Cooperative Binning and Channel Prefixing for Secrecy in Interference Channels

O. Ozan Koyluoglu and Hesham El Gamal

Abstract

This paper investigates the fundamental performance limits of the two-user interference channel in the presence of an external eavesdropper. In this setting, we construct an inner bound, to the secrecy capacity region, based on the idea of cooperative binning and channel prefixing in which the two users *cooperatively* design their binning codebooks and *jointly* optimize their channel prefixing distributions. Our achievability scheme also utilizes message-splitting in order to allow for partial decoding of the interference at the non-intended receiver. Outer bounds are then derived and used to establish the optimality of the proposed scheme in certain cases. In the Gaussian case, the previously proposed cooperative jamming and noise-forwarding techniques are shown to be special cases of our proposed approach. Overall, our results provide structural insights on how the interference can be *exploited* to increase the secrecy capacity of wireless networks.

I. Introduction

Without the secrecy constraint, the interference channel has been investigated extensively in the literature. The best known achievable region was obtained in [2] and was recently simplified in [3]. However, except for some special cases (e.g., [4], [5], [6], [7], [8]), characterizing the capacity region of the two user Gaussian interference channel remains an open problem. On the other hand, recent attempts have shed light on the fundamental limits of the the interference channels with confidential messages [9], [10], [11], [12]. Nonetheless, the external eavesdropper scenario, considered here, has not been addressed adequately in the literature. In fact, to the best of our knowledge, the only relevant work is the recent study on the achievable secure degrees of freedom (DoF) of the K-user Gaussian interference channels under a frequency selective fading model [11], [12].

This work develops a general approach for cooperative binning and channel prefixing for the (discrete) two-user memoryless interference channels operated in the presence of a passive eavesdropper. The proposed scheme allows for cooperation in two distinct ways: 1) The two users jointly optimize their random binning technique [13] and 2)

This work is submitted to the IEEE Transactions on Information Theory.

The authors are with the Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH 43210, USA (e-mail: {koyluogo,helgamal}@ece.osu.edu). Hesham El Gamal also serves as the Director for the Wireless Intelligent Networks Center (WINC), Nile University, Cairo, Egypt.

The material in this work was presented in part at the IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Cannes, France in September 2008 [1].

They jointly introduce randomness in the transmitted signals, to confuse the eavesdropper, via a cooperative channel prefixing approach [14]. The proposed scheme also utilizes message-splitting and partial decoding to enlarge the achievable secrecy rate region [2]. We then derive outer bounds to the secrecy capacity region and use them to establish the optimality of the proposed scheme for some classes of channels. In addition, we argue that some coding techniques for the secure discrete multiple access channel and relay-eavesdropper channel can be obtained as special cases of our cooperative binning and channel prefixing approach.

Recently, noise forwarding (or jamming) has been shown to enhance on the achievable secrecy rate region of several Gaussian multi-user channels (e.g., [15] , [16]). The basic idea is to allow each transmitter to allocate only a fraction of the available power for its binning codebook and use the rest for the generation of independent noise samples. The superposition of the two signals is then transmitted. With the appropriate power allocation policy, one can ensure that the jamming signal results in maximal ambiguity at the eavesdropper while incuring only a minimal loss in the achievable rate at the legitimate receiver(s). Our work reveals the fact that this noise injection technique can be obtained as a manifestation of the cooperative channel prefixing approach. Based on this observation, we obtain a larger achievable region for the secrecy rate in the Gaussian multiple access channel.

The rest of the paper is organized as follows. Section II is devoted to the discrete memoryless scenario where the main results of the paper are derived and few special cases are analyzed. The analysis for the Gaussian channels, along with numerical results in selected scenarios, are given in Section III. Finally, we offer some concluding remarks in Section IV. The proofs are collected in the appendices to enhance the flow of the paper.

II. The Discrete Memoryless Channel

A. System Model and Notations

Throughout this paper, vectors are denoted as $\mathbf{x}^i = \{x(1), \cdots, x(i)\}$, where we omit the subscript i if $i = n$, i.e., $\mathbf{x} = \{x(1), \cdots, x(n)\}$. Random variables are denoted with capital letters X, which are defined over sets denoted by the calligraphic letters $\mathcal{X}$, and random vectors are denoted as bold-capital letters $\mathbf{X}^i$. Again, we drop the subscript i for $\mathbf{X} = \{X(1), \cdots, X(n)\}$. We define, $[x]^+ \triangleq \max\{0, x\}$, $\bar{\alpha} \triangleq 1 - \alpha$, and $\gamma(x) \triangleq \frac{1}{2}\log_2(1 + x)$. The delta function $\delta(x)$ is defined as $\delta(x) = 1$, if $x = 0$; $\delta(x) = 0$, if $x \neq 0$. Also, we use the following shorthand for probability distributions: $p(x) \triangleq p(X = x)$, $p(x|y) \triangleq p(X = x|Y = y)$. The same notation will be used for joint distributions. For any binning codebook, we construct 2^{nR} bins and 2^{nR^x} codewords per bin, where we refer to R as the secrecy rate and R^x as the randomization rate. Finally, for a given set $\mathcal{S}$, $R_{\mathcal{S}} \triangleq \sum\limits_{i\in\mathcal{S}} R_i$ for secrecy rates and $R^x_{\mathcal{S}} \triangleq \sum\limits_{i\in\mathcal{S}} R^x_i$ for the randomization rates.

Our discrete memoryless two-user interference channel with an (external) eavesdropper (IC-E) is denoted by

$$(\mathcal{X}_1 \times \mathcal{X}_2, p(y_1, y_2, y_e|x_1, x_2), \mathcal{Y}_1 \times \mathcal{Y}_2 \times \mathcal{Y}_e),$$

for some finite sets $\mathcal{X}_1, \mathcal{X}_2, \mathcal{Y}_1, \mathcal{Y}_2, \mathcal{Y}_e$ (see Fig. 1). Here the symbols $(x_1, x_2) \in \mathcal{X}_1 \times \mathcal{X}_2$ are the channel inputs and the symbols $(y_1, y_2, y_e) \in \mathcal{Y}_1 \times \mathcal{Y}_2 \times \mathcal{Y}_e$ are the channel outputs observed at the decoder 1, decoder 2, and at the eavesdropper, respectively. The channel is memoryless and time-invariant:

$$p(y_1(i), y_2(i), y_e(i)|\mathbf{x}_1^i, \mathbf{x}_2^i, \mathbf{y}_1^{i-1}, \mathbf{y}_2^{i-1}, \mathbf{y}_e^{i-1})$$
$$= p(y_1(i), y_2(i), y_e(i)|x_1(i), x_2(i)).$$

We assume that each transmitter $k \in \{1,2\}$ has a secret message W_k which is to be transmitted to the respective receiver in n channel uses and to be secured from the eavesdropper. In this setting, an $(n, M_1, M_2, P_{e,1}, P_{e,2})$ secret codebook has the following components:

1) The secret message set $\mathcal{W}_k = \{1, ..., M_k\}$; $k = 1, 2$.

2) A stochastic encoding function $f_k(.)$ at transmitter k which maps the secret messages to the transmitted symbols: $f_k : w_k \to \mathbf{X}_k$ for each $w_k \in \mathcal{W}_k$; $k = 1, 2$.

3) Decoding function $\phi_k(.)$ at receiver k which maps the received symbols to an estimate of the message: $\phi_k(\mathbf{Y}_k) = \hat{w}_k$; $k = 1, 2$.

The reliability of transmission is measured by the following probabilities of error

$$P_{e,k} = \frac{1}{M_1 M_2} \sum_{(w_1,w_2)\in\mathcal{W}_1\times\mathcal{W}_2} \text{Pr}\left\{\phi_k(\mathbf{Y}_k) \neq w_k|(w_1, w_2) \text{ is sent}\right\},$$

for $k = 1, 2$. The secrecy is measured by the equivocation rate

$$\frac{1}{n} H\left(W_1, W_2|\mathbf{Y}_e\right).$$

We say that the rate tuple (R_1, R_2) is achievable for the IC-E if, for any given $\epsilon > 0$, there exists an $(n, M_1, M_2, P_{e,1}, P_{e,2})$ secret codebook such that,

$$\begin{aligned} \frac{1}{n}\log(M_1) &= R_1 \\ \frac{1}{n}\log(M_2) &= R_2, \\ \max\{P_{e,1}, P_{e,2}\} &\leq \epsilon, \end{aligned}$$

and

$$R_1 + R_2 - \frac{1}{n} H\left(W_1, W_2|\mathbf{Y}_e\right) \quad \leq \quad \epsilon \tag{1}$$

for sufficiently large n. The secrecy capacity region is the closure of the set of all achievable rate pairs (R_1, R_2) and is denoted as $\mathbb{C}^{\text{IC-E}}$. Finally, we note that the secrecy requirement imposed on the full message set implies the secrecy of individual messages. In other words, $\frac{1}{n}I(W_1, W_2; \mathbf{Y}_e) \leq \epsilon$ implies $\frac{1}{n}I(W_k; \mathbf{Y}_e) \leq \epsilon$ for $k = 1, 2$.

B. Inner Bound

In this section, we introduce the cooperative binning and channel prefixing scheme, and derive an inner bound to $\mathbb{C}^{\text{IC-E}}$. The proposed strategy allows for cooperation in design of the binning codebooks, as well as in channel prefixing [14]. This way, each user will add only *a sufficient* amount of randomness as the other user will help to increase the randomness seen by the eavesdropper. The achievable secrecy rate region using this approach is stated in the following result.

Theorem 1:

$$\mathcal{R}^{\text{IC-E}} \triangleq \text{ the closure of } \left\{ \bigcup_{p\in\mathcal{P}} \mathcal{R}(p) \right\} \subset \mathbb{C}^{\text{IC-E}}, \tag{2}$$

where $\mathcal{P}$ denotes the set of all joint distributions of the random variables Q, C_1, S_1, O_1, C_2, S_2, O_2, X_1, X_2 that factors as [1]

$$\begin{aligned} p(q,c_1,s_1,o_1,c_2,s_2,o_2,x_1,x_2) &= p(q)p(c_1|q)p(s_1|q)p(o_1|q)p(c_2|q)p(s_2|q)p(o_2|q) \\ & \quad p(x_1|c_1,s_1,o_1)p(x_2|c_2,s_2,o_2), \end{aligned} \tag{3}$$

and $\mathcal{R}(p)$ is the closure of all (R_1,R_2) satisfying

$$\begin{aligned} R_1 &= R_{C_1}+R_{S_1}, \\ R_2 &= R_{C_2}+R_{S_2}, \\ (R_{C_1},R^x_{C_1},R_{S_1},R^x_{S_1},R_{C_2},R^x_{C_2},R^x_{O_2}) &\in \mathcal{R}_1(p), \\ (R_{C_2},R^x_{C_2},R_{S_2},R^x_{S_2},R_{C_1},R^x_{C_1},R^x_{O_1}) &\in \mathcal{R}_2(p), \\ (R^x_{C_1},R^x_{S_1},R^x_{O_1},R^x_{C_2},R^x_{S_2},R^x_{O_2}) &\in \mathcal{R}_e(p), \end{aligned}$$

and

$$\begin{aligned} & R_{C_1}\geq 0, R^x_{C_1}\geq 0, R_{S_1}\geq 0, R^x_{S_1}\geq 0, R^x_{O_1}\geq 0, \\ & R_{C_2}\geq 0, R^x_{C_2}\geq 0, R_{S_2}\geq 0, R^x_{S_2}\geq 0, R^x_{O_2}\geq 0, \end{aligned} \tag{4}$$

for a given joint distribution p. $\mathcal{R}_1(p)$ is the set of all tuples $(R_{C_1},R^x_{C_1},R_{S_1},R^x_{S_1},R_{C_2},R^x_{C_2},R^x_{O_2})$ satisfying

$$R_{\mathcal{S}}+R^x_{\mathcal{S}} \leq I(\mathcal{S};Y_1|\mathcal{S}^c,Q),\ \forall \mathcal{S}\subset\{C_1,S_1,C_2,O_2\}. \tag{5}$$

