Simultaneously Generating Secret and Private Keys in a Cooperative Pairwise-Independent Network

Peng Xu, Zhiguo Ding, *Senior Member, IEEE*, Xuchu Dai, and George K. Karagiannidis, *Fellow, IEEE*

***Abstract*— This paper studies the problem of simultaneously generating a secret key (SK) and a private key (PK) between Alice and Bob, in a cooperative pairwise-independent network (PIN) with two relays. In the PIN, the pairwise source observed by every pair of terminals is independent of those sources observed by any other pairs. The SK needs to be protected from Eve, while the PK needs to be protected not only from Eve but also from the two relays. Two cooperative SK–PK generation algorithms are proposed: both of them first generate common randomness, based on the well-established pairwise key generation technique and the application of the one-time pad; but then, the two algorithms utilize the XOR operation and a specific random-binning-based SK–PK codebook to generate the expected keys, respectively. The achievable SK–PK rate regions of both the two proposed algorithms are analyzed. Of particular interest is the second algorithm with random-bing based codebook, whose achievable key rate region is demonstrated to be exactly the same as the derived outer bound, a crucial step for establishing the key capacity of this PIN model. Finally, the two proposed SK–PK generation algorithms are extended to a cooperative wireless network, where the correlated source observations are obtained from estimating wireless channels during a training phase.**

***Index Terms*— Information-theoretic security, secret key, private key, key capacity region, cooperative PIN model.**

I. Introduction

REALIZING secret key generation in a variety of discrete memoryless source (DMS) models has received considerable attention from an aspect of information-theoretic security [1]. Ahlswede and Csisár first studied in [2] the secret key generation problem between two terminals, based on their correlative observations and public transmissions between them, and found the secret key capacity. Since then, this result has been extended to various multi-terminal models, such as the works in [3]–[11], whose aim is to find the secret key capacity for a variety of DMS models.

The pairwise independent network (PIN) model is a special case of the multi-terminal DMS model in [4], where the pairwise source observed by every pair of terminals is independent of those sources observed by any other pairs. The PIN model was introduced in [6] for group key generation, and the cooperative key generation problem has also been studied in [6]. Many other related works have also investigated PIN models [7]–[10] where each of them aimed to find the secret key capacity of a particular model.

In recent years, the PIN model has been applied to practical wireless communication networks, in which the physical layer (PHY) resources (i.e., wireless channels) have been exploited for key generation. This PHY security approach has recognized as a promising solution in recent years (e.g., [12]–[21]). Based on channel reciprocity for time-division duplex (TDD) systems and noisy estimates of common fading channels, *common randomness* (CR) can be extracted from wireless channels for generating secret keys. A key assumption used in these works is that physical channels associated with the eavesdroppers are independent from the legitimate users' channels. This assumption is valid in rich scattering wireless systems, as long as the eavesdroppers are half-wavelength away from the legitimate users [22]. In addition to these source-model-based secure methods, there also exists another type of research in the area of PHY security, which is based on channel models. Compared to the secrecy communications in channel models (e.g., [23]–[27]), the PHY key generation approach in source models [12]–[21] enjoys the benefit that secret keys can be obtained, no matter how strong the eavesdropping channels are.

Since user cooperation can effectively enlarge the secret key capacity, some existing works have investigated the issue of cooperative key generation using additional helper nodes, such as those in [3], [6], [7], [10], [19], and [20]. Motivated by this, this paper aims to investigate the key generation problem in a four-terminal cooperative PIN model with the public discussion. Unlike most existing works that focused on generating a single key [3], [6], [7], [10], [19], [20], in the considered model, Alice and Bob wish to generate a secret key (SK) and a private key (PK) simultaneously, with the help of two external relays. The SK needs to be protected from Eve that has access to the public discussion, whereas the PK needs to be protected from Eve and the two relays. The

Manuscript received April 17, 2015; revised October 15, 2015; accepted January 6, 2016. Date of publication January 12, 2016; date of current version March 16, 2016. The work of P. Xu and X. Dai was supported in part by the National Natural Science Foundation of China under Grant 61471334, in part by the National Basic Research Program of China (973 Program) under Grant 2013CB329004, and in part by the China Post-Doctoral Science Foundation under Project 2015M570544. The work of Z. Ding was supported in part by the Royal Society under Grant IE140855 and in part by the U.K. Engineering and Physical Sciences Research Council under Grant EP/L025272/1. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Negar Kiyavash.

P. Xu and X. Dai are with the Chinese Academy of Sciences Key Laboratory of Wireless-Optical Communications, School of Information Science and Technology, University of Science and Technology of China, Hefei 230027, China (e-mail: mxp484@mail.ustc.edu.cn; daixc@ustc.edu.cn).

Z. Ding is with the School of Computing and Communications, Lancaster University, Lancaster LA1 4WA, U.K. (e-mail: z.ding@lancaster.ac.uk).

G. K. Karagiannidis is with the Provincial Key Laboratory of Information Coding and Transmission, Southwest Jiaotong University, Sichuan 611756, China, and also with the Electrical and Computer Engineering Department, Aristotle University of Thessaloniki, Thessaloniki GR-54124, Greece (e-mail: geokarag@auth.gr).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2016.2516970

motivation for using this model is that the two terminals may need to agree on several keys, with different security clearance levels in the presence of eavesdroppers in practical systems. For instance, in tactical networks or wireless networks for the financial industry, Alice and Bob may wish to simultaneously exchange two types of data with different security constraints, where one type of data with a lower security constraint can be revealed to the licensed users in these networks, but the other type of data with a higher security constraint is not allowed. Correspondingly, two types of keys with different security clearance levels are required. The work of simultaneously generating the SK-PK pair has been considered in the three-terminal source model in [5] and [11], where a common SK is generated among three terminals, and a PK is generated between two of them. This SK-PK generation problem is fundamentally different from that considered in this paper, as explained in Section II.

The aim of this work is to derive theoretical bounds in terms of key rates, which will shed a new light on generating symmetric keys with different security levels in PIN models. For the considered cooperative PIN model, we summarize the contributions as follows.

1) We first propose a cooperative SK-PK generation algorithm, which is based on the well-established point-to-point pairwise key generation technique [2], application of the one-time pad [1] and the XOR operation. Specifically, this algorithm consists of three main steps: a) the pairwise key is first generated; b) application of the one-time pad enables Alice and Bob to share additional CR; c) the total CR shared by Alice and Bob in the previous two steps is converted to the SK and PK using the XOR operation. In addition, the achievable SK-PK rate region of this proposed algorithm is analyzed.
2) Then, the second cooperative SK-PK generation algorithm is proposed, which also consists of three main steps: the first two steps are the same as those in the first proposed key generation algorithm mentioned above, for generating CR, but the third step utilizes the construction of a specific random-binning based SK-PK codebook to map the total CR into the SK-PK pair. Comparing the two proposed key generation algorithms, the first one enjoys low complexity, whereas the second is demonstrated to achieve a larger SK-PK rate region.
3) The SK-PK capacity region for the considered PIN model is established. Specifically, the analysis shows that the achievable key rate region of the second proposed SK-PK generation algorithm is exactly the same as the derived outer bound, a key step for proving the key capacity region. A few existing works can be viewed as special cases of this SK-PK capacity region.
4) Finally, the two proposed cooperative SK-PK generation algorithms for the PIN model are extended to a practical cooperative wireless network. The terminals utilize the estimates of the wireless channels obtained from a training process as the correlated observations, and the training-based SK-PK rate regions are also developed.

Traditional security schemes rely on public key infrastructures (PKI) to manage secret keys. Unlike the traditional PKI-based schemes that rely on computational hardness of problems, the PHY-based key generation algorithms can achieve information-theoretic secrecy [1], i.e., they do not assume a computationally bounded eavesdropper. In addition, we have to note here that the second proposed SK-PK generation algorithm is an extension of our recent work [10], but the key generation algorithm in [10] only focuses on generating a PK. The problem of simultaneously generating both the SK and PK considered in this paper is more challenging, which is reflected in both the algorithm design and key capacity region analysis.

This paper is organized as following. Section II describes the definitions of the considered cooperative PIN model. Section III provides the main results of this paper, including the two proposed algorithms, their achievable SK-PK rate regions and the capacity region of the considered model. The two proposed algorithms are extended to the wireless network in Section IV. Some conclusion remarks are given in Section V.

Throughout this paper, a random variable is denoted as an upper case letter, such as X, whose realization and finite alphabet are denoted as a lower case letter x and a calligraphic letter $\mathcal{X}$, respectively. Let X^n denote an n-vector $(X_1, \cdots, X^n)$. In addition, for a message W_α obtained over n channel uses, R_α represents its average rate, i.e., $R_\alpha = (1/n)H(W_\alpha)$. For two such messages W_α and W_β, let $W_\alpha \wedge W_\beta$ denote the one of them with a smaller rate. Also, $\mathbf{C}$ represents an arbitrary constant. Note that $W_\alpha = \mathbf{C}$ if $R_\alpha = 0$.

II. A Cooperative Pairwise Independent Network

Consider a cooperative PIN model with four terminals (Alice, Bob, two relay nodes) and a passive eavesdropper (Eve). This network is assumed to be a DMS model with alphabets $(\mathcal{X}_A, \mathcal{X}_B, \mathcal{X}_1, \mathcal{X}_2)$ and a public channel. Note that if there does not exist the public channel, according to [14] and [19], the terminals can still use the wireless channel to exchange messages. Alice, Bob and two relays observe n independent and identically distributed (i.i.d.) repetitions of the random variables (X_A, X_B, X_1, X_2), respectively, denoted by $(X_A^n, X_B^n, X_1^n, X_2^n)$. Assume that Eve does not have source observation correlated to the other terminals' observations, but she has access to the public channel noiseless. In this PIN model, following [6] and [7], suppose that $X_A = (Y_{B,A}, Y_{1,A}, Y_{2,A})$, $X_B = (Y_{A,B}, Y_{1,B}, Y_{2,B})$, $X_i = (Y_{A,i}, Y_{B,i}, Y_{3-i,i})$, $i = 1, 2$, and the pairs $(Y_{j,k}, Y_{k,j})$ are mutually independent, i.e.,

$$p(X_A, X_B, X_1, X_2) \triangleq \prod_{(j,k)\in\mathcal{A}} p_{Y_{j,k},Y_{k,j}}(y_{j,k}, y_{k,j}), \quad (1)$$

where the set $\mathcal{A}$ is defined as

$$\mathcal{A} \triangleq \{(A, 1), (A, 2), (B, 1), (B, 2), (1, 2), (A, B)\}. \quad (2)$$

Without loss of generality, the public discussion over the public channel is assumed to include r rounds with $4r$ successive time slots, in which the two relays, Alice and Bob

