Improved Rate-Equivocation Regions for Secure Cooperative Communication

Ninoslav Marina, *Member, IEEE,* Hideki Yagi, *Member, IEEE,*
and H. Vincent Poor, *Fellow, IEEE*

Abstract

A simple four node network in which cooperation improves the information-theoretic secrecy is studied. The channel consists of two senders, a receiver, and an eavesdropper. One or both senders transmit confidential messages to the receiver, while the eavesdropper tries to decode the transmitted message. The main result is the derivation of a newly achievable rate-equivocation region that is shown to be larger than a rate-equivocation region derived by Lai and El Gamal for the relay-eavesdropper channel. When the rate of the helping interferer is zero, the new rate-equivocation region reduces to the capacity-equivocation region over the wire-tap channel, hence, the new achievability scheme can be seen as a generalization of a coding scheme proposed by Csiszár and Körner. This result can naturally be combined with a rate-equivocation region given by Tang et al. (for the interference assisted secret communication), yielding an even larger achievable rate-equivocation region.

Index Terms

Information-theoretic secrecy, wire-tap channel, eavesdropper channel, rate-equivocation region, secrecy capacity, perfect secrecy, physical layer security, cooperative communication.

I. Introduction

IN this work we propose a scheme that increases the information theoretic secrecy in a simple cooperative communication network. The channel model includes a class of the wire-tap channels with a helping interferer introduced by Lai and El Gamal [1]. These authors considered several cooperation schemes over the relay-eavesdropper channel, in which the relay node helps to enhance the security level of communication between the sender and the receiver. The paper gives an interesting observation indicating that over the multiple access channel (MAC) with an eavesdropper, secret communication can be enhanced with a help of one of the two senders (called, the *helping interferer* or the *helper*). In addition, an achievable equivocation-rate region has been derived for this scheme. Subsequently, Tang et al. [2] have derived an improved rate-equivocation region using the fact that the receiver does not have to decode the sequence transmitted by a helper. One possibility is that the helper sends interference (dummy messages) in order to weaken the channel to the eavesdropper. When the rate of dummy messages of the helper is zero (there is no cooperation from the helper), the channel reduces to the (single-user) *wire-tap channel* introduced by Wyner [3], and generalized later by Csiszár and Körner [4]. In this reduced setting, however, the achievable rate-equivocation regions given by [1] and [2] do not coincide with the capacity-equivocation region over the wire-tap channel, giving only its sub-region. When only perfect-secrecy is imposed (i.e., the eavesdropper is totally ignorant of the transmitted message), their results coincide with the secrecy-capacity of the wire-tap channel.

Motivated by this fact, the first part of this paper gives a new achievable rate-equivocation region (i.e, an inner bound on the capacity-equivocation region) for the wire-tap channel with a helping interferer, showing that the new region is improved over the one given in [1]. When the rate of the helping interferer

N. Marina is with Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (email: nmarina@princeton.edu).

H. Yagi is with Center for Frontier Science and Engineering, The University of Electro-Communications, Chofu-shi, Tokyo 182-8585, Japan (email: yagi@ice.uec.ac.jp).

H. V. Poor is with Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (email: poor@princeton.edu).

is zero, the new rate-equivocation region reduces to the capacity-equivocation region over the wire-tap channel, so the new achievability scheme can be seen as a generalization of the coding scheme given in [4]. Our result can naturally be combined with the additional rate-equivocation region given by [2], yielding an even larger rate-equivocation region.

In the next section we present the previous results on the wire-tap channel with a helper. The main result of this work, that is the improved rate-equivocation region for the wire-tap channel with helping interferer, is presented in Section III, while in Section IV we derive an even larger rate-equivocation region. A note on the broadcast channel with confidential messages and the wire-tap channel with helping interferer is given in Section V. Section VI concludes the paper.

II. PRELIMINARIES

A. The Wire-Tap Channel with a Helping Interferer

The cooperative channel considered in this paper is shown in Fig. 1 and consists of two senders, a receiver, and an eavesdropper, in which one sender transmits confidential messages to the receiver, and the eavesdropper tries to decode the transmitted message. The second sender plays the role of a "helper" to enhance the secrecy of communication. This model is referred to as the wire-tap channel with a (helping) interferer, and will be considered first. Let $\mathcal{X}_t$ be the channel input alphabet of sender t,
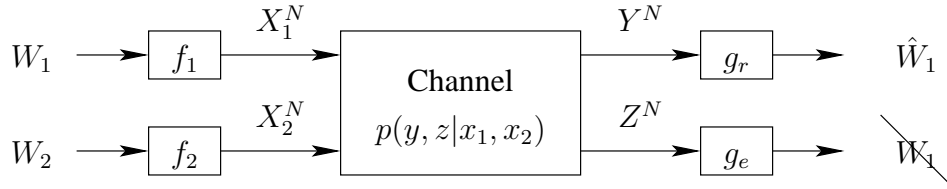

Fig. 1. A four node network of one sender, one receiver, one eavesdropper and one helper.

$t = 1, 2$, and let and $\mathcal{Y}$ and $\mathcal{Z}$ be the output alphabet of the receiver and the eavesdropper, respectively. We assume that all the alphabets are discrete and finite and the channel is memoryless, characterized by a conditional probability mass function (PMF) $P(y, z|x_1 x_2)$ for $(x_1, x_2) \in \mathcal{X}_1 \times \mathcal{X}_2$ and $(y, z) \in \mathcal{Y} \times \mathcal{Z}$, i.e., $\boldsymbol{x}_t \triangleq (x_{t1}, \ldots, x_{tN}) \in \mathcal{X}_t^N$, $\boldsymbol{y} \triangleq (y_1, \ldots, y_N) \in \mathcal{Y}^N$ and $\boldsymbol{z} \triangleq (z_1, \ldots, y_N) \in \mathcal{Y}^N$. Then, we have

$$P_N(\boldsymbol{y}, \boldsymbol{z}|\boldsymbol{x}_1, \boldsymbol{x}_2) = \prod_{n=1}^{N} P(y_n, z_n|x_{1n}, x_{2n})$$

where N denotes the number of channel uses. We assume that both of the receiver and the eavesdropper know $P(y, z|x_1, x_2)$.

Define $\mathcal{W}_t$ with $t = 1, 2$ as the set of integers $\{1, \ldots, M_t\}$ with $M_t \geq 1$. Let $w_1 \in \mathcal{W}_1$ be a uniformly distributed confidential message of sender 1. We also denote a random message of sender 2 by $w_2 \in \mathcal{W}_2$. Encoder t is a deterministic mapping denoted by

$$f_t : \mathcal{W}_t \to \mathcal{X}_t^N. \tag{1}$$

The receiver and the eavesdropper estimate the transmitted message from the received sequence $\boldsymbol{y}$ and $\boldsymbol{z}$, with the decoding functions

$$g_r : \mathcal{Y}^N \to \mathcal{W}_1, \quad \text{and} \quad g_e : \mathcal{Z}^N \to \mathcal{W}_1,$$

respectively. Let R_t, $t = 1, 2$, be an information rate defined as

$$R_t = \log_2 M_t / N.$$

An $(N, M_1, M_2, \{f_t, g_t\}_{t=1,2})$ code for the MAC with a helper consists of message sets $\mathcal{V}_1 \times \mathcal{V}_2$, encoding functions f_t, and decoding functions g_t with $t = 1, 2$. Provided that the transmitted message is $w_1 \in \mathcal{W}_1$,

the decoder makes an *error* if $g_r(\boldsymbol{y}) \neq w_1$. The average probability of decoding error, denoted by $P_{\mathrm{e}}^{(N)}$, is

$$P_{\mathrm{e}}^{(N)} = \frac{1}{M_1} \sum_{w_1 \in \mathcal{W}_1} \Pr(g_r(\boldsymbol{y}) \neq w_1 | \ w_1 \text{ sent}).$$

The *equivocation* rate at the eavesdropper is defined as

$$R_{\mathrm{e}}^{(N)} = \frac{1}{N} H(W_1 | Z^N).$$

The secrecy considered in this paper is defined as follows:

Definition 1: A *rate-equivocation pair* (R_1, R_{e}) is said to be *achievable* if there exists a sequence of (N, M_1) codes such that for every $\epsilon > 0$,

$$R_1 \geq \frac{\log_2 M_1}{N} - \epsilon, \quad P_{\mathrm{e}}^{(N)} \leq \epsilon, \quad \text{and} \quad R_{\mathrm{e}}^{(N)} \geq R_{\mathrm{e}} - \epsilon,$$

for all sufficiently large N.

Definition 2: A *perfect-secrecy rate* R_1 is said to be *achievable* if the rate-equivocation pair (R_1, R_1) is achievable. The *secrecy-capacity* of the wire-tap channel with a helper is defined as the maximum of all achievable perfect-secrecy rates.