$\mathcal{R}_2(p)$ is the rate region defined by reversing the indices 1 and 2 everywhere in the expression for $\mathcal{R}_1(p)$. $\mathcal{R}_e(p)$ is the set of all tuples $(R^x_{C_1},R^x_{S_1},R^x_{O_1},R^x_{C_2},R^x_{S_2},R^x_{O_2})$ satisfying

$$\begin{aligned} R^x_{\mathcal{S}} &\leq I(\mathcal{S};Y_e|\mathcal{S}^c,Q),\ \forall \mathcal{S}\subsetneq\{C_1,S_1,O_1,C_2,S_2,O_2\}, \\ R^x_{\mathcal{S}} &= I(\mathcal{S};Y_e|Q),\ \mathcal{S}=\{C_1,S_1,O_1,C_2,S_2,O_2\}. \end{aligned} \tag{6}$$

Proof: Please refer to Appendix I. ■

The following remarks are now in order.

1) The auxiliary random variable Q serves as a time-sharing parameter.
2) The auxiliary variable C_1 is used to construct the *common* secure signal of transmitter 1 that has to be decoded at both receivers, where the random binning technique of [13] is used for this construction. Similarly, C_2 is used for the *common* secured signal of user 2.

[1] Here $Q, C_1, S_1, O_1, C_2, S_2,$ and O_2 are defined on arbitrary finite sets $\mathcal{Q}$, $\mathcal{C}_1$, $\mathcal{S}_1$, $\mathcal{O}_1$, $\mathcal{C}_2$, $\mathcal{S}_2$, and $\mathcal{O}_2$, respectively.

3) The auxiliary variable S_1 is used to construct the *self* secure signal that has to be decoded at receiver 1 but not at receiver 2, where the random binning technique of [13] is used for this construction. Similarly, S_2 is used for the *self* secure signal of user 2.
4) The auxiliary variable O_1 is used to construct the *other* signal of transmitter 1 that has to be decoded at receiver 2 but not at receiver 1 (conventional random coding [17] is used to construct this signal). Similarly, O_2 is used for the *other* signal of user 2. Note that we use $R_{O_1}^x$, $R_{O_2}^x$, and set $R_{O_1} = R_{O_2} = 0$.
5) Compared to the Han-Kobayashi scheme [2], the common and self random variables are constructed with random binning codebooks. This way, they are used not only for transmitting information, but also for adding randomness. Moreover, we have two additional random variables in this achievability scheme. These extra random variables, namely O_1 and O_2, are used to facilitate cooperation among the network users by adding extra randomness to the channel which has to be decoded by the non-intended receiver. We note that, compared to random variables C_k and S_k, the randomization added via O_k is considered as interference at the receiver k.
6) The gain that can be leveraged from cooperative binning can be attributed to the freedom in the allocation of randomization rates at the two users (e.g., see (6)). This allows the users to cooperatively add randomness to impair the eavesdropper with a minimal impact on the achievable rate at the legitimate receivers. Cooperative channel prefixing, on the other hand, can be achieved by the joint optimization of the probabilistic channel prefixes $p(x_1|c_1, s_1, o_1)$ and $p(x_2|c_2, s_2, o_2)$.

C. Outer Bounds

Theorem 2: For any $(R_1, R_2) \in \mathbb{C}^{\text{IC-E}}$,

$$R_1 \leq \max_{p \in \mathcal{P}_O} I(V_1; Y_1|V_2, U) - I(V_1; Y_e|U) \tag{7}$$

$$R_2 \leq \max_{p \in \mathcal{P}_O} I(V_2; Y_2|V_1, U) - I(V_2; Y_e|U), \tag{8}$$

where $\mathcal{P}_O$ is the set of joint distributions that factors as

$$p(u, v_1, v_2, x_1, x_2) = p(u)p(v_1|u)p(v_2|u)p(x_1|v_1)p(x_2|v_2).$$

Proof: Please refer to Appendix II. ■

Theorem 3: For channels satisfying

$$I(V_2; Y_2|V_1) \leq I(V_2; Y_1|V_1) \tag{9}$$

for any distribution that factors as $p(v_1, v_2, x_1, x_2) = p(v_1)p(v_2)p(x_1|v_1)p(x_2|v_2)$, an upper bound on the sum-rate of the IC-E is given by

$$R_1 + R_2 \leq \max_{p \in \mathcal{P}_O} I(V_1, V_2; Y_1|U) - I(V_1, V_2; Y_e|U), \tag{10}$$

where $\mathcal{P}_O$ is the set of joint distributions that factors as

$$p(u,v_1,v_2,x_1,x_2)=p(u)p(v_1|u)p(v_2|u)p(x_1|v_1)p(x_2|v_2).$$

Proof: Please refer to Appendix III. ■

The previous sum-rate upper bound also holds for the set of channels satisfying

$$I(V_2;Y_2)\leq I(V_2;Y_1) \tag{11}$$

for any distribution that factors as $p(v_1,v_2,x_1,x_2)=p(v_1)p(v_2)p(x_1|v_1)p(x_2|v_2)$. Finally, it is evident that one can obtain another upper bound by reversing the indices 1 and 2 in above expressions.

D. Special Cases

This section focuses on few special cases, where sharp results on the secrecy capacity region can be derived. In all these scenarios, achievability is established using the proposed cooperative binning and channel prefixing scheme. To simplify the presentation, we first define the following set of probability distributions. For random variables T_1 and T_2,

$$\mathcal{P}(T_1,T_2)\triangleq\big\{p(q,t_1,t_2,x_1,x_2)\,|\,p(q,t_1,t_2,x_1,x_2)=p(q)p(t_1|q)p(t_2|q)p(x_1|t_1)p(x_2|t_2)\big\}.$$

Corollary 4: If the IC-E satisfies

$$\begin{aligned}I(V_2;Y_2|V_1,Q)&\leq I(V_2;Y_e|Q)\\ I(V_2;Y_e|V_1,Q)&\leq I(V_2;Y_1|Q)\end{aligned} \tag{12}$$

for all input distributions that factors as $p(q)p(v_1|q)p(v_2|q)p(x_1|v_1)p(x_2|v_2)$, then its secrecy capacity region is given by

$$\mathbb{C}^{\text{IC-E}}=\text{ the closure of }\left\{\bigcup_{p\in\mathcal{P}(S_1,O_2)}\mathcal{R}_{S1}(p)\right\},$$

where $\mathcal{R}_{S1}(p)$ is the set of rate-tuples (R_1,R_2) satisfying

$$\begin{aligned}R_1&\leq[I(S_1;Y_1|O_2,Q)-I(S_1;Y_e|Q)]^+\\ R_2&=0,\end{aligned} \tag{13}$$

for any $p\in\mathcal{P}(S_1,O_2)$.

Proof: Please refer to Appendix IV. ■

Corollary 5: If the IC-E satisfies

$$\begin{aligned}I(V_2;Y_e|Q)\leq I(V_2;Y_1|Q)&\leq I(V_2;Y_2|Q)\\ I(V_1;Y_e|V_2,Q)&\leq I(V_1;Y_1|V_2,Q)\\ I(V_2;Y_2|V_1,Q)&\leq I(V_2;Y_1|V_1,Q)\end{aligned} \tag{14}$$

for all input distributions that factors as $p(q)p(v_1|q)p(v_2|q)p(x_1|v_1)p(x_2|v_2)$, then its secrecy sum capacity is given as follows.

$$\max_{(R_1,R_2)\in\mathcal{C}^{\text{IC-E}}} R_1+R_2 = \max_{p\in\mathcal{P}(S_1,C_2)} I(S_1,C_2;Y_1|Q)-I(S_1,C_2;Y_e|Q).$$

Proof: Please refer to Appendix V. ■

Corollary 6: If the IC-E satisfies

$$\begin{aligned} I(V_2;Y_e|Q)\le I(V_2;Y_1|V_1,Q) &\le I(V_2;Y_e|V_1,Q) \qquad (15)\\ I(V_2;Y_2|V_1,Q) &\le I(V_2;Y_1|V_1,Q)\end{aligned}$$

for all input distributions that factors as $p(q)p(v_1|q)p(v_2|q)p(x_1|v_1)p(x_2|v_2)$, then its secrecy sum capacity is given as follows.

$$\max_{(R_1,R_2)\in\mathcal{C}^{\text{IC-E}}} R_1+R_2 = \max_{p\in\mathcal{P}(S_1,O_2)} I(S_1,O_2;Y_1|Q)-I(S_1,O_2;Y_e|Q).$$

We also note that, in this case, O_2 will not increase the sum-rate, and hence, we can set $|\mathcal{O}_2|=1$

Proof: Please refer to Appendix VI. ■

Another case for which the cooperative binning and channel prefixing approach can attain the sum-capacity is the following.

Corollary 7: If the IC-E satisfies

$$\begin{aligned} I(V_2;Y_1|Q)\le I(V_2;Y_e|V_1,Q) &\le I(V_2;Y_1|V_1,Q) \qquad (16)\\ I(V_2;Y_2|V_1,Q) &\le I(V_2;Y_1|V_1,Q)\end{aligned}$$

for all input distributions that factors as $p(q)p(v_1|q)p(v_2|q)p(x_1|v_1)p(x_2|v_2)$, then its secrecy sum capacity is given as follows.

$$\max_{(R_1,R_2)\in\mathcal{C}^{\text{IC-E}}} R_1+R_2 = \max_{p\in\mathcal{P}(S_1,O_2)} I(S_1,O_2;Y_1|Q)-I(S_1,O_2;Y_e|Q).$$

Proof: Please refer to Appendix VII. ■

Now, we use our results on the IC-E to shed more light on the secrecy capacity of the discrete memoryless multiple access channel. In particular, it is easy to see that the multiple access channel with an eavesdropper (MAC-E) defined by $p(y_1,y_e|x_1,x_2)$ is equivalent to the IC-E defined by $p(y_1,y_2,y_e|x_1,x_2)=p(y_1,y_e|x_1,x_2)\delta(y_2-y_1)$. This allows for specializing the results obtained earlier to the MAC-E.

Corollary 8:

$$\mathcal{R}^{\text{MAC-E}} \triangleq \text{ the closure of} \left\{ \bigcup_{p\in\mathcal{P}(C_1,C_2)} \mathcal{R}(p) \right\},$$

where the channel is given by $p(y_1,y_e|x_1,x_2)\delta(y_2-y_1)$.