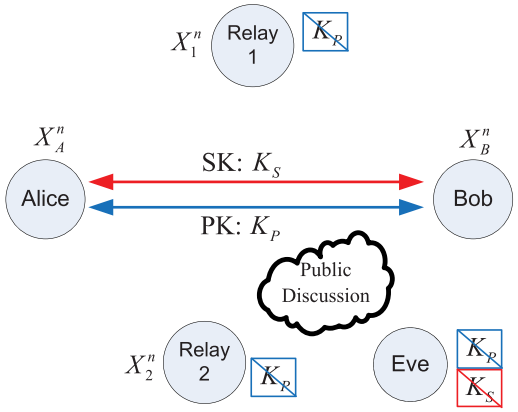


Fig. 1. The cooperative PIN model for the SK and PK generation.

take turns to transmit messages. Let the sequence of $4r$ random variables $\mathbf{F} = (F_1, \cdots, F_{4r})$ to denote these $4r$ transmissions, and F_t is the transmission in the t-th time slot, $1 \leq t \leq 4r$. Specifically, relay 1, relay 2, Alice and Bob transmit $\mathbf{F}_1$, $\mathbf{F}_2$, $\mathbf{F}_3$, $\mathbf{F}_0$, respectively, where $\mathbf{F}_i = \{F_t\}_{t:t \mod 4=i}$, $i = 1, 2, 3, 0$. Each F_t is generated according to its own observation and all the previous transmissions $F^{t-1} = (F_1, \cdots, F_{t-1})$, i.e., $F_t = f_t(X_1^n, F^{t-1})$, $f_t(X_2^n, F^{t-1})$, $f_t(X_A^n, F^{t-1})$, $f_t(X_B^n, F^{t-1})$ when $t \mod 4 = 1, 2, 3, 0$, respectively. Following the definitions in [3], each f_t, $1 \leq t \leq 4r$, is assumed to be a deterministic function.

As shown in Fig. 1, with the help of the two relays, Alice and Bob wish to generate a SK K_S and a PK K_P simultaneously. The SK needs to be protected from Eve but does not need to be secret from the two relays; while the PK needs to be protected from not only Eve but also the two relays. Note that the relays are curious but honest, i.e., they follow the proposed transmission protocols for helping Alice and Bob to generate keys, but would also try to intercept the key information if they can.

The secret key and private key are formally defined as follows, where a random variable U is said to be ϵ-recoverable from another variable V if there exists a deterministic function g such that $Pr(g(V) \neq U) \leq \epsilon$.

Definition 1: A random variable pair (K_S, K_P) is said to be an ϵ-(SK,PK) if they satisfy the requirements [11]:

- K_S and K_P are mutually independent.
- The pair (K_S, K_P) can be ϵ-recoverable from $(X_A^n, \mathbf{F})$ and $(X_B^n, \mathbf{F})$, respectively.
- K_S and K_P are nearly uniformly distributed, i.e.,

$$\frac{1}{n} H(K_S) \geq \frac{1}{n} \log |\mathcal{K}_S| - \epsilon, \tag{3}$$

$$\frac{1}{n} H(K_P) \geq \frac{1}{n} \log |\mathcal{K}_P| - \epsilon, \tag{4}$$

  for sufficiently large n, where $|\mathcal{K}_S|$ and $|\mathcal{K}_p|$ are the alphabet sizes of K_S and K_P, respectively.
- K_S and K_P satisfy the secrecy conditions:

$$\frac{1}{n} I(K_S, K_P; \mathbf{F}) \leq \epsilon, \tag{5}$$

$$\frac{1}{n} I(K_P; \mathbf{F}, X_i^n) \leq \epsilon, \quad i = 1, 2, \tag{6}$$

where (5) implies that Eve intercepts insignificant amount of information about the SK and PK, and (6) ensures that the PK almost does not leak any information to each relay.

Remark 1: Note that the secrecy constraint on the private key K_P in (6) corresponds to the case that the two relays are non-collusive when they try to intercept the private key information. If we consider the case that the two relays are collusive, i.e., they collaborate with each other to intercept the private key, the secrecy constraint in (6) should be replaced by[1]

$$\frac{1}{n} I(K_P; \mathbf{F}, X_1^n, X_2^n) \leq \epsilon. \tag{7}$$

Definition 2: A SK-PK rate pair (R_S, R_P) is said to be *achievable* if for any $\epsilon > 0$, $\delta > 0$ and a sufficiently large n, there exists an ϵ-(SK, PK) pair (K_S, K_P) such that

$$\frac{1}{n} H(K_S) \geq R_S - \delta, \quad \frac{1}{n} H(K_P) \geq R_P - \delta. \tag{8}$$

The set of all achievable rate pairs (R_S, R_P) is defined as the SK-PK capacity region, denoted as $\mathcal{C}_{SP}$. If the case that the two relays are collusive as shown in (7) is considered, the SK-PK capacity region is denoted as $\mathcal{C}_{SP}^{(c)}$.

III. Key Generation: Algorithms and Rate Regions

This section will provide the main results with respect to the cooperative PIN model defined in Section II, including the two proposed key generation algorithms, their achievable SK-PK rate regions and the key capacity of the considered model. For notational convenience, we first define

$$I_{j,k} \triangleq I(Y_{j,k}, Y_{k,j}), \quad \text{for } \forall (j,k) \in \mathcal{A}, \tag{9}$$

where $\mathcal{A}$ is defined in (2). Furthermore, define

$$I_{min}^{(1)} \triangleq \min\{I_{A,1}, I_{A,2}, I_{B,1}, I_{B,2}\}, \tag{10}$$

$$I_{min}^{(2)} \triangleq \min \left\{ \begin{matrix} I_{A,1} + I_{A,2}, I_{A,1} + I_{1,2} + I_{B,2}, \\ I_{B,1} + I_{B,2}, I_{A,2} + I_{1,2} + I_{B,1} \end{matrix} \right\}. \tag{11}$$

We now turn our attention to constructing cooperative key generation algorithms for the considered PIN model.

A. The First Algorithm

The first cooperative SK-PK generation algorithm is proposed based on the careful combination of the point-to-point pairwise key generation technique [2], application of the one-time pad [1] and the XOR operation. Specifically, three main steps are considered: 1) every pair of the four terminals agrees on a pairwise key using their correlative observations; 2) the two relays help Alice and Bob to share additional CR based on repeated application of the one-time pad over the public channel; 3) the total CR shared by Alice and Bob is divided into two parts: one part is agreed on as the expected SK, whereas the other part is converted to the expected PK using the XOR operation. The first SK-PK generation algorithm is summarized in Algorithm 1. The details of each step are provided as follows.

[1]In the rest of this paper, the two relays are assumed to be non-collusive shown in Eq. (6), unless stated otherwise.

Algorithm 1 The First Algorithm for the PIN

Step 1: Pairwise key agreement:
- Based on Slepian-Wolf coding, every pair of the four terminals agrees on a pairwise key using their correlated source observations. In particular, Alice (Bob) and relay i agree on a pairwise key $W_{A,i}$ ($W_{B,i}$), $i = 1, 2$; the two relays agree on $W_{1,2}$; Alice and Bob agree on $W_{A,B}$.

Step 2: Generation of additional CR:
- For each $i = 1, 2$, divide the pairwise keys as: $W_{A,i} = (W^1_{A,i}, W^2_{A,i})$, $W_{B,i} = (W^1_{B,i}, W^2_{B,i})$.
- Each relay i sends $W^1_{A,i} \oplus W^1_{B,i}$ over the public channel, so that Alice and Bob can agree on the common message $W_i \triangleq W_{A,i}$ since they know either $W^1_{A,i}$ or $W^1_{B,i}$.
- Then, the two relays help Alice and Bob to share one more common message $\tilde{W}_{1,2}$, utilizing application of the one-time pad with respect to the pairwise keys $(W^2_{A,1}, W^2_{B,1}, W^2_{A,2}, W^2_{B,2}, W_{1,2})$ as shown in Fig. 2.

Step 3: SK and PK agreement:
- Now, for the CR $(W_{A,B}, W_1, W_2, \tilde{W}_{1,2})$ shared between Alice and Bob in the previous two steps, let $W_{A,B} = (K_{S,3}, K_{P,3})$, $W_i = (K_{S,i}, K_{P,i})$, $i = 1, 2$.
- Alice and Bob agree on $K_S \triangleq (K_{S,1}, K_{S,2}, K_{S,3}, \tilde{W}_{1,2})$ as the final SK, and $K_P \triangleq (K_{P,3}, K_{P,1} \oplus K_{P,2})$ as the final PK.

1) Pairwise Key Agreement: In this step, each pair of the four terminals (Alice, Bob and the two relays) agrees on a pairwise key using their correlative observations. In particular, Alice (Bob) and relay i agree on a pairwise key $W_{A,i}$ ($W_{B,i}$) using the observations $Y^n_{i,A}$ and $Y^n_{A,i}$ ($Y^n_{i,B}$ and $Y^n_{B,i}$), $i = 1, 2$; the two relays agree on $W_{1,2}$ using $Y^n_{2,1}$ and $Y^n_{1,2}$; Alice and Bob agree on $W_{A,B}$ using $Y^n_{B,A}$ and $Y^n_{A,B}$. Each pairwise key $W_{j,k}$, is generated using the standard point-to-point techniques [2], [14], which is based on Slepian-Wolf coding [28], [29] and public communication $F_{j,k}$, where $(j, k) \in \mathcal{A}$ and $\mathcal{A}$ is defined in (2).[2] The rate of each pairwise key $W_{j,k}$ is denoted as $(1/n)H(W_{j,k}) = R_{j,k}$. These rates should satisfy

$$R_{j,k} \le I(Y_{j,k}, Y_{k,j}) - \epsilon_1, \quad \forall (j,k) \in \mathcal{A}, \tag{12}$$

so that each pairwise key is uniformly distributed and ϵ-recoverable at its corresponding terminals. Furthermore, these pairwise keys do not leak any information to the public discussion, i.e.,

$$\frac{1}{n} I(W_{j,k}; F_{j,k}) \le \epsilon, \quad \forall (j,k) \in \mathcal{A}. \tag{13}$$

According to the definition of the PIN model, the pairs $\{(W_{j,k}, F_{j,k})_{(j,k)\in\mathcal{A}}\}$ are mutually independent.

[2]Take the source pair $(Y^n_{A,B}, Y^n_{B,A})$ for example. According to Slepian-Wolf source coding [28], [29], Alice can transmit $nH(Y_{B,A}|Y_{A,B})$ bits of information over the public channel, such that Bob can recover Alice's observation sequence $Y^n_{B,A}$, Then, Alice and Bob utilize correlation between $Y^n_{B,A}$ and $Y^n_{A,B}$ to agree on their pairwise key. One can refer to [2] and [14] for more details of this pairwise key generation.

