Multi-Terminal Communications with Confidential Messages

Ruoheng Liu
WINLAB, ECE
Rutgers University
North Brunswick, NJ 08902, USA
Email: liurh@winlab.rutgers.edu

Ivana Marić
Electrical Engineering
Stanford University
Stanford, CA 94305
Email: ivanam@wsl.stanford.edu

Predrag Spasojević and Roy D. Yates
WINLAB, ECE
Rutgers University
North Brunswick, NJ 08902, USA
Email: {spasojev,ryates}@winlab.rutgers.edu

***Abstract*— We study information-theoretic security for discrete memoryless *interference* and *broadcast* channels with independent confidential messages sent to two receivers. Confidential messages are transmitted to their respective receivers with perfect secrecy. That is, each receiver is kept in total ignorance with respect to the message intended for the other receiver. The secrecy level is measured by the equivocation rate at the eavesdropping receiver. This approach was first introduced by Wyner in 1975 for the wiretap channel model. In this paper, we investigate the secrecy capacity region bounds for these two communication systems. The derived outer bounds have an identical mutual information expression that applies to the broadcast channel when one sender jointly encodes both messages and to the interference channel when two senders offer independent inputs to the channel. We consider a *switch* channel model which is a special case of the interference channel and show that the derived outer and inner bounds meet in this case. Finally, we focus on Gaussian interference channels with confidential messages and describe several transmission schemes and their achievable rate regions under the prefect secrecy requirement.**

I. Introduction

We first consider a discrete memoryless *interference channel* in which two transmitters wish to send independent, confidential messages to their respective receivers. We refer to such a channel as the *interference channel with confidential messages* (IC-CM) and denote it with $(\mathcal{X}_1 \times \mathcal{X}_2, p(y_1, y_2|x_1, x_2), \mathcal{Y}_1 \times \mathcal{Y}_2)$. This communication model is shown in Figure 1.

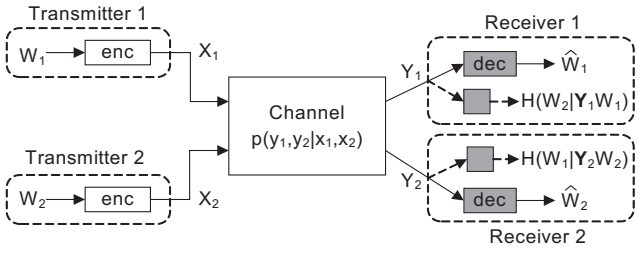

Fig. 1. System model: Interference channel with confidential messages

We also consider the *broadcast channel with confidential messages* (BC-CM), denoted $(\mathcal{X}, p(y_1, y_2|x), \mathcal{Y}_1 \times \mathcal{Y}_2)$, in which confidential messages from a single transmitter are to be communicated to two receivers. The corresponding broadcast communication model is shown in Figure 2. The ignorance of a receiver with respect to the message intended for the other receiver is measured by equivocation. This approach was introduced by Wyner [1] for the wiretap channel, a scenario in which a single source-destination communication is eavesdropped. Under the assumption that the channel to the wire-tapper is a degraded version of that to the receiver, Wyner determined the capacity-secrecy tradeoff. This result was generalized by Csiszár and Körner who determined the capacity region of the broadcast channel with confidential messages [2] in which a message intended for one of the receivers is confidential.

