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

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

Abstract—This paper studies the problem of simultaneously generating secret key (SK) and 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, whereas 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 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-binning 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], [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 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], [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 $W_\alpha$ obtained over $n$ channel uses, $R_\alpha$ represents its average rate, i.e., $R_\alpha = (1/n)H(W_\alpha)$. For two such messages $W_\alpha$ and $W_\beta$, let $W_\alpha \wedge W_\beta$ denote the one of them with a smaller rate. Also, $C$ represents an arbitrary constant. Note that $W_\alpha = C$ if $R_\alpha = 0$.

II. A COOPERATIVE PAIRWISE INDEPENDENT NETWORK

![Fig. 1. The cooperative PIN model for the SK and PK generation.](image)

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], [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], [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.,

$$p(X_A, X_B, X_1, X_2) \triangleq \prod_{(j,k) \in A} p_{Y_{j,k}, Y_{k,j}}(y_{j,k}, y_{k,j}), \quad (1)$$
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 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 $F_i$ is the transmission in the $t$-th time slot, $1 \leq t \leq 4r$. Specifically, relay 1, relay 2, Alice and Bob transmit $F_1, F_2, F_3, F_0$, respectively, where $F_i = \{F_{i,1}, F_{i,2}, \cdots, F_{i,4} \}$ when $t \mod 4 = i$, $i = 1, 2, 3, 0$. Each $F_i$ is generated according to its own observation and all the previous transmissions $F^{t-1} = (F_1, \cdots, F_{t-1})$, i.e., $F_t = f_t(X^n_A, F^{t-1})$, $f_t(X^n_B, F^{t-1})$, $f_t(X^n, F^{t-1})$ 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 $\epsilon$-recoverable from another variable $V$ if there exists a deterministic function $g$ such that $P_r(g(V) \neq U) \leq \epsilon$.

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

- $K_S$ and $K_P$ are mutually independent.
- The pair $(K_S, K_P)$ can be $\epsilon$-recoverable from $(X^n_A, F)$ and $(X^n_B, F)$, respectively.
- $K_S$ and $K_P$ are nearly uniformly distributed, i.e.,
  $${1 \over n} H(K_S) \geq 1 \log |K_S| - \epsilon, \quad (3)$$
  $${1 \over n} H(K_P) \geq 1 \log |K_P| - \epsilon, \quad (4)$$
  for sufficiently large $n$, where $|K_S|$ and $|K_P|$ are the alphabet sizes of $K_S$ and $K_P$, respectively.
- $K_S$ and $K_P$ satisfy the secrecy conditions:
  $${1 \over n} I(K_S; F) \leq \epsilon, \quad (5)$$
  $${1 \over n} I(K_P; F, X^n_i) \leq \epsilon, \quad i = 1, 2, \quad (6)$$

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

$$\frac{1}{n} I(K_P; F, X^n_1, X^n_2) \leq \epsilon. \quad (7)$$

**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 $\epsilon$-(SK,PK) pair $(K_S, K_P)$ such that

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

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

### 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

$$I_{j,k}(y) \triangleq I(Y_{j,k}; Y_{k,j}), \quad \forall (j, k) \in \mathcal{A}, \quad (9)$$

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

$$I_{min}^{(1)}(y) \triangleq \min \{I(A_1, A_2), I(B_1, B_2), I(A_1, B_1), I(A_2, B_2)\}, \quad (10)$$

$$I_{min}^{(2)}(y) \triangleq \min \{I(A_1 + A_2, B_1 + B_2), I(A_1 + B_2, A_2 + B_1), I(A_1 + B_1, A_2 + B_2)\}. \quad (11)$$

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) **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 $Y^n_{A,i}$ and $Y^n_{B,i}$, $i = 1, 2$; the two relays agree on $W_{1,2}$ using $Y^n_{A,1}$ and $Y^n_{B,2}$; Alice and Bob agree on $W_{A,B}$ using $Y^n_{A,B}$ and $Y^n_{A,B}$. Each pairwise key $W_{j,k}$, is generated using the standard point-to-point techniques.

