{i}; \mathbf{Y}_3^{1:B}, (K_{12,p}, K_{21,p}, K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^{1:i-1}, (K'_{12,s}, K'_{21,s}, K'_{13,s}, K'_{23,s})^{i-1:i}) \\
&\overset{(a)}{=} I((K_{12,p}, K_{21,p})^{i}; \mathbf{Y}_3^{i:B}, (K'_{12,s}, K'_{21,s}, K'_{13,s}, K'_{23,s})^{i-1:i}) \\
&\overset{(b)}{=} I((K_{12,p}, K_{21,p})^{i}; \mathbf{Y}_3^{i}, (K'_{12,s}, K'_{21,s}, K'_{13,s}, K'_{23,s})^{i-1:i}) \\
&\leq I((K_{12,p}, K_{21,p})^{i}; \mathbf{Y}_3^{i}, \mathbf{S}_{13}^{i}, \mathbf{S}_{23}^{i}, (K'_{12,s}, K'_{21,s}, K'_{13,s}, K'_{23,s})^{i-1:i}) \\
&\overset{(c)}{=} I((K_{12,p}, K_{21,p})^{i}; \mathbf{Y}_3^{i}, \mathbf{S}_{13}^{i}, \mathbf{S}_{23}^{i}, (K'_{12,s}, K'_{21,s}, K'_{13,s}, K'_{23,s})^{i}) \\
&\overset{(d)}{\leq} I((K_{12,p}, K_{21,p})^{i}; \mathbf{Y}_3^{i}, \mathbf{S}_{13}^{i}, \mathbf{S}_{23}^{i}, \mathbf{T}_{13}^{i}, \mathbf{T}_{23}^{i}, (K'_{12,s}, K'_{21,s})^{i}) \\
&= I((K_{12,p}, K_{21,p})^{i}; \mathbf{Y}_3^{i}, \mathbf{S}_{13}^{i}, \mathbf{S}_{23}^{i}, \mathbf{T}_{13}^{i}, \mathbf{T}_{23}^{i}) + I((K_{12,p}, K_{21,p})^{i}; (K'_{12,s}, K'_{21,s})^{i} | \mathbf{Y}_3^{i}, \mathbf{S}_{13}^{i}, \mathbf{S}_{23}^{i}, \mathbf{T}_{13}^{i}, \mathbf{T}_{23}^{i}) \\
&\overset{(e)}{\leq} \overbrace{I((K_{12,p}, K_{21,p})^{i}; \mathbf{Y}_3^{i}, \mathbf{S}_{13}^{i}, \mathbf{S}_{23}^{i}, \mathbf{T}_{13}^{i}, \mathbf{T}_{23}^{i})}^{A_{1i}} + \overbrace{I((K'_{12,s}, K'_{21,s})^{i}; \mathbf{Y}_3^{i}, \mathbf{S}_{12}^{i}, \mathbf{S}_{21}^{i}, \mathbf{S}_{13}^{i}, \mathbf{S}_{23}^{i}, \mathbf{T}_{13}^{i}, \mathbf{T}_{23}^{i})}^{A_{2i}}
\end{aligned}
$$

where in the above equations, (a), (b) and (c) are, respectively, due to Markov chains (65), (66) and (67). (d) holds

since $k'_{13,s}$ and $k'_{23,s}$ are indices of sequences $\mathbf{t}_{13}$ and $\mathbf{t}_{23}$, respectively. (e) is true due to the fact that $k_{12,p}$ and $k_{21,p}$ are indices of sequences $\mathbf{s}_{12}$ and $\mathbf{s}_{21}$, respectively.

For term B_i, we have:

$$
\begin{aligned}
B_i &= I((K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^i; \mathbf{Y}_3^{1:B}, (K_{12,p}, K_{21,p}, K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^{1:i-1}, (K_{12,p}, K_{21,p})^i) \\
&\overset{(a)}{\leq} I((K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^i; \mathbf{Y}_3^{1:B}, (K_{12,p}, K_{21,p}, K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^{1:i-1}, (\mathbf{S}_{12}, \mathbf{S}_{21})^i) \\
&\leq I((K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^i; \mathbf{Y}_3^{1:B}, (K_{12,p}, K_{21,p}, K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^{1:i-1}, (\mathbf{S}_{12}, \mathbf{S}_{21}, \mathbf{S}_{13}, \mathbf{S}_{23})^i) \\
&\overset{(b)}{=} I((K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^i; \mathbf{Y}_3^{i:B}, (\mathbf{S}_{12}, \mathbf{S}_{21}, \mathbf{S}_{13}, \mathbf{S}_{23})^i) \\
&\leq I((K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^i; \mathbf{Y}_3^{i:B}, (\mathbf{S}_{12}, \mathbf{S}_{21}, \mathbf{S}_{13}, \mathbf{S}_{23})^i, (K'_{12,s}, K'_{21,s}, K'_{13,s}, K'_{23,s})^i) \\
&\overset{(c)}{=} I((K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^i; \mathbf{Y}_3^{i}, (\mathbf{S}_{12}, \mathbf{S}_{21}, \mathbf{S}_{13}, \mathbf{S}_{23})^i, (K'_{12,s}, K'_{21,s}, K'_{13,s}, K'_{23,s})^i) \\
&\leq I((K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^i; \mathbf{Y}_3^{i}, (\mathbf{S}_{12}, \mathbf{S}_{21}, \mathbf{S}_{13}, \mathbf{S}_{23}, \mathbf{T}_{13}, \mathbf{T}_{23})^i, (K'_{12,s}, K'_{21,s})^i) \\
&\overset{(d)}{=} \overbrace{I((K_{12,s}, K_{21,s}, K''_{12,s}, K''_{21,s})^i; \mathbf{Y}_3^{i}, (\mathbf{S}_{12}, \mathbf{S}_{21}, \mathbf{S}_{13}, \mathbf{S}_{23}, \mathbf{T}_{13}, \mathbf{T}_{23})^i | (K'_{12,s}, K'_{21,s})^i)}^{B_{1i}}
\end{aligned}
$$

where in the above equations, (a) is due to the fact that $k_{12,p}$ and $k_{21,p}$ are indices of sequences $\mathbf{s}_{12}$ and $\mathbf{s}_{21}$, respectively. (b) and (c) are deduced from Markov chains (68) and (69), respectively. (d) holds since the indices are independent of each other.

We continue by combining three terms A_{1i}, A_{2i} and B_{1i}. Since in all the three terms, only block index i appears, we drop it in the following. Security condition (63) appears as:

$$
\begin{aligned}
&I((K_{12,p}, K_{21,p}, K_{12,s}, K_{21,s})^{1:B}; \mathbf{Y}_3^{1:B} | (K''_{12,s}, K''_{21,s})^{1:B}) \leq B(A_1 + A_2 + B_1) = \\
&B\big(I(K_{12,p}, K_{21,p}; \mathbf{Y}_3, \mathbf{S}_{13}, \mathbf{S}_{23}, \mathbf{T}_{13}, \mathbf{T}_{23}) + I(K_{12,s}, K_{21,s}, K'_{12,s}, K'_{21,s}, K''_{12,s}, K''_{21,s}; \mathbf{Y}_3, \mathbf{S}_{12}, \mathbf{S}_{21}, \mathbf{S}_{13}, \mathbf{S}_{23}, \mathbf{T}_{13}, \mathbf{T}_{23})\big)
\end{aligned} \tag{70}
$$

We analyze the two terms in (70) separately. Specifically, we use Lemma 2 and Lemma 3 as follows.

Lemma 2: If

$$r'_{12,p} + r'_{21,p} > I(S_{12}, S_{21}; Y_3, S_{13}, S_{23}, T_{13}, T_{23}) + 2\epsilon' \tag{71}$$

$$r'_{12,p} > I(S_{12}; Y_3, S_{13}, S_{23}, T_{13}, T_{23}) + 2\epsilon' \tag{72}$$

$$r'_{21,p} > I(S_{21}; Y_3, S_{13}, S_{23}, T_{13}, T_{23}) + 2\epsilon' \tag{73}$$

$$r'_{13,p} > I(S_{13}; X_2, Y_2, S_{12}, T_{12}) + 2\epsilon' \tag{74}$$

$$r'_{23,p} > I(S_{23}; X_1, Y_1, S_{21}, T_{21}) + 2\epsilon' \tag{75}$$

then we have

$$I(K_{12,p}, K_{21,p}; \mathbf{Y}_3, \mathbf{S}_{13}, \mathbf{S}_{23}, \mathbf{T}_{13}, \mathbf{T}_{23}) < \frac{\epsilon}{2B} \tag{76}$$

$$I(K_{13,p}; \mathbf{Y}_2, \mathbf{X}_2, \mathbf{S}_{12}, \mathbf{T}_{12}) < \frac{\epsilon}{2B} \tag{77}$$

$$I(K_{23,p}; \mathbf{Y}_1, \mathbf{X}_1, \mathbf{S}_{21}, \mathbf{T}_{21}) < \frac{\epsilon}{2B} \tag{78}$$

The proof of Lemma 2 is given in Appendix B.

Lemma 3: If

$$r_{12,s} + r'_{12,s} + r''_{12,s} + r_{21,s} + r'_{21,s} + r''_{21,s} < H(T_{12}, T_{21}|Y_3, S_{12}, S_{21}, S_{13}, S_{23}, T_{13}, T_{23}) - 2\epsilon'' \tag{79}$$

$$r_{12,s} + r'_{12,s} + r''_{12,s} < H(T_{12}|Y_3, S_{12}, S_{21}, S_{13}, S_{23}, T_{13}, T_{23}) - 2\epsilon'' \tag{80}$$

$$r_{21,s} + r'_{21,s} + r''_{21,s} < H(T_{21}|Y_3, S_{12}, S_{21}, S_{13}, S_{23}, T_{13}, T_{23}) - 2\epsilon'' \tag{81}$$

$$r_{13,s} + r'_{13,s} + r''_{13,s} < H(T_{13}|X_2, Y_2, S_{12}, S_{13}, T_{12}) - 2\epsilon'' \tag{82}$$

$$r_{23,s} + r'_{23,s} + r''_{23,s} < H(T_{23}|X_1, Y_1, S_{21}, S_{23}, T_{21}) - 2\epsilon'' \tag{83}$$

then we have

$$I(K_{12,s}, K_{21,s}, K'_{12,s}, K'_{21,s}, K''_{12,s}, K''_{21,s}; \mathbf{Y}_3, \mathbf{S}_{12}, \mathbf{S}_{21}, \mathbf{S}_{13}, \mathbf{S}_{23}, \mathbf{T}_{13}, \mathbf{T}_{23}) < \frac{\epsilon}{2B} \tag{84}$$

$$I(K_{13,s}, K'_{13,s}, K''_{13,s}; \mathbf{Y}_2, \mathbf{X}_2, \mathbf{S}_{12}, \mathbf{S}_{13}, \mathbf{T}_{12}) < \frac{\epsilon}{2B} \tag{85}$$

$$I(K_{23,s}, K'_{23,s}, K''_{23,s}; \mathbf{Y}_1, \mathbf{X}_1, \mathbf{S}_{21}, \mathbf{S}_{23}, \mathbf{T}_{21}) < \frac{\epsilon}{2B} \tag{86}$$

The proof of Lemma 3 is given in Appendix C.