Furthermore, the following result characterizes the secrecy sum rate of the weak MAC-E.

Corollary 9 (MAC-E with a weak eavesdropper): If the eavesdropper is weak for the MAC-E, i.e.,

$$\begin{aligned} I(V_1;Y_e|V_2) &\le I(V_1;Y_1|V_2)\\ I(V_2;Y_e|V_1) &\le I(V_2;Y_1|V_1), \qquad (17)\end{aligned}$$

for all input distributions that factor as $p(v_1)p(v_2)p(x_1|v_1)p(x_2|v_2)$, then the secure sum-rate capacity is characterized as the following.

$$\max_{(R_1,R_2)\in\mathcal{C}^{\text{MAC-E}}} R_1+R_2 = \max_{p\in\mathcal{P}(C_1,C_2)} \{I(C_1,C_2;Y_1|Q) - I(C_1,C_2;Y_e|Q)\}$$

Proof: Please refer to Appendix VIII. ■

Another special case of our model is the relay-eavesdropper channel with a deaf helper. In this scenario, transmitter 1 has a secret message for receiver 1 and transmitter 2 is only interested in helping transmitter 1 in increasing its secure transmission rates. Here, the random variable O_2 at transmitter 2 is utilized to add randomness to the network. Again, the regions given earlier can be specialized to this scenario. For example, the following region is achievable for this relay-eavesdropper model.

$$\mathcal{R}^{\text{RE}} \triangleq \text{ the closure of the convex hull of } \left\{ \bigcup_{p\in\mathcal{P}(S_1,O_2,|\mathcal{Q}|=1)} \mathcal{R}(p) \right\},$$

where $\mathcal{P}(S_1,O_2,|\mathcal{Q}|=1)$ denotes the probability distributions in $\mathcal{P}(S_1,O_2)$ with a deterministic Q.

For this relay-eavesdropper scenario, the noise forwarding (NF) scheme proposed in [18] achieves the following rate.

$$R^{\text{[NF]}} = \max_{p\in\mathcal{P}(S_1,O_2,|\mathcal{Q}|=1)} R_1(p), \tag{18}$$

where $R_1(p) \triangleq [I(S_1;Y_1|O_2)+\min\{I(O_2;Y_1),I(O_2;Y_e|S_1)\}-\min\{I(O_2;Y_1),I(O_2;Y_e)\}-I(S_1;Y_e|O_2)]^+$. The following result shows that show that NF is a special case of the cooperative binning and channel prefixing scheme and provides a simplification of the achievable secrecy rate.

Corollary 10: $(R^{\text{[NF]}},0)\in\mathcal{R}^{\text{RE}}$, where $R^{\text{[NF]}}$ can be simplified as follows.

$$R^{\text{[NF]}} = \max_{p\in\mathcal{P}(S_1,O_2,|\mathcal{Q}|=1) \text{ s.t. } I(O_2;Y_e)\le I(O_2;Y_1)} I(S_1;Y_1|O_2)+\min\{I(O_2;Y_1),I(O_2;Y_e|S_1)\} - I(S_1,O_2;Y_e).$$

Proof: Please refer to Appendix IX. ■

Finally, the next result establishes the optimality of NF in certain relay-eavesdropper channels.

Corollary 11: Noise Forwarding scheme is optimal for the relay-eavesdropper channels which satisfy

$$I(V_2;Y_1)\le I(V_2;Y_e|V_1), \tag{19}$$

for all input distributions that factor as $p(v_1)p(v_2)p(x_1|v_1)p(x_2|v_2)$, and the corresponding secrecy capacity is

$$\mathcal{C}^{\text{RE}} = \max_{p\in\mathcal{P}(S_1,O_2,|\mathcal{Q}|=1) \text{ s.t. } I(O_2;Y_e)\le I(O_2;Y_1)} I(S_1,O_2;Y_1) - I(S_1,O_2;Y_e).$$

Proof: Please refer to Appendix X. ■

III. The Gaussian Channel

A. Inner Bound and Numerical Results

In its standard form [19], the two user Gaussian Interference Channel with an Eavesdropper (GIC-E) is given by

$$\begin{aligned} Y_1 &= X_1 + \sqrt{c_{21}} X_2 + N_1 \\ Y_2 &= \sqrt{c_{12}} X_1 + X_2 + N_2 \\ Y_e &= \sqrt{c_{1e}} X_1 + \sqrt{c_{2e}} X_2 + N_e, \end{aligned} \tag{20}$$

where $N_r \sim \mathcal{N}(0,1)$ is the noise at each receiver $r = 1, 2, e$ and the average power constraints are $\frac{1}{n} \sum_{t=1}^{n} (X_k(t))^2 \leq P_k$ for $k = 1, 2$. The secrecy capacity region of the GIC-E is denoted as $\mathbb{C}^{\text{GIC-E}}$.

The goal here is to specialize the results obtained in the previous section to the Gaussian scenario and illustrate the gains that can be leveraged from cooperative binning and channel prefixing, and time sharing. Towards this end, we will need the following definitions. Consider a probability mass function on the time sharing parameter denoted by $p(q)$. Let $\mathcal{A}(p(q))$ denote the set of all possible power allocations, i.e.,

$$\begin{aligned} \mathcal{A}(p(q)) \;\triangleq\; &\Big\{ \Big(P_1^c(q), P_1^s(q), P_1^o(q), P_2^c(q), P_2^s(q), P_2^o(q), P_1^j(q), P_2^j(q) \Big) \,| \\ &\sum_{q \in \mathcal{Q}} (P_k^c(q) + P_k^s(q) + P_k^o(q) + P_k^j(q)) p(q) \leq P_k, \text{ for } k = 1, 2. \Big\} \end{aligned} \tag{21}$$

Now, we define a set of joint distributions $\mathcal{P}_G$ for the Gaussian case as follows.

$$\begin{aligned} \mathcal{P}_G \;\triangleq\; &\Big\{ p \,|\, p \in \mathcal{P}, (P_1^c(q), P_1^s(q), P_1^o(q), P_2^c(q), P_2^s(q), P_2^o(q), P_1^j(q), P_2^j(q)) \in \mathcal{A}(p(q)), \\ &C_1(q) \sim \mathcal{N}(0, P_1^c(q)), S_1(q) \sim \mathcal{N}(0, P_1^s(q)), O_1(q) \sim \mathcal{N}(0, P_1^o(q)), \\ &C_2(q) \sim \mathcal{N}(0, P_2^c(q)), S_2(q) \sim \mathcal{N}(0, P_2^s(q)), O_2(q) \sim \mathcal{N}(0, P_2^o(q)), \\ &J_1(q) \sim \mathcal{N}(0, P_1^j(q)), J_2(q) \sim \mathcal{N}(0, P_2^j(q)), \\ &X_1(q) = C_1(q) + S_1(q) + O_1(q) + J_1(q), X_2(q) = C_2(q) + S_2(q) + O_2(q) + J_2(q) \Big\}, \end{aligned}$$

where the Gaussian model given in (20) gives $p(y_1, y_2, y_e | x_1, x_2)$. Using this set of distributions, we obtain the following achievable secrecy rate region for the GIC-E.

Corollary 12: $\mathcal{R}^{\text{GIC-E}} \triangleq$ the closure of $\left\{ \bigcup_{p \in \mathcal{P}_G} \mathcal{R}(p) \right\} \subset \mathbb{C}^{\text{GIC-E}}$.

It is interesting to see that our particular choice of the channel prefixing distribution $p(x_k | c_k, s_k, o_k)$ in the above corollary corresponds to a superposition coding approach where $X_k = C_k + S_k + O_k + J_k$. This observation establishes the fact that noise injection scheme of [15] and jamming scheme of [16] are **special cases** of the channel prefixing technique of [14].

The following computationally simple subregion will be used to generate some of our numerical results.

Corollary 13: $\mathcal{R}_2^{\text{GIC-E}} \triangleq$ the convex closure of $\left\{ \bigcup_{p \in \mathcal{P}_{G2}} \mathcal{R}(p) \right\} \subset \mathcal{R}^{\text{GIC-E}} \subset \mathbb{C}^{\text{GIC-E}}$, where

$$\mathcal{P}_{G2} \triangleq \{ p \,|\, p \in \mathcal{P}_G, |\mathcal{Q}| = 1, P_1^s(q) = P_1^o(q) = P_2^s(q) = P_2^o(q) = 0 \text{ for any } Q = q \}.$$

Another simplification can be obtained from the following TDMA-like approach. Here we divide the n channel uses into two parts of lengths represented by αn and $(1-\alpha)n$, where $0 \leq \alpha \leq 1$ and αn is assumed to be an integer. During the first period, transmitter 1 generates binning codewords using power $P_1^s(1)$ and transmitter 2 jams the channel using power $P_2^j(1)$. For the second period, the roles of the users are reversed, where the users use powers $P_2^s(2)$ and $P_1^j(2)$. We refer to this scheme cooperative TDMA (C-TDMA) which achieves the following region.

Corollary 14: $\mathcal{R}_{\text{C-TDMA}} \subset \mathcal{R}^{\text{GIC-E}} \subset \mathbb{C}^{\text{GIC-E}}$, where

$$\mathcal{R}_{\text{C-TDMA}} \triangleq \text{ the closure of } \left\{ \bigcup_{\substack{\alpha\in[0,1] \\ \alpha P_1^s(1)+(1-\alpha)P_1^j(2)\leq P_1 \\ \alpha P_2^j(1)+(1-\alpha)P_2^s(2)\leq P_2}} (R_1, R_2) \right\},$$

where

$$R_1 = \frac{\alpha}{2}\left[\log\left(1+\frac{P_1^s(1)}{1+c_{21}P_2^j(1)}\right) - \log\left(1+\frac{c_{1e}P_1^s(1)}{1+c_{2e}P_2^j(1)}\right)\right]^+,$$

and

$$R_2 = \frac{(1-\alpha)}{2}\left[\log\left(1+\frac{P_2^s(2)}{1+c_{12}P_1^j(2)}\right) - \log\left(1+\frac{c_{2e}P_2^s(2)}{1+c_{1e}P_1^j(2)}\right)\right]^+.$$

Proof: This is a subregion of the $\mathbb{C}^{\text{GIC-E}}$, where we use a time sharing random variable satisfying $p(q=1)=\alpha$ and $p(q=2)=1-\alpha$, and utilize the random variables S_1 and S_2. The proof also follows by respective single-user Gaussian wiretap channel result [20] with the modified noise variances due to the jamming signals. ■

In the C-TDMA scheme above, we only add randomness by noise injection at the *helper* node. However, our cooperative binning and channel prefixing scheme (Corollary 12) allows for the implementation of more general *cooperation* strategies. For example, in a more general TDMA approach, each user can help the other via both binning and channel prefixing (i.e., the noise forwarding scheme described in Section III-B.2). In addition, one can develop enhanced transmission strategies with a time-sharing random variable of cardinality greater than 2.

We now provide numerical results for the following subregions of the achievable region given in Corollary 12.