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

Step 3: SK and PK agreement:

- Now, for the CR $(W_{A,B}, W_1, W_2, W_{1,2})$ 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 $K_S = (K_{S,1}, K_{S,2}, K_{S,3}, W_{1,2})$ as the final SK, and $K_P = (K_{P,3}, K_{P,1} + K_{P,2})$ as the final PK.

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

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

$$
\bar{R}_{1,2} \leq \min \left\{ \frac{R_{2,1}^2 + R_{2,2}^R}{2}, \frac{R_{2,1}^R + R_{2,2}^* + R_{1,2}^* + R_{2,2}^R}{2} \right\}
$$

(16)

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

$$
\hat{R}_{1,2} \leq \min \left\{ \frac{R_{A,1} + R_{A,2} + R_{B,1} + R_{B,2}}{2}, \frac{R_{B,1} + R_{B,2} + R_{A,2} + R_{1,2} + R_{B,2}}{2} \right\}
$$

(18)

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

---

2Take the source pair $(Y_{A,B}^*, Y_{A,B}^0)$ for example. According to Slepian-Wolf source coding [28], [29], Alice can transmit $nH(Y_{A,B}^*, Y_{A,B}^0)$ bits of information over the public channel, such that Bob can recover Alice’s observation sequence $Y_{A,B}^0$. Then, Alice and Bob utilize correlation between $Y_{A,B}^*$ and $Y_{A,B}^0$ to agree on their pairwise key. One can refer to [2], [14] for more details of this pairwise key generation.
i) If \( R_{A,i} \leq R_{B,i} \) for \( \forall i = 1, 2 \), or \( R_{A,i} \geq R_{B,i} \) for \( \forall i = 1, 2 \), we cannot generate \( \tilde{W}_{1,2} \) with a positive rate, so simply set \( W_{1,2} = C \).

ii) Otherwise, if \( R_{A,1} \geq R_{B,1} \) and \( R_{A,2} \leq R_{B,2} \), relay 1 sends \( W_{A,1}^{2} \cup W_{1,2} \) over the public channel, so that relay 2 and Alice can agree on a common message \( W_{A,1}^{2} \). Then, relay 2 sends \( (W_{B,2}^{2} \cup W_{1,2}) \) so that Alice and Bob can agree on \( \tilde{W}_{1,2} = W_{A,1}^{2} \cup W_{1,2} \cup W_{B,2}^{2} \) whose rate is \( \min\{R_{A,1}, R_{1,2}, R_{B,2}^{2}\} \).

iii) Similar to the previous case, if \( R_{A,1} \leq R_{B,1} \) and \( R_{A,2} \geq R_{B,2} \), Alice and Bob can agree on \( W_{1,2} = W_{A,2}^{2} \) with the rate \( \min\{R_{A,2}, R_{1,2}, R_{B,2}^{2}\} \).

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 \((W_{A,B}, W_{1}, W_{2}, W_{1,2})\) between Alice and Bob, i.e.,

\[
\frac{1}{n} I(W_{A,B}, W_{1}, W_{2}, \tilde{W}_{1,2}; F) \leq \epsilon,
\]

where \( W_{A,B} \) is the pairwise key between Alice and Bob, and \( F \) 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 \((W_{A,B}, W_{1}, W_{2}, W_{1,2})\) 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

\[
R_{S,3} + R_{P,3} = R_{A,B}, \\
R_{S,4} + R_{P,4} = R_{i}, \quad i = 1, 2, \\
R_{P,1} = R_{P,2}.
\]

Now, Alice and Bob agree on the SK \( K_{S} \) by concatenating \((K_{S,1}, K_{S,2}, K_{S,3}, \tilde{W}_{1,2})\), 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

\[
R_{S} = R_{S,1} + R_{S,2} + R_{S,3} + \tilde{R}_{1,2}, \\
R_{P} = R_{P,3} + R_{P,1}.
\]

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, \( R_{SP,1} \), for the cooperative PIN model in Section II is achievable, where

\[
R_{SP,1} \triangleq \begin{cases} (R_{S}, R_{P}) : R_{S}, R_{P} \geq 0, & R_{P} \leq I_{A,B} + I_{min}^{(1)}, \\
R_{S} + 2R_{P} \leq 2I_{A,B} + I_{min}^{(2)}, & R_{S} + R_{P} \leq I_{A,B} + I_{min}^{(2)} \end{cases}.
\]