Note that without sender 2, this channel model reduces the (single-user) wire-tap channel [3], [4]. Achievable rate-equivocation pairs, achievable perfect-secrecy rates, and the secrecy capacity for the wire-tap channel are defined analogously.

B. Known Achievable Rate-Equivocation Regions

For the (single-user) wire-tap channel [3], [4], the following rate-equivocation region is the capacity-equivocation region

$$\bigcup_{P_{QU}P_{X_1|U}P_{YZ|X}} \Big\{ (R_1, R_{\mathrm{e}}): \quad 0 \leq R_{\mathrm{e}} \leq R_1,$$

$$R_1 \leq I(U; Y),$$
$$R_{\mathrm{e}} \leq I(U; Y|Q) - I(U; Z|Q) \Big\}, \tag{2}$$

where Q and U are auxiliary random variables satisfying the Markov chain condition

$$Q \to U \to X_1$$

and the cardinality bounds

$$|\mathcal{Q}| \leq |\mathcal{X}_1| + 3 \quad \text{and} \quad |\mathcal{U}| \leq |\mathcal{X}_1|^2 + 4|\mathcal{X}_1| + 3.$$

Since we assume that all rates in this paper are always non-negative, if an upper-bound on R_{e} happens to be negative, it means $R_{\mathrm{e}} = 0$. This rule will be applied throughout the paper when necessary.

For the wire-tap channel with a helper, it was shown in [1, Theorem 3] that the following rate-equivocation region is achievable:

$$\mathrm{co} \bigcup_{P_{U_1}P_{U_2}P_{X_1|U_1}P_{X_2|U_2}P_{YZ|X_1X_2}} \Big\{ (R_1, R_{\mathrm{e}}): R_1 \ \leq \ I(U_1; Y|U_2),$$

$$0 \ \leq \ R_{\mathrm{e}} \leq R_1,$$
$$R_{\mathrm{e}} \ \leq \ I(U_1; Y|U_2) - \min\{I(U_2; Y), I(U_2; Z)\}$$
$$- \ I(U_1; Z|U_2) + \min\{I(U_2; Y), I(U_2; Z|U_1)\} \Big\}, \tag{3}$$

where $\text{co}(\mathcal{S})$ denotes the convex hull of the set $\mathcal{S}$, U_1 and U_2 are auxiliary random variables satisfying the Markov chain condition

$$(U_1, U_2) \to (X_1, X_2) \to (Y, Z).$$

We note that if $I(U_2; Y) \leq I(U_2; Z)$, then the last inequality on R_e becomes

$$0 \leq R_\mathrm{e} \leq I(U_1; Y|U_2) - I(U_1; Z|U_2),$$

implying that the wire-tap channel with a helper becomes the ordinary wire-tap channel, i.e., there is no effect from the user cooperation. In this case, the region given by (2) reduces to a sub-region of the region given by (2). Note that the result of Tang et al. [2] implies that we might still have an advantage from the user cooperation in this case.

For the wire-tap channel with a helper, it is known that the following perfect-secrecy rate is achievable [1, eq. (10)]:

$$R_1 = \sup_{P_{U_1} P_{U_2} P_{X_1|U_1} P_{X_2|U_2}} \left[I(U_1; Y|U_2) - I(U_1; Z|U_2) \ + \ \min\{I(U_2; Y), I(U_2; Z|U_1)\} \right.$$
$$\left. - \ \min\{I(U_2; Y), I(U_2; Z)\} \right]^+, \qquad (4)$$

where $[x]^+$ denotes $\max\{x, 0\}$.

III. Improved Rate-Equivocation Region

In this section we show that it is possible to have a rate-equivocation region larger than the one given by (3). To that end we introduce an auxiliary random variable Q_1 and we get the following improved region.

Proposition 1: The following rate-equivocation region is achievable:

$$\mathcal{C} = \bigcup_{\pi} \left\{ \quad (R_1, R_\mathrm{e}) : 0 \leq R_\mathrm{e} \leq R_1, \right.$$

$$R_1 \leq R_1' + \min\{I(Q_1; Y|U_2), I(Q_1; Z|U_2)\},$$
$$\left. R_\mathrm{e} \leq \max\left\{ R_1' + R_2' - I(U_1; Z|U_2 Q_1) - I(U_2; Y|Q_1), R_1' + R_2' - I(U_1 U_2; Z|Q_1) \right\} \right. \quad (5)$$

where

$$\pi \triangleq P_{Q_1} P_{U_1|Q_1} P_{U_2} P_{X_1|U_1} P_{X_2|U_2} P_{YZ|X_1 X_2},$$
$$R_1' \triangleq I(U_1; Y|U_2 Q_1), \text{ and}$$
$$R_2' \triangleq \min\{I(U_2; Y|Q_1), I(U_2, Z|U_1)\}.$$

Q_1, U_1, and U_2 are auxiliary random variables satisfying the following Markov chain conditions:

$$Q_1 \to U_1 \to X_1, \text{ and}$$
$$(U_1, U_2) \to (X_1, X_2) \to (Y, Z). \qquad (6)$$

As in [4], let the auxiliary random variable Q_1 correspond to the sequence alphabet decoded by both the receiver and the eavesdropper, while letting U_1 and U_2 denote the sequence alphabets that can be decoded only by the receiver. First, we note that the constraint on R_e in (5) can be re-written as

$$R_\mathrm{e} \leq \begin{cases} I(U_1; Y|U_2 Q_1) - I(U_1; Z|U_2 Q_1), & \text{if } I(U_2; Y|Q_1) \leq I(U_2; Z|Q_1), \\ I(U_1 U_2; Y|Q_1) - I(U_1 U_2; Z|Q_1), & \text{if } I(U_2; Z|Q_1) \leq I(U_2; Y|Q_1), \leq I(U_2; Z|U_1), \\ I(U_1; Y|U_2 Q_1) - I(U_1; Z|Q_1), & \text{if } I(U_2; Z|U_1) \leq I(U_2; Y|Q_1). \end{cases}$$

It is straightforward that by setting $\mathcal{Q}_1 = \emptyset$, we have

$$I(U_1; Y|U_2 Q_1) + \min\{I(Q_1; Y|U_2), I(Q_1; Z|U_2)\} = I(U_1; Y|U_2),$$
$$I(U_1; Y|U_2 Q_1) - I(U_1; Z|U_2 Q_1) = I(U_1; Y|U_2) - I(U_1; Z|U_2).$$

On the other hand, since

$$I(U_1; Y|U_2 Q_1) - I(U_1; Z|U_2 Q_1) = I(U_1; Y|U_2) - I(U_1; Z|U_2) + \big(I(Q_1; Z|U_2) - I(Q_1; Y|U_2)\big),$$

we have

$$\sup_{P_{Q_1} P_{U_1|Q_1} P_{U_2}} \big\{ I(U_1; Y|U_2 Q_1) - I(U_1; Z|U_2 Q_1) \big\} \geq \sup_{P_{U_1} P_{U_2}} \big\{ I(U_1; Y|U_2) - I(U_1; Z|U_2) \big\}. \tag{7}$$

A similar derivation of (7) yields

$$\sup_{P_{Q_1} P_{U_1|Q_1} P_{U_2}} \big\{ I(U_1 U_2; Y|Q_1) - I(U_1 U_2; Z|Q_1) \big\} \geq \sup_{P_{U_1} P_{U_2}} \big\{ I(U_1 U_2; Y) - I(U_1 U_2; Z) \big\},$$

and

$$\sup_{P_{Q_1} P_{U_1|Q_1} P_{U_2}} \big\{ I(U_1; Y|U_2 Q_1) - I(U_1; Z|Q_1) \big\} \geq \sup_{P_{U_1} P_{U_2}} \big\{ I(U_1; Y|U_2) - I(U_1; Z) \big\}.$$

Hence, region $\mathcal{C}$ given by (5) is larger than or equal to the region given by (3). The random variable Q_1 plays not only the role of convexification. The achievability of the region $\mathcal{C}$ will be shown in Appendix A.

