The Capacity Region of the Source-Type Model for Secret Key and Private Key Generation

Huishuai Zhang, *Student Member, IEEE*, Lifeng Lai, *Member, IEEE*,
Yingbin Liang, *Member, IEEE*, and Hua Wang, *Member, IEEE*

Abstract—**The problem of simultaneously generating a secret key (SK) and private key (PK) pair among three terminals via public discussion is investigated. In this problem, each terminal observes a component of correlated sources. All three terminals are required to generate the common SK to be concealed from an eavesdropper that has access to the public discussion, while two designated terminals are required to generate an extra PK to be concealed from both the eavesdropper and the remaining terminal. An outer bound on the SK–PK capacity region was established by Ye and Narayan, and was shown to be achievable for a special case. In this paper, the SK–PK capacity region is established in general by developing schemes to achieve the outer bound for the remaining two cases. The main technique lies in the novel design of a random binning-joint decoding scheme that achieves the existing outer bound.**

Index Terms—**Secret key, private key, key capacity region, source model.**

I. Introduction

The problem of secret key generation via public discussion under the source model was initiated by [2], [3], which established a remarkable fact that two terminals, each possessing correlated but not exactly the same observations, can establish a shared secret key by only talking to each other in the public. In the basic source-type model considered in [2] and [3], there are two legitimate terminals, who observe correlated source sequences and can communicate with each other through a public channel, and eavesdroppers, who have perfect access to the public channel. The main observation is that, because of the correlation, terminal $\mathcal{X}$ can recover terminal $\mathcal{Y}$'s source sequence by letting terminal $\mathcal{Y}$ send limited amount of information using distributed source coding technique [4]. Then both terminal $\mathcal{X}$ and terminal $\mathcal{Y}$ can generate a shared secret key based on terminal $\mathcal{Y}$'s source sequence subtracting the information that has been revealed. The close connection between the distributed source coding and secret key generation also holds on more general source-type models [5]. In particular, [5] studied a general network with multiple terminals, in which a subset of terminals need to generate a shared secret key. [5] showed that the secret key capacity is equal to the joint entropy of all source observations subtracting the minimum amount of information needed to enable the subset of terminals to recover all source observations.

Until now, with few exceptions to be discussed in the sequel, most of the existing studies focused on generation of a single key [5]–[10]. However, there are various practical scenarios in which multiple keys need to be simultaneously generated. For instance, a number of terminals can have different security clearance levels, and each terminal is allowed to access confidential documents up to its own clearance level. Terminals with the same clearance level should share the same key, and should be kept ignorant of higher level keys.

There have been several existing studies that addressed generation of multiple keys [1], [11]–[14]. Being of particular interest to us, Ye and Narayan studied a multi-key source-type model in [1] and [14], in which three terminals (say terminals $\mathcal{X}, \mathcal{Y}$ and $\mathcal{Z}$) observe correlated source sequences, and wish to generate a common secret key (SK) among all of them, which should be concealed from eavesdroppers, and a private key (PK) between $\mathcal{X}$ and $\mathcal{Y}$ that should be concealed from $\mathcal{Z}$ and eavesdroppers. [1], [14] provided both outer and inner bounds on the SK-PK capacity region. In particular, the outer bound has three different forms corresponding respectively to three cases of correlations among the sources. In [1] and [14], it was shown that the outer bound is achievable for one case, and hence the SK-PK capacity region was established for this case. However, for the other two cases, there are gaps between the outer bound and the inner bound derived based on the scheme developed in [1] and [14]. Finding schemes to achieve the outer bound for the other two cases was left as an open problem in [1]. In fact, the outer bound in the other two cases suggests the necessity of a scheme such that $\mathcal{X}$ helps $\mathcal{Y}$ to recover $\mathcal{Z}$'s information without revealing any more information of $\mathcal{Z}$ to public. This is the major technical challenge to obtain the SK-PK capacity region in general. Furthermore, we note that although the outer bound in [1] and [14] is derived under the condition that allows additional randomization at each terminal, our proposed scheme achieves the outer bound without any local randomization.

Manuscript received February 18, 2014; accepted June 11, 2014. Date of publication July 17, 2014; date of current version September 11, 2014. H. Zhang and Y. Liang were supported in part by the National Science Foundation CAREER under Award CCF-10-26565 and in part by the National Science Foundation under Grant CNS-11-16932. L. Lai was supported in part by a National Science Foundation CAREER under Award CCF-13-18980 and in part by the National Science Foundation under Grant CNS-13-21223. This paper was presented at the 2014 IEEE International Symposium on Information Theory.

H. Zhang and Y. Liang are with the Department of Electrical Engineering and Computer Science, Syracuse University, Syracuse, NY 13244 USA (e-mail: hzhan23@syr.edu; yliang06@syr.edu).

L. Lai is with the Department of Electrical and Computer Engineering, Worcester Polytechnic Institute, Worcester, MA 01609 USA (e-mail: llai@wpi.edu).

H. Wang is with Qualcomm Inc., Bridgewater, NJ 08807 USA (e-mail: huaw@qti.qualcomm.com).

Communicated by U. M. Maurer, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2014.2340400

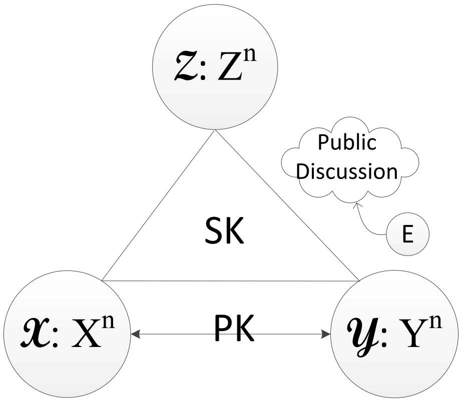

Fig. 1. System model.

Our main contribution in this paper lies in finding schemes that achieve the outer bound for the other two cases for the SK-PK source-type model in [1] and [14]. Then, combined with the result in [1] and [14] for the first case, the full SK-PK capacity region is established. In order to address the technical challenge mentioned above, we design schemes such that terminal $\mathcal{X}$ helps to improve the quality of the side information at $\mathcal{Y}$ in recovering $\mathcal{Z}$'s information rather than directly revealing information of $\mathcal{Z}$.

The paper is organized as follows. Section II contains the model description. Section III presents our main results on the SK-PK capacity region. Section IV and V consist of the proofs of the main theorem for the two cases, respectively. Section VI provides some concluding remarks.

II. System Model

Consider a discrete memoryless source, whose outputs at each time instant are generated based on the joint distribution of random variables (X, Y, Z) with corresponding alphabets $(\mathcal{X}, \mathcal{Y}, \mathcal{Z})$. We consider a system with three terminals $(\mathcal{X}, \mathcal{Y}, \mathcal{Z})$ and an eavesdropper. Here, we use the alphabet symbols to denote the terminals. Terminal $\mathcal{X}$ observes n independent and identically distributed (i.i.d.) repetitions of X, i.e., $X^n = (X_1, \ldots, X_n)$, and terminals $\mathcal{Y}$ and $\mathcal{Z}$ observe $Y^n = (Y_1, \ldots, Y_n)$ and $Z^n = (Z_1, \ldots, Z_n)$, respectively. We assume that the eavesdropper does not have source observations and terminals are allowed to communicate with each other over a public noiseless channel with no rate constraint. We further assume that all transmissions over the public channel are observable to all parties including the eavesdropper. The public discussion can be interactive. Without loss of generality, we assume that terminals $(\mathcal{X}, \mathcal{Y}, \mathcal{Z})$ take turns to transmit for r rounds over $3r$ consecutive time slots. We use $3r$ random variables $F_1, \ldots, F_{3r}$ to denote these transmissions, where F_t denotes the transmission in time slot t for $1 \leq t \leq 3r$. The transmission F_t can be any function of its own observation and all previous transmissions $F_{[1,t-1]} = (F_1, \ldots, F_{t-1})$. We use $\mathbf{F} = (F_1, \ldots, F_{3r})$ to denote all transmissions in $3r$ time slots.