**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 \((R_{1}, R_{2}, R_{1,2}, R_{A,B})\), by applying Fourier-Motzkin elimination to eliminate \( R_{1,2}, R_{S,j}, R_{S,j} \) for \( j = 1, 3 \) in Eqs. (17), (20)-(22), (23)-(24), the rate pair \((R_{S}, R_{P})\) satisfies the constraints in the following region:

\[
R_{P} \leq \min\{R_{1,2}, R_{2}\} + R_{A,B}, \\
R_{S} + 2R_{P} \leq \tilde{R}_{1,2} + 2R_{A,B}, \\
R_{S} + R_{P} \leq \tilde{R}_{1,2} + R_{A,B}.
\]

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 \((W_{A,B}, W_{1}, W_{2}, W_{1,2})\) 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., \( W_{A,B}, R_{i}, \tilde{R}_{1,2} \) 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.

**Codebook Generation:** The alphabets of \( W_{A,B}, W_{1}, W_{2}, \tilde{W}_{1,2} \) are \( W_{A,B} = \{1, \ldots, 2^{R_{A,B}}\}, \ W_{i} = \{1, \ldots, 2^{R_{i}}\}, \ i = 1, 2, \ \tilde{W}_{1,2} = \{1, \ldots, 2^{	ilde{R}_{1,2}}\} \), respectively. Define their Descartes product as \( W \triangleq W_{A,B} \times W_{1} \times W_{2} \times \tilde{W}_{1,2}. \) Then a
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 \(w = (w_{A,B}, w_1, w_2, \tilde{w}_{1,2})\) in the set \(W\) into \(2^{N_{R_P}}\) bins each with \(2^{N_{R_S}}\) elements, where

\[
R_S \geq \max\{R_1, R_2\} + \tilde{R}_{1,2} + \epsilon_2, \quad R_P = R_{A,B} + R_1 + R_2 + \tilde{R}_{1,2} - R_S \geq 0.
\]

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

Key Generation: Alice and Bob find the index \((K_P, K_S)\) in the SK-PK codebook such that the codeword \(w(K_P, K_S) = (W_{A,B}, W_1, W_2, \tilde{W}_{1,2})\), 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.

Analysis of Secrecy Constraints: We will analyze secrecy constrains in (5) and (6) averaged on \(C\). 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

\[
\frac{1}{n} I(K_P; K_S; F|C) \leq \frac{1}{n} I(W_{A,B}; W_1, W_2, \tilde{W}_{1,2}; F|C) \\
= \frac{1}{n} I(W_{A,B}; W_1, W_2, \tilde{W}_{1,2}; F) \leq \epsilon.
\]

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

\[
I(K_P; W_i, \tilde{W}_{1,2}|C) = I(K_P; W_i, \tilde{W}_{1,2}|C) - I(W_i, \tilde{W}_{1,2}|K_P) \\
= I(W; W_i, \tilde{W}_{1,2}|C) - I(W_i, \tilde{W}_{1,2}|K_P) \\
= I(W; W_i, \tilde{W}_{1,2}|C) - H(W|K_P, C) + H(W|W_i, \tilde{W}_{1,2}, K_P) \\
= H(W_i, \tilde{W}_{1,2}) - H(W|K_P, C) + H(W|W_i, \tilde{W}_{1,2}, K_P), \tag{32}
\]

where \((a)\) is due to the fact that \(K_P\) is determined by \(W\). 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

\[
H(W|K_P, C) = H(W|C) + H(K_P|W, C) - H(K_P|C) \\
= H(W) - H(K_P|C) \\
\geq n(R_{A,B} + R_1 + R_2 + \tilde{R}_{1,2}) - nR_P \\
= nR_S, \tag{33}
\]

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),

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

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

Proof: Refer to Appendix C.

