On the Private Key Capacity of the M-Relay Pairwise Independent Network

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

***Abstract*—We study the problem of private key generation in a cooperative pairwise independent network (PIN), with $M+2$ terminals (Alice, Bob and M relays), $M \geq 2$. In the PIN, the correlated source observed by every pair of terminals, is independent of the sources observed by any other pairs of terminals. Moreover, all terminals can communicate with each other over a public channel, which is also observed by Eve, noiselessly. The objective is to generate a private key between Alice and Bob with the help of the M relays; such a private key needs to be protected not only from Eve but also from all relays. A single-letter expression for the *private key capacity* of this PIN model is obtained, where the achievability part is established by proposing a random binning (RB) based key generation algorithm, and the converse part is established by deriving upper bounds of M enhanced source models. Next, we consider a cooperative wireless network and use estimates of fading channels to generate private keys. It has been shown that the proposed RB key generation algorithm can achieve a multiplexing gain of $M-1$, which is an improvement compared with the existing XOR algorithm, whose achievable multiplexing gain is $\lfloor M/2 \rfloor$.**

***Index Terms*—Information-theoretic security, private key generation, private key capacity, PIN model, multiplexing gain**

I. Introduction

The generation of information-theoretically secure symmetric keys between a pair of legitimate users, has received considerable attention from an aspect of information-theoretic security [2]. The works in [3] and [4] first introduced the source model with public discussion to generate secret keys. In this two-terminal discrete memoryless source (DMS) model, the two terminals, namely Alice and Bob, observe a correlated source and can communicate with each other via a public channel, while the eavesdropper (Eve) can also access the public discussion noiselessly. Using a point-to-point distributed source coding technique [5], it has been shown that Alice and Bob can generate a secret key, by extracting common randomness from their correlated source observations. The work in [6] first investigated the multi-terminal DMS model, where a group of terminals, denoted as A, wish to share a common secret key with the help of the remaining terminals. The group key capacity was established based on the concept of "omniscience", i.e., the terminals publicly communicate using the minimum rate to enable each terminal in A to reconstruct near-losslessly all terminals's source observations. Based on omniscience, the secret key capacities of many other multi-terminal DMS models were also established, such as in [7]–[11].

The pairwise independent network (PIN), is actually a special case of the multi-terminal DMS model presented in [6]. In a PIN model, the correlated source observed by every pair of terminals is independent of the sources observed by any other pairs of terminals. A variety of PIN models has been investigated recently, such as in [7], [12]–[15]. Instead of the omniscience scheme, existing works in [7], [12]–[15] proposed more efficient graph-based key generation algorithms. The basic idea is to represent the PIN model by a multigraph and propagate secret keys over this multigraph using the one-time pad [2]. In general, the study of the PIN model is motivated by practical aspects of a wireless communication network. Based on the channel reciprocity in time-division duplex (TDD) systems, the correlated source observations in a PIN model can be obtained by estimating the wireless fading channels, associated with the legitimate terminals. This is because all wireless channels in a network are mutually independent, as long as the terminals are half-wavelength away from each other [16]. This physical layer (PHY) security approach has been recognized recently as a promising solution for generating secret keys (e.g., [17]–[23]).

Scanning the open literature on source models, cooperation from external helper nodes has been demonstrated to be effective, in improving generated key rates [6], [11], [13], [15], [21], [22], [24]. Motivated by this, the present work aims to investigate the private key[1] generation problem in a cooperative PIN model with $M+2$ terminals (Alice, Bob and M relays). With the help of the M relays, Alice and Bob wish to establish a private key, which should be protected not only from Eve but also from all relays. A practical example of this model is a government intelligence network, where it is assumed that not every terminal has the same level of access to the key information, despite operating with agreed protocols and serving as relay nodes in the network. The private key generation problem in the source model is analogous to secure

This paper was presented in part at IEEE International Symposium on Information Theory, HongKong, China in 2015 [1]. P. Xu and X. Dai are with Key Laboratory of Wireless-Optical Communications, Chinese Academy of Sciences, School of Information Science and Technology, University of Science and Technology of China. Address: No. 96 Jinzhai Road, Hefei, Anhui Province, 230026, P. R. China (e-mail: mxp484,daixc@ustc.edu.cn). Zhiguo Ding is with School of Computing and Communications, Lancaster University, LA1 4WA, UK (e-mail:z.ding@lancaster.ac.uk). G. K. Karagiannidis is with Department of Electrical & Computer Engineering, Aristotle University of Thessaloniki, Thessaloniki, Greece (e-mail: geokarag@auth.gr).

The work of P. Xu and X. Dai was supported in part by the National Natural Science Foundation of China under Grant 61471334, and in part by the China Post-Doctoral Science Foundation under Grant 2015M570544.

[1] When the generated secret key needs to be protected not only from Eve but also from unintended terminals (including the helper nodes), it is termed as a "private key" [6], [24], [25]. The private key obviously has a higher security level than a general secret key that is protected only from Eve.

transmission in the wiretap channel model[2] with an untrusted relay [28]–[30], where a transmitter wish to send a message to a receiver with the help of a relay but requires this message to be secret from the relay.

The main contribution in this paper is the development of a RB key generation algorithm, in order to achieve the derived outer bound, and thus the private key capacity of the considered model is established. To prove the achievability of the private key capacity, a algorithm is proposed for generating the private key. Specifically, using the point-to-point pairwise key generation technique [3], [4] and the one-time pad [2], Alice and Bob first agree on M common messages, where each of them is open to a certain relay. Then, a random binning (RB) process is adopted in the key distillation step, in order to map these insecure common messages into the private key. Such an algorithm is termed for simplicity as the *RB algorithm*. Compared to the concept of omniscience [6]–[11], the proposed scheme only requires Alice (Bob) to reconstruct the pairwise key between each relay and Bob (Alice) rather than their source observations. Furthermore, in order to prove the converse, the upper bound of the private key capacity is obtained by considering M enhanced source models, where each of them relaxes the secrecy constraints on some relays, and assumes that part of the relay observations are known by Alice or Bob. The result shows that such an upper bound is tight and matches well with the achievable key rate.

We then consider the key generation problem in the cooperative wireless relay network, where it is assumed that a direct link between Alice and Bob does not exist, due to deep fading. The RB algorithm, proposed for the PIN model, is applied to this wireless network, using estimates of the random channels associated with the relays. Compared to the XOR algorithm in [21], that achieves a multiplexing gain, $\lfloor M/2 \rfloor$, for the considered wireless network, the proposed RB algorithm achieves a multiplexing gain, equal to $M-1$. This is because the proposed approach pays less price for satisfying the secrecy constraints at the relays, by using the RB process to simultaneously confuse all relays. Moreover, the developed principles used to establish the private key capacity are extended to several more general models, i.e., the PIN models with direct link between Alice and Bob, with secrecy constraint on only part of relays, with colluding relays, and with multiple terminals wishing to share a group key.

Note that the RB scheme has been widely used for generating an information-theoretically secure key (e.g., [11], [19], [25], [31]–[33]), whose basic idea is to map the generated common randomness between the legitimate terminals into a random and secret key. However, the works in [19], [25], [31], [32] consider key generation problems without any helper node. In contrast, this work is to investigate the cooperative key generation problem with the help of relay nodes. The works in [11], [33] investigate the problem of generating multiple keys with the help of a single relay node, whereas this paper addresses a more general scenario with multiple relay nodes. Particularly for the case with multiple non-colluding relays, the feature that each relay does not have access to the other relays' sources enables the legitimate terminals to utilize these untrusted relays for private key generation. To the best of the authors' knowledge, this is the first work in the open literature which uses the RB scheme to the considered multiple-relay source model for private key generation.

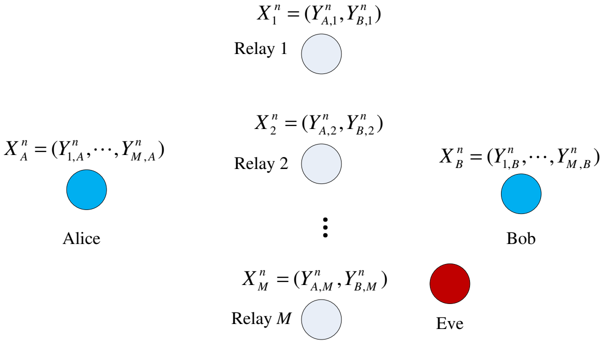

$X_1^n = (Y_{A,1}^n, Y_{B,1}^n)$
Relay 1
$X_2^n = (Y_{A,2}^n, Y_{B,2}^n)$
Relay 2
$X_A^n = (Y_{1,A}^n, \cdots, Y_{M,A}^n)$
Alice
$X_B^n = (Y_{1,B}^n, \cdots, Y_{M,B}^n)$
Bob
$X_M^n = (Y_{A,M}^n, Y_{B,M}^n)$
Relay M
Eve

Fig. 1. The source observations of the considered M-relay PIN model, where Alice and Bob wish to agree on a private key with the help of M relays.

The rest of this paper is organized as follows. Section II, introduces the definition of considered PIN model. Section III, presents the private key capacity, and provides the proof steps for establishing the key capacity. Then, in Section IV, the proposed RB algorithm is extended to a cooperative wireless network. In Section V, several more general PIN models are considered. Concluding remarks are provided in Section VI.

Throughout the paper, we denote a random variable (RV) with an upper case letter (e.g. X), its finite alphabet with a calligraphic letter (e.g., $\mathcal{X}$), and its realization with lower case letter (e.g., x). The probability mass function (pmf) of X is denoted as $p(x)$. Moreover, $\mathbb{E}(X)$ is the expectation of X, and $|\mathcal{X}|$ is the size of $\mathcal{X}$. Finally, X^n denotes a n-vector $\{X_1, \cdots, X_n\}$, whose i-th element is X_i.

II. A Pairwise Independent Network

Consider a cooperative DMS model with $M+2$ terminals (Alice, Bob and M relays, $M \geq 2$) and a passive eavesdropper (Eve). With the help of the relays, Alice and Bob wish to establish a private key that needs to be protected not only from Eve but also from all relays. These relays are assumed to be curious but honest, i.e., they comply with the proposed transmission schemes for helping Alice and Bob to generate a key, but would also try to intercept the key information if possible [21]. The terminals can communicate to each other over a public channel with infinite capacity, but the transmitted information over the public channel is also available to Eve noiselessly.

For $m \in \{1, \cdots, M\}$, let $Y_{m,A}$ and $Y_{A,m}$ denote the correlated source observations at Alice and relay m, respectively, where $Y_{m,B}$ and $Y_{B,m}$ are the correlated source observations at Bob and relay m, respectively. Specifically, Alice observes n independent and identically distributed (i.i.d.) repetitions of the RV $X_A \triangleq (Y_{1,A}, \cdots, Y_{M,A})$, denoted as $X_A^n \triangleq (Y_{1,A}^n, \cdots, Y_{M,A}^n)$; Bob observes n i.i.d. repetitions of the RV $X_B \triangleq (Y_{1,B}, \cdots, Y_{M,B})$, denoted by $X_B^n \triangleq$

[2] The wiretap channel was first studied by Wyner in [26], and generalized by Csizár and Körner in [27]. Since public communication was not allowed in this model, secret key generation was tantamount to secure transmission over the noisy channel.