- $\mathcal{R}_2^{\text{GIC-E}}$: Here we utilize both cooperative binning and channel prefixing.
- $\mathcal{R}_2^{\text{GIC-E}}$(b or cp): Here we utilize either cooperative binning (b) or channel prefixing (cp) scheme at a transmitter, but not both.
- $\mathcal{R}_2^{\text{GIC-E}}$(ncp): Here we only utilize cooperative binning, no channel prefixing (ncp) is implemented.
- $\mathcal{R}_{\text{C-TDMA}}$: This region is an example of utilizing both time-sharing and cooperative channel prefixing.
- $\mathcal{R}_{\text{C-TDMA}}$(ncp): This region is a subregion of $\mathcal{R}_{\text{C-TDMA}}$, for which we set the jamming powers to zero.

The first scenario depicted in Fig. 3 shows the gain offered by the cooperative binning technique, as compared with the various cooperative TDMA approaches. Also, it is shown that cooperative channel prefixing does not increase the secrecy rate region in this particular scenario. In Fig. 4, we consider a channel with a rather capable eavesdropper. In this case, it is straightforward to verify that the corresponding single user channels have zero secrecy capacities.

However, with the appropriate cooperation strategies between the two **interfering users**, the two users can achieve non-zero rates (as reported in the figure). In Fig. 5, we consider an asymmetric scenario, in which the first user has a weak channel to the eavesdropper, but the second user has a strong channel to the eavesdropper. In this case, the proposed cooperative binning technique allows the second user to achieve a positive secure transmission rate, which is not possible by exploiting only the channel prefixing and time-sharing techniques. In addition, by prefixing the channel, the second user can help the first one to increase its secure transmission rate. Finally, we note that for some channel coefficients $\mathcal{R}_{\text{C-TDMA}}$ outperforms $\mathcal{R}_2^{\text{GIC-E}}$ and for some others $\mathcal{R}_2^{\text{GIC-E}}$ outperforms $\mathcal{R}_{\text{C-TDMA}}$. Therefore, in general, the proposed techniques (cooperative binning, cooperative channel prefixing, and time-sharing) should be exploited simultaneously as considered in Corollary 12.

B. Special Cases

1) The Multiple Access Channel: First, we define a set of probability distributions

$$\mathcal{P}_{G3} \triangleq \left\{ p \,|\, p \in \mathcal{P}_G, P_1^s(q) = P_1^o(q) = P_2^s(q) = P_2^o(q) = 0 \text{ for any } Q = q \right\}. \tag{22}$$

Using this notation, one can easily see that the region $\mathcal{R}^{\text{GIC-E}}$ in Corollary 12 reduces to the following achievable secrecy rate region for the Gaussian Multiple Access Channel with an Eavesdropper (GMAC-E).

$$\mathcal{R}^{\text{GMAC-E}} \triangleq \text{ the closure of } \left\{ \bigcup_{p \in \mathcal{P}_{G3}} \mathcal{R}(p) \right\},$$

where the expressions in the region $\mathcal{R}(p)$ are calculated for the channel given by $p(y_1, y_e|x_1, x_2)\delta(y_2 - y_1)$.

The region $\mathcal{R}^{\text{GMAC-E}}$ generalizes the one obtained in [16] for the two user case [2]. The underlying reason is that, in the achievable scheme of [16], the users are either transmitting their codewords or jamming the channel whereas, in our approach, the users can transmit their codewords and jam the channel simultaneously. In addition, our cooperative TDMA approach generalizes the one proposed in [16], as we allow the two users to cooperate in the design of binning codebooks and channel prefixing during the time slots dedicated to either one.

2) The Relay-Eavesdropper Channel: In the previous section, we argued that the noise forwarding (NF) scheme of [18] can be obtained as a special case of our generalized cooperation scheme. Here, we demonstrate the positive impact of channel prefixing on increasing the achievable secrecy rate of the Gaussian relay-eavesdropper channel. In particular, the proposed region for the Gaussian IC-E, when specialized to the Gaussian relay-eavesdropper setting, results in

$$\mathcal{R}^{\text{GRE}} \triangleq \text{ closure of the convex hull of } \left\{ \bigcup_{p \in \mathcal{P}_{G4}} \mathcal{R}(p) \right\},$$

where

$$\mathcal{P}_{G4} \triangleq \left\{ p \,|\, p \in \mathcal{P}_G, |\mathcal{Q}| = 1, P_1^c(q) = P_1^o(q) = P_2^c(q) = P_2^s(q) = 0 \right\}. \tag{23}$$

[2] It is important to note that we have used the binning codebook construction here, whereas in [16] the authors claimed that the same region is achievable with the superposition coding approach.

One the other hand, noise forwarding with no channel prefixing (GNF-ncp) results in the following achievable rate.

$$\begin{aligned} R^{\text{[GNF-ncp]}} &= \left[\frac{1}{2}\log\left(1+P_1\right)+\min\left\{\frac{1}{2}\log\left(1+\frac{c_{21}P_2}{1+P_1}\right),\frac{1}{2}\log\left(1+c_{2e}P_2\right)\right\}\right. \\ &\quad \left. -\min\left\{\frac{1}{2}\log\left(1+\frac{c_{21}P_2}{1+P_1}\right),\frac{1}{2}\log\left(1+\frac{c_{2e}P_2}{1+c_{1e}P_1}\right)\right\}-\frac{1}{2}\log\left(1+c_{1e}P_1\right)\right]^+, \end{aligned} \tag{24}$$

where we choose $X_1 = S_1 \sim \mathcal{N}(0, P_1)$ and $X_2 = O_2 \sim \mathcal{N}(0, P_2)$ in the expression of $R^{\text{[NF]}}$ (see also [18]).

Numerically, the positive impact of channel prefixing is illustrated in the following example. First, it is easy to see that the following secrecy rate is achievable with channel prefixing

$$R_1 = \left[\frac{1}{2}\log\left(1+\frac{P_1}{1+c_{21}P_2}\right)-\frac{1}{2}\log\left(1+\frac{c_{1e}P_1}{1+c_{2e}P_2}\right)\right]^+, \tag{25}$$

since $(R_1, 0) \in \mathcal{R}^{\text{GRE}}$ (i.e., we set $P_1^s = P_1$ and $P_2^j = P_2$). Now, we let $c_{1e} = c_{2e} = 1$ and $P_1 = P_2 = 1$, resulting in $R^{\text{[GNF-ncp]}} = 0$ and $R_1 > 0$ if $c_{21} < 1$.

IV. Conclusions

This work considered the two-user interference channel with an (external) eavesdropper. An inner bound on the achievable secrecy rate region was derived using a scheme that combines random binning, channel prefixing, message splitting, and time-sharing techniques. More specifically, our achievable scheme allows the two users to cooperatively construct their binning codebooks and channel prefixing distributions. Outer bounds are then derived and used to establish the optimality of the proposed scheme in some special cases. For the Gaussian scenario, channel prefixing was used to allow the users to transmit independently generated noise samples using a fraction of the available power. Moreover, as a special case of time sharing, we have developed a novel cooperative TDMA scheme, where a user can add *structured and unstructured* noise to the channel during the allocated slot for the other user. It is shown that this scheme reduces to the noise forwarding scheme proposed earlier for the relay-eavesdropper channel. In the Gaussian multiple-access setting, our cooperative binning and channel prefixing scheme was shown to enlarge the achievable regions obtained in previous works. The most interesting aspect of our results is, perhaps, the illumination of the role of interference in cooperatively adding randomness to increase the achievable secrecy rates in multi-user networks.

Appendix I
Proof of Theorem 1

Fix some $p(q)$, $p(c_1|q)$, $p(s_1|q)$, $p(o_1|q)$, $p(x_1|c_1, s_1, o_1)$, $p(c_2|q)$, $p(s_2|q)$, $p(o_2|q)$, and $p(x_2|c_2, s_2, o_2)$ for the channel given by $p(y_1, y_2, y_e|x_1, x_2)$. Generate a random typical sequence $\mathbf{q}^n$, where $p(\mathbf{q}^n) = \prod_{i=1}^{n} p(q(i))$ and each entry is chosen i.i.d. according to $p(q)$. Every node knows the sequence $\mathbf{q}^n$.

Codebook Generation:

Consider transmitter $k \in \{1, 2\}$ that has secret message $W_k \in \mathcal{W}_k = \{1, 2, \cdots, M_k\}$, where $M_k = 2^{nR_k}$. We construct each element in the codebook ensemble as follows.

- Generate $M_{C_k} M_{C_k}^x = 2^{n(R_{C_k} + R_{C_k}^x - \epsilon_1)}$ sequences $\mathbf{c}_k^n$, each with probability $p(\mathbf{c}_k^n | \mathbf{q}^n) = \prod_{i=1}^{n} p(c_k(i)|q(i))$, where $p(c_k(i)|q(i)) = p(c_k|q)$ for each i. Distribute these into $M_{C_k} = 2^{nR_{C_k}}$ bins, where the bin index is w_{C_k}. Each bin has $M_{C_k}^x = 2^{n(R_{C_k}^x - \epsilon_1)}$ codewords, where we denote the codeword index as $w_{C_k}^x$. Represent each codeword with these two indices, i.e., $\mathbf{c}_k^n(w_{C_k}, w_{C_k}^x)$.
- Similarly, generate $M_{S_k} M_{S_k}^x = 2^{n(R_{S_k} + R_{S_k}^x - \epsilon_1)}$ sequences $\mathbf{s}_k^n$, each with probability $p(\mathbf{s}_k^n | \mathbf{q}^n) = \prod_{i=1}^{n} p(s_k(i)|q(i))$, where $p(s_k(i)|q(i)) = p(s_k|q)$ for each i. Distribute these into $M_{S_k} = 2^{nR_{S_k}}$ bins, where the bin index is w_{S_k}. Each bin has $M_{S_k}^x = 2^{n(R_{S_k}^x - \epsilon_1)}$ codewords, where we denote the codeword index as $w_{S_k}^x$. Represent each codeword with these two indices, i.e., $\mathbf{s}_k^n(w_{S_k}, w_{S_k}^x)$.
- Finally, generate $M_{O_k}^x = 2^{n(R_{O_k}^x - \epsilon_1)}$ sequences $\mathbf{o}_k^n$, each with probability $p(\mathbf{o}_k^n | \mathbf{q}^n) = \prod_{i=1}^{n} p(o_k(i)|q(i))$, where $p(o_k(i)|q(i)) = p(o_k|q)$ for each i. Denote each sequence by index $w_{O_k}^x$ and represent each codeword with this index, i.e., $\mathbf{o}_k^n(w_{O_k}^x)$.

Choose $M_k = M_{C_k} M_{S_k}$, and assign each pair (w_{C_k}, w_{S_k}) to a secret message w_k. Note that, $R_k = R_{C_k} + R_{S_k}$ for $k = 1, 2$.

Every node in the network knows these codebooks.

Encoding:

Consider again user $k \in \{1, 2\}$. To send $w_k \in \mathcal{W}_k$, user k gets corresponding indices w_{C_k} and w_{S_k}. Then user k obtains the following codewords:

- From the codebook for C_k, user k randomly chooses a codeword in bin w_{C_k} according to the uniform distribution, where the codeword index is denoted by $w_{C_k}^x$ and it gets the corresponding entry of the codebook, i.e. $\mathbf{c}_k^n(w_{C_k}, w_{C_k}^x)$.
- Similarly, from the codebook for S_k, user k randomly chooses a codeword in bin w_{S_k} according to the uniform distribution, where the codeword index is denoted by $w_{S_k}^x$ and it gets the corresponding entry of the codebook, i.e. $\mathbf{s}_k^n(w_{S_k}, w_{S_k}^x)$.
- Finally, from the codebook for O_k, it randomly chooses a codeword, which is denoted by $\mathbf{o}_k^n(w_{O_k}^x)$.