For the rate-equivocation region $\mathcal{C}$, if $I(U_2; Y|Q_1) \leq I(U_2; Z|Q_1)$ for every

$$P^*_{Q_1 U_1 U_2 X_1 X_2} \triangleq P_{Q_1 U_1} P_{X_1|U_1} P_{U_2 X_2},$$

the cooperation between sender 1 and sender 2 (the helper) has no effect, and the region is in a simpler form as the convex hull of

$$\tilde{\mathcal{C}} = \bigcup_{P^*_{Q_1 U_1 U_2 X_1 X_2} P_{YZ|X_1 X_2}} \Big\{ (R_1, R_e): \quad 0 \leq R_e \leq R_1,$$
$$R_1 \leq I(U_1; Y|U_2)$$
$$R_e \leq I(U_1; Y|U_2 Q_1) - I(U_1; Z|U_2 Q_1) \Big\}.$$

Although Tang et al. [2] give a larger region in this case, if $I(U_2; Y|U_1) \geq I(U_2; Z|U_1)$, then user cooperation does not take effect. In the following text, we denote the convex hull of $\mathcal{C}$ and $\tilde{\mathcal{C}}$ by $\mathcal{C}^*$ and $\tilde{\mathcal{C}}^*$, respectively. When there is no helping interference, i.e., $R_2 = 0$, then the region $\tilde{\mathcal{C}}$ corresponds to the capacity-equivocation region for the ordinary wire-tap channel given by (2). Note that in the case $R_2 = 0$, the helper transmits a deterministic sequence $u_2^N \in \mathcal{U}_2^N$, and both the receiver and the eavesdropper know this sequence. Therefore, the capacity-equivocation region is still characterized by U_2.

When considering the perfect-secrecy rate, the auxiliary random variable Q_1 introduced to derive a new rate-equivocation region has no impact. For the wire-tap channel with a helper, we can achieve the same perfect-secrecy rate as (4) derived in [1].

As the last result of this section we get the following theorem.

Theorem 1: The rate-equivocation region $\mathcal{C}^*$ is achievable for the wire-tap channel with a helping interferer.

Proof: From the above argument, by the coding scheme given in Appendix A, the region $\mathcal{R}_1(P^*_{Q_1 X_1 X_2})$ is achievable for any given $P^*_{Q_1 X_1 X_2}$, and hence $\mathcal{R}_1$ is achievable. By prefixing a conditional PMF $P_{X_1|U_1} P_{X_2|U_2}$, the region $\mathcal{R}_2$, which is equivalent to $\mathcal{C}$, is also achievable. The convex hull can be taken since we can time-share multiple input PMFs via the *time-sharing principle* [5].

$\square$

IV. An Even Larger Rate-Equivocation Region

We can combine the idea given in [2] with the achievable region $\mathcal{C}^*$ to get a larger achievable rate-equivocation region. The key observation is that the receiver does not necessarily need to decode the dummy message W_2 sent from the helper.

For a fixed $P^*_{Q_1U_1U_2X_1X_2} \triangleq P_{Q_1U_1}P_{X_1|U_1}P_{U_2X_2} \in \mathcal{P}^*$, let $\mathcal{C}_A(P^*_{Q_1U_1U_2X_1X_2})$ be defined as the rate-equivocation region

$$\mathcal{C}_A(P^*_{Q_1U_1U_2X_1X_2}) = \Big\{ \quad (R_1, R_e) : 0 \le R_e \le R_1,$$
$$R_1 \le I(U_1; Y|U_2Q_1) + \min\{I(Q_1; Y|U_2), I(Q_1; Z|U_2)\},$$
$$R_e \le \max\Big\{R'_3 - I(U_1; Z|U_2Q_1) - I(U_2; Y|Q_1), R'_3 - I(U_1U_2; Z|Q_1)\Big\} \quad (8)$$

where

$$R'_2 = \min\{I(U_2; Y|Q_1), I(U_2, Z|U_1)\},$$
$$R'_3 \triangleq I(U_1; Y|U_2Q_1) + R'_2,$$

and Q_1, U_1, and U_2 are auxiliary random variables satisfying Markov chain conditions (6). Then the achievable rate-equivocation region $\mathcal{C}$ is expressed as

$$\mathcal{C} = \bigcup_{P^*_{Q_1U_1U_2X_1X_2}P_{YZ|X_1X_2}} \mathcal{C}_A(P^*_{Q_1U_1U_2X_1X_2}). \qquad (9)$$

We define another rate-equivocation region, for a fixed $P^*_{Q_1U_1U_2X_1X_2} \in \mathcal{P}^*$, as

$$\mathcal{C}_B(P^*_{Q_1U_1U_2X_1X_2}) = \Big\{(R_1, R_e) : \quad R_1 \le I(U_1; Y),$$
$$0 \le R_e \le R_1,$$
$$R_e \le I(U_1; Y|Q_1) - I(U_1; Z|Q_1)\Big\}.$$

Then, a new achievable rate-equivocation region, denoted by $\tilde{\mathcal{C}}$, is given by the convex hull of

$$\tilde{\mathcal{C}} = \bigcup_{P^*_{Q_1U_1U_2X_1X_2}} \Big\{\mathcal{C}_A(P^*_{Q_1U_1U_2X_1X_2}) \cup \mathcal{C}_B(P^*_{Q_1U_1U_2X_1X_2})\Big\}. \qquad (10)$$

From equations (9) and (10), it is readily seen that in general we have $\mathcal{C}^* \subseteq \tilde{\mathcal{C}}^*$ where $\tilde{\mathcal{C}}^*$ denotes the convex hull of $\tilde{\mathcal{C}}$. The region

$$\mathcal{C}_B(P^*) \setminus (\mathcal{C}_A(P^*) \cap \mathcal{C}_B(P^*))$$

expresses an additional region to $\mathcal{C}_A(P^*)$ for a fixed $P^* \in \mathcal{P}^*$, which is given by the observation in [2]. The rate-equivocation region $\tilde{\mathcal{C}}$ can be seen as an extension of the result of [2] in the sense that we derive not only a perfect-secrecy rate but also a rate-equivocation region by introducing the auxiliary random variable Q_1. The key idea lies in the facts that:

(i) The receiver and the eavesdropper can decode a partial message of W_1 at the rate at most

$$\min\{I(Q_1; Y), I(Q_1; Z)\}, \quad \text{and,}$$

(ii) As for the other part of message, dummy message from the helper needs not be decoded, and can be treated as noise.

Note that even though the region $\mathcal{C}_B(P_{Q_1U_1U_2X_1X_2})$ does not involve the rate R_2, user cooperation, i.e., interference by a helper, is necessary to achieve this region, and hence, the PMFs of random variables U_2 and X_2 are also included in the region. The achievability of the region $\tilde{\mathcal{C}}$ is shown in Appendix B.
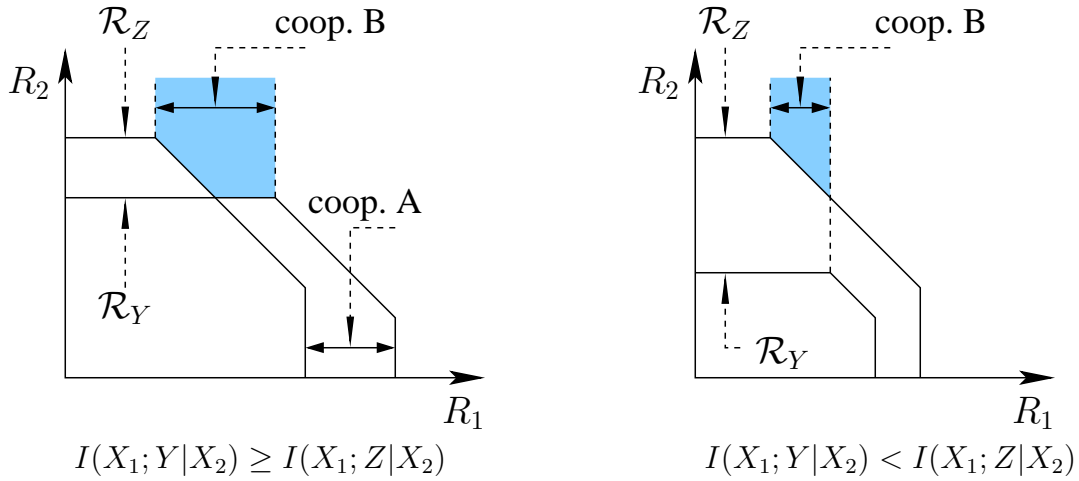
Fig. 2. Pictorial representation for the equivocation gain when cooperation is used for the case (i) of Proposition 2 for the situations $I(X_1; Y|X_2) \geq I(X_1; Z|X_2)$ (left) and $I(X_1; Y|X_2) \geq I(X_1; Z|X_2)$ (right). Pentagons $\mathcal{R}_Y$ and $\mathcal{R}_Z$ express an achievable region for the receiver's MAC and the eavesdropper's MAC, respectively. The cooperation scheme that achieves $\mathcal{C}_A(P^*)$ is labeled "coop. A" and the cooperation scheme that achieves $\mathcal{C}_B(P^*)$, is labeled "coop. B".