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

\[
I(K_P; W_i, \tilde{W}_{1,2}; F|C) \leq I(K_P; W_i, \tilde{W}_{1,2}; C) + I(K_P, W_i; F|W_i, \tilde{W}_{1,2}, C) \\
= I(K_P; W_i, \tilde{W}_{1,2}; C) + I(W_{A,B}, W_2; F|W_i, \tilde{W}_{1,2}, C) \tag{c} \\
\leq n(\delta_n + \epsilon), \tag{34}
\]

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

\[
I(K_P; X^n_i; F|C) \leq I(K_P; W_i, \tilde{W}_{1,2}; F|C) \leq n(\delta_n + 2\epsilon).
\]

Symmetrically, we have \(I(K_P; X^n_2; F|C) \leq n(\delta_n + 2\epsilon)\).

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, \(R_{SP2}\), for the cooperative PIN model in Section II is achievable, where

\[
R_{SP2} \triangleq \left\{ (R_S, R_P) : R_S, R_P \geq 0, \quad \begin{array}{ll}
R_P \leq I_{A,B} + I_{\min}^{(1)}, \\
R_S + R_P \leq I_{A,B} + I_{\min}^{(2)}
\end{array} \right\}. \tag{35}
\]

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

$$R_P \leq \min\{R_{A,1}, R_{A,2}, R_{B,1}, R_{B,2}\} + R_{A,B} - \epsilon_2,$$  
$$R_S + R_P = \overline{R}_{1,2} + R_{A,B},$$

where $\overline{R}_{1,2}$ 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., $C_{SP} = \mathcal{R}_{SP,2}$.

**Proof:** The achievability of $C_{SP}$ 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] (Theorem 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] (Theorem 1) with two relays. The PK generation work can also be found in [19] (Section 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

$$C_{SP}^{(c)} \triangleq \{(R_S, R_P) : R_S, R_P \geq 0, \quad R_P \leq I_{A,B}, \quad R_S + R_P \leq I_{A,B} + I_{SP}^{(2)}\}.$$  

**Proof:** The achievability of $C_{SP}^{(c)}$ 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 $C_{SP}^{(c)} \subseteq \mathcal{R}_{SP,1} \subseteq C_{SP} = \mathcal{R}_{SP,2}$.

### 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, 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
training sequences \((S_1, S_2, S_A, S_B)\) in four successive time slots in each fading block, respectively. The size of each sequence \(S_n\) 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 \(||S_n||^2 = T_\alpha P\).

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 correlated source observations. From \(n\) fading blocks, Alice and relay 1 can collect \(n\) estimates, i.e., \((h_{1,1}^n, h_{1,A}^n)\).

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 \((h_{1,1}^n, h_{2,1}^n, h_{2,A}^n), (h_{2,1}^n, h_{1,1}^n, h_{1,B}^n), (h_{1,2}^n, h_{1,A}^n, h_{1,B}^n), (h_{2,2}^n, h_{1,2}^n, h_{2,B}^n)\), 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 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 how to obtain these correlated channel estimates 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

\[
\mathcal{R}_S^{G,1} \triangleq \bigcup_{\mathbf{T} \in \mathcal{T}} \left\{(R_S, R_P) : R_S, R_P \geq 0, \right. \\
R_P \leq I_{A,B}^{G,1} + I_{min}^{G,1}, \\
R_S + 2R_P \leq 2I_{A,B}^{G,1} + I_{min}^{G,2}, \\
R_S + R_P \leq I_{A,B}^{G,2} + I_{min}^{G,2}\right\},
\]

(43)

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

\[
\mathcal{T} \triangleq \{(T_1, T_2, T_A, T_B) : T_1 + T_2 + T_A + T_B = T\};
\]

(44)

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

\[
\mathcal{R}_S^{G,2} \triangleq \bigcup_{\mathbf{T} \in \mathcal{T}} \left\{(R_S, R_P) : R_S, R_P \geq 0, \right. \\
R_P \leq I_{A,B}^{G,1} + I_{min}^{G,1}, \\
R_S + R_P \leq I_{A,B}^{G,2} + I_{min}^{G,2}\right\},
\]

(45)
Algorithm 2: RG
SP,2
Algorithm 1: RG
SP,1
T=64
T=42
T=28

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

$$C_{SP}^{G(c)} \triangleq \bigcup_{T \in \mathcal{T}} \{(R_S, R_P) : R_S, R_P \geq 0, R_P \leq I_{A,B}^G, R_S + R_P \leq I_{A,B}^G + I_{\text{min}}^G(2)\}$$

