Secrecy in Cooperative Relay Broadcast Channels

Ersen Ekrem, *Student Member, IEEE*, and Sennur Ulukus, *Member, IEEE*

***Abstract*—We investigate the effects of user cooperation on the secrecy of broadcast channels by considering a cooperative relay broadcast channel. We show that user cooperation can increase the achievable secrecy region. We propose an achievable scheme that combines Marton's coding scheme for broadcast channels and Cover and El Gamal's compress-and-forward scheme for relay channels. We derive outer bounds for the rate-equivocation region using auxiliary random variables for single-letterization. Finally, we consider a Gaussian channel and show that both users can have positive secrecy rates, which is not possible for scalar Gaussian broadcast channels without cooperation.**

***Index Terms*—Cooperation, cooperative relay broadcast channel, information theoretic security, secrecy.**

I. Introduction

THE open nature of wireless communications facilitates cooperation by allowing users to exploit the overheard information to increase achievable rates. However, the same open nature of wireless communications makes it vulnerable to security attacks such as eavesdropping and jamming. In this paper, we investigate the interaction of these two phenomena, namely *cooperation* and *secrecy*. In particular, we investigate the effects of cooperation on secrecy.

The eavesdropping attack was first studied from an information theoretic point of view by Wyner in [1], where he established the secrecy capacity for a *single-user degraded* wire-tap channel. Later, Csiszar and Korner [2] studied the general, not necessarily degraded, *single-user* eavesdropping channel, and found the secrecy capacity. More recently, *multi-user* versions of the secrecy problem have been considered for various channel models. [3]–[7] consider multiple-access channels (MAC), where in [3], [4] the eavesdropper is an external entity, while in [5]–[7] the users in the MAC act as eavesdroppers on each other. [8], [9] consider broadcast channels (BCs) where both receivers want to have secure communication with the transmitter; in here as well, each receiver of the BC is an eavesdropper for the other user. [10]–[16] consider secrecy in relay channels, where in [10]–[13], the relay is the eavesdropper, while in [14], [15] there is an external eavesdropper. In [16], the relay helps the transmitter to improve its rate while it receives confidential messages that should be kept hidden from the main receiver.

In a wireless medium, since all users receive a version of all signals transmitted, they can cooperate to improve their communication rates. The simplest example of a cooperative system is the relay channel [17] where the relay helps increase the communication rate of a single-user channel using its over-heard information. Multi-user versions of cooperative communication have been studied more recently. The cooperative MAC is introduced in [18]. In a cooperative MAC, both users overhear a noisy version of the signal transmitted by the other user, and transmit in such a way to increase the achievable rates. The cooperative relay broadcast channel (CRBC) model is introduced in [19], [20]. In a CRBC, cooperation is done on the receiver side, where in a BC, one or both of the receivers transmit cooperative signals to the other receiver to improve the achievable rates of both users [19]–[21].

Our goal is to study the effects of cooperation on the secrecy of *multiple users* where secrecy refers to simultaneous individual confidentiality of all users against each other. In our model, users eavesdrop on each other; there are no external eavesdroppers. One of the simplest models to study this interaction is the CRBC, where there is a single transmitter and two receivers, and each receiver would like to keep its message secret from the other user; see Figs. 1 and 2. In this model, in order to incorporate the effects of cooperation, there is either a single-sided (see Fig. 1) or double-sided (see Fig. 2) cooperative link between the users. For clarity of ideas and simplicity of presentation, for a major part of this paper, we will assume a CRBC with a single-sided cooperation link from the first user to the second user. We will investigate the effects of two-sided cooperation in Section VIII. Focusing on the single-sided CRBC, we note that if we remove the cooperation link, our model reduces to the BC with confidential messages in [8], [9], and if we set the rate of the first user to zero, our model reduces to the relay channel with confidential messages in [10]–[13], and if we both set the rate of the first user to zero and remove the cooperation link between the users, our model reduces to the single-user eavesdropper channel in [1], [2]. Our model is the simplest model (except perhaps for the "dual" model of cooperating transmitters in a MAC with per-user secrecy constraints [7]) that allows us to study the effects of cooperation (or lack thereof) of the first user (the transmitting end of the cooperative link) on its own equivocation rate as well as on the equivocation rate of the other user (receiving end of the cooperative link).

We note that, in our channel model each user eavesdrops as well as helps the other user. That is, the users are untrusted but nonmalicious. There can be such communication scenarios. For

Manuscript received October 16, 2008; revised August 15, 2010; accepted August 16, 2010. Date of current version December 27, 2010. This work was supported by the NSF under Grants CCF 04-47613, CCF 05-14846, CNS 07-16311, and CCF 07-29127. The material in this paper was presented in part at the Information Theory and Applications Workshop, San Diego, CA, January 2008 and the IEEE International Symposium on Information Theory, Toronto, ON, Canada, July 2008.

The authors are with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742 USA (e-mail: ersen@umd.edu; ulukus@umd.edu).

Communicated by A. Nosratinia, Associate Editor for Communication Networks.

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

Digital Object Identifier 10.1109/TIT.2010.2090215

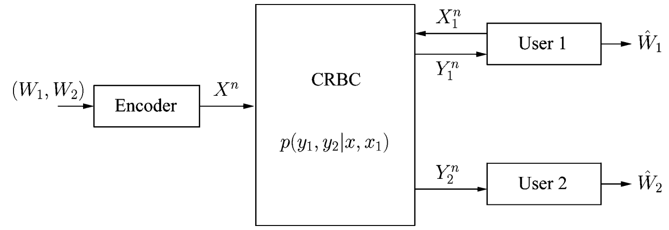

Fig. 1. Cooperative relay broadcast channel (CRBC) with single-sided cooperative link.

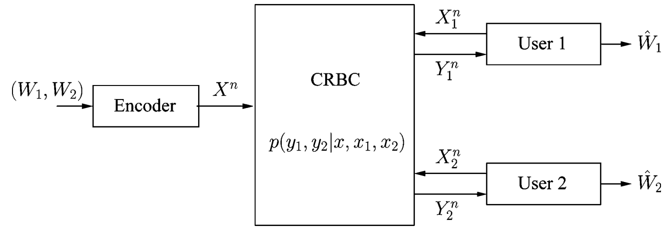

Fig. 2. Cooperative relay broadcast channel (CRBC) with a two-sided cooperation link.

instance, a transmitter can broadcast two different contents intended for two different receivers. The transmitter would want each receiver to decode only the content they paid for (or subscribed to) but be unable to decode the other content they have not paid for (or not subscribed to). However, since both receivers are valid members of the transmitter's network, they have incentive to (or be required to) help each other. Similarly, there can be military or other organizational networks, where even though multiple users are valid members of a network (hence are nonmalicious), they may have different clearance levels with respect to the transmitted information. In this scenario also, users would want to (or be required to) help each other, but would not be allowed to decode each other's message.

Our motivation to study this problem in a CRBC setting can be best explained in a Gaussian example. Imagine a two-user Gaussian BC. This BC is degraded in one direction, hence both users cannot have positive secrecy rates simultaneously [1], [8], [9]. This has motivated [9] to use multiple antennas at the transmitter in order to remove this degradedness in either of the directions and provide positive secrecy rates to both users simultaneously. We wish to achieve a similar effect with a single transmitter antenna, by introducing cooperation from one user to the other. Imagine now a Gaussian CRBC [19], [20] as in Fig. 1, where user 1 acts as a relay for user 2's message, i.e., that there is a cooperative link from user 1 to user 2. Let us assume that in the underlying BC, user 1 has a better channel. Without the cooperative link, user 2 cannot have secure communication with the transmitter. We show that user 1 can transmit cooperative signals and improve the secrecy rate of user 2. Our main idea is that user 1 can use a compress-and-forward (CAF) based relaying scheme to help user 2, and increase user 2's rate to a level which is not decodable by user 1. (This is possible because in the CAF scheme, user 1 does not decode the message of user 2 to help, instead, user 1 forms the compressed version of its observation and sends it to the second user.) Thus, the CAF scheme improves user 2's secrecy. Now, let us assume that in the underlying BC, user 1 has the worse channel. Without cooperation, user 1 cannot have secure communication with the transmitter. We show that user 1 can transmit a jamming signal in the cooperative channel first to guarantee a positive secrecy rate for itself assuming it has enough power. This essentially brings the system to the setting described in the previous case, and now user 1 can send a cooperative signal to user 2 to help it achieve a positive secrecy rate as well.

In this paper, we propose an achievable scheme that combines Marton's coding scheme for BCs [22] and Cover and El Gamal's CAF scheme for relay channels [17]. A similar achievable scheme has appeared in [23] which does not consider any secrecy constraints, hence ours can be viewed as a generalization of [23] to a secrecy context. A similar achievable scheme also appeared in [11]–[13], where CAF is applied to a relay channel to provide improved secrecy for the main transmitter. A relay channel can be considered as a special case of the single-sided CRBC where the rate of the first user is set to zero.

In this paper, we also develop a single-letter outer bound on the rate-equivocation region; we accomplish singe-letterization by using tools proposed in [2], namely by determining suitable auxiliary random variables. Besides this outer bound, for the second user, that is being helped in the single-sided CRBC, we develop another single-letter outer bound which depends only on the channel inputs and outputs.

To visualize the effects of cooperation on secrecy, we consider a Gaussian CRBC and show that both users can have positive secrecy rates through user cooperation. To obtain positive secrecy rates for both users, we provide different assignments for the auxiliary random variables appearing in the achievable rates. These auxiliary random variable assignments have dirty paper coding (DPC) interpretations [24]. In addition, we combine jamming and relaying to provide secrecy for both users when the relaying user is weak. Finally, we consider the CRBC with a two-sided cooperation link and provide an achievable scheme for this channel.

II. The Channel Model and Definitions

From here until the beginning of Section VIII, we will focus on a single-sided CRBC, and refer to it simply as CRBC. The CRBC can be viewed as a relay channel where the transmitter sends messages both to the relay node and the destination. Therefore, one of the users, user 1 in our case, in a CRBC both decodes its own message and also helps the other user. A CRBC consists of two message sets $w_1 \in \mathcal{W}_1$, $w_2 \in \mathcal{W}_2$, two input alphabets, one at the transmitter $x \in \mathcal{X}$ and one at user 1 $x_1 \in \mathcal{X}_1$, and two output alphabets $y_1 \in \mathcal{Y}_1$, $y_2 \in \mathcal{Y}_2$, where the former is for user 1 and the latter is for user 2. The channel is assumed to be memoryless and its transition probability distribution is $p(y_1, y_2|x, x_1)$.

A $\left(2^{nR_1}, 2^{nR_2}, n\right)$ code for this channel consists of two message sets as $\mathcal{W}_1 = \left\{1, \ldots, 2^{nR_1}\right\}$ and $\mathcal{W}_2 = \left\{1, \ldots, 2^{nR_2}\right\}$, an encoder at the transmitter with mapping $\mathcal{W}_1 \times \mathcal{W}_2 \longrightarrow \mathcal{X}^n$, a set of relay functions at user 1, $x_{1,i} = f_i(y_{1,1}, \ldots, y_{1,i-1})$ for $1 \leq i \leq n$, two decoders, one at each user with the mappings $g_1 : \mathcal{Y}_1^n \longrightarrow \mathcal{W}_1$ and $g_2 : \mathcal{Y}_2^n \longrightarrow \mathcal{W}_2$. The probability of error is defined as $P_e^n = \max\left\{P_{e,1}^n, P_{e,2}^n\right\}$ where $P_{e,1}^n =$

$\Pr(g_1(Y_1^n) \neq W_1)$, $P_{e,2}^n = \Pr(g_2(Y_2^n) \neq W_2)$. The secrecy of the users is measured by the equivocation rates which are $\frac{1}{n}H(W_1|Y_2^n)$ and $\frac{1}{n}H(W_2|Y_1^n, X_1^n)$. Since user 1 has its own channel input, we condition the entropy rate of user 2's messages on this channel input.

A rate tuple $(R_1, R_2, R_{e,1}, R_{e,2})$ is said to be achievable if there exists a $\left(2^{nR_1}, 2^{nR_2}, n\right)$ code with $\lim_{n \to \infty} P_e^n = 0$ and

$$\lim_{n \to \infty} \frac{1}{n} H(W_1|Y_2^n) \geq R_{e,1} \tag{1}$$

$$\lim_{n \to \infty} \frac{1}{n} H(W_2|Y_1^n, X_1^n) \geq R_{e,2}. \tag{2}$$

III. An Achievable Scheme

We now provide an achievable scheme which combines Marton's coding scheme for BCs [22], the random binning scheme of [1], [2] for wiretap channels, and Cover and El Gamal's CAF scheme for relay channels [17]. A similar achievable scheme has appeared in [23] without any secrecy considerations. The corresponding achievable rate-equivocation region is given by the following theorem.

Theorem 1: The rate tuples $(R_1, R_2, R_{e,1}, R_{e,2})$ satisfying

$$R_1 \leq I(V_1; Y_1|X_1) \tag{3}$$

$$R_2 \leq I(V_2; Y_2, \hat{Y}_1|X_1) \tag{4}$$

$$\begin{aligned} R_1 + R_2 \leq\ & I(V_1; Y_1|X_1) + I(V_2; Y_2, \hat{Y}_1|X_1) \\ & - I(V_1; V_2) \end{aligned} \tag{5}$$

$$R_{e,1} \leq R_1 \tag{6}$$

$$\begin{aligned} R_{e,1} \leq\ & \big[I(V_1; Y_1|X_1) - I(V_1; Y_2, \hat{Y}_1|V_2, X_1) \\ & - I(V_1; V_2)\big]^+ \end{aligned} \tag{7}$$

$$R_{e,2} \leq R_2 \tag{8}$$

$$\begin{aligned} R_{e,2} \leq\ & \big[I(V_2; Y_2, \hat{Y}_1|X_1) - I(V_2; Y_1|V_1, X_1) \\ & - I(V_1; V_2)\big]^+ \end{aligned} \tag{9}$$

are achievable for any distribution of the form

$$p(v_1, v_2)p(x|v_1, v_2)p(x_1)p(\hat{y}_1|x_1, v_1, y_1)p(y_1, y_2|x, x_1) \tag{10}$$

subject to the constraint

$$I(\hat{Y}_1; Y_1|X_1, V_1) \leq I(\hat{Y}_1, X_1; Y_2). \tag{11}$$

This theorem is a special case of Theorem 4 and obtained from the latter by setting $U = X_1$. Therefore, we will omit the proof of Theorem 1 here and will provide the proof of Theorem 4 in Appendix IV. In (7) and (9), $(x)^+$ is the positivity operator, i.e., $(x)^+ = \max(0, x)$.

In the achievable scheme given in Theorem 1, the transmitter uses a coding scheme that blends Marton's coding scheme and the random binning scheme of [1], [2]. Intuitively, the transmitter divides each user's message into two parts as the confidential and nonconfidential parts, where the confidential part needs to be transmitted in perfect secrecy whereas there is no secrecy constraint on the nonconfidential part. The division of each message into two parts forms the basis of the random binning scheme used in [1], [2] to provide confidentiality. In particular, the nonconfidential message can be viewed as the necessary randomness to protect the confidential message. The transmitter encodes all these messages by using Marton's coding scheme, where the messages of one user, say user 1, are first encoded by using a standard single-user codebook, and the messages of the other user, say user 2, are encoded by using Gelfand–Pinsker's scheme [25]. While using Gelfand–Pinsker's scheme [25] for user 2's messages, the knowledge of user 1's codeword is exploited to improve the rate of user 2. Furthermore, to enlarge the achievable region, the transmitter can reverse the order of encoding, i.e., first encode user 2's messages, next encode user 1's messages by using the knowledge of user 2's codeword, and also use time-sharing between the two possible encoding orders. In the achievable scheme given in Theorem 1, user 1 first decodes its own message, and next uses the CAF scheme to help user 2, i.e., forms a compressed version of its own observation and sends it to user 2. However, there are slight differences between the CAF used in the achievable scheme given in Theorem 1 and the original form of the CAF scheme in [17]. These differences originate from the secrecy concerns in our model, and are outlined in the following remark.