Combining (70), (76) and (84), the strong secrecy condition of the key between Users 1 and 2 is deduced as:

$$I((K_{12,p}, K_{21,p}, K_{12,s}, K_{21,s})^{1:B}; \mathbf{Y}_3^{1:B} | (K''_{12,s}, K''_{21,s})^{1:B}) \leq \epsilon \tag{87}$$

Using similar Markov chains as in (65)-(69) for keys $K_{13,p}, K_{23,p}, K_{13,s}, K_{23,s}$ and exploiting Lemma 2 and 3, the other strong secrecy conditions in (6) are deduced as:

$$I((K_{13,p}, K_{13,s})^{1:B}; (\mathbf{X}_2, \mathbf{Y}_2)^{1:B} | (K''_{13,s})^{1:B}) \leq \epsilon \tag{88}$$

$$I((K_{23,p}, K_{23,s})^{1:B}; (\mathbf{X}_1, \mathbf{Y}_1)^{1:B} | (K''_{23,s})^{1:B}) \leq \epsilon \tag{89}$$

Replacing equations (71)-(75) in (22)-(26), we obtain:

$$
\begin{aligned}
&r_{12,p} < I(S_{12}; X_2, Y_2) - I(S_{12}; Y_3, S_{13}, S_{23}, T_{13}, T_{23}) \triangleq \mathbf{r_{12,p}},\\
&r_{21,p} < I(S_{21}; X_1, Y_1) - I(S_{21}; Y_3, S_{13}, S_{23}, T_{13}, T_{23}) \triangleq \mathbf{r_{21,p}},\\
&r_{12,p} + r_{21,p} < I(S_{12}; X_2, Y_2) + I(S_{21}; X_1, Y_1) - I(S_{12}, S_{21}; Y_3, S_{13}, S_{23}, T_{13}, T_{23})\\
&= \mathbf{r_{12,p}} + \mathbf{r_{21,p}} - \mathbf{I_{12,p}},\\
&r_{13,p} < I(S_{13}; Y_3|S_{23}) - I(S_{13}; Y_2, X_2, S_{12}, T_{12}|S_{23}) \triangleq \mathbf{r_{13,p}},\\
&r_{23,p} < I(S_{23}; Y_3|S_{13}) - I(S_{23}; Y_1, X_1, S_{21}, T_{21}|S_{13}) \triangleq \mathbf{r_{23,p}},\\
&r_{13,p} + r_{23,p} < I(S_{13}, S_{23}; Y_3) - I(S_{13}; Y_2, X_2, S_{12}, T_{12}|S_{23}) - I(S_{23}; Y_1, X_1, S_{21}, T_{21}|S_{13})\\
&= \mathbf{r_{13,p}} + \mathbf{r_{23,p}} - \mathbf{I_{3,p}}
\end{aligned} \tag{90}
$$

By setting $\overline{r}_{12,p} = r_{12,p} + r_{21,p}, \overline{r}_{13,p} = r_{13,p}, \overline{r}_{23,p} = r_{23,p}$ and applying Fourier-Motzkin elimination [26] to the above region, the primary keys rates of Theorem 3 (and also Theorem 1) are derived.

Replacing equations (79)-(83) with (46)-(50), the following rates are achievable for the secondary keys:

$$
\begin{aligned}
&r_{12,s} < I(T_{12}; X_2, Y_2|S_{12}, S_{21}) - I(T_{12}; Y_3, S_{13}, S_{23}, T_{13}, T_{23}|S_{12}, S_{21}) \triangleq \mathbf{r_{12,s}},\\
&r_{21,s} < I(T_{21}; X_1, Y_1|S_{12}, S_{21}) - I(T_{21}; Y_3, S_{13}, S_{23}, T_{13}, T_{23}|S_{12}, S_{21}) \triangleq \mathbf{r_{21,s}},\\
&r_{12,s} + r_{21,s} < I(T_{12}; X_2, Y_2|S_{12}, S_{21}) + I(T_{21}; X_1, Y_1|S_{12}, S_{21}) - I(T_{12}; T_{21}|S_{12}, S_{21})\\
&-I(T_{12}, T_{21}; Y_3, S_{13}, S_{23}, T_{13}, T_{23}|S_{12}, S_{21}) = \mathbf{r_{12,s}} + \mathbf{r_{21,s}} - \mathbf{I_{12,s}},\\
&r_{13,s} < I(T_{13}; Y_3|S_{13}, S_{23}, T_{23}) - I(T_{13}; X_2, Y_2, S_{12}, T_{12}|S_{13}, S_{23}, T_{23}) \triangleq \mathbf{r_{13,s}},\\
&r_{23,s} < I(T_{23}; Y_3|S_{13}, T_{13}, S_{23}) - I(T_{23}; X_1, Y_1, S_{21}, T_{21}|S_{13}, T_{13}, S_{23}) \triangleq \mathbf{r_{23,s}},\\
&r_{13,s} + r_{23,s} < I(T_{13}, T_{23}; Y_3|S_{13}, S_{23}) - I(T_{13}; T_{23}|S_{13}, S_{23}) - I(T_{13}; X_2, Y_2, S_{12}, T_{12}|S_{13}, S_{23}, T_{23}) -\\
&I(T_{23}; X_1, Y_1, S_{21}, T_{21}|S_{13}, T_{13}, S_{23}) = \mathbf{r_{13,s}} + \mathbf{r_{23,s}} - \mathbf{I_{3,s}}
\end{aligned} \tag{91}
$$

By setting $\overline{r}_{12,s} = r_{12,s} + r_{21,s}, \overline{r}_{13,s} = r_{13,s}, \overline{r}_{23,s} = r_{23,s}$ and applying Fourier-Motzkin elimination [26] to the above region, the secondary keys rates of Theorem 3 are derived.

To show that the total rate of the secret key between Users 1 and 2 is the sum of the rates $\overline{r}_{12,p}$ and $\overline{r}_{12,s}$, we should prove the independence of the primary and the secondary keys. Since $K_{12,p}$ and $K_{21,p}$ are indices of $\mathbf{S}_{12}$ and $\mathbf{S}_{21}$, respectively, (84) implies that:

$$I(K_{12,s}, K_{21,s}; K_{12,p}, K_{21,p}) \leq \epsilon,$$

and hence:

$$H(K_{12,s}, K_{21,s}, K_{12,p}, K_{21,p}) \geq H(K_{12,s}, K_{21,s}) + H(K_{12,p}, K_{21,p}) - \epsilon.$$

Furthermore, we need to prove the independence of the primary and the secondary keys of different blocks. Referring to (64), we have:

$$\sum_{i=1}^{B} I((K_{12,p}, K_{21,p}, K_{12,s}, K_{21,s})^i; \mathbf{Y}_3^{1:B}, (K_{12,p}, K_{21,p}, K_{12,s}, K_{21,s})^{1:i-1}) < \epsilon$$

and hence:

$$\sum_{i=1}^{B} I((K_{12,p}, K_{21,p}, K_{12,s}, K_{21,s})^i; (K_{12,p}, K_{21,p}, K_{12,s}, K_{21,s})^{1:i-1}) < \epsilon$$

which proves the independence of the keys of different blocks.

Similar arguments as above hold for the key between Users 1 and 3, and also the key between Users 2 and 3.

Finally the following rate is achievable between Users $j \in \{1, 2\}$ and $l \in \{1, 2, 3\}$ where $j \neq l$:

$$R_{jl} = \frac{nB\bar{r}_{jl,p} + n(B-1)\bar{r}_{jl,s}}{nB}$$

which is approximately equal to $\bar{r}_{jl,p} + \bar{r}_{jl,s}$ if B is large enough. Hence, the achievability of the secret-key rate region in Theorem 3 is deduced according to (90) and (91).

This completes achievability of the key rate region in Theorem 3 in strong sense.

APPENDIX B
PROOF OF STRONG SECRECY OF THE PRIMARY KEYS IN THEOREM 3

We note that in the pre-generated keys scheme, the generalized nature of the GDMMAC as feedback is not exploited, and the observations are merely used as side information. Consequently, the mechanisms exploited for secrecy reduce to secure communication over a wiretap channel. In this scheme, strong secrecy can be obtained as a byproduct of channel resolvability. Specifically, given a message M to be secured against an observation Z^n, notice that:

$$I(M; Z^n) = D(p_{MZ^n} \parallel p_M p_{Z^n}) \leq E_M(D(p_{Z^n|M} \parallel q_{Z^n})) \tag{92}$$

for any $q_{Z^n} \in \Delta(\mathcal{Z}^n)$.

We start by establishing a general result that we use in the sequel to prove the strong secrecy of the pre-generated keys in Lemma 2 of Appendix A. We consider the general model illustrated in Fig. 10 in which each user is active and generates keys to share with the other two users. In this model, k_{ij} is the key generated by User i to be shared with User j which should be kept secret from the remaining user as the potential eavesdropper where

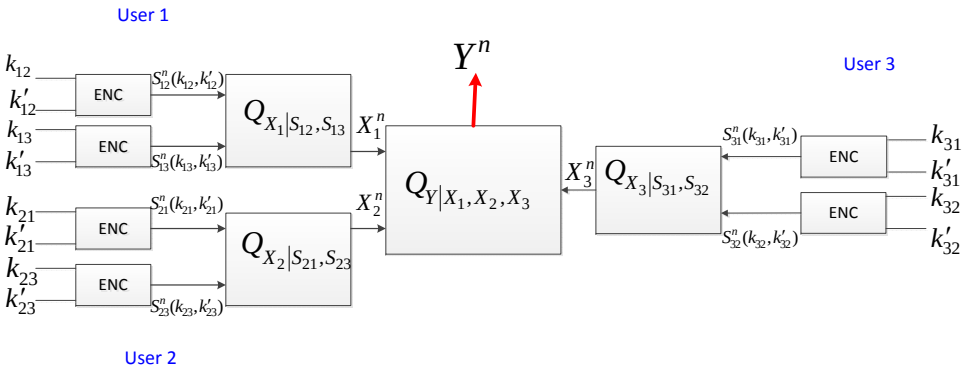


Fig. 10: Model for Proposition 1

$i, j \in \{1, 2, 3\}, i \neq j$ and S_{ij} is the respective auxiliary random variable to k_{ij}. The channel output Y^n represents the output received by the potential eavesdropper which can be any of the three users. Since the model is symmetric, it is sufficient to prove strong secrecy of the keys shared between each pair of the users and then, the result can be extended to the other pairs' secret keys. In continue, we consider the case where User 3 is the eavesdropper and we intend to prove strong secrecy of the keys between Users 1 and 2, i.e., (k_{12}, k_{21}). We assume that User 3 has already decoded his intended codewords $s_{13}^n(k_{13}, k'_{13})$ and $s_{23}^n(k_{23}, k'_{23})$ from Users 1 and 2, respectively. Hence, User 3's observation is $z^n = (y^n, x_3^n, k_{13}, k'_{13}, k_{23}, k'_{23})$. In Proposition 1, strong secrecy of the keys between Users 1 and 2 against User 3's observation is given by using the inequality in (92). In continue, the notations are borrowed from Appendix A.

Proposition 1:

$$E(D(P^n_{Y^n X_3^n K_{13} K'_{13} K_{23} K'_{23}|K_{12}K_{21}} \parallel \widehat{P}^n_{Y^n X_3^n K_{13} K'_{13} K_{23} K'_{23}})) \to 0 \tag{93}$$

for sufficiently large n.

Proof:

Let $Q \in \Delta(\mathcal{S}_{12} \times \mathcal{S}_{13} \times \mathcal{S}_{21} \times \mathcal{S}_{23} \times \mathcal{S}_{31} \times \mathcal{S}_{32} \times \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_3 \times \mathcal{Y})$ denote the PMF defined by the channel and the random coding argument. The independent and identically distributed (iid) product distribution on $\Delta(\mathcal{S}_{12}^n \times \mathcal{S}_{13}^n \times \mathcal{S}_{21}^n \times \mathcal{S}_{23}^n \times \mathcal{S}_{31}^n \times \mathcal{S}_{32}^n \times \mathcal{X}_1^n \times \mathcal{X}_2^n \times \mathcal{X}_3^n \times \mathcal{Y}^n)$ is denoted by $Q^{\otimes n}$. In contrast let $P^n \in \Delta(\mathcal{S}_{12}^n \times \mathcal{S}_{13}^n \times \mathcal{S}_{21}^n \times \mathcal{S}_{23}^n \times \mathcal{S}_{31}^n \times \mathcal{S}_{32}^n \times \mathcal{X}_1^n \times \mathcal{X}_2^n \times \mathcal{X}_3^n \times \mathcal{Y}^n)$ denote the distribution induced by the coding

scheme. By construction:

$$P^n\left(k_{12},k'_{12},k_{13},k'_{13},k_{21},k'_{21},k_{23},k'_{23},k_{31},k'_{31},k_{32},k'_{32},\mathbf{x}_1,\mathbf{x}_2,\mathbf{x}_3,\mathbf{y}\right) \triangleq$$
$$Q^{\otimes n}\left(\mathbf{y}|\mathbf{x}_1,\mathbf{x}_2,\mathbf{x}_3\right) Q^{\otimes n}(\mathbf{x}_1|\mathbf{s}_{12}(k_{12},k'_{12})\mathbf{s}_{13}(k_{13},k'_{13}))Q^{\otimes n}(\mathbf{x}_2|\mathbf{s}_{21}(k_{21},k'_{21})\mathbf{s}_{23}(k_{23},k'_{23}))$$
$$Q^{\otimes n}(\mathbf{x}_3|\mathbf{s}_{31}(k_{31},k'_{31})\mathbf{s}_{32}(k_{32},k'_{32}))\frac{1}{|\mathcal{K}_{12}\|\mathcal{K}'_{12}\|\mathcal{K}_{13}\|\mathcal{K}'_{13}\|\mathcal{K}_{21}\|\mathcal{K}'_{21}\|\mathcal{K}_{23}\|\mathcal{K}'_{23}\|\mathcal{K}_{31}\|\mathcal{K}'_{31}\|\mathcal{K}_{32}\|\mathcal{K}'_{32}|}. \quad (94)$$

where $|\mathcal{K}_{ij}|$ is the cardinality of key set $\mathcal{K}_{ij}$.

