On Generating Multiple Keys with Restricted Public Discussion

Wenwen Tu, Mario Goldenbaum, Lifeng Lai, and H. Vincent Poor

***Abstract*—In this paper, the problem of simultaneously generating multiple keys in a model where the key generating parties have restricted access to public discussions is considered. This model is a cascade of a source model and a channel model. It consists of four terminals, i.e., Alice, Bob, Carol and Eve. Alice and Bob are connected via a noiseless channel while Bob connects with Carol and Eve via a wiretap channel. There is no direct link connecting Alice with Carol or Eve, hence Carol and Eve do not have direct access to the discussion between Alice and Bob. Alice wishes to share a secret key with Carol while Bob wishes to share another independent secret key with Carol. This model incorporates many classical models as special cases, and we provide inner and outer bounds on the corresponding secret-key capacity region. And under some important special cases where certain Markov chain relationships hold, we provide inner and outer bounds that match, thus fully characterize the secret-key capacity region.**

***Index Terms*—Correlated sources, multiple key generation, public discussion, source-channel model, wiretap channel.**

I. Introduction

Enabling multiple terminals to generate a common secret key plays an important role in information-theoretic security [2]–[6]. Recently, as an important and natural extension, the problem of simultaneously generating multiple keys has received considerable attention [7]–[11].

The paradigm of secret key generation via public discussion is typically investigated either from a source or a channel perspective [12]–[18]. Under the source model, the legitimate terminals have access to correlated random sequences, based on which they are able to share a secret key via exchanging messages over a public noiseless channel that is fully accessible to an eavesdropper [2], [3], [5], [6]. While under the channel model, the legitimate terminals typically have no access to correlated random sequences, but they can exploit differences in channel statistics to generate a secret key [4], [19]–[21].

The work of W. Tu and L. Lai was supported in part by National Science Foundation under Grants CCF-1665073, ECCS-1660140 and CNS-1824553. The work of M. Goldenbaum was supported in part by the German Research Foundation (DFG) under Grant GO 2669/1-1. The work of H. V. Poor was supported in part by National Science Foundation under Grants CCF-093970 and CCF-1513915. This paper was presented in part at the IEEE Conference on Communications and Network Security, Workshop on Physical-Layer Methods for Wireless Security, Philadelphia, PA, Oct. 2016 [1].

W. Tu and L. Lai are with the Department of Electrical and Computer Engineering, University of California, Davis, CA 95616 USA (e-mail: wwtu@ucdavis.edu; lflai@ucdavis.edu).

M. Goldenbaum and H. V. Poor are with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: goldenbaum@princeton.edu; poor@princeton.edu).

In addition, it is commonly assumed in most of the existing works on key generation that the public discussion is accessible to all terminals. This assumption simplifies the model and facilitates the derivation of exact key capacity results. However, in practice, this assumption may not always be valid. For example, in key generation for wireless networks [16], [22], [23], the public discussion needs to be carried out through wireless channels. Hence, users that are far away from the transmitter may not be able to receive the public discussion directly.

In our recent works [24] and [25], we made an initial attempt to understand the key generation problem in a joint source-channel model without the above-mentioned assumption. In the considered model therein, there are three legitimate terminals (say Alice, Bob and Carol), where Alice and Bob are connected via a noiseless link. Bob and Carol, on the other hand, are connected via a wiretap channel in the presence of an eavesdropper Eve. There is no direct link between Alice and Carol, thus the discussion between Alice and Bob is not accessible to Carol. But we assumed Eve could observe the messages exchanged over the noiseless link for the sake of strong secrecy. In this model, Alice and Bob would like to share two individual secret keys with Carol, and we provided a single-letter characterization of the corresponding secret-key capacity region.

However, there are many practical scenarios in which it is practically very difficult for Eve to overhear the discussion over the noiseless link between Alice and Bob (e.g., a fiber optical cable). Thus, in this paper we make a nontrivial extension to the model considered in [24] and [25] by further restricting Eve to not having access to the discussion channel between Alice and Bob. More specifically, Alice and Bob wish to agree with Carol on two individual secret keys. Alice and Bob are connected via a noiseless channel while Bob connects with Carol in the presence of Eve via a wiretap channel. There is no direct link connecting Alice with Carol or Eve, hence Carol and Eve do not have direct access to the discussion between Alice and Bob. Under this model, we investigate the corresponding secret-key capacity region of these two keys.

To facilitate understanding, we first study the case when Eve has no side information, and we provided both an inner and an outer bounds on the secret-key capacity region. We show that these two bounds match if a certain Markov chain relationship holds. Compared with the result obtained in [25], the capacity region is enlarged. This is mainly due to the fact that Eve cannot observe the discussion between Alice and Bob. We design a scheme to show that Alice is able to transfer partial

secret key information to Bob. Utilizing this secret information from Alice, Bob is able to generate a key at a larger rate. In other words, the rate of the key shared by Bob and Carol can be increased by partially sacrificing the rate of the key shared by Alice and Carol. We then consider the more general case in which Eve has side information, and also provide inner and outer bounds on the corresponding secret-key capacity region. For the important special case that the sources and channels fulfill two specific Markov chain conditions, we refine these two bounds and fully characterize the corresponding capacity region.

As mentioned above, this paper is related to two of our recent works [1], [25]. [1] is a conference version of this paper: it presents the results of the special case when Eve has no side information. We extend the results in [1] by adding the results of the more general and interesting case where Eve has side information in this journal version. Furthermore, the model studied in this paper is related to the model considered in [25]. The main difference is that, in this paper, we assume that Eve can only observe the output of the wiretap channel, while Eve is also allowed to have access to the public discussion between Alice and Bob in [25]. This model difference makes the problem considered in this paper different from and significantly more challenging than the problem considered in [25].

The remainder of the paper is organized as follows. The problem setup is described in Section II. In Section III, we present our main results while the corresponding proofs are provided in Appendices. Finally, we offer our concluding remarks in Section IV.

II. Problem Setup

Two terminals, Alice and Bob wish to share with terminal Carol two independent secret keys K_1 and K_2. K_1 is required to be secure from Bob while K_2 has to be secure from Alice. Furthermore, (K_1, K_2) needs to be kept confidential from an eavesdropper Eve. Alice and Bob are connected via a noiseless channel while Bob is connected with Carol via a wiretap channel in the presence of Eve. The wiretap channel is modeled as $P_{YZ|X}(\mathcal{Y}, \mathcal{Z}|\mathcal{X})$, where $\mathcal{X}, \mathcal{Y}$ and $\mathcal{Z}$ denote the channel input and output alphabets. However, there are no direct links between Alice, Carol, and Eve. The system model is illustrated in Fig. 1.

The link between Alice and Bob is two-way, and they are allowed to exchange messages over it. The assumption that there is no direct link between Alice, Carol and Eve above means that Carol and Eve do not have access to the discussion occurred between Alice and Bob. This is the main difference between our work and the existing work that assume every party has access to the discussion. On the other hand, the wiretap channel between Bob and Carol is one-way. Since Eve can only observe the output of the wiretap channel, the messages exchanged over the noiseless link are secure from Eve. Alice, Carol and Eve are assumed to have access to correlated sequences U^N, V^N and W^N in advance,

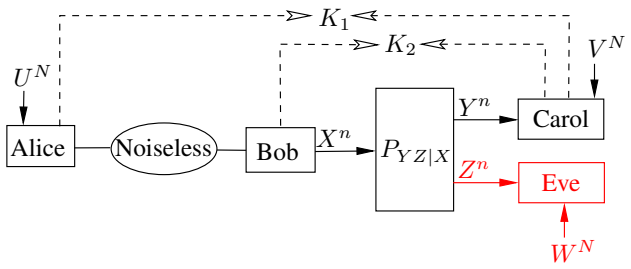

Fig. 1. System model.

and (U^N, V^N, W^N) are generated according to a given joint probability mass function

$$P_{U^N V^N W^N}(u^N, v^N, w^N) = \prod_{i=1}^{N} P_{UVW}(u_i, v_i, w_i), \qquad (1)$$

where U, V and W take values from the alphabets $\mathcal{U}, \mathcal{V}$ and $\mathcal{W}$, respectively.

At the beginning of communication, Alice generates local randomness F_A and Bob generates F_B. Then, Alice and Bob take turns to exchange messages with each other. The transmitted messages from Alice are functions of U^N, F_A and all previously received messages from Bob (when starting the communication it is $\emptyset$), and the transmitted messages from Bob are generated in a similar manner. After the discussion between Alice and Bob ends, Bob transmits a sequence X^n over the wiretap channel that is a function of $\mathbf{F}$ and F_B, where $\mathbf{F}$ summarizes all the messages exchanged between Alice and Bob. On the other hand, at the end of the discussion Alice computes K_1 as a function of $(U^N, F_A, \mathbf{F})$, Bob generates K_2 as a function of $(F_B, \mathbf{F})$ and Carol generates two keys K_1' and K_2' as functions of (Y^n, V^N).