Remark 1: We note that both the form of the probability distribution in (10) and the constraint in (11) in Theorem 1 are somewhat different than those of the classical CAF scheme in [17]. First, we condition the distribution of $\hat{Y}_1$ on V_1 to prevent the compressed version of Y_1 to leak any additional information regarding user 1's message on top of what user 2 already has through its own observation. The constraint in (11) also reflects this concern. Similar constraints on the distribution of $\hat{Y}_1$ and on the compression rate have appeared in [23], where these modifications are not due to secrecy constraints contrary to here. In [23], these are imposed to obtain higher rates for user 2 by removing user 1's private message from the compressed signal, whereas here, they are imposed not to let $\hat{Y}_1$ leak any additional information regarding user 1's message. Moreover, if we let user 1 compress its observation without erasing its own message from the observation, i.e., if we change the conditional distribution of $\hat{Y}_1$ to $p(\hat{y}_1|x_1, y_1)$, we can recover the constraint in [17] (see (29)–(31) in [23]).

Remark 2: If we disable the assistance of user 1 to user 2 by setting $X_1 = \hat{Y}_1 = \phi$, the channel model reduces to the BC with secrecy constraints, and the achievable equivocation region becomes

$$R_{e,1}^{BC} \leq I(V_1; Y_1) - I(V_1; Y_2|V_2) - I(V_1; V_2) \tag{12}$$

$$R_{e,2}^{BC} \leq I(V_2; Y_2) - I(V_2; Y_1|V_1) - I(V_1; V_2) \tag{13}$$

where we require the Markov chain $(V_1, V_2) \rightarrow X \rightarrow (Y_1, Y_2)$. This result was derived in [9].

Remark 3: If we disable both cooperation between receivers by setting $X_1 = \hat{Y}_1 = \phi$, and also the confidential messages sent to user 1 by setting $V_1 = \phi$, the channel model reduces to the single-user eavesdropper channel, and the achievable equivocation rate for the second user becomes

$$R_{e,2} \leq I(V_2; Y_2) - I(V_2; Y_1) \tag{14}$$

and the Markov chain $V_2 \rightarrow X \rightarrow (Y_1, Y_2)$ is required by the probability distribution in (10). This is exactly the secrecy capacity of the single-user eavesdropper channel given in [2].

Remark 4: If we disable the confidential messages sent to user 1 by setting $V_1 = \phi$, the channel model reduces to a relay channel with secrecy constraints, and the achievable equivocation rate for the second user becomes

$$R_{e,2} \leq I(V_2; Y_2, \hat{Y}_1 | X_1) - I(V_2; Y_1 | X_1) \tag{15}$$

subject to

$$I(\hat{Y}_1; Y_1 | X_1) \leq I(\hat{Y}_1, X_1; Y_2) \tag{16}$$

and the corresponding joint distribution reduces to $p(v_2, x)p(x_1)p(\hat{y}_1|x_1, y_1)p(y_1, y_2|x, x_1)$. Further, if we make the potentially suboptimal selection of $V_2 = X$, the corresponding achievable secrecy rate and the constraint coincide with their counterparts found in [11], [13] for the relay channel.

Remark 5: By comparing the equivocation rates of the users in (7) and (9) and the equivocation rates of the users in the corresponding BC given in (12) and (13), we observe that the equivocation rate of user 1 may decrease depending on the information contained in $\hat{Y}_1$ and the equivocation rate of user 2 may increase depending on the channel conditions.

Remark 6: We will show in the next section, where we develop outer bounds for the rate-equivocation region, that if the channel of user 2 is degraded with respect to the channel of user 1 then $R_{e,2} = 0$ (see Remark 8), where degradedness is defined through the Markov chain $X \rightarrow (X_1, Y_1) \rightarrow Y_2$. Here, we show, as an interesting evaluation, that this achievable scheme cannot yield any positive secrecy rates in this case, as expected

$$\begin{aligned}
&I(V_2; Y_2, \hat{Y}_1 | X_1) - I(V_2; Y_1 | V_1, X_1) - I(V_1; V_2) \\
&\quad \leq I(V_2; Y_2, \hat{Y}_1, V_1 | X_1) - I(V_2; Y_1 | V_1, X_1) \\
&\qquad - I(V_1; V_2) && (17)\\
&\quad = I(V_2; Y_2, \hat{Y}_1 | V_1, X_1) + I(V_2; V_1 | X_1) \\
&\qquad - I(V_2; Y_1 | V_1, X_1) - I(V_1; V_2) && (18)\\
&\quad = I(V_2; Y_2, \hat{Y}_1 | V_1, X_1) - I(V_2; Y_1 | V_1, X_1) && (19)\\
&\quad \leq I(V_2; Y_2, \hat{Y}_1, Y_1 | V_1, X_1) - I(V_2; Y_1 | V_1, X_1) && (20)\\
&\quad = I(V_2; Y_2, Y_1 | V_1, X_1) + I(V_2; \hat{Y}_1 | V_1, X_1, Y_1, Y_2) \\
&\qquad - I(V_2; Y_1 | V_1, X_1) && (21)\\
&\quad = I(V_2; Y_2, Y_1 | V_1, X_1) - I(V_2; Y_1 | V_1, X_1) && (22)\\
&\quad = I(V_2; Y_2 | V_1, X_1, Y_1) && (23)\\
&\quad = 0 && (24)
\end{aligned}$$

where in (19), we used the fact that X_1 and (V_1, V_2) are independent, i.e., $I(V_1; V_2 | X_1) = I(V_1; V_2)$, in (22), we used the Markov chain $(V_2, Y_2) \rightarrow (V_1, X_1, Y_1) \rightarrow \hat{Y}_1$ which implies $I(V_2; \hat{Y}_1 | V_1, X_1, Y_1, Y_2) = 0$, and in (24), we used the Markov chain $(V_1, V_2) \rightarrow X \rightarrow (X_1, Y_1) \rightarrow Y_2$ which is due to the assumed degradedness.

IV. An Outer Bound

We now provide an outer bound for the rate-equivocation region. Our first outer bound in Theorem 2 uses auxiliary random variables. Next, in Theorem 3, we provide a simpler outer bound for user 2 using only the channel inputs and outputs, without employing any auxiliary random variables.

Theorem 2: The rate-equivocation region of the CRBC lies in the union of the following rate tuples[1]:

$$\begin{aligned}
R_1 &\leq I(V_1; Y_1 | X_1) && (25)\\
R_2 &\leq I(V_2; Y_2) && (26)\\
R_{e,1} &\leq \min\left\{\tilde{R}_{e,1}, \bar{R}_{e,1}, R_1\right\} && (27)\\
R_{e,2} &\leq \min\left\{\tilde{R}_{e,2}, \bar{R}_{e,2}, R_2\right\} && (28)
\end{aligned}$$

where

$$\begin{aligned}
\tilde{R}_{e,1} &= I(V_1; Y_1 | U) - I(V_1; Y_2 | U) && (29)\\
\tilde{R}_{e,2} &= I(V_2; Y_2 | U) - I(V_2; Y_1 | U) && (30)\\
\bar{R}_{e,1} &= I(V_1; Y_1 | V_2) - I(V_1; Y_2 | V_2) && (31)\\
\bar{R}_{e,2} &= I(V_2; Y_2 | V_1) - I(V_2; Y_1 | V_1) && (32)
\end{aligned}$$

where the union is taken over all joint distributions satisfying the Markov chain

$$U \rightarrow (V_1, V_2) \rightarrow (X, X_1, Y_1) \rightarrow Y_2. \tag{33}$$

The proof of this theorem is given in Appendix I.

The outer bounds on the equivocation rates given in Theorem 2 are reminiscent of the outer bound for the secrecy capacity of the discrete memoryless wiretap channel obtained in [2]. While the outer bound in [2] is tight for the wiretap channel, the outer bounds here for the CRBC are generally not tight. However, our outer bounds can be interpreted by referring to the outer bound in [2]. For example, user 1's equivocation rate is bounded by the minimum of three terms, see (27), where the first term, see (29), can be viewed as an outer bound for the secrecy capacity of the wiretap channel between the transmitter, user 1 (main receiver) and user 2 (eavesdropper), when one ignores the message sent to user 2, because this outer bound does not involve V_2. The second term, see (31), can be viewed similarly. This outer bound now considers the message sent to user 2, however, eliminates it by conditioning both mutual information terms in (31) on V_2.

Remark 7: The bounds on the equivocation rates in Theorem 2 and those in [9], where the outer bounds are for the equivocation rates in a two-user BC with per-user secrecy constraints as in here, have the same expressions. The only difference between the two outer bounds is in the Markov chain over which the union is taken. The Markov chain in (33) contains the one in [9], which is

$$U \rightarrow (V_1, V_2) \rightarrow X \rightarrow (Y_1, Y_2) \tag{34}$$

[1] Unfortunately, in the conference version [26] of this paper, the outer bound appeared with some typos.

which means that our outer bound here evaluates to a larger region than the one in [9]. This should be expected since the achievable rate-equivocation region here in our CRBC contains the achievable region in the BC.

We also provide a simpler outer bound for the equivocation rate of user 2 which does not involve any auxiliary random variables.

Theorem 3: The equivocation rate of user 2 is bounded as follows:

$$R_{e,2} \leq \max_{p(x,x_1)} I(X;Y_2|X_1,Y_1). \tag{35}$$

The proof of this theorem is given in Appendix II.

This outer bound is obtained by providing extra (i.e., side) information to user 2. In particular, to obtain the outer bound in Theorem 3, we consider a new channel where user 2 has access to user 1's observation. Thus, in this new channel, user 2's observation is improved as compared to the original channel. Consequently, an outer bound for the new channel also serves as an outer bound for the original channel.

Remark 8: If the channel is degraded, then the equivocation rate of user 2 is zero, since

$$I(X;Y_2|X_1,Y_1) = 0 \tag{36}$$

which follows from the Markov chain $X \rightarrow (X_1,Y_1) \rightarrow Y_2$ which is a consequence of the degradedness.

Remark 9: We generally expect the outer bound in Theorem 3 to be loose because it essentially assumes that user 2 has a complete access to user 1's observation[2] whereas, in reality, user 2 has only limited information about user 1's observation, which it obtains through the cooperative link. However, if the link from user 1 to user 2 is strong enough, user 1 may be able to convey its observation to user 2 precisely in which case the outer bound in Theorem 3 can be close to the achievable rate obtained via the CAF scheme. For example, such a situation arises if the channel satisfies the following Markov chain

$$X \rightarrow (X_1,Y_2) \rightarrow Y_1. \tag{37}$$

For such channels, by selecting $V_2 = X$, $V_1 = \hat{Y}_1 = \phi$ in the achievable scheme, we get the following equivocation rate for user 2

$$\begin{aligned} & I(X;Y_2|X_1) - I(X;Y_1|X_1) \\ & = I(X;Y_2,Y_1|X_1) - I(X;Y_1|X_1) \qquad (38) \\ & = I(X;Y_2|X_1,Y_1) \qquad (39) \end{aligned}$$

where the first equality is due to the Markov chain in (37). Hence, the outer bound in (35) gives the secrecy capacity for channels satisfying (37).

Remark 10: Although we are able to provide a simple outer bound for the equivocation rate of user 2, that depends only on the channel inputs and outputs, finding such a simple outer bound for the equivocation rate of user 1 does not seem to be possible. One reason for this is that, user 1 can use its observation, i.e., Y_1, for encoding its input, i.e., X_1, and create correlation between its channel inputs and outputs across time. Consequently, this correlation cannot be accounted for without using auxiliary random variables. Another reason will be discussed in Remark 13.

V. An Example: Gaussian CRBC

We now provide an example to show how the proposed achievable scheme can enlarge the secrecy region for a Gaussian BC. The channel outputs of a Gaussian CRBC are

$$Y_1 = X + Z_1 \tag{40}$$

$$Y_2 = X + X_1 + Z_2 \tag{41}$$

where $Z_1 \sim \mathcal{N}(0,N_1)$, $Z_2 \sim \mathcal{N}(0,N_2)$ and are independent, $E\left[X^2\right] \leq P$, $E\left[X_1^2\right] \leq aP$. In this section, we assume that $N_2 > N_1$, i.e., user 1 has a stronger channel in the corresponding BC. Note that, in this case, if user 1 does not help user 2, e.g., in the corresponding BC, $R_{e,2} = 0$. We present two different achievable schemes for this channel where each one corresponds to a particular selection of the underlying random variables in Theorem 1 satisfying the probability distribution condition in (10). Proposition 1 assigns independent channel inputs for each user, whereas Proposition 2 uses a DPC scheme. For simplicity, we provide only the achievable equivocation region in the following propositions.

Proposition 1: The following equivocation rates are achievable for all $\alpha \in [0,1]$

$$R_{e,1} \leq \frac{1}{2}\log\left(1+\frac{\alpha P}{\bar{\alpha}P+N_1}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{N_2}\right) \tag{42}$$

$$\begin{aligned} R_{e,2} \leq & \frac{1}{2}\log\left(1+\bar{\alpha}P\left(\frac{1}{\alpha P+N_2}+\frac{1}{N_1+N_c}\right)\right) \\ & -\frac{1}{2}\log\left(1+\frac{\bar{\alpha}P}{N_1}\right) \qquad (43) \end{aligned}$$

where $\bar{\alpha} = 1-\alpha$ and N_c is subject to

$$N_c \geq \frac{N_2(\bar{\alpha}P+N_1)+P(\alpha\bar{\alpha}P+N_1)}{aP}. \tag{44}$$

Proof: This achievable region can be obtained by selecting $V_1 \sim \mathcal{N}(0,\alpha P)$, $V_2 \sim \mathcal{N}(0,\bar{\alpha}P)$, $X = V_1 + V_2$, $X_1 \sim \mathcal{N}(0,aP)$, $\hat{Y}_1 = Y_1 - V_1 + Z_c = V_2 + Z_1 + Z_c$ and $Z_c \sim \mathcal{N}(0,N_c)$, where V_1, V_2, X_1 and Z_c are independent. The rates are found by direct calculation of the expressions in Theorem 1 using the above selection of random variables. ■

This achievable region can be enlarged by introducing correlation between V_1, V_2. Since a joint encoding is performed at the transmitter, one of the users' signals can be treated as a noncausally known interference, and DPC [24] can be used. In the

[2] In fact, this Sato-type [27] upper-bounding technique is used as a first step (before introducing noise correlation to tighten the upper bound) in finding the secrecy capacity of the MIMO wiretap channel [28]–[31].

following proposition, the transmitter treats user 2's signal as a noncausally known interference.