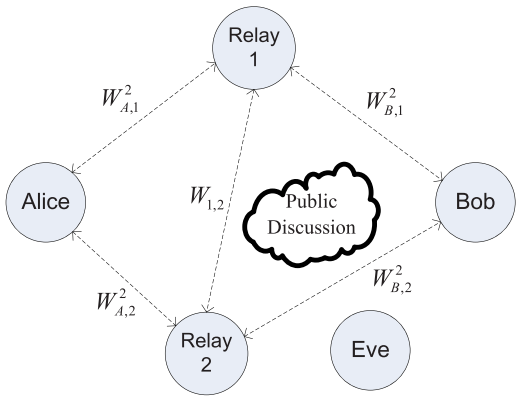


Fig. 2. The CR generation model formed by the pairwise keys $(W^2_{A,1}, W^2_{B,1}, W^2_{A,2}, W^2_{B,2}, W_{1,2})$, from which the common message $\tilde{W}_{1,2}$ can be generated between Alice and Bob in Step 2.

2) Generation of Additional CR: In the previous step, Alice and bob have generated some CR (i.e., the pairwise key $W_{A,B}$). In this step, the two relays will help Alice and Bob to share additional CR (or common messages) based on repeated application of the one-time pad [1]. Each relay i divides the keys $W_{A,i}$ and $W_{B,i}$ into two non-overlapping parts, i.e., $W_{A,i=}(W^1_{A,i}, W^2_{A,i})$, $W_{B,i=}(W^1_{B,i}, W^2_{B,i})$, with each part's rate fixed as

$$R^1_{A,i} = R^1_{B,i} = \min\{R_{A,i}, R_{B,i}\} \triangleq R_i, \tag{14}$$

$$R^2_{A,i} = R_{A,i} - R_i, \;\; R^2_{B,i} = R_{B,i} - R_i. \tag{15}$$

Note that $W^1_{A,i}$ and $W^1_{B,i}$ have the same size; $R^2_{A,i} = 0$ if $R_{A,i} \le R_{B,i}$, $R^2_{B,i} = 0$ if $R_{A,i} \ge R_{B,i}$. These partitions can be obtained via the mappings: $\mathcal{W}_{A,i} \to \mathcal{W}^1_{A,i} \times \mathcal{W}^2_{A,i}$ and $\mathcal{W}_{B,i} \to \mathcal{W}^1_{B,i} \times \mathcal{W}^2_{B,i}$. These mappings are revealed to all the other nodes (including Eve). In the next, additional CR will be generated.

First, each relay i sends $W^1_{A,i} \oplus W^1_{B,i}$ over the public channel. Since Alice and Bob know either $W^1_{A,i}$ or $W^1_{\beta_i,i}$, they can decode both $W^1_{A,i}$ and $W^1_{B,i}$ and set the $W_i \triangleq W^1_{A,i}$ as the common message, $W_i \in \mathcal{W}_i$. The rate of W_i is R_i defined in (14). Due to the concept of the one-time pad in [1], $W_i (= W^1_{A,i})$ is information-theoretically secret from the public transmission when $R^1_{A,i} = R^1_{B,i}$.

Second, the two relays will help Alice and Bob to further generate one more common message $\tilde{W}_{1,2}$, based on the CR generation model in Fig. 2 that is formed by the pairwise keys $(W^2_{A,1}, W^2_{B,1}, W^2_{A,2}, W^2_{B,2}, W_{1,2})$. A classical method, termed as the "tree-based SK generation method", can be utilized to generate $\tilde{W}_{1,2}$, by treating the model in Fig. 2 as a weighted graph [6], [7]. According to [6], [7] and Eq. (15), the optimal rate of $\tilde{W}_{1,2}$ is

$$\tilde{R}_{1,2} \triangleq \min \left\{ \begin{matrix} R^2_{A,1} + R^2_{A,2}, R^2_{A,1} + R_{1,2} + R^2_{B,2} \\ R^2_{B,1} + R^2_{B,2}, R^2_{A,2} + R_{1,2} + R^2_{B,1} \end{matrix} \right\} \tag{16}$$

$$= \hat{R}_{1,2} - R_1 - R_2 \tag{17}$$

where, for simplicity, $\hat{R}_{1,2}$ is defined as

$$\hat{R}_{1,2} \triangleq \min \begin{Bmatrix} R_{A,1}+R_{A,2}, R_{A,1}+R_{1,2}+R_{B,2} \\ R_{B,1}+R_{B,2}, R_{A,2}+R_{1,2}+R_{B,1} \end{Bmatrix}. \quad (18)$$

Alternatively, another simpler approach (without finding the maximum spanning tree) can be used to generate $\tilde{W}_{1,2}$, by observing that at least two of the messages $(W^2_{A,1}, W^2_{A,2}, W^2_{B,1}, W^2_{B,2})$ have a zero rate as shown in (14) and (15). Three cases are considered:

i) If $R_{A,i} \le R_{B,i}$ for $\forall i = 1, 2$, or $R_{A,i} \ge R_{B,i}$ for $\forall i = 1, 2$, we cannot generate $\tilde{W}_{1,2}$ with a positive rate, so simply set $\tilde{W}_{1,2} = \mathbf{C}$.

ii) Otherwise, if $R_{A,1} \ge R_{B,1}$ and $R_{A,2} \le R_{B,2}$, relay 1 sends $W^2_{A,1} \oplus W_{1,2}$ over the public channel, so that relay 2 and Alice can agree on a common message $W^2_{A,1} \wedge W_{1,2}$. Then, relay 2 sends $(W^2_{A,1} \wedge W_{1,2}) \oplus W^2_{B,2}$ so that Alice and Bob can agree on $\tilde{W}_{1,2} \triangleq W^2_{A,1} \wedge W_{1,2} \wedge W^2_{B,2}$, whose rate is $\min\{R^2_{A,1}, R_{1,2}, R^2_{B,2}\}$.

iii) Similar to the previous case, if $R_{A,1} \le R_{B,1}$ and $R_{A,2} \ge R_{B,2}$, Alice and Bob can agree on $\tilde{W}_{1,2} \triangleq W^2_{A,2} \wedge W_{1,2} \wedge W^2_{B,1}$ with the rate $\min\{R^2_{A,2}, R_{1,2}, R^2_{B,1}\}$.

Summarizing these three cases, the rate of $\tilde{W}_{1,2}$ is equal to Eq. (16) or (17).

Since the criterion of the one-time pad is used, the public discussion will not leak any information about these common messages $(W_{A,B}, W_1, W_2, \tilde{W}_{1,2})$ between Alice and Bob, i.e.,

$$\frac{1}{n} I(W_{A,B}, W_1, W_2, \tilde{W}_{1,2}; \mathbf{F}) \le \epsilon, \quad (19)$$

where $W_{A,B}$ is the pairwise key between Alice and Bob, and $\mathbf{F}$ is the set of all the transmissions over the public channel (including the public communications in the first two steps). However, each relay observes part of the common messages: relay 1 observes $(W_1, \tilde{W}_{1,2})$ and relay 2 observes $(W_2, \tilde{W}_{1,2})$.

3) SK-PK Agreement: In this step, Alice and Bob will agree on the SK-PK pair based on the total CR $(W_{A,B}, W_1, W_2, \tilde{W}_{1,2})$ assembled from the above two steps. Specifically, the common message $W_{A,B}$ is divided into two non-overlapping parts: $W_{A,B} = (K_{S,3}, K_{P,3})$; similarly, let $W_i = (K_{S,i}, K_{P,i})$, $i = 1, 2$. Here we set

$$R_{S,3} + R_{P,3} = R_{A,B}, \quad (20)$$

$$R_{S,i} + R_{P,i} = R_i, \quad i = 1, 2, \quad (21)$$

$$R_{P,1} = R_{P,2}. \quad (22)$$

Now, Alice and Bob agree on the SK K_S by concatenating $(K_{S,1}, K_{S,2}, K_{S,3}, \tilde{W}_{1,2})$, i.e., $K_s = (K_{S,1}, K_{S,2}, K_{S,3}, \tilde{W}_{1,2})$, which is obviously secret from Eve shown in (19). Moreover, Alice and Bob implement the XOR operation on $K_{P,1}$ and $K_{P,2}$, and agree on $K_P = (K_{P,3}, K_{P,1} \oplus K_{P,2})$ as the final PK. Since $K_{P,1} \oplus K_{P,2}$ is independent of $K_{P,1}$ and $K_{P,2}$, it is not difficult to prove that K_P is secret from both Eve and each relay. Hence the secrecy constraints in (5) and (6) are satisfied, and the achievable SK-PK rate pair (R_S, R_P) can be expressed as

$$R_S = R_{S,1} + R_{S,2} + R_{S,3} + \tilde{R}_{1,2}, \quad (23)$$

$$R_P = R_{P,3} + R_{P,1}. \quad (24)$$

In summary, the key rate region achieved by the first proposed algorithm is given in the following theorem.

Theorem 1: The SK-PK rate region, $\mathcal{R}_{SP,1}$, for the cooperative PIN model in Section II is achievable, where

$$\mathcal{R}_{SP,1} \triangleq \Big\{ (R_S, R_P) : R_S, R_P \ge 0, \; R_P \le I_{A,B} + I^{(1)}_{min}, \; R_S + 2R_P \le 2I_{A,B} + I^{(2)}_{min}, \; R_S + R_P \le I_{A,B} + I^{(2)}_{min} \Big\}. \quad (25)$$

Proof: We have verified that the rate pair (R_S, R_P) in (23) and (24) is achieved; here, we only need to show that it can be transformed into Eq. (25). For a given tuple $(R_1, R_2, \hat{R}_{1,2}, R_{A,B})$, by applying Fourier-Motzkin elimination to eliminate $\tilde{R}_{1,2}$, $R_{S,j}$, $R_{S,j}$ for $j = 1, 2, 3$ in Eqs. (17), (20)-(22), (23)-(24), the rate pair (R_S, R_P) satisfies the constraints in the following region:

$$R_P \le \min\{R_1, R_2\} + R_{A,B}, \quad (26)$$

$$R_S + 2R_P \le \hat{R}_{1,2} + 2R_{A,B}, \quad (27)$$

$$R_S + R_P \le \hat{R}_{1,2} + R_{A,B}. \quad (28)$$

Recalling the definitions in (14), (18) and the constraints in (12), the region of (R_S, R_P) given in (25) is achievable, and Theorem 1 has been proved. ■

B. The Second Algorithm

Now we consider the second cooperative SK-PK generation algorithm which is based on the careful combination of point-to-point pairwise key generation technique, application of the one-time pad and the construction of a specific random-binning based SK-PK codebook. There are three main steps, where the first two of them are the same as those in the first algorithm mentioned above, but in the third step, Alice and Bob map the total CR assembled from the previous two steps into the SK-PK pair (K_S, K_P) via a random-binning based SK-PK codebook. The second SK-PK generation algorithm is summarized in Algorithm 2. The details are provided as follows.