Then, user k, generates the channel inputs $\mathbf{x}_k^n$, where each entry is chosen according to $p(x_k|c_k, s_k, o_k)$ using the codewords $\mathbf{c}_k^n(w_{C_k}, w_{C_k}^x)$, $\mathbf{s}_k^n(w_{S_k}, w_{S_k}^x)$, and $\mathbf{o}_k^n(w_{O_k}^x)$; and it transmits the constructed $\mathbf{x}_k^n$ in n channel uses. See Fig. 2.

Decoding:

Here we remark that although each user needs to decode only its own message, we also require receivers to decode common and other information of the other transmitter. Suppose receiver 1 has received $\mathbf{y}_1^n$. Let $A_{1,\epsilon}^n$ denote the set of typical $(\mathbf{q}^n, \mathbf{c}_1^n, \mathbf{s}_1^n, \mathbf{c}_2^n, \mathbf{o}_2^n, \mathbf{y}_1^n)$ sequences. Decoder 1 chooses $(w_{C_1}, w_{C_1}^x, w_{S_1}, w_{S_1}^x, w_{C_2}, w_{C_2}^x, w_{O_2}^x)$ s.t.

$$(\mathbf{q}^n, \mathbf{c}_1^n(w_{C_1}, w_{C_1}^x), \mathbf{s}_1^n(w_{S_1}, w_{S_1}^x), \mathbf{c}_2^n(w_{C_2}, w_{C_2}^x), \mathbf{o}_2^n(w_{O_2}^x), \mathbf{y}_1^n) \in A_{1,\epsilon}^n,$$

if such a tuple exists and is unique. Otherwise, the decoder declares an error. Decoding at receiver 2 is symmetric and a description of it can be obtained by reversing the indices 1 and 2 above.

Probability of Error Analysis:

Below we show that the decoding error probability of user k averaged over the ensemble can be arbitrarily made small for sufficiently large n. This demonstrates the existence of a codebook with the property that $\max(P_{e,1}, P_{e,2}) \leq \epsilon$, for any given $\epsilon > 0$. The analysis follows from similar arguments given in [2]. See also [17] for joint typical decoding error computations. Here, for any given $\epsilon > 0$, each receiver can decode corresponding messages given above with an error probability less than ϵ as $n \to \infty$, if the rates satisfy the following equations.

$$R_{\mathcal{S}} + R_{\mathcal{S}}^x \leq I(\mathcal{S}; Y_1 | \mathcal{S}^c, Q), \;\; \forall \mathcal{S} \subset \{C_1, S_1, C_2, O_2\}, \tag{26}$$

$$R_{\mathcal{S}} + R_{\mathcal{S}}^x \leq I(\mathcal{S}; Y_2 | \mathcal{S}^c, Q), \;\; \forall \mathcal{S} \subset \{C_1, O_1, C_2, S_2\}. \tag{27}$$

Equivocation Computation:

We first write the following.

$$\begin{aligned}
H(W_1, W_2 | \mathbf{Y}_e) &= H(W_{C_1}, W_{S_1}, W_{C_2}, W_{S_2} | \mathbf{Y}_e) && (28)\\
&\geq H(W_{C_1}, W_{S_1}, W_{C_2}, W_{S_2} | \mathbf{Y}_e, \mathbf{Q}) && (29)\\
&= H(W_{C_1}, W_{S_1}, W_{C_2}, W_{S_2}, \mathbf{Y}_e | \mathbf{Q}) - H(\mathbf{Y}_e | \mathbf{Q}) && (30)\\
&= H(\mathbf{C}_1, \mathbf{S}_1, \mathbf{O}_1, \mathbf{C}_2, \mathbf{S}_2, \mathbf{O}_2 | \mathbf{Q}) + H(W_{C_1}, W_{S_1}, W_{C_2}, W_{S_2}, \mathbf{Y}_e | \mathbf{C}_1, \mathbf{S}_1, \mathbf{O}_1, \mathbf{C}_2, \mathbf{S}_2, \mathbf{O}_2, \mathbf{Q})\\
&\quad - H(\mathbf{C}_1, \mathbf{S}_1, \mathbf{O}_1, \mathbf{C}_2, \mathbf{S}_2, \mathbf{O}_2 | W_{C_1}, W_{S_1}, W_{C_2}, W_{S_2}, \mathbf{Y}_e, \mathbf{Q}) - H(\mathbf{Y}_e | \mathbf{Q}) && (31)\\
&\geq H(\mathbf{C}_1, \mathbf{S}_1, \mathbf{O}_1, \mathbf{C}_2, \mathbf{S}_2, \mathbf{O}_2 | \mathbf{Q}) + H(\mathbf{Y}_e | \mathbf{C}_1, \mathbf{S}_1, \mathbf{O}_1, \mathbf{C}_2, \mathbf{S}_2, \mathbf{O}_2, \mathbf{Q})\\
&\quad - H(\mathbf{C}_1, \mathbf{S}_1, \mathbf{O}_1, \mathbf{C}_2, \mathbf{S}_2, \mathbf{O}_2 | W_{C_1}, W_{S_1}, W_{C_2}, W_{S_2}, \mathbf{Y}_e, \mathbf{Q}) - H(\mathbf{Y}_e | \mathbf{Q}) && (32)\\
&= H(\mathbf{C}_1, \mathbf{S}_1, \mathbf{O}_1, \mathbf{C}_2, \mathbf{S}_2, \mathbf{O}_2 | \mathbf{Q}) - I(\mathbf{C}_1, \mathbf{S}_1, \mathbf{O}_1, \mathbf{C}_2, \mathbf{S}_2, \mathbf{O}_2; \mathbf{Y}_e | \mathbf{Q})\\
&\quad - H(\mathbf{C}_1, \mathbf{S}_1, \mathbf{O}_1, \mathbf{C}_2, \mathbf{S}_2, \mathbf{O}_2 | W_{C_1}, W_{S_1}, W_{C_2}, W_{S_2}, \mathbf{Y}_e, \mathbf{Q}), && (33)
\end{aligned}$$

where inequalities are due to the fact that conditioning does not increase entropy.

Here,

$$H(\mathbf{C}_1, \mathbf{S}_1, \mathbf{O}_1, \mathbf{C}_2, \mathbf{S}_2, \mathbf{O}_2 | \mathbf{Q}) = n(R_{C_1} + R_{C_1}^x + R_{S_1} + R_{S_1}^x + R_{O_1}^x + R_{C_2} + R_{C_2}^x + R_{S_2} + R_{S_2}^x + R_{O_2}^x - 6\epsilon_1), \tag{34}$$

as, given $\mathbf{Q} = \mathbf{q}$, the tuple $(\mathbf{C}_1, \mathbf{S}_1, \mathbf{O}_1, \mathbf{C}_2, \mathbf{S}_2, \mathbf{O}_2)$ has $2^{n(R_{C_1} + R_{C_1}^x + R_{S_1} + R_{S_1}^x + R_{O_1}^x + R_{C_2} + R_{C_2}^x + R_{S_2} + R_{S_2}^x + R_{O_2}^x - 6\epsilon_1)}$ possible values each with equal probability.

Secondly,

$$I(\mathbf{C}_1, \mathbf{S}_1, \mathbf{O}_1, \mathbf{C}_2, \mathbf{S}_2, \mathbf{O}_2; \mathbf{Y}_e | \mathbf{Q}) \leq nI(C_1, S_1, O_1, C_2, S_2, O_2; Y_e | Q) + n\epsilon_2, \tag{35}$$

where $\epsilon_2 \to 0$ as $n \to \infty$. See, for example, Lemma 8 of [13].

Lastly, for any $W_{C_1} = w_{C_1}$, $W_{S_1} = w_{S_1}$, $W_{C_2} = w_{C_2}$, $W_{S_2} = w_{S_2}$, and $\mathbf{Q} = \mathbf{q}$, we have

$$H(\mathbf{C}_1, \mathbf{S}_1, \mathbf{O}_1, \mathbf{C}_2, \mathbf{S}_2, \mathbf{O}_2 | W_{C_1} = w_{C_1}, W_{S_1} = w_{S_1}, W_{C_2} = w_{C_2}, W_{S_2} = w_{S_2}, \mathbf{Y}_e, \mathbf{Q} = \mathbf{q}) \leq n\epsilon_3, \tag{36}$$

for some $\epsilon_3 \to 0$ as $n \to \infty$. This is due to the Fano's inequality together with the binning codebook construction: Given all the bin indices of two users, eavesdropper can decode the randomization indices among those bins. Due to joint typicality, this latter argument holds as long as the rates satisfy the following equations.

$$R_{\mathcal{S}}^x \quad \leq \quad I(\mathcal{S}; Y_e|\mathcal{S}^c, Q), \;\; \forall \mathcal{S} \subset \{C_1, S_1, O_1, C_2, S_2, O_2\}. \tag{37}$$

This follows as given bin indices W_{C_1}, W_{S_1}, W_{C_2}, and W_{S_2}, this reduces to MAC probability of error computation among the codewords of those bins. See [17] for details of computing error probabilities in MAC. Then, averaging over W_{C_1}, W_{S_1}, W_{C_2}, W_{S_2}, and $\mathbf{Q}$, we obtain

$$H(\mathbf{C}_1, \mathbf{S}_1, \mathbf{O}_1, \mathbf{C}_2, \mathbf{S}_2, \mathbf{O}_2|W_{C_1}, W_{S_1}, W_{C_2}, W_{S_2}, \mathbf{Y}_e, \mathbf{Q}) \leq n\epsilon_3. \tag{38}$$

Hence, using (34), (35), and (38) in (28) we obtain

$$R_1 + R_2 - \frac{1}{n} H(W_1, W_2|Y_e^n) \leq 6\epsilon_1 + \epsilon_2 + \epsilon_3 \triangleq \epsilon \to 0, \tag{39}$$

as $n \to \infty$, where we set

$$R_{\mathcal{S}}^x = I(\mathcal{S}; Y_e|Q), \; \mathcal{S} = \{C_1, S_1, O_1, C_2, S_2, O_2\}. \tag{40}$$

Combining (26), (27), (37), and (40) we obtain the result, i.e., $\mathcal{R}(p)$ is achievable for any $p \in \mathcal{P}$.