Proposition 2: The following equivocation rates are achievable for any γ and all $\alpha \in [0,1]$

$$R_{e,1} \le \frac{1}{2}\log\left(1+\frac{(\bar{\alpha}\gamma+\alpha)^2P}{(\alpha+\gamma^2\bar{\alpha})N_1+(\gamma-1)^2\alpha\bar{\alpha}P}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{N_2}\right) - \frac{1}{2}\log\left(1+\gamma^2\frac{\bar{\alpha}}{\alpha}\right) \quad (45)$$

$$R_{e,2} \le \frac{1}{2}\log\left(1+\frac{\bar{\alpha}P}{\alpha P+N_2}+\frac{\bar{\alpha}(1-\gamma)^2P}{N_1+N_c}\right) - \frac{1}{2}\log\left(1+\frac{\alpha\bar{\alpha}(\gamma-1)^2P}{(\alpha+\gamma^2\bar{\alpha})N_1}\right) - \frac{1}{2}\log\left(1+\gamma^2\frac{\bar{\alpha}}{\alpha}\right) \quad (46)$$

where $\bar{\alpha} = 1-\alpha$ and N_c is subject to

$$N_c \ge \frac{-\eta+\sqrt{\eta^2+4\theta\omega}}{2\theta} \quad (47)$$

where

$$\theta = a(\alpha+\bar{\alpha}\gamma^2)P \quad (48)$$

$$\eta = \left(\alpha+\gamma^2\bar{\alpha}\right)P\left[aN_1+(1-\gamma)^2\bar{\alpha}P(a+\bar{\alpha})\right] - (P+N_2)\left[N_1(\alpha+\gamma^2\bar{\alpha})+\alpha\bar{\alpha}(\gamma-1)^2P\right] \quad (49)$$

$$\omega = \left\{(P+N_2)\left[(1-\gamma)^2\bar{\alpha}P+N_1\right] - (1-\gamma)^2\bar{\alpha}^2P^2\right\} \times \left\{N_1\left(\alpha+\gamma^2\bar{\alpha}\right)+P\alpha\bar{\alpha}(\gamma-1)^2\right\}. \quad (50)$$

Proof: These equivocation rates are obtained by applying DPC for user 1. Let the channel input of the transmitter be $X = U_1 + U_2$ where $U_1 \sim \mathcal{N}(0,\alpha P)$, $U_2 \sim \mathcal{N}(0,\bar{\alpha}P)$ and are independent. The auxiliary random variables are selected as $V_2 = U_2$, $V_1 = U_1 + \gamma U_2$, where for user 1, the signal of user 2 is treated as noncausally known interference at the transmitter. The channel output of user 1 is compressed as $\hat{Y}_1 = Y_1 - V_1 + Z_c = (1-\gamma)U_2 + Z_1 + Z_c$ where $Z_c \sim \mathcal{N}(0,N_c)$ is the compression noise. The channel input of user 1 is selected as $X_1 \sim \mathcal{N}(0,aP)$. Here, again, U_1, U_2, Z_c, and X_1 are all independent. The rates are then found by direct calculation of the expressions in Theorem 1 using the above selection of random variables. ■

We note that, in both of the propositions above, $R_{e,2}$ is a monotonically decreasing function of N_c. Consequently, achievable $R_{e,2}$ depends on the quality of the cooperative link between the users. If this link gets better allowing user 1 to convey its observation in a finer form, user 2's secrecy increases. For illustrative purposes, the rate regions given by Propositions 1 and 2 are evaluated for the parameters $P = 8$, $N_1 = 1$, $N_2 = 2$, and the corresponding plots are given in Figs. 3 and 4. Note that since $N_2 > N_1$, if there was no cooperation between the users, user 2 could not have a positive secrecy rate. We observe from these figures that, thanks to the cooperation of the users, both users enjoy positive secrecy rates. However, we observe that a positive secrecy for user 2 comes at the expense of a decrease in the secrecy of user 1. In particular, for both propositions, maximum secrecy rate for user 2 is achieved when user 1 does not have any message itself and acts as a pure relay for user 2. Similarly, user 1 achieves the maximum secrecy rate when user 2 does not have any message.

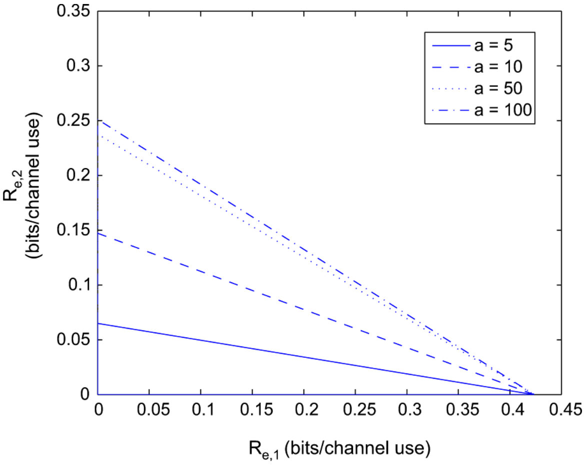

Fig. 3. Achievable equivocation rate region for single-sided CRBC using Proposition 1 where V_1 and V_2 are independent. $P = 8$, $N_1 = 1$, $N_2 = 2$, i.e., user 2 has no secrecy rate in the underlying BC.

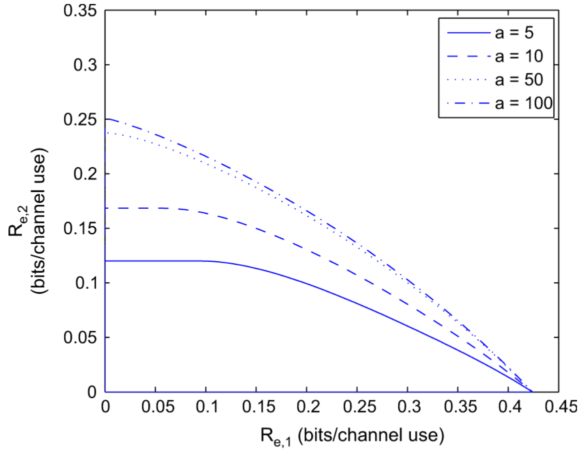

Fig. 4. Achievable equivocation region for single-sided CRBC using Proposition 2 where V_1, V_2 are correlated, admitting a DPC interpretation. $P = 8$, $N_1 = 1$, $N_2 = 2$, i.e., user 2 has no secrecy rate in the underlying BC.

We also note that the achievable secrecy rate regions for both Proposition 1 and Proposition 2 are monotonically increasing in a, i.e., the available power at user 1. In fact, for any given (P, N_1, N_2), there exist threshold values for a, denoted by $a_1^*(P,N_1,N_2)$ and $a_2^*(P,N_1,N_2)$, for Propositions 1 and 2, respectively, such that if $a \le a_1^*(P,N_1,N_2)$ (respectively $a \le a_2^*(P,N_1,N_2)$), Proposition 1 (respectively Proposition 2) cannot provide any positive secrecy rate for user 2, and if $a > a_1^*(P,N_1,N_2)$ (respectively $a > a_2^*(P,N_1,N_2)$), Proposition 1 (respectively Proposition 2) can provide a positive secrecy rate for user 2. Since the rate expressions involved in Propositions 1 and 2 are rather complicated, it does not seem that $a_j^*(P,N_1,N_2)$ admits a simple closed form expression. However, we numerically evaluated the threshold values for $(P = 8, N_1 = 1, N_2 = 2)$ (which is the parameter set that we use to obtain Figs. 3 and 4) as $a_1^*(8,1,2) \approx 3.25$ and $a_2^*(8,1,2) \approx 1.25$. Thus, for $(P = 8, N_1 = 1, N_2 = 2)$, the minimum power required at user 1 to provide a positive secrecy rate for user 2 by Proposition 2 is less than the minimum power required by Proposition 1. In fact, since Proposition 1 corresponds to a special case of Proposition 2, i.e., Proposition 1 can be recovered from Proposition 2 by setting $\gamma = 0$, in general, we have $a_2^*(P, N_1, N_2) \leq a_1^*(P, N_1, N_2)$.

Next, we note that, for both achievable schemes, as $a \longrightarrow \infty$, the equivocation rate of user 2 approaches a limit. This is due to the fact that, as $a \longrightarrow \infty$, the achievable equivocation rates are limited by the link between the transmitter and user 1. Moreover, as $a \longrightarrow \infty$, user 1 can send its observation to user 2 perfectly. Thus, in this case, user 2 can be assumed to have a channel output of (Y_1, Y_2), which makes the channel of user 1 degraded with respect to the channel of user 2. Consequently, following the analysis carried out in Remark 9, we expect the outer bound in Theorem 3 to become tight as $a \longrightarrow \infty$, which is stated in the next corollary.

Corollary 1: As $a \longrightarrow \infty$, the maximum achievable equivocation rate for user 2 becomes

$$R_{e,2} = \frac{1}{2}\log\left(1 + P\left(\frac{1}{N_1} + \frac{1}{N_2}\right)\right) - \frac{1}{2}\log\left(1 + \frac{P}{N_1}\right). \tag{51}$$

The proof of this corollary is given in Appendix III.

VI. Joint Jamming and Relaying

The proposed achievability scheme and its application to Gaussian CRBC show us that user cooperation can enlarge the secrecy region. However, this achievability scheme and the Gaussian example provide us with only a limited picture of what can be achieved. In particular, the achievability scheme proposed in Section III is designed with the cooperating user (user 1) being the stronger of the two users in mind. Next, we want to explore what can be done when the cooperating user (user 1) is the weaker of the two users. In this case, without the cooperative link, user 1 cannot have a positive secrecy rate. Therefore, the first question to ask is, whether user 1 can have a positive secrecy rate by utilizing the cooperative link. The answer to this question is positive if user 1 uses the cooperative link to send a jamming signal to user 2. However, a more interesting question is whether both users can achieve positive secrecy simultaneously. The following theorem provides an achievable scheme, where user 1 performs a combination of jamming and relaying, to provide both users with positive secrecy rates.

Theorem 4: The rate quadruples $(R_1, R_2, R_{e,1}, R_{e,2})$ satisfying

$$R_1 \leq I(V_1; Y_1|X_1) \tag{52}$$

$$R_2 \leq I(V_2; Y_2, \hat{Y}_1|U) \tag{53}$$

$$R_1 + R_2 \leq I(V_1; Y_1|X_1) + I(V_2; Y_2, \hat{Y}_1|U) - I(V_1; V_2) \tag{54}$$

$$R_{e,1} \leq R_1 \tag{55}$$

$$R_{e,1} \leq \left[I(V_1; Y_1|X_1) - I(V_1; Y_2, \hat{Y}_1|V_2, U) - I(V_1; V_2)\right]^+ \tag{56}$$

$$R_{e,2} \leq R_2 \tag{57}$$

$$R_{e,2} \leq \left[I(V_2; Y_2, \hat{Y}_1|U) - I(V_2; Y_1|V_1, X_1) - I(V_1; V_2)\right]^+ \tag{58}$$

are achievable for any distribution of the form

$$p(v_1, v_2)p(x|v_1, v_2)p(u)p(x_1|u)p(\hat{y}_1|u, v_1, y_1)p(y_1, y_2|x, x_1) \tag{59}$$

subject to the following constraint

$$I(\hat{Y}_1; Y_1|X_1, V_1, U) \leq I(\hat{Y}_1, U; Y_2). \tag{60}$$

The proof of this theorem is given in Appendix IV.

We note that the achievable scheme given in Theorem 4 corresponds to the generalization of the achievable scheme given in Theorem 1 by using *channel pre-fixing* [2] at user 1. Channel pre-fixing refers to the construction of a hypothetical channel between the encoding scheme used at user 1 and the channel input of user 1. By means of this hypothetical channel, additional randomness can be introduced, and this randomness might be useful to improve the equivocation rates [2]. Besides channel pre-fixing, both achievable schemes use the same techniques, namely Marton's achievable scheme and random binning at the transmitter, and CAF scheme at user 1.

Remark 11: In Theorem 4, U denotes the actual help signal, while the channel input X_1, which is correlated with U, may include an additional jamming attack. The intuition behind this achievable scheme is that, although user 2 should be able to decode U, it cannot decode the entire X_1. Therefore, since user 2 cannot decode and eliminate X_1 from Y_2, its channel becomes an attacked one, where decoding V_1 may be impossible. Therefore, in this scheme, user 1 first attacks user 2 to make its channel worse by associating U with many X_1s (hence, it confuses user 2), and then helps it to improve its secrecy rate.

Remark 12: We note that this achievable scheme is reminiscent of "cooperative jamming" [32]. In [32], the focus is on a two user MAC with an external eavesdropper, where one of the users attacks both the legitimate receiver and the eavesdropper, with the hope that it hurts the eavesdropper more than it hurts the legitimate receiver, and improves the secrecy of the legitimate receiver. In contrast, in our work, the relay (user 1) attacks user 2 to improve its own secrecy.

VII. Gaussian Example Revisited

Consider again the Gaussian CRBC, now with $N_1 > N_2$. The scheme proposed in Theorem 4 works as follows: user 1 divides X_1 into two parts. The first part carries the noise and the second part carries the bin index of $\hat{Y}_1$. Although Theorem 4 is valid for all cases, assume here that user 1 has large enough power. Then, the first part makes user 2's channel noisier than user 1's channel. This brings the situation to the case studied in Section V. Consequently, we can now have a positive secrecy rate for user 1, and also provide a positive secrecy rate to user 2, by sending a compressed version of Y_1 to it, as in Section V.

Proposition 3: The following equivocation rates are achievable for all $(\alpha, \beta) \in [0,1] \times [0,1]$

$$\begin{aligned} R_{e,1} \leq & \frac{1}{2}\log\left(1 + \frac{\alpha P}{\bar{\alpha}P + N_1}\right) \\ & - \frac{1}{2}\log\left(1 + \frac{\alpha P}{a\bar{\beta}P + N_2}\right) \end{aligned} \tag{61}$$

$$\begin{aligned} R_{e,2} \leq & \frac{1}{2}\log\left(1 + \bar{\alpha}P\left(\frac{1}{N_1 + N_c} \right.\right. \\ & \left.\left. + \frac{1}{\alpha P + N_2 + a\bar{\beta}P}\right)\right) \\ & - \frac{1}{2}\log\left(1 + \frac{\bar{\alpha}P}{N_1}\right) \end{aligned} \tag{62}$$

where $\bar{\alpha} = 1 - \alpha$, $\bar{\beta} = 1 - \beta$, and N_c is subject to

$$N_c \geq \frac{\bar{\alpha}P(\alpha P + N_2 + a\bar{\beta}P) + N_1(P + N_2 + a\bar{\beta}P)}{a\beta P}. \tag{63}$$

Proof: This achievable region is obtained by selecting the random variables in Theorem 4 as $X = V_1 + V_2$ where $V_1 \sim \mathcal{N}(0, \alpha P)$, $V_2 \sim \mathcal{N}(0, \bar{\alpha}P)$, $X_1 = U + Z_j$ where $U \sim \mathcal{N}(0, a\beta P)$, $Z_j \sim \mathcal{N}(0, a\bar{\beta}P)$, $\hat{Y}_1 = Y_1 - V_1 + Z_c = V_2 + Z_1 + Z_c$ where $Z_c \sim \mathcal{N}(0, N_c)$. Moreover, V_1, V_2, U, Z_j, Z_c are all independent. Here, Z_j serves as the jamming signal, and U serves as the helper signal. User 1 first jams user 2 and makes its channel noisier than its own by using Z_j and then helps user 2 through sending a compressed version of its observation by using U. The rates are then found by direct calculation of the expressions in Theorem 4 using the above selection of random variables. ■

Moreover, as in Section V, we can use DPC based schemes in this case also. The following proposition characterizes the DPC scheme for Theorem 4.