Define:

$$\widehat{P}^n_{Y^nX_3^nK_{13}K'_{13}K_{23}K'_{23}}(\mathbf{y},\mathbf{x}_3,k_{13},k'_{13},k_{23},k'_{23}) \triangleq Q^{\otimes n}_{Y^n|X_3^nS_{13}^nS_{23}^n}(\mathbf{y}|\mathbf{x}_3,\mathbf{s}_{13}(k_{13},k'_{13}),\mathbf{s}_{23}(k_{23},k'_{23}))$$
$$P^n_{X_3^nK_{13}K'_{13}K_{23}K'_{23}}(\mathbf{x}_3,k_{13},k'_{13}k_{23},k'_{23}). \quad (95)$$

We analyze $E(D(P^n_{Y^nX_3^nK_{13}K'_{13}K_{23}K'_{23}|K_{12}=k_{12}K_{21}=k_{21}} \parallel \widehat{P}^n_{Y^nX_3^nK_{13}K'_{13}K_{23}K'_{23}}))$, where the average is over the randomly generated code. Note that:

$$D(P^n_{Y^nX_3^nK_{13}K'_{13}K_{23}K'_{23}|K_{12}=k_{12}K_{21}=k_{21}} \parallel \widehat{P}^n_{Y^nX_3^nK_{13}K'_{13}K_{23}K'_{23}})$$
$$= \sum_{\mathbf{y}\mathbf{x}_3k_{13}k'_{13}k_{23}k'_{23}} P^n(\mathbf{y},\mathbf{x}_3,k_{13},k'_{13},k_{23},k'_{23}|k_{12},k_{21})\log_2\frac{P^n(\mathbf{y},\mathbf{x}_3,k_{13},k'_{13},k_{23},k'_{23}|k_{12},k_{21})}{\widehat{P}^n(\mathbf{y},\mathbf{x}_3,k_{13},k'_{13},k_{23},k'_{23})}$$
$$= \sum_{\mathbf{x}_3k_{13}k'_{13}k_{23}k'_{23}} P^n(\mathbf{x}_3,k_{13},k'_{13},k_{23},k'_{23})\sum_{\mathbf{y}} P^n(\mathbf{y}|\mathbf{x}_3,k_{13},k'_{13},k_{23},k'_{23},k_{12},k_{21})$$
$$\log_2\frac{P^n(\mathbf{y}|\mathbf{x}_3,k_{13},k'_{13},k_{23},k'_{23},k_{12},k_{21})}{Q^{\otimes n}_{Y^n|X_3^nS_{13}^nS_{23}^n}(\mathbf{y}|\mathbf{x}_3\mathbf{s}_{13}(k_{13},k'_{13})\mathbf{s}_{23}(k_{23},k'_{23}))} \quad (96)$$

where by construction:

$$P^n(\mathbf{x}_3,k_{13},k'_{13},k_{23},k'_{23}) = \sum_{k_{31}k'_{31}k_{32}k'_{32}} Q^{\otimes n}(\mathbf{x}_3|\mathbf{s}_{31}(k_{31},k'_{31})\mathbf{s}_{32}(k_{32},k'_{32}))\frac{1}{|\mathcal{K}_{13}\|\mathcal{K}'_{13}\|\mathcal{K}_{23}\|\mathcal{K}'_{23}\|\mathcal{K}_{31}\|\mathcal{K}'_{31}\|\mathcal{K}_{32}\|\mathcal{K}'_{32}|} \quad (97)$$

and

$$P^n(\mathbf{y}|\mathbf{x}_3,k_{13},k'_{13},k_{23},k'_{23},k_{12},k_{21}) =$$
$$\sum_{\mathbf{x}_1\mathbf{x}_2k'_{12}k'_{21}} Q^{\otimes n}(\mathbf{y}|\mathbf{x}_1\mathbf{x}_2\mathbf{x}_3)Q^{\otimes n}(\mathbf{x}_1|\mathbf{s}_{12}(k_{12},k'_{12})\mathbf{s}_{13}(k_{13},k'_{13}))Q^{\otimes n}(\mathbf{x}_2|\mathbf{s}_{21}(k_{21},k'_{21})\mathbf{s}_{23}(k_{23},k'_{23}))\frac{1}{|\mathcal{K}'_{12}||\mathcal{K}'_{21}|} \quad (98)$$

so that

$$D(P^n_{Y^n X_3^n K_{13} K'_{13} K_{23} K'_{23}|K_{12}=k_{12}K_{21}=k_{21}} \parallel \widehat{P}^n_{Y^n X_3^n K_{13} K'_{13} K_{23} K'_{23}}) =$$

$$\frac{1}{|\mathcal{K}'_{12}||\mathcal{K}'_{21}||\mathcal{K}_{13}\|\mathcal{K}'_{13}\|\mathcal{K}_{23}\|\mathcal{K}'_{23}\|\mathcal{K}_{31}\|\mathcal{K}'_{31}\|\mathcal{K}_{32}\|\mathcal{K}'_{32}|}$$

$$\sum_{\mathbf{y}\mathbf{x}_1\mathbf{x}_2\mathbf{x}_3 k'_{12}k'_{21}k_{13}k'_{13}k_{23}k'_{23}k_{31}k'_{31}k_{32}k'_{32}} Q^{\otimes n}(\mathbf{y}|\mathbf{x}_1\mathbf{x}_2\mathbf{x}_3) Q^{\otimes n}(\mathbf{x}_1|\mathbf{s}_{12}(k_{12},k'_{12})\mathbf{s}_{13}(k_{13},k'_{13}))$$

$$Q^{\otimes n}(\mathbf{x}_2|\mathbf{s}_{21}(k_{21},k'_{21})\mathbf{s}_{23}(k_{23},k'_{23})) Q^{\otimes n}(\mathbf{x}_3|\mathbf{s}_{31}(k_{31},k'_{31})\mathbf{s}_{32}(k_{32},k'_{32}))$$

$$\log_2 \frac{\sum_{\tilde{\mathbf{x}}_1\tilde{\mathbf{x}}_2\tilde{k}'_{12}\tilde{k}'_{21}} Q^{\otimes n}(\mathbf{y}|\tilde{\mathbf{x}}_1\tilde{\mathbf{x}}_2\mathbf{x}_3) Q^{\otimes n}(\tilde{\mathbf{x}}_1|\mathbf{s}_{12}(k_{12},\tilde{k}'_{12})\mathbf{s}_{13}(k_{13},k'_{13})) Q^{\otimes n}(\tilde{\mathbf{x}}_2|\mathbf{s}_{21}(k_{21},\tilde{k}'_{21})\mathbf{s}_{23}(k_{23},k'_{23}))^{\frac{1}{|\mathcal{K}'_{12}||\mathcal{K}'_{21}|}}}{Q^{\otimes n}_{Y^n|X_3^n S_{13}^n S_{23}^n}(\mathbf{y}|\mathbf{x}_3\mathbf{s}_{13}(k_{13},k'_{13})\mathbf{s}_{23}(k_{23},k'_{23}))} \tag{99}$$

Let us focus on the average of the log term, taking the average over all codewords $\mathbf{s}_{12}$ and $\mathbf{s}_{21}$ *except* than $\mathbf{s}_{12}(k_{12},k'_{12})$ and $\mathbf{s}_{21}(k_{21},k'_{21})$. Then,