$(Y^n_{1,B}, \cdots, Y^n_{M,B})$; relay m observes n i.i.d. repetitions of the RV $X_m = (Y_{A,m}, Y_{B,m})$, denoted by $X^n_m = (Y^n_{A,m}, Y^n_{B,m})$. This multi-terminal DMS model belongs to a PIN in the sense that [12]

$$I(Y_{i,\alpha}, Y_{\alpha,i}; \{Y_{j,\beta}, Y_{\beta,j} : (j,\beta) \neq (i,\alpha)\}) = 0, \quad \text{for } i,j \in \{1,\cdots,M\}; \alpha,\beta \in \{A,B\}. \tag{1}$$

This implies that each source accessible to a pair of terminals (e.g., the source $(Y_{m,A}, Y_{A,m})$ accessible to Alice and relay m) is independent of all the other sources. This model does not include the correlated sources, observed by the pair of Alice and Bob, nor any pair of the relays.

Remark 1: The considered relay network in Fig. 1 is analogous to the so-called "diamond" relay network [34]–[38]. However, these existing works investigated the diamond relay network from reliability perspective [34], [35] or security perspective for channel models [36]–[38], which are fundamentally different from this work.

More definitions in this PIN model are given below:

- Without loss of generality, assume that the terminals use the public channel to communicate in a round robin fashion over q rounds. Let $1 \leq l \leq q$, and $1 \leq m \leq M$. Specifically, relay m transmits during rounds l satisfying

  $$l \mod (M+2) = m; \tag{2}$$

  Alice transmits during rounds l satisfying

  $$l \mod (M+2) = M+1; \tag{3}$$

  and Bob transmits during rounds l satisfying

  $$l \mod (M+2) = 0. \tag{4}$$

- A $(2^{n\tilde{R}_1}, \cdots, 2^{n\tilde{R}_q})$ code for key generation consists of :

  (i) $M+2$ randomized encoders, one for each terminal. In rounds l satisfying (2), relay m generates an index $F_l \in \{1,\cdots,2^{n\tilde{R}_l}\}$ according to $p(f_l|x^n_m, f^{l-1})$; in rounds l satisfying (3), Alice generates an index $F_l \in \{1,\cdots,2^{n\tilde{R}_l}\}$ according to $p(f_l|x^n_A, f^{l-1})$; finally, in rounds l satisfying (4), Bob generates an index $F_l \in \{1,\cdots,2^{n\tilde{R}_l}\}$ according to $p(f_l|x^n_B, f^{l-1})$.

  (ii) Two decoders, for Alice (decoder A) and Bob (decoder B), respectively. After receiving the q rounds of transmissions (i.e., $F^q = \{F_1,\cdots,F_q\}$) over the public channel, decoder A generates a random key K_A, according to $K_A = K_A(X^n_A, F^q)$, and Decoder B generates a random key K_B, according to $K_B = K_B(X^n_B, F^q)$.

- A private key rate R is said to be achievable, if there exists a $(2^{n\tilde{R}_1}, \cdots, 2^{n\tilde{R}_q})$ code such that

  $$Pr(K_A \neq K_B) \leq \epsilon, \tag{5}$$

  $$\frac{1}{n}H(K_A) \geq R - \epsilon, \tag{6}$$

  $$\frac{1}{n}H(K_A) \geq \frac{1}{n}\log_2|\mathcal{K}_A| - \epsilon, \tag{7}$$

  $$\frac{1}{n}I(K_A; X^n_m, F^q) \leq \epsilon, \text{ for } \forall m \in \{1,\cdots,M\}, \tag{8}$$

  where $|\mathcal{K}_A|$ denotes the size of the alphabet of key K_A. Note that, following the definitions in [3], [19]–[24], the constraint on K_B is redundant. Since K_A and K_B are the same with a high probability (shown in (5)), K_B can also satisfy (6)-(8), and the individual secrecy constraint on K_A can guarantee the joint secrecy constraint on K_A and K_B.

  Remark 2: Different from the original definition of the private key in [6] with respect to the fully colluding relays, this paper mainly considers the case that all relay nodes are non-colluding as shown in (8). The case with colluding relays nodes will be considered later in Section V-C.

- The private key capacity C_K is the supremum of all achievable rates R. Next, $C_K^{(D)}$ is used to denote the private key capacity with deterministic encoding and key generation functions. In Section III-B, we will show that $C_K^{(D)} = C_K$, which means that randomization is useless for key generation in the addressed source model.

III. Private Key Capacity of the PIN Model

For simplicity, we first define

$$I_i \triangleq \min\{I(Y_{i,A}; Y_{A,i}), I(Y_{i,B}; Y_{B,i})\}, \forall i \in \{1,\cdots,M\}. \tag{9}$$

Furthermore, these parameters are ordered as $I_{(1)} \leq I_{(2)} \leq \cdots \leq I_{(M)}$.

Theorem *1:* For the considered PIN model with M relays, the private key capacity is given by

$$C_K \triangleq \sum_{i=1}^{M} I_i - \max_{m\in\{1,\cdots,M\}} I_m = \sum_{i=1}^{M-1} I_{(i)}. \tag{10}$$

Proof: To prove the achievability, a key generation algorithm is proposed based on two steps: key agreement and key distillation. In the key agreement step, based on the point-to-point key generation technique [3], [4] and the one-time pad [2], Alice and Bob agree on M common messages with the help of the relays. In the key distillation step, both Alice and Bob map all common messages into the unique codeword in the pre-constructed private-key codebook, and set the bin number of this codeword as the final private key. Note that such a private-key codebook is generated based on the RB scheme, so it provides necessary randomness, such that the bin number is secret from all relays and Eve.

To prove the converse, M symmetric enhanced source models will be constructed. In each enhanced model, the secrecy constraint on the relays is relaxed, and Alice or Bob is assumed to have the *a priori* knowledge of the observations of part of relays.

The details of the proof will be provided in the following two subsections. ■

Example 1: Let the source observation pair $(Y_{A,i}, Y_{i,A})$ or $(Y_{B,i}, Y_{i,B})$ be RVs, each uniformly distributed on $\{0,1\}$. Furthermore, suppose that

$$p(y_{\alpha,i}, y_{i,\alpha}) = \frac{1-q_\alpha}{2}\mu(y_{\alpha,i}, y_{i,\alpha}) + \frac{q_\alpha}{2}(1-\mu(y_{\alpha,i}, y_{i,\alpha})), \tag{11}$$

$\forall \alpha \in \{A,B\}, \forall i \in \{1,\cdots,M\}$, where $0 < q_A, q_B < 1/2$ and $\mu(x,y) = \begin{cases} 0, & \text{if } x \neq y, \\ 1, & \text{if } x = y, \end{cases}$. Straightforward analysis gives

Algorithm 1: Proposed RB Algorithm for PIN model

Step 1: Key Agreement:

- Alice and Relay i agree on a pairwise key $W_{A,i}$ from the correlated observations $(Y_{i,A}^n, Y_{A,i}^n)$, $i = 1, \cdots M$.
- Bob and Relay i agree on a pairwise key $W_{B,i}$ from the correlated observations $(Y_{i,B}^n, Y_{B,i}^n)$, $i = 1, \cdots M$.
- Relay i sends $W_{A,i} \oplus W_{B,i}$ over the public channel, so Alice and Bob can obtain both $W_{A,i}$ and $W_{B,i}$, $i = 1, \cdots M$. Then they will choose the one with a smaller size as the common message, denoted as $W_i \in \mathcal{W}_i$.

Step 2: Key Distillation:

- In advance, randomly partition all sequences w^M in $\mathcal{W}^M \triangleq \mathcal{W}_1 \times \mathcal{W}_2 \times \cdots \times \mathcal{W}_M$ into $2^{n(R_{key}-\epsilon)}$ bins each with an equal amount of codewords. All terminals (including Eve) know this private-key codebook.
- Alice and Bob find the sequence $W^M = (W_1, \cdots, W_M)$ in the RB based private-key codebook, and choose its bin number as the final private key.

$I(Y_{\alpha,i}; Y_{i,\alpha}) = 1 - h(q_\alpha)$, where

$$h(x) = -x \log_2 x - (1-x)\log_2(1-x)$$

that is the binary entropy function, with $0 < x < 1/2$. Obviously, $h(x)$ is monotonically increasing in x, when $0 < x < 1/2$. Then, according to Theorem 1, the private key capacity is

$$C_K = (M-1)\min\{1 - h(q_A), 1 - h(q_B)\}.$$

Another more complicated example with respect to the wireless network will be illustrated in Section IV.

A. Proof of Achievability of Theorem 1

Algorithm 1 briefly shows the achievable scheme that is based on two steps: key agreement and key distillation. Let

$$R_{A,i} \triangleq I(Y_{A,i}; Y_{i,A}) - \epsilon,\ R_{B,i} \triangleq I(Y_{B,i}; Y_{i,B}) - \epsilon, \quad (12)$$

$$R_i \triangleq \min\{R_{A,i}, R_{B,i}\} = I_i - \epsilon,\ \text{for } 1 \le i \le M. \quad (13)$$

Moreover, $R_1, \cdots, R_M$ are ordered according to $R_{(1)} \le \cdots \le R_{(M)}$, and $R_{key} \triangleq \sum_{i=1}^{M-1} R_{(i)}$.

1) Key Agreement: In the key agreement step, Alice and Bob agree on M common messages.

First, based on the standard point-to-point techniques [3], [4], each relay i and Alice agree on a pairwise key using their correlated sources $(Y_{A,i}^n, Y_{i,A}^n)$. Briefly speaking, relay i chooses a pairwise key $W_{A,i}$ from $\mathcal{W}_{A,i} \triangleq \{1, \cdots, 2^{nR_{A,i}}\}$, and then sends a public message $F_{A,i}$ such that Alice can estimate this pairwise key as $W_{i,A}$. Similarly, relay i chooses a pairwise key $W_{B,i}$ from $\mathcal{W}_{B,i} \triangleq \{1, \cdots, 2^{nR_{B,i}}\}$, and sends $F_{B,i}$ such that Bob can estimate this pairwise key as $W_{i,B}$. More details of such a pairwise key agreement have been provided in [3], [4]. For $\forall \epsilon_0, \epsilon_1, \epsilon_2 > 0$, the pairwise keys $W_{A,i}$ and $W_{B,i}$ have the following properties [12], [13], [21]:

(i) $W_{\alpha,i}$ and $W_{\alpha,i}$ are the same with a high probability, i.e.,

$$Pr(W_{\alpha,i} \ne W_{i,\alpha}) \le \epsilon_0,\ \forall \alpha \in \{A, B\}, i \in \{1, \cdots, M\}. \quad (14)$$

(ii) Negligible information will be leaked to the public transmissions, i.e.,

$$\frac{1}{n} I(W_{\alpha,i}; F_{\alpha,i}) \le \epsilon_1,\ \forall \alpha \in \{A, B\}, i \in \{1, \cdots, M\}. \quad (15)$$

(iii) They are nearly uniformly distributed, i.e.,

$$\frac{1}{n} H(W_{\alpha,i}) \ge \frac{1}{n}\log_2(|\mathcal{W}_{\alpha,i}|) - \epsilon_2 = R_{\alpha,i} - \epsilon_2, \\ \forall \alpha \in \{A, B\}, i \in \{1, \cdots, M\}. \quad (16)$$

(iv) The tuples $\{(W_{\alpha,i}, F_{\alpha,i}, Y_{\alpha,i}^n, Y_{i,\alpha}^n)\}_{\alpha \in \{A,B\}, i \in \{1,\cdots,M\}}$ are mutually independent, due to the definitions of the PIN model shown in (1).