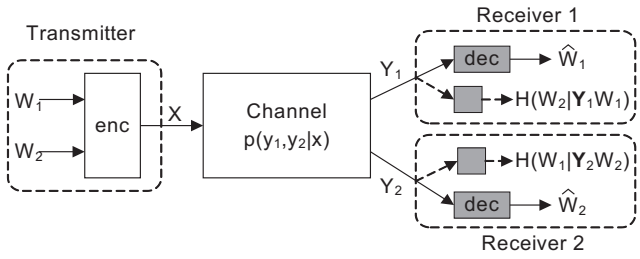

Fig. 2. System model: Broadcast channel with confidential messages

Here, we study inner and outer bounds for achievable secrecy regions of both the broadcast and the interference channel under the requirement of *perfect secrecy*. That is, each receiver is kept in total ignorance with respect to the message intended for the other receiver. We first derive outer bounds which have an identical mutual information expressions that apply to the broadcast channel when one sender jointly encodes both messages and to the interference channel when two senders offer independent inputs to the channel. The difference is that the optimization is over different input probability distributions, as will be described in the next section. We also summary the inner bounds for the IC-CM and BC-CM derived in our previous work [3]. Since we require perfect security for confidential messages, no partial decoding of the other transmitter's message is allowed at a receiver. Hence, rate-splitting schemes used by Carleial [4] and Han and Kobayashi [5] for the classical interference channel are precluded. The inner bound for the BC-CM based on the *double-binning*, which is using for joint encoding and preserving confidentiality. We note that no common message in the sense of Marton [6] in the broadcast channel is conveyed

to the receivers since we only consider sending confidential messages. Next, we consider a switch channel model which is a special case of the interference channel and show that the derived outer and inner bounds meet in this case. Finally, we focus on Gaussian interference channels with confidential messages and describe several transmission schemes and their achievable rate regions under the prefect secrecy requirement.

The remainder of this paper is organized as follows: we introduce the channel model and state our main results in Sec. II. We derive outer bounds in Sec. III. We study the switch and channel with confidential messages in Sec. IV and the Gaussian IC-CM in Sec. V.

II. Channel Model and Statement of the Result

A. Notation

Throughout the paper, random variables are denoted with upper case letters and the values they take are denoted with the corresponding lower case letters. Boldface symbols denote sequences. Also, define

$$\mathbf{X} = [X_{1,1}, \ldots, X_{1,n}], \quad \mathbf{X}^i = [X_{1,1}, \ldots, X_{1,i}],$$
$$\text{and} \quad \tilde{\mathbf{X}}^i = [X_{2,i}, \ldots, X_{2,n}].$$

B. The Interference Channel

A discrete memoryless interference channel with confidential messages is described using finite sets $\mathcal{X}_1$, $\mathcal{X}_2$, $\mathcal{Y}_1$, $\mathcal{Y}_2$ and a conditional probability distribution $p(y_1, y_2|x_1, x_2)$. As shown in Figure 1, symbols $(x_1, x_2) \in (\mathcal{X}_1 \times \mathcal{X}_2)$ are channel inputs at transmitters 1 and 2, and $(y_1, y_2) \in (\mathcal{Y}_1 \times \mathcal{Y}_2)$ are channel outputs at receivers 1 and 2, respectively.

A transmitter t, $t = 1, 2$, intends to send an independent message $W_t \in \{1, \ldots, M_t\}$ to the desired receiver t in n channel uses with perfect secrecy. The channel is memoryless in the sense that

$$p(\mathbf{y}_1, \mathbf{y}_2|\mathbf{x}_1, \mathbf{x}_2) = \prod_{i=1}^{n} p(y_{1,i}, y_{2,i}|x_{1,i}, x_{2,i}). \tag{1}$$

A stochastic encoder for the transmitter t is specified by a matrix of conditional probabilities $f_t(\mathbf{x}_t|w_t)$, where $\mathbf{x}_t \in \mathcal{X}_t^n$, $w_t \in \mathcal{W}_t$, and

$$\sum_{\mathbf{x}_t \in \mathcal{X}_t^n} f_t(\mathbf{x}_t|w_t) = 1. \tag{2}$$

Decoding functions are mappings $\psi_t : \mathcal{Y}_t \to \mathcal{W}_t$. Secrecy levels at receivers 1 and 2 are measured with respect to the normalized equivocations

$$\frac{1}{n} H(W_2|\mathbf{Y}_1, W_1) \quad \text{and} \quad \frac{1}{n} H(W_1|\mathbf{Y}_2, W_2). \tag{3}$$