(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 ($R_{SP,1}^G$ and $R_{SP,2}^G$) for different values of block length $T$, where we set the power as $P = 20$, and $\left(\delta_{A,1}, \delta_{A,2}, \delta_{B,1}, \delta_{B,2}, \delta_{T,1}, \delta_{T,2}, \delta_{A,B}\right) = (0.5, 1.1, 3.7, 2.1, 3.1, 0.1)$. 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 $C_{SP}^G$ for different values of the channel parameters $\delta_{1,2}$ between the two relays, 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 $\delta_{1,2}$ increases, but the PK rate cannot. This is consistent with the rate region shown in (40). However, when $\delta_{1,2} > 0.5$, the inter-relay channel is not helpful to further enhance the SK rate. This is because the bottleneck in (45) is $I_{A,1}^G + I_{A,2}^G$ or $I_{B,1}^G + I_{B,2}^G$, which is not relevant to the inter-relay channel.

Fig. 7 compares the training-based SK-PK capacity regions $C_{SP}^G$ and $C_{SP}^{G(c)}$ with respect to the non-collusive and collusive cases, respectively. Different values of the variance of the direct link ($\delta_{A,B}$) have been considered, and we set $T = 28$, $P = 20$, $\left(\delta_{A,1}, \delta_{A,2}, \delta_{B,1}, \delta_{B,2}, \delta_{T,1}, \delta_{T,2}, \delta_{A,B}\right) = (0.5, 1.1, 3.7, 2.1, 3.1)$. 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-binning 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 $R_S + R_P$, 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., $(1/n)I(K_P; X^n_i, F \leq \epsilon)$) and the secrecy constraint on relay $3-i$ is ignored. Moreover, assume Alice to be a genie-aided upper terminal which combines its own observation and the observation of relay $3-i$, so Alice observes $X^n_3 \triangleq (X^n_A, X^n_{3-i})$ now. This enhanced source model with alphabets $(X^n_A, X^n_{B, i})$ becomes a special case of the cooperative DMS model in [3]. According to Eq. (2.38) in [3], the private key capacity of this enhanced source model is $I(X^n_A, X^n_{B, i})$ with $X^n_A \triangleq (X_A, X_{3-i})$, which implies that the upper bound on the private key rate can be obtained as

$$R_P \leq I(X_A, X_{3-i}; X_B|X_i) = I(Y_{B,A}, Y_{1,A}, Y_{2,A}, Y_{B,3-i}, Y_{B,3-i}, Y_{3-i};$$

$$Y_{A,B}, Y_{1,B}, Y_{2,B}|Y_{A,i}, Y_{B,i}, Y_{3-i}) \leq I(Y_{B,A}, Y_{3,i-A}, Y_{A,3-i}, Y_{B,3-i}; Y_{A,B}, Y_{3-i,B})$$

$$= I_{A,B} + I_{B,3-i}. \tag{47}$$

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

$$R_P \leq I_{A,B} + \min_{i=1,2} \min \{I_{B,3-i}, I_{A,3-i}\} = I_{A,B} + I_{1, min}. \tag{48}$$

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 $\epsilon$-recoverable requirement in Definition 1 ensures the reliable requirement, which implies that

$$H(K_S, K_P|F, X^n_3) \leq \epsilon \log(|K_S| \times |K_P|) + 1 \triangleq n\delta_1, \tag{49}$$

$$H(K_S, K_P|F, X^n_3) \leq n\delta_1, \tag{50}$$

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

$$n(R_S + R_P - 2\delta) \leq H(K_S, K_P) = H(K_S, K_P|F) + I(K_S, K_P; F) \leq H(K_S, K_P|F) + n\epsilon$$

$$\leq H(K_S, K_P|F) - H(K_S, K_P|F, X^n_3) + n(\epsilon + \delta_1) \leq I(K_S, K_P, X^n_3; X^n_B|F) + n(\epsilon + \delta_1)$$

$$\leq I(X^n_3; X^n_B|F) + H(K_S, K_P|F, X^n_3) + n(\epsilon + \delta_1) \leq I(X^n_3; X^n_B|F) + n(\epsilon + 2\delta_1) \leq \min \{I(X^n_3; X^n_B; X^n_3; X^n_B; F), I(X^n_3; X^n_B; X^n_3; X^n_B; F) \} + n(\epsilon + 2\delta_1), \tag{51}$$