When only the perfect-secrecy rate is concerned, the obtained rate-equivocation region is reduced to

$$\tilde{\mathcal{C}}' = \bigcup_{\pi_{12}} \left\{ \mathcal{C}'_A(\pi_{12}) \cup \mathcal{C}'_B(\pi_{12}) \right\}, \tag{11}$$

where

$$\mathcal{C}'_A(\pi_{12}) \triangleq \Big\{ R_1 : \quad R_1 \geq 0,$$
$$R_1 \leq \max \big\{ I(U_1; Y|U_2) - I(U_1; Z|U_2) + R'_2 - I(U_2; Y),$$
$$I(U_1; Y|U_2) + R'_2 - I(U_1 U_2; Z) \big\} \Big\}$$

and

$$\mathcal{C}'_B(\pi_{12}) = \Big\{ R_1 : 0 \leq R_1 \leq [I(U_1; Y) - I(U_1; Z)]^+ \Big\}.$$

for a fixed input distribution $\pi_{12} = P_{U_1 X_1} P_{U_2 X_2}$. Then, the following perfect-secrecy rate is achievable:

$$\sup_{\pi_{12}} \big\{ \mathcal{C}'_A(\pi_{12}) \cup \mathcal{C}'_B(\pi_{12}) \big\}$$

which is the same as the one given in [2].

We next consider conditions under which we get an improvement to region $\mathcal{C}_B(P^*)$, i.e.,

$$\mathcal{C}_B(P^*) \setminus (\mathcal{C}_A(P^*) \cap \mathcal{C}_B(P^*)) \neq \emptyset.$$

We have the following proposition:

Proposition 2: For a given $P^* \in \mathcal{P}^*$, $\mathcal{C}_B(P^*) \setminus (\mathcal{C}_A(P^*) \cap \mathcal{C}_B(P^*)) \neq \emptyset$ if and only if either of the following two conditions is satisfied:

$$(i) \quad I(U_1; Y|Q) > I(U_1; Z|Q) \quad \text{and}$$
$$0 \leq I(U_2; Z|Q_1) - I(U_2; Y|Q_1) \leq I(U_2; Z|U_1) - I(U_2; Y|U_1), \tag{12}$$
$$(ii) \quad I(U_1; Y|Q) > I(U_1; Z|Q) \quad \text{and}$$
$$I(U_2; Z|Q_1) \leq I(U_2; Y|Q_1) \leq I(U_2; Y|U_1) \leq I(U_2; Z|U_1). \tag{13}$$
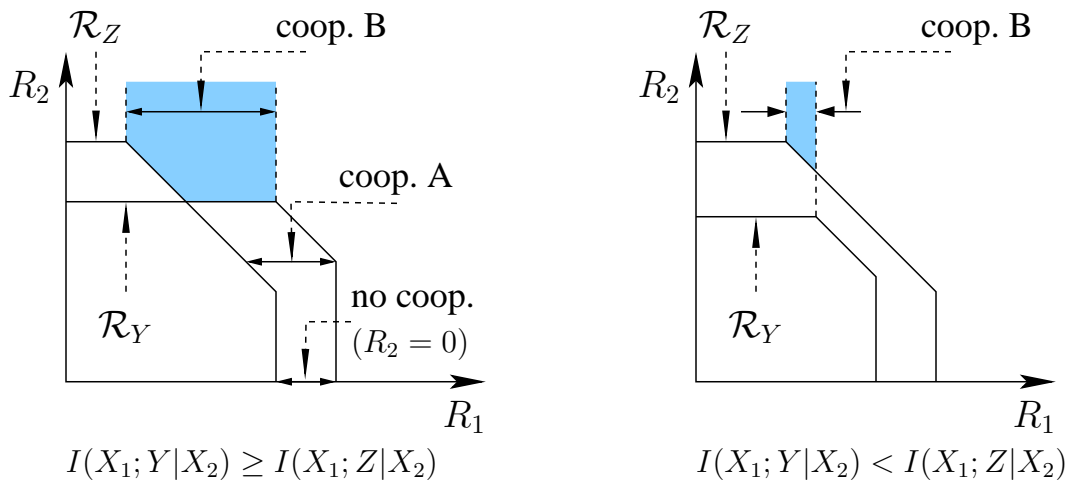
Proof: See Appendix C. □

Fig. 3. Pictorial representation for the equivocation gain when cooperation is used for the case (ii) in Proposition 2 for the situations $I(X_1;Y|X_2) \geq I(X_1;Z|X_2)$ (left) and $I(X_1;Y|X_2) \geq I(X_1;Z|X_2)$ (right). Pentagons $\mathcal{R}_Y$ and $\mathcal{R}_Z$ express an achievable region for the receiver's MAC and the eavesdropper's MAC, respectively. The cooperation scheme that achieves $\mathcal{C}_A(P^*)$ is labeled "coop. A" and the cooperation scheme that achieves $\mathcal{C}_B(P^*)$, is labeled "coop. B".

We illustrate both cases, in which $\mathcal{C}_B(P^*)$ is effective, in Figs. 2 and 3. For illustrative purpose, we consider rate-equivocation regions given by $P_{X_1|Q_1}P_{X_2}$. The actual region is obtained by prefixing $P_{X_1|U_1}P_{X_2|U_2}$ as discussed in Appendix A. Fig. 2 describes the case that satisfies (12) in the following two situations: $I(X_1;Y|X_2) \geq I(X_1;Z|X_2)$ (left) and $I(X_1;Y|X_2) \geq I(X_1;Z|X_2)$ (right). Fig. 3 describes the case that satisfies that satisfies (13) in the following two situations: $I(X_1;Y|X_2) \geq I(X_1;Z|X_2)$ (left) and $I(X_1;Y|X_2) \geq I(X_1;Z|X_2)$ (right). In the figures "coop. A" denotes the cooperation scheme that achieves $\mathcal{C}_A(P^*)$, while "coop. B" the cooperation scheme that achieves $\mathcal{C}_B(P^*)$. Observe that in the right subfigures of both figures only cooperation scheme B gives positive equivocation, implying the usefulness of this cooperation scheme.

V. A Note on the Broadcast Channel with Confidential Messages and a Helping Interferer

Since the effect of Q_1 is not completely clear, one might doubt the true effect of Q_1. In this section, we discuss about the role of the introduced Q_1 by comparing relationship between the broadcast channel with confidential messages (BCC) and the wire-tap channel with a helping interferer. We consider the following two items:

(1) The constraint on R_1 in the new achievable rate-equivocation region $\mathcal{C}$ involves the term

$$\min\{I(Q_1;Y|U_2), I(Q_1;Z|U_2)\},$$

whereas the capacity equivocation region for the ordinary wire-tap channel does not (c.f., (2)).

(2) Although by introducing another auxiliary random variable Q_1 we have a wider rate-equivocation region, this random variable gives no impact in terms of perfect-secrecy (i.e., (4)).

Csiszár and Körner show in [4] that for the broadcast channel with confidential messages (BCC), the use of Q_1 is essential.

In the model of BCC (Fig. 4), there are two receivers, and the sender wishes to send public messages $\mathcal{W}_0$ of rate R_0 to both receivers while public messages $\mathcal{W}_1$ of rate R_1 is confidential to receiver 2. It is
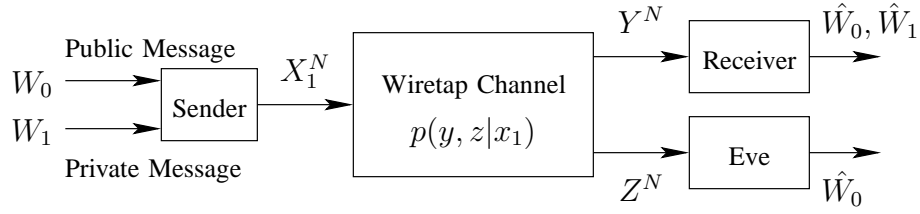
Fig. 4. The broadcast channel with confidential messages (BCC).