In this system (see Fig. 1), terminals $\mathcal{X}, \mathcal{Y}$ and $\mathcal{Z}$ wish to generate a common secret key K_S, which is required to be kept secure from the eavesdropper (that has access to only the public discussion). Furthermore, terminals $\mathcal{X}$ and $\mathcal{Y}$ wish to generate a private key K_P, which is required to be kept secure not only from the eavesdropper but also from terminal $\mathcal{Z}$.

We next introduce the mathematical definition of the secret key and the private key. A random variable U is said to be *ϵ-recoverable* from another random variable V, if there exists a function f such that

$$\Pr\{U \neq f(V)\} < \epsilon. \tag{1}$$

Definition 1: A pair (K_S, K_P) is said to be an ϵ-(SK, PK) if K_S and K_P satisfy the following requirements.

- *K_S is* ϵ-recoverable *at each of the three terminals with the public transmission* $\mathbf{F}$*, i.e., it can be* ϵ-recoverable *from* $(X^n, \mathbf{F})$*,* $(Y^n, \mathbf{F})$ *and* $(Z^n, \mathbf{F})$*, respectively;*
- *K_P is* ϵ-recoverable *at terminals $\mathcal{X}$ and $\mathcal{Y}$ with public transmission* $\mathbf{F}$*, i.e., it can be* ϵ-recoverable *from* $(X^n, \mathbf{F})$ *and* $(Y^n, \mathbf{F})$*, respectively;*
- *K_S and K_P satisfy the secrecy condition*

$$\frac{1}{n} I(K_S; \mathbf{F}) < \epsilon, \tag{2}$$

$$\frac{1}{n} I(K_P; \mathbf{F}, Z^n) < \epsilon \tag{3}$$

for large enough n, where ϵ can be arbitrarily small; and

- *K_S and K_P satisfy the uniformity condition*

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

$$\frac{1}{n} H(K_P) \geq \frac{1}{n} \log |\mathcal{K_P}| - \epsilon, \tag{5}$$

for large enough n, where $|\mathcal{K_S}|$ and $|\mathcal{K_P}|$ denote the alphabet sizes of the random variable K_S and K_P, respectively.

We note that the secrecy conditions (2) and (3) are in the weak sense, and can be strengthened to the strong sense without loss of performance as in [15].

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

$$\frac{1}{n} H(K_S^{(n)}) > R_S - \delta, \qquad \frac{1}{n} H(K_P^{(n)}) > R_P - \delta. \tag{6}$$

The SK-PK capacity region is defined to be the set that contains all achievable rate pairs (R_S, R_P).

Our goal is to characterize this *SK-PK capacity region*.

III. Main Results

A. Preliminaries

The model introduced in Section II has been studied by Ye and Narayan in [1], which provided outer and inner bounds on the SK-PK capacity region (see [14, Ch. 3] for more details). We cite the outer bound in [1] below, which is useful for presenting our results in the next subsection. For notational convenience, we define

$$R_A := I(Z;XY), \tag{7}$$

$$R_B := \min\{I(X;YZ), I(Y;XZ)\}, \tag{8}$$

$$R_C := \frac{1}{2}(H(X)+H(Y)+H(Z)-H(X,Y,Z)). \tag{9}$$

Theorem 1 [1]: An outer bound on the SK-PK capacity region for the model in Section II contains the rate pairs (R_S, R_P) satisfying

$$R_S \leq R_A, \tag{10}$$

$$R_P \leq I(X;Y|Z), \tag{11}$$

$$R_S + R_P \leq R_B, \tag{12}$$

$$2R_S + R_P \leq 2R_C. \tag{13}$$

where the constants R_A, R_B and R_C are defined in (7)-(9).

It is instructional to first note a few observations about the above outer bound.

1. If we dedicate to generate the private key K_P without considering the secret key K_S, then the model becomes the private key model studied in [5]. The outer bound on R_P is (11), which can be achieved by letting terminal $\mathcal{Z}$ reveal all its information to public. Here terminal $\mathcal{Z}$ is curious but honest, and helps to generate the private key.
2. If we dedicate to generate the secret key K_S without considering the private key K_P, then the model reduces to the secret key model studied in [5]. Correspondingly the above outer bound reduces to $R_S \leq \min\{R_A, R_B, R_C\}$ based on (10), (12) and (13). According to [5], this bound is achievable by applying the "omniscience" scheme, which requires each terminal recover the sources of all three terminals after the public discussion.
3. The sum rate bound (12) can be viewed as a cut-set type bound, because both $\mathcal{X}$ and $\mathcal{Y}$ need to generate two keys K_S and K_P simultaneously.

We next further explain the above outer bound in detail. We note that this outer bound can take three different structures corresponding respectively to the following three cases: **case 1** with $R_B = \min\{R_A, R_B, R_C\}$, **case 2** with $R_C = \min\{R_A, R_B, R_C\}$, and **case 3** with $R_A = \min\{R_A, R_B, R_C\}$.

For case 1, it was shown in [1] that the outer bound (as illustrated in Fig. 2) is achievable. It is clear that the point B with the rate coordinates $(R_B, 0)$ is achievable by applying the "omniscience" scheme in [5] and the point E with the rate coordinates $(0, I(X;Y|Z))$ is achievable by letting $\mathcal{Z}$ reveal all of its information to public. The corner point T with the rate coordinates $(R_B - I(X;Y|Z), I(X;Y|Z))$ is shown to be achievable in [1]. The idea is to let $\mathcal{Z}$ reveal information at rate $R_{\mathcal{Z}} = \max\{H(Z|X), H(Z|Y)\}$ so that both $\mathcal{X}$ and $\mathcal{Y}$ can recover Z^n correctly with probability close to 1. Now Z^n is the information shared by three terminals, and hence the secret key K_S can be generated based on Z^n with rate $R_S = H(Z) - R_{\mathcal{Z}} = \min\{I(X;Z), I(Y;Z)\}$. Then, given Z^n, terminals $\mathcal{X}$ and $\mathcal{Y}$ can generate a private key with rate $R_P = I(X;Y|Z)$ if terminal $\mathcal{X}$ reveals information at rate $R_{\mathcal{X}} = H(X|YZ)$ to terminal $\mathcal{Y}$. Finally, the entire outer bound can be achieved by time-sharing scheme.

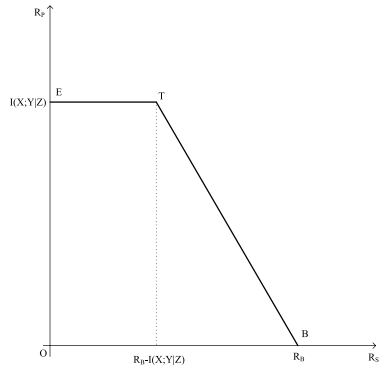

Fig. 2. Out bound for case 1: the quadrangle O-E-T-B-O.

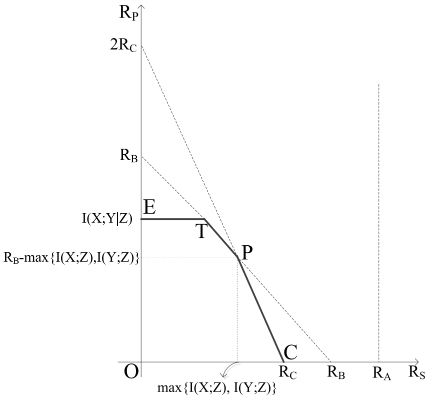

Fig. 3. Outer bound for case 2: the pentagon O-E-T-P-C-O.

In this paper, we show that the outer bound can be achieved for cases 2 and 3. Thus, this outer bound is the SK-PK capacity region in general.

B. Main Theorem

Our main contribution in this paper lies in finding schemes that achieve the outer bound in Theorem 1 for cases 2 and 3. Thus, combined with the result in [1] for case 1, the SK-PK capacity region is established in general. We provide our main result in the following theorem.

Theorem 2: The outer bound in Theorem 1 is achievable for cases 2 and 3, and hence is the SK-PK capacity region for the model given in Section II in general.

We next provide general ideas for the design of achievable schemes for cases 2 and 3. The detailed proof is provided in Sections IV and V.