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 $\forall t \leq 4r$, $H(F_i|X^n_B, F^{t-1}) = 0$, $H(F_i|X^n_A, F^{t-1}) = 0$, $H(F_i|X^n_A, F^{t-1}) = 0$ when $t \mod 4 = 0, 3, 2, 1$, respectively. Therefore, if $t \mod 4 = 0,$

$$I(X^n_A, X^n_3, X^n_B; X^n_B|F^t) = H(X^n_A, X^n_3, X^n_B|F^t) - H(X^n_A, X^n_3, X^n_B|X^n_B, F^t)$$

$$= H(X^n_A, X^n_3, X^n_B|F^t) - H(X^n_A, X^n_3, X^n_B|X^n_B, F^{t-1}) \leq I(X^n_A, X^n_3, X^n_B; X^n_B|F^{t-1}). \tag{52}$$

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

$$I(X^n_A, X^n_3, X^n_B; X^n_B|F^t) = H(X^n_B|F^t) - H(X^n_A, X^n_3, X^n_B|X^n_B, F^t)$$

$$= H(X^n_B|F^t) - H(X^n_B|X^n_A, X^n_3, X^n_B, F^{t-1}) \leq I(X^n_A, X^n_3, X^n_B; X^n_B|F^{t-1}). \tag{53}$$

Repeating this procedure $4r$ times from $t = 4r$ to $t = 1,$

$$I(X^n_A, X^n_3, X^n_B; X^n_B|F) \leq I(X^n_A, X^n_3, X^n_B; X^n_B) \leq nI(X_A, X_3, X_B)$$

Hence the first term in the min-function in (51) can be upper bounded as

$$I(X^n_A, X^n_3, X^n_B; X^n_B|F) \leq nI(X_A, X_3, X_B) = n(I_{A,B} + I_{B,1} + I_{B,2}). \tag{54}$$

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

$$R_S + R_P \leq I_{A,B} + I_{1, min} + \epsilon + 2\delta_1 + 2\delta. \tag{55}$$

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 \( \epsilon \)-recoverable requirement in Definition 1 that ensures the reliable requirement, we have

\[
H(K_P|F, X^n_1) \leq \epsilon \log(|K_P|) + 1 = n\delta_1, \tag{56}
\]

\[
H(K_P|F, X^n_2) \leq n\delta_1, \tag{57}
\]

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

\[
n(R_P - \delta) \leq H(K_P) \\
= H(K_P|F, X^n_1, X^n_2) + I(K_P; F, X^n_1, X^n_2) \\
\leq H(K_P|F, X^n_1, X^n_2) + n\epsilon + 2\delta_1 \\
\leq nI(X^2_A; X^2_B|X^n_1, X^n_2) + n(\epsilon + 2\delta_1) \\
\leq nI(X^2_A; X^2_B|X^n_1, X^n_2) + n(\epsilon + 2\delta_1) \\
\leq nI(Y_A; Y_B) + n(\epsilon + 2\delta_1) \tag{58}
\]

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

\[
R_P \leq I(\hat{Y}_A; \hat{Y}_B) + \delta + \epsilon + 2\delta_1.
\]

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 \( H(W|W_1, W_{1,2}, K^1_P, C) \) will be upper bounded; \( H(W|W_2, W_{1,2}, K, P, C) \) can be calculated similarly. Firstly,

\[
H(W|W_1, W_{1,2}, K, P, C) = \sum_{w_1, w_{1,2}, k, p} p(w_1, w_{1,2}, k, p) H(W|w_1, w_{1,2}, k, p, C). \tag{59}
\]

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

\[
\mathbb{E}[N(w_1, w_{1,2}, k, p, C)] = 2^n R_S - R_1 - R_{1,2}, \\
\text{Var}[N(w_1, w_{1,2}, k, p, C)] = 2^n R_S - R_1 - R_{1,2}. \tag{60}
\]