The first two steps follow the same protocol as that in Algorithm 1, from which Alice and Bob agree on the total CR $(W_{A,B}, W_1, W_2, \tilde{W}_{1,2})$ based on pairwise key generation technique and repeated application of the one-time pad over the public channel. The rates of these common messages, i.e., $W_{A,B}$, R_i and $\tilde{R}_{1,2}$ are given in Eqs. (12), (14) and (17), respectively. Note that $W_{A,B}$ is only known by Alice and Bob; W_1 and W_2 are revealed to relay 1 and relay 2, respectively; $\tilde{W}_{1,2}$ is known by all the four terminals. These common messages satisfy the constraint (19).

Now, we will describe the third step in details. In this SK-PK agreement step, Alice and Bob will generate a SK-PK pair (K_S, K_P). In particular, a random-binning based SK-PK codebook is utilized which maps the total CR $(W_{A,B}, W_1, W_2, \tilde{W}_{1,2})$ into the SK-PK pair (K_S, K_P), whose details are given as follows.

Algorithm 2 The Second Algorithm for the PIN

Steps 1 and 2: Follow the same protocol as that in Algorithm 1, from which:

- Alice and Bob agree on the total CR $(W_{A,B}, W_1, W_2, \tilde{W}_{1,2})$ based on the pairwise key generation technique and repeated application of the one-time pad over the public channel.
- Here $W_{A,B}$ is only known by Alice and Bob; W_1 and W_2 are revealed to relay 1 and relay 2, respectively; $\tilde{W}_{1,2}$ is known by all the four terminals. All these common messages are secret from Eve.

Step 3: SK and PK agreement:

- Randomly grouped all the four-dimensional sequence $\mathbf{w} = (w_{A,B}, w_1, w_2, \tilde{w}_{1,2})$ in $\mathcal{W} \triangleq \mathcal{W}_{A,B} \times \mathcal{W}_1 \times \mathcal{W}_2 \times \tilde{\mathcal{W}}_{1,2}$ into a certain amount of bins each with an equal number of codewords. This binning assignment is termed as the SK-PK codebook, which is revealed to all the terminals (including Eve).
- Alice and Bob find the common-message sequence $(W_{A,B}, W_1, W_2, \tilde{W}_{1,2})$ in the SK-PK codebook, then set its indices of the bin number and the number in this bin, i.e., (K_P, K_S), as the final PK and SK.

1) Codebook Generation: The alphabets of $W_{A,B}$, W_1, W_2, $\tilde{W}_{1,2}$ are $\mathcal{W}_{A,B} = \{1, \cdots, 2^{nR_{A,B}}\}$, $\mathcal{W}_i = \{1, \cdots, 2^{nR_i}\}$, $i = 1, 2$, $\tilde{\mathcal{W}}_{1,2} = \{1, \cdots, 2^{n\tilde{R}_{1,2}}\}$, respectively. Define their Descartes product as $\mathcal{W} \triangleq \mathcal{W}_{A,B} \times \mathcal{W}_1 \times \mathcal{W}_2 \times \tilde{\mathcal{W}}_{1,2}$. Then a SK-PK codebook is constructed. Specifically, randomly and independently partitions all the $2^{n(R_{A,B}+R_1+R_2+\tilde{R}_{1,2})}$ four-dimensional elements $\mathbf{w} = (w_{A,B}, w_1, w_2, \tilde{w}_{1,2})$ in the set $\mathcal{W}$ into 2^{nR_P} bins each with 2^{nR_S} elements, where

$$R_S \geq \max\{R_1, R_2\} + \tilde{R}_{1,2} + \epsilon_2, \tag{29}$$

$$R_P = R_{A,B} + R_1 + R_2 + \tilde{R}_{1,2} - R_S \geq 0. \tag{30}$$

Each codeword in this SK-PK codebook can be indexed as $\mathbf{w}(k_P, k_S)$, where $k_P \in \{1, \cdots, 2^{nR_P}\}$, $k_S \in \{1, \cdots, 2^{nR_S}\}$. The binning assignment for this SK-PK codebook (denoted as $\mathcal{C}$) is revealed to all the other terminals (including Eve).

2) Key Generation: Alice and Bob find the index (K_P, K_S) in the SK-PK codebook such that the codeword $\mathbf{w}(K_P, K_S) = (W_{A,B}, W_1, W_2, \tilde{W}_{1,2})$, where $(W_{A,B}, W_1, W_2, \tilde{W}_{1,2})$ is the common-message sequence generated in the previous two steps; K_P and K_S represent this codeword's bin number and the number in this bin, respectively, which are independent of each other and uniformly distributed.

3) Analysis of Secrecy Constraints: We will analyze secrecy constrains in (5) and (6) averaged on $\mathcal{C}$. Based on Eq. (19) and the fact that both K_S and K_P are determined by $(W_{A,B}, W_1, W_2, \tilde{W}_{1,2})$, we have

$$\begin{aligned}\frac{1}{n} I(K_S, K_P; \mathbf{F}|\mathcal{C}) &\leq \frac{1}{n} I(W_{A,B}, W_1, W_2, \tilde{W}_{1,2}; \mathbf{F}|\mathcal{C}) \\ &= \frac{1}{n} I(W_{A,B}, W_1, W_2, \tilde{W}_{1,2}; \mathbf{F}) \leq \epsilon. \end{aligned} \tag{31}$$

Next, averaged over $\mathcal{C}$, we will prove that $(1/n) I(K_P; X_i^n, \mathbf{F}|\mathcal{C})$ is arbitrarily small for $\forall i = 1, 2$, as long as n is sufficiently large. We first calculate $I(K_P; W_i, \tilde{W}_{1,2}|\mathcal{C})$ as following. Define $\mathbf{W} \triangleq (W_{A,B}, W_1, W_2, \tilde{W}_{1,2})$ for simplicity, then

$$\begin{aligned} & I(K_P; W_i, \tilde{W}_{1,2}|\mathcal{C}) \\ &= I(K_P, \mathbf{W}; W_i, \tilde{W}_{1,2}|\mathcal{C}) - I(\mathbf{W}; W_i, \tilde{W}_{1,2}|K_P, \mathcal{C}) \\ &\overset{(a)}{=} I(\mathbf{W}; W_i, \tilde{W}_{1,2}|\mathcal{C}) - H(\mathbf{W}|K_P, \mathcal{C}) \\ &\quad + H(\mathbf{W}|W_i, \tilde{W}_{1,2}, K_P, \mathcal{C}) \\ &= H(W_i, \tilde{W}_{1,2}) - H(\mathbf{W}|K_P, \mathcal{C}) + H(\mathbf{W}|W_i, \tilde{W}_{1,2}, K_P, \mathcal{C}), \end{aligned} \tag{32}$$

where (a) is due to the fact that K_P is determined by $\mathbf{W}$. The first term in the above equation is $H(W_i, \tilde{W}_{1,2}) = n(R_i + \tilde{R}_{1,2})$, and the second term can be calculated as

$$\begin{aligned} H(\mathbf{W}|K_P, \mathcal{C}) &= H(\mathbf{W}|\mathcal{C}) + H(K_P|\mathbf{W}, \mathcal{C}) - H(K_P|\mathcal{C}) \\ &= H(\mathbf{W}) - H(K_P|\mathcal{C}) \\ &\geq n(R_{A,B} + R_1 + R_2 + \tilde{R}_{1,2}) - nR_P \\ &\overset{(b)}{=} nR_S, \end{aligned} \tag{33}$$

where (b) is obtained according to (30). The third term in (32) can be bounded in the subsequent lemma.

Lemma 2: When R_S satisfies (29),

$$H(\mathbf{W}|W_i, \tilde{W}_{1,2}, K_P, \mathcal{C}) \leq n(R_S - R_i - \tilde{R}_{1,2} + \delta_n)$$

for $i = 1, 2$, where $\delta_n \to 0$ as $n \to \infty$.

Proof: Refer to Appendix C. ∎

Now, recalling Eq. (32), $I(K_P; W_i, \tilde{W}_{1,2}|\mathcal{C}) \leq n\delta_n$ can be obtained. Without loss of generality, let $i = 1$, then

$$\begin{aligned} & I(K_P; W_1, \tilde{W}_{1,2}, \mathbf{F}|\mathcal{C}) \\ &\leq I(K_P; W_1, \tilde{W}_{1,2}|\mathcal{C}) + I(K_P, \mathbf{W}; \mathbf{F}|W_1, \tilde{W}_{1,2}, \mathcal{C}) \\ &= I(K_P; W_1, \tilde{W}_{1,2}|\mathcal{C}) + I(W_{A,B}, W_2; \mathbf{F}|W_1, \tilde{W}_{1,2}, \mathcal{C}) \\ &\overset{(c)}{\leq} n(\delta_n + \epsilon), \end{aligned} \tag{34}$$

where (c) is obtained according to (19). In this key generation algorithm, $X_1^n - (W_1, \tilde{W}_{1,2}, \mathbf{F}) - K_P$ is a Markov chain, so

$$I(K_P; X_1^n, \mathbf{F}|\mathcal{C}) \leq I(K_P; W_1, \tilde{W}_{1,2}, \mathbf{F}|\mathcal{C}) \leq n(\delta_n + \epsilon).$$

Symmetrically, we have $I(K_P; X_2^n, \mathbf{F}|\mathcal{C}) \leq n(\delta_n + 2\epsilon)$.

In summary, the key rate region achieved by the second proposed algorithm is given in the following theorem.

Theorem 3: The SK-PK rate region, $\mathcal{R}_{SP,2}$, for the cooperative PIN model in Section II is achievable, where

$$\begin{aligned} \mathcal{R}_{SP,2} \triangleq \Big\{ & (R_S, R_P) : R_S, R_P \geq 0, \\ & R_P \leq I_{A,B} + I_{min}^{(1)}, \\ & R_S + R_P \leq I_{A,B} + I_{min}^{(2)} \Big\}. \end{aligned} \tag{35}$$

Proof: We have verified that the rate pair (R_S, R_P) in (29), (30) is achieved; here, we only need to show that it can be transformed into Eq. (35). Given a fixed tuple $(R_{A,B}, R_1, R_2, \tilde{R}_{1,2})$, the region of (R_S, R_P) in (29) and (30) can be equivalently rewritten as

$$R_P \leq \min\{R_1, R_2\} + R_{A,B} - \epsilon_2, \tag{36}$$

$$R_S + R_P = R_1 + R_2 + \tilde{R}_{1,2} + R_{A,B}. \tag{37}$$

Then, according to (14) and (17), the above region of (R_S, R_P) can be shown as

$$R_P \leq \min\{R_{A,1}, R_{A,2}, R_{B,1}, R_{B,2}\} + R_{A,B} - \epsilon_2, \quad (38)$$

$$R_S + R_P = \hat{R}_{1,2} + R_{A,B}, \quad (39)$$

where $\hat{R}_{1,2}$ is defined in (18). Now, according to the constraint on each pairwise key rate in (12), the region of (R_S, R_P) given in (35) is achievable, and Theorem 3 has been proved. ■

Remark 2: From Theorems 1 and 3, one can observe that the second algorithm achieves a larger key rate region, but the first algorithm enjoys lower complexity since only a simple XOR operation is used in the third step.