Definition 1. *A rate-pair (R_1, R_2) is said to be achievable if for any given $\epsilon > 0$ there exists an $n(\epsilon) \in \mathbb{N}$ such that for all $n \geq n(\epsilon)$ there exists a scheme that fulfills*

$$\Pr\{K_i \neq K_i'\} \leq \epsilon, \quad i = 1, 2, \qquad (2)$$

$$\frac{1}{n} I(K_1; F_B, \mathbf{F}) \leq \epsilon, \qquad (3)$$

$$\frac{1}{n} I(K_2; U^N, F_A, \mathbf{F}) \leq \epsilon, \qquad (4)$$

$$\frac{1}{n} I(K_1, K_2; Z^n, W^N) \leq \epsilon, \qquad (5)$$

$$\frac{1}{n} H(K_i) \geq \frac{1}{n} \log |K_i| - \epsilon, \quad i = 1, 2, \qquad (6)$$

$$\frac{1}{n} H(K_1) \geq R_1 - \epsilon, \ \frac{1}{n} H(K_2) \geq R_2 - \epsilon. \qquad (7)$$

Here, (2) indicates that the keys generated at the corresponding key sharing parties should be the same with high probability. Furthermore, (3) means that the generated key K_1 is secure from Bob, (4) implies that the generated key K_2 is secure from Alice and K_1 and K_2 are independent, and (5) implies that (K_1, K_2) should be jointly secure from Eve. In addition, (6) requires that the generated keys should be nearly

uniformly distributed, and (7) indicates that R_1 and R_2 are two achievable key rates of K_1 and K_2, respectively.

Definition 2. *The secret-key capacity region $\mathcal{C}$ is defined as*

$$\mathcal{C} \triangleq \big\{(R_1, R_2) \in \mathbb{R}_+^2 \,|\, (R_1, R_2) \text{ is achievable}\big\},$$

and

$$C_1 \triangleq \sup_{(R_1,R_2)\in\mathcal{C}} R_1,\ C_2 \triangleq \sup_{(R_1,R_2)\in\mathcal{C}} R_2.$$

In the following, our goal is to find a single-letter characterization of the secret-key capacity $\mathcal{C}$.

III. Main Results

In this section, we first focus on the case when Eve has no side information, i.e. $\mathcal{W} = \emptyset$. Then, we consider the case when Eve has side information. In both cases, we provide corresponding inner and outer bounds on the secret-key capacity region. In the case with no side information, we show that the inner bound and the outer bound match if a certain Markov chain condition holds; and in the case with side information, we refine the obtained outer bound, providing a matching characterization on the capacity region if two certain Markov chain conditions hold. For notational convenience, we let $\beta \triangleq n/N$.

A. No Side Information at Eve

For auxiliary random variables S_1, S_2 and T_2 satisfying $S_1 \to U \to V$ and $T_2 \to S_2 \to X \to (Y, Z)$, we define

$$\mathcal{R}_1^o(P_{S_1|U}, P_{T_2|S_2}P_{S_2X}) \triangleq \Big\{(R_1, R_2) \in \mathbb{R}_+^2 :$$

$$R_1 \le \frac{1}{\beta} I(S_1; V), \tag{8}$$

$$R_2 \le I(S_2; Y) - \frac{1}{\beta}[I(S_1; U) - I(S_1; V)], \tag{9}$$

$$R_1 + R_2 \le \frac{1}{\beta} I(S_1; V) + \big[I(S_2; Y|T_2) - I(S_2; Z|T_2)\big]^+\Big\}. \tag{10}$$

Note that (9) implies that $[I(S_1; U) - I(S_1; V)] \le \beta I(S_2; Y)$. In addition, we define

$$\mathcal{R}_2^o(P_{S_1|U}, P_X) \triangleq \Big\{(R_1, R_2) \in \mathbb{R}_+^2 :$$

$$R_1 \le \frac{1}{\beta} I(S_1; V), \tag{11}$$

$$R_2 \le I(X; Y) - \frac{1}{\beta}[I(S_1; U) - I(S_1; V)], \tag{12}$$

$$R_1 + R_2 \le \frac{1}{\beta} I(S_1; V) + I(X; Y|Z)\Big\}. \tag{13}$$

In this case, we denote the secret-key capacity region by $\mathcal{C}^o$, and C_1^o and C_2^o are denoted in a similar manner. Then, we have the following result.

Theorem 1. *$\mathcal{R}_1^o(P_{S_1|U}, P_{T_2|S_2}P_{S_2X})$ is an achievable secret-key rate region, and an inner bound on $\mathcal{C}^o$ is given by*

$$\mathcal{R}_{\text{in}}^o = \bigcup_{P_{S_1|U}, P_{T_2|S_2}P_{S_2X}} \mathcal{R}_1^o(P_{S_1|U}, P_{T_2|S_2}P_{S_2X}). \tag{14}$$

Proof: (Outline) We will generate $2^{N(I(S_1;U)+\epsilon)}$ sequences U^N at Alice's side, and ask Bob to use partial sequence of X^n to convey Alice's message to Carol, so that Carol can share a common secret randomness of rate $I(S_1; V) - \epsilon$, with Alice. Then, Alice splits the common secret randomness into two parts: one as the secret key K_1, and the other one is released to Bob so that Bob can use it to generate a key with rate larger than $I(S_2; Y|T_2) - I(S_2; Z|T_2) - \epsilon$, with Carol (note that $I(S_2; Y|T_2) - I(S_2; Z|T_2) - \epsilon$ is the largest rate Bob can share with Carol if no secret randomness is provided to Bob, given $P_{T_2|S_2}P_{S_2X}$). Meanwhile, Bob will use a distillation method so that the generated key K_2 is also independent with the secret randomness provided by Alice. For detailed proof, please refer to Appendix A. ∎

Theorem 1 implies that

$$C_2^o \ge \max_{\substack{P_{S_1|U},\\ P_{T_2|S_2}P_{S_2X}}} \min\Big\{I(S_2; Y) - \frac{1}{\beta}[I(S_1; U) - I(S_1; V)],$$
$$\frac{1}{\beta} I(S_1; V) + I(S_2; Y|T_2) - I(S_2; Z|T_2)\Big\}. \tag{15}$$

The right-hand side of (15) is larger than $\max_{P_{S_2X}}\{I(S_2; Y) - I(S_2; Z)\}$, which is obvious by setting $S_1 = \emptyset$ and $T_2 = \emptyset$. This result indicates that the existence of (U^N, V^N) indeed helps Bob in increasing the rate of K_2, which is in contrast to [24, Cor. 2]. The main reason is that, in the model considered in this paper, Eve cannot observe the discussion between Alice and Bob, and hence Alice can send partial information of U^N to Bob, which Bob can use to further confuse Eve and increase the key rate of K_2.

Theorem 2. *An outer bound on $\mathcal{C}^o$ is given by*

$$\mathcal{R}_{\text{out}}^o = \bigcup_{P_{S_1|U}, P_X} \mathcal{R}_2^o(P_{S_1|U}, P_X). \tag{16}$$

And if the wiretap channel is degraded (i.e., $X \to Y \to Z$ forms a Markov chain in that order), $\mathcal{C}^o$ is given by

$$\mathcal{C}^o = \bigcup_{P_{S_1|U}, P_X} \mathcal{R}_2^o(P_{S_1|U}, P_X). \tag{17}$$

Proof: The proof of the first part (16) is postponed to Appendix B. Here, we only show the second part, i.e., the proof of (17).

It suffices to show that given any $(P_{S_1|U}, P_X)$, $\mathcal{R}_2^o(P_{S_1|U}, P_X)$ is achievable under the Markov chain $X \to Y \to Z$.

By setting $S_2 = X$ and $T_2 = \emptyset$, we have that (12) is equivalent to (9), and

$$\begin{aligned} I(S_2; Y|T_2) - I(S_2; Z|T_2) &= I(X; Y) - I(X; Z) \\ &= I(X; Y|Z), \end{aligned}$$

which indicates that (10) and (13) are equivalent. Thus

$$\mathcal{R}_2^o(P_{M|U}, P_X) = \mathcal{R}_1^o(P_{M|U}, P_X),$$

and $\mathcal{R}_1^o(P_{M|U}, P_X)$ is achievable according to Theorem 1. This completes the proof of the second part. ∎

From Theorem 2, we can conclude that C_2^o is upper-bounded by

$$C_2^o \le \max_{P_{S_1|U},P_X} \min\Big\{\frac{1}{\beta}I(S_1;V)+I(X;Y|Z), \\ I(X;Y)-\frac{1}{\beta}[I(S_1;U)-I(S_1;V)]\Big\} \quad (18)$$

in general. We have the following corollary.

Corollary 1. *If the wiretap channel between Bob, Carol and Eve is degraded (i.e., $X \to Y \to Z$), then*

$$C_2^o = \max_{P_{S_1|U},P_X} \min\Big\{\frac{1}{\beta}I(S_1;V)+I(X;Y|Z), \\ I(X;Y)-\frac{1}{\beta}[I(S_1;U)-I(S_1;V)]\Big\}. \quad (19)$$

Furthermore, taking both Theorems 1 and 2 into consideration, we have the following corollary.

Corollary 2.

$$C_1^o = \max_{S_1-U-V} \frac{1}{\beta}I(S_1;V) \\ \text{s.t.} \quad I(S_1;U)-I(S_1;V) \le \max_{P_X}\beta I(X;Y). \quad (20)$$

Corollary 2 shows that if we only focus on K_1, the channel between Alice and Carol can be viewed as a noiseless channel with rate constraint $R = \max_{P_X}\beta I(X;Y)$, in which case the result is consistent with [24, Cor. 1].

B. Eve Has Side Information

In this subsection, we consider the more general case when Eve has side information that is correlated with U^N and V^N, i.e., $\mathcal{W} \neq \emptyset$.