$$\begin{aligned}
&E(\log_2 \frac{\sum_{\tilde{\mathbf{x}}_1\tilde{\mathbf{x}}_2\tilde{k}'_{12}\tilde{k}'_{21}} Q^{\otimes n}(\mathbf{y}|\tilde{\mathbf{x}}_1\tilde{\mathbf{x}}_2\mathbf{x}_3) Q^{\otimes n}(\tilde{\mathbf{x}}_1|\mathbf{s}_{12}(k_{12},\tilde{k}'_{12})\mathbf{s}_{13}(k_{13},k'_{13})) Q^{\otimes n}(\tilde{\mathbf{x}}_2|\mathbf{s}_{21}(k_{21},\tilde{k}'_{21})\mathbf{s}_{23}(k_{23},k'_{23}))^{\frac{1}{|\mathcal{K}'_{12}||\mathcal{K}'_{21}|}}}{Q^{\otimes n}_{Y^n|X_3^n S_{13}^n S_{23}^n}(\mathbf{y}|\mathbf{x}_3\mathbf{s}_{13}(k_{13},k'_{13})\mathbf{s}_{23}(k_{23},k'_{23}))})\\
&\overset{(a)}{\leq} \log_2 \frac{E(\sum_{\tilde{\mathbf{x}}_1\tilde{\mathbf{x}}_2\tilde{k}'_{12}\tilde{k}'_{21}} Q^{\otimes n}(\mathbf{y}|\tilde{\mathbf{x}}_1\tilde{\mathbf{x}}_2\mathbf{x}_3) Q^{\otimes n}(\tilde{\mathbf{x}}_1|\mathbf{s}_{12}(k_{12},\tilde{k}'_{12})\mathbf{s}_{13}(k_{13},k'_{13})) Q^{\otimes n}(\tilde{\mathbf{x}}_2|\mathbf{s}_{21}(k_{21},\tilde{k}'_{21})\mathbf{s}_{23}(k_{23},k'_{23}))^{\frac{1}{|\mathcal{K}'_{12}||\mathcal{K}'_{21}|}})}{Q^{\otimes n}_{Y^n|X_3^n S_{13}^n S_{23}^n}(\mathbf{y}|\mathbf{x}_3\mathbf{s}_{13}(k_{13},k'_{13})\mathbf{s}_{23}(k_{23},k'_{23}))}\\
&= \log_2 \Bigg(\frac{1}{|\mathcal{K}'_{12}||\mathcal{K}'_{21}|} \frac{\sum_{\tilde{\mathbf{x}}_1\tilde{\mathbf{x}}_2} Q^{\otimes n}(\mathbf{y}|\tilde{\mathbf{x}}_1\tilde{\mathbf{x}}_2\mathbf{x}_3) Q^{\otimes n}(\tilde{\mathbf{x}}_1|\mathbf{s}_{12}(k_{12},k'_{12})\mathbf{s}_{13}(k_{13},k'_{13})) Q^{\otimes n}(\tilde{\mathbf{x}}_2|\mathbf{s}_{21}(k_{21},k'_{21})\mathbf{s}_{23}(k_{23},k'_{23}))}{Q^{\otimes n}_{Y^n|X_3^n S_{13}^n S_{23}^n}(\mathbf{y}|\mathbf{x}_3\mathbf{s}_{13}(k_{13},k'_{13})\mathbf{s}_{23}(k_{23},k'_{23}))}\\
&\quad + \frac{|\mathcal{K}'_{12}|-1}{|\mathcal{K}'_{12}||\mathcal{K}'_{21}|} \frac{\sum_{\tilde{\mathbf{x}}_1\tilde{\mathbf{x}}_2} Q^{\otimes n}(\mathbf{y}|\tilde{\mathbf{x}}_1\tilde{\mathbf{x}}_2\mathbf{x}_3) Q^{\otimes n}(\tilde{\mathbf{x}}_1|\mathbf{s}_{13}(k_{13},k'_{13})) Q^{\otimes n}(\tilde{\mathbf{x}}_2|\mathbf{s}_{21}(k_{21},k'_{21})\mathbf{s}_{23}(k_{23},k'_{23}))}{Q^{\otimes n}_{Y^n|X_3^n S_{13}^n S_{23}^n}(\mathbf{y}|\mathbf{x}_3\mathbf{s}_{13}(k_{13},k'_{13})\mathbf{s}_{23}(k_{23},k'_{23}))}\\
&\quad + \frac{|\mathcal{K}'_{21}|-1}{|\mathcal{K}'_{12}||\mathcal{K}'_{21}|} \frac{\sum_{\tilde{\mathbf{x}}_1\tilde{\mathbf{x}}_2} Q^{\otimes n}(\mathbf{y}|\tilde{\mathbf{x}}_1\tilde{\mathbf{x}}_2\mathbf{x}_3) Q^{\otimes n}(\tilde{\mathbf{x}}_1|\mathbf{s}_{12}(k_{12},k'_{12})\mathbf{s}_{13}(k_{13},k'_{13})) Q^{\otimes n}(\tilde{\mathbf{x}}_2|\mathbf{s}_{23}(k_{23},k'_{23}))}{Q^{\otimes n}_{Y^n|X_3^n S_{13}^n S_{23}^n}(\mathbf{y}|\mathbf{x}_3\mathbf{s}_{13}(k_{13},k'_{13})\mathbf{s}_{23}(k_{23},k'_{23}))}\\
&\quad + \frac{(|\mathcal{K}'_{12}|-1)(|\mathcal{K}'_{21}|-1)}{|\mathcal{K}'_{12}||\mathcal{K}'_{21}|} \frac{\sum_{\tilde{\mathbf{x}}_1\tilde{\mathbf{x}}_2} Q^{\otimes n}(\mathbf{y}|\tilde{\mathbf{x}}_1\tilde{\mathbf{x}}_2\mathbf{x}_3) Q^{\otimes n}(\tilde{\mathbf{x}}_1|\mathbf{s}_{13}(k_{13},k'_{13})) Q^{\otimes n}(\tilde{\mathbf{x}}_2|\mathbf{s}_{23}(k_{23},k'_{23}))}{Q^{\otimes n}_{Y^n|X_3^n S_{13}^n S_{23}^n}(\mathbf{y}|\mathbf{x}_3\mathbf{s}_{13}(k_{13},k'_{13})\mathbf{s}_{23}(k_{23},k'_{23}))} \Bigg)\\
&\leq \log_2 \Bigg(\frac{1}{|\mathcal{K}'_{12}||\mathcal{K}'_{21}|} \frac{Q^{\otimes n}(\mathbf{y}|\mathbf{x}_3\mathbf{s}_{12}(k_{12},k'_{12})\mathbf{s}_{13}(k_{13},k'_{13})\mathbf{s}_{21}(k_{21},k'_{21})\mathbf{s}_{23}(k_{23},k'_{23}))}{Q^{\otimes n}_{Y^n|X_3^n S_{13}^n S_{23}^n}(\mathbf{y}|\mathbf{x}_3\mathbf{s}_{13}(k_{13},k'_{13})\mathbf{s}_{23}(k_{23},k'_{23}))}\\
&\quad + \frac{1}{|\mathcal{K}'_{21}|} \frac{Q^{\otimes n}(\mathbf{y}|\mathbf{x}_3\mathbf{s}_{13}(k_{13},k'_{13})\mathbf{s}_{21}(k_{21},k'_{21})\mathbf{s}_{23}(k_{23},k'_{23}))}{Q^{\otimes n}_{Y^n|X_3^n S_{13}^n S_{23}^n}(\mathbf{y}|\mathbf{x}_3\mathbf{s}_{13}(k_{13},k'_{13})\mathbf{s}_{23}(k_{23},k'_{23}))}\\
&\quad + \frac{1}{|\mathcal{K}'_{12}|} \frac{Q^{\otimes n}(\mathbf{y}|\mathbf{x}_3\mathbf{s}_{12}(k_{12},k'_{12})\mathbf{s}_{13}(k_{13},k'_{13})\mathbf{s}_{23}(k_{23},k'_{23}))}{Q^{\otimes n}_{Y^n|X_3^n S_{13}^n S_{23}^n}(\mathbf{y}|\mathbf{x}_3\mathbf{s}_{13}(k_{13},k'_{13})\mathbf{s}_{23}(k_{23},k'_{23}))}\\
&\quad + \frac{Q^{\otimes n}(\mathbf{y}|\mathbf{x}_3\mathbf{s}_{13}(k_{13},k'_{13})\mathbf{s}_{23}(k_{23},k'_{23}))}{Q^{\otimes n}_{Y^n|X_3^n S_{13}^n S_{23}^n}(\mathbf{y}|\mathbf{x}_3\mathbf{s}_{13}(k_{13},k'_{13})\mathbf{s}_{23}(k_{23},k'_{23}))} \Bigg)
\end{aligned} \tag{100}$$

where (a) is deduced from Jensen's inequality.

Substituting the upper bound of (100) back and taking the average over all other codewords, we obtain,

$$E(D(P^n_{Y^n X_3^n K_{13} K'_{13} K_{23} K'_{23}|K_{12}K_{21}} \parallel \widehat{P}^n_{Y^n X_3^n K_{13} K'_{13} K_{23} K'_{23}})) \leq \sum_{\mathbf{y x_3 s_{12} s_{13} s_{21} s_{23}}} Q^{\otimes n}(\mathbf{y x_3 s_{12} s_{13} s_{21} s_{23}}) \log_2 \left(\frac{1}{|\mathcal{K}'_{12}||\mathcal{K}'_{21}|} \frac{Q^{\otimes n}(\mathbf{y}|\mathbf{x}_3\mathbf{s}_{12}\mathbf{s}_{13}\mathbf{s}_{21}\mathbf{s}_{23})}{Q^{\otimes n}_{Y^n|X_3^n S_{13}^n S_{23}^n}(\mathbf{y}|\mathbf{x}_3,\mathbf{s}_{13},\mathbf{s}_{23})} + \frac{1}{|\mathcal{K}'_{21}|} \frac{Q^{\otimes n}(\mathbf{y}|\mathbf{x}_3\mathbf{s}_{13}\mathbf{s}_{21}\mathbf{s}_{23})}{Q^{\otimes n}_{Y^n|X_3^n S_{13}^n S_{23}^n}(\mathbf{y}|\mathbf{x}_3,\mathbf{s}_{13},\mathbf{s}_{23})} + \frac{1}{|\mathcal{K}'_{12}|} \frac{Q^{\otimes n}(\mathbf{y}|\mathbf{x}_3\mathbf{s}_{12}\mathbf{s}_{13}\mathbf{s}_{23}))}{Q^{\otimes n}_{Y^n|X_3^n S_{13}^n S_{23}^n}(\mathbf{y}|\mathbf{x}_3,\mathbf{s}_{13},\mathbf{s}_{23})} + 1 \right) \quad (101)$$

We split the sum between the sequences that are jointly typical, and those that are not.

- If $(\mathbf{y}, \mathbf{x}_3, \mathbf{s}_{12}, \mathbf{s}_{13}, \mathbf{s}_{21}, \mathbf{s}_{23}) \in \mathcal{T}^n_{\epsilon'}(Q_{Y X_3 S_{12} S_{13} S_{21} S_{23}})$, the log argument is upper bounded by

$$\frac{2^{n(I(S_{12},S_{21};Y|X_3,S_{13},S_{23})+2\epsilon')}}{|\mathcal{K}'_{12}||\mathcal{K}'_{21}|} + \frac{2^{n(I(S_{21};Y|X_3,S_{13},S_{23})+2\epsilon')}}{|\mathcal{K}'_{21}|} + \frac{2^{n(I(S_{12};Y|X_3,S_{13},S_{23})+2\epsilon')}}{|\mathcal{K}'_{12}|} + 1 \quad (102)$$

  If we have

$$r'_{12} + r'_{21} > I(S_{12}, S_{21}; Y|X_3, S_{13}, S_{23}) + 2\epsilon'. \quad (103)$$

$$r'_{21} > I(S_{21}; Y|X_3, S_{13}, S_{23}) + 2\epsilon' \quad (104)$$

$$r'_{12} > I(S_{12}; Y|X_3, S_{13}, S_{23}) + 2\epsilon'. \quad (105)$$

  then for sufficiently large n, the log argument can be bounded by $3\epsilon' + 1$.

- If $(\mathbf{y}, \mathbf{x}_3, \mathbf{s}_{12}, \mathbf{s}_{13}, \mathbf{s}_{21}, \mathbf{s}_{23}) \notin \mathcal{T}^n_{\epsilon'}(Q_{Y X_3 S_{12} S_{13} S_{21} S_{23}})$, the log term is upper bounded by $\log_2(3\mu^{-n}+1)$ where

$$\mu \triangleq \min_{Q(y|x_3 s_{13} s_{23})>0} Q(y|x_3 s_{13} s_{23}). \quad (106)$$

  Hence, the sum over the non typical sequences is bounded by $\epsilon' \log_2(3\mu^{-n} + 1)$.

Finally, the sum in (101) is bounded as

$$E(D(P^n_{Y^n X_3^n K_{13} K'_{13} K_{23} K'_{23}|K_{12}K_{21}} \parallel \widehat{P}^n_{Y^n X_3^n K_{13} K'_{13} K_{23} K'_{23}})) \leq \epsilon' \log_2(3\mu^{-n} + 1) + \log(3\epsilon' + 1) \quad (107)$$

which vanishes as n goes to infinity and ϵ' goes to zero. ■

Now, we follow secure communication between each pair of the users in the pre-generated keys scheme using the general result in Proposition 1. Since the model in Fig. 10 is symmetric, we can appropriately substitute the random variables to deduce secrecy from resolvability condition against the intended user. In particular:

- by substituting $Y = Y_3, X_3 = S_{31} = S_{32} = K_{31} = K_{32} = K'_{31} = K'_{32} = \phi$ in Fig. 10 and using Proposition 1, secrecy from resolvability condition against User 3 is obtained.
- by substituting $Y = Y_2, X_3 = S_{31} = S_{32} = K_{31} = K_{32} = K'_{31} = K'_{32} = \phi$ in Fig. 10 and using Proposition

1, secrecy from resolvability condition against User 2 is obtained.

- by substituting $Y = Y_1, X_3 = S_{31} = S_{32} = K_{31} = K_{32} = K'_{31} = K'_{32} = \phi$ in Fig. 10 and using Proposition 1, secrecy from resolvability condition against User 1 is obtained.

Lemma 4 (Secrecy from channel resolvability conditions): If (71)-(75) hold, then there exist $\alpha > 0, \beta > 0$ and $\gamma > 0$ such that

$$E(D(P^n_{Y_3^n K_{13} K'_{13} K_{23} K'_{23}|K_{12}K_{21}} \parallel \widehat{P}^n_{Y_3^n K_{13} K'_{13} K_{23} K'_{23}})) \leq 2^{-\alpha n} \tag{108}$$

$$E(D(P^n_{Y_2^n X_2^n K_{12} K'_{12}|K_{13}} \parallel \widehat{P}^n_{Y_2^n X_2^n K_{12} K'_{12}})) \leq 2^{-\beta n} \tag{109}$$

$$E(D(P^n_{Y_1^n X_1^n K_{21} K'_{21}|K_{23}} \parallel \widehat{P}^n_{Y_1^n X_1^n K_{21} K'_{21}})) \leq 2^{-\gamma n} \tag{110}$$

To deduce (76)-(78) in Lemma 2 in Appendix A, we substitute $Y_3 = (Y_3, T_{13}, T_{23}), Y_2 = (Y_2, T_{12})$ and $Y_1 = (Y_1, T_{21})$ in (108)-(110) and use the independence of auxiliary random variables S_{12}, S_{13}, S_{21} and S_{23}.