An (M_1, M_2, n, P_e) code for the interference channel consists of two encoding functions f_1, f_2, two decoding functions ψ_1, ψ_2, and the corresponding maximum average error probability

$$P_e \triangleq \max\{P_{e,1},\, P_{e,2}\} \tag{4}$$

where for $t = 1, 2$,

$$P_{e,t} = \sum_{w_1, w_2} \frac{1}{M_1 M_2} P\big[\psi_t(\mathbf{Y}_t) \neq w_t | (w_1, w_2) \text{ sent}\big].$$

A rate pair $(R_1,\, R_2)$ is said to be *achievable* for the interference channel with confidential messages if, for any $\epsilon_0 > 0$, there exists a (M_1, M_2, n, P_e) code such that

$$M_t \geq 2^{nR_t}, \quad P_e \leq \epsilon_0 \quad \text{for } t = 1, 2 \tag{5}$$

and the perfect security requirements

$$H(W_1) - H(W_1|\mathbf{Y}_2, W_2) \leq n\epsilon_0 \tag{6}$$
$$H(W_2) - H(W_2|\mathbf{Y}_1, W_1) \leq n\epsilon_0 \tag{7}$$

are satisfied.

C. The Broadcast Channel

A discrete memoryless broadcast channel with confidential messages is described using finite sets $\mathcal{X}$, $\mathcal{Y}_1$, $\mathcal{Y}_2$, and a conditional probability distribution $p(y_1, y_2|x)$. Symbols $x \in \mathcal{X}$ are channel inputs and $(y_1, y_2) \in (\mathcal{Y}_1 \times \mathcal{Y}_2)$ are channel outputs at receivers 1 and 2, respectively. The transmitter intends to send an independent message $W_t \in \{1, \ldots, M_t\} \triangleq \mathcal{W}_t$ to respective receiver $t \in \{1,\, 2\}$ in n channel uses with perfect secrecy, as measured by the equivocation at the other receiver. The channel is memoryless in the sense that

$$p(\mathbf{y}_1, \mathbf{y}_2|\mathbf{x}) = \prod_{i=1}^{n} p(y_{1,i}, y_{2,i}|x_i). \tag{8}$$

A stochastic encoder is specified by a matrix of conditional probabilities $f(\mathbf{x}|w_1, w_2)$, where $\mathbf{x} \in \mathcal{X}^n$, $w_t \in \mathcal{W}_t$, and

$$\sum_{\mathbf{x} \in \mathcal{X}^n} f(\mathbf{x}|w_1, w_2) = 1. \tag{9}$$

Note that $f(\mathbf{x}|w_1, w_2)$ is the probability that the messages (w_1, w_2) are encoded as the channel input $\mathbf{x}$. The decoding function at the receiver t is a mapping $\phi_t : \mathcal{Y}_t \to \mathcal{W}_t$. The secrecy levels with respect to the confidential messages W_1 and W_2 are measured, respectively, at receivers 1 and 2 with respect to the normalized equivocations (3).

An (M_1, M_2, n, P_e) code for the broadcast channel consists of the encoding function f, decoding functions ϕ_1, ϕ_2, and the maximum error probability P_e in (4), where

$$P_{e,t} = \sum_{w_1, w_2} \frac{1}{M_1 M_2} P\big[\phi_t(\mathbf{Y}_t) \neq w_t | (w_1, w_2) \text{ sent}\big],$$

for $t = 1, 2$. A rate pair $(R_1,\, R_2)$ is said to be achievable for the broadcast channel with confidential messages if, for any $\epsilon_0 > 0$, there exists a (M_1, M_2, n, P_e) code which satisfies (5)–(7).

D. Statement of the Result

The following theorems are the main results of this paper. The theorems give the outer and inner bounds on capacity regions of interference and broadcast channels with confidential messages.