Remark 3: The two proposed SK-PK generation algorithms can be extended to the cooperative PIN model with $M(\geq 2)$ relays, in which the tree-based SK generation approaches [6], [7] can be utilized in the second step for key propagation among these relays. This could be the topic of future research and will not be considered in this paper.

C. SK-PK Capacity

The following theorem shows that the second proposed algorithm can achieve the capacity region.

Theorem 4: The SK-PK capacity region of the considered PIN model is equivalent to $\mathcal{R}_{SP,2}$, i.e., $\mathcal{C}_{SP} = \mathcal{R}_{SP,2}$.

Proof: The achievability of $\mathcal{C}_{SP}$ has been proved in Theorem 3, and the proof of the converse will be provided in Appendix A. ■

A few existing works can be viewed as special cases of the SK-PK capacity region in Theorem 4.

Remark 4: If Alice and Bob only generate the SK R_S (i.e., set $R_P = 0$), Theorem 4 reduces to the SK capacity in [6, Th. 2] when $m = 4$ therein.

Remark 5: If Alice and Bob only generate the PK R_P (i.e., set $R_S = 0$), Theorem 4 reduces to the PK capacity in [10, Th. 1] with two relays. The PK generation work can also be found in [19, Sec. VI], where a training-based approach is utilized to generate the relay-oblivious key (i.e., PK) in a cooperative wireless network.

If the two relays are collusive as shown in (7), the capacity region is given in the following.

Lemma 5: When the two relays are collusive, the SK-PK capacity region of the considered PIN model is

$$\mathcal{C}_{SP}^{(c)} \triangleq \Big\{(R_S, R_P) : R_S, R_P \geq 0, \; R_P \leq I_{A,B}, \; R_S + R_P \leq I_{A,B} + I_{min}^{(2)}\Big\}. \quad (40)$$

Proof: The achievability of $\mathcal{C}_{SP}^{(c)}$ can be easily proved, where only the point-to-point pairwise key between Alice and Bob can be utilized to generate the PK. The proof of the converse will be provided in Appendix B. ■

Fig. 3 illustrates the three SK-PK rate regions, where $\mathcal{C}_{SP}^{(c)} \subseteq \mathcal{R}_{SP,1} \subseteq \mathcal{C}_{SP}(= \mathcal{R}_{SP,2})$.

D. Discussion for the General DMS Model

In a general DMS model, all the terminals may not observe pairwise independent sources defined in Section II,

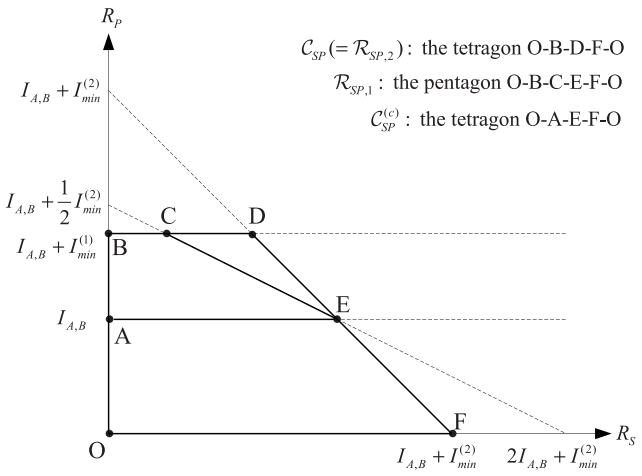


Fig. 3. The three SK-PK rate regions.

and we should consider the general source distribution $p(X_A, X_B, X_1, X_2)$ rather than its special case in Eq. (1). Obviously, analyzing the SK-PK capacity region of this general DMS model is more challenging. For the addressed PIN model, the two-terminal Slepian-Wolf source coding scheme has been employed among every pair of the four terminals, in order to generate CR between Alice and Bob. But, for the general DMS model, we need to employ the multi-terminal Slepian-Wolf source coding scheme [4], [28], [29] for the four terminals to generate CR between Alice and Bob. Then, CR shared by Alice and Bob can be converted to the SK and PK by using a method similar to the third step of Algorithm 1 or 2. Designing key-generation algorithms for such a general scenario is out of the scope of this paper, and the study of the SK-PK capacity region for the general DMS model is a promising future research direction.

IV. Key Generation in Wireless Network

In this section, the SK and PK generation problem is studied via the PHY resources in the wireless network, and the algorithms and analysis results in the previous section for the PIN model will be extended to the wireless network.

A. Model

Fig. 4 shows the considered cooperative wireless network, which is a practical example of the PIN model in Section II, where the correlated source observations can be obtained from channel estimates. In this wireless network, there exists a wireless link between every pair of the four terminals, and these wireless channels are assumed to be reciprocal. Hence there are six wireless channels associated with the terminals, whose coefficients are denoted as $h_{j,k}(= h_{k,j})$ for $\forall(j,k) \in \mathcal{A}$, where $\mathcal{A}$ is defined in (2). Specifically, the channel gain from Alice to relay 1, relay 2 and Bob are denoted $h_{A,1}$, $h_{A,2}$, $h_{A,B}$, respectively; the channel gain from Bob to relay 1, relay 2 are denoted as $h_{B,1}$, $h_{B,2}$, respectively; the channel gain between the two relays is $h_{1,2}$. For simplicity, these channel gains are assumed to be Gaussian random variables, i.e., $h_{j,k} \sim \mathcal{N}(0, \delta_{j,k})^2$. All the terminals know the statistics

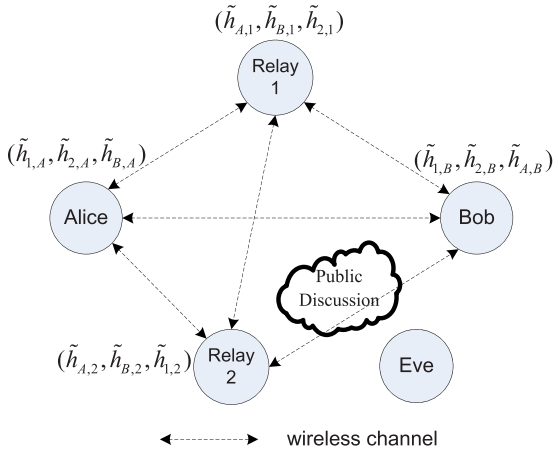


Fig. 4. Illustration of the cooperative wireless network and the channel estimates at each terminal.

of these channel gains, but do not know their exact values *a priori*. This model is ergodic block fading in the sense that all the channel gains remain fixed for a block of T symbols and change randomly to other values in the next block.

All the four terminals are half-duplex constrained and equipped with a single antenna. Let $\mathbf{S}_\alpha = [s_\alpha(1), \cdots, s_\alpha(L_\alpha)]^T$ for $\alpha \in \{1, 2, A, B\}$. In particular, $(\mathbf{S}_1, \mathbf{S}_2, \mathbf{S}_A, \mathbf{S}_B)$ denote the signals transmitted by (relay 1, relay 2, Alice, Bob) in (L_1, L_2, L_A, L_B) channel uses, respectively. For simplicity, an equal power constraint is assumed for each of these four terminals during its transmit period, i.e.,

$$\frac{1}{L_\alpha}\mathbb{E}\{\mathbf{S}_\alpha^T, \mathbf{S}_\alpha\} \le P, \quad \alpha \in \{1, 2, A, B\}. \tag{41}$$

Eve receives messages from the wireless channels and the public channel but does not send any signals. Since rich scattering is assumed for the considered wireless network, the wireless channels experienced by Eve are independent of the channels associated the four terminals. Note that such an assumption is commonly used in many existing works for PHY-based key generation (e.g., [12]–[21]).[3]

B. Training-Based SK-PK Generation

The correlative source observations in Section II can be obtained via a training process [13], [19]. In the training period, (relay 1, relay 2, Alice, Bob) take turns to transmit training sequences $(\mathbf{S}_1, \mathbf{S}_2, \mathbf{S}_A, \mathbf{S}_B)$ in four successive time slots in each fading block, respectively. The size of each sequence $\mathbf{S}_\alpha$ is $T_\alpha \times 1$ for $\alpha \in \{1, 2, A, B\}$, where $T_\alpha \in \mathbb{Z}^+$ and $T_1 + T_2 + T_A + T_B = T$. According to the power constraints in (41), the energy of each sequence is $||\mathbf{S}_\alpha||^2 = T_\alpha P$. After the training period, all the four terminals estimate the corresponding wireless channels, and the channel estimates can be obtained at each terminal shown in Fig. 4, which can be treated as correlative source observations. From n fading blocks, Alice and relay 1 can collect n estimates, i.e., $(\tilde{h}_{1,A}^n, \tilde{h}_{A,1}^n)$. Similarly, channel estimates associated with the other five wireless channels can be obtained by corresponding terminals, i.e., Alice, Bob, relay 1 and relay 2 observe $(\tilde{h}_{1,A}^n, \tilde{h}_{2,A}^n, \tilde{h}_{B,A}^n)$, $(\tilde{h}_{1,B}^n, \tilde{h}_{2,B}^n, \tilde{h}_{A,B}^n)$, $(\tilde{h}_{2,1}^n, \tilde{h}_{A,1}^n, \tilde{h}_{B,1}^n)$, $(\tilde{h}_{1,2}^n, \tilde{h}_{A,2}^n, \tilde{h}_{B,2}^n)$, respectively. The details of how to obtain these correlated channel estimates have been provided in many existing works (e.g., [14], [19], [20]), so they are omitted in this paper for simplicity.

Using these correlated channel estimates, the four terminals can generate six independent pairwise keys $W_{j,k}, \forall (j,k) \in \mathcal{A}$, where $\mathcal{A}$ is given in (2). According to existing works for training-based key generation (e.g., [14], [19]), these pairwise key rates have the following rates:

$$I_{j,k}^G \triangleq I(\tilde{h}_{j,k}; \tilde{h}_{k,j}) = \frac{1}{2T}\log_2\left(1 + \frac{T_j T_k P^2 \delta_{j,k}^4}{\delta^4 + (T_j + T_k)\delta^2 \delta_{j,k}^2 P}\right), \quad \forall (j,k) \in \mathcal{A}, \tag{42}$$

where δ^2 is the variance of Gaussian noise at each terminal in the training period.

Using these pairwise keys, the SK-PK generation scheme in Algorithms 1 and 2 can be utilized to simultaneously generate the secret key and private key shared by Alice and Bob. The details of these proposed algorithms are provided in Section III. Next, the SK-PK rate regions achieved by these algorithms will be presented.