Remark 3: For the sake of brevity in the following discussion, instead of using both $W_{A,i}$ and $W_{i,A}$ ($W_{B,i}$ and $W_{i,B}$) to denote the value of the pairwise key between relay i and Alice (Bob), we will use $W_{A,i}$ ($W_{B,i}$) to denote both keys with the understanding that there is a small probability that $W_{A,i} \ne W_{i,A}$ ($W_{B,i} \ne W_{i,B}$) as shown in property (i).

Second, each relay i sends $W_{A,i} \oplus W_{B,i}$ over the public channel to help Alice and Bob to decode both the two pairwise keys. Then, they choose the one with a smaller size as the common message, denoted as W_i, i.e., $W_i = W_{A,i}$ if $R_{A,i} \le R_{B,i}$; $W_i = W_{B,i}$, otherwise. This implies that the alphabet of W_i is $\mathcal{W}_i = \{1, \cdots, 2^{nR_i}\}$. Assuming, without loss of generality, $W_i = W_{A,i}$, i.e., $R_{A,i} \le R_{B,i}$, then these common messages can be proved to be secret from the public discussion. Specifically, denote the overall public discussion sequence as $\mathbf{F} \triangleq (F_{A,i}, F_{B,i}, W_{A,i} \oplus W_{B,i})_{i \in \{1,\cdots,M\}}$, then

$$\begin{aligned} &\frac{1}{n} I(W_1, \cdots, W_M; \mathbf{F}) \\ &\overset{(a)}{=} \frac{1}{n}\sum_{i=1}^{M} I(W_i; F_{A,i}, F_{B,i}, W_{A,i} \oplus W_{B,i}) \\ &= \frac{1}{n}\sum_{i=1}^{M} I(W_{A,i}; F_{A,i}) \\ &\overset{(b)}{\le} M\epsilon_1, \end{aligned} \quad (17)$$

where (a) follows from property (iv) of the generated pairwise keys, as mentioned above, and the fact the W_i is determined by $W_{A,i}$ and $W_{B,i}$; (b) follows from the first property of the generated pairwise keys, as mentioned above. The security constraint for the case where $W_i = W_{B,i}$ can be proved symmetrically.

Now, a proposition is given as follows, which will be used later in the next step.

Proposition 1: These RVs, $W_{]m[}, \mathbf{F}, X_m^n, W_m$, form a Markov chain: $W_{]m[} - \mathbf{F} - (X_m^n, W_m)$, where $W_{]m[} \triangleq \{W_i\}_{i \in \{1,\cdots,M\}, i \ne m}$.

Proof: Specifically, the conditional pmf, $p\left(w_{]m[}|\mathbf{f}, x_m^n, w_m\right)$, can be expressed as

$$\begin{aligned} & p\left(w_{]m[}|\mathbf{f}, x_m^n, w_m\right) \\ & \overset{(a)}{=} \sum_{x_{]m[}^n} p\left(x_{]m[}^n|\mathbf{f}, x_m^n, w_m\right) p\left(w_{]m[}|\mathbf{f}, x_m^n, w_m, x_{]m[}^n\right) \\ & \overset{(b)}{=} \sum_{x_{]m[}^n} p\left(x_{]m[}^n|\mathbf{f}_{]m[}\right) p\left(w_{]m[}|\mathbf{f}, x_m^n, w_m, x_{]m[}^n\right) \\ & \overset{(c)}{=} \sum_{x_{]m[}^n} p\left(x_{]m[}^n|\mathbf{f}\right) p\left(w_{]m[}|\mathbf{f}, x_m^n, w_m, x_{]m[}^n\right) \\ & \overset{(d)}{=} \sum_{x_{]m[}^n} p\left(x_{]m[}^n|\mathbf{f}\right) p\left(w_{]m[}|\mathbf{f}, x_{]m[}^n\right) \\ & = p\left(w_{]m[}|\mathbf{f}\right), \end{aligned} \tag{18}$$

where (a) follows from the definition that $X_{]m[}^n \triangleq \{X_i^n\}_{i\in\{1,\cdots,M\}, i\neq m}$, and its pmf is $p\left(x_{]m[}^n\right)$; (b) and (c) hold since $(X_m^n, W_m, F_{A,m}, F_{B,m}, W_{A,m} \oplus W_{B,m})$ are independent of $\left(X_{]m[}^n, \mathbf{F}_{]m[}\right)$, where $\mathbf{F}_{]m[} \triangleq \{(F_{A,i}, F_{B,i}, W_{A,i} \oplus W_{B,i})\}_{i\in\{1,\cdots,M\}, i\neq m}$; and (d) follows from the fact that $W_{]m[}$ is determined by $\left(\mathbf{F}, X_{]m[}^n\right)$, i.e., $W_{A,i}$ and $W_{B,i}$ are determined by $(\mathbf{F}, X_i^n)$ in the pairwise key generation. ■

2) Key Distillation: In the key distillation step, both Alice and Bob map these insecure common randomness (i.e., the common messages $(W_1, \cdots, W_M)$) assembled from the key agreement step into the unique codeword in the private-key codebook, and set the bin number of this codeword as the final private key. We will provide more details of the RB-based codebook in the following.

Codebook Generation: In advance, randomly and uniformly partition all sequences w^M in the set $\mathcal{W}^M \triangleq \mathcal{W}_1 \times \mathcal{W}_2 \times \cdots \times \mathcal{W}_M$ into $2^{n(R_{key}-\epsilon)}$ bins each with $2^{n(R_{(M)}+\epsilon)}$ codewords, where $w^M = (w_1, \cdots, w_M)$ and $w_i \in \mathcal{W}_i = \{1, \cdots, 2^{nR_i}\}$. So each codeword w^M can be indexed as $w^M(k, \tilde{k})$, where $k \in \{1, \cdots, 2^{n(R_{key}-\epsilon)}\}$, $\tilde{k} \in \{1, \cdots, 2^{n(R_{(M)}+\epsilon)}\}$. Fig. 2 illustrates the binning assignment (i.e., private-key codebook), denoted by $\mathcal{C}$, that is known by all terminals (including Eve). $\mathcal{C}$ can be viewed as a RV, where the randomness is introduced by the random bin assignment.

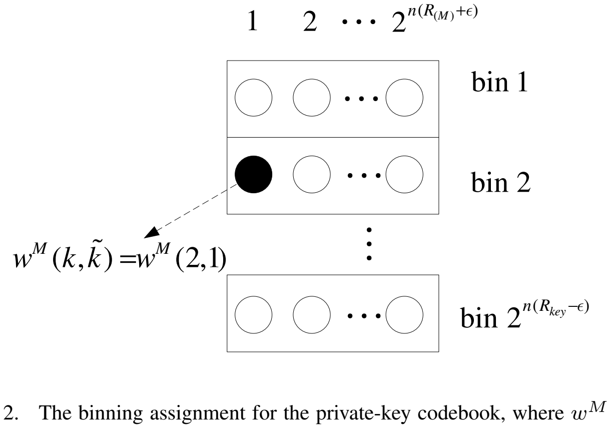

1
2
⋯
$2^{n(R_{(M)}+\epsilon)}$
bin 1
bin 2
$w^M(k,\tilde{k})=w^M(2,1)$
bin $2^{n(R_{key}-\epsilon)}$

Fig. 2. The binning assignment for the private-key codebook, where $w^M = (w_1, \cdots, w_M) \in \mathcal{W}^M$, $w_i \in \{1, \cdots, 2^{nR_i}\}$.

Decoding and key generation: Based on the M common messages obtained in the key agreement step, Alice and Bob can find their corresponding indices in the private-key codebook. Specifically, knowing $(W_1, \cdots, W_M)$, Alice finds the index pair $(k, \tilde{k})$ from the private-key codebook such that $w^M(k, \tilde{k}) = (W_1, \cdots, W_M)$. Then, it sets its key as $K_A = k$. Similarly, Bob can also find its key as $K_B = k$.

From the decoding process, $K_A \neq K_B$ if and only if the values of the common message sequence $(W_1, \cdots, W_M)$ estimated by Alice and Bob are different. In addition, according to the key agreement step, the values of the common message sequence estimated by Alice and Bob are different if and only if $W_{i,\alpha} \neq W_{\alpha,i}$ for some $\alpha \in \{A, B\}$, $i \in \{1, \cdots, M\}$. Thus, the probability that $K_A \neq K_B$ can be expressed as

$$\begin{aligned} Pr(K_A \neq K_B) &= Pr\left(\bigcup_{\alpha\in\{A,B\}, i\in\{1,\cdots,M\}} \{W_{i,\alpha} \neq W_{\alpha,i}\}\right) \\ &= 1 - Pr\left(\bigcap_{\alpha\in\{A,B\}, i\in\{1,\cdots,M\}} \{W_{i,\alpha} = W_{\alpha,i}\}\right) \\ &= 1 - \prod_{\alpha\in\{A,B\}, i\in\{1,\cdots,M\}} Pr\left(\{W_{i,\alpha} = W_{\alpha,i}\}\right) \\ &\overset{(a)}{\leq} 1 - (1-\epsilon_0)^{2M} \triangleq \delta_1(\epsilon_0) \end{aligned} \tag{19}$$

where (a) is due to (14). Obviously, $\delta_1(\epsilon_0) \to 0$ as $\epsilon_0 \to 0$.

Analysis of the key rate: Since the private-key codebook generation is based on the random binning assignment, averaged over the codebook (i.e., $\mathcal{C}$), K_A is uniformly distributed on $\{1, \cdots, 2^{n(R_{key}-\epsilon)}\}$. Therefore, it can be obviously obtained that $H(K_A|\mathcal{C}) = n(R_{key} - \epsilon)$.

Analysis of the secrecy constraints: For $m \in \{1, \cdots, M\}$, we will prove that the generated private key is secret from relay m. Fist, consider the following proposition of a Markov relationship.

Proposition 2: These RVs, $K_A, W_m, \mathbf{F}, \mathcal{C}, X_m^n$, form a Markov chain: $K_A - (W_m, \mathbf{F}, \mathcal{C}) - X_m^n$.