known that the following region is the capacity-equivocation region for the BCC [4, Theorem 1]

$$\mathcal{C}_{BCC} = \Big\{(R_1, R_e, R_0): \quad 0 \le R_0, 0 \le R_e \le R_1,$$
$$R_0 + R_1 \le I(U_1; Y|Q_1) + \min\{I(Q_1; Y), I(Q_1; Z)\},$$
$$R_e \le I(U_1; Y|Q_1) - I(U_1; Z|Q_1),$$
$$R_0 \le \min\{I(Q_1; Y), I(Q_1; Z)\}\Big\} \quad (14)$$

where the random variables satisfy

$$Q_1 \to U_1 \to X_1 \to (Y, Z). \quad (15)$$

From (14), the constraint on $R_0 + R_1$ also involves the term $\min\{I(Q_1; Y), I(Q_1; Z)\}$ (c.f., above item 1). Furthermore, the random variable Q_1 is essentially necessary because receiver 2 should estimate W_0 from Z^N reliably. Having this in mind, we can argue the *BCC with a helping interferer* as in Fig. 5, and we can achieve the following rate-equivocation region, that is the convex hull of

$$\mathcal{C}_{BCCH} = \bigcup_{\pi^*} \{\mathcal{C}'_A(\pi^*) \cup \mathcal{C}'_B(\pi^*)\}. \quad (16)$$

where

$$\mathcal{C}'_A(\pi^*) \triangleq \Big\{(R_1, R_e, R_0): \quad 0 \le R_0, 0 \le R_e \le R_1,$$
$$R_0 + R_1 \le I(U_1; Y|U_2 Q_1) + \min\{I(Q_1; Y|U_2), I(Q_1; Z|U_2)\},$$
$$R_e \le I(U_1; Y|U_2 Q_1) - I(U_1; Z|U_2 Q_1),$$
$$R_0 \le \min\{I(Q_1; Y|U_2), I(Q_1; Z|U_2)\}\Big\},$$

and

$$\mathcal{C}'_B(\pi^*) = \Big\{(R_1, R_e, R_0): \quad 0 \le R_0, 0 \le R_e \le R_1,$$
$$R_0 + R_1 \le I(U_1; Y|Q_1) + \min\{I(Q_1; Y), I(Q_1; Z)\},$$
$$R_e \le I(U_1; Y|Q_1) - I(U_1; Z|Q_1),$$
$$R_0 \le \min\{I(Q_1; Y), I(Q_1; Z)\}\Big\}.$$

Here, Q_1, U_1, and U_2 are auxiliary random variables satisfying the Markov chain conditions (6). Therefore, we think that in the case of the BCC with a helper, the use of Q_1 is also *essential*. Furthermore, when $R_2 = 0$, the above region reduces to the capacity-equivocation region for the BCC.

Remark 1: We cannot directly use the achievability scheme from Appendix A, and the constraint on $R_e \in \mathcal{C}'_A(P^*)$, which is always achieved with $R_2 = 0$, is smaller than that in $\mathcal{C}_A(P^*)$ given in (8) for the wire-tap channel with a helper. The main reason for this is that, by setting
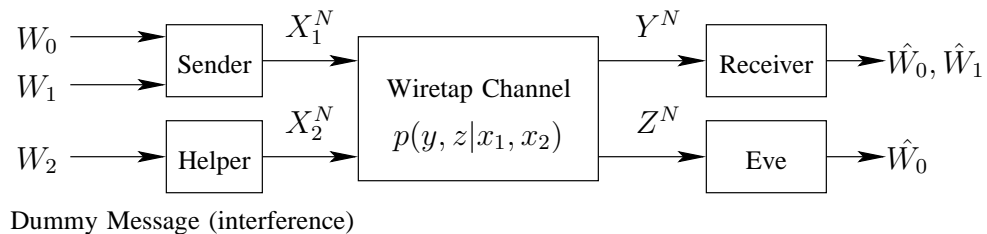
$$R_2 \le \min\{I(U_2; Y|Q_1), I(U_2; Z|U_1)\}$$

Fig. 5. BC with confidential messages and with a helper.

as in Appendix A, then receiver 2 cannot always decode W_2 (and equivalently, U_2^N) correctly, and it cannot decode W_0 accordingly for some

$$R_0 \leq \min\{I(Q_1; Y|U_2), I(Q_1; Z|U_2)\}.$$

If $I(Q_1; Y|U_2) \leq I(Q_1; Z)$ is satisfied, then there is a possibility to have an advantage. On the other hand, in the case of the wire-tap channel with a helper, W_2 needs not be decoded by the eavesdropper, so this problem does not occur.

Despite the above remark, from (14) and (16), the cooperation by a helper gives a larger rate-equivocation region compared with the case of the ordinary BCC (with no helpers). This indicates that the cooperation has an effect even for the BCC case, and observation by Tang et al. [2] is also useful.

VI. CONCLUSION

We have derived a new achievable rate-equivocation region for a class of wire-tap channels with a helping interferer, which has been shown to be larger than the rate-equivocation region given by [1]. Our result can naturally adopt the observation given by [2], yielding an even larger rate-equivocation region than the previously known regions. We also discussed about some relationship of our result with the capacity-equivocation over the broadcast channel with confidential messages in order to explain the role of the newly introduced random variable.

APPENDIX A
ACHIEVABILITY OF THE NEW REGION

We shall show an achievability scheme for the region $\mathcal{C}$ via random coding. As in the wire-tap channel [4], we introduce rate splitting of R_1 into R_{10} and R_{11}, where R_{10} denotes the rate of messages that can be decoded by both the receiver and the eavesdropper, and R_{11} denotes the rate of messages that can be decoded only by the receiver. First we define the following region:

$$
\mathcal{R}_1 = \bigcup_{P_{X_1 Q_1} P_{X_2} P_{YZ|X_1 X_2}} \Big\{ (R_1, R_e): \quad R_1 = R_{10} + R_{11}, 0 \leq R_{10}, 0 \leq R_e \leq R_1,
$$
$$
R_{10} \leq \min\{I(Q_1; Y|X_2), I(Q_1; Z|X_2)\},
$$
$$
R_{11} \leq I(X_1; Y|X_2 Q_1),
$$
$$
R_e \leq \max \Big\{ I(X_1; Y|U_2 Q_1) - I(X_1; Z|X_2 Q_1),
$$
$$
I(X_1; Y|X_2 Q_1) - I(X_1 X_2; Z|Q_1)
$$
$$
+ \min\{I(X_2; Y|Q_1), I(X_2; Z|X_1)\} \Big\}. \quad (17)
$$

As discussed in [4], if $\mathcal{R}_1$ is achievable, the following region $\mathcal{R}_2$ is achievable by prefixing a conditional PMF $P_{X_1|U_1}P_{X_2|U_2}$:

$$\mathcal{R}_2 = \bigcup_{P_{Q_1}P_{U_1|Q_1}P_{U_2}P_{X_1|U_1}P_{X_2|U_2}P_{YZ|X_1X_2}} \Big\{ (R_1, R_e): \quad R_1 = R_{10} + R_{11}, 0 \leq R_{10}, 0 \leq R_e \leq R_1,$$

$$R_{10} \leq \min\{I(Q_1; Y|U_2), I(Q_1; Z|U_2)\},$$
$$R_{11} \leq I(U_1; Y|U_2Q_1),$$
$$R_e \leq \max\Big\{ I(U_1; Y|U_2Q_1) - I(U_1; Z|U_2Q_1),$$
$$I(U_1; Y|U_2Q_1) - I(U_1U_2; Z|Q_1)$$
$$+ \min\{I(U_2; Y|Q_1), I(U_2; Z|U_1)\}\Big\}.$$

By using the relation $R_{10} = R_1 - R_{11}$, Fourier-Motzkin elimination yields the region $\mathcal{C}$ given by (5). Hence, in terms of the achievability to the region $\mathcal{C}$, it suffices to show that the rate-equivocation region $\mathcal{R}_1$ is achievable for every given $P_{Q_1X_1}P_{X_2}$.

Next we show the achievability of $\mathcal{R}_1$, given by (17), via random coding and the joint *asymptotic equipartition property* (AEP) [5]. We fix a joint PMF $P^*_{Q_1X_1X_2} \triangleq P_{Q_1X_1}P_{X_2}$, and let the target region be denoted by $\mathcal{R}_1(P^*_{Q_1X_1X_2})$. We consider two cases that will be called Case 1 and Case 2.

A. Case 1: $I(X_1; Y|X_2Q_1) \leq I(X_1; Z|X_2Q_1)$

In this case, we need to consider only the case $I(X_2; Y|Q_1) \geq I(X_2; Z|Q_1)$, since otherwise the rate-equivocation becomes zero because the first constraint on R_e in (17) is apparently negative (i.e., it gives a trivial upper-bound on R_e). Then, the constraint on R_e is expressed as

$$R_e \leq [I(X_1; Y|X_2Q_1) + \min\{I(X_2; Y|Q_1), I(X_2; Z|X_1)\} - I(X_1X_2; Z|Q_1)]^+. \tag{18}$$