Let U, V_1, and V_2 be auxiliary random variables. We define π as a class of joint distributions. In particular, we consider the following three classes of joint distributions. For the interference channel, let $\pi_{\mathrm{IC-O}}$ be the class of distributions $p(u, v_1, v_2, x_1, x_2, y_1, y_2)$ that factor as

$$p(u)p(v_1, v_2|u)p(x_1|v_1)p(x_2|v_2)p(y_1, y_2|x_1, x_2), \tag{10}$$

and $\pi_{\mathrm{IC-I}}$ be the class of distributions that factor as

$$p(u)p(v_1|u)p(v_2|u)p(x_1|v_1)p(x_2|v_2)p(y_1, y_2|x_1, x_2). \tag{11}$$

For broadcast channel, let π_{BC} denote the class of distributions $p(u, v_1, v_2, x, y_1, y_2)$ that factor as

$$p(u)p(v_1, v_2|u)p(x|v_1, v_2)p(y_1, y_2|x). \tag{12}$$

Let $\mathbb{R}_{\mathrm{O}}(\pi)$ denote the union of all (R_1, R_2) satisfying

$$0 \le R_1 \le \min \left[\begin{array}{l} I(V_1; Y_1|U) - I(V_1; Y_2|U), \\ I(V_1; Y_1|V_2, U) - I(V_1; Y_2|V_2, U) \end{array} \right] \tag{13}$$

$$0 \le R_2 \le \min \left[\begin{array}{l} I(V_2; Y_2|U) - I(V_2; Y_1|U), \\ I(V_2; Y_2|V_1, U) - I(V_2; Y_1|V_1, U) \end{array} \right] \tag{14}$$

over all distributions in π.

Theorem 1. (outer bound)

- *For the interference channel*

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

with confidential messages, the capacity region

$$\mathbb{C}_{\mathrm{IC}} \subseteq \mathbb{R}_{\mathrm{O}}(\pi_{\mathrm{IC-O}}).$$

- *For the broadcast channel*

$$(\mathcal{X}, p(y_1, y_2|x), \mathcal{Y}_1 \times \mathcal{Y}_2)$$

with confidential messages, the capacity region

$$\mathbb{C}_{\mathrm{BC}} \subseteq \mathbb{R}_{\mathrm{O}}(\pi_{\mathrm{BC}}).$$

Proof: We provide the proof of Theorem 1 in Sec. III. □

We have established inner bounds associated with the achievable coding scheme for IC-CM and BC-CM in [3]. Here we review these results as follows.

Let $\mathbb{R}_{\mathrm{IC-I}}(\pi_{\mathrm{IC-I}})$ denote the union of all (R_1, R_2) satisfying

$$\begin{aligned} 0 \le R_1 &\le I(V_1; Y_1|U) - I(V_1; Y_2|V_2, U) \\ 0 \le R_2 &\le I(V_2; Y_2|U) - I(V_2; Y_1|V_1, U) \end{aligned} \tag{15}$$

over all distributions in $\pi_{\mathrm{IC-I}}$.

Theorem 2. (inner bound for IC-CM) *Any rate pair $(R_1, R_2) \in \mathbb{R}_{\mathrm{IC-I}}(\pi_{\mathrm{IC-I}})$ is achievable for the interference channel with confidential messages.*

Let $\mathbb{R}_{\mathrm{BC-I}}(\pi_{\mathrm{BC}})$ denote the union of all (R_1, R_2) satisfying

$$\begin{aligned} 0 \le R_1 &\le I(V_1; Y_1|U) - I(V_1; Y_2|V_2, U) - I(V_1; V_2|U) \\ 0 \le R_2 &\le I(V_2; Y_2|U) - I(V_2; Y_1|V_1, U) - I(V_1; V_2|U) \end{aligned}$$

over all distributions in π_{BC}.

Theorem 3. (inner bound for BC-CM) *Any rate pair $(R_1, R_2) \in \mathbb{R}_{\mathrm{BC-I}}(\pi_{\mathrm{BC}})$ is achievable for the broadcast channel with confidential messages.*

We note that, for BC-CM, we can employ joint encoding at the transmitter. However, to preserve confidentiality, each achievable rate includes a penalty term $I(V_1; V_2|U)$. Hence, compared with Marton's broadcast channel inner bound [6], here, we pay "double" with jointly encoding at the transmitter.