In case 2, $R_C = \min\{R_A, R_B, R_C\}$. The outer bound in Theorem 1 is plotted in Fig. 3 as the pentagon O-E-T-P-C-O. It has been shown in [1] that the corner points E, T and C are achievable. It is thus sufficient to show that the point P is achievable. Then the entire pentagon can be achieved by time sharing.

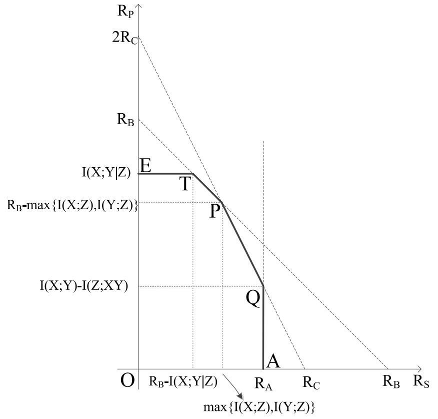

Fig. 4. Outer bound for case 3: the hexagon O-E-T-P-Q-A-O.

We note that the rate coordinates of the point P is

$$\Big(\max\{I(X;Z), I(Y;Z)\}, R_B - \max\{I(X;Z), I(Y;Z)\}\Big).$$

Without loss of generality, we assume that $I(X;Z) > I(Y;Z)$ (the argument for the opposite assumption is similar), and hence $R_B = I(Y;XZ)$ and the point P becomes $(I(X;Z), I(Y;XZ) - I(X;Z))$. The SK rate $R_S = I(X;Z)$ suggests that the highest rate that $\mathcal{Z}$ can transmit publicly is $H(Z|X)$, with which $\mathcal{X}$ can recover Z^n, but $\mathcal{Y}$ cannot recover Z^n. Then $\mathcal{X}$ must transmit some information to help $\mathcal{Y}$ to recover Z^n so that all three terminals can generate a secret key based on Z^n. Furthermore, the information transmitted by terminal $\mathcal{X}$ also helps $\mathcal{Y}$ to recover X^n so that $\mathcal{X}$ and $\mathcal{Y}$ can generate a private key. The critical part of our achievable scheme lies in that terminal $\mathcal{X}$'s transmission should help $\mathcal{Y}$ to recover Z^n without revealing more information about Z^n to public beyond terminal $\mathcal{Z}$'s transmission. Otherwise, the SK rate $R_S = I(X;Z)$ is not achievable. The idea is that $\mathcal{X}$ helps $\mathcal{Y}$ to improve its resolvability of Z^n rather than revealing information about Z^n directly. Section IV-B provides further technical intuition of the achievable scheme based on typicality arguments.

In case 3, $R_A = \min\{R_A, R_B, R_C\}$. The outer bound in Theorem 1 is plotted in Fig. 4 as the hexagon O-E-T-P-Q-A-O. It has been shown in [1] that the corner points E, T and A are achievable. The point P can be achieved by applying the same scheme as in case 2. It is thus sufficient to show that the point Q is achievable. Then the entire hexagon can be achieved by time sharing.

The rate coordinates of the point Q is given by $(I(Z;XY), I(X;Y) - I(Z;XY))$. The SK rate $I(Z;XY)$ suggests that the highest rate that $\mathcal{Z}$ can transmit publicly is $H(Z|XY)$, with which neither $\mathcal{X}$ nor $\mathcal{Y}$ can recover Z^n. Then both $\mathcal{X}$ and $\mathcal{Y}$ must help each other to recover Z^n so that all three terminals can generate a secret key based on Z^n. Furthermore, terminal $\mathcal{Y}$ also helps terminal $\mathcal{X}$ to recover Y^n so that $\mathcal{X}$ and $\mathcal{Y}$ can generate a private key. The critical part lies in that $\mathcal{X}$ and $\mathcal{Y}$'s transmission help each other to recover Z^n without revealing more information about Z^n to public beyond terminal $\mathcal{Z}$'s transmission. Otherwise, the SK rate $R_S = I(Z;XY)$ is not achievable. The idea is that $\mathcal{X}$ and $\mathcal{Y}$ help each other to improve their resolvability of Z^n rather than revealing information about Z^n directly. Section V-B provides further technical intuition of the achievable scheme based on typicality arguments.

IV. Achievability Proof for Case 2

In this section, we provide the achievability proof for case 2 with subsection IV-A containing the technical proof and subsection IV-B containing further intuitive justification.

A. Technical Proof

In this subsection, we show that the outer bound given in Theorem 1 for case 2 is achievable. In this case, $R_C = \min\{R_A, R_B, R_C\}$. The case with $R_C = R_B$ reduces to case 1. Hence, we assume that $R_C < R_B$, where the strict inequality is useful for designing our achievable scheme. This assumption implies the following inequalities:

$$I(X;Z) < I(Y;XZ), \tag{14}$$

$$I(Y;Z) < I(X;YZ). \tag{15}$$

The outer bound for case 2 is plotted in Fig. 3 as the pentagon O-E-T-P-C-O. As we mentioned in Section III-B it has been shown in [1] that the corner points E, T and C are achievable. It is thus sufficient to show that the point P is achievable. Then the entire pentagon can be achieved by time sharing. We note that the rate coordinate corresponding to the point P is $(\max\{I(X;Z), I(Y;Z)\}, R_B - \max\{I(X;Z), I(Y;Z)\})$. Without loss of generality, we assume that

$$I(X;Z) > I(Y;Z), \tag{16}$$

(the following argument can be similarly constructed if $I(X;Z) < I(Y;Z)$). Then $R_B = I(Y;XZ)$ and the point P becomes $(I(X;Z), I(Y;XZ) - I(X;Z))$. Our scheme to achieve point P is based on random binning and joint typicality, given that (14) and (16) hold.

Codebook Generation: At terminal $\mathcal{Z}$, randomly and independently assign a bin index f to each sequence $z^n \in \mathcal{Z}^n$, where $f \in [1 : 2^{nR_{\mathcal{Z}}}]$ with $R_{\mathcal{Z}}$ given by

$$R_{\mathcal{Z}} = H(Z|X) + \epsilon. \tag{17}$$

We use $f(z^n)$ to denote the bin index of the sequence z^n, and use $B_{\mathcal{Z}}(f)$ to denote the bin indexed by f. Then randomly and independently assign a sub-bin index ϕ to each sequence in each nonempty bin $B_{\mathcal{Z}}(f)$, where $\phi \in [1 : 2^{nR_S}]$ with R_S given by

$$R_S = I(X;Z) - 2\delta(\epsilon) - 2\epsilon. \tag{18}$$

We further use $B_{\mathcal{Z}}(f, \phi)$ to denote the sub-bin indexed by ϕ within the bin $B_{\mathcal{Z}}(f)$.

At terminal $\mathcal{X}$, randomly and independently assign a bin index g to each sequence $x^n \in \mathcal{X}^n$, where $g \in [1 : 2^{nR_{\mathcal{X}}}]$ with $R_{\mathcal{X}}$ given by

$$R_{\mathcal{X}} = H(XZ|Y) - H(Z|X). \tag{19}$$

We use $g(x^n)$ to denote the bin index of the sequence x^n, and use $B_{\mathcal{X}}(g)$ to denote the bin indexed by g. Then randomly and independently assign a sub-bin index ψ to each sequence in each nonempty bin $B_{\mathcal{X}}(g)$, where $\psi \in [1 : 2^{nR_P}]$ with R_P given by

$$R_P = I(XZ; Y) - I(X; Z) - 2\delta(\epsilon) - \epsilon. \tag{20}$$

We further use $B_{\mathcal{X}}(g, \psi)$ to denote the sub-bin indexed by ψ within the bin $B_{\mathcal{X}}(g)$.

It can be verified that $R_{\mathcal{X}} < H(X|Z)$ and $R_P > 0$ based on the case assumption (14).

This codebook assignment is known to all parties, i.e., terminals $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ and the eavesdropper.

Encoding and Transmission: Given a sequence z^n, terminal $\mathcal{Z}$ finds the index pair (f, ϕ) such that $z^n \in B_{\mathcal{Z}}(f, \phi)$, and then reveals the index $f = f(z^n)$ over the public channel to all parties, i.e., terminals $\mathcal{X}, \mathcal{Y}$ and the eavesdropper.