1) Codebook generation: For a given $P^*_{Q_1X_1X_2}$, we first generate $2^{NR_{10}}$ independent and identically distributed(i.i.d.) sequences at random according to

$$P_{Q_1^N}(\boldsymbol{q}) \triangleq \prod_{n=1}^{N} P_{Q_1}(q_n),$$

and index them as $\boldsymbol{q}(i), i \in [1, 2^{NR_{10}}]$, with

$$R_{10} \leq \min\{I(Q_1; Y|X_2), I(Q_1; Z|X_2)\}. \tag{19}$$

When $j_1 \leq j_2$, $[j_1, j_2]$ denotes the set of all integers from j_1 to j_2. For given $\boldsymbol{q}(i), i \in [1, 2^{NR_{10}}]$, we generate $2^{NR_{11}}$ i.i.d. sequences at random according to

$$P_{X_1^N|Q_1^N}(\boldsymbol{x}_1|\boldsymbol{q}) \triangleq \prod_{n=1}^{N} P_{X_1|Q_1}(x_{1n}|q_n),$$

and index them as $\boldsymbol{x}_1(i, b), b \in [1, 2^{NR}]$, with

$$R \leq I(X_1; Y|X_2Q_1). \tag{20}$$

We also generate 2^{NR_2} i.i.d. sequences at random according to $P_{X_2^N}(\boldsymbol{x}_2) \triangleq \prod_{n=1}^{N} P_{X_2}(x_{2n})$, and index them as $\boldsymbol{x}_2(k), k \in [1, 2^{NR_2}]$, with

$$R_2 \leq \min\{I(X_2; Y|Q_1), I(X_2; Z|X_1)\}. \tag{21}$$

Let

$$R' \triangleq [R + R_2 - I(X_1X_2; Z|Q_1)]^+ \tag{22}$$

express the rate that exceeds the eavesdropper's ability to decode a sequence reliably. We also define $\mathcal{W} = [1, 2^{NR'}]$, $\mathcal{L} = [1, 2^{N(R-R')}]$, and $\mathcal{B} = \mathcal{W} \times \mathcal{L} = [1, 2^{NR}]$. Note that $R' \leq R$ since

$$R - R' \geq I(X_1 X_2; Z|Q_1) - I(X_2; Z|X_1) = I(X_1; Z|Q_1).$$

Hereafter, we assume $R' > 0$ for simplicity. If this is not the case, no security level can be reached, and we achieve only $(R_1, 0)$ such that $R_1 \leq R$ which is still inside the rate-equivocation region $\mathcal{R}_1$. We call this codebook generation and the encoding and decoding scheme described below *Coding Scheme 1*.

2) Encoding: For a given rate-equivocation pair (R_{10}, R_{11}, R_e) such that $R_1 = R_{10} + R_{11}$ and $R_e \leq R_1$, we consider the following encoding scheme: Assume that a secret message $w_1 = (w_{10}, w_{11}) \in \mathcal{W}_1$ with $w_{10} \in \mathcal{W}_{10} \triangleq [1, 2^{NR_{10}}]$ and $w_{11} \in \mathcal{W}_{11} \triangleq [1, 2^{NR_{11}}]$ is input to sender 1 and a random message $w_2 \in [1, 2^{NR_2}]$ is generated at sender 2.

The encoding function for w_{11} at sender 1 operates in the following stochastic manner:

(i) If $R_{11} > R'$, then we divide $\mathcal{W}_{11}$ into $\mathcal{W}$ and $\mathcal{J} \triangleq [1, 2^{N(R_{11}-R')}]$ as $\mathcal{W}_{11} = \mathcal{W} \times \mathcal{J}$. Let g be the partition that divides $\mathcal{L}$ into $|\mathcal{J}| = 2^{N(R_{11}-R')}$ subsets $\mathcal{L}'_1, \ldots, \mathcal{L}'_{2^{N(R_{11}-R')}}$ with equal cardinalities $2^{N(R-R_{11})}$. The encoder determines (w, l) from $w_{11} = (w, j)$ such that l is uniformly chosen from the partition $\mathcal{L}'_j$ at random. In this case, there is a one-to-one correspondence between $\{(w, l)\}$ and $[1, 2^{NR}]$.

(ii) If $R_{11} \leq R'$, then the encoder obtains (w, l) by setting $w \triangleq w_{11}$ and uniformly choosing l from $\mathcal{L}$ at random. In this case, there is a one-to-one correspondence between $\{(w, l)\}$ and $[1, 2^{N(R_{11}+R-R')}]$.

The transmitted sequence from sender 1 is $\boldsymbol{x}_1(i, b)$ with $i = w_{10}$ and $b = (w, l) \in [1, 2^{NR}]$. Sender 2 transmits the sequence $\boldsymbol{x}_2(k)$ with $k = w_2$, where $w_2 \in [1, 2^{NR_2}]$ is uniformly selected.

3) Decoding:: Upon receiving $\boldsymbol{y} \in \mathcal{Y}^N$, the receiver seeks a message pair $(\hat{i}, \hat{k})$ such that

$$\left(\boldsymbol{q}(\hat{i}), \boldsymbol{x}_2(\hat{k}), \boldsymbol{y} \right) \in \mathcal{A}_\epsilon^{(N)}$$

where $\mathcal{A}_\epsilon^{(N)}$ denotes the ϵ-jointly typical set [5] for any fixed $\epsilon > 0$. If there does not exist or there are more than one such sequence, then the receiver declares a decoding error. Then, the receiver seeks a message $\hat{b} = (\hat{w}, \hat{l})$ such that

$$\left(\boldsymbol{q}(\hat{i}), \boldsymbol{x}_1(\hat{i}, \hat{b}), \boldsymbol{x}_2(\hat{k}), \boldsymbol{y} \right) \in \mathcal{A}_\epsilon^{(N)}$$

for given $(\hat{i}, \hat{k})$. Having $(\hat{i}, \hat{b})$ such that $\hat{b} = (\hat{w}, \hat{l})$, the receiver obtains the estimates of the transmitted message $w_1 = (w_{10}, w_{11})$ by setting

$$\hat{w}_{10} \triangleq \hat{i}, \hat{w}_{11} \triangleq (\hat{w}, g(\hat{l})), \quad \text{if} \quad R_{11} > R', \quad \text{and}$$
$$\hat{w}_{10} \triangleq \hat{i}, \hat{w}_{11} \triangleq \hat{w}, \quad \quad \text{if} \quad R_{11} \leq R'.$$

4) Analysis of Reliability: The average probability of decoding error for the receiver, denoted by $\overline{P}_e^{(N)}(i, b, k)$ provided that (i, b, k) is sent, is upper-bounded as

$$\overline{P}_e^{(N)}(i, b, k) \leq \overline{P}_{e,1}^{(N)}(i, k) + \overline{P}_{e,2}^{(N)}(b|i, k), \tag{23}$$

where $\overline{P}_{e,1}^{(N)}(i, k)$ and $\overline{P}_{e,2}^{(N)}(b|i, k)$ denote the probabilities of decoding error for the first step (estimation of (i, k)) and the second step (estimation of b given a true transmitted pair (i, k)), respectively. It is easily seen that the error probability of the first decoding step can be made arbitrarily small for all sufficiently large N by the AEP [5] since R_{10} and R_2 satisfy (19), (21), and

$$\begin{aligned} R_{10} + R_2 &\leq \min\{I(Q_1; Y), I(Q_1; Z)\} + \min\{I(X_2; Y|Q_1), I(X_2; Z|X_1)\} \\ &\leq I(Q_1 X_2; Y). \end{aligned} \tag{24}$$

Also, the error probability of the second decoding step can be made arbitrarily small for sufficiently large N by the AEP and (20), and so can the probability $\overline{P}_e^{(N)}(i, b, k)$.

5) Analysis of Equivocation: The equivocation $R_e^{(N)} = \frac{1}{N}H(W_1|Z^N)$ is lower-bounded by

$$
\begin{aligned}
R_e^{(N)} &= \frac{1}{N}H(W_{10}W_{11}|Z^N) \\
&\geq \frac{1}{N}H(W_{10}W_{11}|Z^N W_{10}) \\
&= \frac{1}{N}H(W_{11}|Z^N W_{10}),
\end{aligned}
\tag{25}
$$

where the inequality follows from the fact that conditioning does not increase the entropy. By a similar expansion for $H(W_{11}|Z^N W_{10})$ as in [1, eq. (45)], we obtain

$$
H(W_{11}|Z^N W_{10}) \geq H(X_1^N X_2^N|W_{10}) - I(X_1^N X_2^N; Z^N|W_{10}) - H(X_1^N X_2^N|W_{10}W_{11}Z^N).
\tag{26}
$$