For auxiliary random variables S_1, T_1, S_2 and T_2 satisfying $T_1 \to S_1 \to U \to (V,W)$ and $T_2 \to S_2 \to X \to (Y,Z)$, we define

$$\mathcal{R}_1(P_{T_1|S_1}P_{S_1|U}, P_{T_2|S_2}P_{S_2X}) \triangleq \Big\{(R_1,R_2)\in\mathbb{R}_+^2 : \\ R_1 \le \frac{1}{\beta}I(S_1;V), \quad (21)$$

$$R_1 \le \frac{1}{\beta}[I(S_1;U)-I(S_1;W)] \quad (22)$$

$$R_2 \le I(S_2;Y)-\frac{1}{\beta}[I(S_1;U)-I(S_1;V)], \quad (23)$$

$$R_1+R_2 \le \frac{1}{\beta}[I(S_1;V|T_1)-I(S_1;W|T_1)]^+ \\ +\big[I(S_2;Y|T_2)-I(S_2;Z|T_2)\big]^+\Big\}, \quad (24)$$

and

$$\mathcal{R}_2(P_{T_1|S_1}P_{S_1|U}, P_X) \triangleq \Big\{(R_1,R_2)\in\mathbb{R}_+^2 : \\ R_1 \le \frac{1}{\beta}I(S_1;V), \quad (25)$$

$$R_1 \le \frac{1}{\beta}H(U|W), \quad (26)$$

$$R_2 \le I(X;Y)-\frac{1}{\beta}[I(S_1;U)-I(S_1;V)], \quad (27)$$

$$R_1+R_2 \le \frac{1}{\beta}[I(S_1;V|T_1)-I(S_1;W|T_1)]^+ \\ +I(X;Y|Z)\Big\}. \quad (28)$$

Then, we have the following result.

Theorem 3. *$\mathcal{R}_1(P_{T_1|S_1}P_{S_1|U}, P_{T_2|S_2}P_{S_2X})$ is an achievable secret-key rate region, and an inner bound on $\mathcal{C}$ is given by*

$$\mathcal{R}_{\text{in}} = \bigcup_{\substack{P_{T_1|S_1}P_{S_1|U},\\ P_{T_2|S_2}P_{S_2X}}} \mathcal{R}_1(P_{T_1|S_1}P_{S_1|U}, P_{T_2|S_2}P_{S_2X}). \quad (29)$$

Proof: (Outline) The main idea to design a coding scheme to show the validity of this inner bound follows that in the proof of Theorem 1. That is, Alice sends out two messages to Bob, one is intended for Carol so that she can use it to decode the sequence S_1^N, and the other one serves as transfering partial secret-key information of K_1 to Bob. Then, Bob uses a short sequence $S_2^{n_1}$ to convey the message from Alice to Carol and utilizes another sequence $S_2^{n_2}$, where $n = n_1 + n_2$, so that Alice and Bob can share certain common randomnesses with Carol. Finally, Alice, Bob and Carol will distill keys from these randomnesses. Detailed proof is provided in Appendix C. ∎

We note that, from Corollary 2, the wiretap channel between Bob and Carol acts as a noiseless relay with rate constraint $R = \max_{P_X} I(X;Y)$ to Alice and Carol in the case of $\mathcal{W} = \emptyset$. And compared with that of the real noiseless channel with the same rate constraint, the existence of this relay does not help in increasing the key capacity of K_1. However, the situation is different in the case of $\mathcal{W} \neq \emptyset$. In this case, we can see, from Theorem 3, that

$$C_1 \ge \max_{\substack{P_{T_1|S_1}P_{S_1|U},\\ P_{T_2|S_2}P_{S_2X}}} \min\Big\{\frac{1}{\beta}I(S_1;V), \frac{1}{\beta}[I(S_1;U)-I(S_1;W)], \\ \frac{1}{\beta}[I(S_1;V|T_1)-I(S_1;W|T_1)]+\big[I(S_2;Y|T_2)-I(S_2;Z|T_2)\big]^+\Big\} \\ \text{s.t.} \quad I(S_1;U)-I(S_1;V) \le \beta I(S_2;Y),$$

which is larger than that in [6]:

$$\max_{P_{T_1|S_1}P_{S_1|U},P_X} \frac{1}{\beta}[I(S_1;V|T_1)-I(S_1;W|T_1)] \\ \text{s.t.} \quad I(S_1;U)-I(S_1;V) \le \beta I(S_2;Y).$$

Thus, we can conclude that the wiretap channel indeed helps in increasing the key capacity of K_1. Furthermore, we can also obtain a similar lower bound on C_2 as that in (15).

Theorem 4. *An outer bound on $\mathcal{C}$ is given by*

$$\mathcal{R}_{\text{out}} = \bigcup_{P_{T_1|S_1}P_{S_1|U},P_X} \mathcal{R}_2(P_{T_1|S_1}P_{S_1|U}, P_X). \tag{30}$$

Proof: Please refer to Appendix D for details. ∎

The above inner bound $\mathcal{R}_{\text{in}}$ and the outer bound $\mathcal{R}_{\text{out}}$ do not match in general, but under the conditions that the wiretap channel is degraded and that $U \to V \to W$, the outer bound R_{out} can be refined to match the inner bound R_{in}.

Theorem 5. *If the wiretap channel is degraded (i.e., $X \to Y \to Z$) and the Markov chain condition $U \to V \to W$ holds, we have that*

$$\mathcal{C} = \bigcup_{P_{S_1|U},P_X} \mathcal{R}(P_{S_1|U}, P_X), \tag{31}$$

where $\mathcal{R}(P_{S_1|U}, P_X)$ is defined as

$$\begin{aligned}
\mathcal{R}(P_{S_1|U}, P_X) \triangleq \Big\{&(R_1, R_2) \in \mathbb{R}_+^2 : \\
&R_1 \le \frac{1}{\beta} I(S_1; V), && (32)\\
&R_1 \le \frac{1}{\beta}[I(S_1; U) - I(S_1; W)] && (33)\\
&R_2 \le I(X; Y) - \frac{1}{\beta}[I(S_1; U) - I(S_1; V)], && (34)\\
&R_1 + R_2 \le \frac{1}{\beta}[I(S_1; V) - I(S_1; W)] + I(X; Y|Z)\Big\}. && (35)
\end{aligned}$$

Proof: Please refer to Appendix E for details. ∎

Intuitively, given an auxiliary random variable S_1, (32) reflects the upper bound on the rate of K_1 that can be made secure from Bob, and (33) represents the bound due to that K_1 is required to be confidential from Eve. The bound defined in (34) indicates that with the assistance of Alice, the key rate of K_2 can be potentially enlarged (note that if there is no Alice, the key capacity is $\max_{P_X} I(X; Y|Z)$ [3]), but in order to use the information contained in S_1, Bob needs to partially sacrifice information in X to convey the information of S_1 to Carol. And (35) reflects that fact that both K_1 and K_2 should be kept secure from Eve.

Furthermore, under the conditions $X \to Y \to Z$ and $U \to V \to W$, we can also obtain single-letter characterizations of C_1 and C_2 (see Theorem 5).

Corollary 3. *If the wiretap channel is degraded (i.e., $X \to Y \to Z$) and $U \to V \to W$ holds, we have that*

$$\begin{aligned}
C_1 = \max_{P_{S_1|U},P_X} \min \Big\{&\frac{1}{\beta} I(S_1; V), \frac{1}{\beta} I(S_1; U|W), \\
&\frac{1}{\beta} I(S_1; V|W) + I(X; Y|Z)\Big\} \\
\textit{s.t.}\quad & I(S_1; U) - I(S_1; V) \le \beta I(X; Y)
\end{aligned}$$

and

$$C_2 = \max_{P_{S_1|U},P_X} \min \left\{ I(X; Y) - \frac{1}{\beta} I(S_1; U|V), \frac{1}{\beta} I(S_1; V|W) + I(X; Y|Z) \right\}.$$

If we only care about C_1, the noisy channel can be taken as a noiseless channel with rate constraint $R \le I(X; Y)$. However, compared with the forward capacity in the noiseless channel with rate constraint [6]:

$$\begin{aligned}
&\max_{P_{S_1|U}} \frac{1}{\beta} I(S_1; V|W), \\
\text{s.t.}\quad &\frac{1}{\beta}\left[I(S_1; U) - I(S_1; V)\right] \le I(X; Y),
\end{aligned}$$

C_1 is increased, which is due to the fact that with the help from Bob, the message transmitted over the noisy channel is partially masked, thus Eve only observes partial public discussion from Alice to Carol. On the other hand, if we only care about C_2, it is also enlarged, compared with the case without help from Alice: $\max_{P_X} I(X; Y|Z)$, the reason is that Bob can utilize the information from Alice to further confuse Eve.

IV. Conclusion

We have considered a new variation of the problem of simultaneously generating multiple secret keys with restricted public discussion and have compared the obtained results with related results known from the literature. More specifically, we have first studied the case in which an eavesdropper has no side information and provided both inner and outer bounds on the corresponding key capacity region. The inner and outer bounds coincide if the wiretap channel is physically degraded. Then, we have considered the more general case in which the eavesdropper has side information and also provided single-letter inner and outer bounds on the key capacity region. Finally, these bounds were refined in such a way that under the assumption certain Markov chain conditions are fulfilled lead to a full characterization of the secret-key capacity region.