Proposition 4: The following equivocation rates are achievable for any γ and for all $(\alpha, \beta) \in [0,1] \times [0,1]$

$$\begin{aligned} R_{e,1} \leq & \frac{1}{2}\log\left(1 + \frac{(\bar{\alpha}\gamma + \alpha)^2 P}{(\alpha + \gamma^2\bar{\alpha})N_1 + (\gamma - 1)^2\alpha\bar{\alpha}P}\right) \\ & - \frac{1}{2}\log\left(1 + \frac{\alpha P}{(a\bar{\beta}P + N_2)}\right) \\ & - \frac{1}{2}\log\left(1 + \gamma^2\frac{\bar{\alpha}}{\alpha}\right) \end{aligned} \tag{64}$$

$$\begin{aligned} R_{e,2} \leq & \frac{1}{2}\log\left(1 + \frac{\bar{\alpha}P}{\alpha P + a\bar{\beta}P + N_2} + \frac{\bar{\alpha}(1 - \gamma)^2 P}{N_1 + N_c}\right) \\ & - \frac{1}{2}\log\left(1 + \frac{\alpha\bar{\alpha}(\gamma - 1)^2 P}{(\alpha + \gamma^2\bar{\alpha})N_1}\right) \\ & - \frac{1}{2}\log\left(1 + \gamma^2\frac{\bar{\alpha}}{\alpha}\right) \end{aligned} \tag{65}$$

where $\bar{\alpha} = 1 - \alpha$, $\bar{\beta} = 1 - \beta$ and N_c is subject to

$$N_c \geq \frac{-\eta + \sqrt{\eta^2 + 4\theta\omega}}{2\theta} \tag{66}$$

where

$$\theta = a\beta(\alpha + \bar{\alpha}\gamma^2)P \tag{67}$$

$$\begin{aligned} \eta = & \left(\alpha + \gamma^2\bar{\alpha}\right) P\left[a\beta N_1 + (1 - \gamma)^2\bar{\alpha}P(a\beta + \bar{\alpha})\right] \\ & - (P + a\bar{\beta}P + N_2)\left[N_1(\alpha + \gamma^2\bar{\alpha}) + \alpha\bar{\alpha}(\gamma - 1)^2 P\right] \end{aligned} \tag{68}$$

$$\begin{aligned} \omega = & \left[(P + a\bar{\beta} + N_2)\left[(1 - \gamma)^2\bar{\alpha}P + N_1\right] - (1 - \gamma)^2\bar{\alpha}^2P^2\right] \\ & \times \left[N_1\left(\alpha + \gamma^2\bar{\alpha}\right) + P\alpha\bar{\alpha}(\gamma - 1)^2\right]. \end{aligned} \tag{69}$$

Proof: All random variable selections are the same as in Proposition 2 except for X_1, U. Here, we choose $X_1 = Z_j + U$ and $U \sim \mathcal{N}(0, a\beta P)$, $Z_j \sim \mathcal{N}(0, a\bar{\beta}P)$. U, Z_j are independent. ■

We first note that Propositions 3, 4 reduce to Propositions 1, 2, respectively, by simply selecting $\beta = 0$, i.e., no jamming. We provide a numerical example in Figs. 5 and 6 for $P = 8$, $N_1 = 2$, $N_2 = 1$. Since $N_1 > N_2$, a positive secrecy rate for user 1 would not be possible if the cooperative link did not exist. However, if user 1 has enough power to make user 2's channel noisier by injecting Gaussian noise to it, user 1 can provide secrecy for itself. For user 1 to have positive secrecy, we need

$$a \geq \frac{N_1 - N_2}{P}. \tag{70}$$

Otherwise, user 1 cannot have positive secrecy by using strategies employed in Propositions 3, 4. In addition, contrary to Section V, we observe from Figs. 5 and 6 that here DPC based schemes do not provide any gain with respect to the independent selection of V_1, V_2. Furthermore, we also apply Propositions 3 and 4 to the case where user 1 is stronger than user 2 by selecting the noise variances as $N_1 = 1$, $N_2 = 2$ as in Section V to show that propositions presented in this section cover the ones in Section V. We provide the corresponding graphs in Figs. 7 and 8. Comparing Fig. 3 (respectively 4) and 7 (respectively 8), we observe that even though the maximum secrecy rate of user 2 remains the same, the maximum secrecy rate of user 1 is improved significantly. This improvement comes, because through Propositions 3 and 4, user 1 jams the receiver of user 2.

Next, we examine Figs. 3 and 7 in more detail. In Fig. 3, for instance when $a = 100$, the largest $R_{e,2}$, which is about 0.25 bits/channel use, is obtained when $R_{e,1} = 0$. This corresponds to the case where user 1's rate and secrecy rate are set to zero. In this case, user 1 serves as a pure relay for user 2. The secrecy rate we obtain at this extreme is the same as [11]–[13]. At the other extreme, the largest $R_{e,1}$, which is about 0.42 bits/channel use, is obtained when $R_{e,2} = 0$. In this case, user 2 is just an eavesdropper in a single-user channel from the transmitter to user 1. The secrecy rate we obtain at this extreme is the same as [1], [2], [33]. Moreover, as we see from Fig. 3, whenever user 1 helps user 2 to have positive secrecy, it needs to deviate from this extreme point. Thus, user 2's positive secrecy rates come at the expense of a decrease in user 1's secrecy rate. If we consider Fig. 7, the largest $R_{e,2}$ is the same as that in Fig. 3, which is again achieved when $R_{e,1} = 0$, i.e., when user 1 acts as a pure relay for user 2. However, in Fig. 7, user 1's maximum secrecy rate increases dramatically due to its jamming capabilities in Proposition 3. In Fig. 7, user 1 achieves its maximum secrecy rate, which is about 1.58 bits/channel use, when it uses all of its power for jamming user 2's receiver and when

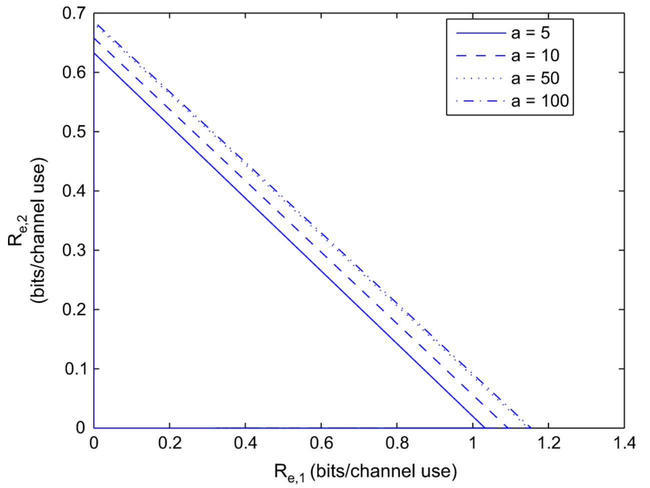

Fig. 5. Achievable equivocation rate region using Proposition 3 where user 1 jams and relays, and V_1, V_2 are independent. $P = 8, N_1 = 2, N_2 = 1$, i.e., user 1 cannot have any positive secrecy in the underlying BC.

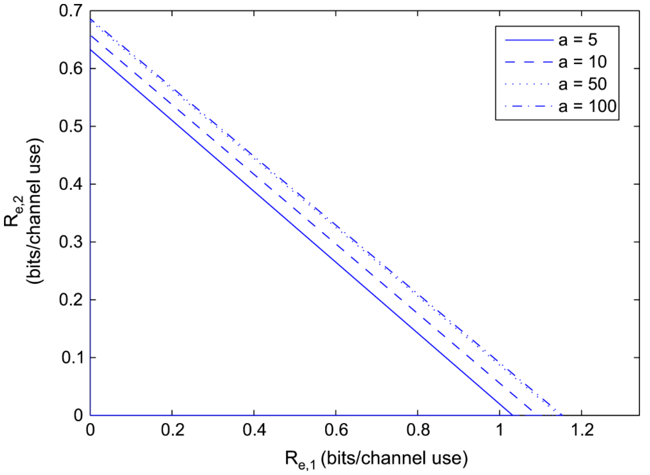

Fig. 6. Achievable equivocation rate region using Proposition 4 where user 1 jams and relays, and V_1, V_2 are correlated, admitting a DPC interpretation. $P = 8, N_1 = 2, N_2 = 1$, i.e., user 1 cannot have any positive secrecy in the underlying BC.

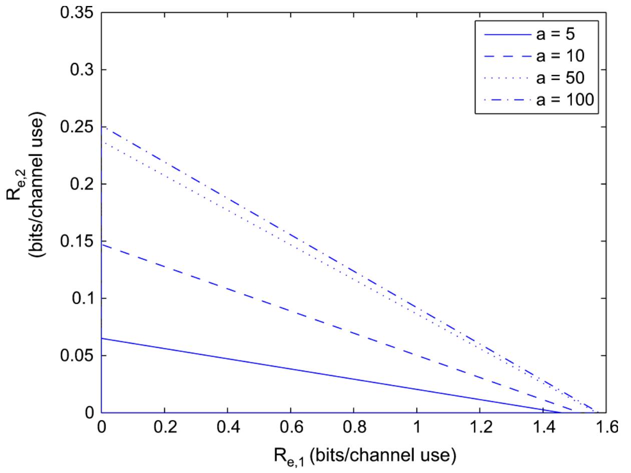

Fig. 7. Achievable equivocation rate region using Proposition 3 where user 1 jams and relays, and V_1, V_2 are independent. $P = 8, N_1 = 1, N_2 = 2$, i.e., user 1's channel is stronger than user 2.

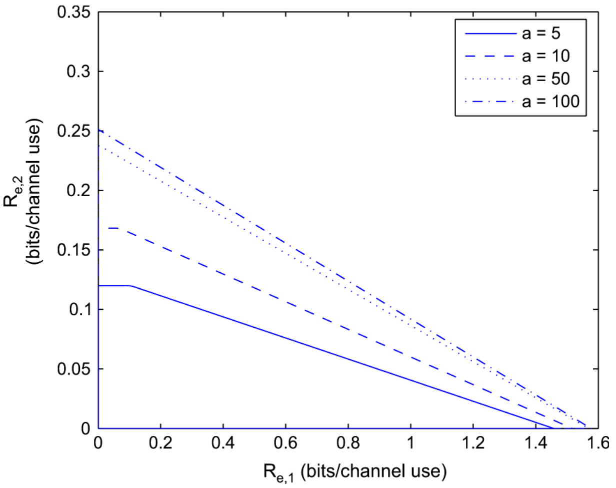

Fig. 8. Achievable equivocation rate region using Proposition 4 where user 1 jams and relays, and V_1, V_2 are correlated, admitting a DPC interpretation. $P = 8, N_1 = 1, N_2 = 2$, i.e., user 1's channel is stronger than user 2.

the rate of user 2 is set to zero. We note that this rate is larger than that is achievable in the corresponding single-user eavesdropper channel from the transmitter to user 1, while user 2 is an eavesdropper. We observe from Fig. 7 that when user 1 is able to jam and relay jointly, it can provide secrecy for user 2 while its own secrecy rate is still larger than that of the corresponding single-user eavesdropper channel. Thus, as opposed to the case where it can only relay, i.e., Proposition 1, both users enjoy secrecy in Proposition 3, while user 1 does not have to compromise from its own secrecy rate that is achievable in the underlying eavesdropper channel.

At first sight, this result may seem counterintuitive, because although user 1 spends some of its available power to jam user 2, user 2 still gets the same equivocation rate as if user 1 helps user 2 by using all its available power. However, this surprising result can be better understood by noting the fact that jamming and helping do not occur simultaneously, i.e., user 1 does not jam and help at the same time, instead, it uses time-sharing between jamming and relaying. In particular, Fig. 7 clearly demonstrates the fact that user 1 uses time-sharing between two extreme operating points of Proposition 3 in order to provide a larger achievable secrecy rate region than the one in Fig. 3. At one extreme operating point, user 1, to which no message is sent, acts as a pure relay for user 2, and at the other extreme operating point, user 1 acts as a pure jammer for user 2, to which no message is sent. The same conclusion holds for Fig. 8, i.e., Proposition 4, as well. However, in this case, at the extreme point where the maximum equivocation rate of user 2 is obtained, the equivocation rate of user 1 is not always zero, see the cases $a = 5, 10$ in Figs. 4 and 8. In particular, Fig. 9 shows the fact that user 1 employs time-sharing between two extreme operating points, where two extreme points, points A and B, are also noted.

Remark 13: We are now ready to discuss why we could not find an outer bound for the equivocation rate of user 1 that relies only on the channel inputs and outputs. To understand this, we first examine the outer bound we found on the equivocation rate of user 2 in Theorem 3. This outer bound is obtained by giving the entire observation of user 1 to user 2 (i.e., $N_c = 0$). Hence,

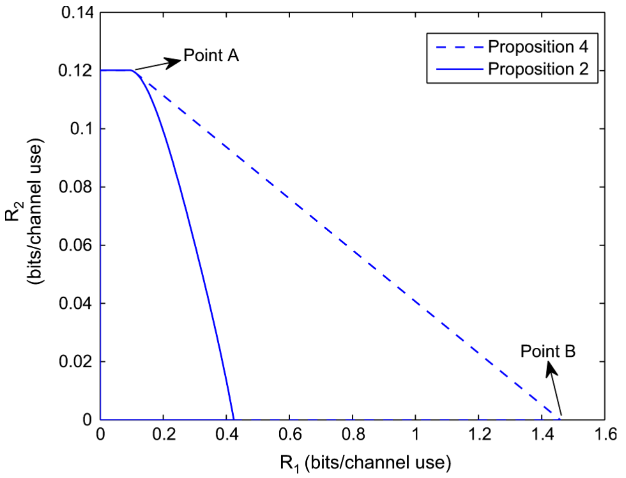

Fig. 9. Achievable equivocation rate regions using Propositions 2 and 4 where user 1 jams and relays, and V_1, V_2 are correlated, admitting a DPC interpretation. $a = 5$, $P = 8$, $N_1 = 1$, $N_2 = 2$, i.e., user 1's channel is stronger than user 2.

this is the best possible scenario as far as the channel of user 2 is concerned, and thus, it yields an outer bound. However, a similar approach cannot work for user 1, because although user 1 can have access to the observation of user 2, user 1 still has additional freedom (and opportunities) to increase its own secrecy rate by sending jamming signals over the cooperative link, as shown in this section. This is the main reason why we could not find a simple outer bound for user 1's secrecy rate using only the channel inputs/outputs.

VIII. Two-Sided Cooperation

In this section, we provide an achievable scheme for the CRBC with two-sided cooperation. In this case, each user can act as a relay for the other one; see Fig. 2. The corresponding channel consists of two message sets $w_1 \in \mathcal{W}_1$, $w_2 \in \mathcal{W}_2$, three input alphabets, one at the transmitter $x \in \mathcal{X}$, one at user 1 $x_1 \in \mathcal{X}_1$ and one at user 2 $x_2 \in \mathcal{X}_2$. The channel consists of two output alphabets denoted by $y_1 \in \mathcal{Y}_1$, $y_2 \in \mathcal{Y}_2$ at the two users. The channel is assumed to be memoryless and its transition probability distribution is $p(y_1, y_2|x, x_1, x_2)$.

A $\left(2^{nR_1}, 2^{nR_2}, n\right)$ code for this channel consists of two message sets as $\mathcal{W}_1 = \left\{1, \ldots, 2^{nR_1}\right\}$ and $\mathcal{W}_2 = \left\{1, \ldots, 2^{nR_2}\right\}$, an encoder at the transmitter which maps each pair $(w_1, w_2) \in (\mathcal{W}_1 \times \mathcal{W}_2)$ to a codeword $x^n \in \mathcal{X}^n$, a set of relay functions at user 1, $x_{1,i} = f_{1,i}(y_{1,1}, \ldots, y_{1,i-1})$, $1 \leq i \leq n$, and a set of relay functions at user 2, $x_{2,i} = f_{2,i}(y_{2,1}, \ldots, y_{2,i-1})$, $1 \leq i \leq n$, two decoders, one at user 1 and one at user 2 with the mappings $g_1 : \mathcal{Y}_1^n \rightarrow \mathcal{W}_1$, $g_2 : \mathcal{Y}_2^n \rightarrow \mathcal{W}_2$. Definitions for the error probability for this two-sided case are the same as in the single-sided case. The secrecy of the users is again measured by the equivocation rates which are $\frac{1}{n}H(W_1|Y_2^n, X_2^n)$ and $\frac{1}{n}H(W_2|Y_1^n, X_1^n)$. In this case, since user 2 has a channel input also, we condition the entropy rate of user 1's messages on this channel input.

A rate tuple $(R_1, R_2, R_{e,1}, R_{e,2})$ is said to be achievable if there exists a $\left(2^{nR_1}, 2^{nR_2}, n\right)$ code with $\lim_{n \rightarrow \infty} P_e^n = 0$, and

$$\lim_{n \rightarrow \infty} \frac{1}{n} H(W_1|Y_2^n, X_2^n) \geq R_{e,1} \tag{71}$$

$$\lim_{n \rightarrow \infty} \frac{1}{n} H(W_2|Y_1^n, X_1^n) \geq R_{e,2}. \tag{72}$$

The following theorem characterizes an achievable region for this channel model.