We shall consider bounding each term in (26). For the first term, we have

$$
H(X_1^N X_2^N|W_{10}) = H(X_1^N|W_{10}) + H(X_2^N)
$$

and

$$
H(X_1^N|W_{10}) = H(X_1^N|W_{10}Q_1^N) = H(X_1^N|Q_1^N),
$$

where the first equality is due to the fact that Q_1^N is a deterministic function of W_{10}, while the last equality follows from the Markov chain relationship $W_{10} \to Q_1^N \to X_1^N$. Since the codewords are generated according to i.i.d. distributions, it follows that

$$
H(X_1^N|Q_1^N) = NH(X_1|Q_1) \geq NR,
\tag{27}
$$

and

$$
H(X_2^N) = NH(X_2) \geq NR_2.
\tag{28}
$$

It is sufficient that we directly replace these inequalities with

$$
NH(X_1|Q_1) \geq NI(X_1;Y|X_2Q_1)
$$

and

$$
NH(X_2) \geq N\min\{I(X_2;Y|Q_1), I(X_2;Z|X_1)\}.
$$

For the second term in (26), we expand

$$
I(X_1^N X_2^N; Z^N|W_{10}) = H(Z^N|W_{10}) - H(Z^N|X_1^N X_2^N W_{10}),
\tag{29}
$$

for which we have

$$
H(Z^N|W_{10}) = H(Z^N|Q_1^N) = NH(Z|Q_1)
\tag{30}
$$

due to the fact that Q_1^N is a deterministic function of W_{10}, the Markov chain relationship $W_{10} \to Q_1^N \to Z^N$, and an i.i.d. distribution for Z^N given Q_1^N. We also have

$$
H(Z^N|X_1^N X_2^N W_{10}) = H(Z^N|X_1^N X_2^N Q_1^N) = NH(Z|X_1X_2Q_1).
\tag{31}
$$

It follows from (30) and (31) that (29) becomes

$$
I(X_1^N X_2^N; Z^N|W_{10}) = NI(X_1X_2; Z|Q_1).
\tag{32}
$$

We now consider the third term in (26). Consider decoding of l given $w_1 = (w_{10}, w_{11}) \in \mathcal{W}_1$ by observing $z \in \mathcal{Z}^N$. For the case $R_{11} > R'$, since this decoder knows $j \in \mathcal{J}$, which is given by $w_{11} = (w, j) \in \mathcal{W}_{11}$, and using the following inequalities

$$
\frac{1}{N}\log_2 |\mathcal{L}_j'| + R_2 \leq R - R' + R_2 = I(X_1X_2; Z|Q_1),
$$

and

$$\frac{1}{N}\log_2|\mathcal{L}'_j| \leq R \leq I(X_1; Z|X_2Q_1), \tag{33}$$

the average probability of decoding error can be made arbitrarily small for sufficiently large N. Note that, in this case,

$$R \leq I(X_1; Y|X_2Q_1) \leq I(X_1; Z|X_2Q_1).$$

For the case $R_{11} \leq R'$, we also have

$$\frac{1}{N}\log_2|\mathcal{L}| + R_2 \leq R - R' + R_2 = I(X_1X_2; Z|Q_1),$$

and

$$\frac{1}{N}\log_2|\mathcal{L}| \leq R \leq I(X_1; Z|X_2Q_1). \tag{34}$$

Again, the average probability of decoding error can be made arbitrarily small with all sufficiently large N. Therefore, by Fano's inequality [5], for any given $\epsilon' > 0$, we have

$$\frac{1}{N}H(X_1^N X_2^N|W_{10}W_{11}Z^N) \leq \epsilon' \tag{35}$$

for sufficiently large N. Substituting (28), (32), and (35) into (26) yields, for any given $\epsilon' > 0$,

$$R_{\mathrm{e}}^{(N)} \geq R + R_2 - I(X_1X_2; Z|Q_1) - \epsilon'$$

for N sufficiently large. Since we can choose any pair of R and R_2 subject to (20) and (21), there exist R and R_2 such that, for any $\epsilon' > 0$,

$$R_{\mathrm{e}}^{(N)} \geq I(X_1; Y|X_2Q_1) + \min\{I(X_2; Y|Q_1), I(X_2; Z|X_1)\} - I(X_1X_2; Z|Q_1) - \epsilon'. \tag{36}$$

Hence, it follows from (22) and (36) that any equivocation R_{e} satisfying (18) is achievable.

B. Case 2: $I(X_1; Y|X_2Q_1) > I(X_1; Z|X_2Q_1)$

In this case, if $I(X_2; Y|Q_1) \geq I(X_2; Z|Q_1)$, then the constraint on R_{e} is given by (18). We can use Coding Scheme 1 discussed in Case 1 with a slight modification. We set

$$R' = \left[R + \min\{I(X_2; Y|Q_1), I(X_2; Z|X_1)\} - I(X_1X_2; Z|Q_1)\right]^+,$$

and we assume that $R' > 0$, because no security level is obtained otherwise. Then, for the analysis of equivocation, the left hand side of (33) is bounded as

$$\frac{1}{N}\log_2|\mathcal{L}'_j| \leq R - R' = I(X_1X_2; Z|Q_1) - \min\{I(X_2; Y|Q_1), I(X_2; Z|X_1)\}.$$

Since $I(X_2; Z|Q_1) \leq \min\{I(X_2; Y|Q_1), I(X_2; Z|X_1)\}$ and

$$\begin{aligned}
I(X_2; Z|Q_1) &= H(X_2) - H(X_2|Q_1Z) \\
&\leq H(X_2) - H(X_2|Q_1X_1Z) \\
&= I(X_2; Z|X_1)
\end{aligned}$$

where the last equality follows from the Markov chain relationship

$$Q_1 \to (X_1, Z) \to X_2,$$

we have (33) if $R_{11} > R'$. From the same reasoning, we also have (34) if $R_{11} \leq R'$. Other arguments are quite similar to those for Case 1, and we can show that any rate-equivocation pair $(R_1, R) \in \mathcal{R}_1(P^*_{Q_1X_1X_2})$ is achievable.

We then consider the case $I(X_2; Y|Q_1) \leq I(X_2; Z|Q_1)$. In this case, the constraint on R_e in (17) is given by

$$R_e \leq I(X_1; Y|X_2 Q_1) - I(X_1; Z|X_2 Q_1),$$

which can be achieved by a similar coding/decoding scheme to Coding Scheme 1 by letting

$$
\begin{aligned}
R &\leq I(X_1; Y|X_2 Q_1), \text{ and} \\
R' &= [R_1 - I(X_1; Z|X_2 Q_1)]^+.
\end{aligned}
$$

In this case, R_2 can be arbitrarily set in the range $0 \leq R_2 \leq I(X_2; Y|Q_1)$. We call this coding scheme *Coding Scheme 2*.

To show the equivocation at the eavesdropper, note that

$$
\begin{aligned}
R_e^{(N)} &= \frac{1}{N} H(W_{10} W_{11}|Z^N) \\
&\geq \frac{1}{N} H(W_{11}|Z^N X_2^N W_{10}).
\end{aligned}
$$

Similarly to the derivation [1, eq. (49)], we obtain

$$H(W_{11}|Z^N X_2^N W_{10}) \geq H(X_1^N|W_{10}) - I(X_1^N; Z^N|W_{10} X_2^N) - H(X_1^N|W_{10} W_{11} Z^N X_2^N),$$

in which the right hand side is lower-bounded by

$$N(I(X_1; Y|X_2 Q_1) - I(X_1; Z|X_2 Q_1) - \epsilon),$$

for any given $\epsilon > 0$, for all sufficiently large N. This completes the proof of the achievability to the region $\mathcal{R}_1(P^*_{Q_1 X_1 X_2})$.

APPENDIX B
AN ACHIEVABLE SCHEME FOR THE REGION $\mathcal{R}_B$

We give an achievability scheme for the region $\tilde{\mathcal{C}}$ given in (10). Let $\pi^* = P^*_{Q_1 U_1 U_2 X_1 X_2}$ and $\mathcal{R}_B(\pi^*)$ be defined as

$$
\mathcal{R}_B(\pi^*) = \Big\{ (R_1, R_e) : \quad R_1 = R_{10} + R_{11}, 0 \leq R_{10},
$$
$$
0 \leq R_e \leq R_1,
$$
$$
R_{10} \leq \min\{I(Q_1; Y), I(Q_1; Z)\},
$$
$$
R_{11} \leq I(U_1; Y|Q_1),
$$
$$
R_e \leq I(U_1; Y|Q_1) - I(U_1; Z|Q_1) \Big\}. \tag{37}
$$

By virtue of Fourier-Motzkin elimination, it is readily shown that

$$\bigcup_{\pi^*} \mathcal{C}_B(\pi^*) = \bigcup_{\pi^*} \mathcal{R}_B(\pi^*), \tag{38}$$

and from (9) and (10),

$$
\begin{aligned}
\tilde{\mathcal{C}} &= \bigcup_{\pi^*} \{\mathcal{C}_A(\pi^*) \cup \mathcal{R}_B(\pi^*)\} \\
&= \mathcal{C} \cup \bigcup_{\pi^*} \mathcal{R}_B(\pi^*).
\end{aligned}
$$

The region $\mathcal{C}$ is achievable by the coding method given in Section III. Therefore, if we have an achievability scheme to achieve $\mathcal{R}_B(P^*_{Q_1 U_1 U_2 X_1 X_2})$ for any given $P^*_{Q_1 U_1 U_2 X_1 X_2} \in \mathcal{P}^*$, then the region $\tilde{\mathcal{C}}$ is also achievable.