Appendix A
Proof of Theorem 1

For the convenience of presentation, we assume $T_2 = \emptyset$ since the case with $T_2 \neq \emptyset$ is straight forward following a similar scheme as follows. Thus, we show that given $(P_{S_1|U}, P_{S_2X})$, for any $(R_1, R_2) \in \mathcal{R}_1^o(P_{S_1|U}, P_{S_2X})$ there exists a scheme such that (R_1, R_2) is achievable. Towards this end, we propose a novel key generation scheme. For simplicity of notation, we assume $\beta = 1$, i.e. $N = n$. It suffices to show that the pair $(R_1, \min\{I(S_2; Y) - I(S_2; Z) + \tilde{R}_1, I(S_2; Y) - I(S_1; U) + I(S_1; V)\} - \epsilon)$ with $R_1 + \tilde{R}_1 = I(S_1; V) - \epsilon$ is achievable.

The novel scheme consists of two phases: Key Agreement and Key Distillation.

Phase I: **Key Agreement**.

Codebook generation: *Codebook at Alice $\mathcal{C}_A$.* Given $P_{S_1|U}P_{UV}$, randomly and independently generate 2^{nR_0} sequences S_1^n, according to $\prod_{i=1}^n P_{S_1}(S_{1i})$, and randomly assign to each sequence three indices (f, ϕ_1, ϕ_2) with $f \in [1 : 2^{nR_{00}}], \phi_1 \in [1 : 2^{nR_{01}}], \phi_2 \in [1 : 2^{nR_{02}}]$ being independently

and uniformly distributed. Here, for some arbitrarily small $\epsilon > 0$, we set

$$R_0 = I(S_1;U) + \epsilon,\ R_{00} = I(S_1;U) - I(S_1;V) + 2\epsilon,$$
$$R_{01} + R_{02} = R_0 - R_{00} = I(S_1;V) - \epsilon.$$

Codebook at Bob $\mathcal{C}_B$. Split the number n as summation of $n_1 + n_2$ with $n_1 = nR_{00}/R_{10}$. Given $P_{S_2X}P_{YZ|X}$, first randomly and independently generate $2^{n_1R_{10}}$ sequences $S_2^{n_1}$, according to $\prod_{i=1}^{n_1} P_{S_2}(S_{2i})$, and randomly assign each sequence an index pair (f_1, f_2) with $f_1 \in [1 : 2^{n_1R_{11}}]$ and $f_2 \in [1 : 2^{n_1R_{12}}]$ being independently and uniformly distributed. Then, randomly and independently generate $2^{n_2R_{10}+nR_{01}}$ sequences $S_2^{n_2}$, according to $\prod_{i=1}^{n_2} P_{S_2}(S_{2i})$, and randomly assign each sequence three indices (ϕ_1, φ, ψ) with $\varphi \in [1 : 2^{n_2R_{11}}]$ and $\psi \in [1 : 2^{n_2R_{12}}]$ being independently and uniformly distributed. Here,

$$R_{10} = I(S_2;Y) - \epsilon,\ R_{11} = I(S_2;Y) - I(S_2;Z) - 2\epsilon,$$
$$R_{12} = R_{10} - R_{11} = I(S_2;Z) + \epsilon.$$

We use $S_1^n(f, \phi_1, \cdot)$ to denote the bin of all S_1^n sequences with the same index (f, ϕ_1), and use similar notation for the other sequences, e.g., $S_2^{n_1}(f_1, \cdot)$. Due to the fact that the cardinality of the set of indices (f_1, f_2) equals that of the set of indices f, we can define a bijective mapping between f and (f_1, f_2). Without loss of generality, we assume $f = (f_1, f_2)$.

Encoding: Having observed U^n, Alice looks into $\mathcal{C}_A$, and tries to find a sequence S_1^n that is jointly typical according to P_{S_1U}. If there are more than one such sequence, randomly select one of them; if there is no such sequence, randomly select one sequence S_1^n from all possible sequences. Then, Alice transmits the indices $(f(S_1^n), \phi_1(S_1^n))$ to Bob.

Upon receiving (f, ϕ_1), Bob looks into $\mathcal{C}_B$, selecting the sequence $S_2^{n_1}(f_1, f_2)$, and randomly and uniformly selects $S_2^{n_2}$ within $S_2^{n_2}(\phi_1, \cdot, \cdot)$. Finally, Bob transmits the sequence $S_2^n = (S_2^{n_1}, S_2^{n_2})$ over the channel $P_{X|S_2}P_{YZ|X}$.

Decoding: Upon receiving $Y^n = (Y^{n_1}, Y^{n_2})$, Carol first looks into $\mathcal{C}_B$ and tries to decode $\hat{S}_2^{n_1}$ from Y^{n_1} by looking for a sequence that is jointly typical with respect to P_{S_2Y}. After decoding $\hat{S}_2^{n_1}$, Carol looks into $\mathcal{C}_A$, trying to decode a sequence $\hat{S}_1^n$, within $S_1^n(f(\hat{S}_2^{n_1}))$, that is jointly typical with V^n according to P_{S_1V}. Finally, with the obtained index $\phi_1(\hat{S}_1^n)$, Carol decodes $\hat{S}_2^{n_2}$ from Y^{n_2} by looking for a sequence that is jointly typical with Y^{n_2} according to P_{S_2Y}. Among the above three decoding steps, if there is no or more than one jointly typical sequence in any step, declare an error.

Phase II: **Key Distillation**. Set $R_{13} = \min\{I(S_2;Y) - I(S_2;Z) + R_{01} - 4\epsilon, I(S_2;Y) - I(S_1;U) + I(S_1;V) - 4\epsilon\}$. Randomly and independently assign all possible indices $(f_1, \phi_1, \varphi, \psi)$ to $2^{nR_{13}}$ bins which are indexed by θ. Set

$$K_1 = \phi_2(S_1^n), K_1' = \phi_2(\hat{S}_1^n);$$
$$K_2 = \theta(f_1(S_1^n), \phi_1(S_2^n), \varphi(S_2^n), \psi(S_2^n)),$$
$$K_2' = \theta(f_1(\hat{S}_1^n), \phi_1(\hat{S}_2^n), \varphi(\hat{S}_2^n), \psi(\hat{S}_2^n)).$$

Analysis of error probability: According to the Channel Coding Theorem [26], we conclude that Carol can correctly decode $S_2^{n_1}$ with a probability larger than $1 - \epsilon/3$. Then, with the decoded index $f(S_2^{n_1})$, Carol can use (f, V^n) to decode S_1^n correctly with a probability larger than $1 - \epsilon/3$, which follows from the Slepian-Wolf Theorem. Finally, Carol can use the obtained index $\phi_1(S_1^n)$ to locate bin $S_2^{n_2}(\phi_1, \cdot, \cdot)$ and decode $S_2^{n_2}$ correctly from Y^{n_2} with a probability larger than $1 - \epsilon/3$. Thus, the total probability of decoding error is upper bounded by ϵ.

Analysis of key rates: According to the codebook construction, we have that $(\phi_2, f_1, \phi_1, \varphi, \psi)$ are independent. Thus, we easily obtain

$$R_1 = R_{02}, R_2 = R_{13}.$$

Analysis of secrecy: Since (f, ϕ_1) is the only randomness shared by Alice and Bob, and

$$I(K_1; f, \phi_1) = I(\phi_2; f, \phi_1) \le n\epsilon,$$

K_1 is secure from Bob.

To verify that K_2 is secure from Alice, we first have

$$\begin{aligned} I(K_2; f, \phi_1) &= I(\theta; f_1, f_2, \phi_1) = I(\theta; f_1, \phi_1) \\ &= H(\theta) - H(\theta|f_1, \phi_1). \end{aligned}$$

Since $(f_1, \phi_1, \varphi, \psi)$ are independent and they are uniformly and independently assigned to $|\theta|$ bins, we can show that

$$H(\theta|f_1, \phi_1) \ge H(\theta) - n\epsilon$$

as long as $|\varphi||\psi| > |\theta|$. Since

$$\begin{aligned} \log|\varphi||\psi| &= n_2R_{11} + n_2R_{12} = n_2R_{10} \\ &= (n - n_1)R_{10} = nR_{10} - nR_{00} \\ &= n[I(S_2;Y) - I(S_1;U) + I(S_1;V) - 3\epsilon] \\ &> \log|\theta|, \end{aligned}$$

we have $I(K_2; f, \phi_1) \le n\epsilon$.

Now, in order to bound $I(K_1, K_2; Z^n)$, consider

$$\begin{aligned} I(K_1, K_2; Z^n) &= I(K_2; Z^n) + I(K_1; Z^n|K_2) \\ &\le I(\theta; Z^n) + I(\phi_2; f, \phi_1) \le I(\theta; Z^n) + n\epsilon \\ &= H(\theta) - H(\theta|Z^n) + n\epsilon. \end{aligned}$$

We can also verify that $H(\theta|Z^n) \ge H(\theta) - n\epsilon$ as long as $H(f_1, \phi_1, \varphi, \psi|Z^n) > nR_{13}$. Note that

$$\begin{aligned} H(f_1, \phi_1, \varphi, \psi|Z^n) &= H(f_1, S_2^{n_2}|Z^n) \\ &= H(f_1|Z^n) + H(S_2^{n_2}|Z^n, f_1) \\ &= H(f_1|Z^{n_1}) + H(S_2^{n_2}|Z^{n_2}). \end{aligned}$$

Since in each bin $S_2^{n_1}(f_1, \cdot)$ there are $2^{n_1(I(S_2;Z)+n\epsilon)}$ sequences $S_2^{n_1}$, there exists at least one sequence $S_2^{n_1}$ that is jointly typical with Z^{n_1} in bin $S_2^{n_1}(f_1, \cdot)$ with high probability. Thus, we obtain $H(f_1|Z^{n_1}) \ge n_1R_{11} - n_1\epsilon$. Furthermore, since there are $2^{n_2R_{10}+nR_{01}}$ randomly generated $S_2^{n_2}$ sequences, the average number of those sequences that are jointly typical with Z^{n_2} is $2^{n_2R_{10}+nR_{01}-n_2I(S_2;Z)}$. As a consequence, we obtain

$$\begin{aligned} H(S_2^{n_2}|Z^{n_2}) &\ge n_2R_{10} + nR_{01} - n_2I(S_2;Z) - n_2\epsilon \\ &= n_2R_{11} + nR_{01}. \end{aligned}$$

Hence, we have

$$H(f_1,\phi_1,\varphi,\psi|Z^n) \geq n_1R_{11} - n_1\epsilon + n_2R_{11} + nR_{01} \\ > n(I(S_2;Y) - I(S_2;Z) + R_{01} - 3\epsilon) > R_{13}$$

which implies $I(K_1,K_2;Z^n) \leq 2\epsilon$ as desired.