Theorem 5: The rate tuples $(R_1, R_2, R_{e,1}, R_{e,2})$ satisfying

$$R_1 \leq I(V_1; Y_1, \hat{Y}_2|X_1, U_2) \tag{73}$$

$$R_2 \leq I(V_2; Y_2, \hat{Y}_1|X_2, U_1) \tag{74}$$

$$R_1 + R_2 \leq I(V_1; Y_1, \hat{Y}_2|X_1, U_2) + I(V_2; Y_2, \hat{Y}_1|X_2, U_1) - I(V_1; V_2) \tag{75}$$

$$R_{e,1} \leq R_1 \tag{76}$$

$$R_{e,1} \leq \left[I(V_1; Y_1, \hat{Y}_2|X_1, U_2) - I(V_1; Y_2, \hat{Y}_1|V_2, X_2, U_1) - I(V_1; V_2)\right]^+ \tag{77}$$

$$R_{e,2} \leq R_2 \tag{78}$$

$$R_{e,2} \leq \left[I(V_2; Y_2, \hat{Y}_1|X_2, U_1) - I(V_2; Y_1, \hat{Y}_2|V_1, X_1, U_2) - I(V_1; V_2)\right]^+ \tag{79}$$

are achievable for any distribution of the form

$$p(v_1, v_2)p(x|v_1, v_2)p(u_1, x_1)p(\hat{y}_1|u_1, y_1)p(u_2, x_2) \times p(\hat{y}_2|u_2, y_2)p(y_1, y_2|x, x_1, x_2) \tag{80}$$

subject to the following constraints

$$I(\hat{Y}_1; Y_1|U_1, X_1, U_2) \leq I(\hat{Y}_1, U_1; Y_2|X_2) \tag{81}$$

$$I(\hat{Y}_2; Y_2|U_2, X_2, U_1) \leq I(\hat{Y}_2, U_2; Y_1|X_1). \tag{82}$$

The proof of this theorem is given in Appendix V.

Similar to the achievable schemes given in Theorems 1 and 4, the achievable scheme in Theorem 5 also blends Marton's achievable scheme for BCs [22], the random binning scheme of [2] to provide confidentiality, and the CAF scheme [17]. In particular, the transmitter uses Marton's achievable scheme and random binning, and each user employs a CAF-based cooperation scheme to help the other user. Similar to Theorem 4, in Theorem 5, channel pre-fixing is used as well. The main difference between the previous achievable schemes in Theorems 1, 4 and the achievable scheme in Theorem 5 comes from how CAF is performed as a cooperation strategy, and in particular, how compression is performed. Contrary to the previous achievable schemes given in Theorem 1 and 4, here users do not compress their observations after erasing their codewords from the observations; this is why we did not condition $\hat{Y}_1$ (respectively $\hat{Y}_2$) on V_1 (respectively V_2) in (80). In fact, they cannot remove their own codewords from their observations because each user employs a sliding-window type decoding scheme, i.e., they should wait until the next block to decode their own codewords, whereas compression should be performed right after the reception of the previous block, at which time they have not yet decoded their own messages. However, we note that this achievable scheme also provides opportunities for jamming as did the achievable scheme provided in Section VI.

IX. Gaussian Example for Two-Sided Cooperation

The channel outputs of a Gaussian CRBC with two-sided cooperation are

$$Y_1 = X + X_2 + Z_1 \tag{85}$$
$$Y_2 = X + X_1 + Z_2 \tag{86}$$

where $Z_1 \sim \mathcal{N}(0, N_1)$, $Z_2 \sim \mathcal{N}(0, N_2)$ and are independent, $E\left[X^2\right] \leq P$, $E\left[X_1^2\right] \leq a_1 P$, $E\left[X_2^2\right] \leq a_2 P$.

We present the following proposition which characterizes an achievable equivocation region.

Proposition 5: The equivocation rate pairs $(R_{e,1}, R_{e,2})$ satisfying (83)–(84) at the bottom of the page are achievable for all $(\alpha, \beta_1, \beta_2) \in [0,1]^3$ where $\bar{\alpha} = 1-\alpha$, $\bar{\beta}_1 = 1-\beta_1$, $\bar{\beta}_2 = 1-\beta_2$, and $N_{c,1}$, $N_{c,2}$ are subject to

$$N_{c,1} \geq \frac{-b_{11} + \sqrt{b_{11}^2 + 4a_{11}c_{11}}}{2a_{11}} \tag{87}$$
$$N_{c,2} \geq \frac{-b_{22} + \sqrt{b_{22}^2 + 4a_{22}c_{22}}}{2a_{22}} \tag{88}$$

and

$$a_{11} = a_1\beta_1 P \tag{89}$$
$$b_{11} = P\big(P + a_1\beta_1(P+N_1)\big) - (P + N_1 + a_2\bar{\beta}_2 P)(P + N_2 + a_1\bar{\beta}_1 P) \tag{90}$$
$$c_{11} = (P + N_1 + a_2\bar{\beta}_2 P)\big(PN_1 + (P+N_1)(N_2 + a_1\bar{\beta}_1 P)\big) \tag{91}$$
$$a_{22} = a_2\beta_2 P \tag{92}$$
$$b_{22} = P\big(P + a_2\beta_2(P+N_2)\big) - (P + N_1 + a_2\bar{\beta}_2 P)(P + N_2 + a_1\bar{\beta}_1 P) \tag{93}$$
$$c_{22} = (P + N_2 + a_1\bar{\beta}_1 P)\big(PN_2 + (P+N_2)(N_1 + a_2\bar{\beta}_2 P)\big). \tag{94}$$

Proof: This achievable region is obtained by selecting $X = V_1 + V_2$ where $V_1 \sim \mathcal{N}(0, \alpha P)$, $V_2 \sim \mathcal{N}(0, \bar{\alpha} P)$ and are independent, $X_i = U_i + \tilde{Z}_i$ where $U_i \sim \mathcal{N}(0, a_i\beta_i P)$, $\tilde{Z}_i \sim \mathcal{N}(0, a_i\bar{\beta}_i P)$, $i = 1,2$ and independent, and $\hat{Y}_i = Y_i + Z_{c,i}$ where $Z_{c,i} \sim \mathcal{N}(0, N_{c,i})$, $i = 1,2$ and are independent of all other random variables. Direct calculation of rates in Theorem 5 with these random variable selections yields the achievable region. ■

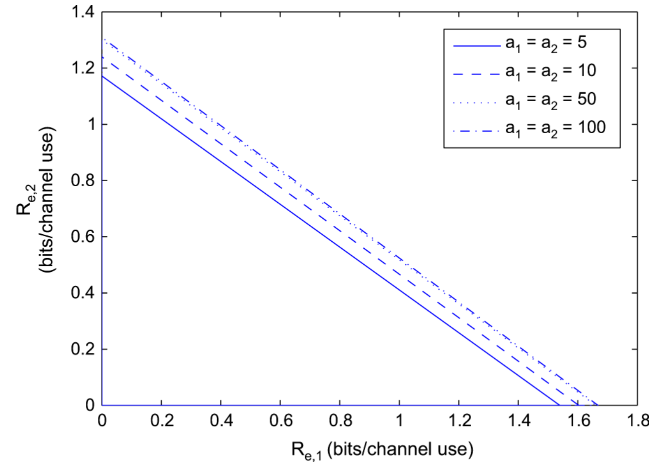

Fig. 10. Achievable equivocation rate region using Proposition 5 where each user can jointly jam and relay. $P = 8$, $N_1 = 1$, $N_2 = 2$, i.e., user 2 cannot have any positive secrecy in the underlying BC.

A numerical example is given in Fig. 10 for the case $P = 8$, $N_1 = 1$, $N_2 = 2$. Comparing Fig. 10 with Figs. 7 and 8, we observe that user 2's secrecy rate improves significantly because now user 2 can jam user 1 to improve its own secrecy rate. We also observe that user 1's secrecy rate improves as well, compared to Section VII. The increase in user 1's secrecy in this two-sided case is due to the fact that user 2 now acts as a relay for user 1. However, when user 1 jams user 2 using all of its power, it limits the help that comes from user 2, hence Theorem 5 provides only a modest secrecy rate increase for user 1 on top of what Theorem 4 already provides.

X. Conclusion

In this paper, we investigated the effects of cooperation on secrecy. We showed that user cooperation can increase secrecy, i.e., even an untrusted party can help. An important point to observe though is that whether cooperation can improve secrecy or not depends on the cooperation method employed. For instance, even though a decode-and-forward (DAF) based cooperation

$$R_{e,1} \leq \frac{1}{2}\log\left(1 + \frac{\alpha P(N_1 + a_2\bar{\beta}_2 P + N_2 + N_{c,2})}{\bar{\alpha} P(N_1 + a_2\bar{\beta}_2 P + N_2 + N_{c,2}) + (N_1 + a_2\bar{\beta}_2 P)(N_2 + N_{c,2})}\right) - \frac{1}{2}\log\left(1 + \alpha P\left(\frac{1}{a_1\bar{\beta}_1 P + N_2} + \frac{1}{N_1 + N_{c,1}}\right)\right) \tag{83}$$

$$R_{e,2} \leq \frac{1}{2}\log\left(1 + \frac{\bar{\alpha} P(N_2 + a_1\bar{\beta}_1 P + N_2 + N_{c,1})}{\alpha P(N_2 + a_1\bar{\beta}_1 P + N_1 + N_{c,1}) + (N_2 + a_1\bar{\beta}_1 P)(N_1 + N_{c,1})}\right) - \frac{1}{2}\log\left(1 + \alpha P\left(\frac{1}{a_2\bar{\beta}_2 P + N_1} + \frac{1}{N_2 + N_{c,2}}\right)\right). \tag{84}$$

scheme can increase the rate, it cannot improve the secrecy, because in this case the cooperating party, which is also the eavesdropper, needs to decode the message it forwards. However, in CAF, we do not require the cooperating party to decode the message. In fact, in CAF, the cooperating party helps increase the rate of the main transmitter to levels which it itself cannot decode, hence improving the secrecy of the main transmitter-receiver pair against itself.

Appendix I
Proof of Theorem 2

Here we prove the outer bound on the capacity-equivocation region of the CRBC given in Theorem 2 which closely follows the converse given in [2] and the outer bound in [9]. First, define the following random variables:

$$U_i = Y_1^{i-1} Y_{2,i+1}^n \tag{95}$$

$$V_{1,i} = W_1 U_i \tag{96}$$

$$V_{2,i} = W_2 U_i \tag{97}$$

which satisfy the following Markov chain

$$U_i \rightarrow (V_{1,i}, V_{2,i}) \rightarrow (X_i, X_{1,i}, Y_{1,i}) \rightarrow Y_{2,i} \tag{98}$$

but do not satisfy the following one:

$$U_i \rightarrow (V_{1,i}, V_{2,i}) \rightarrow (X_i, X_{1,i}) \rightarrow (Y_{1,i}, Y_{2,i}) \tag{99}$$

because of the encoding function employed at user 1 which can generate correlation between $Y_{1,i}$ and $\left(Y_{1,i+1}^n, Y_{2,i+1}^n\right)$ through $X_{1,i+1}$ that cannot be resolved by conditioning on $(X_i, X_{1,i})$. For a similar discussion, the reader can refer to [19].

We start with the achievable rate of user 1

$$nR_1 = H(W_1) = I(W_1; Y_1^n) + H(W_1|Y_1^n) \tag{100}$$

$$\leq I(W_1; Y_1^n) + \epsilon_n \tag{101}$$

$$= \sum_{i=1}^n I(W_1; Y_{1,i}|Y_1^{i-1}) + \epsilon_n \tag{102}$$

$$= \sum_{i=1}^n H(W_1|Y_1^{i-1}) - H(W_1|Y_1^{i-1}, Y_{1,i}) + \epsilon_n \tag{103}$$

$$= \sum_{i=1}^n H(W_1|Y_1^{i-1}, X_{1,i}) - H(W_1|Y_1^{i-1}, Y_{1,i}) + \epsilon_n \tag{104}$$

$$\leq \sum_{i=1}^n H(W_1|Y_1^{i-1}, X_{1,i}) - H(W_1|Y_1^{i-1}, Y_{1,i}, X_{1,i}) + \epsilon_n \tag{105}$$

$$= \sum_{i=1}^n I(W_1; Y_{1,i}|Y_1^{i-1}, X_{1,i}) + \epsilon_n \tag{106}$$

$$\leq \sum_{i=1}^n H(Y_{1,i}|X_{1,i}) - H(Y_{1,i}|Y_1^{i-1}, X_{1,i}, W_1) + \epsilon_n \tag{107}$$

$$\leq \sum_{i=1}^n H(Y_{1,i}|X_{1,i}) - H(Y_{1,i}|Y_1^{i-1}, X_{1,i}, W_1, Y_{2,i+1}^n) + \epsilon_n \tag{108}$$

$$= \sum_{i=1}^n I(V_{1,i}; Y_{1,i}|X_{1,i}) + \epsilon_n \tag{109}$$

where (101) is due to Fano's lemma, (104) follows from the Markov chain $W_1 \rightarrow Y_1^{i-1} \rightarrow X_{1,i}$, (105), (107) and (108) are due to the fact that conditioning cannot increase entropy, and (109) follows from the definition of $V_{1,i}$ in (96). Similarly, for the achievable rate of user 2, we have

$$nR_2 \leq I(W_2; Y_2^n) + \epsilon_n \tag{110}$$

$$= \sum_{i=1}^n I(W_2; Y_{2,i}|Y_{2,i+1}^n) + \epsilon_n \tag{111}$$

$$= \sum_{i=1}^n H(Y_{2,i}|Y_{2,i+1}^n) - H(Y_{2,i}|Y_{2,i+1}^n, W_2) + \epsilon_n \tag{112}$$

$$\leq \sum_{i=1}^n H(Y_{2,i}) - H(Y_{2,i}|Y_{2,i+1}^n, W_2, Y_1^{i-1}) + \epsilon_n \tag{113}$$

$$\leq \sum_{i=1}^n I(V_{2,i}; Y_{2,i}) + \epsilon_n \tag{114}$$

where (110) is due to Fano's lemma, (113) is due to the fact that conditioning cannot increase entropy, and (114) follows from the definition of $V_{2,i}$ given in (97).