APPENDIX II
PROOF OF THEOREM 2

We bound R_1 below. The bound on R_2 can be obtained by following similar steps below and reversing the indices 1 and 2. We first state the following definitions. For any random variable Y, $\tilde{\mathbf{Y}}^{i+1} \triangleq [Y(i+1) \cdots Y(n)]$, and

$$I_1 \quad \triangleq \quad \sum_{i=1}^{n} I(\tilde{\mathbf{Y}}_e^{i+1}; Y_1(i)|\mathbf{Y}_1^{i-1}) \tag{41}$$

$$\hat{I}_1 \quad \triangleq \quad \sum_{i=1}^{n} I(\mathbf{Y}_1^{i-1}; Y_e(i)|\tilde{\mathbf{Y}}_e^{i+1}) \tag{42}$$

$$I_2 \quad \triangleq \quad \sum_{i=1}^{n} I(\tilde{\mathbf{Y}}_e^{i+1}; Y_1(i)|\mathbf{Y}_1^{i-1}, W_1) \tag{43}$$

$$\hat{I}_2 \quad \triangleq \quad \sum_{i=1}^{n} I(\mathbf{Y}_1^{i-1}; Y_e(i)|\tilde{\mathbf{Y}}_e^{i+1}, W_1) \tag{44}$$

Then, we consider the following bound.

$$\begin{aligned}
R_1-\epsilon &\leq \frac{1}{n}H(W_1|\mathbf{Y}_e)\\
&= \frac{1}{n}\left(H(W_1)-I(W_1;\mathbf{Y}_e)\right)\\
&= \frac{1}{n}\left(H(W_1|\mathbf{Y}_1)+I(W_1;\mathbf{Y}_1)-I(W_1;\mathbf{Y}_e)\right)\\
&\leq \epsilon_1+\frac{1}{n}\left(\sum_{i=1}^{n}I(W_1;Y_1(i)|\mathbf{Y}_1^{i-1})-\sum_{i=1}^{n}I(W_1;Y_e(i)|\tilde{\mathbf{Y}}_e^{i+1})\right)\\
&= \epsilon_1+\frac{1}{n}\Bigg(\sum_{i=1}^{n}I(W_1;Y_1(i)|\mathbf{Y}_1^{i-1},\tilde{\mathbf{Y}}_e^{i+1})+I_1-I_2\\
&\quad -\sum_{i=1}^{n}I(W_1;Y_e(i)|\mathbf{Y}_1^{i-1},\tilde{\mathbf{Y}}_e^{i+1})-\hat{I}_1+\hat{I}_2\Bigg)\\
&= \epsilon_1+\frac{1}{n}\left(\sum_{i=1}^{n}I(W_1;Y_1(i)|\mathbf{Y}_1^{i-1},\tilde{\mathbf{Y}}_e^{i+1})-\sum_{i=1}^{n}I(W_1;Y_e(i)|\mathbf{Y}_1^{i-1},\tilde{\mathbf{Y}}_e^{i+1})\right), \qquad (45)
\end{aligned}$$

where the first inequality is due to Lemma 15 given at the end of this section, the second inequality is due to the Fano's inequality at the receiver 1 with some $\epsilon_1 \to 0$ as $n \to \infty$, the last equality is due to observations $I_1 = \hat{I}_1$ and $I_2 = \hat{I}_2$ (see [14, Lemma 7]).

We define $U(i) \triangleq (\mathbf{Y}_1^{i-1}, \tilde{\mathbf{Y}}_e^{i+1}, i)$, $V_1(i) \triangleq (U(i), W_1)$, and $V_2(i) \triangleq (U(i), W_2)$. Using standard techniques (see, e.g., [17]), we introduce a random variable J, which is uniformly distributed over $\{1, \cdots, n\}$, and continue as below.

$$\begin{aligned}
R_1-\epsilon &\leq \epsilon_1+\frac{1}{n}\left(\sum_{i=1}^{n}I(W_1;Y_1(i)|\mathbf{Y}_1^{i-1},\tilde{\mathbf{Y}}_e^{i+1})-\sum_{i=1}^{n}I(W_1;Y_e(i)|\mathbf{Y}_1^{i-1},\tilde{\mathbf{Y}}_e^{i+1})\right)\\
&= \epsilon_1+\frac{1}{n}\left(\sum_{i=1}^{n}I(V_1(i);Y_1(i)|U(i))-\sum_{i=1}^{n}I(V_1(i);Y_e(i)|U(i))\right)\\
&= \epsilon_1+\sum_{j=1}^{n}I(V_1(j);Y_1(j)|U(j))p(J=j)-\sum_{j=1}^{n}I(V_1(j);Y_e(j)|U(j))p(J=j)\\
&\leq \epsilon_1+\sum_{j=1}^{n}I(V_1(j);Y_1(j)|V_2(j),U(j))p(J=j)-\sum_{j=1}^{n}I(V_1(j);Y_e(j)|U(j))p(J=j)\\
&= \epsilon_1+I(V_1;Y_1|V_2,U)-I(V_1;Y_e|U), \qquad (46)
\end{aligned}$$

where the last inequality follows from the fact that $V_1(j) \to U(j) \to V_2(j)$, which implies $I(V_1(j); Y_1(j)|U(j)) \leq I(V_1(j); Y_1(j)|V_2(j), U(j))$ after using the fact that conditioning does not increase entropy, and the last equality follows by using a standard information theoretic argument in which we define random variables for the single-letter expression, e.g., V_1 has the same distribution as $V_1(J)$. Hence, we obtain the bound,

$$R_1 \leq \left[I(V_1;Y_1|V_2,U)-I(V_1;Y_e|U)\right]^+, \qquad (47)$$

for some auxiliary random variables that factors as $p(u)p(v_1|u)p(v_2|u)p(x_1|v_1)p(x_2|v_2)p(y_1, y_2, y_e|x_1, x_2)$.

Lemma 15: The secrecy constraint

$$R_1 + R_2 - \frac{1}{n}H(W_1, W_2|\mathbf{Y}_e) \leq \epsilon$$

implies that

$$R_1 - \frac{1}{n}H(W_1|\mathbf{Y}_e) \leq \epsilon,$$

and

$$R_2 - \frac{1}{n}H(W_2|\mathbf{Y}_e) \leq \epsilon.$$

Proof:

$$\begin{aligned}
\frac{1}{n}H(W_1|\mathbf{Y}_e) &= \frac{1}{n}H(W_1, W_2|\mathbf{Y}_e) - \frac{1}{n}H(W_2|\mathbf{Y}_e, W_1) && (48)\\
&\geq R_1 - \epsilon + R_2 - \frac{1}{n}H(W_2|\mathbf{Y}_e, W_1) && (49)\\
&= R_1 - \epsilon + \frac{1}{n}H(W_2) - \frac{1}{n}H(W_2|\mathbf{Y}_e, W_1) && (50)\\
&\geq R_1 - \epsilon, && (51)
\end{aligned}$$

where the second equality follows by $H(W_2) = nR_2$, and the last inequality follows due to the fact that conditioning does not increase entropy. Second statement follows from a similar observation. ■

Appendix III
Proof of Theorem 3

From arguments given in [5, Lemma], the assumed property of the channel implies the following.

$$I(\mathbf{V}_2; \mathbf{Y}_2|\mathbf{V}_1) \leq I(\mathbf{V}_2; \mathbf{Y}_1|\mathbf{V}_1) \qquad (52)$$

Then, by considering $V_1(i) = W_1$ and $V_2(i) = W_2$, for $i = 1, \cdots, n$, we get

$$I(W_2; \mathbf{Y}_2|W_1) \leq I(W_2; \mathbf{Y}_1|W_1) \qquad (53)$$

We continue as follows.

$$\begin{aligned}
\frac{1}{n}H(W_1, W_2|\mathbf{Y}_1) &= \frac{1}{n}H(W_1|\mathbf{Y}_1) + \frac{1}{n}H(W_2|\mathbf{Y}_1, W_1)\\
&\leq \epsilon_1 + \frac{1}{n}H(W_2|\mathbf{Y}_1, W_1)\\
&\leq \epsilon_1 + \frac{1}{n}H(W_2|\mathbf{Y}_2, W_1)\\
&\leq \epsilon_1 + \frac{1}{n}H(W_2|\mathbf{Y}_2)\\
&\leq \epsilon_1 + \epsilon_2, && (54)
\end{aligned}$$

where the first inequality is due to the Fano's inequality at the receiver 1 with some $\epsilon_1 \to 0$ as $n \to \infty$, the second inequality follows from (53), the third one is due to conditioning can not increase entropy, and the last one follows from the Fano's inequality at the receiver 2 with some $\epsilon_2 \to 0$ as $n \to \infty$.

We then proceed following the standard techniques given in [13], [14]. We first state the following definitions.

$$I_1 \triangleq \sum_{i=1}^{n} I(\tilde{\mathbf{Y}}_e^{i+1};Y_1(i)|\mathbf{Y}_1^{i-1}) \tag{55}$$

$$\hat{I}_1 \triangleq \sum_{i=1}^{n} I(\mathbf{Y}_1^{i-1};Y_e(i)|\tilde{\mathbf{Y}}_e^{i+1}) \tag{56}$$

$$I_3 \triangleq \sum_{i=1}^{n} I(\tilde{\mathbf{Y}}_e^{i+1};Y_1(i)|\mathbf{Y}_1^{i-1},W_1,W_2) \tag{57}$$

$$\hat{I}_3 \triangleq \sum_{i=1}^{n} I(\mathbf{Y}_1^{i-1};Y_e(i)|\tilde{\mathbf{Y}}_e^{i+1},W_1,W_2), \tag{58}$$

where $\tilde{\mathbf{Y}}^{i+1}=[Y(i+1)\cdots Y(n)]$ for random variable Y.

Then, we bound the sum rate as follows.

$$\begin{aligned}
R_1+R_2-\epsilon &\leq \frac{1}{n}H(W_1,W_2|\mathbf{Y}_e)\\
&= \frac{1}{n}\left(H(W_1,W_2|\mathbf{Y}_1)+I(W_1,W_2;\mathbf{Y}_1)-I(W_1,W_2;\mathbf{Y}_e)\right)\\
&\leq \epsilon_1+\epsilon_2+\frac{1}{n}\left(\sum_{i=1}^{n} I(W_1,W_2;Y_1(i)|\mathbf{Y}_1^{i-1})-\sum_{i=1}^{n} I(W_1,W_2;Y_e(i)|\tilde{\mathbf{Y}}_e^{i+1})\right)\\
&= \epsilon_1+\epsilon_2+\frac{1}{n}\Bigg(\sum_{i=1}^{n} I(W_1,W_2;Y_1(i)|\mathbf{Y}_1^{i-1},\tilde{\mathbf{Y}}_e^{i+1})+I_1-I_3\\
&\quad -\sum_{i=1}^{n} I(W_1,W_2;Y_e(i)|\mathbf{Y}_1^{i-1},\tilde{\mathbf{Y}}_e^{i+1})-\hat{I}_1+\hat{I}_3\Bigg)\\
&= \epsilon_1+\epsilon_2+\frac{1}{n}\left(\sum_{i=1}^{n} I(W_1,W_2;Y_1(i)|\mathbf{Y}_1^{i-1},\tilde{\mathbf{Y}}_e^{i+1})-\sum_{i=1}^{n} I(W_1,W_2;Y_e(i)|\mathbf{Y}_1^{i-1},\tilde{\mathbf{Y}}_e^{i+1})\right),
\end{aligned}$$

where the first inequality is due to the secrecy requirement, the last inequality follows by (54), and the last equality follows by the fact that $I_1=\hat{I}_1$ and $I_3=\hat{I}_3$, which can be shown using arguments similar to [14, Lemma 7].