Given a sequence x^n, terminal $\mathcal{X}$ finds the index pair (g, ψ) such that $x^n \in B_{\mathcal{X}}(g, \psi)$, and then reveals the index $g = g(x^n)$ over the public channel to all parties, i.e., terminals $\mathcal{Y}, \mathcal{Z}$ and the eavesdropper.

Decoding: The decoding scheme is based on the joint typicality. We use $T_\epsilon^{(n)}(P_{XYZ})$ to denote the strongly joint ϵ-typical set based on the joint distribution P_{XYZ}.

Terminal $\mathcal{X}$, given x^n and the bin index f, claims $\tilde{z}^n$ as recovery of z^n if there exists a unique sequence $\tilde{z}^n \in B_{\mathcal{Z}}(f)$ that satisfies $(\tilde{z}^n, x^n) \in T_\epsilon^{(n)}(P_{XZ})$, or claims decoding failure otherwise.

Terminal $\mathcal{Y}$, given y^n and the bin indexes f and g, claims $(\hat{z}^n, \hat{x}^n)$ as recovery of (z^n, x^n), if there exist a unique pair of sequences $(\hat{z}^n, \hat{x}^n)$ such that $\hat{z}^n \in B_{\mathcal{Z}}(f)$, $\hat{x}^n \in B_{\mathcal{X}}(g)$, and $(\hat{x}^n, \hat{z}^n, y^n) \in T_\epsilon^{(n)}(P_{XYZ})$, or claims decoding failure otherwise.

Due to (16), (17) and (19), it can be verified that $R_{\mathcal{Z}} > H(Z|XY)$, $R_{\mathcal{X}} > H(X|YZ)$ and $R_{\mathcal{X}} + R_{\mathcal{Z}} > H(XZ|Y)$ which implies the following inequalities hold according to the result of distributed source coding problem in [4], [5] and [16]:

$$\Pr\{Z^n \neq \tilde{Z}^n\} < \epsilon, \tag{21}$$

$$\Pr\{X^n \neq \hat{X}^n \textit{ or } Z^n \neq \hat{Z}^n\} < \epsilon. \tag{22}$$

Key Generation: Terminal $\mathcal{Z}$ claims $K_S = \phi(Z^n)$. Terminal $\mathcal{X}$ claims $\tilde{K}_S = \phi(\tilde{Z}^n)$ and $K_P = \psi(X^n)$. Terminal $\mathcal{Y}$ claims $\hat{K}_S = \phi(\hat{Z}^n)$ and $\hat{K}_P = \psi(\hat{X}^n)$. Due to (21) and (22), we have

$$\Pr\{K_S = \tilde{K}_S = \hat{K}_S\} > 1 - \epsilon, \tag{23}$$

$$\Pr\{K_P = \hat{K}_P\} > 1 - \epsilon. \tag{24}$$

Analysis of Secrecy: We evaluate the leakage key rate averaged over the random codebook ensemble. Due to (21) and (22), in order to prove that the secrecy requirements (2) and (3) hold, it is sufficient to show the following two inequalities hold:

$$\frac{1}{n} I(K_S; \mathbf{F}|\mathcal{C}) < \epsilon, \tag{25}$$

$$\frac{1}{n} I(K_P; \mathbf{F}Z^n|\mathcal{C}) < \epsilon. \tag{26}$$

To simplify notations, let $f := f(Z^n)$, and $g := g(X^n)$. Hence f and g are random variables transmitted over the public channel, where the randomness is not only due to random realizations of the source sequences, but also due to random binning assignments (i.e., random codebook generation). It is also clear that the public transmission $\mathbf{F} = \{f, g\}$. We further let $\phi := \phi(Z^n)$ and $\psi := \psi(X^n)$. Hence, $K_P = \psi$ and $K_S = \phi$. Then, we have

$$\begin{aligned} I(K_S; \mathbf{F}|\mathcal{C}) &= I(\phi; f, g|\mathcal{C}) \\ &= I(\phi; f|\mathcal{C}) + I(\phi; g|f, \mathcal{C}) \\ &\leq I(\phi; f|\mathcal{C}) + I(\phi, f; g|\mathcal{C}) \\ &\overset{(a)}{\leq} I(\phi; f|\mathcal{C}) + I(Z^n; g|\mathcal{C}) \end{aligned} \tag{27}$$

where (a) follows from the fact that f and ϕ are determined by Z^n given a codebook $\mathcal{C}$. We further derive

$$\begin{aligned} I(K_P; \mathbf{F}, Z^n|\mathcal{C}) &= I(\psi; f, g, Z^n|\mathcal{C}) \\ &= I(\psi; g, Z^n|\mathcal{C}) \\ &= I(\psi; g|\mathcal{C}) + I(\psi; Z^n|g, \mathcal{C}) \\ &\leq I(\psi; g|\mathcal{C}) + I(\psi, g; Z^n|\mathcal{C}). \end{aligned} \tag{28}$$

We next show that each of the three terms $I(\phi; f|\mathcal{C})$, $I(\psi; g|\mathcal{C})$ and $I(\psi, g; Z^n|\mathcal{C})$ can be arbitrarily small for n large enough. We first consider

$$\begin{aligned} I(\phi; f|\mathcal{C}) &= I(\phi, Z^n; f|\mathcal{C}) - I(Z^n; f|\phi, \mathcal{C}) \\ &= I(Z^n; f|\mathcal{C}) - I(Z^n; f|\phi, \mathcal{C}) \\ &= H(Z^n|\mathcal{C}) - H(Z^n|f, \mathcal{C}) - H(Z^n|\phi, \mathcal{C}) \\ &\quad + H(Z^n|f, \phi, \mathcal{C}). \end{aligned}$$

It is clear that

$$\begin{aligned} H(Z^n|f, \mathcal{C}) &= H(Z^n, f|\mathcal{C}) - H(f|\mathcal{C}) \\ &= H(Z^n|\mathcal{C}) - H(f|\mathcal{C}) \geq H(Z^n|\mathcal{C}) - nR_{\mathcal{Z}}. \end{aligned}$$

Similarly, we have $H(Z^n|\phi, \mathcal{C}) \geq H(Z^n|\mathcal{C}) - nR_S$. Thus,

$$I(\phi; f|\mathcal{C}) \leq n(R_S + R_{\mathcal{Z}} - H(Z)) + H(Z^n|f, \phi, \mathcal{C}) \tag{29}$$

where we used the fact that Z^n is independent from $\mathcal{C}$, and hence $H(Z^n|\mathcal{C}) = nH(Z)$. In order to bound the last term, we introduce the following useful lemma.

Lemma 1: If $R_S + R_{\mathcal{Z}} < H(Z) - 2\delta(\epsilon)$, then

$$\limsup_{n\to\infty} \frac{1}{n} H(Z^n|f, \phi, \mathcal{C}) < H(Z) - R_S - R_{\mathcal{Z}} + \delta(\epsilon)$$

Proof: See Appendix A. □

Following from Lemma 1 and (17) and (18), we have

$$\frac{1}{n} I(\phi; f|\mathcal{C}) < \delta(\epsilon) \tag{30}$$

for sufficiently large n.

Following the same argument for showing (29), we can derive

$$I(\psi; g|\mathcal{C}) \leq n(R_P + R_{\mathcal{X}} - H(X)) + H(X^n|g, \psi, \mathcal{C}) \tag{31}$$

Then using a simple variant of Lemma 1, we show that

$$\frac{1}{n} I(\psi; g|\mathcal{C}) < \delta(\epsilon) \tag{32}$$

for sufficiently large n.