Proof: Define $W^M \triangleq (W_1, \cdots, W_M)$. The conditional pmf, $p\left(k_A|w_m, \mathbf{f}, c, x_m^n\right)$, can be expressed as

$$\begin{aligned} & p\left(k_A|w_m, \mathbf{f}, c, x_m^n\right) \\ & \overset{(a)}{=} \sum_{w_{]m[}} p\left(w_{]m[}|w_m, \mathbf{f}, c, x_m^n\right) p\left(k_A|w^M, \mathbf{f}, c, x_m^n\right) \\ & \overset{(b)}{=} \sum_{w_{]m[}} p\left(w_{]m[}|\mathbf{f}, c\right) p\left(k_A|w^M, \mathbf{f}, c, x_m^n\right) \\ & \overset{(c)}{=} \sum_{w_{]m[}} p\left(w_{]m[}|\mathbf{f}, c\right) p\left(k_A|w^M, \mathbf{f}, c\right) \\ & = p(k_A|w_m, c, \mathbf{f}), \end{aligned} \tag{20}$$

where (a) follows by the definition of $w_{]m[}$ in Proposition 1, i.e., $w_{]m[} = \{w_1, \cdots, w_{m-1}, w_{m+1}, \cdots, w_M\}$, and the fact that $w^M = (w_{]m[}, w_m)$; (b) is based on the Markov chain in Proposition 1 and the fact that random codebook $\mathcal{C}$ is independent of $(W^M, \mathbf{F}, X_m^n)$; and (c) is due to the fact that K_A is determined by $(W^M, \mathcal{C})$ as shown in the key generation process. ■

Then, averaged over $\mathcal{C}$, we have

$$\begin{aligned}
I(K_A;\mathbf{F},X_m^n|\mathcal{C}) &\le I(K_A;\mathbf{F},W_m,X_m^n|\mathcal{C})\\
&\overset{(a)}{=} I(K_A;\mathbf{F},W_m|\mathcal{C})\\
&\le I(K_A;W_m|\mathcal{C}) + I(K_A,W^M;\mathbf{F}|W_m,\mathcal{C})\\
&\overset{(b)}{=} I(K_A;W_m|\mathcal{C}) + I(W^M;\mathbf{F}|W_m)\\
&\overset{(c)}{\le} I(K_A;W_m|\mathcal{C}) + nM\epsilon_1\\
&= I(K_A;W_m|\mathcal{C}) + nM\epsilon_1. \qquad (21)
\end{aligned}$$

where (a) is based on Proposition 2; (b) holds since K_A is determined by W^M for a given codebook, and $\mathcal{C}$ is independent of $(W^M;\mathbf{F})$; (c) is due to (17) and the relationship:

$$I(W^M;\mathbf{F}|W_m) \le I(W^M,W_m;\mathbf{F}) = I(W^M;\mathbf{F}).$$

Furthermore,

$$\begin{aligned}
I(K_A;W_m|\mathcal{C}) &= I(K_A,W^M;W_m|\mathcal{C}) - I(W^M;W_m|K_A,\mathcal{C})\\
&= I(W^M;W_m|\mathcal{C}) - H(W^M|K_A,\mathcal{C})\\
&\qquad + H(W^M|W_m,K_A,\mathcal{C})\\
&= H(W_m|\mathcal{C}) - H(W^M|K_A,\mathcal{C})\\
&\qquad + H(W^M|W_m,K_A,\mathcal{C}). \qquad (22)
\end{aligned}$$

Since W_m is independent of $\mathcal{C}$, obviously the first term can be upper bounded as

$$H(W_m|\mathcal{C}) = H(W_m) \le \log(\mathcal{W}_m) = nR_m. \qquad (23)$$

From (16), we have $H(W_i) \ge n(R_i - \epsilon_2)$, and hence $H(W^M) \ge n\sum_{i=1}^{M}(R_{(i)} - \epsilon_2)$. Thus, the second term can be lower bounded as

$$\begin{aligned}
H(W^M|K_A,\mathcal{C}) &= H(W^M|\mathcal{C}) + H(K_A|W^M,\mathcal{C}) - H(K_A|\mathcal{C})\\
&= H(W^M|\mathcal{C}) - H(K_A|\mathcal{C})\\
&= H(W^M) - n(R_{key} - \epsilon)\\
&\ge n\sum_{i=1}^{M}(R_{(i)} - \epsilon_2) - n(R_{key} - \epsilon)\\
&= n(R_{(M)} + \epsilon - M\epsilon_2). \qquad (24)
\end{aligned}$$

The third term is bounded using the following lemma.

Lemma 1: When $R_{(M)} = \max\{R_1,\cdots,R_M\}$ and n is sufficiently large, then

$$H(W^M|W_m,K_A,\mathcal{C}) \le n(R_{(M)} - R_m + \delta_2(\epsilon)). \qquad (25)$$

Proof: This lemma can be proved following a similar approach with existing relevant works, such as [39] (proof of Lemma 22.3) and [25], with some necessary variations. The details are provided in Appendix A. ■

Combining (22) with (23), (24) and (25), we have

$$\frac{1}{n}I(K_A;W_m|\mathcal{C}) \le \delta_2(\epsilon) + M\epsilon_2 - \epsilon. \qquad (26)$$

Then, return to (21),

$$\frac{1}{n}I(K_A;\mathbf{F},X_m^n|\mathcal{C}) \le \delta_2(\epsilon) + M(\epsilon_1 + \epsilon_2) - \epsilon. \qquad (27)$$

So the key rate

$$R_{key} = \sum_{i=1}^{M-1} R_{(i)} = \sum_{i=1}^{M-1} I_{(i)} - (M-1)\epsilon$$

is achievable.

B. Proof of Converse of Theorem 1

The basic idea of the calculation of the upper bound is based on M symmetric enhanced channels. For the m-th enhanced source model, $m = 1,\cdots,M$, we only consider the secrecy constraint on relay m, and ignore the secrecy constraints on the other relays. Moreover, Alice and Bob are assumed to know the observations of two subsets of relays a priori, respectively. The definitions of the two subsets are given in the following.

For a given $m \in \{1,\cdots,M\}$, we form two sets of terminals $\mathcal{A}_{]m[}$ and $\mathcal{B}_{]m[}$ as follows. First, allocate Alice and Bob to $\mathcal{A}_{]m[}$ and $\mathcal{B}_{]m[}$, respectively. Second, for relay i, $i \neq m$, if $I(Y_{A,i};Y_{i,A}) > I(Y_{B,i};Y_{i,B})$, allocate it to $\mathcal{A}_{]m[}$; otherwise, allocate it to $\mathcal{B}_{]m[}$. Thus, if relay i lies in $\mathcal{A}_{]m[}$,

$$I(Y_{B,i};Y_{i,B}) = \min\{I(Y_{A,i};Y_{i,A}), I(Y_{B,i};Y_{i,B})\}; \qquad (28)$$

if the relay i lies in $\mathcal{B}_{]m[}$,

$$I(Y_{A,i};Y_{i,A}) = \min\{I(Y_{A,i};Y_{i,A}), I(Y_{B,i};Y_{i,B})\}. \qquad (29)$$

Then, assume, without loss of generality, that relays A_1, A_2, $\cdots$, A_j are allocated to $\mathcal{A}_{]m[}$, and relays B_1, B_2, $\cdots$, B_{M-1-j} are allocated to $\mathcal{B}_{]m[}$, $0 \le j \le M-1$[3]. In this case,

$$\begin{aligned}
&\{A_1,\cdots,A_j\}\bigcap\{B_1,\cdots,B_{M-1-j}\} = \emptyset,\\
&\text{and } \{A_1,\cdots,A_j\}\bigcup\{B_1,\cdots,B_{M-1-j}\}\\
&\qquad\qquad = \{1,\cdots,m-1,m+1,\cdots,M\}.
\end{aligned}$$

Thus, $\mathcal{A}_{]m[}$ = {Alice, relays A_1, $\cdots$, A_j}; $\mathcal{B}_{]m[}$ ={Bob, relays B_1, $\cdots$, B_{M-1-j}}.

Define $\mathbf{X}_{\mathcal{A},]m[} \triangleq (X_A^n, X_{A_1}^n,\cdots,X_{A_j}^n)$ and $\mathbf{X}_{\mathcal{B},]m[} \triangleq (X_B^n, X_{B_1}^n,\cdots,X_{B_{M-1-j}}^n)$, which are the observations of all terminals in sets $\mathcal{A}_{]m[}$ and $\mathcal{B}_{]m[}$, respectively. Then $C_K^{(D)}$ can be upper bounded as:

$$\begin{aligned}
&n(C_K^{(D)} - \epsilon) \overset{(a)}{\le} H(K_A)\\
&= I(K_A;X_m^n,F^q) + H(K_A|X_m^n,F^q)\\
&\overset{(b)}{\le} H(K_A|X_m^n,F^q) + n\epsilon_1\\
&\overset{(c)}{\le} H(K_A|X_m^n,F^q) - H(K_A|K_B) + n(\epsilon_1+\epsilon_2)\\
&\le H(K_A|X_m^n,F^q) - H(K_A|K_B,\mathbf{X}_{\mathcal{B},]m[},X_m^n,F^q)\\
&\qquad\qquad\qquad + n(\epsilon_1+\epsilon_2) \qquad (30)\\
&\overset{(d)}{=} I(K_A;\mathbf{X}_{\mathcal{B},]m[}|X_m^n,F^q) + n(\epsilon_1+\epsilon_2)\\
&\le I(K_A,\mathbf{X}_{\mathcal{A},]m[},F^q;\mathbf{X}_{\mathcal{B},]m[}|X_m^n,F^q) + n(\epsilon_1+\epsilon_2) \qquad (31)\\
&\overset{(e)}{=} I(\mathbf{X}_{\mathcal{A},]m[};\mathbf{X}_{\mathcal{B},]m[}|X_m^n,F^q)+n(\epsilon_1+\epsilon_2), \qquad (32)
\end{aligned}$$

[3] If $j = 0$, $\{A_1,\cdots,A_j\} = \emptyset$ and $\mathcal{A}_{]m[}$ = {Alice}; if $j = M-1$, $\{B_1,\cdots,B_{M-1-j}\} = \emptyset$ and $\mathcal{B}_{]m[}$ = {Bob}.

where (a) is due to (6); (b) is due to the private key requirement in (8); (c) is due to the condition that $Pr(K_A \neq K_B) \leq \epsilon$ and Fano's inequality, so we have $H(K_A|K_B) \leq n\epsilon_2$; (d) follows from the fact that K_B is determined by (X_B^n, F^q); (e) follows from the fact that K_A is determined by (X_A^n, F^q). Note that Eqs. (30) and (31) have assumed that $\mathbf{X}_{\mathcal{A},]m[}$ and $\mathbf{X}_{\mathcal{B},]m[}$ are known by Alice and Bob for key generation, respectively.

Since deterministic functions are considered for $C_K^{(D)}$, $\forall 1 \leq l \leq q$, it holds that

(1) $H(F_l|X_B^n, F^{l-1}) = 0$ if $l \mod (M+2) = 0$;
(2) $H(F_l|X_A^n, F^{l-1}) = 0$ if $l \mod (M+2) = M+1$;
(3) $H(F_l|X_i^n, F^{l-1}) = 0$ if $l \mod (M+2) = i$, $\forall i \in \{1, \cdots, M\}$.