According to Theorem 1, Algorithm 1 achieves the region

$$\begin{aligned}\mathcal{R}_{SP,1}^G \triangleq \bigcup_{\mathbf{T}\in\mathcal{T}} \Big\{ &(R_S, R_P) : R_S, R_P \ge 0, \\ &R_P \le I_{A,B}^G + I_{min}^{G,(1)}, \\ &R_S + 2R_P \le 2I_{A,B}^G + I_{min}^{G,(2)}, \\ &R_S + R_P \le I_{A,B}^G + I_{min}^{G,(2)} \Big\},\end{aligned} \tag{43}$$

where $I_{min}^{G,(1)}$ and $I_{min}^{G,(2)}$ are defined in Eqs. (10) and (11) by replacing $I_{j,k}$ with $I_{j,k}^G$, $(j,k) \in \mathcal{A}$; $\mathcal{T}$ is defined as

$$\begin{aligned}\mathcal{T} \triangleq \Big\{ &(T_1, T_2, T_A, T_B) : T_1, T_2, T_A, T_B \ge 0, \\ &T_1 + T_2 + T_A + T_B = T \Big\};\end{aligned} \tag{44}$$

According to Theorem 3 and Theorem 4, Algorithm 2 achieves the training-based SK-PK capacity region that is

$$\begin{aligned}\mathcal{R}_{SP,2}^G = \mathcal{C}_{SP}^G \triangleq \bigcup_{\mathbf{T}\in\mathcal{T}} \Big\{ &(R_S, R_P) : R_S, R_P \ge 0, \\ &R_P \le I_{A,B}^G + I_{min}^{G,(1)}, \\ &R_S + R_P \le I_{A,B}^G + I_{min}^{G,(2)} \Big\},\end{aligned} \tag{45}$$

[3]The issue with respect to sparse scattering is more challenging, since sparsity leads to sparsity leads to increased spatial correlation between Eve's channel gains and the four terminals'. In this case, we should consider the general DMS model without the pairwise independent assumption, and the proposed algorithms should be modified, in which Alice and Bob need to sacrifice part of secret/private key rates in order to confuse Eve, as shown in [3] for the general DMS model with only one relay. The study of key generation in sparse scattering environments is out of the scope of this paper, which could be a topic of future research.

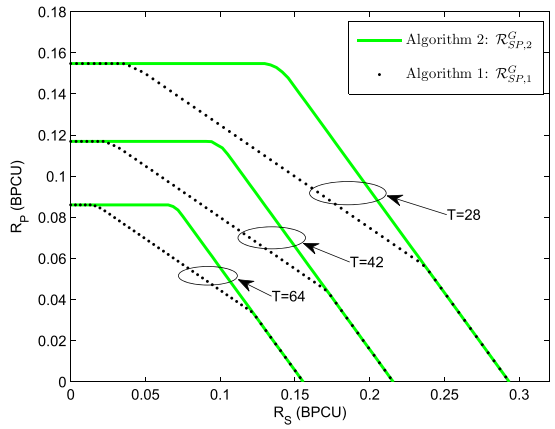


Fig. 5. Training-based SK-PK rate regions achieved by the two proposed algorithms for different values of T, where $P = 20$, $(\delta^2_{A,1}, \delta^2_{A,2}, \delta^2_{B,1}, \delta^2_{B,2}, \delta^2_{1,2}, \delta^2_{A,B}) = (0.5, 1.1, 3.7, 2.1, 3.1, 0.1)$.

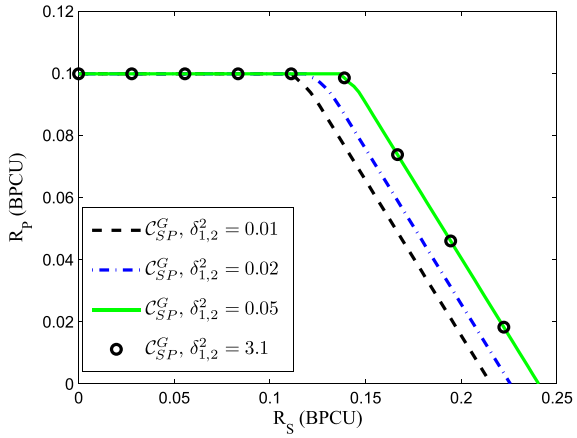


Fig. 6. Training-based SK-PK capacity regions for different values of $\delta^2_{1,2}$ between the two relays, where $T = 28$, $P = 20$, $(\delta^2_{A,1}, \delta^2_{A,2}, \delta^2_{B,1}, \delta^2_{B,2}, \delta^2_{A,B}) = (3.7, 0.5, 1.1, 2.1, 0)$.

If the two relays are collusive as shown in (7), according to Lemma 5, the training-based SK-PK capacity region is

$$\mathcal{C}^{G,(c)}_{SP} \triangleq \bigcup_{\mathbf{T}\in\mathcal{T}} \Big\{ (R_S, R_P) : R_S, R_P \geq 0, \; R_P \leq I^G_{A,B}, \; R_S + R_P \leq I^G_{A,B} + I^{G,(2)}_{min} \Big\}. \quad (46)$$

C. Numerical Results

In this subsection, some numerical results of the SK-PK rate region in Eqs. (43)-(46) will be provided for different choices of the parameters.

Fig. 5 shows the SK-PK rate regions ($\mathcal{R}^G_{SP,1}$ and $\mathcal{R}^G_{SP,2}$) for different values of block length T, where we set the power as $P = 20$, and $(\delta^2_{A,1}, \delta^2_{A,2}, \delta^2_{B,1}, \delta^2_{B,2}, \delta^2_{1,2}, \delta^2_{A,B}) = (0.5, 1.1, 3.7, 2.1, 3.1, 0.1)$. As shown in this figure, both the two regions are enlarged as the block length T decreases. In addition, the second proposed key generation algorithm (Algorithm 2) yields larger regions in comparison with the first proposed one (Algorithm 1).

Fig. 6 plots the SK-PK capacity region $\mathcal{C}^G_{SP}$ for different values of the channel parameters $\delta^2_{1,2}$ between the two relays,

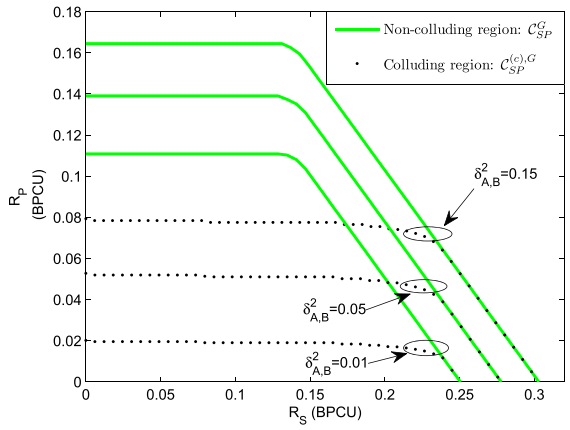


Fig. 7. Training-based SK-PK capacity regions in the non-collusive and collusive cases for different values of $\delta^2_{A,B}$, where $T = 28$, $P = 20$, $(\delta^2_{A,1}, \delta^2_{A,2}, \delta^2_{B,1}, \delta^2_{B,2}, \delta^2_{1,2}) = (0.5, 1.1, 3.7, 2.1, 3.1)$.

where we fix $T = 28$, $P = 20$. As shown in this figure, the SK rate can be enlarged as the variance of the inter-relay channel $\delta^2_{1,2}$ increases, but the PK rate cannot. This is consistent with the rate region shown in (40). However, when $\delta^2_{1,2} > 0.5$, the inter-relay channel is not helpful to further enhance the SK rate. This is because the bottleneck in (45) is $I^G_{A,1} + I^G_{A,2}$ or $I^G_{B,1} + I^G_{B,2}$, which is not relevant to the inter-relay channel.

Fig. 7 compares the training-based SK-PK capacity regions $\mathcal{C}^G_{SP}$ and $\mathcal{C}^{G,(c)}_{SP}$ with respect to the non-collusive and collusive cases, respectively. Different values of the variance of the direct link ($\delta^2_{A,B}$) have been considered, and we set $T = 28$, $P = 20$, $(\delta^2_{A,1}, \delta^2_{A,2}, \delta^2_{B,1}, \delta^2_{B,2}, \delta^2_{1,2}) = (0.5, 1.1, 3.7, 2.1, 3.1)$. From this figure, one can observe that, for the collusive case, the PK rate decreases greatly as the direct link becomes weaker. On the other hand, the PK rate in the non-collusive case is much larger than that in the collusive case. This is because the two relays can help Alice and Bob to improve the PK rate in the non-collusive case, whereas the PK rate in the collusive case is only depending on the quality of the direct link between Alice and Bob.

V. Conclusion

This paper investigated a cooperative PIN model for simultaneously generating SK and PK with the public discussion. The SK needs to be protected from Eve, while the PK needs to be protected from not only Eve but also from the two relays. Two cooperative SK-PK generation algorithms are proposed for this model, whose key features are to utilize the XOR operation and a specific random-binning based SK-PK codebook to generate the expected keys, respectively. The achievable SK-PK rate regions of these two proposed algorithms are also analyzed. The result shows that the achievable key rate region of the second algorithm with random-bing based codebook is demonstrated to be exactly the same as the derived outer bound, and hence the capacity region of this PIN model is established. Next, the two proposed SK-PK generation algorithms are extended to a cooperative wireless network, where the correlated source observations are obtained from estimating wireless channels during a training phase. As a future direction, this SK-PK generation problem can

be extended to more general networks with more than two relays, or with more than two terminals that wish to share common keys.

APPENDIX A
PROOF OF THE CONVERSE OF THEOREM 4

The converse of Theorem 4 can be proved by deriving the outer bound that consists of the upper bounds on R_P and $R_P + R_S$, respectively.

The upper bound of the private key rate R_P can be obtained based on several enhanced source models. In particular, for any given $i = 1, 2$, construct an enhanced source model in which only the secrecy constraint on relay i is considered (i.e., $(1/n)I(K_P; X_i^n, \mathbf{F} \leq \epsilon)$) and the secrecy constraint on relay $3-i$ is ignored. Moreover, assume Alice to be a genie-aided supper terminal which combines its own observation and the observation of relay $3-i$, so Alice observes $\tilde{X}_A^n \triangleq (X_A^n, X_{3-i}^n)$ now. This enhanced source model with alphabets $(\tilde{\mathcal{X}}_A, \mathcal{X}_B, \mathcal{X}_i)$ becomes a special case of the cooperative DMS model in [3]. According to [3, eq. (2.38)] the *private key capacity* of this enhanced source model is $I(\tilde{X}_A, X_B|X_i)$ with $\tilde{X}_A \triangleq (X_A, X_{3-i})$, which implies that the upper bound on the private key rate can be obtained as

$$\begin{aligned} R_P &\leq I(X_A, X_{3-i}; X_B|X_i) \\ &= I(Y_{B,A}, Y_{1,A}, Y_{2,A}, Y_{A,3-i}, Y_{B,3-i}, Y_{i,3-i}; \\ &\qquad Y_{A,B}, Y_{1,B}, Y_{2,B}|Y_{A,i}, Y_{B,i}, Y_{3-i,i}) \\ &\overset{(a)}{=} I(Y_{B,A}, Y_{3-i,A}, Y_{A,3-i}, Y_{B,3-i}; Y_{A,B}, Y_{3-i,B}) \\ &= I_{A,B} + I_{B,3-i}, \end{aligned} \tag{47}$$

where (a) is due to the definition of the PIN model in (1).