We define $U(i)\triangleq(\mathbf{Y}_1^{i-1},\tilde{\mathbf{Y}}_e^{i+1},i)$, $V_1(i)\triangleq(U(i),W_1)$, and $V_2(i)\triangleq(U(i),W_2)$. Using standard techniques (see, e.g., [17]), we introduce a random variable J, which is uniformly distributed over $\{1,\cdots,n\}$, and continue as below.

$$\begin{aligned}
R_1+R_2-\epsilon &\leq \epsilon_1+\epsilon_2+\frac{1}{n}\left(\sum_{i=1}^{n} I(W_1,W_2;Y_1(i)|\mathbf{Y}_1^{i-1},\tilde{\mathbf{Y}}_e^{i+1})-\sum_{i=1}^{n} I(W_1,W_2;Y_e(i)|\mathbf{Y}_1^{i-1},\tilde{\mathbf{Y}}_e^{i+1})\right)\\
&= \epsilon_1+\epsilon_2+\frac{1}{n}\left(\sum_{i=1}^{n} I(V_1(i),V_2(i);Y_1(i)|U(i))-\sum_{i=1}^{n} I(V_1(i),V_2(i);Y_e(i)|U(i))\right)\\
&= \epsilon_1+\epsilon_2+\sum_{j=1}^{n} I(V_1(j),V_2(j);Y_1(j)|U(j))p(J=j)-\sum_{j=1}^{n} I(V_1(j),V_2(j);Y_e(j)|U(j))p(J=j)\\
&= \epsilon_1+\epsilon_2+I(V_1,V_2;Y_1|U)-I(V_1,V_2;Y_e|U),
\end{aligned} \tag{59}$$

where, using a standard information theoretic argument, we have defined the random variables for the single-letter expression, e.g., V_1 has the same distribution as $V_1(J)$. Now, due to the memoryless property of the channel, we have $(U, V_1, V_2) \to (X_1, X_2) \to (Y_1, Y_2, Y_e)$, which implies $p(y_1, y_2, y_e|x_1, x_2, v_1, v_2, u) = p(y_1, y_2, y_e|x_1, x_2)$. As we define $V_1(J) = (U(J), W_1)$ and $V_2(J) = (U(J), W_2)$, we have $V_1 \to U \to V_2$, which implies $p(v_1, v_2|u) = p(v_1|u)p(v_2|u)$. Finally, as $X_1(J)$ is a stochastic function of W_1, $X_2(J)$ is a stochastic function of W_2, and W_1 and W_2 are independent, we have $X_1(J) \to V_1(J) \to V_2(J)$, $X_2(J) \to V_2(J) \to V_1(J)$, and $X_1(J) \to (V_1(J), V_2(J)) \to X_2(J)$, which together implies that $p(x_1, x_2|v_1, v_2, u) = p(x_1, x_2|v_1, v_2) = p(x_1|v_1, v_2)p(x_2|v_1, v_2) = p(x_1|v_1)p(x_2|v_2)$.

Hence, we obtain a sum-rate bound,

$$R_1 + R_2 \leq \left[I(V_1, V_2; Y_1|U) - I(V_1, V_2; Y_e|U)\right]^+, \tag{60}$$

for some auxiliary random variables that factors as $p(u)p(v_1|u)p(v_2|u)p(x_1|v_1)p(x_2|v_2)p(y_1, y_2, y_e|x_1, x_2)$, if (9) holds.

Appendix IV
Proof of Corollary 4

Achievability follows from Theorem 1 by only utilizing S_1 and O_2 together with the second equation in (12), where we set $R_2 = 0$ and set R_1 as follows. For a given $p \in \mathcal{P}(S_1, O_2)$, if $I(S_1; Y_1|O_2, Q) \leq I(S_1; Y_e|Q)$, we set $R_1 = 0$; otherwise we assign the following rates.

$$\begin{aligned} R_{S_1} &= I(S_1; Y_1|O_2, Q) - I(S_1; Y_e|Q) \\ R^x_{S_1} &= I(S_1; Y_e|Q) \\ R^x_{O_2} &= I(O_2; Y_e|S_1, Q), \end{aligned}$$

where $R_1 = R_{S_1}$.

Converse follows from Theorem 2. That is, if (R_1, R_2) is achieavable, then $R_1 \leq \max\limits_{p \in \mathcal{P}_O} I(S_1; Y_1|O_2, Q) - I(S_1; Y_e|Q)$ and $R_2 = 0$, due to the first condition given in (12).

Appendix V
Proof of Corollary 5

Achievability follows from Theorem 1 by only utilizing S_1 and C_2 together with the channel condition given in (14). For a given $p \in \mathcal{P}(S_1, C_2)$, if $I(S_1, C_2; Y_1|Q) \leq I(S_1, C_2; Y_e|Q)$, we set $R_1 = R_2 = 0$; otherwise we assign the following rates.

$$\begin{aligned} R_{S_1} &= I(S_1; Y_1|C_2, Q) - I(S_1; Y_e|C_2, Q) \\ R^x_{S_1} &= I(S_1; Y_e|C_2, Q) \\ R_{C_2} &= I(C_2; Y_1|Q) - I(C_2; Y_e|Q) \\ R^x_{C_2} &= I(C_2; Y_e|Q), \end{aligned}$$

where $R_1 = R_{S_1}$ and $R_2 = R_{C_2}$.

Converse follows from Theorem 3 as the needed condition is satisfied by the channel.

APPENDIX VI
PROOF OF COROLLARY 6

Achievability follows from Theorem 1 by only utilizing S_1 and O_2 together with the channel condition given in (15). For a given $p \in \mathcal{P}(S_1, O_2)$, if $I(S_1, O_2; Y_1|Q) \leq I(S_1, O_2; Y_e|Q)$, we set $R_1 = R_2 = 0$; otherwise we assign the following rates.

$$\begin{aligned} R_{S_1} &= I(S_1, O_2; Y_1|Q) - I(S_1, O_2; Y_e|Q) \\ R^x_{S_1} &= I(S_1, O_2; Y_e|Q) - I(O_2; Y_1|S_1, Q) \\ R^x_{O_2} &= I(O_2; Y_1|S_1, Q), \end{aligned}$$

where $R_1 = R_{S_1}$ and $R_2 = 0$.

Converse follows from Theorem 3 as the needed condition is satisfied by the channel.

APPENDIX VII
PROOF OF COROLLARY 7

Achievability follows from Theorem 1 by only utilizing S_1 and O_2 together with the channel condition given in (16). For a given $p \in \mathcal{P}(S_1, O_2)$, if $I(S_1, O_2; Y_1|Q) \leq I(S_1, O_2; Y_e|Q)$, we set $R_1 = R_2 = 0$; otherwise we assign the following rates.

$$\begin{aligned} R_{S_1} &= I(S_1, O_2; Y_1|Q) - I(S_1, O_2; Y_e|Q) \\ R^x_{S_1} &= I(S_1; Y_e|Q) \\ R^x_{O_2} &= I(O_2; Y_e|S_1, Q), \end{aligned}$$

where $R_1 = R_{S_1}$ and $R_2 = 0$.

Converse follows from Theorem 3 as the needed condition is satisfied by the channel.

APPENDIX VIII
PROOF OF COROLLARY 9

For a given MAC-E with $p(y_1, y_e|x_1, x_2)$, we consider an IC-E defined by $p(y_1, y_2, y_e|x_1, x_2) = p(y_1, y_e|x_1, x_2)\delta(y_2 - y_1)$ and utilize Theorem 1 with $p \in \mathcal{P}(C_1, C_2)$ satisfying (17). Then, the achievable region becomes

$$\begin{aligned} R_1 = R_{C_1} &\leq I(C_1; Y_1|C_2, Q) - R^x_{C_1} \\ R_2 = R_{C_2} &\leq I(C_2; Y_1|C_1, Q) + R^x_{C_1} - I(C_1, C_2; Y_e|Q), \\ R_1 + R_2 = R_{C_1} + R_{C_2} &\leq I(C_1, C_2; Y_1|Q) - I(C_1, C_2; Y_e|Q), \end{aligned} \tag{61}$$

where $I(C_1; Y_e|Q) \leq R^x_{C_1} \leq I(C_1; Y_e|C_2, Q)$ and $R^x_{C_2} = I(C_1, C_2; Y_e|Q) - R^x_{C_1}$. Hence, $R_1 + R_2 = [I(C_1, C_2; Y_1|Q) - I(C_1, C_2; Y_e|Q)]^+$ is achievable for any $p \in \mathcal{P}(C_1, C_2)$ satisfying (17).

The following outer bound on the sum rate follows by Theorem 3, as the constructed IC-E satisfies the needed condition of the theorem.

$$R_1 + R_2 \leq I(C_1, C_2; Y_1|Q) - I(C_1, C_2; Y_e|Q),$$

for any $p \in \mathcal{P}(C_1, C_2)$. Which is what needed to be shown.

Appendix IX
Proof of Corollary 10

We first remark that $R^{[\text{NF}]}$ will remain the same if we restrict the union over the set of probability distributions

$$\tilde{\mathcal{P}}(S_1, O_2, |\mathcal{Q}| = 1) \triangleq \{p \mid p \in \mathcal{P}(S_1, O_2, |\mathcal{Q}| = 1), I(O_2; Y_e) \leq I(O_2; Y_1)\}.$$

As for any $p \in \mathcal{P}(S_1, O_2, |\mathcal{Q}| = 1)$ satisfying $I(O_2; Y_e) \geq I(O_2; Y_1)$, $R_1(p) = [I(S_1; Y_1|O_2) - I(S_1; Y_e|O_2)]^+$ since $I(O_2; Y_1) \leq I(O_2; Y_e) \leq I(O_2; Y_e|S_1)$ in this case. And the highest rate achievable with the NF scheme occurs if O_2 is chosen to be deterministic, and hence $I(O_2; Y_1) = I(O_2; Y_e)$ case will result in the highest rate among the probability distributions $p \in \mathcal{P}(S_1, O_2, |\mathcal{Q}| = 1)$ satisfying $I(O_2; Y_e) \geq I(O_2; Y_1)$. Therefore, without loss of generality, we can write

$$R^{[\text{NF}]} = \max_{p \in \tilde{\mathcal{P}}(S_1, O_2, |\mathcal{Q}|=1)} R_1(p),$$

where $R_1(p) = [I(S_1; Y_1|O_2) + \min\{I(O_2; Y_1), I(O_2; Y_e|S_1)\} - I(S_1, O_2; Y_e)]^+$.

Now, fix some $p \in \tilde{\mathcal{P}}(S_1, O_2, |\mathcal{Q}| = 1)$, and set $R^x_{O_2} = \min\{I(O_2; Y_1), I(O_2; Y_e|S_1)\}$, $R^x_{S_1} = I(S_1, O_2; Y_e) - \min\{I(O_2; Y_1), I(O_2; Y_e|S_1)\}$, and $R_{S_1} = I(S_1; Y_1|O_2) - I(S_1, O_2; Y_e) + \min\{I(O_2; Y_1), I(O_2; Y_e|S_1)\}$, where we set $R_1 = 0$ if the latter is negative. Here,

$$R_1 = [I(S_1; Y_1|O_2) + \min\{I(O_2; Y_1), I(O_2; Y_e|S_1)\} - I(S_1, O_2; Y_e)]^+$$

is achievable, i.e., $(R_1(p), 0) \in \mathcal{R}^{\text{RE}}$ for any $p \in \tilde{\mathcal{P}}(S_1, O_2, |\mathcal{Q}| = 1)$. Observing that $(R^{[\text{NF}]}, 0) \in \mathcal{R}^{\text{RE}}$, we conclude that the noise forwarding (NF) scheme of [18] is a special case of the proposed scheme.