III. Outer Bound

Here we prove Theorem 1 and derive the outer bound for R_1. The outer bound for R_2 follows by symmetry.

The bases for the outer bound derivation are the reliable communication and perfect security requirements, i.e., receiver 1 can correctly decode the message W_1 and receiver 2 is kept in total ignorance with respect to W_1. Based on Fano's inequality, the reliable transmission requirement (5) implies that

$$H(W_1|\mathbf{Y}_1) \le \epsilon_0 \log(M_1 - 1) + h(\epsilon_0) \triangleq n\delta_1. \tag{16}$$

where $h(x)$ is the binary entropy function. On the other hand, the secrecy requirement (6) implies that

$$nR_1 = H(W_1) \le H(W_1|\mathbf{Y}_2, W_2) + n\epsilon_0. \tag{17}$$

In fact, the outer bound (13) is based on the following two different upper bounds on the equivocation rate $H(W_1|\mathbf{Y}_2, W_2)$.

A. First Bound on the Equivocation Rate

The first upper bound is derived by bounding the equivocation rate as follows.

$$\begin{aligned} &H(W_1|\,\mathbf{Y}_2, W_2) \\ &\quad \le H(W_1|\mathbf{Y}_2) \qquad (18) \\ &\quad = H(W_1) - I(W_1; \mathbf{Y}_2) \\ &\quad = I(W_1; \mathbf{Y}_1) - I(W_1; \mathbf{Y}_2) + H(W_1|\mathbf{Y}_1). \qquad (19) \end{aligned}$$

Based on Fano's inequality (16), we can bound (19) as follows

$$\begin{aligned} H(W_1|\mathbf{Y}_2, W_2) &\le I(W_1; \mathbf{Y}_1) - I(W_1; \mathbf{Y}_2) + n\delta_1. \qquad (20) \\ &= H(W_1|\mathbf{Y}_2) - H(W_1|\mathbf{Y}_1) + n\delta_1 \qquad (21) \end{aligned}$$

Let

$$U_i = (\mathbf{Y}_1^{i-1}, \tilde{\mathbf{Y}}_2^{i+1}). \tag{22}$$

We can easily verify

$$\begin{aligned} (U_i, Y_{2,i}) &= (U_{i-1}, Y_{1,i-1}), \\ \mathbf{Y}_1 &= (U_n, Y_{1,n}), \\ \mathbf{Y}_2 &= (U_1, Y_{2,1}). \end{aligned}$$

Hence, we can rewrite (21) as follows

$$\begin{aligned}
&H(W_1|\,\mathbf{Y}_2, W_2)\\
&\quad\le H(W_1|\mathbf{Y}_2) + \sum_{i=2}^{n} H(W_1|U_i, Y_{2,i}) -\\
&\qquad - H(W_2|\mathbf{Y}_1) - \sum_{i=2}^{n} H(W_1|U_{i-1}, Y_{1,i-1}) + n\delta_1\\
&\quad= H(W_1|U_1, Y_{2,1}) + \sum_{i=2}^{n} H(W_1|U_i, Y_{2,i})\\
&\qquad - H(W_2|U_n, Y_{1,n}) - \sum_{i=1}^{n-1} H(W_1|U_i, Y_{1,i}) + n\delta_1\\
&\quad= \sum_{i=1}^{n}[H(W_1|U_i, Y_{2,i}) - H(W_1|U_i, Y_{1,i})] + n\delta_1\\
&\quad= \sum_{i=1}^{n}[I(W_1; Y_{2,i}|U_i) - I(W_1; Y_{1,i}|U_i)] + n\delta_1\ . \qquad (23)
\end{aligned}$$