We now derive the outer bounds on the equivocation rates. We start with user 1

$$nR_{e,1} = H(W_1|Y_2^n) = H(W_1) - I(W_1; Y_2^n) \tag{115}$$

$$= I(W_1; Y_1^n) - I(W_1; Y_2^n) + H(W_1|Y_1^n) \tag{116}$$

$$\leq I(W_1; Y_1^n) - I(W_1; Y_2^n) + \epsilon_n \tag{117}$$

$$= \sum_{i=1}^n I(W_1; Y_{1,i}|Y_1^{i-1}) - I(W_1; Y_{2,i}|Y_{2,i+1}^n) + \epsilon_n \tag{118}$$

$$\begin{aligned} = \sum_{i=1}^n & I(W_1, Y_{2,i+1}^n; Y_{1,i}|Y_1^{i-1}) \\ & - I(Y_{2,i+1}^n; Y_{1,i}|Y_1^{i-1}, W_1) \\ & - I(W_1, Y_1^{i-1}; Y_{2,i}|Y_{2,i+1}^n) \\ & + I(Y_1^{i-1}; Y_{2,i}|Y_{2,i+1}^n, W_1) + \epsilon_n \end{aligned} \tag{119}$$

where (117) is due to Fano's lemma. Using [2]

$$\sum_{i=1}^n I(Y_{2,i+1}^n; Y_{1,i}|Y_1^{i-1}, W_1) = \sum_{i=1}^n I(Y_1^{i-1}; Y_{2,i}|Y_{2,i+1}^n, W_1) \tag{120}$$

in (119), we obtain

$$nR_{e,1} \leq \sum_{i=1}^n I(W_1, Y_{2,i+1}^n; Y_{1,i}|Y_1^{i-1}) - I(W_1, Y_1^{i-1}; Y_{2,i}|Y_{2,i+1}^n) + \epsilon_n \tag{121}$$

$$\begin{aligned}&= \sum_{i=1}^{n} I(W_1; Y_{1,i}|Y_1^{i-1}, Y_{2,i+1}^{n}) \\ &\quad + I(Y_{2,i+1}^{n}; Y_{1,i}|Y_1^{i-1}) \\ &\quad - I(W_1; Y_{2,i}|Y_{2,i+1}^{n}, Y_1^{i-1}) \\ &\quad - I(Y_1^{i-1}; Y_{2,i}|Y_{2,i+1}^{n}) + \epsilon_n. \qquad (122)\end{aligned}$$

Now, using [2]

$$\sum_{i=1}^{n} I(Y_{2,i+1}^{n}; Y_{1,i}|Y_1^{i-1}) = \sum_{i=1}^{n} I(Y_1^{i-1}; Y_{2,i}|Y_{2,i+1}^{n}) \qquad (123)$$

in (122), we obtain

$$\begin{aligned}nR_{e,1} &\leq \sum_{i=1}^{n} I(W_1; Y_{1,i}|Y_1^{i-1}, Y_{2,i+1}^{n}) \\ &\quad - I(W_1; Y_{2,i}|Y_{2,i+1}^{n}, Y_1^{i-1}) + \epsilon_n \qquad (124) \\ &= \sum_{i=1}^{n} I(W_1; Y_{1,i}|U_i) - I(W_1; Y_{2,i}|U_i) + \epsilon_n \qquad (125) \\ &= \sum_{i=1}^{n} I(W_1, U_i; Y_{1,i}|U_i) - I(W_1, U_i; Y_{2,i}|U_i) \\ &\quad + \epsilon_n \qquad (126) \\ &= \sum_{i=1}^{n} I(V_{1,i}; Y_{1,i}|U_i) - I(V_{1,i}; Y_{2,i}|U_i) + \epsilon_n \qquad (127)\end{aligned}$$

where (125) and (127) follow from the definitions of U_i and $V_{1,i}$ given in (95) and (96), respectively. Similarly, we can use the preceding technique for user 2's equivocation rate as well after noting that

$$nR_{e,2} \leq H(W_2|Y_1^n, X_1^n) \leq H(W_2|Y_1^n) \qquad (128)$$

which leads to

$$nR_{e,2} \leq \sum_{i=1}^{n} I(V_{2,i}; Y_{2,i}|U_i) - I(V_{2,i}; Y_{1,i}|U_i) + \epsilon_n. \qquad (129)$$

The other bounds on the equivocation rates can be derived as follows:

$$\begin{aligned}nR_{e,1} &= H(W_1|Y_2^n) \leq H(W_1, W_2|Y_2^n) \qquad (130) \\ &= H(W_1|W_2, Y_2^n) + H(W_2|Y_2^n) \qquad (131) \\ &\leq H(W_1|W_2, Y_2^n) + \epsilon_n \qquad (132) \\ &= I(W_1; Y_1^n|W_2) - I(W_1; Y_2^n|W_2) \\ &\quad + H(W_1|W_2, Y_1^n) + \epsilon_n \qquad (133) \\ &\leq I(W_1; Y_1^n|W_2) - I(W_1; Y_2^n|W_2) + \epsilon_n' \qquad (134) \\ &= \sum_{i=1}^{n} I(W_1; Y_{1,i}|W_2, Y_1^{i-1}) \\ &\quad - I(W_1; Y_{2,i}|W_2, Y_{2,i+1}^{n}) + \epsilon_n' \qquad (135) \\ &= \sum_{i=1}^{n} I(W_1, Y_{2,i+1}^{n}; Y_{1,i}|W_2, Y_1^{i-1}) \\ &\quad - I(W_1, Y_1^{i-1}; Y_{2,i}|W_2, Y_{2,i+1}^{n}) + \epsilon_n' \qquad (136) \\ &= \sum_{i=1}^{n} I(W_1; Y_{1,i}|W_2, Y_1^{i-1}, Y_{2,i+1}^{n}) \\ &\quad - I(W_1; Y_{2,i}|W_2, Y_{2,i+1}^{n}, Y_1^{i-1}) + \epsilon_n' \qquad (137) \\ &= \sum_{i=1}^{n} I(W_1; Y_{1,i}|W_2, U_i) \\ &\quad - I(W_1; Y_{2,i}|W_2, U_i) + \epsilon_n' \qquad (138) \\ &= \sum_{i=1}^{n} I(W_1, U_i; Y_{1,i}|W_2, U_i) \\ &\quad - I(W_1, U_i; Y_{2,i}|W_2, U_i) + \epsilon_n' \qquad (139) \\ &= \sum_{i=1}^{n} I(V_{1,i}; Y_{1,i}|V_{2,i}) \\ &\quad - I(V_{1,i}; Y_{2,i}|V_{2,i}) + \epsilon_n' \qquad (140)\end{aligned}$$

where (132) and (134) are due to Fano's lemma, and (136) and (137) are due to the following identities [2]:

$$\begin{aligned}&\sum_{i=1}^{n} I(Y_{2,i+1}^{n}; Y_{1,i}|W_1, W_2, Y_1^{i-1}) \\ &\quad = \sum_{i=1}^{n} I(Y_1^{i-1}; Y_{2,i}|W_1, W_2, Y_{2,i+1}^{n}) \qquad (141) \\ &\sum_{i=1}^{n} I(Y_{2,i+1}^{n}; Y_{1,i}|W_2, Y_1^{i-1}) \\ &\quad = \sum_{i=1}^{n} I(Y_1^{i-1}; Y_{2,i}|W_2, Y_{2,i+1}^{n}) \qquad (142)\end{aligned}$$

respectively. Finally, (138) and (140) follow from the definitions of U_i, $V_{1,i}$ and $V_{2,i}$ given in (95), (96) and (97), respectively. Similarly, we can use this technique to bound user 2's equivocation rate after noting that $H(W_2|Y_1^n, X_1^n) \leq H(W_2|Y_1^n)$, which leads to

$$\begin{aligned}nR_{e,2} &\leq H(W_2|Y_1^n, X_1^n) \leq H(W_2|Y_1^n) \qquad (143) \\ &\leq \sum_{i=1}^{n} I(V_{2,i}; Y_{2,i}|V_{1,i}) \\ &\quad - I(V_{2,i}; Y_{2,i}|V_{1,i}) + \epsilon_n'. \qquad (144)\end{aligned}$$

To express the outer bounds obtained above in a single-letter form, we define $U = JU_J$, $V_1 = V_{1,J}$, $V_2 = V_{2,J}$, $X = X_J$, $X_1 = X_{1,J}$, $Y_1 = Y_{1,J}$, $Y_2 = Y_{2,J}$ where J is a random variable which is uniformly distributed over $\{1, \ldots, n\}$. Using these new definitions, we can reach the single-letter expressions given in Theorem 2, hence completing the proof.

Appendix II
Proof of Theorem 3

The proof is as follows:

$$\begin{aligned}R_{e,2} &\leq H(W_2|Y_1^n, X_1^n) \qquad (145) \\ &\leq I(W_2; Y_2^n|X_1^n) - I(W_2; Y_1^n|X_1^n) \\ &\quad + H(W_2|Y_2^n, X_1^n) \qquad (146) \\ &\leq I(W_2; Y_2^n|X_1^n) - I(W_2; Y_1^n|X_1^n) + \epsilon_n \qquad (147)\end{aligned}$$

$$\begin{aligned}
&\le I(W_2; Y_2^n | X_1^n, Y_1^n) + \epsilon_n && (148)\\
&\le I(X^n, W_2; Y_2^n | X_1^n, Y_1^n) + \epsilon_n && (149)\\
&= I(X^n; Y_2^n | X_1^n, Y_1^n) + \epsilon_n && (150)\\
&= \sum_{i=1}^{n} I(X^n; Y_{2,i} | X_1^n, Y_1^n, Y_2^{i-1}) + \epsilon_n && (151)\\
&\le \sum_{i=1}^{n} H(Y_{2,i} | X_{1,i}, Y_{1,i})\\
&\quad - H(Y_{2,i} | X_1^n, Y_1^n, Y_2^{i-1}, X^n) + \epsilon_n && (152)\\
&= \sum_{i=1}^{n} H(Y_{2,i} | X_{1,i}, Y_{1,i})\\
&\quad - H(Y_{2,i} | X_{1,i}, Y_{1,i}, X_i) + \epsilon_n && (153)\\
&= \sum_{i=1}^{n} I(X_i; Y_{2,i} | X_{1,i}, Y_{1,i}) + \epsilon_n && (154)
\end{aligned}$$

where (147) is due to Fano's lemma, (150) follows from the fact that given X^n, W_2 is independent of all other random variables, (152) is due to the fact that conditioning cannot increase entropy, and (153) follows from the Markov chains

$$\begin{aligned}
(Y_{1,i}, Y_{2,i}) &\rightarrow (X_i, X_{1,i})\\
&\rightarrow (Y_1^{i-1}, Y_2^{i-1}, X^{i-1}, X_1^{i-1}) && (155)\\
Y_{2,i} &\rightarrow (X_i, X_{1,i}, Y_{1,i}) \rightarrow (Y_{1,i+1}^n, X_{i+1}^n, X_{1,i+1}^n). && (156)
\end{aligned}$$

Thus, after defining an independent random variable J, that is uniformly distributed over $\{1, \ldots, n\}$, and $X = X_J$, $X_1 = X_{1,J}$, $Y_1 = Y_{1,J}$, $Y_2 = Y_{2,J}$, we can obtain the single-letter expression in Theorem 3, completing the proof.

Appendix III
Proof of Corollary 1

In Propositions 1 and 2, if we take $a \rightarrow \infty$, then the secrecy rate in (51) can be shown to be achievable. As a notational remark, $H(\cdot)$ denotes the differential entropy in this section. We now compute an outer bound for $R_{e,2}$ using Theorem 3,

$$\begin{aligned}
R_{e,2} &\le I(X; Y_2 | X_1, Y_1) && (157)\\
&= H(Y_2 | X_1, Y_1) - H(Z_2 | Z_1) && (158)\\
&\le H(X + Z_2 | Y_1) - H(Z_2) && (159)\\
&\le H(X + Z_2 - \alpha Y_1) - \frac{1}{2}\log(2\pi e N_2) && (160)\\
&\le \frac{1}{2}\log(2\pi e) E\left[(X + Z_2 - \alpha Y_1)^2\right]\\
&\quad - \frac{1}{2}\log(2\pi e N_2) && (161)\\
&\le \frac{1}{2}\log\left((1-\alpha)^2 P + \alpha^2 N_1 + N_2\right)\\
&\quad - \frac{1}{2}\log(N_2) && (162)
\end{aligned}$$

where in (159), we used the fact that conditioning cannot increase entropy and that $H(Z_2|Z_1) = H(Z_2)$ due to the independence of Z_1 and Z_2. Equation (160) is again due to the fact that conditioning cannot increase entropy, (161) comes from the fact that Gaussian distribution maximizes entropy subject to a power constraint, and (162) is obtained by using the power constraint on X. Finally, we note that (162) is a valid outer bound for every α and if we select α as

$$\alpha = \frac{P}{P + N_1} \tag{163}$$

we get (51), completing the proof.

Appendix IV
Proof of Theorem 4

The transmitter uses the joint encoding scheme of Marton [22] and user 1 uses a CAF scheme [17]. User 2 employs list decoding to find which $\hat{Y}_1$ is sent. Let $A_\epsilon^n(V_1)$ and $A_\epsilon^n(V_2)$ denote the sets of strongly typical independent and identically distributed (i.i.d.) length-n sequences of $\mathbf{v}_1$ and $\mathbf{v}_2$, respectively. Let $A_\epsilon^n\,(V_1|\mathbf{v}_2)$ (respectively, $A_\epsilon^n\,(V_2|\mathbf{v}_1)$) denote the set of length-n sequences V_1 (respectively V_2) that are jointly typical with $\mathbf{v}_2$ (respectively, $\mathbf{v}_1$). Furthermore, let $S_\epsilon^n(\mathbf{v}_1)$ (respectively, $S_\epsilon^n(\mathbf{v}_2)$) denote the set of $\mathbf{v}_1$ (respectively, $\mathbf{v}_2$) sequences for which $A_\epsilon^n\,(V_2|\mathbf{v}_1)$ (respectively, $A_\epsilon^n\,(V_1|\mathbf{v}_2)$) are nonempty. Fix the probability distribution as

$$p(v_1, v_2)p(x|v_1, v_2)p(u, x_1)p(\hat{y}_1|u, v_1, y_1). \tag{164}$$

Codebook structure:

1) Select $2^{nR(V_i)}$ $\mathbf{v}_i$ sequences through

$$p(\mathbf{v}_i) = \begin{cases} \frac{1}{\|S_\epsilon^n(\mathbf{v}_i)\|}, & \text{if } \mathbf{v}_i \in S_\epsilon^n(\mathbf{v}_i)\\ 0, & \text{otherwise} \end{cases} \tag{165}$$

in an i.i.d. manner and index them as $\mathbf{v}_i(w_i, \tilde{w}_i, l_i)$ where $w_i \in \{1, \ldots, 2^{nR_i}\}$, $\tilde{w}_i \in \{1, \ldots, 2^{n\tilde{R}_i}\}$ and $l_i \in \{1, \ldots, 2^{nL_i}\}$ for $i = 1, 2$. R_i, $\tilde{R}_i$, L_i, and $R(V_i)$ are related through

$$R(V_i) = R_i + \tilde{R}_i + L_i, \quad i = 1, 2. \tag{166}$$

Furthermore, we set

$$L_1 + L_2 = I(V_1; V_2) + \epsilon \tag{167}$$

to ensure that for given pairs $(w_1, \tilde{w}_1)$ and $(w_2, \tilde{w}_2)$, we can find a jointly typical pair $(\mathbf{v}_1(w_1, \tilde{w}_1, l_1), \mathbf{v}_2(w_2, \tilde{w}_2, l_2))$ for some l_1, l_2.

2) For each (w_1, w_2), the transmitter randomly picks $(\tilde{w}_1, \tilde{w}_2)$ and finds a pair $(\mathbf{v}_1(w_1, \tilde{w}_1, l_1), \mathbf{v}_2(w_2, \tilde{w}_2, l_2))$ that is jointly typical. Such a pair exists with high probability due to (167). Then, given this pair of $(\mathbf{v}_1, \mathbf{v}_2)$, the transmitter generates its channel inputs through $\prod_{i=1}^n p(x_i|v_{1,i}, v_{2,i})$.

3) User 1 generates 2^{nR_0} length-n sequences $\mathbf{u}$ through $p(\mathbf{u}) = \prod_{i=1}^n p(u_i)$ and labels them as $\mathbf{u}(s_i)$ where $s_i \in \{1, \ldots, 2^{nR_0}\}$.

4) For each $\mathbf{u}(s_i)$, user 1 generates $2^{n\hat{R}}$ length-n sequences $\hat{\mathbf{y}}_1$ through $p(\hat{\mathbf{y}}_1|\mathbf{u}) = \prod_{i=1}^n\ p(\hat{y}_{1,i}|u_i)$ and indexes them as $\hat{\mathbf{y}}_1(z_i|s_i)$ where $z_i \in \{1, \ldots, 2^{n\hat{R}}\}$.

5) For each $\mathbf{u}(s_i)$, user 1 generates $2^{nR_0'}$ length-n sequences $\mathbf{x}_1$ through $p(\mathbf{x}_1|\mathbf{u}) = \prod_{i=1}^n\ p(x_{1,i}|u_i)$ and indexes them as $\mathbf{x}_1(t_i|s_i)$ where $t_i \in \{1, \ldots, 2^{nR_0'}\}$.