APPENDIX C
PROOF OF STRONG SECRECY OF THE SECONDARY KEYS IN THEOREM 3

In the generalized scheme, both wiretap coding and secret key generation are used where the latter uses the channel outputs correlation as induced sources. For the wiretap codebook, the channel resolvability was used in Appendix B to prove strong secrecy of the primary keys. For the secondary keys, the outputs of the GDMMAC are exploited as source observations to share secret keys and the transmitted information by Users 1 and 2 needs to satisfy (46)-(50). We consider the secondary keys generation between Users 1 and 2 and prove strong secrecy for the secondary key pair $(k_{12,s}, k_{21,s})$ where the notations are borrowed from Appendix A. Here, we drop the index s since we just deal with the secondary keys. The secondary keys generation between Users 1 and 2 against User 3 is shown in Fig. 11.

The objective is to extract uniformly distributed keys $k_{12} \in \{1,...,2^{nr_{12}}\}$ and $k_{21} \in \{1,...,2^{nr_{21}}\}$ at User 2 and User 1, respectively, where the keys are independent of each other and of User 3's observation, i.e.,

$$\mathbf{z} = z^n = (y_3^n, t_{13}^n, t_{23}^n, s_{13}^n, s_{23}^n, s_{12}^n, s_{21}^n) \tag{111}$$

We assume that User 3 has already decoded his intended codewords t_{13}^n and t_{23}^n of the secondary keys from Users 1 and 2, respectively, and all the codewords of the primary keys, i.e., $(s_{13}^n, s_{23}^n, s_{12}^n, s_{21}^n)$. To prove Lemma 3 in Appendix A, we show that:

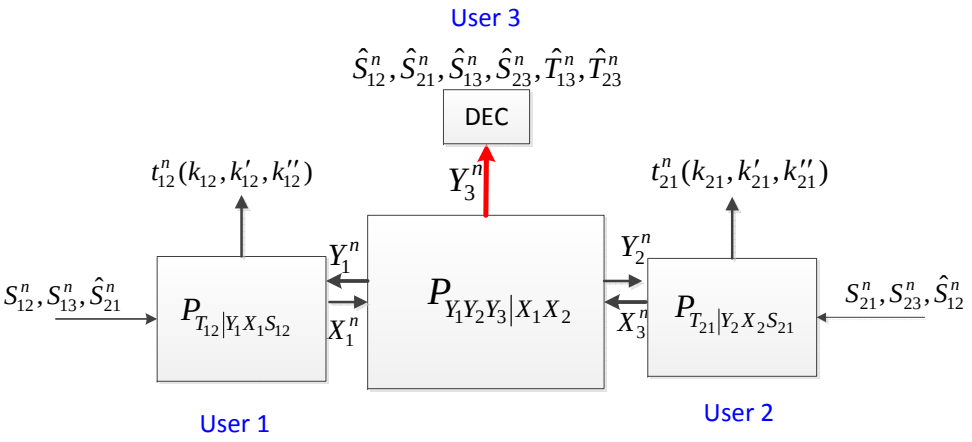


Fig. 11: Model for Proposition 2

Proposition 2:

$$I(K_{12}, K_{21}, K_{12}', K_{21}', K_{12}'', K_{21}''; Z^n) \leq$$

$$E(D(P_{K_{12},K_{21},K_{12}',K_{21}',K_{12}'',K_{21}'',Z^n} \parallel q_{K_{12}} q_{K_{21}} q_{K_{12}'} q_{K_{21}'} q_{K_{12}''} q_{K_{21}''} P_{Z^n})) \to 0 \tag{112}$$

for sufficiently large n, where $q_{K_{ij}}$, $q_{K_{ij}'}$ and $q_{K_{ij}''}$ have uniform distributions over $\{1,...,2^{nr_{ij}}\}, \{1,...,2^{nr_{ij}'}\}$ and $\{1,...,2^{nr_{ij}''}\}$, respectively, for $i = 1, 2$, $j = 1, 2$ and $i \neq j$.

Proof: To prove Proposition 2, we use the random binning mappings ϕ_{ij}, ψ_{ij} and θ_{ij} as defined in Appendix A.

Using the law of total probability, the joint distribution $p_{k_{12},k_{21},k_{12}',k_{21}',k_{12}'',k_{21}'',z^n}$ can be expressed as follows:

$$p(k_{12}, k_{21}, k_{12}', k_{21}', k_{12}'', k_{21}'', z^n) = \sum_{\mathbf{t}_{12}\mathbf{t}_{21}} p(\mathbf{t}_{12}, \mathbf{t}_{21}, \mathbf{z}) \Pr\{\phi_{12}(\mathbf{t}_{12}) = k_{12}\} \Pr\{\psi_{12}(\mathbf{t}_{12}) = k_{12}'\}$$

$$\Pr\{\theta_{12}(\mathbf{t}_{12}) = k_{12}''\} \Pr\{\phi_{21}(\mathbf{t}_{21}) = k_{21}\} \Pr\{\psi_{21}(\mathbf{t}_{21}) = k_{21}'\} \Pr\{\theta_{21}(\mathbf{t}_{21}) = k_{21}''\} \tag{113}$$

To simplify the notation, we define:

$$P(\phi_{ij}, \psi_{ij}, \theta_{ij}, \mathbf{t}_{ij}, k_{ij}, k_{ij}', k_{ij}'') \triangleq \Pr\{\phi_{ij}(\mathbf{t}_{ij}) = k_{ij}\} \Pr\{\psi_{ij}(\mathbf{t}_{ij}) = k_{ij}'\} \Pr\{\theta_{ij}(\mathbf{t}_{ij}) = k_{ij}''\} \tag{114}$$

Now, we evaluate $E_{\Phi_{12}\Psi_{12}\Theta_{12}\Phi_{21}\Psi_{21}\Theta_{21}}(D(P_{K_{12},K_{21},K_{12}',K_{21}',K_{12}'',K_{21}'',Z^n} \| q_{K_{12}} q_{K_{21}} q_{K_{12}'} q_{K_{21}'} q_{K_{12}''} q_{K_{21}''} P_{Z^n}))$.

By definition, we have:

$$
\begin{aligned}
&D(P_{K_{12},K_{21},K'_{12},K'_{21},K''_{12},K''_{21},Z^n} \parallel q_{K_{12}}q_{K_{21}}q_{K'_{12}}q_{K'_{21}}q_{K''_{12}}q_{K''_{21}}P_{Z^n}) \\
&\qquad = \sum_{k_{12}k_{21}k'_{12}k'_{21}k''_{12}k''_{21}\mathbf{z}} p(k_{12},k_{21},k'_{12},k'_{21},k''_{12},k''_{21},\mathbf{z}) \log_2 \frac{p(k_{12},k_{21},k'_{12},k'_{21},k''_{12},k''_{21},\mathbf{z})}{q_{k_{12}}q_{k_{21}}q_{k'_{12}}q_{k'_{21}}q_{k''_{12}}q_{k''_{21}}p_{\mathbf{z}}} \\
&\quad = \sum_{k_{12}k_{21}k'_{12}k'_{21}k''_{12}k''_{21}\mathbf{t}_{12}\mathbf{t}_{21}\mathbf{z}} p(\mathbf{t}_{12},\mathbf{t}_{21},\mathbf{z})P(\phi_{12},\psi_{12},\theta_{12},\mathbf{t}_{12},k_{12},k'_{12},k''_{12})P(\phi_{21},\psi_{21},\theta_{21},\mathbf{t}_{21},k_{21},k'_{21},k''_{21})\times \\
&\qquad\qquad \log_2 \frac{\sum_{\tilde{\mathbf{t}}_{12}\tilde{\mathbf{t}}_{21}} p(\tilde{\mathbf{t}}_{12},\tilde{\mathbf{t}}_{21},\mathbf{z})P(\phi_{12},\psi_{12},\theta_{12},\tilde{\mathbf{t}}_{12},k_{12},k'_{12},k''_{12})P(\phi_{21},\psi_{21},\theta_{21},\tilde{\mathbf{t}}_{21},k_{21},k'_{21},k''_{21})}{q_{k_{12}}q_{k_{21}}q_{k'_{12}}q_{k'_{21}}q_{k''_{12}}q_{k''_{21}}p_{\mathbf{z}}}
\end{aligned} \tag{115}
$$

Then, we focus on the log term in (115) and take the average over possible values of $\Phi_{ij}(\tilde{t}^n_{ij})\Psi_{ij}(\tilde{t}^n_{ij})$ and $\Theta_{ij}(\tilde{t}^n_{ij})$ for all $\tilde{t}^n_{12} \neq t^n_{12}$ and $\tilde{t}^n_{21} \neq t^n_{21}$ which is denoted by $\tilde{E}$. We have:

$$
\begin{aligned}
&\tilde{E}(\log_2 \frac{\sum_{\tilde{\mathbf{t}}_{12}\tilde{\mathbf{t}}_{21}} p(\tilde{\mathbf{t}}_{12},\tilde{\mathbf{t}}_{21},\mathbf{z})P(\phi_{12},\psi_{12},\theta_{12},\tilde{\mathbf{t}}_{12},k_{12},k'_{12},k''_{12})P(\phi_{21},\psi_{21},\theta_{21},\tilde{\mathbf{t}}_{21},k_{21},k'_{21},k''_{21})}{q_{k_{12}}q_{k_{21}}q_{k'_{12}}q_{k'_{21}}q_{k''_{12}}q_{k''_{21}}p_{\mathbf{z}}}) \\
&\qquad \overset{(a)}{\leq} \log_2 \frac{\tilde{E}(\sum_{\tilde{\mathbf{t}}_{12}\tilde{\mathbf{t}}_{21}} p(\tilde{\mathbf{t}}_{12},\tilde{\mathbf{t}}_{21},\mathbf{z})P(\phi_{12},\psi_{12},\theta_{12},\tilde{\mathbf{t}}_{12},k_{12},k'_{12},k''_{12})P(\phi_{21},\psi_{21},\theta_{21},\tilde{\mathbf{t}}_{21},k_{21},k'_{21},k''_{21}))}{q_{k_{12}}q_{k_{21}}q_{k'_{12}}q_{k'_{21}}p_{\mathbf{z}}}
\end{aligned} \tag{116}
$$

where (a) is deduced from Jensen's inequality.

We extend various terms inside $\tilde{E}$ in (116) as follow:

$$
\begin{aligned}
&\tilde{E}(\sum_{\tilde{\mathbf{t}}_{12}\tilde{\mathbf{t}}_{21}} p(\tilde{\mathbf{t}}_{12},\tilde{\mathbf{t}}_{21},\mathbf{z})P(\phi_{12},\psi_{12},\theta_{12},\tilde{\mathbf{t}}_{12},k_{12},k'_{12},k''_{12})P(\phi_{21},\psi_{21},\theta_{21},\tilde{\mathbf{t}}_{21},k_{21},k'_{21},k''_{21})) \\
&\qquad = p(\mathbf{t}_{12},\mathbf{t}_{21},\mathbf{z})P(\phi_{12},\psi_{12},\theta_{12},\mathbf{t}_{12},k_{12},k'_{12},k''_{12})P(\phi_{21},\psi_{21},\theta_{21},\mathbf{t}_{21},k_{21},k'_{21},k''_{21}) + \\
&\qquad\qquad \sum_{\tilde{\mathbf{t}}_{21}\neq\mathbf{t}_{21}} p(\mathbf{t}_{12},\tilde{\mathbf{t}}_{21},\mathbf{z})P(\phi_{12},\psi_{12},\theta_{12},\mathbf{t}_{12},k_{12},k'_{12},k''_{12})\frac{1}{2^{n(r_{21}+r'_{21}+r''_{21})}} + \\
&\qquad\qquad \sum_{\tilde{\mathbf{t}}_{12}\neq\mathbf{t}_{12}} p(\tilde{\mathbf{t}}_{12},\mathbf{t}_{21},\mathbf{z})P(\phi_{21},\psi_{21},\theta_{21},\mathbf{t}_{21},k_{21},k'_{21},k''_{21})\frac{1}{2^{n(r_{12}+r'_{12}+r''_{12})}} + \\
&\qquad\qquad\qquad \sum_{\tilde{\mathbf{t}}_{12}\neq\mathbf{t}_{12}\tilde{\mathbf{t}}_{21}\neq\mathbf{t}_{21}} p(\tilde{\mathbf{t}}_{12},\tilde{\mathbf{t}}_{21},\mathbf{z})\frac{1}{2^{n(r_{12}+r'_{12}+r''_{12}+r_{21}+r'_{21}+r''_{21})}} \\
&\qquad \leq p(\mathbf{t}_{12},\mathbf{t}_{21},\mathbf{z})P(\phi_{12},\psi_{12},\theta_{12},\mathbf{t}_{12},k_{12},k'_{12},k''_{12})P(\phi_{21},\psi_{21},\theta_{21},\mathbf{t}_{21},k_{21},k'_{21},k''_{21}) + \\
&\qquad\qquad p(\mathbf{t}_{12},\mathbf{z})P(\phi_{12},\psi_{12},\theta_{12},\mathbf{t}_{12},k_{12},k'_{12},k''_{12})\frac{1}{2^{n(r_{21}+r'_{21}+r''_{21})}} + \\
&\qquad p(\mathbf{t}_{21},\mathbf{z})P(\phi_{21},\psi_{21},\theta_{21},\mathbf{t}_{21},k_{21},k'_{21},k''_{21})\frac{1}{2^{n(r_{12}+r'_{12}+r''_{12})}} + p(\mathbf{z})\frac{1}{2^{n(r_{12}+r'_{12}+r''_{12}+r_{21}+r'_{21}+r''_{21})}}
\end{aligned} \tag{117}
$$