Therefore, when $l \mod (M+2) = 0$ or $l \mod (M+2) = i$, where $i \in \{B_1, \cdots, B_{M-1-j}\}$,

$$\begin{aligned}
&I(\mathbf{X}_{\mathcal{A},]m[}; \mathbf{X}_{\mathcal{B},]m[}|X_m^n, F^l) \\
&= H(\mathbf{X}_{\mathcal{A},]m[}|X_m^n, F^l) - H(\mathbf{X}_{\mathcal{A},]m[}|\mathbf{X}_{\mathcal{B},]m[}, X_m^n, F^l) \\
&= H(\mathbf{X}_{\mathcal{A},]m[}|X_m^n, F^l) - H(\mathbf{X}_{\mathcal{A},]m[}|\mathbf{X}_{\mathcal{B},]m[}, X_m^n, F^{l-1}) \\
&\leq H(\mathbf{X}_{\mathcal{A},]m[}|X_m^n, F^{l-1}) - H(\mathbf{X}_{\mathcal{A},]m[}|\mathbf{X}_{\mathcal{B},]m[}, X_m^n, F^{l-1}) \\
&= I(\mathbf{X}_{\mathcal{A},]m[}; \mathbf{X}_{\mathcal{B},]m[}|X_m^n, F^{l-1}). \qquad (33)
\end{aligned}$$

When $l \mod (M+2) = M+1$ or $l \mod (M+2) = i$, where $i \in \{A_1, \cdots, A_j\}$,

$$\begin{aligned}
&I(\mathbf{X}_{\mathcal{A},]m[}; \mathbf{X}_{\mathcal{B},]m[}|X_m^n, F^l) \\
&= H(\mathbf{X}_{\mathcal{B},]m[}|X_m^n, F^l) - H(\mathbf{X}_{\mathcal{B},]m[}|\mathbf{X}_{\mathcal{A},]m[}, X_m^n, F^l) \\
&= H(\mathbf{X}_{\mathcal{B},]m[}|X_m^n, F^l) - H(\mathbf{X}_{\mathcal{B},]m[}|\mathbf{X}_{\mathcal{A},]m[}, X_m^n, F^{l-1}) \\
&\leq H(\mathbf{X}_{\mathcal{B},]m[}|X_m^n, F^{l-1}) - H(\mathbf{X}_{\mathcal{B},]m[}|\mathbf{X}_{\mathcal{A},]m[}, X_m^n, F^{l-1}) \\
&= I(\mathbf{X}_{\mathcal{B},]m[}; \mathbf{X}_{\mathcal{A},]m[}|X_m^n, F^{l-1}). \qquad (34)
\end{aligned}$$

When $l \mod (M+2) = m$, obviously we have

$$I(\mathbf{X}_{\mathcal{A},]m[}; \mathbf{X}_{\mathcal{B},]m[}|X_m^n, F^l) = I(\mathbf{X}_{\mathcal{A},]m[}; \mathbf{X}_{\mathcal{B},]m[}|X_m^n, F^{l-1}),$$

since F_l is determined by (X_m^n, F^{l-1}).

Iteratively repeating the above procedure q times results in

$$I(\mathbf{X}_{\mathcal{A},]m[}; \mathbf{X}_{\mathcal{B},]m[}|X_m^n, F^l) \leq I(\mathbf{X}_{\mathcal{A},]m[}; \mathbf{X}_{\mathcal{B},]m[}|X_m^n).$$

Furthermore, define

$$\tilde{X}_A^n \triangleq X_A^n \backslash Y_m^n = (Y_{1,A}^n, \cdots, Y_{m-1,A}^n, Y_{m+1,A}^n, \cdots, Y_{M,A}^n),$$

$$\tilde{X}_B^n \triangleq X_B^n \backslash Y_m^n = (Y_{1,B}^n, \cdots, Y_{m-1,B}, Y_{m+1,B}, \cdots, Y_{M,B}^n).$$

Now, according to Eq. (32), $C_K^{(D)}$ is upper bounded as

$$\begin{aligned}
&n(C_K^{(D)} - \epsilon - \epsilon_1 - \epsilon_2) \leq I(\mathbf{X}_{\mathcal{A},]m[}; \mathbf{X}_{\mathcal{B},]m[}|X_m^n) \\
&\overset{(a)}{=} I(Y_{m,A}^n; Y_{m,B}^n|X_m^n) + \\
&\quad I(\tilde{X}_A^n, X_{A_1}^n, \cdots, X_{A_j}^n; \tilde{X}_B^n, X_{B_1}^n, \cdots, X_{B_{M-1-j}}^n) \\
&\overset{(b)}{=} I(\tilde{X}_A^n, X_{A_1}^n, \cdots, X_{A_j}^n; \tilde{X}_B^n, X_{B_1}^n, \cdots, X_{B_{M-1-j}}^n) \\
&\overset{(c)}{=} I(Y_{B_1,A}^n, \cdots, Y_{B_{M-1-j},A}^n, Y_{B,A_1}^n \cdots, Y_{B,A_j}^n; \\
&\qquad \tilde{X}_B^n, X_{B_1}^n, \cdots, X_{B_{M-1-j}}^n) \qquad (35) \\
&\overset{(d)}{=} I\Big(Y_{B_1,A}^n, \cdots, Y_{B_{M-1-j},A}^n, Y_{B,A_1}^n \cdots, Y_{B,A_j}^n; \\
&\qquad Y_{A_1,B}^n, \cdots, Y_{A_j,B}^n, Y_{A,B_1}^n, \cdots, Y_{A,B_{M-1-j}}^n\Big) \qquad (36) \\
&= \sum_{i \in \{B_1, \cdots, B_{M-1-j}\}} I(Y_{i,A}^n; Y_{A,i}^n) \\
&\qquad + \sum_{i \in \{A_1, \cdots, A_j\}} I(Y_{B,i}^n; Y_{i,B}^n) \\
&\overset{(e)}{\leq} n\Bigg(\sum_{i \in \{B_1, \cdots, B_{M-1-j}\}} I(Y_{i,A}; Y_{A,i}) + \\
&\qquad \sum_{i \in \{A_1, \cdots, A_j\}} I(Y_{B,i}; Y_{i,B})\Bigg) \\
&\overset{(f)}{=} n \sum_{i \in \{1, \cdots, m-1, m+1, \cdots, M\}} I_i \qquad (37) \\
&= n\left(\sum_{i=1}^{M} I_i\right) - nI_m \qquad (38)
\end{aligned}$$

where (a) is due to the fact that $(Y_{m,A}^n, X_m^n, Y_{m,B}^n)$ is independent of $(\tilde{X}_A^n, \tilde{X}_B^n)$ and also independent of X_i^n, $i \neq m$; (b) is due to the fact that $Y_{m,A}^n - X_m^n - Y_{m,B}^n$ is a Markov chain; (c) is due to the PIN model in which $\Big((Y_{A_1,A}^n, Y_{A,A_1}^n), \cdots, (Y_{A_j,A}^n, Y_{A,A_j}^n)\Big)$ is independent of any other random variables in (35); (d) is due to the PIN model in which $\Big((Y_{B_1,B}^n, Y_{B,B_1}^n), \cdots, (Y_{B_{M-1-j},B}^n, Y_{B,B_{M-1-j}}^n)\Big)$ is independent of any other random variables in (36); (e) is due to the fact that the source observations are i.i.d.; (f) is due to the partition criterion as shown in (28) and (29), where I_i is defined in Eq. (9).

Next, considering all the M enhanced source models (i.e., all possible $m \in \{1, \cdots, M\}$ in (38)), we can obtain

$$C_K^{(D)} \leq \sum_{i=1}^{M} I_i - \max_{m \in \{1, \cdots, M\}} I_m + \epsilon + \epsilon_1 + \epsilon_2. \qquad (39)$$

The upper bound for $C_K^{(D)}$ has been proved. On the other hand, we will deal with randomized encoding and key generation as following. Let V_A, V_B and V_i be the random variables at Alice, Bob and relay i, $i \in \{1, \cdots, M\}$, which are independent of each other and of $X_A^n, X_B^n, X_1^n, \cdots, X_M^n$. Note that randomization is essentially equivalent to using deterministic functions of these random variables, messages received from the public channel, and source observation

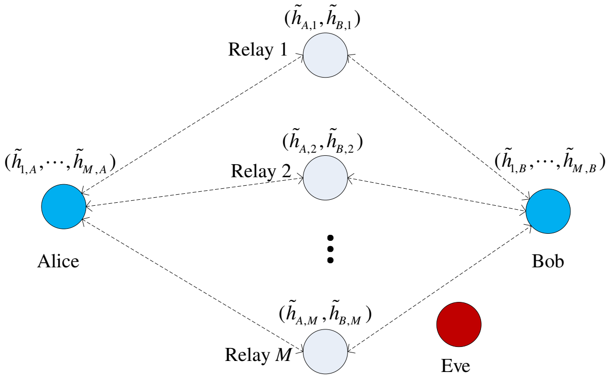

$(\tilde{h}_{A,1},\tilde{h}_{B,1})$
Relay 1
$(\tilde{h}_{A,2},\tilde{h}_{B,2})$
Relay 2
$(\tilde{h}_{1,A},\cdots,\tilde{h}_{M,A})$
$(\tilde{h}_{1,B},\cdots,\tilde{h}_{M,B})$
Alice
Bob
$(\tilde{h}_{A,M},\tilde{h}_{B,M})$
Relay M
Eve

Fig. 3. A system diagram for the cooperative wireless network with multiple relays, where Alice and Bob wish to agree on a private key.

at each terminal. Based on this equivalence, it is not difficult to prove that $I(Y_{i,A},V_A;Y_{A,i},V_i) = I(Y_{i,A};Y_{A,i})$ and $I(Y_{i,B},V_B;Y_{B,i},V_i) = I(Y_{i,B};Y_{B,i})$. Thus, according to (39), C_K can be upper bounded as

$$\begin{aligned}
C_K &= \sup_{p(v_A)p(v_B)p(v_1)\cdots p(v_M)} C_K^{(D)}(V_A,V_B,V_1,\cdots,V_M)\\
&\le \sup_{p(v_A)p(v_B)p(v_1)\cdots p(v_M)} \sum_{i=1}^{M}\\
&\quad \min\left\{I(Y_{i,A},V_A;Y_{A,i},V_i), I(Y_{i,B},V_B;Y_{B,i},V_i)\right\}\\
&\quad - \max_{m\in\{1,\cdots,M\}} \min\{I(Y_{m,A},V_A;Y_{A,m},V_m),\\
&\qquad\qquad I(Y_{m,B},V_B;Y_{B,m},V_m)\} + \epsilon + \epsilon_1 + \epsilon_2\\
&= \sum_{i=1}^{M} I_i - \max_{m\in\{1,\cdots,M\}} I_m + \epsilon + \epsilon_1 + \epsilon_2. \qquad (40)
\end{aligned}$$

Theorem 1 has been proved.

IV. Key Generation in the Wireless Network

In this section, we will extend the RB algorithm proposed for the PIN model into the wireless network, and use estimates of wireless fading channels as source observations for private key generation.

A. Model

Fig. 3 shows the considered wireless network, which can be viewed as a practical example of the PIN model in Section II, where the correlated source observations can be obtained from estimates of wireless fading channels. All terminals are equipped with a single antenna and are half-duplex constrained. Furthermore, these $M+2$ terminals can transmit over the wireless and public channels, whereas Eve only receives messages form these channels without sending signals. For simplicity, it is assumed that a direct link between Alice and Bob does not exist, i.e., the channel gain between Alice and Bob is in deep fading.

Denote $h_{A,i}$ ($h_{B,i}$) as the fading channel gains between relay i and Alice (Bob). All channels are assumed to be reciprocal. It is reasonable to assume that all fading channel gains and noises are RVs and independent of each other. An ergodic *block fading* model is considered, in which all channel gains remain constant for a block of T symbols and change randomly to other independent values after the current block. For simplicity, we assume $h_{A,i} \sim \mathcal{N}(0,\delta_{A,i}^2)$, $h_{B,i} \sim \mathcal{N}(0,\delta_{B,i}^2)$. Moreover, no terminal knows the values of $h_{A,i}$ and $h_{B,i}$ a priori, but all terminals know their statistics.