Inequalities (17) and (23) imply that

$$nR_1 - n(\delta_1 + \epsilon_0) \le \sum_{i=1}^{n}[I(W_1; Y_{1,i}|U_i) - I(W_1; Y_{2,i}|U_i)].$$

Now, for $\delta \triangleq \delta_1 + \epsilon_0$, we have

$$R_1 \le \frac{1}{n}\sum_{i=1}^{n}[I(W_1; Y_{1,i}|U_i) - I(W_1; Y_{2,i}|U_i)] + \delta. \qquad (24)$$

Following [7, Chapter 14], we introduce a random variable Q uniformly distributed over $\{1, 2, \ldots, n\}$ and independent of $(W_1, W_2, \mathbf{X}_1, \mathbf{X}_2, \mathbf{Y}_1, \mathbf{Y}_2)$. Now we can bound R_1 as follows

$$\begin{aligned}
R_1 &\le \frac{1}{n}\sum_{i=1}^{n}[I(W_1; Y_{1,i}|U_i, Q=i)\\
&\qquad - I(W_1; Y_{2,i}|U_i, Q=i)] + \delta\\
&= \sum_{i=1}^{n} p(Q=i)[I(W_1; Y_{1,Q}|U_Q, Q=i)\\
&\qquad - I(W_1; Y_{2,Q}|\mathbf{Y}_1^{Q-1}, \tilde{\mathbf{Y}}_2^{Q+1}, Q=i)] + \delta\\
&= I(W_1; Y_{1,Q}|U_Q, Q) - I(W_1; Y_{2,Q}|U_Q, Q) + \delta \qquad (25)
\end{aligned}$$

Let

$$\begin{aligned}
&U \triangleq (U_Q, Q)\\
&Y_1 \triangleq Y_{1,Q},\quad Y_2 \triangleq Y_{2,Q},\quad V_1 \triangleq W_1,\ \text{and}\ V_2 \triangleq W_2. \qquad (26)
\end{aligned}$$

We rewrite (25) as

$$R_1 \le I(V_1; Y_1|U) - I(V_1; Y_2|U) + \delta. \qquad (27)$$

Remark 1. Inequality (18) implies that this bound is tight when $I(W_1; W_2|\mathbf{Y}_2) = 0$, e.g., for the case of two *independent parallel* channels without an eavesdropper.

B. Second Bound on the Equivocation Rate

We next consider the second bound on $H(W_1|\mathbf{Y}_2, W_2)$. This bound assumes that a genie gives receiver 1 message information W_2 whereas the Receiver 1 attempts to decode W_1 based on this side information. We have

$$H(W_1|\mathbf{Y}_1, W_2) \le H(W_1|\mathbf{Y}_1) \le n\delta_1 \qquad (28)$$

where the second inequality follows from Fano's inequality (16). Hence, the equivocation rate is upper bounded by

$$\begin{aligned}
&H(W_1|\,\mathbf{Y}_2, W_2)\\
&\quad= H(W_1|W_2) - I(W_1; \mathbf{Y}_2|W_2)\\
&\quad= I(W_1; \mathbf{Y}_1|W_2) - I(W_1; \mathbf{Y}_2|W_2) + H(W_1|\mathbf{Y}_1, W_2)\\
&\quad\le I(W_1; \mathbf{Y}_1|W_2) - I(W_1; \mathbf{Y}_2|W_2) + n\delta_1\\
&\quad= H(W_1|\mathbf{Y}_2, W_2) - H(W_1|\mathbf{Y}_1, W_2) + n\delta_1 \qquad (29)
\end{aligned}$$

Following the same approach as in (21)–(24), we can bound R_1 as follows

$$R_1 \le \frac{1}{n}\sum_{i=1}^{n}[I(W_1; Y_{1,i}|U_i, W_2) - I(W_1; Y_{2,i}|U_i, W_2)] + \delta. \qquad (30)$$

Next, following the approach in (25)–(26), we obtain

$$R_1 \le I(V_1; Y_1|V_2, U) - I(V_1; Y_2|V_2, U) + \delta. \qquad (31)$$

Remark 2. Since we assume that receiver 1 knows W_2 in advance, (28) implies that this bound is tight whenever $I(W_1; W_2|\mathbf{Y}_1) = 0$, e.g., when W_2 is a constant or is the common message.