Since $q_{k_{ij}} = \frac{1}{2^{nr_{ij}}},, q_{k'_{ij}} = \frac{1}{2^{nr'_{ij}}}$ and $q_{k''_{ij}} = \frac{1}{2^{nr''_{ij}}}$, the log term in (116) is obtained as:

$$\log_2 \frac{\tilde{E}(\sum_{\tilde{\mathbf{t}}_{12}\tilde{\mathbf{t}}_{21}} p(\tilde{\mathbf{t}}_{12},\tilde{\mathbf{t}}_{21},\mathbf{z})P(\phi_{12},\psi_{12},\theta_{12},\tilde{\mathbf{t}}_{12},k_{12},k'_{12},k''_{12})P(\phi_{21},\psi_{21},\theta_{21},\tilde{\mathbf{t}_{21}},k_{21},k'_{21},k''_{21}))}{q_{k_{12}}q_{k_{21}}q_{k'_{12}}q_{k'_{21}}p_{\mathbf{z}}}$$

$$\leq \log_2\Big(p(\mathbf{t}_{12},\mathbf{t}_{21}|\mathbf{z})P(\phi_{12},\psi_{12},\theta_{12},\mathbf{t}_{12},k_{12},k'_{12},k''_{12})P(\phi_{21},\psi_{21},\theta_{21},\mathbf{t}_{21},k_{21},k'_{21},k''_{21})2^{n(r_{12}+r_{21}+r'_{12}+r'_{21}+r''_{12}+r''_{21})}+$$

$$p(\mathbf{t}_{12}|\mathbf{z})P(\phi_{12},\psi_{12},\theta_{12},\mathbf{t}_{12},k_{12},k'_{12},k''_{12})2^{n(r_{12}+r'_{12}+r''_{12})}+$$

$$p(\mathbf{t}_{21}|\mathbf{z})P(\phi_{21},\psi_{21},\theta_{21},\mathbf{t}_{21},k_{21},k'_{21},k''_{21})2^{n(r_{21}+r'_{21}+r''_{21})}+1\Big) \quad (118)$$

By substituting (118) in (115) and taking the average over all random binning mappings, we have:

$$E_{\Phi_{12}\Psi_{12}\Theta_{12}\Phi_{21}\Psi_{21}\Theta_{21}}(D(P_{K_{12},K_{21},K'_{12},K'_{21},K''_{12},K''_{21},Z^n} \parallel q_{K_{12}}q_{K_{21}}q_{K'_{12}}q_{K'_{21}}q_{K''_{12}}q_{K''_{21}}P_{Z^n})) \leq$$

$$\sum_{k_{12}k_{21}k'_{12}k'_{21}k''_{12}k''_{21}\mathbf{t}_{12}\mathbf{t}_{21}\mathbf{z}} p(\mathbf{t}_{12},\mathbf{t}_{21},\mathbf{z}) \sum_{\phi_{12}(\mathbf{t}_{12})\psi_{12}(\mathbf{t}_{12})\theta_{12}(\mathbf{t}_{12})} \frac{P(\phi_{12},\psi_{12},\theta_{12},\mathbf{t}_{12},k_{12},k'_{12},k''_{12})}{2^{n(r_{12}+r'_{12}+r''_{12})}} \sum_{\phi_{21}(\mathbf{t}_{21})\psi_{21}(\mathbf{t}_{21})\theta_{21}(\mathbf{t}_{21})} \frac{P(\phi_{21},\psi_{21},\theta_{21},\mathbf{t}_{21},k_{21},k'_{21},k''_{21})}{2^{n(r_{21}+r'_{21}+r''_{21})}}$$

$$\times \log_2\Big(p(\mathbf{t}_{12},\mathbf{t}_{21}|\mathbf{z})P(\phi_{12},\psi_{12},\theta_{12},\mathbf{t}_{12},k_{12},k'_{12},k''_{12})P(\phi_{21},\psi_{21},\theta_{21},\mathbf{t}_{21},k_{21},k'_{21},k''_{21})2^{n(r_{12}+r_{21}+r'_{12}+r'_{21}+r''_{12}+r''_{21})}+$$

$$p(\mathbf{t}_{12}|\mathbf{z})P(\phi_{12},\psi_{12},\theta_{12},\mathbf{t}_{12},k_{12},k'_{12},k''_{12})2^{n(r_{12}+r'_{12}+r''_{12})}+$$

$$p(\mathbf{t}_{21}|\mathbf{z})P(\phi_{21},\psi_{21},\theta_{21},\mathbf{t}_{21},k_{21},k'_{21},k''_{21})2^{n(r_{21}+r'_{21}+r''_{21})}+1\Big)$$

$$\leq \sum_{k_{12}k_{21}k'_{12}k'_{21}k''_{12}k''_{21}\mathbf{t}_{12}\mathbf{t}_{21}\mathbf{z}} p(\mathbf{t}_{12},\mathbf{t}_{21},\mathbf{z}) \sum_{\phi_{12}(\mathbf{t}_{12})\psi_{12}(\mathbf{t}_{12})\theta_{12}(\mathbf{t}_{12})} \frac{P(\phi_{12},\psi_{12},\theta_{12},\mathbf{t}_{12},k_{12},k'_{12},k''_{12})}{2^{n(r_{12}+r'_{12}+r''_{12})}} \sum_{\phi_{21}(\mathbf{t}_{21})\psi_{21}(\mathbf{t}_{21})\theta_{21}(\mathbf{t}_{21})} \frac{P(\phi_{21},\psi_{21},\theta_{21},\mathbf{t}_{21},k_{21},k'_{21},k''_{21})}{2^{n(r_{21}+r'_{21}+r''_{21})}}$$

$$\times \log_2\left(p(\mathbf{t}_{12},\mathbf{t}_{21}|\mathbf{z})2^{n(r_{12}+r'_{12}+r''_{12}+r_{21}+r'_{21}+r''_{21})}+p(\mathbf{t}_{12}|\mathbf{z})2^{n(r_{12}+r'_{12})}+p(\mathbf{t}_{21}|\mathbf{z})2^{n(r_{21}+r'_{21})}+1\right)$$

$$= \sum_{\mathbf{t}_{12}\mathbf{t}_{21}\mathbf{z}} p(\mathbf{t}_{12},\mathbf{t}_{21},\mathbf{z}) \log_2\left(p(\mathbf{t}_{12},\mathbf{t}_{21}|\mathbf{z})2^{n(r_{12}+r'_{12}+r''_{12}+r_{21}+r'_{21}+r''_{21})}+p(\mathbf{t}_{12}|\mathbf{z})2^{n(r_{12}+r'_{12}+r''_{12})}+p(\mathbf{t}_{21}|\mathbf{z})2^{n(r_{21}+r'_{21}+r''_{21})}+1\right) \quad (119)$$

To analyze (119), we split the sum between the following sequences:

- If $(\mathbf{t}_{12},\mathbf{t}_{21},\mathbf{z}) \in \mathcal{T}^n_{\epsilon''}(P_{T_{12}T_{21}Z})$, then the log term in (119) is upper bounded by

$$\log_2\left(2^{-n(H(T_{12},T_{21}|Z)-2\epsilon'')}2^{n(r_{12}+r'_{12}+r''_{12}+r_{21}+r'_{21}+r''_{21})}+2^{-n(H(T_{12}|Z)-2\epsilon'')}2^{n(r_{12}+r'_{12}+r''_{12})}+\right.$$

$$\left.2^{-n(H(T_{21}|Z)-2\epsilon'')}2^{n(r_{21}+r'_{21}+r''_{21})}+1\right) \quad (120)$$

  By substituting $Z = (Y_3, T_{13}, T_{23}, S_{13}, S_{23}, S_{12}, S_{21})$ in (120) and using the conditions (79)-(81) in Lemma 3, the log term in (120) can be bounded by $\log(3\epsilon''+1)$ for sufficiently large n.

- If $(\mathbf{t}_{12},\mathbf{t}_{21},\mathbf{z}) \notin \mathcal{T}^n_{\epsilon''}(P_{T_{12}T_{21}Z})$, then the log term in (119) is upper bounded by

$$\log_2\Big(p(\mathbf{t}_{12},\mathbf{t}_{21}|\mathbf{z})2^{n(r_{12}+r'_{12}+r''_{12}+r_{21}+r'_{21}+r''_{21})}+p(\mathbf{t}_{12}|\mathbf{z})2^{n(r_{12}+r'_{12}+r''_{12})}+p(\mathbf{t}_{21}|\mathbf{z})2^{n(r_{21}+r'_{21}+r''_{21})}+1\Big)$$

$$\leq \log_2\left(\mu^{-n}2^{n(r_{12}+r'_{12}+r''_{12}+r_{21}+r'_{21}+r''_{21})}+\mu^{-n}2^{n(r_{12}+r'_{12}+r''_{12})}+\mu^{-n}2^{n(r_{21}+r'_{21}+r''_{21})}+1\right)$$

$$\leq \log_2(3\mu^{-n}2^{n(r_{12}+r'_{12}+r''_{12}+r_{21}+r'_{21}+r''_{21})}+1)$$

where

$$\mu \triangleq \min_{p(z)>0} p(z). \tag{121}$$

Hence, the sum over the non-typical sequences is bounded by

$$\epsilon'' \log_2(3\mu^{-n} 2^{n(r_{12}+r'_{12}+r''_{12}+r_{21}+r'_{21}+r''_{21})}+1).$$

Finally, the sum in (119) is bounded as

$$\begin{aligned} E(D(P_{K_{12},K_{21},K'_{12},K'_{21},K''_{12},K''_{21},Y_3^n,T_{13}^n,T_{23}^n,S_{13}^n,S_{23}^n,S_{12}^n,S_{21}^n} \parallel q_{K_{12}} q_{K_{21}} q_{K'_{12}} q_{K'_{21}} q_{K''_{12}} q_{K''_{21}} P_{Z^n})) \leq \\ \epsilon'' \log_2(3\mu^{-n} 2^{n(r_{12}+r'_{12}+r''_{12}+r_{21}+r'_{21}+r''_{21})}+1)+\log(3\epsilon''+1) \end{aligned} \tag{122}$$

which vanishes as n goes to infinity and ϵ'' goes to zero. To obtain (122) we substituted z as in (111). ■

The same approach as in Proposition 2 can be applied to the secondary keys between Users 1 and 3 and, between Users 2 and 3. In particular, by using (82) and (83) in Lemma 3, we have:

$$\begin{aligned} E_(D(P_{K_{13},K'_{13},K''_{13},Y_2^n,X_2^n,S_{12}^n,T_{12}^n,S_{13}^n,S_{23}^n,T_{23}^n} \parallel q_{K_{13}} q_{K'_{13}} q_{K''_{13}} P_{Y_2^n,X_2^n,S_{12}^n,T_{12}^n,S_{13}^n,S_{23}^n,T_{23}^n})) \leq \\ \epsilon'' \log_2(\mu'^{-n} 2^{n(r_{13}+r'_{13}+r''_{13})}+1) + \log(\epsilon''+1) \end{aligned} \tag{123}$$

$$\begin{aligned} E_(D(P_{K_{23},K'_{23},K''_{23},Y_1^n,X_1^n,S_{21}^n,T_{21}^n,S_{13}^n,S_{23}^n,T_{13}^n} \parallel q_{K_{23}} q_{K'_{23}} q_{K''_{23}} P_{Y_1^n,X_1^n,S_{21}^n,T_{21}^n,S_{13}^n,S_{23}^n,T_{13}^n})) \leq \\ \epsilon'' \log_2(\mu''^{-n} 2^{n(r_{23}+r'_{23}+r''_{23})}+1) + \log(\epsilon''+1) \end{aligned} \tag{124}$$

Now, we follow the result in Proposition 2 and also (123)-(124) to show strong secrecy of the secondary keys between the users.