Let the sequences $\mathbf{S}_i = [s_i(1),\cdots,s_i(L_i)]^T$, $\mathbf{S}_A = [s_A(1),\cdots,s_A(L_A)]^T$ and $\mathbf{S}_B = [s_B(1),\cdots,s_B(L_B)]^T$ denote the signals sent by relay i, Alice and Bob in L_i, L_A and L_B channel uses, respectively, where $i = 1,\cdots,M$. For simplicity, we consider an equal power constraint [21] for the legitimate terminals, that is

$$\frac{1}{L_i}\mathbb{E}\{\mathbf{S}_i^T\mathbf{S}_i\}, \frac{1}{L_A}\mathbb{E}\{\mathbf{S}_A^T\mathbf{S}_A\}, \frac{1}{L_B}\mathbb{E}\{\mathbf{S}_B^T\mathbf{S}_B\} \le P. \qquad (41)$$

B. Application of Proposed RB Algorithm

Algorithm 1 in Section III-A can be applied for private key generation in the considered wireless network, where the correlated source observations at each terminal can be obtained using an orthogonal training[4] method. Specifically, each fading block is divided into $M+2$ time slots; all relays, Alice and Bob take turns to broadcast training sequences during these time slots. The numbers of symbols in these time slots are $T_1,\cdots,T_M$, T_A, T_B, respectively. The tuple $(T_A,T_B,T_1,\cdots,T_M)$ satisfies

$$T_A + T_B + \sum_{i=1}^{M} T_M = T,\ T_A,T_B,T_1,\cdots,T_M \ge 0 \qquad (42)$$

Suppose that relay i sends a known training sequence $\mathbf{S}_i$ of size $T_i \times 1$; Alice sends a known training sequence $\mathbf{S}_A$ of size $T_A \times 1$; Bob sends a known training sequence $\mathbf{S}_B$ of size $T_B \times 1$. The energy of each sequence is $||\mathbf{S}_i||^2 = T_iP$, $||\mathbf{S}_A||^2 = T_AP$, $||\mathbf{S}_B||^2 = T_BP$, where $||\cdot||$ denotes the Euclidean norm.

From the training process, Alice can obtain estimates $(\tilde{h}_{1,A},\cdots,\tilde{h}_{M,A})$; Bob can obtain estimates $(\tilde{h}_{1,B},\cdots,\tilde{h}_{M,B})$; relay i can obtain estimates $(\tilde{h}_{A,i},\tilde{h}_{B,i})$, $i = 1,\cdots,M$. Here the pairs $\{(\tilde{h}_{i,\alpha},\tilde{h}_{i,\alpha})\}_{\alpha\in\{A,B\},i\in\{1,\cdots,M\}}$ are mutually independent. The details of how to obtain these correlated channel estimates have been provided in many existing works (e.g., [21], [22]), which are omitted here for simplicity. The mutual information between $\tilde{h}_{i,\alpha}$ and $\tilde{h}_{i,\alpha}$ can be written as [19], [21], [22]:

$$\begin{aligned}
I_{\alpha,i}^G \triangleq \frac{1}{2}\log_2\left(1 + \frac{T_iT_\alpha P^2\delta_{\alpha,i}^4}{\delta^4 + (T_i+T_\alpha)\delta^2\delta_{\alpha,i}^2P}\right),\\
\forall\alpha\in\{A,B\}, i\in\{1,\cdots,M\} \qquad (43)
\end{aligned}$$

[4] For an orthogonal training method, all terminals transmit training symbols in orthogonal time slots, which has been adopted in most relevant works [17]–[22]. A non-orthogonal training method was proposed in [23], for which Alice and Bob transmit training symbols simultaneously to confuse all untrusted relays. This training method requires perfect synchronization, which is challenging to implement in practice. This paper only considers the orthogonal training method, unless otherwise state.

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

In the following corollary, we will justify that the proposed RB algorithm is optimal.

Corollary 1: Among training-based approaches for private key generation, Algorithm 2 achieves the optimal key rate, i.e., R_{key}^G bits per channel use (BPCU), for some tuple $(T_A, T_B, T_1, \cdots, T_M)$. Here R_{key}^G can be written as

$$R_{key}^G \triangleq \frac{1}{T}\left(\sum_{i=1}^{M} I_i^G - \max_{i\in\{1,\cdots,M\}} I_i^G\right), \tag{44}$$

where $I_i^G \triangleq \min\{I_{A,i}^G, I_{B,i}^G\}$, and $I_{A,i}^G$ and $I_{B,i}^G$ are given in (43).

Proof: Using the observations from channel estimation, I_i defined in (9) can be evaluated as

$$I_i = \min\{I(\tilde{h}_{i,A}, \tilde{h}_{A,i}), I(\tilde{h}_{i,B}, \tilde{h}_{B,i})\} = I_i^G$$

for a given tuple $(T_A, T_B, T_1, \cdots, T_M)$. Then, according to the private key capacity in (10), we can obtain the key rate shown in Eq. (44), where the factor $1/T$ is due to the fact that each channel gain keeps unchanged for T symbols, and *only one* value of the channel statistics can be observed for every T symbols.

Now, we will prove the optimality of R_{key}^G in Eq. (44). According to [19], [21], we know that, from the training process, the optimal pairwise key between Alice (Bob) and relay i is $I_{A,i}^G$ ($I_{B,i}^G$), for a given tuple $(T_A, T_B, T_1, \cdots, T_M)$. Thus, according to the result of the private key capacity in Theorem 1, R_{key}^G is the optimal rate for a given tuple $(T_A, T_B, T_1, \cdots, T_M)$. So the proposed RB algorithm is optimal among training-based approaches for private key generation. ■

To further show the impact of the proposed scheme on the performance gain of the key rate, the multiplexing gain (introduced in [21]) is studied.

Corollary 2: For the considered wireless network with M relays, the proposed RB algorithm achieves the optimal multiplexing gain among training-based key generation approaches, that is $M-1$.

Proof: Based on the definition of in [21], the multiplexing gain of the proposed algorithm is $\lim_{P\to\infty} R_{key}^G/R_s$, where $R_s = \frac{1}{2T}\log_2 P$ as $P\to\infty$.

From Eq. (43), it is easy to obtain that $\lim_{P\to\infty} I_i^G/R_s = T$, so we have

$$\lim_{P\to\infty}\frac{R_{key}^G}{R_s} = M-1.$$

Furthermore, from Theorem 1 and Corollary 1, obviously this multiplexing gain is optimal. ■

Remark 4: For the private key generation algorithm in [21] (Corollary 10) without the direct link between Alice and Bob, its multiplexing gain is $\lfloor M/2\rfloor$. Compared to the XOR scheme, the proposed RB scheme effectively enhances the performance of the private key generation.

Remark 5: The main difference between the proposed algorithm and that in [21] lies in the key distillation step: the former is based on the RB process and the latter is based on an XOR process. In [21], Alice and Bob concatenate $(W_1 \oplus W_2, \cdots, W_{M-1} \oplus W_M)$ as the final private key in the key distillation step. Here M is assumed to be an even number. Compared the proposed algorithm with the algorithm in [21], the proposed algorithm pays less price for satisfying the secrecy constraints at the relays, i.e., the proposed algorithm utilizes RB to provide the necessary randomness in the private-key codebook, and the dummy message in each bin is used to confuse all relays simultaneously.

C. Numerical Results

In this subsection, the performance of the proposed RB algorithm will be illustrated by using some numerical examples. The block length is set to be $T = 20$, and the variances of the channel gains are set to be $\delta_{A,i}^2 = \delta_{B,i}^2 = 1$, $i = 1, \cdots, M$. Moreover, the variances of all Gaussian noises are set to be $\delta^2 = 1$.

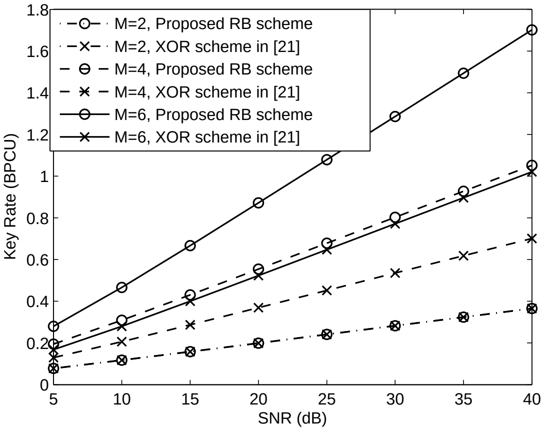


Fig. 4. Comparison of key rates of the two key generation algorithms.

Figure 4 compares the proposed RB algorithm with the XOR algorithm in [21], where the key rate is shown as a function of the signal-to-noise ratio (SNR), with different number of relays. When $M = 2$, the two algorithms achieve the same key rate. But when M increases, the proposed RB algorithm outperforms the XOR one. Moreover, the performance gap between these two schemes enlarges as M increases.

Figure 5 compares the key rates of these two algorithms as a function of the number of the relays (i.e., M), where the SNR is fixed as 20dB. In addition, the key rate without secrecy constraints at the relays [21] is also shown in the figure. Specifically, the slope of the proposed RB algorithm is the same as that without secrecy constraints at the relays, whereas the slope of the XOR algorithm is less. This is because the multiplexing gain of the proposed RB algorithm is $M-1$, whereas the multiplexing gain of the XOR algorithm is about $M/2$, as discussed in Remark 4.

V. Discussion

In this section, the proposed RB algorithm as well as the developed principles used to establish the private key capacity in the previous section will be extended to several more general PIN models.

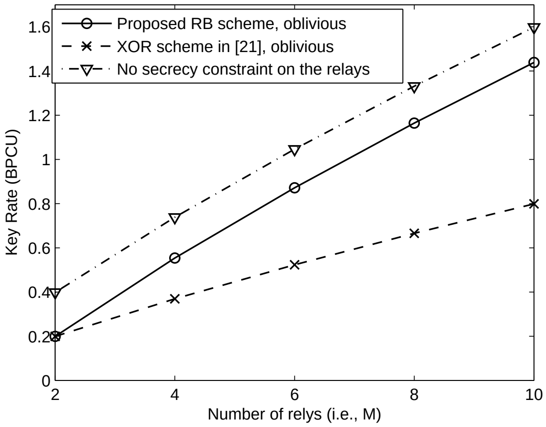


Fig. 5. Key rates vs the number of relays, where the SNR is fixed as 20dB.

A. Direct Link between Alice and Bob

The PIN model in Section II assumes that no direct link exists, i.e., no correlated source exists between Alice and Bob. This subsection considers the case that Alice and Bob observe n i.i.d. repetitions of the correlated RVs, $Y_{B,A}$ and $Y_{A,B}$, respectively. Following the definition of the PIN model in (1), the pair $(Y_{B,A}, Y_{A,B})$ is assumed be independent of any other pair $(Y_{i,\alpha}, Y_{\alpha,i})$, $\forall \alpha \in \{A, B\}$, $i \in \{1, \cdots, M\}$. The private key capacity of this PIN model is given in the following.