We then consider the term $I(\psi, g; Z^n|\mathcal{C})$ and have

$$\begin{aligned} &I(\psi, g; Z^n|\mathcal{C}) \\ &\quad= I(\psi, g, X^n; Z^n|\mathcal{C}) - I(X^n; Z^n|\psi, g, \mathcal{C}) \\ &\quad= I(X^n; Z^n|\mathcal{C}) - I(X^n; Z^n|\psi, g, \mathcal{C}) \\ &\quad= H(X^n|\mathcal{C}) - H(X^n|Z^n, \mathcal{C}) - H(X^n|\psi, g, \mathcal{C}) \\ &\qquad+ H(X^n|Z^n, \psi, g, \mathcal{C}) \end{aligned}$$

where

$$\begin{aligned} H(X^n|\psi, g, \mathcal{C}) &= H(X^n, \psi, g|\mathcal{C}) - H(\psi, g|\mathcal{C}) \\ &= H(X^n|\mathcal{C}) - H(\psi, g|\mathcal{C}) \\ &\geq H(X^n|\mathcal{C}) - n(R_{\mathcal{X}} + R_P). \end{aligned}$$

Hence,

$$\begin{aligned} &I(\psi, g; Z^n|\mathcal{C}) \\ &\quad\leq n(R_{\mathcal{X}} + R_P - H(X|Z)) + H(X^n|Z^n, \psi, g, \mathcal{C}) \end{aligned}$$

Similarly to Lemma 1, we can show that if

$$R_{\mathcal{X}} + R_P < H(X|Z) - 2\delta(\epsilon), \tag{33}$$

then,

$$\limsup_{n\to\infty} \frac{1}{n} H(X^n|Z^n, \psi, g, \mathcal{C}) < H(X|Z) - R_{\mathcal{X}} - R_P + \delta(\epsilon).$$

Consequently,

$$\frac{1}{n} I(\psi, g; Z^n|\mathcal{C}) < \delta(\epsilon) \tag{34}$$

for sufficiently large n. This also implies that

$$\frac{1}{n} I(g; Z^n|\mathcal{C}) < \delta(\epsilon) \tag{35}$$

for sufficiently large n. Therefore, substituting (30), (32), (34) and (35) into (27) and (28), we show that the leakage rates vanish for large enough n.

Uniformity: Following from [16, Lemma 22.2], we conclude that if $R_S < H(Z) - 4\delta(\epsilon)$, then

$$\liminf_{n\to\infty} \frac{1}{n} H(K_S|\mathcal{C}) \geq R_S - \delta(\epsilon), \tag{36}$$

and if $R_P < H(X) - 4\delta(\epsilon)$, then

$$\liminf_{n\to\infty} \frac{1}{n} H(K_P|\mathcal{C}) \geq R_P - \delta(\epsilon), \tag{37}$$

which prove the uniformity of the two keys.

Existence of a Codebook: We finally note that we have shown that

$$\begin{aligned} &\Pr\{K_S = \tilde{K}_S = \hat{K}_S\} + \Pr\{K_P = \hat{K}_P\} + I(K_S; \mathbf{F}|\mathcal{C}) \\ &\quad+ I(K_P; \mathbf{F}Z^n|\mathcal{C}) + \big[R_S - \frac{1}{n} H(K_S|\mathcal{C})\big] \\ &\quad+ \big[R_P - \frac{1}{n} H(K_P|\mathcal{C})\big] \end{aligned}$$

converges to zero as $n \to \infty$. This implies

$$\begin{aligned} \sum_c \Pr(\mathcal{C} = c)\Big\{ &\Pr\{K_S = \tilde{K}_S = \hat{K}_S\big|\mathcal{C} = c\} \\ &+ \Pr\{K_P = \hat{K}_P\big|\mathcal{C} = c\} + I(K_S; \mathbf{F}|\mathcal{C} = c) \\ &+ I(K_P; \mathbf{F}Z^n|\mathcal{C} = c) \\ &+ \big[R_S - \frac{1}{n} H(K_S|\mathcal{C} = c)\big] \\ &+ \big[R_P - \frac{1}{n} H(K_P|\mathcal{C} = c)\big]\Big\} \end{aligned}$$

converges to zero as $n \to \infty$. Thus, there must exist one codebook $\mathcal{C}$ such that each term converges to zero as $n \to \infty$ due to non-negativity of all terms. Therefore, such a codebook satisfies all requirements simultaneously.

B. Intuitive Justification of Secrecy

In this subsection, we intuitively explain that the generated K_S and K_P satisfy the secrecy requirements (2) and (3).

We first justify that K_S, which is set as $\phi(Z^n)$, is almost independent from the public communication. Firstly, $\phi(Z^n)$, as the sub-bin index, is assigned independently from the bin index $f(Z^n)$, and hence is almost independent from the public transmission by $\mathcal{Z}$. It is then sufficient to justify that ϕ is almost independent of $g(X^n)$ given f. Given g, the bin $B_{\mathcal{X}}(g)$ contains $2^{nI(XZ;Y)}$ typical x^n sequences on average. This implies that there are the same number $2^{n(I(XZ;Y)-I(X;Z))} \geq 1$ of x^n that are jointly typical with any typical z^n in $B_{\mathcal{Z}}(f)$. Hence, the bin index g does not distinguish among z^n within the bin $B_{\mathcal{Z}}(f)$, and hence does not distinguish among $\phi(z^n)$. On the other hand, if the alphabet of g is too large such that $|B_{\mathcal{X}}(g)| < 2^{nI(X;Z)}$, then there must exist some z^n in bin $B_{\mathcal{Z}}(f)$ for which joint typical x^n does not exist in the bin $B_{\mathcal{X}}(g)$. In this case, g reveals some information about z^n, which can suggest exclusion of ϕ indices of those z^n from being the key.

We then justify that K_P, which is set as $\psi(X^n)$, is almost independent from the public communication and Z^n. It is clear that $\psi(X^n)$ is independent from $g(X^n)$. It is then sufficient to justify that ψ is almost independent from Z^n given g. On average, any sub-bin within the bin g contains $2^{nI(X;Z)}$ typical sequences x^n. This implies that there exists one x^n (on average) in each sub-bin that is jointly typical with a typical z^n. Hence, knowing Z^n does not distinguish among sub-bins of x^n. This justifies $\psi(X^n)$ is almost independent from Z^n.

V. Achievability Proof for Case 3

In this section, we provide the achievability proof for case 2 with subsection V-A containing the technical proof and subsection V-B containing further intuitive justification.

A. Technical Proof

In this subsection, we show that the outer bound given in Theorem 1 for case 3 is achievable. In case 3, $R_A = \min\{R_A, R_B, R_C\}$. We note that the case with $R_A < R_B < R_C$ is not possible as pointed out in [1]. Hence, it suffices to consider the case with $R_A \leq R_C \leq R_B$. It is clear that the case with $R_A = R_C \leq R_B$ reduces to case 2. Hence, it suffices to consider $R_A < R_C \leq R_B$, where the strict inequality is useful for designing our achievable scheme. This implies the following inequalities:

$$I(X; Y) > I(Z; XY), \tag{38}$$

$$I(X; Z) \leq I(Y; XZ), \tag{39}$$

$$I(Y; Z) \leq I(X; YZ). \tag{40}$$

The outer bound in Theorem 1 for case 3 is plotted in Fig. 4 as the hexagon O-E-T-P-Q-A-O. It has been shown in [1] that the corner points E, T and A are achievable. The point P can be achieved by the same scheme as in case 2, given that $R_C \leq R_B$. It is thus sufficient to show that the point Q whose rate coordinates are given by $(I(Z;XY), I(X;Y) - I(Z;XY))$, is achievable. Then the entire hexagon can be achieved by time sharing. Our scheme to achieve the point Q is based on random binning and joint typicality.

Codebook Generation: At terminal $\mathcal{Z}$, randomly and independently assign a bin index f to each sequence $z^n \in \mathcal{Z}^n$, where $f \in [1 : 2^{nR_{\mathcal{Z}}}]$ with $R_{\mathcal{Z}}$ given by

$$R_{\mathcal{Z}} = H(Z|XY) + \epsilon + 2\delta(\epsilon). \tag{41}$$

We use $f(z^n)$ to denote the bin index of the sequence z^n, and use $B_{\mathcal{Z}}(f)$ to denote the bin indexed by f. Then randomly and independently assign a sub-bin index ϕ to each sequence in each nonempty bin $B_{\mathcal{Z}}(f)$, where $\phi \in [1 : 2^{nR_S}]$ with R_S given by

$$R_S = I(Z;XY) - 2\epsilon - 4\delta(\epsilon). \tag{42}$$

We further use $B_{\mathcal{Z}}(f,\phi)$ to denote the sub-bin indexed by ϕ within the bin $B_{\mathcal{Z}}(f)$.