Lemma 5 (Strong secrecy of the secondary keys): If (79)-(83) hold, then there exist $\alpha > 0, \beta > 0$ and $\gamma > 0$ such that

$$E_{\Phi\Psi}(D(P_{K_{12},K_{21},K'_{12},K'_{21},K''_{12},K''_{21},Y_3^n,T_{13}^n,T_{23}^n,S_{13}^n,S_{23}^n,S_{12}^n,S_{21}^n} \| q_{K_{12}} q_{K_{21}} P_{Y_3^n,T_{13}^n,T_{23}^n,S_{13}^n,S_{23}^n,S_{12}^n,S_{21}^n})) \leq 2^{-\alpha n} \tag{125}$$

$$E_(D(P_{K_{13},K'_{13},K''_{13},Y_2^n,X_2^n,S_{12}^n,T_{12}^n,S_{13}^n,S_{23}^n,T_{23}^n} \parallel q_{K_{13}} P_{Y_2^n,X_2^n,S_{12}^n,T_{12}^n,S_{13}^n,S_{23}^n,T_{23}^n})) \leq 2^{-\beta n} \tag{126}$$

$$E_(D(P_{K_{23},K'_{23},K''_{23},Y_1^n,X_1^n,S_{21}^n,T_{21}^n,S_{13}^n,S_{23}^n,T_{13}^n} \parallel q_{K_{23}} P_{Y_1^n,X_1^n,S_{21}^n,T_{21}^n,S_{13}^n,S_{23}^n,T_{13}^n})) \leq 2^{-\gamma n} \tag{127}$$

It should be note that we performed the security analysis based on the simpler distribution P as in (31) in Appendix A. To show that the same analysis is valid for the induced distribution $\tilde{P}$ from the encoding scheme as in (30), we use the fact that according to (45), the distance between distributions P and $\tilde{P}$ is arbitrarily small and hence the same security analysis holds for distribution $\tilde{P}$.

Furthermore, applying the same approach as in the decoding error probability analysis in Appendix A, we can show:

$$E_{K_{12}''K_{21}''}(D(P_{K_{12},K_{21},K_{12}',K_{21}',Y_3^n,T_{13}^n,T_{23}^n,S_{13}^n,S_{23}^n,S_{12}^n,S_{21}^n|K_{12}'',K_{21}''} \,\|\, q_{K_{12}}q_{K_{21}}q_{K_{12}'}q_{K_{21}'}P_{Y_3^n,T_{13}^n,T_{23}^n,S_{13}^n,S_{23}^n,S_{12}^n,S_{21}^n})) \leq 2^{-\alpha n} \quad (128)$$

$$E_{K_{13}''}(D(P_{K_{13},K_{13}',Y_2^n,X_2^n,S_{12}^n,T_{12}^n,S_{13}^n,S_{23}^n,T_{23}^n|K_{13}''} \,\|\, q_{K_{13}}q_{K_{13}'}P_{Y_2^n,X_2^n,S_{12}^n,T_{12}^n,S_{13}^n,S_{23}^n,T_{23}^n})) \leq 2^{-\beta n} \quad (129)$$

$$E_{K_{23}''}(D(P_{K_{23},K_{23}',Y_1^n,X_1^n,S_{21}^n,T_{21}^n,S_{13}^n,S_{23}^n,T_{13}^n|K_{23}''} \,\|\, q_{K_{23}}q_{K_{23}'}P_{Y_1^n,X_1^n,S_{21}^n,T_{21}^n,S_{13}^n,S_{23}^n,T_{13}^n})) \leq 2^{-\gamma n} \quad (130)$$

and similarly, for the chosen $k_{12}^{''*}, k_{21}^{''*}, k_{13}^{''*}$ and $k_{23}^{''*}$ in Appendix A, we have:

$$D(P_{K_{12},K_{21},K_{12}',K_{21}',Y_3^n,T_{13}^n,T_{23}^n,S_{13}^n,S_{23}^n,S_{12}^n,S_{21}^n|k_{12}^{''*},k_{21}^{''*}} \,\|\, q_{K_{12}}q_{K_{21}}q_{K_{12}'}q_{K_{21}'}P_{Y_3^n,T_{13}^n,T_{23}^n,S_{13}^n,S_{23}^n,S_{12}^n,S_{21}^n})) \leq 3.2^{-\alpha n} \quad (131)$$

$$D(P_{K_{13},K_{13}',Y_2^n,X_2^n,S_{12}^n,T_{12}^n,S_{13}^n,S_{23}^n,T_{23}^n|k_{13}^{''*}} \,\|\, q_{K_{13}}q_{K_{13}'}P_{Y_2^n,X_2^n,S_{12}^n,T_{12}^n,S_{13}^n,S_{23}^n,T_{23}^n})) \leq 3.2^{-\beta n} \quad (132)$$

$$D(P_{K_{23},K_{23}',Y_1^n,X_1^n,S_{21}^n,T_{21}^n,S_{13}^n,S_{23}^n,T_{13}^n|k_{23}^{''*}} \,\|\, q_{K_{23}}q_{K_{23}'}P_{Y_1^n,X_1^n,S_{21}^n,T_{21}^n,S_{13}^n,S_{23}^n,T_{13}^n})) \leq 3.2^{-\gamma n} \quad (133)$$

Hence, Lemma 3 in Appendix A is deduced.

APPENDIX D
PROOF OF THE OUTER BOUND IN THEOREM 2

Since the pre-generated keys scheme is a special case of the generalized scheme, the outer bound on the secret-key capacity region of the generalized scheme applies to the pre-generated keys scheme, as well. Since, the upper bounds on R_{12} are the same in Theorem 2 and Theorem 4, we refer the reader to the bound on R_{12} derived as part of the proof of Theorem 4 in Appendix E. In the following, we only prove upper bounds on R_{13} and R_{23}.

In the pre-generated keys scheme, Users 1 and 2 independently generate the uniformly distributed keys K_{13} and K_{23}, respectively, to share with User 3. After sending the channel inputs by Users 1 and 2, Y_i^n is received by User i for $i \in \{1,2,3\}$. Applying Fano's inequality on K_{13} and K_{23}, for an arbitrary small $\epsilon > 0$, we obtain:

$$H(K_{13}, K_{23}|Y_3^n) \leq n\left(\frac{h(\epsilon)}{n} + \epsilon \log(|\mathcal{K}_{13}||\mathcal{K}_{23}| - 1)\right) \triangleq n\epsilon_1 \quad (134)$$

where $|\mathcal{K}_{13}|$ is the cardinality of key set $\mathcal{K}_{13}$, and $\epsilon_1 \to 0$ if $\epsilon \to 0$. Furthermore, the security conditions should be satisfied as:

$$I(K_{13}; X_2^n, Y_2^n) < n\epsilon \quad (135)$$

$$I(K_{23}; X_1^n, Y_1^n) < n\epsilon \quad (136)$$

Next, we show that for secret key K_{13} satisfying the reliability and security conditions, the upper bound on R_{13}

in Theorem 2 is satisfied. The upper bound on R_{23} may be proved in an identical way.

$$\begin{aligned} nR_{13} \leq H(K_{13}) + n\epsilon &\overset{(a)}{\leq} H(K_{13}|X_2^n, Y_2^n) + 2n\epsilon \\ &\overset{(b)}{\leq} H(K_{13}|X_2^n, Y_2^n) - H(K_{13}|Y_3^n) + 2n\epsilon + n\epsilon_1 \\ &\leq H(K_{13}|X_2^n, Y_2^n) - H(K_{13}|X_2^n, Y_2^n, Y_3^n) + 2n\epsilon + n\epsilon_1 \\ &= I(K_{13}; Y_3^n|X_2^n, Y_2^n) + 2n\epsilon + n\epsilon_1 \\ &\overset{(c)}{\leq} I(X_{13}^n; Y_3^n|X_2^n, Y_2^n) + 2n\epsilon + n\epsilon_1 \\ &\overset{(d)}{\leq} nI(X_{13}; Y_3|X_2, Y_2) + 2n\epsilon + n\epsilon_1 \end{aligned}$$

where (a) results from the security condition (135), (b) from Fano's inequality in (134), (c) from the Markov chain $K_{13} - X_1^n - (X_2^n, Y_1^n, Y_2^n, Y_3^n)$ and (d) from the memoryless property of the channel.

APPENDIX E
PROOF OF THE OUTER BOUND IN THEOREM 4

In the generalized scheme, after receiving the channel outputs, the users generate the corresponding keys as stochastic functions of the information available at them. In particular, User 1 generates K_{12} and K_{13} for sharing with Users 2 and 3, respectively, as stochastic functions of (X_1^n, Y_1^n). Similarly, $\hat{K}_{12}$ and K_{23} are generated by User 2 for sharing with Users 1 and 3, respectively, as functions of (X_2^n, Y_2^n). User 3 estimates $\hat{K}_{13}$ and $\hat{K}_{23}$ as stochastic functions of Y_3^n.

For an arbitrary $\epsilon > 0$, applying Fano's inequality to the keys yields

$$H(K_{12}|\hat{K}_{12}) \leq n\left(\frac{h(\epsilon)}{n} + \epsilon \log(|\mathcal{K}_{12}| - 1)\right) \triangleq n\epsilon_1 \tag{137}$$

$$H(K_{13}|\hat{K}_{13}) \leq n\left(\frac{h(\epsilon)}{n} + \epsilon \log(|\mathcal{K}_{13}| - 1)\right) \triangleq n\epsilon_2 \tag{138}$$

$$H(K_{23}|\hat{K}_{23}) \leq n\left(\frac{h(\epsilon)}{n} + \epsilon \log(|\mathcal{K}_{23}| - 1)\right) \triangleq n\epsilon_3 \tag{139}$$

where $|\mathcal{K}_{12}|$ is the cardinality of key set $\mathcal{K}_{12}$, and for $i = 1, 2, 3$, $\epsilon_i \to 0$ if $\epsilon \to 0$. Furthermore, the secrecy conditions should be satisfied, i.e.,

$$I(K_{12}; Y_3^n) < n\epsilon \tag{140}$$

$$I(K_{13}; X_2^n, Y_2^n) < n\epsilon \tag{141}$$

$$I(K_{23}; X_1^n, Y_1^n) < n\epsilon \tag{142}$$

We show next that for secret keys K_{12} and K_{13} satisfying the reliability and security conditions, R_{12} and R_{13}

must satisfy the upper bounds in Theorem 4. The upper bound on R_{23} may be proved in similar way to R_{13}. To upper bound on R_{12}, first note that