Corollary 3: For the PIN model with direct link between Alice and Bob, the private key capacity is $C_K + I(Y_{B,A}; Y_{A,B})$, where C_K is defined in (10).

Proof: Based on the point-to-point key generation technique [3], [4], Alice and Bob can agree on a pairwise key, denoted as $K_{A,B}$, whose rate is $I(Y_{B,A}; Y_{A,B})$. From Section III-A, a private key (whose values are K_A and K_B at Alice and Bob, respectively) can be generated using the proposed RB algorithm. Similar to Remark 3, for brevity, we use K_A to denote both K_A and K_B with the understanding that they are different with a small probability. Then, Alice and Bob concatenate K_A and $K_{A,B}$ as the private key. Such a private key $(K_A, \tilde{K}_{B,A})$ is obviously secret from both Eve and all relays. Since K_A and $K_{A,B}$ are independent due to the definition of the PIN model, the achievable rate of the private key $(K_A, K_{A,B})$ is $C_K + I(Y_{B,A}; Y_{A,B})$.

On the other hand, The converse can be proved by extending the proof steps in Section III-B in a straightforward manner. ■

B. Secrecy Constraint on Part of Relays

The secrecy constraint in (8) for the PIN model in Section II requires the generated key to be secret from all relays. However, when the generated key is required to be secret from only part of the relays, the secrecy constraint in (8) should be changed into

$$\frac{1}{n} I(K_A; X_m^n, F^q) \leq \epsilon, \forall m \in \{1, \cdots, M_p\}, \qquad (45)$$

where without loss of generality, K_A is assumed to be secret from relays $1, \cdots, M_p$, $1 \leq M_p \leq M$. The private key capacity of this PIN model with the secrecy constraint on part of relays is given in the following corollary.

Corollary 4: When the generated key is required to be secret from relays $1, \cdots, M_p$, the private key capacity is given by

$$C_K^{(p)} \triangleq \sum_{i=1}^{M} I_i - \max_{m \in \{1, \cdots, M_p\}} I_m, \qquad (46)$$

where I_i is defined in (9).

Proof: The proof of this corollary is trivial, which can be obtained by extending the proof steps of Theorem 1 in a straightforward manner. ■

C. Colluding Relays

The secrecy constraint in (8) for the PIN model in Section II corresponds to the case that all relays are *non-colluding*. When part of the relays are *colluding*, i.e., they collaborate with each other to intercept the private key, the secrecy constraint in (8) should be changed into

$$\frac{1}{n} I(K_A; X_1^n, \cdots, X_{M_c}^n, F^q) \leq \epsilon,$$
$$\frac{1}{n} I(K_A; X_m^n, F^q) \leq \epsilon, \forall m \in \{M_c + 1, \cdots, M\}, \qquad (47)$$

where without loss of generality, the relays $1, \cdots, M_c$ are assumed to be colluding, and relays $M_c + 1, \cdots, M$ are non-colluding, $1 \leq M_c \leq M$. The private key capacity of this PIN model with part of colluding relays can be determined in the following corollary.

Corollary 5: When relays $1, \cdots, M_c$ are colluding, the private key capacity is given by

$$C_K^{(c)} \triangleq \sum_{i=1}^{M} I_i - \max\left\{ \sum_{i=1}^{M_c} I_i, \max_{m \in \{M_c+1, \cdots, M\}} I_m \right\}. \qquad (48)$$

Proof: In this colluding case, relays $1, \cdots, M_c$ are equivalent to a super relay node that utilizes the joint observation $(X_1^n, \cdots, X_{M_c}^n)$ in order to intercept the private key information. Then, this corollary can be proven by extending the proof steps of Theorem 1 in a straightforward manner. ■

D. Group Key Generation

The PIN model in Section II requires to generate a private only between two terminals. This subsection considers the private key generation problem among L terminals, $L \geq 2$. Consider a cooperative DMS model with $M + L$ terminals. Denote $\mathcal{L} \triangleq \{1, \cdots, L\}$ and $\mathcal{M} \triangleq \{L + 1, \cdots, L + M\}$. All terminals in $\mathcal{L}$ wish to share a private key with the help of the terminals in $\mathcal{M}$, i.e., the terminals in $\mathcal{M}$ act as the M relays. For $\forall l \in \mathcal{L}$ and $m \in \mathcal{M}$, let $Y_{m,l}$ and $Y_{l,m}$ denote the correlated source observations at terminals l and m, respectively. Specifically, terminal l observes n i.i.d. repetitions of the RV $X_l \triangleq (Y_{1,l}, \cdots, Y_{M,l})$, denoted as $X_l^n \triangleq (Y_{L+1,l}^n, \cdots, Y_{L+M,l}^n)$; terminal m observes n i.i.d. repetitions of the RV $X_m \triangleq (Y_{1,m}, \cdots, Y_{L,m})$, denoted as $X_m^n \triangleq (Y_{1,m}^n, \cdots, Y_{L,m}^n)$. In this PIN model,

$$I(Y_{i,\alpha}, Y_{\alpha,i}; \{Y_{j,\beta}, Y_{\beta,j} : (j, \beta) \neq (i, \alpha)\}) = 0,$$
$$\text{for } i, j \in \mathcal{M}; \alpha, \beta \in \mathcal{L}. \qquad (49)$$

Algorithm 2: Extension of RB Algorithm for Group Key Generation

Step 1: Key Agreement:

- Terminals l and m agree on a pairwise key $W_{l,m}$ from the correlated observations $(Y_{m,l}^n, Y_{l,m}^n)$, $\forall l \in \mathcal{L}$, $m \in \mathcal{M}$.
- Terminal m chooses the shortest key among $\{W_{1,m}, \cdots, W_{L,m}\}$, denoted as $W_{l_m,m}$, $\forall m \in \mathcal{M}$; then, it successively sends $W_{l_m,m} \oplus W_{l,m}$, $\forall l \in \mathcal{L}\backslash l_m$, from which all terminals in $\mathcal{L}$ can obtain $W_{l_m,m}$.

Step 2: Key Distillation:

- In advance, randomly partition all sequences $\tilde{w}^M$ in $\tilde{\mathcal{W}}^M \triangleq \mathcal{W}_{l_1,1} \times \cdots \times \mathcal{W}_{l_M,M}$ into $2^{n(R_{key}^{(g)}-\epsilon)}$ bins each with an equal amount of codewords. All terminals know this private-key codebook.
- All terminals in $\mathcal{L}$ find the sequence $\tilde{W}^M = (W_{l_1,1}, \cdots, W_{l_M,M})$ in the RB based private-key codebook, and choose its bin number as the final private key.

Note that the considered PIN model only includes correlated sources between all terminal pairs $(l,m)_{\forall l\in\mathcal{L}, m\in\mathcal{M}}$, but does not include correlated sources between any terminal pair in the same set $\mathcal{L}$ nor $\mathcal{M}$. For this cooperative PIN model, an achievable group key rate is given in the following corollary.

Corollary 6: An achievable group key rate of the considered cooperative PIN model is

$$R_{key}^{(g)} \triangleq \sum_{m=1}^{M-1} I_{(m)}^{(g)}, \tag{50}$$

where $I_{(1)}^{(g)} \leq I_{(2)}^{(g)} \leq \cdots \leq I_{(M)}^{(g)}$, which is the ordering of $(I_1^{(g)}, \cdots, I_M^{(g)})$, and

$$I_m^{(g)} \triangleq \min_{l\in\mathcal{L}} I(Y_{l,m}; Y_{m,l}), \ \forall m \in \mathcal{M}. \tag{51}$$

Proof: The rate in (50) can be achieved by extending the proposed RB algorithm in Section III-A. Such an extended algorithm is summarized in Algorithm 2, which also includes the key agreement and key distillation steps. Since Algorithm 2 is obtained by slightly modifying Algorithm 1 in Section III-A, we only briefly describe it in the next.

In the key agreement step, every terminal pair (l,m) agrees on a pairwise key $W_{l,m}$, $\forall l \in \mathcal{L}$, $m \in \mathcal{M}$; then relay m sends $W_{l_m,m} \oplus W_{l,m}$, $\forall l \in \mathcal{L}\backslash l_m$, from which all terminals in $\mathcal{L}$ can obtain $W_{l_m,m}$, where $W_{l_m,m}$ is the shortest key among $(W_{1,m}, \cdots, W_{L,m})$. Denote $\mathcal{W}_{m,l} \triangleq \{1, \cdots, 2^{n(I(Y_{l,m};Y_{m,l})-\epsilon)}\}$, so $W_{l_m,m} \in \mathcal{W}_{l_m,m} \triangleq 2^{n(I_m^{(g)}-\epsilon)}$, which is the m-th common message among all terminals in $\mathcal{L}$. In the key distillation step, randomly partition all sequences $\tilde{w}^M$ in $\tilde{\mathcal{W}}^M \triangleq \mathcal{W}_{l_1,1} \times \mathcal{W}_{l_2,2} \times \cdots \times \mathcal{W}_{l_M,M}$ into $2^{n(R_{key}^{(g)}-\epsilon)}$ bins, and all terminals in $\mathcal{L}$ choose the bin number of the sequence $\tilde{W}^M = (W_{l_1,1}, \cdots, W_{l_M,M})$ in the RB based private-key codebook as the final private key. Following similar proof steps in Section III-A, one can verify that rate $R_{key}^{(g)}$ is achievable. ■

From Theorem 1, the achievable rate in Corollary 6 is optimal when $L = 2$. The following corollary shows that the achievable rate in Corollary 6 is also optimal when the number of relays is $M = 2$.

Corollary 7: When only two relay nodes exist, i.e., $M = 2$, the group key capacity of the considered PIN model is $C_K^{(g)} \triangleq \min\{I_1^{(g)}, I_2^{(g)}\}$.

Proof: When $M = 2$, from Corollary 6, $C_K^{(g)}$ can be achieved by the proposed RB algorithm in Algorithm 2.

To prove the converse, we can consider two enhanced source models. For the first enhanced model, we only consider the secrecy constraint on terminal $L+1$, and ignore the secrecy constraint on terminal $L+2$. Moreover, assume that there is a genie-aided terminal that knows the source observations of all terminals in the set $\mathcal{G}$, where $\mathcal{G} = \{1, \cdots, l^*-1, l^*+1, \cdots, L, L+2\}$ and $l^* = \arg\min_{l\in\mathcal{L}} I(Y_{l,2}; Y_{2,l})$. Furthermore, such a genie-aided terminal and terminal l^* wish to generate a secret key which is protected from terminal $L+1$, denoted as K_{l^*}. From Section III-B, the capacity of K_{l^*} can be upper bounded as $I_1^{(g)}$ (defined in (51)).

Obviously, the group key capacity $C_K^{(g)}$ is upper bounded by the capacity of K_{l^*}, and $C_K^{(g)} \leq I_1^{(g)}$ can be obtained. Similarly, we have $C_K^{(g)} \leq I_2^{(g)}$ by constructing the second enhanced model. ■

VI. Conclusion

In this paper, we have investigated the problem of private key generation. A particular cooperative PIN model with $M+2$ terminals is considered, where Alice, Bob and M relays observe pairwise independent sources. With the help of the relays, Alice and Bob wish to establish a private key that is secure from Eve and all relays. In this paper, we have presented a single-letter characterization of the private key capacity of this PIN model, where the achievability part is proved via a RB algorithm for generating the private key, and the converse part is proved by deriving upper bounds of M enhanced source models. Then, we further considered a cooperative wireless network, in which estimates of wireless channels are considered as the correlated source observations. Compared to the XOR algorithm in [21] whose multiplexing gain is $\lfloor M/2 \rfloor$, the proposed RB algorithm achieves a larger multiplexing gain $M-1$. Finally, several more general PIN models are investigated, by applying the basic idea of the proposed achievable scheme.