Appendix B
Proof of Theorem 2

It suffices to show that any achievable pair (R_1,R_2) is included in $\mathcal{R}_2^o(P_{S_1|U},P_X)$, for some $(P_{S_1|U},P_X)$.

First, we have

$$\begin{aligned} H(K_1) &= H(K_1|Y^n,V^N) + I(K_1;Y^n,V^N) \\ &\leq I(K_1;Y^n,V^N) + n\epsilon \\ &= I(K_1;Y^n) + I(K_1;V^N|Y^n) + n\epsilon \\ &\overset{(a)}{\leq} I(K_1;\mathbf{F}) + I(K_1;V^N|Y^n) + n\epsilon \\ &\leq \sum_{i=1}^N I(K_1;V_i|Y^n,V^{i-1}) + 2n\epsilon \\ &\leq \sum_{i=1}^N I(K_1,K_2,U_{i+1}^n,V^{i-1},Y^n;V_i) + 2n\epsilon \\ &= \sum_{i=1}^N I(S_{1i};V_i) + 2n\epsilon \\ &= N\sum_{i=1}^N \frac{1}{N} I(S_{1Q};V_Q|Q=i) + 2n\epsilon \\ &= NI(S_1;V) + 2n\epsilon, \end{aligned} \tag{36}$$

in which $S_{1i} := (K_1,K_2,U_{i+1}^n,V^{i-1},Y^n)$, $S_1 := (S_{1Q},Q)$, and Q is an independent random variable uniformly distributed over $[1:N]$. Note that (a) follows from the condition $U^N - \mathbf{F} - (Y^n,Z^n)$. Thus, it follows that $S_1 - U - V$.

Second, we have

$$\begin{aligned} &H(K_1) + H(K_2) \\ &= H(K_1,K_2) \\ &= H(K_1,K_2|Y^n,V^N) + I(K_1,K_2;Y^n,V^N) \\ &\leq I(K_1,K_2;Y^n,V^N) + n\epsilon \\ &\leq I(K_1,K_2;Y^n) + I(K_1,K_2;V^N|Y^n) + n\epsilon. \end{aligned} \tag{37}$$

For the first term on the right-hand side of (37), it follows that

$$\begin{aligned} I(K_1,K_2;Y^n) &\leq I(K_1,K_2;Y^n) - I(K_1,K_2;Z^n) + 2n\epsilon \\ &\leq I(K_1,K_2;Y^n,Z^n) - I(K_1,K_2;Z^n) + 2n\epsilon \\ &\leq I(K_1,K_2;Y^n|Z^n) + 2n\epsilon \\ &\leq I(X^n;Y^n|Z^n) + 2n\epsilon \\ &\leq \sum_i \left[H(Y_i|Y^{i-1}Z^n) - H(Y_i|X^nY^{i-1}Z^n)\right] \\ &\leq \sum_i \left[H(Y_i|Z_i) - H(Y_i|X^nY^{i-1}Z^n)\right] \\ &\overset{(a)}{\leq} \sum_i \left[H(Y_i|Z_i) - H(Y_i|X_iZ_i)\right] \\ &= nI(X;Y|Z) + 2n\epsilon, \end{aligned} \tag{38}$$

where (a) is true due to

$$\begin{aligned} & (X^n,Y^{i-1},Z^{i-1},Z_{i+1}^n) - X_i - (Y_i,Z_i) \\ \Rightarrow\quad & (X^n,Y^{i-1},Z^n) - (X_i,Z_i) - Y_i. \end{aligned}$$

Moreover, the second term of (37) can be bounded as

$$\begin{aligned} I(K_1,K_2;V^N|Y^n) &= \sum_{i=1}^N I(K_1,K_2;V_i|V^{i-1},Y^n) \\ &\leq \sum_{i=1}^N I(K_1,K_2,V^{i-1},Y^n,U_{i+1}^N;V_i) \\ &= NI(S_1;V). \end{aligned} \tag{39}$$

Thus,

$$R_1 + R_2 \leq I(X;Y|Z) + \frac{1}{\beta} I(S_1;V) + 4\epsilon.$$

Furthermore, we have

$$\begin{aligned} & I(U^N;Y^n) - I(V^N;Y^n) \\ &\leq I(\mathbf{F};Y^n) - I(V^N;Y^n) \\ &= I(\mathbf{F};Y^n,K_2) - I(\mathbf{F};K_2|Y^n) - I(V^N;Y^n) \\ &\leq I(\mathbf{F};Y^n|K_2) - I(\mathbf{F};K_2|Y^n) - I(V^N;Y^n) + n\epsilon \\ &= I(\mathbf{F},K_2;Y^n) - I(K_2;Y^n) - I(\mathbf{F};K_2|Y^n) \\ &\qquad\qquad - I(V^N;Y^n) + n\epsilon \\ &= I(\mathbf{F},K_2;Y^n) - I(\mathbf{F},Y^n;K_2) - I(V^N;Y^n) + n\epsilon \\ &\overset{(a)}{\leq} I(\mathbf{F},K_2;Y^n) - I(V^N,Y^n;K_2) - I(V^N;Y^n) + n\epsilon \\ &= I(\mathbf{F},K_2;Y^n|V^N) - I(V^N,Y^n;K_2) + n\epsilon \\ &\leq I(\mathbf{F},K_2;Y^n|V^N) - H(K_2) + 2n\epsilon \\ &= \sum_{i=1}^n I(\mathbf{F},K_2;Y_i|Y^{i-1},V^N) - H(K_2) + 2n\epsilon \\ &\leq \sum_{i=1}^n I(\mathbf{F},K_2,Y^{i-1},V^N;Y_i) - H(K_2) + 2n\epsilon \\ &\leq \sum_{i=1}^n I(X_i;Y_i) - H(K_2) + 2n\epsilon \\ &= nI(X;Y) - H(K_2) + 2n\epsilon, \end{aligned} \tag{40}$$

in which (a) follows from

$$\begin{aligned} & \begin{cases} V^N \to \mathbf{F} \to K_2 \\ V^N \to \mathbf{F}, K_2 \to Y^n \end{cases} \\ \Rightarrow\quad & V^N \to \mathbf{F} \to Y^n, K_2 \\ \Rightarrow\quad & V^N, Y^n \to \mathbf{F}, Y^n \to K_2. \end{aligned} \tag{41}$$

On the other hand,

$$\begin{aligned}
&I(U^N;Y^n) - I(V^N;Y^n)\\
&= I(U^N;Y^n,K_1,K_2) - I(V^N;Y^n,K_1,K_2)\\
&\quad -I(U^N;K_1,K_2|Y^n) + I(V^N;K_1,K_2|Y^n)\\
&= I(U^N;Y^n,K_1,K_2) - I(V^N;Y^n,K_1,K_2)\\
&\quad +H(K_1,K_2|Y^n,U^N) - H(K_1,K_2|Y^n,V^N)\\
&\geq I(U^N;Y^n,K_1,K_2) - I(V^N;Y^n,K_1,K_2) - n\epsilon\\
&= \sum_{i=1}^{N}\Big(I(Y^n,K_1,K_2;U_i|U_{i+1}^N,V^{i-1})\\
&\quad -I(Y^n,K_1,K_2;V_i|U_{i+1}^N,V^{i-1})\Big) - n\epsilon\\
&= \sum_{i=1}^{N}\Big(I(Y^n,K_1,K_2,U_{i+1}^N,V^{i-1};U_i)\\
&\quad -I(Y^n,K_1,K_2,U_{i+1}^N,V^{i-1};V_i)\Big) - n\epsilon\\
&= \sum_{i=1}^{N} I(S_{1i};U_i) - I(S_{1i};V_i) - n\epsilon\\
&= N\big(I(S_1;U) - I(S_1;V)\big) - n\epsilon. \qquad (42)
\end{aligned}$$

Thus, we have

$$I(S_1;U) - I(S_1;V) + \beta R_2 \leq \beta I(X;Y) + 3\epsilon.$$

As ϵ can be chosen arbitrarily small, this concludes the proof.