Partitioning:

- Partition $2^{n\hat{R}}$ into cells S_{s_i} where $s_i \in \{1,\ldots,2^{nR_0}\}$.

Encoding:

The transmitter sends $\mathbf{x}$ corresponding to the pair (w_1, w_2). User 1 (relay) sends $\mathbf{x}_1(t_i|s_i)$ if the estimate of $\mathbf{y}_1(i-1)$, i.e., $\hat{z}_{i-1}$, falls into S_{s_i} and t_i is chosen randomly from $\{1,\ldots,2^{nR_0'}\}$. The use of many $\mathbf{x}_1(t_i|s_i)$ for actual help signal $\mathbf{u}(s_i)$ aims to confuse user 2 and to decrease its decoding capability.

Decoding:

a. **Decoding at user 1:**

1) User 1 seeks a unique typical pair of $(\mathbf{y}_1(i), \mathbf{v}_1(w_{1,i}, \tilde{w}_{1,i}, l_i), \mathbf{x}_1(t_i|s_i))$ which can be achieved with vanishingly small error probability if

$$R(V_1) \leq I(V_1; Y_1|X_1). \tag{168}$$

2) User 1 decides that z_i is received if there exists a jointly typical pair $(\hat{\mathbf{y}}_1(z_i|s_i), \mathbf{y}_1(i), \mathbf{v}_1(w_{1,i}, \tilde{w}_{1,i}, l_i), \mathbf{x}_1(t_i|s_i))$ which can be guaranteed to occur if

$$\hat{R} \geq I(\hat{Y}_1; Y_1|U, X_1, V_1). \tag{169}$$

b. **Decoding at user 2**:

1) User 2 seeks a unique jointly typical pair of $(\mathbf{y}_2(i), \mathbf{u}(s_i))$ which can be found with vanishingly small error probability if

$$R_0 \leq I(U; Y_2). \tag{170}$$

2) User 2 employs list decoding to decode $\hat{\mathbf{y}}_1(z_{i-1}|s_{i-1})$. It first calculates its ambiguity set as

$$\begin{aligned}\mathcal{L}\left(\hat{\mathbf{y}}_1(z_{i-1}|\hat{s}_{i-1})\right) &= \big\{\hat{\mathbf{y}}_1(z_{i-1}|\hat{s}_{i-1}) :\\ &(\hat{\mathbf{y}}_1(z_{i-1}|\hat{s}_{i-1}), \mathbf{y}_2(i-1)) \text{ is jointly typical}\big\}\end{aligned} \tag{171}$$

and takes its intersection with $S_{\hat{s}_i}$ which results in a unique and correct intersection point if

$$\hat{R} \leq I(\hat{Y}_1; Y_2|U) + R_0 \leq I(\hat{Y}_1, U; Y_2). \tag{172}$$

Equation (169) and (172) lead to the compression constraint in (60).

3) User 2 decides that $\mathbf{v}_2(w_{2,i-1}, \tilde{w}_{2,i-1}, l_{2,i-1})$ is received if there exists a unique jointly typical pair $(\mathbf{v}_2(w_{2,i-1}, \tilde{w}_{2,i-1}, l_{2,i-1}), \mathbf{y}_2(i-1), \hat{\mathbf{y}}_1(\hat{z}_{i-1}|\hat{s}_{i-1}))$, which can be found with vanishingly small error probability if

$$R(V_2) \leq I(V_2; Y_2, \hat{Y}_1|U). \tag{173}$$

Equivocation computation:

We now show that $R_{e,1}$ and $R_{e,2}$ satisfying (55)–(58) are achievable with the coding scheme presented. To this end, we treat several possible cases separately. First, assume that

$$\begin{aligned}R_1 \geq\ & I(V_1; Y_1|X_1) - I(V_1; Y_2, \hat{Y}_1|V_2, U)\\ & - I(V_1; V_2) \qquad (174)\\ R_2 \geq\ & I(V_2; Y_2, \hat{Y}_1|U) - I(V_2; Y_1|V_1, X_1)\\ & - I(V_1; V_2). \qquad (175)\end{aligned}$$

For this case, we select the total number of codewords, i.e., $R(V_i),\ i = 1, 2$, as

$$R(V_1) = I(V_1; Y_1|X_1) \tag{176}$$

$$R(V_2) = I(V_2; Y_2, \hat{Y}_1|U). \tag{177}$$

With this selection, we have

$$\tilde{R}_1 + L_1 \leq I(V_1; Y_2, \hat{Y}_1|V_2, U) + I(V_1; V_2) \tag{178}$$

$$\tilde{R}_2 + L_2 \leq I(V_2; Y_1|V_1, X_1) + I(V_1; V_2). \tag{179}$$

We start with user 1's equivocation rate

$$\begin{aligned}H(W_1|Y_2^n) &\geq H(W_1|Y_2^n, V_2^n, U^n, \hat{Y}_1^n) &(180)\\ &= H(W_1, Y_2^n, V_2^n, \hat{Y}_1^n|U^n)\\ &\quad - H(Y_2^n, V_2^n, \hat{Y}_1^n|U^n) &(181)\\ &= H(V_1^n, W_1, Y_2^n, V_2^n, \hat{Y}_1^n|U^n)\\ &\quad - H(V_1^n|W_1, Y_2^n, V_2^n, \hat{Y}_1^n, U^n)\\ &\quad - H(Y_2^n, V_2^n, \hat{Y}_1^n|U^n) &(182)\\ &= H(V_1^n|U^n)\\ &\quad + H(W_1, Y_2^n, V_2^n, \hat{Y}_1^n|U^n, V_1^n)\\ &\quad - H(V_1^n|W_1, Y_2^n, V_2^n, \hat{Y}_1^n, U^n)\\ &\quad - H(Y_2^n, V_2^n, \hat{Y}_1^n|U^n) &(183)\\ &\geq H(V_1^n|U^n)\\ &\quad - I(V_1^n; Y_2^n, V_2^n, \hat{Y}_1^n|U^n)\\ &\quad - H(V_1^n|W_1, Y_2^n, V_2^n, \hat{Y}_1^n, U^n) &(184)\end{aligned}$$

where each term will be treated separately. First term is

$$H(V_1^n|U^n) = H(V_1^n) = nR(V_1) = nI(V_1; Y_1|X_1) \tag{185}$$

where the first equality is due to the independence of U^n and V_1^n. The second equality follows from the fact that V_1^n can take $2^{nR(V_1)}$ values with equal probability. The third equality comes from our selection in (176). The second term of (184) can be bounded as

$$I(V_1^n; Y_2^n, V_2^n, \hat{Y}_1^n|U^n) \leq nI(V_1; Y_2, V_2, \hat{Y}_1|U) + n\epsilon_n \tag{186}$$

using the approach devised in Lemma 3 of [9]. To bound the last term in (184), we assume that user 2 is trying to decode V_1^n given the side information $W_1 = w_1$. Since V_1^n can take less than $2^{n(I(V_1;Y_2,\hat{Y}_1|U,V_2)+I(V_1;V_2))}$ values (see (178)) given $W_1 = w_1$, user 2 can decode V_1^n with vanishingly small error probability as long as $W_1 = w_1$ is given. Consequently, the use of Fano's lemma yields

$$H(V_1^n|W_1, Y_2^n, V_2^n, \hat{Y}_1^n, U^n) \leq \epsilon_n. \tag{187}$$

Plugging (185), (186) and (187) into (184), we get

$$\begin{aligned}H(W_1|Y_2^n) \geq\ & nI(V_1; Y_1|X_1) - nI(V_1; Y_2, \hat{Y}_1, V_2|U)\\ & - n\epsilon_n \qquad (188)\end{aligned}$$

$$= nI(V_1;Y_1|X_1) - nI(V_1;Y_2,\hat{Y}_1|V_2,U) - nI(V_1;V_2) - n\epsilon_n \quad (189)$$

where (189) follows from the independence of (V_1,V_2) and U, i.e., $I(V_1;V_2|U)=I(V_1;V_2)$. Similarly, we can bound equivocation of user 2 as follows:

$$\begin{aligned} H(W_2|Y_1^n,X_1^n) &\geq H(W_2|Y_1^n,X_1^n,V_1^n) && (190)\\ &= H(W_2,Y_1^n,V_1^n|X_1^n) \\ &\quad - H(Y_1^n,V_1^n|X_1^n) && (191)\\ &= H(W_2,V_2^n,Y_1^n,V_1^n|X_1^n) \\ &\quad - H(V_2^n|W_2,Y_1^n,V_1^n,X_1^n) \\ &\quad - H(Y_1^n,V_1^n|X_1^n) && (192)\\ &= H(V_2^n|X_1^n) \\ &\quad + H(W_2,Y_1^n,V_1^n|X_1^n,V_2^n) \\ &\quad - H(V_2^n|W_2,Y_1^n,V_1^n,X_1^n) \\ &\quad - H(Y_1^n,V_1^n|X_1^n) && (193)\\ &\geq H(V_2^n|X_1^n) - I(V_2^n;Y_1^n,V_1^n|X_1^n) \\ &\quad - H(V_2^n|W_2,Y_1^n,V_1^n,X_1^n) && (194) \end{aligned}$$

where the first term is

$$\begin{aligned} H(V_2^n|X_1^n) &= H(V_2^n) = nR(V_2) \\ &= nI(V_2;Y_2,\hat{Y}_1|U) && (195) \end{aligned}$$

where the first equality is due to the independence of V_2^n and X_1^n, the second equality comes from the fact that V_2^n can take $2^{nR(V_2)}$ values with equal probability and the last equality is a consequence of our choice in (177). The second term of (194) can be bounded as

$$I(V_2^n;Y_1^n,V_1^n|X_1^n) \leq nI(V_2;Y_1,V_1|X_1) + n\epsilon_n \quad (196)$$

following the approach of Lemma 3 of [9]. To bound the last term of (194), we assume that user 1 is trying to decode V_2^n given the side information $W_2=w_2$. Since V_2^n can take at most $2^{n(I(V_2;Y_1|V_1,X_1)+I(V_2;V_1))}$ values (see (179)) given $W_2=w_2$, user 1 can decode V_2^n with vanishingly small error probability as long as this side information is available. Consequently, the use of Fano's lemma yields

$$H(V_2^n|W_2,Y_1^n,V_1^n,X_1^n) \leq \epsilon_n. \quad (197)$$

Plugging (195), (196) and (197) into (194), we get

$$\begin{aligned} H(W_2|Y_1^n,X_1^n) &\geq nI(V_2;Y_2,\hat{Y}_1|U) \\ &\quad - nI(V_2;Y_1,V_1|X_1) - n\epsilon_n && (198)\\ &= nI(V_2;Y_2,\hat{Y}_1|U) \\ &\quad - nI(V_2;Y_1|V_1,X_1) \\ &\quad - nI(V_1;V_2) - n\epsilon_n && (199) \end{aligned}$$

where (199) follows from the independence of (V_1,V_2) and X_1, i.e., $I(V_1;V_2|X_1)=I(V_1;V_2)$.

We have completed the equivocation calculation for the case described by (174)–(175). The proofs of other cases involve no different arguments besides decreasing the total number codewords in (176)–(177). For example, if

$$R_1 \leq I(V_1;Y_1|X_1) - I(V_1;Y_2,\hat{Y}_1|V_2,U) - I(V_1;V_2) \quad (200)$$

then we select the total number of codewords for user 1 as

$$R(V_1) = R_1 + I(V_1;Y_2,\hat{Y}_1|V_2,U) + I(V_1;V_2) \quad (201)$$

which is equivalent to saying that

$$\tilde{R}_1 + L_1 = I(V_1;Y_2,\hat{Y}_1|V_2,U) + I(V_1;V_2). \quad (202)$$

In this case, following the steps from (180) to (184), we can bound the equivocation of user 1 as follows,

$$\begin{aligned} H(W_1|Y_2^n) \geq{}& H(V_1^n|U^n) - I(V_1^n;Y_2^n,V_2^n,\hat{Y}_1^n|U^n) \\ & - H(V_1^n|W_1,Y_2^n,V_2^n,\hat{Y}_1^n,U^n) && (203) \end{aligned}$$

where the first term is now

$$\begin{aligned} H(V_1^n|U^n) &= H(V_1^n) && (204)\\ &= nR(V_1) && (205)\\ &= n(R_1 + I(V_1;Y_2,\hat{Y}_1|V_2,U) \\ &\quad + I(V_1;V_2)) && (206) \end{aligned}$$

where the first equality is due to the independence of V_1^n and U^n, the second equality is due to the fact that V_1^n can take at most $2^{nR(V_1)}$ values with equal probability and the last equality is a consequence of our choice in (201). An upper bound on the second term was already obtained in (186). The third term can also be shown to decay to zero as n goes to infinity considering the case that user 2 is decoding V_1^n using side information $W_1=w_1$. Since V_1^n can take $2^{n(I(V_1;Y_2,\hat{Y}_1|V_2,U)+I(V_1;V_2))}$ values given $W_1=w_1$, user 2 can decode V_2^n with vanishingly small error probability as long as this side information is available. Therefore, the use of Fano's lemma implies

$$H(V_1^n|W_1,Y_2^n,V_2^n,\hat{Y}_1^n,U^n) \leq \epsilon_n. \quad (207)$$

Plugging (186), (206), (207) into (203), we get

$$\begin{aligned} H(W_1|Y_2^n) &\geq n(R_1 + I(V_1;Y_2,\hat{Y}_1|V_2,U) \\ &\quad + I(V_1;V_2)) \\ &\quad - I(V_1;Y_2,V_2,\hat{Y}_1|U) - n\epsilon_n && (208)\\ &= nR_1 - n\epsilon_n && (209) \end{aligned}$$

where we used the fact that U and (V_1,V_2) are independent, i.e., $I(V_1;V_2|U)=I(V_1;V_2)$. The other cases leading to different equivocation rates can be proved similarly, hence omitted.

Appendix V
Proof of Theorem 5

Fix the probability distribution as

$$p(v_1,v_2)p(x|v_1,v_2)p(u_1,x_1) \\ \times p(\hat{y}_1|u_1,y_1)p(u_2,x_2)p(\hat{y}_2|u_2,y_2). \quad (210)$$

Codebook structure:

1) Select $2^{nR(V_i)}$ $\mathbf{v}_i$ sequences through

$$p(\mathbf{v}_i) = \begin{cases} \frac{1}{\|S_\epsilon^n(\mathbf{v}_i)\|}, & \text{if } \mathbf{v}_i \in S_\epsilon^n(\mathbf{v}_i) \\ 0, & \text{otherwise} \end{cases} \quad (211)$$

in an i.i.d. manner and index them as $\mathbf{v}_i(w_i,\tilde{w}_i,l_i)$ where $w_i \in \{1,\ldots,2^{nR_i}\}$, $\tilde{w}_i \in \{1,\ldots,2^{n\tilde{R}_i}\}$ and $l_i \in \{1,\ldots,2^{nL_i}\}$ for $i=1,2$. $R_i, \tilde{R}_i, L_i$ and $R(V_i)$ are related through

$$R(V_i) = R_i + \tilde{R}_i + L_i, \quad i=1,2. \quad (212)$$

Furthermore, we set

$$L_1 + L_2 = I(V_1;V_2) + \epsilon \quad (213)$$

to ensure that for given pairs $(w_1,\tilde{w}_1)$ and $(w_2,\tilde{w}_2)$, we can find a jointly typical pair $(\mathbf{v}_1(w_1,\tilde{w}_1,l_1),\mathbf{v}_2(w_2,\tilde{w}_2,l_2))$ for some l_1, l_2.