$$
\begin{aligned}
nR_{12} &\leq H(K_{12}) + n\epsilon \\
&\overset{(a)}{\leq} H(K_{12}|Y_3^n) + 2n\epsilon \\
&\overset{(b)}{\leq} H(K_{12}|Y_3^n) - H(K_{12}|\hat{K}_{12}) + 2n\epsilon + n\epsilon_1 \\
&\leq H(K_{12}|Y_3^n) - H(K_{12}|\hat{K}_{12}, X_2^n, Y_2^n) + 2n\epsilon + n\epsilon_1 \\
&\overset{(c)}{=} H(K_{12}|Y_3^n) - H(K_{12}|X_2^n, Y_2^n) + 2n\epsilon + n\epsilon_1 \\
&\leq I(K_{12}; X_2^n, Y_2^n|Y_3^n) + 2n\epsilon + n\epsilon_1 \\
&\leq I(K_{12}, X_1^n, Y_1^n; X_2^n, Y_2^n|Y_3^n) + 2n\epsilon + n\epsilon_1 \\
&\overset{(d)}{=} I(X_1^n, Y_1^n; X_2^n, Y_2^n|Y_3^n) + 2n\epsilon + n\epsilon_1 \\
&= I(X_1^n; Y_2^n|X_2^n, Y_3^n) + I(X_2^n; Y_1^n|X_1^n, Y_3^n) + I(Y_1^n; Y_2^n|X_1^n, X_2^n, Y_3^n) + I(X_1^n; X_2^n|Y_3^n) + n\epsilon_1 + 2n\epsilon \\
&\overset{(e)}{\leq} \sum_{i=1}^{n} [I(X_{1,i}; Y_{2,i}|X_{2,i}, Y_{3,i}) + I(X_{2,i}; Y_{1,i}|X_{1,i}, Y_{3,i}) + I(Y_{1,i}; Y_{2,i}|X_{1,i}, X_{2,i}, Y_{3,i})] + I(X_1^n; X_2^n|Y_3^n) + n\epsilon_1 + 2n\epsilon
\end{aligned}
$$

where (a) results from the security condition (140), (b) from Fano's inequality in (137), (c) and (d) from the fact that $\hat{K}_{12}$ and K_{12} are stochastic functions of (X_2^n, Y_2^n) and (X_1^n, Y_1^n), respectively, so that $\hat{K}_{12} - (X_2^n, Y_2^n) - (X_1^n, Y_1^n) - K_{12}$ forms a Markov chain. Inequality (e) follows since the first three terms can be single-letterized using the memoryless property of the channel as, e.g.,

$$
\begin{aligned}
I(X_1^n; Y_2^n|X_2^n, Y_3^n) &\leq \sum_{i=1}^{n} H(Y_{2,i}|X_{2,i}, Y_{3,i}) - H(Y_2^n|X_1^n, X_2^n, Y_3^n) \\
&= \sum_{i=1}^{n} [H(Y_{2,i}|X_{2,i}, Y_{3,i}) - H(Y_{2,i}|X_{1,i}, X_{2,i}, Y_{3,i})].
\end{aligned}
$$

To single-letterize the fourth term, note that

$$
\begin{aligned}
I(X_1^n; X_2^n|Y_3^n) &\overset{(a)}{=} I(X_1^n; Y_3^n|X_2^n) - I(X_1^n; Y_3^n) \\
&= \sum_{i=1}^{n} I(X_1^n; Y_{3,i}|X_2^n, Y_3^{i-1}) - I(X_1^n; Y_3^n) \\
&\overset{(b)}{\leq} \sum_{i=1}^{n} I(X_{1,i}; Y_{3,i}|X_{2,i}, Y_3^{i-1}) - I(X_1^n; Y_3^n) \\
&= \sum_{i=1}^{n} I(X_{1,i}; Y_{3,i}|X_{2,i}, Y_3^{i-1}) - \sum_{i=1}^{n} I(X_1^n; Y_{3,i}|Y_3^{i-1})
\end{aligned}
$$

$$\leq \sum_{i=1}^{n} I(X_{1,i}; Y_{3,i}|X_{2,i}, Y_3^{i-1}) - \sum_{i=1}^{n} I(X_{1,i}; Y_{3,i}|Y_3^{i-1})$$
$$\stackrel{(c)}{=} \sum_{i=1}^{n} [I(X_{1,i}; Y_{3,i}|X_{2,i}, U_i) - I(X_{1,i}; Y_{3,i}|U_i)]$$

where (a) results from the independence of X_1^n and X_2^n, (b) from the memoryless property of the channel and (c) from the definition of auxiliary random variable $U_i \triangleq Y_3^{i-1}$. Combining all the above, we obtain

$$nR_{12} \leq \sum_{i=1}^{n} [I(X_{1,i};Y_{2,i}|X_{2,i},Y_{3,i}) + I(X_{2,i};Y_{1,i}|X_{1,i},Y_{3,i}) + I(Y_{1,i};Y_{2,i}|X_{1,i},X_{2,i},Y_{3,i}) + I(X_{1,i};Y_{3,i}|X_{2,i},U_i) - I(X_{1,i};Y_{3,i}|U_i)] + n\epsilon_1 + 2n\epsilon.$$

Finally, introducing random variable Q which is uniformly distributed on $\{1, 2, ..., n\}$ and independent of all the other variables, and defining $X_1 = X_{1,Q}, X_2 = X_{2,Q}, Y_1 = Y_{1,Q}, Y_2 = Y_{2,Q}, Y_3 = (Y_{3,Q}, Q), U = (U_Q, Q)$, we have

$$R_{12} \leq I(X_1;Y_2|X_2,Y_3) + I(X_2;Y_1|X_1,Y_3) + I(Y_1;Y_2|X_1,X_2,Y_3) + I(X_1;Y_3|X_2,U) - I(X_1;Y_3|U) + \epsilon_1 + 2\epsilon$$

To upper bound on R_{13}, note that

$$\begin{aligned}
nR_{13} \leq H(K_{13}) + n\epsilon &\stackrel{(a)}{\leq} H(K_{13}|X_2^n, Y_2^n) + 2n\epsilon \\
&\stackrel{(b)}{\leq} H(K_{13}|X_2^n, Y_2^n) - H(K_{13}|\hat{K}_{13}) + 2n\epsilon + n\epsilon_2 \\
&\leq H(K_{13}|X_2^n, Y_2^n) - H(K_{13}|\hat{K}_{13}, Y_3^n) + 2n\epsilon + n\epsilon_2 \\
&\stackrel{(c)}{=} H(K_{13}|X_2^n, Y_2^n) - H(K_{13}|Y_3^n) + 2n\epsilon + n\epsilon_2 \\
&\leq I(K_{13}; Y_3^n|X_2^n, Y_2^n) + 2n\epsilon + n\epsilon_2 \\
&\leq I(K_{13}, X_1^n, Y_1^n; Y_3^n|X_2^n, Y_2^n) + 2n\epsilon + n\epsilon_2 \\
&\stackrel{(d)}{=} I(X_1^n, Y_1^n; Y_3^n|X_2^n, Y_2^n) + 2n\epsilon + n\epsilon_2 \\
&\stackrel{(e)}{\leq} nI(Y_3; X_1, Y_1|X_2, Y_2) + n\epsilon_2 + 2n\epsilon
\end{aligned}$$

where (a) results from the security condition (141), (b) from Fano's inequality in (138), (c) and (d) from the fact that $\hat{K}_{13}$ and K_{13} are stochastic functions of Y_3^n and (X_1^n, Y_1^n), respectively, so that $\hat{K}_{13} - Y_3^n - (X_1^n, Y_1^n) - K_{13}$ forms a Markov chain. Inequality (e) follows from the memoryless property of the channel.

REFERENCES

[1] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography, part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[2] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[3] I. Csiszár, P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp.344-366, Mar 2000.

[4] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.

[5] C. Ye, P. Narayan, "The secret key-private key capacity region for three terminals," *IEEE Int .Symp. Inf. Theory*, Adelaide, Australia, pp. 2142–2146, Sep. 2005.

[6] S. Salimi, M. Salmasizadeh, M. R. Aref, "Rate Regions of Secret Key Sharing in a New Source Model," *IET Communications*, Vol. 5, Issue 4, pp. 443–455, Mar. 2011.

[7] S. Salimi, M. Salmasizadeh, M. R. Aref, J. Dj Golić, "Key Agreement over Multiple Access Channel," *IEEE Trans. on Information Forensics and Security*, vol. 6, Issue 3, pp. 775-790, Sep. 2011.

[8] S. Salimi, M. Salmasizadeh, M. R. Aref, "Key Agreement over Multiple Access Channel Using Feedback Channel," *IEEE Int. Symp. Inf. Theory (ISIT)*, Saint Petersburg, Russia, pp. 1936-1940, Aug. 2011.

[9] S. Salimi, M. Skoglund, J. Dj Golić, M. Salmasizadeh, M. R. Aref, "Key Agreement over a Generalized Multiple Access Channel Using Noiseless and Noisy Feedback," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1765–1778, Sep. 2013.

[10] P. Babaheidarian, S. Salimi, M. R. Aref, "Simultaneously Generating Multiple keys in a Four-Terminal Network," *IET Information Security*, vol. 6, Issue. 3, pp. 190-201, Sep. 2012.

[11] S. Nitinawarat, C. Ye, A. Barg, P. Narayan, A. Reznik, "Secret Key Generation for a Pairwise Independent Network Model," *IEEE Int. Symp. Inf. Theory (ISIT)*, Toronto, Canada, pp. 1015–1019, Jul. 2008.

[12] S. Salimi, M. Skoglund, M. Salmasizadeh, M. R. Aref, "Pairwise Secret Key Agreement Using the Source Common Randomness," *Int. Sym. on Wireless Communication Systems (ISWCS)*, pp. 751–755 , Paris, France, Aug. 2012.

[13] A. El Gamal, O. O. Koyluoglu, M. Youssef, H. El Gamal, "Achievable Secrecy Rate Regions for the Two-Way Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 59, Issue 12, pp. 8099-8114, Dec. 2013.

[14] E. Tekin, A. Yener, "The General Gaussian Multiple-Access and Two-Way Wiretap Channels: Achievable Rates and Cooperative Jamming," *IEEE Trans. Inf. Theory*, vol. 54, Issue 6, pp. 2735-2751, Jun. 2008.

[15] X. He, A. Yener, "Gaussian Two-way Wiretap Channel with an Arbitrarily Varying Eavesdropper," *GLOBECOM Workshop on Physical-Layer Security*, Houston, US, pp. 884-888, Dec. 2011.

[16] A. J. Pierrot and M. R. Bloch, "Strongly Secure Communications Over the Two-Way Wiretap Channel," *IEEE Trans. Inf. Forensics and Security*, vol. 6, no. 3, pp. 595–605, September 2011.

[17] Y. Liang and V. Poor, "Multiple access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976-1002, Mar. 2008.

[18] M. Bloch and J. N. Laneman, "Strong secrecy from channel resolvability," *IEEE Trans. Inf. Theory*, vol. 59, Issue 12, pp. 8077-8098, Dec. 2013.

[19] M. Hayashi, "General Nonasymptotic and Asymptotic Formulas in Channel Resolvability and Identification Capacity and their Application to the Wiretap Channels," *IEEE Trans. Inf. Theory*, vol. 52, Issue 4, pp. 1562–1575, Apr. 2006.

[20] C. H. Bennett, G. Brassard, C. Crépeau, U. Maurer, "Generalized Privacy Amplification," *IEEE Trans. Inf. Theory*, vol. 41, Issue 6, pp. 1915–1923, Nov. 1995.

[21] M. Bloch, "Channel Intrinsic Randomness," *IEEE Int. Symp. Inf. Theory (ISIT)*, Texas, US, pp. 2607-2611, Jun. 2010.

[22] J. Muramatsu, H. Koga, T. Mukouchi, "On the problem of generating mutually independent random sequences," *IEICE Transactions on Fundamentals*, vol. E-86-A, Issue 5, pp. 1275–1284, Apr. 2003.

[23] S. Salimi, F. Gabry, M. Skoglund, "Pairwise Key Agreement over a Generalized Multiple Access Channel: Capacity Bounds and Game-Theoretic Analysis," *The Tenth Int. Symp. on Wireless Communication Systems*, Ilmenau, Germany, pp. 219-223, Aug. 2013.

[24] D. Slepian, J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471– 471, Jul. 1973.

[25] M. H. Yassaee, M. R. Aref. A. Gohari, "Achievability Proof via Output Statistics of Random Binning," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6760–6786, Nov. 2014.

[26] G.B. Dantzig, and B.C. Eaves, "Fourier-Motzkin Elimination and its Dual," *Journal of Combinatorial Theory*, Ser. A, 14:288-297, 1973.

[27] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley Series in Telecommunications and Signal Processing, Wiley-Interscience 2006.

[28] A. El Gamal and Y.-H. Kim, *Network Information Theory*, Cambridge University Press, 2011.