At terminal $\mathcal{X}$, randomly and independently assign a bin index g to each sequence $x^n \in \mathcal{X}^n$, where $g \in [1 : 2^{nR_{\mathcal{X}}}]$ with $R_{\mathcal{X}}$ given by

$$R_{\mathcal{X}} = H(X|Y) + \epsilon. \tag{43}$$

We use $g(x^n)$ to denote the bin index of the sequence x^n, and use $B_{\mathcal{X}}(g)$ to denote the bin indexed by g. Then randomly and independently assign a sub-bin index ψ to each sequence in each nonempty bin $B_{\mathcal{X}}(g)$, where $\psi \in [1 : 2^{nR_P}]$ with R_P given by

$$R_P = I(X;Y) - I(Z;XY) - 2\epsilon - 2\delta(\epsilon). \tag{44}$$

We further use $B_{\mathcal{X}}(g,\psi)$ to denote the sub-bin indexed by ψ within the bin $B_{\mathcal{X}}(g)$.

At terminal $\mathcal{Y}$, randomly and independently assign a bin index l to each sequence $y^n \in \mathcal{Y}^n$, where $l \in [1 : 2^{nR_{\mathcal{Y}}}]$ with $R_{\mathcal{Y}}$ given by

$$R_{\mathcal{Y}} = H(Y|X) - 2\delta(\epsilon). \tag{45}$$

We use $l(y^n)$ to denote the bin index of the sequence y^n, and use $B_{\mathcal{Y}}(l)$ to denote the bin indexed by l.

It can be verified that $R_P > 0$ based on the case assumption (38).

This codebook assignment is revealed to all parties, i.e., terminals $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ and the eavesdropper.

Encoding and Transmission: Given a sequence z^n, terminal $\mathcal{Z}$ finds the index pair (f,ϕ) such that $z^n \in B_{\mathcal{Z}}(f,\phi)$, and then reveals the index $f = f(z^n)$ over the public channel to all parties, i.e., terminals $\mathcal{X}, \mathcal{Y}$ and the eavesdropper. Given a sequence x^n, terminal $\mathcal{X}$ finds the index pair (g,ψ) such that $x^n \in B_{\mathcal{X}}(g,\psi)$, and then reveals the index $g = g(x^n)$ over the public channel to all parties, i.e., terminals $\mathcal{Y}, \mathcal{Z}$ and the eavesdropper. Given a sequence y^n, terminal $\mathcal{Y}$ finds the index l such that $y^n \in B_{\mathcal{Y}}(l)$, and then reveals the index $l = l(y^n)$ over the public channel to all parties, i.e., terminals $\mathcal{X}, \mathcal{Z}$ and the eavesdropper.

Decoding: Terminal $\mathcal{X}$, given x^n and the bin indexes f of z^n and l of y^n, claims $(\tilde{z}^n, \tilde{y}^n)$ as recovery of (z^n, y^n) if there exists a unique pair $(\tilde{z}^n, \tilde{y}^n)$ such that $\tilde{z}^n \in B_{\mathcal{Z}}(f)$, $\tilde{y}^n \in B_{\mathcal{Y}}(l)$, and $(\tilde{z}^n, \tilde{y}^n, x^n) \in T_\epsilon^{(n)}(P_{XYZ})$, or claims decoding failure otherwise.

Terminal $\mathcal{Y}$, given y^n and the bin indexes f of z^n and g of x^n, claims $(\hat{z}^n, \hat{x}^n)$ as recovery of (z^n, x^n) if there exists a unique pair $(\hat{z}^n, \hat{x}^n)$ such that $\hat{z}^n \in B_{\mathcal{Z}}(f)$, $\hat{x}^n \in B_{\mathcal{X}}(g)$, and $(\hat{z}^n, \hat{x}^n, y^n) \in T_\epsilon^{(n)}(P_{XYZ})$, or claims decoding failure otherwise.

We further assume that

$$H(Y|X) > H(Y|XZ). \tag{46}$$

The case of equality implies that the point Q coincides with the point P, and can hence be achieved using the scheme given in case 2. Then due to (41), (43) and (45), it can be verified that $R_{\mathcal{Z}} > H(Z|XY)$, $R_{\mathcal{X}} > H(X|YZ)$, $R_{\mathcal{Y}} > H(Y|XZ)$, $R_{\mathcal{X}} + R_{\mathcal{Z}} > H(XZ|Y)$ and $R_{\mathcal{Y}} + R_{\mathcal{Z}} > H(YZ|X)$ hold. It can then be shown that the following inequalities hold, according to the result of distributed source coding problem in [4], [5], and [16]:

$$\Pr\{Z^n \neq \tilde{Z}^n \ or \ Y^n \neq \tilde{Y}^n\} < \epsilon, \tag{47}$$

$$\Pr\{X^n \neq \hat{X}^n \ or \ Z^n \neq \hat{Z}^n\} < \epsilon. \tag{48}$$

Key Generation: Terminal $\mathcal{Z}$ claims $K_S = \phi(Z^n)$. Terminal $\mathcal{X}$ claims $\tilde{K}_S = \phi(\tilde{Z}^n)$ and $K_P = \psi(X^n)$. Terminal $\mathcal{Y}$ claims $\hat{K}_S = \phi(\hat{Z}^n)$ and $\hat{K}_P = \psi(\hat{X}^n)$. Due to (47) and (48), we have

$$\Pr\{K_S = \tilde{K}_S = \hat{K}_S\} > 1 - \epsilon, \tag{49}$$

$$\Pr\{K_P = \hat{K}_P\} > 1 - \epsilon. \tag{50}$$

Analysis of Secrecy: We evaluate the key leakage rates averaged over the random codebook ensemble as follows. We let $l := l(Y^n)$ and now $\mathbf{F} = \{f, g, l\}$. We then derive the following bounds:

$$\begin{aligned} I(K_S;\mathbf{F}|\mathcal{C}) &= I(\phi; f, g, l|\mathcal{C}) \\ &= I(\phi; f|\mathcal{C}) + I(\phi; g, l|f, \mathcal{C}) \\ &\leq I(\phi; f|\mathcal{C}) + I(\phi, f; g, l|\mathcal{C}) \\ &\leq I(\phi; f|\mathcal{C}) + I(Z^n; g, l|\mathcal{C}) \end{aligned} \tag{51}$$

$$\begin{aligned} &I(K_P;\mathbf{F}, Z^n|\mathcal{C}) \\ &\quad = I(\psi; f, g, l, Z^n|\mathcal{C}) \\ &\quad = I(\psi; g, l, Z^n|\mathcal{C}) \\ &\quad = I(\psi; g|\mathcal{C}) + I(\psi; l|g, \mathcal{C}) + I(\psi; Z^n|g, l, \mathcal{C}) \\ &\quad \leq I(\psi; g|\mathcal{C}) + I(\psi, g; l|\mathcal{C}) + I(\psi, g, l; Z^n|\mathcal{C}). \end{aligned} \tag{52}$$

We next show that each of the four terms $I(\phi; f|\mathcal{C})$, $I(\psi; g|\mathcal{C})$, $I(\psi, g; l|\mathcal{C})$ and $I(\psi, g, l; Z^n|\mathcal{C})$ can be arbitrarily small for large enough n. Following the same steps as in case 2 we can show that

$$I(\phi; f|\mathcal{C}) < \delta(\epsilon), \tag{53}$$

$$I(\psi; g|\mathcal{C}) < \delta(\epsilon) \tag{54}$$

for large enough n. We then consider the term $I(\psi, g; l|\mathcal{C})$, and have

$$\begin{aligned}
I(\psi, g; l|\mathcal{C}) &\le I(\psi, g, X^n; l|\mathcal{C})\\
&= I(X^n; l|\mathcal{C})\\
&= I(X^n; l, Y^n|\mathcal{C}) - I(X^n; Y^n|l, \mathcal{C})\\
&= I(X^n; Y^n|\mathcal{C}) - I(X^n; Y^n|l, \mathcal{C})\\
&= H(Y^n|\mathcal{C}) - H(Y^n|X^n, \mathcal{C}) - H(Y^n|l, \mathcal{C})\\
&\quad + H(Y^n|X^n, l, \mathcal{C})\\
&\le H(Y^n|\mathcal{C}) - H(Y^n|X^n, \mathcal{C})\\
&\quad -(H(Y^n|\mathcal{C}) - nR_{\mathcal{Y}}) + H(Y^n|X^n, l, \mathcal{C})\\
&= n(R_{\mathcal{Y}} - H(Y|X)) + H(Y^n|X^n, l, \mathcal{C})
\end{aligned}$$

Similarly to Lemma 1, we can show that if

$$R_{\mathcal{Y}} \le H(Y|X) - 2\delta(\epsilon), \tag{55}$$

then

$$\limsup_{n\to\infty} \frac{1}{n} H(Y^n|X^n, l, \mathcal{C}) < H(Y|X) - R_{\mathcal{Y}} + \delta(\epsilon). \tag{56}$$

Consequently, we obtain

$$\frac{1}{n} I(\psi, g; l|\mathcal{C}) < \delta(\epsilon) \tag{57}$$

for sufficiently large n.