Appendix C
Proof of Theorem 3

As the proof follows allong similar lines as that of Theorem 1, we only provide the codebook construction. Without loss of generality, we assume $I(S_2;Y|T_2) - I(S_2;Z|T_2) \geq 0$, $I(S_1;V|T_1) - I(S_1;W|T_1) \geq 0$ and $\beta = 1$, i.e. $N = n$. Then, it is equivalent to proving that given $(P_{T_1|S_1}P_{S_1|U}, P_{T_2|S_2}P_{S_2X})$, for any $(R_1,R_2) \in \mathcal{R}_1(P_{T_1|S_1}P_{S_1|U}, P_{T_2|S_2}P_{S_2X})$ there exists a scheme such that (R_1,R_2) is achievable. Set $R_2 = \min\{I(S_2;Y|T_2) - I(S_2;Z|T_2) + \tilde{R}_1, I(S_2;Y) - I(S_1;U) + I(S_1;V), I(S_1;V|T_1) - I(S_1;W|T_1) + I(S_2;Y|T_2) - I(S_2;Z|T_2) - R_1\} - 4\epsilon$ with $R_1 + \tilde{R}_1 = \min\{I(S_1;V), I(S_1;U) - I(S_1;W)\} - \epsilon$, it suffices to show that the pair (R_1,R_2) is achievable. The scheme consists of two phases: Key Agreement and Key Distillation.

Phase I: **Key Agreement**.

Codebook generation: *Codebook at Alice* $\mathcal{C}_A$. Given $P_{T_1|S_1}P_{S_1|U}P_{UV}$, randomly and independently generate 2^{nR_0} sequences T_1^n according to $\prod_{i=1}^n P_{T_1}(T_{1i})$, which are indexed by (f_1,f_2) with $f_1 \in [1:2^{nR_{01}}]$ and $f_2 \in [1:2^{nR_{02}}]$. For each T_1^n, randomly and independently generate $2^{nR_{03}}$ sequences S_1^n according to $\prod_{i=1}^n P_{S_1|T_1}(S_{1i}|T_{1i})$, which are indexed by (ϕ_1,ϕ_2) with $\phi_1 \in [1:2^{nR_{04}}]$ and $\phi_2 \in [1:2^{nR_{05}}]$. Then, randomly assign the tuple (f_2,ϕ_2) into $2^{n\tilde{R}_1}$ bins indexed by f_3. Here,

$$\begin{aligned}
R_0 &= I(T_1;U) + \epsilon,\\
R_{01} &= I(T_1;U) - I(T_1;V) + 2\epsilon,\\
R_{02} &= I(T_1;V) - \epsilon,\\
R_{03} &= I(S_1;U|T_1) + \epsilon,\\
R_{04} &= I(S_1;U|T_1) - I(S_1;V|T_1) + \epsilon,\\
R_{05} &= I(S_1;V|T_1) - \epsilon.
\end{aligned}$$

Codebook at Bob $\mathcal{C}_{B_1}$. Split the number n as summation of n_1+n_2 with $n_1 = n(R_{01}+R_{04})/R_{12}$. Given $P_{T_2}P_{S_2X}P_{YZ|X}$, first randomly and independently generate $2^{n_1R_{10}}$ sequences $T_2^{n_1}$, according to $\prod_{i=1}^{n_1} P_{T_2}(T_{2i})$. For each $T_2^{n_1}$, randomly and independently generate $2^{nR_{11}}$ sequences $S_2^{n_1}$ according to $\prod_{i=1}^{n_1} P_{S_2|T_2}(S_{2i}|T_{2i})$. Then, randomly assign a index $\psi_1 \in [1:2^{n_1R_{12}}]$ to the pair $(T_2^{n_1},S_2^{n_1})$, and set a bijective mapping between ψ_1 and (f_1,ϕ_1).

$\mathcal{C}_{B_2}$. Randomly and independently generate $2^{n_2R_{10}+n\tilde{R}_1}$ sequences $T_2^{n_2}$, according to $\prod_{i=1}^{n_2} P_{T_2}(T_{2i})$, and randomly assign each sequence into $2^{n\tilde{R}_1}$ bins. Then, similar as above, generate $2^{nR_{11}}$ sequences $S_2^{n_2}$ for each $T_2^{n_2}$. Denote the bin index of $T_2^{n_2}$ by ψ_3, the index of $T_2^{n_2}$ within each bin by ψ_4 and index of $S_2^{n_2}$ by ψ_5 respectively, with $\psi_3 \in [1:2^{n\tilde{R}_1}], \psi_4 \in [1:2^{n_2R_{10}}]$ and $\psi_5 \in [1:2^{n_2R_{11}}]$.

$$\begin{aligned}
R_{10} &= I(T_2;Y) - \epsilon,\\
R_{11} &= I(S_2;Y|T_2) - \epsilon,\\
R_{12} &= I(S_2;Y) - \epsilon,
\end{aligned}$$

Encoding: Having observed the sequence U^n, Alice looks into $\mathcal{C}_A$, and tries to find a sequence T_1^n that is jointly typical according to P_{T_1U}. If there are more than one such sequence, randomly select one of them; if there is no such sequence, randomly select one sequence T_1^n from all possible sequences. Similarly, for all sequences S_1^n that are generated by T_1^n, select a sequence S_1^n that is jointly typical with (T_1^n,U^n). If there is no such sequence, randomly select one. Alice transmits the indices (f_1,ϕ_1) as well as the bin index f_3 to Bob.

Upon receiving (f,ϕ_1), Bob looks into $\mathcal{C}_{B_1}$, selecting the sequence $S_2^{n_1}(\psi_1)$. And he looks into the f_3-th bin of $T_2^{n_2}$, randomly and uniformly selecting $T_2^{n_2}$ and $S_2^{n_2}$. Finally, Bob transmits the sequence $S_2^n = (S_2^{n_1},S_2^{n_2})$ over the channel $P_{X|S_2}P_{YZ|X}$.

Decoding: Upon receiving $Y^n = (Y^{n_1},Y^{n_2})$, Carol first looks into $\mathcal{C}_{B_1}$ and tries to decode $\hat{T}_2^{n_1}$ and $\hat{S}_2^{n_1}$ from Y^{n_1} by looking for a pair of sequences that is jointly typical with Y^{n_1} with respect to $P_{T_2S_2Y}$. After decoding $\hat{T}_2^{n_1}$ and $\hat{S}_2^{n_1}$, Carol looks into $\mathcal{C}_A$, trying to decode the sequence pair $(\hat{T}_1^n,\hat{S}_1^n)$ with the parameters (f_1,ψ_1), that is jointly typical with V^n according to $P_{T_1S_1V}$. Finally, with the obtained index f_3 from $(\hat{T}_1^n,\hat{S}_1^n)$, Carol decodes $(\hat{T}_2^{n_2},\hat{S}_2^{n_2})$ from Y^{n_2} according to $P_{T_2S_2Y}$. Among the above three decoding steps, if there is no or more than one jointly typical sequence in any step, declare an error.

Phase II: **Key Distillation**. Randomly and independently assign all possible indices $(f_1, f_2, \phi_1, \phi 2)$ to 2^{nR_1} bins which are indexed by θ_1, and $(\psi_1, \psi_3, \psi_4, \psi_5)$ to 2^{nR_2} bins which are indexed by θ_2. And set $K_1 = \theta_1$ and $K_2 = \theta_2$.

Then, follow a similar analysis process as that in the proof of Theorem 1, we can verify that with a probability larger than $1-\epsilon$, Alice and Bob will successfully share secret keys with Carol with rate R_1 and R_2, respectively.

Appendix D
Proof of Theorem 4

To prove Theorem 4 is equivalent to showing that given any achievable key rate pair (R_1, R_2), there exists some $(P_{T_1|S_1}P_{S_1|U}, P_X)$ subject to $(R_1, R_2) \in \mathcal{R}_2(P_{T_1|S_1}P_{S_1|U}, P_X)$.

First, from (36), we have

$$\begin{aligned} H(K_1) &= \sum_{i=1}^{N} I(K_1; V_i|Y^n, V^{i-1}) + 2n\epsilon \\ &\le \sum_{i=1}^{N} I(K_1, K_2, V^{i-1}, W_{i+1}^n, Y^n; V_i) + 2n\epsilon \\ &= \sum_{i=1}^{N} I(S_{1i}; V_i) + 2n\epsilon \\ &= NI(S_1; V) + 2n\epsilon, \end{aligned} \tag{43}$$

in which $S_{1i} := (K_1, K_2, V^{i-1}, W_{i+1}^n, Y^n)$, $S_1 := (S_{1Q}, Q)$. And we can easily verify that $S_1 - U - V$. Thus, we have

$$R_1 \le \frac{1}{\beta} I(S_1; V) + 2\epsilon. \tag{44}$$

Second, the proof of $R_1 \le \frac{1}{\beta} H(U|W)$ is trivial following from

$$\begin{aligned} H(K_1) &= H(K_1|U^N) + I(K_1; U^N) \\ &\le I(K_1; U^N) - I(K_1; W^N) + n\epsilon \\ &= I(K_1; U^N|W^N) + n\epsilon \\ &\le I(U^N; U^N|W^N) + n\epsilon \\ &= H(U^N|W^N) + n\epsilon \\ &= NH(U|W) + n\epsilon. \end{aligned}$$