Similar to the above procedure, another symmetric enhanced source model can also be constructed, in which Bob is a genie-aided which has access to the observation of relay $3-i$ in advance, and hence the rate R_P can also be upper bounded by $R_P \leq I_{A,B} + I_{A,3-i}$. Thus, for any $i = 1, 2$, $R_P \leq I_{A,B} + \min\{I_{B,3-i}, I_{A,3-i}\}$, and the tight upper bound on R_P can be obtained as

$$\begin{aligned} R_P &\leq I_{A,B} + \min_{i=1,2} \min\{I_{B,3-i}, I_{A,3-i}\} \\ &= I_{A,B} + I_{min}^{(1)}. \end{aligned} \tag{48}$$

In addition, $R_S + R_P$ will be upper bounded in the next, based on the secrecy requirement and the reliable requirement. In particular, the ϵ-recoverable requirement in Definition 1 ensures the reliable requirement, which implies that

$$H(K_S, K_P|\mathbf{F}, X_A^n) \leq \epsilon \log(|\mathcal{K}_S| \times |\mathcal{K}_P|) + 1 \triangleq n\delta_1, \tag{49}$$

$$H(K_S, K_P|\mathbf{F}, X_B^n) \leq n\delta_1, \tag{50}$$

where Fano's inequality is utilized. Based on the above relationships, we have

$$\begin{aligned} &n(R_S + R_P - 2\delta) \\ &\overset{(b)}{\leq} H(K_S, K_P) \\ &= H(K_S, K_P|\mathbf{F}) + I(K_S, K_P; \mathbf{F}) \\ &\overset{(c)}{\leq} H(K_S, K_P|\mathbf{F}) + n\epsilon \\ &\leq H(K_S, K_P|\mathbf{F}) - H(K_S, K_P|\mathbf{F}, X_B^n) + n(\epsilon + \delta_1) \\ &\leq I(K_S, K_P, X_A^n; X_B^n|\mathbf{F}) + n(\epsilon + \delta_1) \\ &\leq I(X_A^n; X_B^n|\mathbf{F}) + H(K_S, K_P|\mathbf{F}, X_A^n) + n(\epsilon + \delta_1) \\ &\leq I(X_A^n; X_B^n|\mathbf{F}) + n(\epsilon + 2\delta_1) \\ &\leq \min \left\{ \begin{array}{l} I(X_A^n, X_1^n, X_2^n; X_B^n|\mathbf{F}),\ I(X_A^n; X_B^n, X_1^n, X_2^n|\mathbf{F}) \\ I(X_A^n, X_1^n; X_B^n, X_2^n|\mathbf{F}),\ I(X_A^n, X_2^n; X_B^n, X_1^n|\mathbf{F}) \end{array} \right\} \\ &\quad + n(\epsilon + 2\delta_1), \end{aligned} \tag{51}$$

where (b) is based on Definition 2 and the fact that K_S is independent of K_P; (c) is obtained according to the secrecy requirement in (5). Now, the first term in the min-function in (51) will be calculated, and the other three terms can be analyzed using similar procedures.

As shown in Section II, for $\forall 1 \leq t \leq 4r$, $H(F_t|X_B^n, F^{t-1}) = 0$, $H(F_t|X_A^n, F^{t-1}) = 0$, $H(F_t|X_2^n, F^{t-1}) = 0$, $H(F_t|X_1^n, F^{t-1}) = 0$ when $t \mod 4 = 0, 3, 2, 1$, respectively. Therefore, if $t \mod 4 = 0$,

$$\begin{aligned} &I(X_A^n, X_1^n, X_2^n; X_B^n|F^t) \\ &\quad = H(X_A^n, X_1^n, X_2^n|F^t) - H(X_A^n, X_1^n, X_2^n|X_B^n, F^t) \\ &\quad = H(X_A^n, X_1^n, X_2^n|F^t) - H(X_A^n, X_1^n, X_2^n|X_B^n, F^{t-1}) \\ &\quad \leq I(X_A^n, X_1^n, X_2^n; X_B^n|F^{t-1}). \end{aligned} \tag{52}$$

If $t \mod 4 = 3, 2, 1$,

$$\begin{aligned} &I(X_A^n, X_1^n, X_2^n; X_B^n|F^t) \\ &\quad = H(X_B^n|F^t) - H(X_B^n|X_A^n, X_1^n, X_2^n, F^t) \\ &\quad = H(X_B^n|F^t) - H(X_B^n|X_A^n, X_1^n, X_2^n, F^{t-1}) \\ &\quad \leq I(X_A^n, X_1^n, X_2^n; X_B^n|F^{t-1}). \end{aligned} \tag{53}$$

Repeating this procedure $4r$ times from $t = 4r$ to $t = 1$, $I(X_A^n, X_1^n, X_2^n; X_B^n|\mathbf{F}) \leq I(X_A^n, X_1^n, X_2^n; X_B^n)$ can be obtained. Then due to the fact that the source observation at each terminal is i.i.d., it is not difficult to prove that $I(X_A^n, X_1^n, X_2^n; X_B^n) \leq nI(X_A, X_1, X_2; X_B)$. Hence the first term in the min-function in (51) can be upper bounded as

$$\begin{aligned} I(X_A^n, X_1^n, X_2^n; X_B^n|\mathbf{F}) &\leq nI(X_A, X_1, X_2; X_B) \\ &= n(I_{A,B} + I_{B,1} + I_{B,2}). \end{aligned} \tag{54}$$

Using similar proof steps to the other three terms in the min-function in (51), the upper bound on $R_S + R_P$ can be expressed as

$$R_S + R_P \leq I_{A,B} + I_{min}^{(2)} + \epsilon + 2\delta_1 + 2\delta. \tag{55}$$

The converse has been proved according to (48) and (55).

APPENDIX B
PROOF OF THE CONVERSE OF LEMMA 5

The converse of Lemma 5 can be proved by deriving the outer bound that consists of the upper bounds on R_P and $R_P + R_S$, respectively. The upper bound on $R_P + R_S$ with respect to this collusive case is the same as that in Appendix A with respect to the non-collusive case, which has been derived in (55). In the next, we only need to derive the upper bound on the private key rate R_P when the two relay are collusive.

According to the ϵ-recoverable requirement in Definition 1 that ensures the reliable requirement, we have

$$H(K_P|\mathbf{F}, X_A^n) \le \epsilon \log(|\mathcal{K}_P|) + 1 \triangleq n\delta_1, \quad (56)$$
$$H(K_P|\mathbf{F}, X_B^n) \le n\delta_1, \quad (57)$$

where Fano's inequality is utilized. Based on the above relationships, we have

$$\begin{aligned}
n(R_P - \delta) &\overset{(a)}{\le} H(K_P) \\
&= H(K_P|\mathbf{F}, X_1^n, X_2^n) + I(K_P; \mathbf{F}, X_1^n, X_2^n) \\
&\overset{(b)}{\le} H(K_P|\mathbf{F}, X_1^n, X_2^n) + n\epsilon \\
&\le H(K_P|\mathbf{F}, X_1^n, X_2^n) - H(K_P|\mathbf{F}, X_B^n) + n(\epsilon + \delta_1) \\
&\le I(K_P, X_A^n; X_B^n|\mathbf{F}) + n(\epsilon + \delta_1) \\
&\le I(X_A^n; X_B^n|\mathbf{F}, X_1^n, X_2^n) + H(K_P|\mathbf{F}, X_A^n) + n(\epsilon + \delta_1) \\
&\le I(X_A^n; X_B^n|\mathbf{F}, X_1^n, X_2^n) + n(\epsilon + 2\delta_1) \\
&\overset{(c)}{\le} nI(X_A, X_B|X_1, X_2) + n(\epsilon + 2\delta_1) \\
&\overset{(d)}{=} nI(Y_A; Y_B) + n(\epsilon + 2\delta_1) \quad (58)
\end{aligned}$$

where (a) is based on Definition 2; (b) is obtained according to the secrecy requirement in (7) with respect to the collusive case; (c) follows similar derivation steps from Eq. (52) to (54); (d) is based on the definition of the PIN model in Section II.

Thus, when the two relays are collusive, R_P can be upper bounded as

$$R_P \le I(Y_A; Y_B) + \delta + \epsilon + 2\delta_1.$$

Appendix C
Proof of Lemma 2

The proof adopts the procedure in [30, Proof of Lemma 22.3] with variations. Without loss of generality, only $H(\mathbf{W}|W_1, \tilde{W}_{1,2}, K_P^1, \mathcal{C})$ will be upper bounded; $H(\mathbf{W}|W_2, \tilde{W}_{1,2}, K_P, \mathcal{C})$ can be calculated similarly. Firstly,

$$\begin{aligned}
&H(\mathbf{W}|W_1, \tilde{W}_{1,2}, K_P, \mathcal{C}) \\
&\quad = \sum_{w_1, \tilde{w}_{1,2}, k_P} p(w_1, \tilde{w}_{1,2}, k_P) H(\mathbf{W}|w_1, \tilde{w}_{1,2}, k_P, \mathcal{C}). \quad (59)
\end{aligned}$$

Now, for a codebook c and a given tuple $(w_1, \tilde{w}_{1,2}, k_P)$, denote $N(w_1, \tilde{w}_{1,2}, k_P, c)$ as the number of the codewords $\mathbf{w} \in \mathcal{W} = \mathcal{W}_{A,B} \times \mathcal{W}_1 \times \mathcal{W}_2 \times \tilde{\mathcal{W}}_{1,2}$ satisfying: (i) $\mathbf{w}$ is in the k_P-th bin of the SK-PK codebook; (ii) the second and the fourth elements of the sequence $\mathbf{w}$ is w_1 and $\tilde{w}_{1,2}$, respectively. Since the SK-PK codebook is constructed based on random-binning, $N(w_1, \tilde{w}_{1,2}, k_P, \mathcal{C})$ is binomially distributed, i.e., $N(w_1, \tilde{w}_{1,2}, k_P, \mathcal{C}) \sim B(2^{-n(R_1+\tilde{R}_{1,2})}, 2^{nR_S})$, where 2^{nR_S} is the number of codewords in each bin. Hence its expectation and variance are

$$\begin{aligned}
\mathbb{E}[N(w_1, \tilde{w}_{1,2}, k_P, \mathcal{C})] &= 2^{n(R_S - R_1 - \tilde{R}_{1,2})}, \\
Var[N(w_1, \tilde{w}_{1,2}, k_P, \mathcal{C})] &= 2^{n(R_S - R_1 - \tilde{R}_{1,2})}. \quad (60)
\end{aligned}$$

Now, define an indicator variable as

$$\begin{aligned}
&E_1(w_1, \tilde{w}_{1,2}, k_P, \mathcal{C}) \\
&= \begin{cases} 1, & \text{if } N(w_1, \tilde{w}_{1,2}, k_P, \mathcal{C}) \ge 2\mathbb{E}[N(w_1, \tilde{w}_{1,2}, k_P, \mathcal{C})], \\ 0, & \text{otherwise.} \end{cases} \quad (61)
\end{aligned}$$

Then, by Chebyshev inequality

$$\begin{aligned}
P\{E_1 = 1\} &\le \frac{Var[N(w_1, \tilde{w}_{1,2}, k_P, \mathcal{C})]}{\mathbb{E}^2[N(w_1, \tilde{w}_{1,2}, k_P, \mathcal{C})]} \\
&\le 2^{-n(R_S - R_1 - \tilde{R}_{1,2})}, \quad (62)
\end{aligned}$$

which is arbitrarily small when n is sufficiently large.