For the term $I(\psi, g, l; Z^n|\mathcal{C})$, we derive the following bound:

$$\begin{aligned}
&I(\psi, g, l; Z^n|\mathcal{C})\\
&= I(\psi, g, l, X^n, Y^n; Z^n|\mathcal{C}) - I(X^n, Y^n; Z^n|\psi, g, l, \mathcal{C})\\
&= I(X^n, Y^n; Z^n|\mathcal{C}) - I(X^n, Y^n; Z^n|\psi, g, l, \mathcal{C})\\
&= H(X^n, Y^n|\mathcal{C}) - H(X^n, Y^n|Z^n, \mathcal{C})\\
&\quad - H(X^n, Y^n|\psi, g, l, \mathcal{C}) + H(X^n, Y^n|Z^n, \psi, g, l, \mathcal{C})\\
&\le H(X^n, Y^n|\mathcal{C}) - H(X^n, Y^n|Z^n, \mathcal{C}) - (H(X^n, Y^n|\mathcal{C})\\
&\quad - n(R_{\mathcal{X}} + R_{\mathcal{Y}} + R_P)) + H(X^n, Y^n|Z^n, \psi, g, l, \mathcal{C})\\
&= n(-H(X, Y|Z) + R_{\mathcal{X}} + R_{\mathcal{Y}} + R_P)\\
&\quad + H(X^n, Y^n|Z^n, \psi, g, l, \mathcal{C})
\end{aligned}$$

Similarly to Lemma 1, we can show that if

$$R_{\mathcal{X}} + R_{\mathcal{Y}} + R_P < H(X, Y|Z) - 2\delta(\epsilon), \tag{58}$$

then,

$$\begin{aligned}
&\limsup_{n\to\infty} \frac{1}{n} H(X^n, Y^n|Z^n, \psi, g, l, \mathcal{C})\\
&\quad < H(X, Y|Z) - R_{\mathcal{X}} - R_{\mathcal{Y}} - R_P + \delta(\epsilon).
\end{aligned} \tag{59}$$

Consequently, we have

$$\frac{1}{n} I(\psi, g, l; Z^n|\mathcal{C}) < \delta(\epsilon) \tag{60}$$

for large enough n. This also implies that

$$\frac{1}{n} I(g, l; Z^n|\mathcal{C}) < \delta(\epsilon) \tag{61}$$

for sufficiently large n. Therefore, substituting (53), (54), (57), (60) and (61) into (51) and (52), we show that the leakage rates vanish for large enough n.

Uniformity: Following from [16, Lemma 22.2], we conclude that if $R_S < H(Z) - 4\delta(\epsilon)$, then

$$\liminf_{n\to\infty} \frac{1}{n} H(K_S|\mathcal{C}) \ge R_S - \delta(\epsilon),$$

and if $R_P < H(X) - 4\delta(\epsilon)$, then

$$\liminf_{n\to\infty} \frac{1}{n} H(K_P|\mathcal{C}) \ge R_P - \delta(\epsilon),$$

which prove the uniformity of the two keys.

Existence of a Codebook: This can be argued in the similar way as for case 2.

B. Intuitive Justification of Secrecy

In this subsection, we intuitively explain that the generated secret and private keys K_S and K_P satisfy the secrecy requirements (2) and (3).

We first justify that K_S, which is set as $\phi(Z^n)$, is almost independent from the public communication. Firstly, it is clear that $\phi(Z^n)$ is almost independent from f. It is then sufficient to justify that $\phi(Z^n)$ is almost independent of $g(X^n)$ and $l(Y^n)$ given $f(Z^n)$. For any given g and l, there are on average $2^{nI(X;Y)}$ jointly typical pairs of (x^n, y^n) such that $(x^n, y^n) \in B_{\mathcal{X}}(g) \times B_{\mathcal{Y}}(l)$. This implies that there are $2^{n(I(X;Y)-I(XY;Z))} \ge 1$ pairs of (x^n, y^n) being jointly typical with any typical z^n in $B_{\mathcal{Z}}(f)$. Hence, the bin indexes g and l do not distinguish among z^n within the bin $B_{\mathcal{Z}}(f)$, and hence do not distinguish among the index ϕ of z^n.

We then justify that K_P, which is set as $\psi(X^n)$, is almost independent from the public communication and Z^n. It is clear that $\psi(X^n)$ is independent from $g(X^n)$. Similarly to case 2, we can argue that ψ is almost independent from the bin index l of Y^n given g. It is then sufficient to justify that ψ is independent from Z^n given l and g. On average, any sub-bin $B_{\mathcal{X}}(g, \psi)$ within the bin $B_{\mathcal{X}}(g)$ contains $2^{nI(XY;Z)}$ typical sequences x^n, and thus for a given l, there are $2^{nI(XY;Z)}$ jointly typical pairs of (x^n, y^n) in each $B_{\mathcal{X}}(g, \psi) \times B_{\mathcal{Y}}(l)$ for any ψ. This implies that there exists one pair (x^n, y^n) (on average) in each $B_{\mathcal{X}}(g, \psi) \times B_{\mathcal{Y}}(l)$ that is jointly typical with a typical z^n. Hence, given l and g, knowing Z^n does not distinguish among sub-bins of x^n. This justifies that, knowing Z^n and the bin index pair (g, l), one does not have preference of determining the sub-bin in which the true X^n lies.

VI. Conclusion

In this paper, we have studied the three-terminal source-type model of simultaneously generating a secret and private key pair. We have shown that random binning and joint decoding schemes achieve an existing outer bound on the SK-PK capacity region established in [1] for two cases. Hence, jointly with the capacity region established in [1] for one case, the SK-PK capacity region for this model is characterized in general. As future work, we will extend this study to more general networks with more than three terminals. We will also apply the idea of our achievable schemes to other multi-key generation source models.

APPENDIX A
PROOF OF LEMMA 1

The proof adapts the [16, proof of Lemma 22.3] with variations. For the sake of completeness, we provide the detail here.

Let

$$E_1 = \begin{cases} 1, & \text{if } Z^n \notin T_\epsilon^{(n)}(P_Z), \\ 0, & \text{otherwise.} \end{cases} \tag{62}$$

Hence $\Pr\{E_1 = 1\} \to 0$ as $n \to \infty$.