Furthermore, to show (27), we first have

$$I(U^N; Y^n) - I(V^N; Y^n) \le nI(X; Y) - H(K_2) + 2n\epsilon,$$

according to (40). On the other hand, we have

$$\begin{aligned} & I(U^N; Y^n) - I(V^N; Y^n) \\ &\overset{(a)}{\ge} \sum_{i=1}^{N} \Big(I(K_1, K_2, U_{i+1}^N, V^{i-1}, Y^n; U_i) \\ &\quad - I(K_1, K_2, U_{i+1}^N, V^{i-1}, Y^n; V_i) \Big) - n\epsilon \\ &\overset{(b)}{=} \sum_{i=1}^{N} \Big[I(K_1, K_2, U_{i+1}^N, V^{i-1}, W_{i+1}^N, Y^n; U_i) \\ &\quad - I(K_1, K_2, U_{i+1}^N, V^{i-1}, W_{i+1}^N, Y^n; V_i) \Big] - n\epsilon \\ &= \sum_{i=1}^{N} \Big[I(S_{1i}; U_i) - I(S_{1i}; V_i) \Big] \\ &\quad + \sum_{i=1}^{N} \Big[I(U_{i+1}^N; U_i|S_{1i}) - I(U_{i+1}^N; V_i|S_{1i}) \Big] - n\epsilon \\ &= \sum_{i=1}^{N} \Big[I(S_{1i}; U_i) - I(S_{1i}; V_i) \Big] \\ &\quad + \sum_{i=1}^{N} \Big[I(U_{i+1}^N; S_{1i}, U_i, V_i) - I(U_{i+1}^N; S_{1i}, V_i) \Big] - n\epsilon \\ &\overset{(c)}{\ge} \sum_{i=1}^{N} \Big[I(S_{1i}; U_i) - I(S_{1i}; V_i) \Big] - n\epsilon \\ &= N\Big[I(S_1; U) - I(S_1; V) \Big] - n\epsilon. \end{aligned} \tag{45}$$

where (a) is due to (42), (b) follows from

$$\begin{aligned} & W_{i+1}^N \to U_{i+1}^N \to (U^N, V^i) \\ \Rightarrow \quad & W_{i+1}^N \to U_{i+1}^N \to (K_1, \mathbf{F}, U_i, V^i) \\ \Rightarrow \quad & W_{i+1}^N \to U_{i+1}^N \to (K_1, K_2, Y^n, U_i, V^i) \\ \Rightarrow \quad & W_{i+1}^N \to (K_1, K_2, U_{i+1}^N, V^{i-1}, Y^n) \to (U_i, V_i) \\ \Rightarrow \quad & \begin{cases} W_{i+1}^N \to (K_1, K_2, U_{i+1}^N, V^{i-1}, Y^n) \to U_i \\ W_{i+1}^N \to (K_1, K_2, U_{i+1}^N, V^{i-1}, Y^n) \to V_i \end{cases}, \end{aligned} \tag{46}$$

and (c) is true since

$$\begin{aligned} & (U^N, V^{i-1}, W_{i+1}^N) \to U_i \to V_i \\ \Rightarrow \quad & (K_1, \mathbf{F}, U_{i+1}^N, V^{i-1}, W_{i+1}^N) \to U_i \to V_i \\ \Rightarrow \quad & (K_1, K_2, Y^n, U_{i+1}^N, V^{i-1}, W_{i+1}^N) \to U_i \to V_i \\ \Rightarrow \quad & U_{i+1}^N \to (K_1, K_2, V^{i-1}, W_{i+1}^N, Y^n, U_i) \to V_i. \end{aligned} \tag{47}$$

Thus, it follows

$$N[I(S_1; U) - I(S_1; V)] \le nI(X; Y) - H(K_2) + 3n\epsilon,$$

which implies

$$R_2 \le I(X; Y) - \frac{1}{\beta}\left[I(S_1; U) - I(S_1; V) \right] + 3\epsilon.$$

As the last step, we have that

$$\begin{aligned} & H(K_1) + H(K_2) \\ &= H(K_1, K_2) \\ &= H(K_1, K_2|Y^n, W^N) + I(K_1, K_2; Y^n, W^N) \\ &\le H(K_1, K_2|Y^n, W^N) - H(K_1, K_2|Y^n, V^N) \\ &\quad + I(K_1, K_2; Y^n, W^N) - I(K_1, K_2; Z^n, W^N) + n\epsilon \\ &= I(K_1, K_2; Y^n, V^N) - I(K_1, K_2; Y^n, W^N) \\ &\quad + I(K_1, K_2; Y^n, W^N) - I(K_1, K_2; Z^n, W^N) + n\epsilon \\ &= I(K_1, K_2; V^N|Y^n) - I(K_1, K_2; W^N|Y^n) \\ &\quad + I(K_1, K_2; Y^n|W^N) - I(K_1, K_2; Z^n|W^N) + n\epsilon \\ &\le \sum_{i=1}^{N} [I(K_1, K_2; V_i|V^{i-1}, W_{i+1}^N, Y^n) \\ &\quad - I(K_1, K_2; W_i|V^{i-1}, W_{i+1}^N, Y^n)] \end{aligned}$$

$$
\begin{aligned}
&+I(K_1,K_2;Y^n,Z^n|W^N)-I(K_1,K_2;Z^n|W^N)+n\epsilon\\
&=\sum_{i=1}^{N}[I(K_1,K_2,V^{i-1},W_{i+1}^N,Y^n;V_i|V^{i-1},W_{i+1}^N,Y^n)\\
&\quad -I(K_1,K_2,V^{i-1},W_{i+1}^N,Y^n;W_i|V^{i-1},W_{i+1}^N,Y^n)]\\
&\quad +I(K_1,K_2;Y^n|Z^n,W^N)+n\epsilon\\
&\le\sum_{i=1}^{N}[I(S_{1i};V_i|T_{1i})-I(S_{1i};W_i|T_{1i})]\\
&\quad +I(K_1,K_2,W^N;Y^n|Z^n)+n\epsilon\\
&\le N[I(S_1;V|T_1)-I(S_1;W|T_1)]+I(X^n;Y^n|Z^n)+n\epsilon\\
&=N[I(S_1;V|T_1)-I(S_1;W|T_1)]+nI(X;Y|Z)+n\epsilon. \quad (48)
\end{aligned}
$$

Thus, we have

$$R_1+R_2\le\frac{1}{\beta}[I(S_1;V|T_1)-I(S_1;W|T_1)]+I(X;Y|Z)+\epsilon,$$

and this completes the proof since ϵ is an arbitrary small number.

Appendix E
Proof of Theorem 5

Under conditions $X\to Y\to Z$ and $U\to V\to W$, to show that $\bigcup_{P_{S_1|U},P_X}\mathcal{R}(P_{S_1|U},P_X)$ is a single-letter characterization on $\mathcal{C}$ is equivalent to showing that $\bigcup_{P_{S_1|U},P_X}\mathcal{R}(P_{S_1|U},P_X)$ is both an inner bound and an outer bound on $\mathcal{C}$, simultaneously.

First of all, by setting $T_1=T_2=\emptyset$ and $S_2=X$, we conclude that

$$\mathcal{R}(P_{S_1|U},P_X)=\mathcal{R}_1(P_{T_1|S_1}P_{S_1|U},P_{T_2|S_2}P_{S_2X}),$$

Thus, $\bigcup_{P_{S_1|U},P_X}\mathcal{R}(P_{S_1|U},P_X)$ is an inner bound according to Theorem 3.

Now, we show the converse of Theorem 5. First, similar as (43), we have

$$R_1\le\frac{1}{\beta}I(S_1;V)+2\epsilon,$$

in which $S_1\triangleq(S_{1Q},Q)$ and $S_{1i}\triangleq(K_1,K_2,U_{i+1}^N,V^{i-1},W^{i-1},W_{i+1}^n,Y^n)$. In addition, we also have that S_1-U-V.

Second, it follows that

$$
\begin{aligned}
H(K_1)&\le I(K_1;U^N)-I(K_1;W^N)+n\epsilon\\
&=\sum_{i=1}^{N}[I(K_1;U_i|U_{i+1}^N,W^{i-1})\\
&\quad -I(K_1;W_i|U_{i+1}^N,W^{i-1})]+n\epsilon\\
&=\sum_{i=1}^{N}[I(K_1,U_{i+1}^N,W^{i-1};U_i)\\
&\quad -I(K_1,U_{i+1}^N,W^{i-1};W_i)]+n\epsilon\\
&=\sum_{i=1}^{N}[I(S_{1i};U_i)-I(S_{1i};W_i)]\\
&\quad -\sum_{i=1}^{N}\big[I(S_{1i};U_i|K_1,U_{i+1}^N,W^{i-1})\\
&\quad -I(S_{1i};W_i|K_1,U_{i+1}^N,W^{i-1})\big]+n\epsilon\\
&\overset{(a)}{=}\sum_{i=1}^{N}[I(S_{1i};U_i)-I(S_{1i};W_i)]\\
&\quad -\sum_{i=1}^{N}\big[I(S_{1i};U_i|W_i,K_1,U_{i+1}^N,W^{i-1})\big]+n\epsilon\\
&\le\sum_{i=1}^{N}[I(S_{1i};U_i)-I(S_{1i};W_i)]+n\epsilon\\
&\le N[I(S_1;U)-I(S_1;W)]+n\epsilon \qquad (49)
\end{aligned}
$$

in which (a) is due to

$$
\begin{aligned}
&S_{1i}\to U_i\to W_i\\
\Rightarrow\quad &S_{1i}\to(U_i,K_1,U_{i+1}^N,W^{i-1})\to W_i.
\end{aligned}
$$