Now, denote $R = R_{A,B} + R_1 + R_2 + \tilde{R}_{1,2}$, then,

$$\begin{aligned}
&H(\mathbf{W}|w_1, \tilde{w}_{1,2}, k_P, \mathcal{C}) \\
&\quad \le H(\mathbf{W}, E_1|w_1, \tilde{w}_{1,2}, k_P, \mathcal{C}) \\
&\quad = H(E_1) + P(E_1 = 1)H(\mathbf{W}|w_1, \tilde{w}_{1,2}, k_P, E_1 = 1, \mathcal{C}) \\
&\qquad + P(E_1 = 0)H(\mathbf{W}|w_1, \tilde{w}_{1,2}, k_P, E_1 = 0, \mathcal{C}) \\
&\quad \overset{(a)}{\le} 1 + P\{E_1 = 1\} \log |\mathcal{W}| \\
&\qquad + H(\mathbf{W}|w_1, \tilde{w}_{1,2}, k_P, E_1 = 0, \mathcal{C}) \\
&\quad \overset{(b)}{\le} 1 + nR \times 2^{-n(R_S - R_1 - \tilde{R}_{1,2})} \\
&\qquad + H(\mathbf{W}|w_1, \tilde{w}_{1,2}, k_P, E_1 = 0, \mathcal{C}) \\
&\quad \overset{(c)}{\le} 1 + nR \times 2^{-n(R_S - R_1 - \tilde{R}_{1,2})} \\
&\qquad + \log\left(2 \times 2^{n(R_S - R_1 - \tilde{R}_{1,2})}\right), \quad (63)
\end{aligned}$$

where (a) follows from the fact that $H(E_1) \le 1$; (b) is due to (62); (c) is due to the fact that $N(w_1, \tilde{w}_{1,2}, k_P, \mathcal{C}) < 2 \times 2^{n(R_S - R_1 - \tilde{R}_{1,2})}$ when $E_1 = 0$. So

$$H(\mathbf{W}|w_1, \tilde{w}_{1,2}, k_P, \mathcal{C}) \le n(R_S - R_1 - \tilde{R}_{1,2} + \delta_n), \quad (64)$$

where $\delta_n = \frac{2}{n} + R \times 2^{-n(R_S - R_1 - \tilde{R}_{1,2})}$. Since $R_S > R_1 + \tilde{R}_{1,2}$ as shown in (29), $\delta_n \to 0$ as $n \to \infty$. Recalling (59), $H(\mathbf{W}|W_1, \tilde{W}_{1,2}, K_P, \mathcal{C}) \le n(R_S - R_1 - \tilde{R}_{1,2} + \delta_n)$ has been proved.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[2] 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.

[3] I. Csiszár and 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 and P. Narayan, "The secret key–private key capacity region for three terminals," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Sep. 2005, pp. 2142–2146.

[6] C. Ye and A. Reznik, "Group secret key generation algorithms," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 2596–2600.

[7] S. Nitinawarat, C. Ye, A. Barg, P. Narayan, and A. Reznik, "Secret key generation for a pairwise independent network model," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6482–6489, Dec. 2010.

[8] L. Lai and L. Huie, "Simultaneously generating multiple keys in many to one networks," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2013, pp. 2394–2398.

[9] L. Lai and S.-W. Ho, "Key generation algorithms for pairwise independent networks based on graphical models," *IEEE Trans. Inf. Theory*, vol. 61, no. 9, pp. 4828–4837, Sep. 2015.

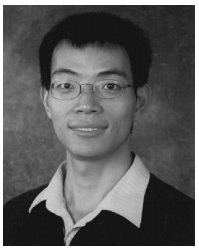
[10] P. Xu, Z. Ding, and X. Dai, "The private key capacity of a cooperative pairwise-independent network," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2015, pp. 286–290.

[11] H. Zhang, L. Lai, Y. Liang, and H. Wang, "The capacity region of the source-type model for secret key and private key generation," *IEEE Trans. Inf. Theory*, vol. 60, no. 10, pp. 6389–6398, Oct. 2014.

[12] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 364–375, Sep. 2007.

[13] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 240–254, Jun. 2010.
[14] L. Lai, Y. Liang, and H. V. Poor, "A unified framework for key agreement over wireless fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 480–490, Apr. 2012.
[15] A. Khisti, "Interactive secret key generation over reciprocal fading channels," in *Proc. IEEE 50th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2012, pp. 1374–1381.
[16] B. T. Quist and M. A. Jensen, "Optimal channel estimation in beamformed systems for common-randomness-based secret key establishment," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 7, pp. 1211–1220, Jul. 2013.
[17] B. T. Quist and M. A. Jensen, "Maximizing the secret key rate for informed radios under different channel conditions," *IEEE Trans. Wireless Commun.*, vol. 12, no. 10, pp. 5146–5153, Oct. 2013.
[18] Q. Wang, K. Xu, and K. Ren, "Cooperative secret key generation from phase estimation in narrowband fading channels," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 9, pp. 1666–1674, Oct. 2012.
[19] L. Lai, Y. Liang, and W. Du, "Cooperative key generation in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 8, pp. 1578–1588, Sep. 2012.
[20] H. Zhou, L. M. Huie, and L. Lai, "Secret key generation in the two-way relay channel with active attackers," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 3, pp. 476–488, Mar. 2014.
[21] D. Chen, Z. Qin, X. Mao, P. Yang, Z. Qin, and R. Wang, "SmokeGrenade: An efficient key generation protocol with artificial interference," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1731–1745, Nov. 2013.
[22] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[23] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
[24] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
[25] P. Xu, Z. Ding, X. Dai, and K. K. Leung, "A general framework of wiretap channel with helping interference and state information," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 182–195, Feb. 2014.
[26] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.
[27] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. K. Leung, "Secrecy rate optimizations for a mimo secrecy channel with a multiple-antenna eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 63, no. 4, pp. 1678–1690, May 2014.
[28] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471–480, Jul. 1973.
[29] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Hoboken, NJ, USA: Wiley, 2006.
[30] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

Peng Xu received the B.Eng. and Ph.D. degrees in electronic and information engineering from the University of Science and Technology of China, Anhui, China, in 2009 and 2014, respectively. Since 2014, he has been a Postdoctoral Researcher with the Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei, China. He has also been visiting Lancaster University since 2015. His current research interests include cooperative communications, information theory, information-theoretic secrecy, and 5G networks.



Zhiguo Ding (S'03–M'05–SM'15) received the B.Eng. degree in electrical engineering from the Beijing University of Posts and Telecommunications, in 2000, and the Ph.D. degree in electrical engineering from Imperial College London, in 2005. From 2005 to 2014, he was with Queen's University Belfast, Imperial College, and Newcastle University. Since 2014, he has been with Lancaster University as a Chair Professor.

His research interests are 5G networks, game theory, cooperative and energy harvesting networks, and statistical signal processing. He serves as an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGIES, the IEEE WIRELESS COMMUNICATION LETTERS, the IEEE COMMUNICATION LETTERS, and the *Journal of Wireless Communications and Mobile Computing*. He received the best paper award at the IET Communication Conference on Wireless, Mobile and Computing 2009, the IEEE Communication Letter Exemplary Reviewer 2012, and the EU Marie Curie Fellowship from 2012 to 2014.

Xuchu Dai received the B.Eng. degree in electrical engineering from Airforce Engineering University, Xi'an, China, in 1984, and the M.Eng. and Ph.D. degrees in communication and information system from the University of Science and Technology of China, Hefei, China, in 1991 and 1998, respectively.

He is a Professor with the Department of Electronic Engineering and Information Science, University of Science and Technology of China. From 2000 to 2002, he was with the Hong Kong University of Science and Technology as a Postdoctoral Researcher. His current research interests include wireless communication systems, blind adaptive signal processing, and signal detection.

George K. Karagiannidis (M'96–SM'03–F'14) was born in Pithagorion, Greece. He received the University Diploma and Ph.D. degrees in electrical and computer engineering from the University of Patras, in 1987 and 1999, respectively. From 2000 to 2004, he was a Senior Researcher with the Institute for Space Applications and Remote Sensing, National Observatory of Athens, Greece. In 2004, he joined the faculty of Aristotle University of Thessaloniki, Greece, where he is currently a Professor with the Electrical and Computer Engineering Department and the Director of the Digital Telecommunications Systems and Networks Laboratory.

His research interests are in the broad area of digital communications systems with an emphasis on wireless communications, optical wireless communications, wireless power transfer and applications, molecular communications, communications and robotics, and wireless security.

He has authored or coauthored over 400 technical papers in scientific journals and presented at international conferences. He is also author of the Greek edition of a book on *Telecommunications Systems*, and coauthor of the book *Advanced Optical Wireless Communications Systems* (Cambridge Publications, 2012).

Dr. Karagiannidis has been involved as General Chair, Technical Program Chair, and member of Technical Program Committees in several IEEE and non-IEEE conferences. He was an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS, a Senior Editor of the IEEE COMMUNICATIONS LETTERS, an Editor of the *EURASIP Journal of Wireless Communications & Networks*, and several times Guest Editor in IEEE Selected Areas in Communications. From 2012 to 2015, he was the Editor-in Chief of the IEEE COMMUNICATIONS LETTERS. He is an Honorary Professor at South West Jiaotong University, Chengdu, China. He was selected as a 2015 Thomson Reuters Highly Cited Researcher.