Appendix X
Proof of Corollary 11

For any given $p \in \mathcal{P}(S_1, O_2, |\mathcal{Q}| = 1)$ satisfying $I(O_2; Y_e) \leq I(O_2; Y_1)$, we see that $R_1 = [I(S_1, O_2; Y_1) - I(S_1, O_2; Y_e)]^+$ is achievable due to (19) and Corollary 10. The converse follows by Theorem 3 as the needed condition is satisfied by considering an IC-E defined as $p(y_1, y_e|x_1, x_2)\delta(y_2 - y_1)$, where we set $|\mathcal{Q}| = 1$ in the upper bound as the time sharing random variable is not needed for this scenario, and further limit the input distributions to satisfy $I(O_2; Y_e) \leq I(O_2; Y_1)$. The latter does not reduce the maximization for the upper bound due to a similar reasoning given in the Proof of Corollary 10.

REFERENCES

[1] O. O. Koyluoglu and H. El Gamal, "On the Secrecy Rate Region for the Interference Channel," in *Proc. 2008 IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'08)*, Cannes, France, Sep. 2008.

[2] T. Han and K. Kobayashi, "A new achievable rate region for the interference channel," *IEEE Trans. Inf. Theory*, vol. 27, no. 1, pp. 49–60, Jan. 1981.

[3] H. Chong, M. Motani, H. Garg, and H. El Gamal, "On the Han-Kobayashi region for the interference channel," *IEEE Trans. Inf. Theory*, vol. 54, pp. 3188–3195, Jul. 2008.

[4] H. Sato, "The capacity of the gaussian interference channel under strong interference," *IEEE Trans. Inf. Theory*, vol. 27, no. 6, pp. 786–788, Nov. 1981.

[5] M. H. Costa and A. El Gamal, "The capacity region of the discrete memoryless interference channel with strong interference," *IEEE Trans. Inf. Theory*, vol. 33, no. 5, pp. 710–711, Sep. 1987.

[6] X. Shang, G. Kramer, and B. Chen, "A new outer bound and the noisy-interference sum-rate capacity for gaussian interference channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 689–699, Feb. 2009.

[7] V. S. Annapureddy and V. V. Veeravalli, "Gaussian interference networks: Sum capacity in the low interference regime and new outer bounds on the capacity region," *IEEE Trans. Inf. Theory*, submitted for publication.

[8] A. S. Motahari and A. K. Khandani, "Capacity bounds for the gaussian interference channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 620–643, Feb. 2009.

[9] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdu, "Cognitive interference channels with confidential messages," in *Proc. of the 45th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, Sep. 2007.

[10] 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.

[11] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "On the secure degrees of freedom in the K-user gaussian interference channel," in *Proc. 2008 IEEE International Symposium on Information Theory (ISIT08)*, Toronto, ON, Canada, Jul. 2008.

[12] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf. Theory*, submitted for publication.

[13] A. D. Wyner, "The Wire-Tap Channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[14] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339-348, May. 1978.

[15] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. 2005 IEEE 62nd Vehicular Technology Conference, (VTC-2005-Fall)*, 2005.

[16] 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.

[17] T. Cover and J. Thomas, "Elements of Information Theory," John Wiley and Sons, Inc., 1991.

[18] 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.

[19] A. Carleial, "Interference channels," *IEEE Trans. Inf. Theory*, vol. 24, no. 1, pp. 60-70, Jan. 1978.

[20] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451-456, Jul. 1978.

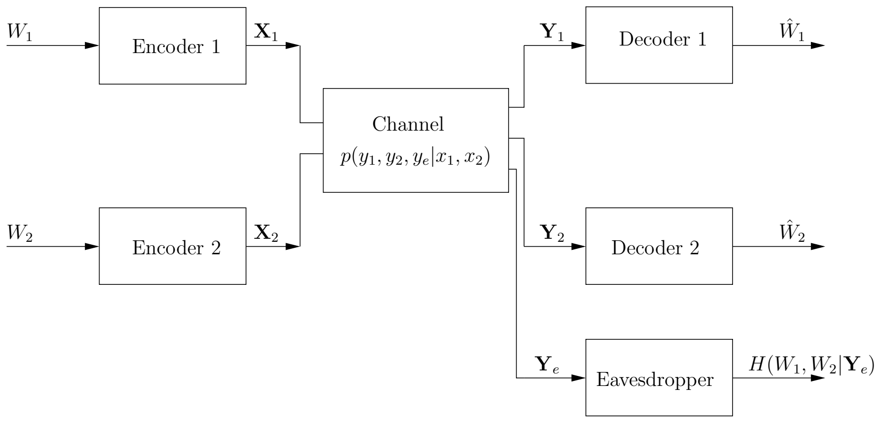

Fig. 1. The discrete memoryless interference channel with an eavesdropper (IC-E).

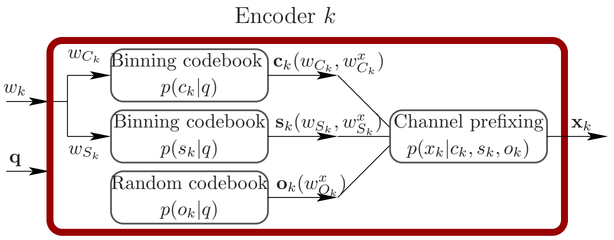

Fig. 2. Proposed encoder structure for the IC-E.

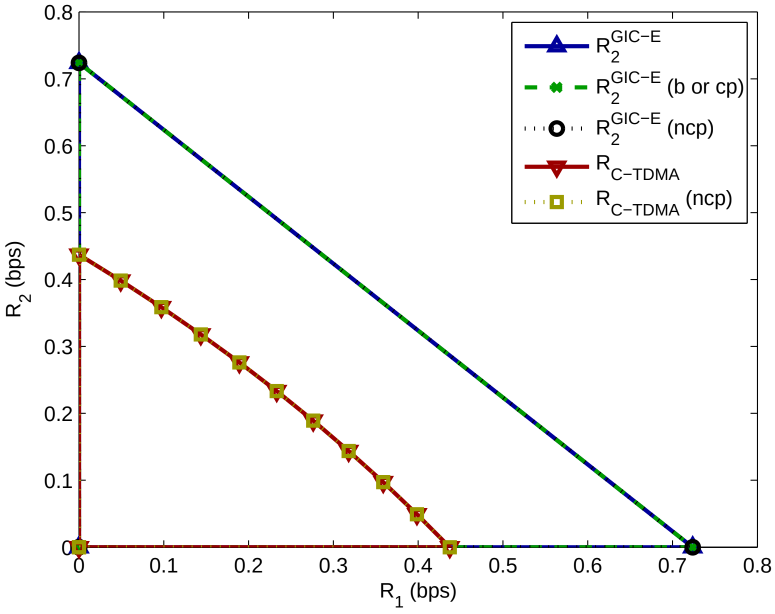

Fig. 3. Numerical results for GIC-E with $c_{12} = c_{21} = 1.9$, $c_{1e} = c_{2e} = 0.5$, $P_1 = P_2 = 10$.

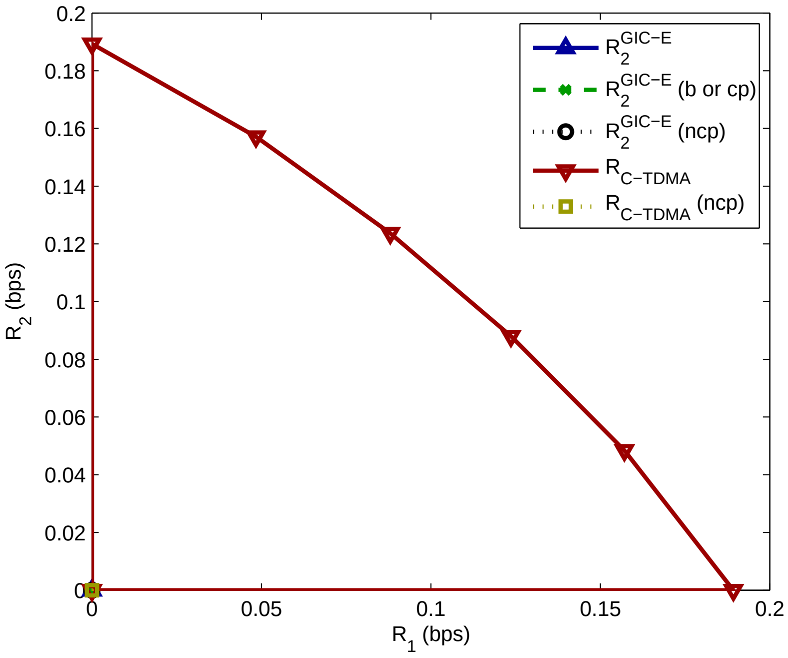

Fig. 4. Numerical results for GIC-E with $c_{12} = c_{21} = 0.6$, $c_{1e} = c_{2e} = 1.1$, $P_1 = P_2 = 10$.

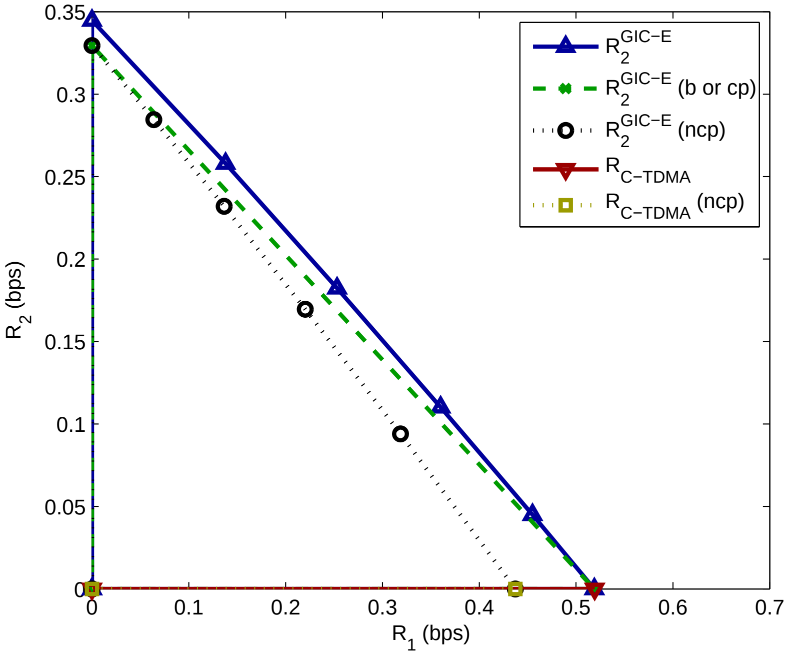

Fig. 5. Numerical results for GIC-E with $c_{12} = 1.9$, $c_{21} = 1$, $c_{1e} = 0.5$, $c_{2e} = 1.6$, $P_1 = P_2 = 10$.