2) For each (w_1,w_2), the transmitter randomly picks $(\tilde{w}_1,\tilde{w}_2)$ and finds a pair $(\mathbf{v}_1(w_1,\tilde{w}_1,l_1),\mathbf{v}_2(w_2,\tilde{w}_2,l_2))$ that is jointly typical. Such a pair exists with high probability due to (213). Then, given this pair of $(\mathbf{v}_1,\mathbf{v}_2)$, the transmitter generates its channel inputs through $\prod_{i=1}^n p(x_i|v_{1,i},v_{2,i})$.

3) User j generates $2^{nR_{0,j}}$ length-n sequences $\mathbf{u}_j$ through $p(\mathbf{u}_j) = \prod_{i=1}^n p(u_{j,i})$ and labels them as $\mathbf{u}_j(s_{j,i})$ where $s_{j,i} \in \{1,\ldots,2^{nR_{0,j}}\}$ where $j=1,2$.

4) For each $\mathbf{u}_j(s_{j,i})$, user j generates $2^{n\hat{R}_j}$ length-n sequences $\hat{\mathbf{y}}_j$ through $p(\hat{\mathbf{y}}_j|\mathbf{u}_j) = \prod_{i=1}^n p(\hat{y}_{j,i}|u_{j,i})$ and indexes them as $\hat{\mathbf{y}}_j(z_{j,i}|s_{j,i})$ where $z_{j,i} \in \{1,\ldots,2^{n\hat{R}_j}\}$, $j=1,2$.

5) For each $\mathbf{u}_j(s_{j,i})$, user j generates $2^{nR'_{0,j}}$ length-n sequences $\mathbf{x}_j$ through $p(\mathbf{x}_j|\mathbf{u}_j) = \prod_{i=1}^n p(x_{j,i}|u_{j,i})$ and indexes them as $\mathbf{x}_j(t_{j,i}|s_{j,i})$ where $t_{j,i} \in \{1,\ldots,2^{nR'_{0,j}}\}$, $j=1,2$.

Partitioning:

- Partition $2^{n\hat{R}_j}$ into cells $S_{s_{j,i}}$ where $s_{j,i} \in \{1,\ldots,2^{nR_{0,j}}\}$, $j=1,2$.

Encoding:

The transmitter sends $\mathbf{x}$ corresponding to the pair (w_1,w_2). User j sends $\mathbf{x}_j(t_{j,i}|s_{j,i})$ if the estimate of $\mathbf{y}_j(i-1)$, i.e., $\hat{z}_{j,i-1}$, falls into $S_{s_{j,i}}$ and $t_{j,i}$ is chosen randomly from $\{1,\ldots,^{nR'_{0,j}}\}$. The use of many $\mathbf{x}_j(t_{j,i}|s_{j,i})$ for actual help signal $\mathbf{u}_j(s_{j,i})$ aims to confuse the other user and to decrease its decoding capability.

Decoding:

We only consider decoding at user 1. Final expressions regarding user 2 will follow due to symmetry.

1) User 1 seeks a unique jointly typical pair of $(\mathbf{y}_1(i),\mathbf{u}_2(s_{2,i}))$ which can be found with vanishingly small error probability if

$$R_{0,2} \le I(U_2;Y_1|X_1) \quad (214)$$

2) User 1 decides on $\hat{\mathbf{y}}_1(z_{1,i}|s_{1,i})$ by looking for a jointly typical pair $(\hat{\mathbf{y}}_1(z_{1,i}|s_{1,i}),\mathbf{y}_1(i),\mathbf{u}_2(s_{2,i}),\mathbf{x}_1(t_{1,i}|s_{1,i}))$ which can be ensured to exist if

$$\hat{R}_1 \ge I(\hat{Y}_1;Y_1|U_1,U_2,X_1) \quad (215)$$

3) User 1 employs list decoding to decode $\hat{\mathbf{y}}_2(z_{2,i-1}|s_{2,i-1})$. It first calculates its ambiguity set as

$$\mathcal{L}\left(\hat{\mathbf{y}}_2(z_{2,i-1}|\hat{s}_{2,i-1})\right) = \big\{\hat{\mathbf{y}}_2(z_{2,i-1}|\hat{s}_{2,i-1}): \\ (\hat{\mathbf{y}}_2(z_{2,i-1}|\hat{s}_{2,i-1}),\mathbf{y}_1(i-1)) \text{ is jointly typical}\big\} \quad (216)$$

and then takes its intersection with $S_{\hat{s}_{2,i}}$ which results in a unique and correct intersection point if

$$\hat{R}_2 \le I(\hat{Y}_2;Y_1|U_2,X_1) + R_{0,2} \le I(\hat{Y}_2,U_2;Y_1|X_1) \quad (217)$$

4) User 1 decides that $\mathbf{v}_1(w_{1,i-1},\tilde{w}_{1,i-1},l_{1,i-1})$ is received if there exists a unique jointly typical pair $(\mathbf{v}_1(w_{1,i-1},\tilde{w}_{1,i-1},l_{1,i-1}),\mathbf{y}_1(i-1),\hat{\mathbf{y}}_2(\hat{z}_{2,i-1}|\hat{s}_{2,i-1}))$ which can be found with vanishingly small error probability if

$$R(V_1) \le I(V_1;Y_1,\hat{Y}_2|X_1,U_2) \quad (218)$$

Equivocation computation:

Similar to the previous proofs, we treat each case separately. Due to symmetry, we only consider user 1. If the rate of user 1 is such that

$$R_1 \ge I(V_1;Y_1,\hat{Y}_2|X_1,U_2) - I(V_1;Y_2,\hat{Y}_1|X_2,V_2,U_1) \\ - I(V_1;V_2) \quad (219)$$

then we select the total number of codewords as

$$R(V_1) = I(V_1;Y_1,\hat{Y}_2|X_1,U_2) \quad (220)$$

which implies that

$$\tilde{R}_1 + L_1 \le I(V_1;Y_2,\hat{Y}_1|X_2,V_2,U_1) + I(V_1;V_2). \quad (221)$$

The equivocation rate can be bounded as follows:

$$\begin{aligned} &H(W_1|Y_2^n,X_2^n) \\ &\quad \ge H(W_1|Y_2^n,X_2^n,\hat{Y}_1^n,V_2^n,U_1^n) && (222)\\ &\quad = H(W_1,Y_2^n,\hat{Y}_1^n,V_2^n|X_2^n,U_1^n) \\ &\qquad - H(Y_2^n,\hat{Y}_1^n,V_2^n|X_2^n,U_1^n) && (223)\\ &\quad = H(W_1,V_1^n,Y_2^n,\hat{Y}_1^n,V_2^n|X_2^n,U_1^n) \\ &\qquad - H(V_1^n|W_1,Y_2^n,\hat{Y}_1^n,V_2^n,X_2^n,U_1^n) \\ &\qquad - H(Y_2^n,\hat{Y}_1^n,V_2^n|X_2^n,U_1^n) && (224)\\ &\quad = H(V_1^n|X_2^n,U_1^n) \\ &\qquad + H(W_1,Y_2^n,\hat{Y}_1^n,V_2^n|X_2^n,U_1^n,V_1^n) \\ &\qquad - H(V_1^n|W_1,Y_2^n,\hat{Y}_1^n,V_2^n,X_2^n,U_1^n) \\ &\qquad - H(Y_2^n,\hat{Y}_1^n,V_2^n|X_2^n,U_1^n) && (225)\\ &\quad \ge H(V_1^n|X_2^n,U_1^n) - I(V_1^n;Y_2^n,\hat{Y}_1^n,V_2^n|X_2^n,U_1^n) \\ &\qquad - H(V_1^n|W_1,Y_2^n,\hat{Y}_1^n,V_2^n,X_2^n,U_1^n). && (226) \end{aligned}$$

We treat each term in (226) separately. The first term is

$$\begin{aligned} H(V_1^n|X_2^n, U_1^n) &= H(V_1^n) && (227)\\ &= nR(V_1) && (228)\\ &= nI(V_1; Y_1, \hat{Y}_2|X_1, U_2) && (229) \end{aligned}$$

where the first equality is due to the independence of V_1^n and (X_2^n, U_1^n), the second equality follows from the fact that V_1^n can take $2^{nR(V_1)}$ values with equal probability and the last equality is due to our choice in (220). The second term of (226) can be bounded as

$$\begin{aligned} I(V_1^n; Y_2^n, \hat{Y}_1^n, V_2^n|X_2^n, U_1^n)& \\ \leq nI(V_1; Y_2, \hat{Y}_1, V_2|X_2, U_1) + n\epsilon_n& \quad (230) \end{aligned}$$

following Lemma 3 of [9]. To bound the last term of (226), we consider the case that user 2 is trying to decode V_1^n given the side information $W_1 = w_1$. Since V_1^n can take $2^{n(I(V_1;Y_2,\hat{Y}_1|X_2,V_2,U_1)+I(V_1;V_2))}$ values at most, user 2 can decode V_1^n with vanishingly small error probability as long as this side information is available. Hence, the use of Fano's lemma yields

$$H(V_1^n|W_1, Y_2^n, \hat{Y}_1^n, V_2^n, X_2^n, U_1^n) \leq \epsilon_n. \quad (231)$$

Plugging (229), (230), (231) into (226), we get

$$\begin{aligned} H(W_1|Y_2^n, X_2^n) &\geq nI(V_1; Y_1, \hat{Y}_2|X_1, U_2)\\ &\quad - nI(V_1; Y_2, \hat{Y}_1, V_2|X_2, U_1)\\ &\quad - n\epsilon_n && (232)\\ &= nI(V_1; Y_1, \hat{Y}_2|X_1, U_2)\\ &\quad - nI(V_1; Y_2, \hat{Y}_1|X_2, V_2, U_1)\\ &\quad - nI(V_1; V_2) - n\epsilon_n && (233) \end{aligned}$$

where (233) follows from the independence of (X_2, U_1) and (V_1, V_2), i.e., $I(V_1; V_2|X_2, U_1) = I(V_1; V_2)$.

For the other case, i.e., if the rate of user 1 is such that

$$\begin{aligned} R_1 \leq & I(V_1; Y_1, \hat{Y}_2|X_1, U_2)\\ & - I(V_1; Y_2, \hat{Y}_1|X_2, V_2, U_1) - I(V_1; V_2) \quad (234) \end{aligned}$$

we select the total number of codewords as

$$R(V_1) = R_1 + I(V_1; Y_2, \hat{Y}_1|X_2, V_2, U_1) + I(V_1; V_2) \quad (235)$$

and following the same lines of computation, we can show that

$$H(W_1|Y_2^n, X_2^n) \geq nR_1 - n\epsilon_n \quad (236)$$

completing the proof.

References

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

[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[3] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[4] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Multiple access channels with generalized feedback and confidential messages," in *Proc. IEEE Inf. Theory Workshop on Frontiers in Coding Theory*, Sep. 2007.

[5] Y. Liang and H. V. Poor, "Multiple access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[6] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006.

[7] E. Ekrem and S. Ulukus, "Effects of cooperation on the secrecy of multiple access channels with generalized feedback," in *Proc. Conf. Inf. Sci. Syst.*, Mar. 2008.

[8] R. Liu and H. V. Poor, "Secrecy capacity region of a multi-antenna Gaussian broadcast channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1235–1249, Mar. 2009.

[9] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[10] Y. Oohama, Relay Channels With Confidential Messages [Online]. Available: http://arxiv.org/abs/cs/0611125

[11] X. He and A. Yener, "On the equivocation region of relay channels with orthogonal components," in *Proc. 41th Asilomar Conf. Signals, Syst., Comp.*, Nov. 2007.

[12] X. He and A. Yener, "The role of an untrusted relay in secret communication," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2008.

[13] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[14] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[15] M. Yuksel and E. Erkip, "The relay channel with a wire-tapper," in *Proc. Conf. Inf. Sci. Syst.*, Mar. 2007.

[16] M. Bloch and A. Thangaraj, "Confidential messages to a cooperative relay," in *Proc. IEEE Inf. Theory Workshop*, May 2008.

[17] T. M. Cover and A. El Gamal, "Capacity theorems for the relay channel," *IEEE Trans. Inf. Theory*, vol. IT-25, no. 5, pp. 572–584, Sep. 1979.

[18] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity-Part I: System description," *IEEE Trans. Commun.*, vol. 51, pp. 1927–1938, Nov. 2003.

[19] Y. Liang and G. Kramer, "Rate regions for relay broadcast channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 10, pp. 3517–3535, Oct. 2007.

[20] R. Dabora and S. Servetto, "Broadcast channels with cooperating decoders," *IEEE Trans. Inf. Theory*, vol. 52, no. 12, pp. 5438–5454, Dec. 2006.

[21] Y. Liang and V. V. Veeravalli, "Cooperative relay broadcast channels," *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 900–928, Mar. 2007.

[22] K. Marton, "A coding theorem for the discrete memoryless channels," *IEEE Trans. Inf. Theory*, vol. 25, no. 1, pp. 306–311, May 1979.

[23] R. Tanniuos and A. Nosratinia, "Relay channels with private messages," *IEEE Trans. Inf. Theory*, vol. 53, no. 10, pp. 3777–3785, Oct. 2007.

[24] M. H. M. Costa, "Writing on dirty paper," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 3, pp. 439–441, May 1983.

[25] S. I. Gelfand and M. S. Pinsker, "Coding for channel with random parametres," *Probl. Contr. Inf. Theory*, vol. 9, no. 1, pp. 19–31, 1980.

[26] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2008.

[27] H. Sato, "An outer bound to the capacity region of broadcast channels," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 374–377, May 1978.

[28] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.

[29] A. Khisti and G. Wornell, "Secure transmission with multiple antennas-I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[30] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, Oct. 2007.

[31] T. Liu and S. Shamai, “A note on the secrecy capacity of the multi-antenna wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[32] E. Tekin and A. Yener, “The Gaussian multiple access wire-tap channel,” *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[33] S. K. Leung-Yan-Cheong and M. E. Hellman, “The Gaussian wire-tap channel,” *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

Ersen Ekrem (S’07) received the B.S. and M.S. degrees in electrical and electronics engineering from Bogaziçi University, Istanbul, Turkey, in 2006 and 2007, respectively. Currently, he is working toward the Ph.D. degree in the Department of Electrical and Computer Engineering at the University of Maryland, College Park.

His research interests include information theory and wireless communications.

Sennur Ulukus (M’00) received the B.S. and M.S. degrees in electrical and electronics engineering from Bilkent University, Ankara, Turkey, in 1991 and 1993, respectively, and the Ph.D. degree in electrical and computer engineering from Rutgers University, NJ, in 1998. During her Ph.D. studies, she was with the Wireless Information Network Laboratory (WINLAB), Rutgers University.

From 1998 to 2001, she was a Senior Technical Staff Member at AT&T Labs-Research in New Jersey. In 2001, she joined the University of Maryland at College Park, where she is currently an Associate Professor in the Department of Electrical and Computer Engineering, with a joint appointment at the Institute for Systems Research (ISR). Her research interests are in wireless communication theory and networking, network information theory for wireless networks, signal processing for wireless communications and security for multi-user wireless communications.

Dr. Ulukus is a recipient of the 2005 NSF CAREER Award, and a corecipient of the 2003 IEEE Marconi Prize Paper Award in Wireless Communications. She serves/served as an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION THEORY since 2007, as an Associate Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS between 2003–2007, as a Guest Editor for the IEEE TRANSACTIONS ON INFORMATION THEORY for the special issue on interference networks, as a Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS for the special issue on multiuser detection for advanced communication systems and networks, as the Co-Chair of the Communication Theory Symposium at the 2007 IEEE Global Telecommunications Conference, as the Co-Chair of the Medium Access Control (MAC) Track at the 2008 IEEE Wireless Communications and Networking Conference, as the Co-Chair of the Wireless Communications Symposium at the 2010 IEEE International Conference on Communications, as the Co-Chair of the 2011 Communication Theory Workshop, and as the Secretary of the IEEE Communication Theory Technical Committee (CTTC) in 2007–2009.