Furthermore, we have

$$
\begin{aligned}
&I(U^N;Y^n)-I(V^N;Y^n)\\
&\ge\sum_{i=1}^{N}\Big[I(K_1,K_2,U_{i+1}^N,V^{i-1},Y^n;U_i)\\
&\quad -I(K_1,K_2,U_{i+1}^N,V^{i-1},Y^n;V_i)\Big]-n\epsilon\\
&\ge\sum_{i=1}^{N}\Big[I(S_{1i};U_i)-I(S_{1i};V_i)\Big]\\
&\quad -\sum_{i=1}^{N}\Big[I(W^{i-1},W_{i+1}^N;U_i|K_1,K_2,U_{i+1}^N,V^{i-1},Y^n)\\
&\quad -I(W^{i-1},W_{i+1}^N;V_i|K_1,K_2,U_{i+1}^N,V^{i-1},Y^n)\Big]-n\epsilon\\
&\overset{(a)}{\ge}\sum_{i=1}^{N}\Big[I(S_{1i};U_i)-I(S_{1i};V_i)\Big]-n\epsilon, \qquad (50)\\
&=N[I(S_{1i};U_i)-I(S_{1i};V_i)]-n\epsilon, \qquad (51)
\end{aligned}
$$

where (a) is due to

$$
\begin{aligned}
&U\to V\to W\\
\Rightarrow\ &(W^{i-1},W_{i+1}^N)\to(U_{i+1}^N,V^{i-1})\to(U^N,V^N)\\
\Rightarrow\ &(W^{i-1},W_{i+1}^N)\to(U_{i+1}^N,V^{i-1})\to(K_1,K_2,Y^n,U_i,V_i)\\
\Rightarrow\ &(W^{i-1},W_{i+1}^N)\to(K_1,K_2,U_{i+1}^N,V^{i-1},Y^n)\to(U_i,V_i)\\
\Rightarrow\ &\begin{cases}(W^{i-1},W_{i+1}^N)\to(K_1,K_2,U_{i+1}^N,V^{i-1},Y^n)\to U_i\\(W^{i-1},W_{i+1}^N)\to(K_1,K_2,U_{i+1}^N,V^{i-1},Y^n)\to V_i\end{cases}.
\end{aligned}
$$

On the other hand, we have

$$I(U^N;Y^n)-I(V^N;Y^n)\le nI(X;Y)-H(K_2)+2n\epsilon,$$

whose derivation is the same as (40). Thus, we obtain that

$$R_2\le I(X;Y)-\frac{1}{\beta}\left[I(S_1;U)-I(S_1;V)\right]+3\epsilon.$$

At last, we have

$$\begin{aligned}
&\sum_{i=1}^{N}[I(V^{i-1},W_{i+1}^N,Y^n;V_i)-I(V^{i-1},W_{i+1}^N,Y^n;W_i)]\\
&=\sum_{i=1}^{N}[I(Y^n;V_i|V^{i-1},W_{i+1}^N)-I(Y^n;W_i|V^{i-1},W_{i+1}^N)]\\
&=I(Y^n;V^N)-I(Y^n;W^N)\\
&\geq 0,
\end{aligned}$$

since $Y^n \to U^N \to V^N \to W^N$. Thus, from (48) we have

$$\begin{aligned}
&H(K_1)+H(K_2)\\
&\leq \sum_{i=1}^{N}[I(K_1,K_2;V_i|V^{i-1},W_{i+1}^N,Y^n)\\
&\quad -I(K_1,K_2;W_i|V^{i-1},W_{i+1}^N,Y^n)]+nI(X;Y|Z)+n\epsilon\\
&\leq \sum_{i=1}^{N}[I(K_1,K_2,V^{i-1},W_{i+1}^N,Y^n;V_i)\\
&\quad -I(K_1,K_2,V^{i-1},W_{i+1}^N,Y^n;W_i)]+nI(X;Y|Z)+n\epsilon\\
&\leq \sum_{i=1}^{N}[I(S_{1i};V_i)-I(S_{1i};W_i)]+nI(X;Y|Z)+n\epsilon\\
&\quad -\sum_{i=1}^{N}\Big[I(U_{i+1}^N,W^{i-1};V_i|K_1,K_2,V^{i-1},W_{i+1}^N,Y^n)\\
&\quad -I(U_{i+1}^N,W^{i-1};W_i|K_1,K_2,V^{i-1},W_{i+1}^N,Y^n)\Big]\\
&=\sum_{i=1}^{N}[I(S_{1i};V_i)-I(S_{1i};W_i)]+nI(X;Y|Z)+n\epsilon\\
&\quad -\sum_{i=1}^{N}I(U_{i+1}^N,W^{i-1};V_i|W_i,K_1,K_2,V^{i-1},W_{i+1}^N,Y^n)\\
&\leq \sum_{i=1}^{N}[I(S_{1i};V_i)-I(S_{1i};W_i)]+nI(X;Y|Z)+n\epsilon\\
&=N[I(S_1;V|T_1)-I(S_1;W|T_1)]+nI(X;Y|Z)+n\epsilon. \quad (52)
\end{aligned}$$

Thus, we have

$$R_1+R_2 \leq \frac{1}{\beta}[I(S_1;V|T_1)-I(S_1;W|T_1)]+I(X;Y|Z)+\epsilon.$$

Hence, it follows that $\bigcup_{P_{S_1|U},P_X}\mathcal{R}(P_{S_1|U},P_X)$ is an outer bound as well. And this completes the proof.

REFERENCES

[1] W. Tu, M. Goldenbaum, L. Lai, and H. V. Poor, "Multiple key generation with restricted public discussion structure," in *Proc. IEEE Conf. on Communications and Network Security*, (Philadelphia, PA), pp. 641–645, Oct. 2016.

[2] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, pp. 733–742, May 1993.

[3] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography, Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, pp. 1121–1132, July 1993.

[4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, pp. 339–348, May 1978.

[5] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, pp. 3047–3061, Dec. 2004.

[6] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, pp. 344–366, Mar. 2000.

[7] H. Zhang, L. Lai, Y. Liang, and H. Wang, "The capacity region of the source-type model for secret key and private key generation," *IEEE Trans. Inf. Theory*, vol. 60, pp. 6389–6398, Jul. 2014.

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

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

[10] C. Ye and P. Narayan, "Secret key and private key constructions for simple multiterminal source models," *IEEE Trans. Inf. Theory*, vol. 58, pp. 639–651, Feb. 2012.

[11] P. Xu, Z. Ding, X. Dai, and G. Karagiannidis, "Simultaneously generating secret and private keys in a cooperative pairwise independent network," *IEEE Trans. Inf. Forensics Security*, vol. 11, pp. 1139–1150, Jan. 2016.

[12] S. Watanabe and Y. Oohama, "Secret key agreement from vector Gaussian sources by rate limited public communication," *IEEE Trans. Inf. Forensics Security*, vol. 6, pp. 541–550, Sept. 2011.

[13] A. Agrawal, Z. Rezki, A. Khisti, and M.-S. Alouini, "Noncoherent capacity of secret-key agreement with public discussion," *IEEE Trans. Inf. Forensics Security*, vol. 6, pp. 565–574, Sept. 2011.

[14] N. Wang, N. Zhang, and T. A. Gulliver, "Cooperative key agreement for wireless networking: Key rates and practical protocol design," *IEEE Trans. Inf. Forensics Security*, vol. 9, pp. 272–284, Jan. 2014.

[15] C. W. Wong, T. F. Wong, and J. M. Shea, "Secret-sharing LDPC codes for the BPSK-constrained Gaussian wiretap channel," *IEEE Trans. Inf. Forensics Security*, vol. 6, pp. 551–564, Sept. 2011.

[16] K. Chen, B. B. Natarajan, and S. Shattil, "Secret key generation rate with power allocation in relay-based LTE-A networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, pp. 2424–2434, Nov. 2015.

[17] M. F. Haroun and T. A. Gulliver, "Secret key generation using chaotic signals over frequency selective fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 10, pp. 1764–1775, Aug. 2015.

[18] S. Tomasin and A. Dall'Arche, "Resource allocation for secret key agreement over parallel channels with full and partial eavesdropper CSI," *IEEE Trans. Inf. Forensics Security*, vol. 10, pp. 2314–2324, Nov. 2015.

[19] A. Khisti, S. N. Diggavi, and G. W. Wornell, "Secret-key agreement with channel state information at the transmitter," *IEEE Trans. Inf. Forensics Security*, vol. 6, pp. 672–681, Sept. 2011.

[20] I. Csiszar and P. Narayan, "Secrecy capacities for multiterminal channel models," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2437–2452, Jun. 2008.

[21] A. Zibaeenejad, "Key generation over wiretap models with non-causal side information," *IEEE Trans. Inf. Forensics Security*, vol. 10, pp. 1456–1471, Jul. 2015.

[22] H. Zhou, L. M. Huie, and L. Lai, "Secret key generation in the two-way relay channel with active attackers," *IEEE Trans. Inf. Forensics Security*, vol. 9, pp. 476–488, Feb. 2014.

[23] Y. Oohama, "Capacity theorems for relay channels with confidential messages," in *Proc. IEEE Int. Symp. Inf. Theory*, (Nice, France), pp. 926–930, IEEE, Jun. 2007.

[24] W. Tu, M. Goldenbaum, L. Lai, and H. V. Poor, "Simultaneously generating multiple keys over a cascade of a noiseless channel and a wiretap channel," in *Proc. IEEE Inf. Theory Workshop*, (Cambridge, UK), pp. 206–210, Sept. 2016.

[25] W. Tu, M. Goldenbaum, L. Lai, and H. V. Poor, "On simultaneously generating multiple keys in a joint source-channel model," *IEEE Trans. Inf. Forensics Security*, vol. 12, pp. 298–308, Feb. 2017.

[26] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: John Wiley & Sons, 2012.