We turn to showing an achievable scheme to the region $\mathcal{R}_B(P^*_{Q_1 U_1 U_2 X_1 X_2})$ for arbitrarily fixed $\pi^* = P^*_{Q_1 U_1 U_2 X_1 X_2} \in \mathcal{P}^*$. The description of a achievability scheme is a combination of the scheme in Appendix A and the scheme given in [2].

APPENDIX C
PROOF OF PROPOSITION 2

The condition $I(U_1; Y|Q) > I(U_1; Z|Q)$ is necessary since otherwise there is no equivocation in $\mathcal{C}_B(P^*)$. As we have seen in (7), there are three cases for which the region $\mathcal{C}_A(P^*)$ is of different form.

If $I(U_2; Y|Q_1) \leq I(U_2; Z|Q_1)$, then the constraint on $R_e \in \mathcal{C}_A(P^*)$ is given by

$$R_e \leq [I(U_1; Y|U_2Q_1) - I(U_1; Z|U_2Q_1)]^+.$$

Then the constraint on $R_e \in \mathcal{C}_B(P^*)$ has an effect iff

$$I(U_1; Y|Q_1) - I(U_1; Z|Q_1) \geq I(U_1; Y|U_2Q_1) - I(U_1; Z|U_2Q_1). \tag{39}$$

First note that

$$\begin{aligned}
& I(U_1; Y|Q_1) - I(U_1; Z|Q_1) - (I(U_1; Y|U_2Q_1) - I(U_1; Z|U_2Q_1)) \\
& = I(U_1; Z|U_2Q_1) - I(U_1; Z|Q_1) - (I(U_1; Y|U_2Q_1) - I(U_1; Y|Q_1)).
\end{aligned} \tag{40}$$

Since

$$\begin{aligned}
I(U_1; Z|U_2Q_1) - I(U_1; Z|Q_1) &= I(U_1U_2; Z|Q_1) - I(U_1; Z|Q_1) - I(U_2; Z|Q_1) \\
&= I(U_2; Z|U_1) - I(U_2; Z|Q_1)
\end{aligned}$$

and also

$$I(U_1; Y|U_2Q_1) - I(U_1; Y|Q_1) = I(U_2; Y|U_1) - I(U_2; Y|Q_1),$$

then (40) becomes

$$\begin{aligned}
& I(U_1; Y|Q_1) - I(U_1; Z|Q_1) - (I(U_1; Y|U_2Q_1) - I(U_1; Z|U_2Q_1)) \\
& = I(U_2; Z|U_1) - I(U_2; Z|Q_1) - (I(U_2; Y|U_1) - I(U_2; Y|Q_1))).
\end{aligned} \tag{41}$$

Therefore, (39) holds iff

$$I(U_2; Z|U_1) - I(U_2; Z|Q_1) \geq I(U_2; Y|U_1) - I(U_2; Y|Q_1),$$

leading to (12).

If $I(U_2; Z|Q_1) \leq I(U_2; Y|Q_1) \leq I(U_2; Z|U_1)$, then the constraint on $R_e \in \mathcal{C}_A(P^*)$ is given by

$$R_e \leq [I(U_1U_2; Y|Q_1) - I(U_1U_2; Z|Q_1)]^+.$$

Then the constraint on $R_e \in \mathcal{C}_B(P^*)$ has an effect iff

$$I(U_1; Y|Q_1) - I(U_1; Z|Q_1) \geq I(U_1U_2; Y|Q_1) - I(U_1U_2; Z|Q_1). \tag{42}$$

We note that

$$\begin{aligned}
& I(U_1; Y|Q_1) - I(U_1; Z|Q_1) - (I(U_1U_2; Y|Q_1) - I(U_1U_2; Z|Q_1)) \\
& = I(U_2; Z|U_1) - I(U_2; Y|U_1).
\end{aligned} \tag{43}$$

Therefore, (42) holds iff (13) holds.

If $I(U_2; Z|U_1) \leq I(U_2; Y|Q_1)$, then the constraint on $R_e \in \mathcal{C}_A(P^*)$ is given by $R_e \leq [I(U_1U_2; Y|Q_1) - I(U_1; Z|Q_1)]^+$. In this case, since it always holds

$$I(U_1; Y|Q_1) - I(U_1; Z|Q_1) \leq I(U_1U_2; Y|Q_1) - I(U_1; Z|Q_1), \tag{44}$$

the constraint on $R_e \in \mathcal{C}_B(P^*)$ has *no effect*. $\qquad\square$

APPENDIX D
THE WIRE-TAP CHANNEL WITH A DEAF-INTERFERER

In wireless network settings, sender 2 (the helper) in the wire-tap channel with a helper can observe a noisy sequence of the transmitted sequence X_1^N from sender 1. Let Y_1^N denote the sequence observed by sender 2. For some security systems, it is desired to avoid leaking information about W_1 to sender 2, which motivates the introduction of another type of the wire-tap channel with a helper, called the wire-tap channel with a *deaf-helper* (a *deaf-interferer*) [1].

The wire-tap channel with a deaf-helper looks like the relay-eavesdropper channel, in which a relay node observes Y_1^N and helps to increase the rate of W_1 or the equivocation at the eavesdropper. Note that in this channel model, the relay node might (partially) decode the message W_1 for the cooperation. On the other hand, the scenario of the wire-tap channel with a deaf-helper describes the setting in which sender 1 with secret messages does not fully trust the other sender (the helper) but still wishes to get help from the user cooperation. As in [1], we assume that sender 2 is not malicious, and willing to help the communication from sender 1 to the receiver. Since sender 2 "forwards" a dummy sequence instead of forwarding a (partial) message of sender 1, the cooperation scheme is called a *noise-forwarding (NF)* strategy.

In this setting, a rate-equivocation region is defined by introducing an additional security constraint as follows:

Definition 3: A *rate-equivocation pair* (R_1, R_e) is said to be *achievable* if there exists a sequence of (N, M_1) codes such that for every $\epsilon > 0$,

$$R_1 \geq \frac{\log_2 M_1}{N} - \epsilon,$$

$$P_e^{(N)} \leq \epsilon,$$

$$R_e^{(N)} \triangleq \frac{1}{N} H(W_1|Z^N) \geq R_e - \epsilon,$$

$$R_s^{(N)} \triangleq \frac{1}{N} H(W_1|Y_1^N X_2^N) \geq R_e - \epsilon$$

for all sufficiently large N.

We conjecture that the convex hull of the following rate-equivocation region is achievable

$$\mathcal{C}_{\mathrm{DH}} = \bigcup_{P_{Q_1} P_{U_1|Q_1} P_{U_2} P_{X_1|U_1} P_{X_2|U_2} P_{YZ|X_1 X_2}} \Big\{ (R_1, R_e) : 0 \leq R_e \leq R_1,$$

$$R_1 \leq I(U_1; Y|U_2 Q_1) + \min\{I(Q_1; Y|U_2), I(Q_1; Z|U_2)\},$$

$$R_e \leq \max\Big\{ R_3' - I(U_1; Z|U_2 Q_1) - I(U_2; Y|Q_1), R_3' - I(U_1 U_2; Z|Q_1) \Big\}$$

$$R_e \leq [I(U_1; Y|U_2 Q_1) - I(U_1; Y_1|U_2 Q_1)]^+ \Big\}$$

where

$$R_2' = \min\{I(U_2; Y|Q_1), I(U_2, Z|U_1)\},$$

$$R_3' = I(U_1; Y|U_2 Q_1) + R_2',$$

and Q_1, U_1 and U_2 are auxiliary random variables satisfying the Markov chain conditions given by (6).

As for the perfect-secrecy rate, the above achievable rate-equivocation region reduces to the following result, which is the same as that given in [1, Theorem 6].

Theorem 2: The perfect-secrecy rate for the wire-tap channel with a deaf-helper, given by

$$R_1 = \sup_{P_{U_1 X_1} P_{U_2 X_2}} \min\{R_{\mathbf{e},1}, R_{\mathbf{e},2}\},$$

where

$$R_{\mathsf{e},1} \triangleq \max\left\{I(U_1;Y|U_2) - I(U_1;Z|U_2) + R_2' - I(U_2;Y|), I(U_1;Y|U_2) + R_2' - I(U_1U_2;Z)\right\}, \text{and}$$

$$R_{\mathsf{e},2} \triangleq [I(U_1;Y|U_2) + R_2' - I(U_1;Y_1|U_2)]^+,$$

is achievable.

REFERENCES

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

[2] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "Interference assisted secret communication," in *Proc. IEEE Inform. Theory Workshop*, Porto, Portugal, 2008.

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

[4] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[5] T. M. Cover and J. A. Thomas, *Elements of Information Theory*.   New York, NY: John Wiley & Sons, 1991.