Appendix A
Proof of Lemma 1

First, $H(W^M|W_m, K_A, \mathcal{C})$ can be expressed as

$$H(W^M|W_m, K_A, \mathcal{C}) = \sum_{w_m, k_A} p(w_m, k_A) H(W^M|w_m, k_A, \mathcal{C}). \tag{52}$$

Given (w_m, k_A) and a codebook c, denote $\hat{\mathcal{W}}^M$ as the set which is formed by all codewords w^M satisfying: (i) $w^M \in \mathcal{W}^M$; (ii) w^M lies in the k_A-th bin of the private-key codebook; (iii) the m-th element of w^M is w_m. Furthermore, let $N(w_m, k_A, c) = |\hat{\mathcal{W}}^M|$, which denotes the number of codewords in $\hat{\mathcal{W}}^M$. Since all sequences $w^M \in \mathcal{W}^M$ are randomly partitioned when constructing the codebook, averaged over the RB-based codebook $\mathcal{C}$, the probability that the m-th element of a codeword is w_m is 2^{-nR_m}. Thus, $N(w_m, k_A, \mathcal{C})$ is binomially distributed averaged over $\mathcal{C}$, i.e., $N(w_m, k_A, \mathcal{C}) \sim B(2^{n(R_{(M)}+\epsilon)}, 2^{-nR_m})$, where $2^{n(R_{(M)}+\epsilon)}$ is the number of codewords in the k_A-th bin. Thus, the expectation and variance of $N(w_m, k_A, \mathcal{C})$ can be expressed as

$$\mathbb{E}[N(w_m, k_A, \mathcal{C})] = 2^{-nR_m} 2^{n(R_{(M)}+\epsilon)} = 2^{n(R_{(M)}-R_m+\epsilon)}, \tag{53}$$

$$\begin{aligned} Var[N(w_m, k_A, \mathcal{C})] &= 2^{-nR_m} 2^{n(R_{(M)}+\epsilon)} (1 - 2^{-nR_m}) \\ &\leq 2^{n(R_{(M)}-R_m+\epsilon)}. \end{aligned} \tag{54}$$

Now, define an indicator function with respect to $N(w_m, k_A, \mathcal{C})$ as

$$I_d(N(w_m, k_A, \mathcal{C})) = \begin{cases} 1, & \text{if } N(w_m, k_A, \mathcal{C}) \\ & \geq 2 \quad \mathbb{E}[N(w_m, k_A, \mathcal{C})] \\ 0, & \text{otherwise.} \end{cases} \tag{55}$$

Then, by Chebyshev inequality

$$\begin{aligned} P\{I_d(N(w_m, k_A, \mathcal{C})) = 1\} &\leq \frac{Var[N(w_m, k_A, c)]}{\mathbb{E}^2[N(w_m, k_A, c)]} \\ &\leq 2^{-n(R_{(M)}-R_m+\epsilon)}. \end{aligned} \tag{56}$$

Thus, by using $H(I_d) \leq 1$, we have

$$\begin{aligned} & H(W^M | w_m, k_A, \mathcal{C}) \leq H(W^M, I_d | w_m, k_A, \mathcal{C}) \\ & = H(I_d) + \sum_{i=0}^{1} P\{I_d = i\} H(W^M | w_m, k_A, \mathcal{C}, I_d = i) \\ & \leq 1 + P\{I_d = 1\} \log_2 |\mathcal{W}^M| + H(W^M | w_m, k_A, \mathcal{C}, I_d = 0) \\ & \leq 1 + n 2^{-n(R_{(M)}-R_m+\epsilon)} \times \sum_{i=1}^{M} R_i \\ & \quad + \log_2 \left(2 \times 2^{n(R_{(M)}-R_m+\epsilon)} \right), \end{aligned}$$

where the last relationship is due to (56), and the fact that $N(w_m, k_A, \mathcal{C}) < 2 \times 2^{n(R_{(M)}-R_m+\epsilon)}$ if $I_d = 0$. Recalling (52),

$$H(W^M | W_m, K_A, \mathcal{C}) \leq n(R_{(M)} - R_m + \delta_2(\epsilon)) \tag{57}$$

where

$$\delta_2(\epsilon) = \frac{2}{n} + 2^{-n(R_{(M)}-R_m+\epsilon)} \times \sum_{i=1}^{M} R_i + \epsilon.$$

References

[1] P. Xu, Z. Ding, and X. Dai, "The private key capacity of a cooperative pairwise-independent network," in *IEEE International Symposium on Information Theory (ISIT)*, 2015, pp. 286–290.

[2] C. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[3] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. Part I: secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, 1993.

[4] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[5] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Transactions on Information theory*, vol. 19, no. 4, pp. 471–480, 1973.

[6] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3047–3061, 2004.

[7] S. Nitinawarat and P. Narayan, "Perfect omniscience, perfect secrecy, and steiner tree packing," *IEEE Transactions on Information Theory*, vol. 56, no. 12, pp. 6490–6500, 2010.

[8] ——, "Secret key generation for correlated Gaussian sources," *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 3373–3391, 2012.

[9] C. Ye and P. Narayan, "Secret key and private key constructions for simple multiterminal source models," *IEEE Transactions on Information Theory*, vol. 58, no. 2, pp. 639–651, Feb 2012.

[10] A. A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals—Part I," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3973–3996, 2010.

[11] H. Zhang, Y. Liang, L. Lai, and S. Shamai, "Two-key generation for a cellular model with a helper," in *IEEE International Symposium on Information Theory (ISIT)*, 2015, pp. 715–719.

[12] C. Ye and A. Reznik, "Group secret key generation algorithms," in *IEEE International Symposium on Information Theory*, 2007, pp. 2596–2600.

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

[14] L. Lai and L. Huie, "Simultaneously generating multiple keys in many to one networks," in *IEEE International Symposium on Information Theory Proceedings (ISIT)*, 2013, pp. 2394–2398.

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

[16] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge university press, 2005.

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

[18] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, 2010.

[19] L. Lai, Y. Liang, and H. V. Poor, "A unified framework for key agreement over wireless fading channels," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 480–490, 2012.

[20] A. Khisti, "Interactive secret key generation over reciprocal fading channels," in *IEEE 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2012, pp. 1374–1381.

[21] L. Lai, Y. Liang, and W. Du, "Cooperative key generation in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 8, pp. 1578–1588, 2012.

[22] H. Zhou, L. Huie, and L. Lai, "Secret key generation in the two-way relay channel with active attackers," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 3, pp. 476–488, 2014.

[23] C. D. T. Thai, J. Lee, C. Cheng, and T. Q. Quek, "Physical-layer secret key generation with untrusted relays," in *Globecom Workshops (GC Wkshps)*, 2014, pp. 1385–1390.

[24] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 344–366, 2000.

[25] 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. Information Theory*, vol. 60, no. 10, pp. 6389–6398, Oct 2014.

[26] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[27] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory,*, vol. 24, no. 3, pp. 339–348, May 1978.

[28] Y. Oohama, "Relay channels with confidential messages," 2007. [Online]. Available: http://arxiv.org/abs/cs/0611125

[29] X. He and A. Yener, "Two-hop secure communication using an untrusted relay," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, p. 9, 2009.

[30] ——, “Cooperation with an untrusted relay: A secrecy perspective,” *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[31] A. Khisti, S. N. Diggavi, and G. W. Wornell, “Secret-key generation using correlated sources and channels,” *IEEE Transactions on Information Theory*, vol. 58, no. 2, pp. 652–670, 2012.

[32] V. M. Prabhakaran, K. Eswaran, and K. Ramchandran, “Secrecy via sources and channels,” *IEEE Transactions on Information Theory*, vol. 58, no. 11, pp. 6747–6765, 2012.

[33] H. Zhang, Y. Liang, L. Lai, and S. Shamai, “Multi-key generation over a cellular model with a helper,” *Submitted to IEEE Transactions on Information Theory*, Available: http://hzhan23.mysite.syr.edu/journals/KeyCellularModel_IT2015.pdf.

[34] B. E. Schein, “Distributed coordination in network information theory,” Ph.D. dissertation, Massachusetts Institute of Technology, Cambridge, 2001.

[35] W. Kang and S. Ulukus, “Capacity of a class of diamond channels,” *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4955–4960, 2011.

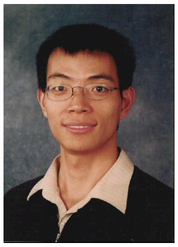
[36] U. Niesen and S. N. Diggavi, “The approximate capacity of the Gaussian N-relay diamond network,” *IEEE Transactions on Information Theory*, vol. 59, no. 2, pp. 845–859, 2013.

[37] S. Sarma, S. Agnihotri, and J. Kuri, “Secure transmission in amplify-and-forward diamond networks with a single eavesdropper,” *Available: http://arxiv.org/abs/1504.03149*.

[38] S.-H. Lee and A. Khisti, “The degraded Gaussian diamond-wiretap channel,” *IEEE Transactions on Communications (Submitted)*, Available: http://arxiv.org/abs/1504.05900.

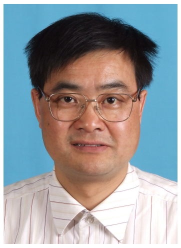
[39] A. El Gamal and Y.-H. Kim, *Network information theory*. Cambridge University Press, 2011.

Peng Xu received the B.Eng. and the 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 July 2014, he has been working as a postdoctoral researchers with the Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei, China. His current research interests include cooperative communications, information theory, information-theoretic secrecy, and 5G networks. He received IEEE Wireless Communications Letters Exemplary Reviewer 2015.



Zhiguo Ding (S’03-M’05-SM’15) 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.

Dr Ding’s research interests are 5G networks, game theory, cooperative and energy harvesting networks and statistical signal processing. He is serving as an Editor for *IEEE Transactions on Communications*, *IEEE Transactions on Vehicular Technologies*, *IEEE Wireless Communication Letters*, *IEEE Communication Letters*, and *Journal of Wireless Communications and Mobile Computing*. He received the best paper award in IET Comm. Conf. on Wireless, Mobile and Computing, 2009, IEEE Communication Letter Exemplary Reviewer 2012, and the EU Marie Curie Fellowship 2012-2014.



Xuchu Dai received the B.Eng. degree in Electrical Engineering in 1984 from Airforce Engineering University, Xi’an, China, the M.Eng. degree in 1991 and the Ph.D. degree in 1998 from University of Science and Technology of China, Hefei, China, both in Communication and Information System.

He now is a Professor with the Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei, China. From 2000 to 2002, he was with 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] (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.

He is the author or co-author of more than 400 technical papers published in scientific journals and presented at international conferences. He is also author of the Greek edition of a book on “Telecommunications Systems” and co-author 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. 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.