We have the following bound:

$$\begin{aligned} & H(Z^n|f,\phi,\mathcal{C}) \\ & \le H(Z^n, E_1|f,\phi,\mathcal{C}) \\ & = H(E_1|f,\phi,\mathcal{C}) + H(Z^n|E_1, f,\phi,\mathcal{C}) \\ & \le 1 + n\Pr\{E_1 = 1\}\log|\mathcal{Z}| + H(Z^n|E_1 = 0, f,\phi,\mathcal{C}) \\ & = 1 + n\Pr\{E_1 = 1\}\log|\mathcal{Z}| \\ & \quad + \sum_{(i,j)} \Big(\Pr\big(f = i, \phi = j \big| E_1 = 0\big) \\ & \qquad \cdot H(Z^n|E_1 = 0, f = i, \phi = j, \mathcal{C}) \Big). \end{aligned} \tag{63}$$

For a given codebook c, let $N(c)$ be the number of sequences $z^n \in B_{\mathcal{Z}}(i,j) \cap T_\epsilon^{(n)}(P_Z)$. Define

$$E_2(\mathcal{C}) = \begin{cases} 1, & \text{if } N(\mathcal{C}) \ge 2\mathrm{E}[N(\mathcal{C})], \\ 0, & \text{otherwise.} \end{cases} \tag{64}$$

Note that $N(\mathcal{C}) \sim Binomial(|T_\epsilon^{(n)}(P_Z)|, 2^{-n(R_S+R_{\mathcal{Z}})})$. Thus,

$$\mathrm{E}[N(\mathcal{C})] = 2^{-n(R_S+R_{\mathcal{Z}})}|T_\epsilon^{(n)}(P_Z)|, \tag{65}$$

$$\mathsf{Var}[N(\mathcal{C})] \le 2^{-n(R_S+R_{\mathcal{Z}})}|T_\epsilon^{(n)}(P_Z)|. \tag{66}$$

By Chebyshev Inequality, we have

$$\begin{aligned} \Pr\{E_2(\mathcal{C}) = 1\} & \le \frac{\mathsf{Var}[N(\mathcal{C})]}{(\mathrm{E}[N(\mathcal{C})])^2} \\ & \le 2^{-n[H(Z)-R_S-R_{\mathcal{Z}}-\delta(\epsilon)]}. \end{aligned} \tag{67}$$

Hence, if $R_S + R_{\mathcal{Z}} \le H(Z) - 2\delta(\epsilon)$, then $\Pr\{E_2(\mathcal{C}) = 1\} \to 0 \;\; as \;\; n \to \infty$. Now,

$$\begin{aligned} & H(Z^n|E_1 = 0, f = i, \phi = j, \mathcal{C}) \\ & = \sum_c H(Z^n|E_1 = 0, f = i, \phi = j, \mathcal{C} = c)\Pr\{\mathcal{C} = c\} \\ & = \sum_{c:E_2(c)=0} H(Z^n|E_1 = 0, f = i, \phi = j, \mathcal{C} = c)\Pr\{\mathcal{C} = c\} \\ & \quad + \sum_{c:E_2(c)=1} H(Z^n|E_1 = 0, f = i, \phi = j, \mathcal{C} = c)\Pr\{\mathcal{C} = c\} \\ & \le \sum_{c:E_2(c)=0} [n(H(Z) - R_S - R_{\mathcal{Z}} + \delta(\epsilon)]\Pr\{\mathcal{C} = c\} \\ & \quad + \sum_{c:E_2(c)=1} (n\log|\mathcal{Z}|)\Pr\{\mathcal{C} = c\} \\ & \le n(H(Z) - R_S - R_{\mathcal{Z}} + \delta(\epsilon)) + n\Pr\{E_2(\mathcal{C}) = 1\}\log|\mathcal{Z}| \end{aligned} \tag{68}$$

Substituting (68) into (63), we conclude that if

$$R_S + R_{\mathcal{Z}} \le H(Z) - 2\delta(\epsilon), \tag{69}$$

then

$$\frac{1}{n}H(Z^n|f,\phi,\mathcal{C}) \le H(Z) - R_S - R_{\mathcal{Z}} + \delta(\epsilon), \;\; as \;\; n \to \infty.$$

ACKNOWLEDGMENT

The authors would like to thank the associate editor and anonymous reviewers for their helpful comments, which helped to improve the presentation of the paper greatly.

REFERENCES

[1] C. Ye and P. Narayan, "The secret key private key capacity region for three terminals," in *Proc. Int. Symp. Inf. Theory (ISIT)*, Adelaide, Australia, Sep. 2005, pp. 2142–2146.

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

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

[4] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471–480, Jul. 1973.

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

[6] U. M. Maurer and S. Wolf, "Unconditionally secure key agreement and the intrinsic conditional information," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 499–514, Mar. 1999.

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

[8] U. M. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels. I. Definitions and a completeness result," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 822–831, Apr. 2003.

[9] U. M. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels-Part II: The simulatability condition," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 832–838, Apr. 2003.

[10] U. M. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels. II. Privacy amplification," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 839–851, Apr. 2003.

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

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

[13] L. Lai and S.-W. Ho, "Simultaneously generating multiple keys and multi-commodity flow in networks," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Lausanne, Switzerland, Sep. 2012, pp. 627–631.

[14] C. Ye, "Information theoretic generation of multiple secret keys," Ph.D. dissertation, Dept. Elect. Eng., Univ. Maryland, College Park, MD, USA, 2005.

[15] U. M. Maurer and S. Wolf, "From weak to strong information-theoretic key agreement," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Sorrento, Italy, Jun. 2000, p. 18.

[16] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

Huishuai Zhang (S'14) received the B.E. degree from University of Science and Technology of China, Hefei, China in 2009 and the M.E. degree from Graduate University of Chinese Academy of Sciences, Beijing, China in 2012. Since Aug. 2012, he has been a Ph.D student at Syracuse University. His research interests focus on information theory and wireless communications.

Lifeng Lai (M'07) received the B.E. and M. E. degrees from Zhejiang University, Hangzhou, China in 2001 and 2004 respectively, and the PhD degree from The Ohio State University at Columbus, OH, in 2007. He was a postdoctoral research associate at Princeton University from 2007 to 2009, and was an assistant professor at University of Arkansas, Little Rock from 2009 to 2012. Since Aug. 2012, he has been an assistant professor at Worcester Polytechnic Institute. Dr. Lai's research interests include information theory, stochastic signal processing and their applications in wireless communications, security and other related areas.

Dr. Lai was a Distinguished University Fellow of the Ohio State University from 2004 to 2007. He is a co-recipient of the Best Paper Award from IEEE Global Communications Conference (Globecom) in 2008, the Best Paper Award from IEEE Conference on Communications (ICC) in 2011 and the Best Paper Award from IEEE Smart Grid Communications (SmartGridComm) in 2012. He received the National Science Foundation CAREER Award in 2011, and Northrop Young Researcher Award in 2012. He served as a Guest Editor for IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, SPECIAL ISSUE ON SIGNAL PROCESSING TECHNIQUES FOR WIRELESS PHYSICAL LAYER SECURITY. He is currently serving as an Editor for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS.

Yingbin Liang (S'01–M'05) received the Ph.D. degree in Electrical Engineering from the University of Illinois at Urbana-Champaign in 2005. In 2005–2007, she was working as a postdoctoral research associate at Princeton University. In 2008–2009, she was an assistant professor at the Department of Electrical Engineering at the University of Hawaii. Since December 2009, she has been on the faculty at Syracuse University, where she is an associate professor. Dr. Liang's research interests include information theory, wireless communications and networks, and machine learning.

Dr. Liang was a Vodafone Fellow at the University of Illinois at Urbana-Champaign during 2003-2005, and received the Vodafone-U.S. Foundation Fellows Initiative Research Merit Award in 2005. She also received the M. E. Van Valkenburg Graduate Research Award from the ECE department, University of Illinois at Urbana-Champaign, in 2005. In 2009, she received the National Science Foundation CAREER Award, and the State of Hawaii Governor Innovation Award. More recently, her paper received the 2014 EURASIP Best Paper Award for the *EURASIP Journal on Wireless Communications and Networking*. She is currently serving as an Associate Editor for the Shannon Theory of the IEEE TRANSACTIONS ON INFORMATION THEORY.

Hua Wang (S'02–M'08) received the Ph.D. degree in Electrical and Computer Engineering from the University of Illinois at Urbana-Champaign in 2007. He is currently a senior staff engineer with Qualcomm Research, Bridgewater, NJ, USA. Dr. Wang's research interests include wireless communications, wireless networking, and information theory.

Dr. Wang was a Vodafone Fellow at the University of Illinois at Urbana-Champaign during 2004-2006, he also received the M. E. Van Valkenburg Graduate Research Award from the ECE Department, University of Illinois at Urbana-Champaign (2007).