Now, define an indicator variable as

\[
E_1 = \{1, \text{ if } N(w_1, w_{1,2}, k, p, C) \geq 2n[N(w_1, w_{1,2}, k, p, C)], \}
\]

\[
0, \text{ otherwise.} \tag{61}
\]

Then, by Chebyshev inequality

\[
P\{E_1 = 1\} \leq \frac{\text{Var}[N(w_1, w_{1,2}, k, p, C)]}{2^{n(R_S - R_1 - R_{1,2})}} \tag{62}
\]

which is arbitrarily small when \( n \) is sufficiently large. Now, denote \( R = R_{A,B} + R_1 + R_2 + R_{1,2} \), then

\[
H(W|w_1, w_{1,2}, k, p, C) \leq H(W, E_1|w_1, w_{1,2}, k, p, C) = H(E_1) + P(E_1 = 1)H(W|w_1, w_{1,2}, k, p, E_1 = 1, C) + P(E_1 = 0)H(W|w_1, w_{1,2}, k, p, E_1 = 0, C) \tag{63}
\]

\[
\leq 1 + \log |W| + H(W|w_1, w_{1,2}, k, p, E_1 = 0, C) \tag{64}
\]

\[
\leq 1 + nR \times 2^{-n(R_S - R_1 - R_{1,2})} + \log \left( \frac{2}{2^{n(R_S - R_1 - R_{1,2})}} \right) \tag{65}
\]

where (a) follows from the fact that \( H(E_1) \leq 1 \); (b) is due to (62); (c) is due to the fact that \( N(w_1, w_{1,2}, k, p, C) < 2^{n(R_S - R_1 - R_{1,2}) \text{ when } E_1 = 0} \). So

\[
H(W|w_1, w_{1,2}, k, p, C) \leq n(R_S - R_1 - R_{1,2} + \delta_n) \tag{66}
\]

where \( \delta_n = \frac{2}{n + R + 2^{-n(R_S - R_1 - R_{1,2})}} \), Since \( R_S > R_1 + R_{1,2} \) as shown in (29), \( \delta_n \to 0 \) as \( n \to \infty \). Recalling (59), \( H(W|W_1, W_{1,2}, K, P, C) \leq n(R_S - R_1 - R_{1,2} + \delta_n) \) has been proved.

REFERENCES

Zhiguo Ding (S’03–M’05) received his B.Eng 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 Jul. 2005 to Aug. 2014, he was working in Queen’s University Belfast, Imperial College and Newcastle University. Since Sept. 2014, he has been with Lancaster University as a Chair Professor.


Xuchu Dai received the B.Eng. degree in Electronic Engineering from China University of Posts and Telecommunications in 2009, and the Ph.D. degree in Electrical Engineering from the University of Science and Technology of China, Hefei, China. He is currently working as a postdoc at Lancaster University since August 2015. His current research interests include cooperative communications, information theory, information-theoretic secrecy, and 5G networks.
George K. Karagiannidis [M’96-SM’03-F’14] (geokaragauth.gr) was born in Pithagorion, Samos Island, Greece. He received the University Diploma (5 years) and PhD degree, both in electrical and computer engineering from the University of Patras, in 1987 and 1999, respectively. From 2000 to 2004, he was a Senior Researcher at the Institute for Space Applications and Remote Sensing, National Observatory of Athens, Greece. In June 2004, he joined the faculty of Aristotle University of Thessaloniki, Greece where he is currently Professor in the Electrical & Computer Engineering Dept. and Director of Digital Telecommunications Systems and Networks Laboratory.

His research interests are in the broad area of Digital Communications Systems with emphasis on Wireless Communications, Optical Wireless Communications, Wireless Power Transfer and Applications, Molecular Communications, Communications and Robotics and Wireless Security.


Dr. Karagiannidis has been involved as General Chair, Technical Program Chair and member of Technical Program Committees in several IEEE and non-IEEE conferences. In the past he was Editor in IEEE Transactions on Communications, Senior Editor of IEEE Communications Letters, 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 IEEE Communications Letters. He is a Honorary Professor at South West Jiaotong University, Chengdu, China. Dr. Karagiannidis has been selected as a 2015 Thomson Reuters Highly Cited Researcher.