C. Outer Bound and Discussion

Combining the two outer bounds (27) with (31) and assuming $\delta \to 0$, we have

$$R_1 \le \min\left[\begin{array}{l} I(V_1; Y_1|U) - I(V_1; Y_2|U),\\ I(V_1; Y_1|V_2, U) - I(V_1; Y_2|V_2, U)\end{array}\right]. \qquad (32)$$

Similarly, we can bound R_2 as

$$R_2 \le \min\left[\begin{array}{l} I(V_2; Y_2|U) - I(V_2; Y_1|U),\\ I(V_2; Y_2|V_1, U) - I(V_2; Y_1|V_1, U)\end{array}\right]. \qquad (33)$$

Note that, due to (26), the joint distribution $p(u, v_1, v_2, x, y_1, y_2)$ factors as (12) for a broadcast channel and the joint distribution $p(u, v_1, v_2, x_1, x_2, y_1, y_2)$ factors as (10) for an interference channel.

Now, we show that the combination outer bound is indeed tighter than individual bounds derived in Sec. III-A and Sec. III-B, respectively. Let

$$\begin{aligned}
\Delta_1 &= I(V_1; Y_1|U) - I(V_1; Y_2|U)\\
\Delta_2 &= I(V_2; Y_2|U) - I(V_2; Y_1|U)\\
\Delta_3 &= I(V_1; Y_1|V_2, U) - I(V_1; Y_2|V_2, U)\\
\Delta_4 &= I(V_2; Y_2|V_1, U) - I(V_2; Y_1|V_1, U).
\end{aligned}$$

The following lemma leads to a constraint on sum rate.

Lemma 1.

$$\Delta_1 + \Delta_2 = \Delta_3 + \Delta_4 \tag{34}$$

$$\min[\Delta_1 + \Delta_4,\, \Delta_2 + \Delta_3] \le \Delta_1 + \Delta_2 \tag{35}$$

$$\min[\Delta_1 + \Delta_4,\, \Delta_2 + \Delta_3] \le \Delta_3 + \Delta_4. \tag{36}$$

Proof: We provide the proof in Appendix A. □

Lemma 1 implies that we can choose the sum rate upper bound as

$$R_1 + R_2 \le \min[\Delta_1 + \Delta_4,\, \Delta_2 + \Delta_3]. \tag{37}$$

IV. Switch Channel

In this section, we obtain the security capacity region for the switch channel (SC), a special case of the interference channel. Here, as shown in Figure 3, neither receiver can listen to both transmissions (from encoder 1 and 2) at the same time. For example, the two encoders transmit at different frequencies, whereas each receiver can listen on only one frequency during each symbol time i.

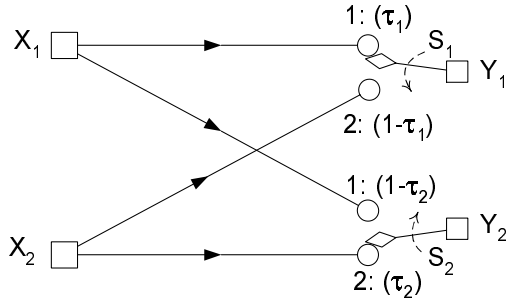

Fig. 3. Switch channel model

We assume that receiver t has a random switch $s_t \in \{1, 2\}$, for $t = 1, 2$, which chooses between t and $\bar{t}$ independently each symbol time i with probabilities

$$P(S_{t,i} = t) = \tau_t$$
$$P(S_{t,i} = \bar{t}) = 1 - \tau_t \quad \text{for } i = 1, \ldots, n$$

where $\bar{t}$ is the complement of t. Further, receiver t listens to its own information $x_{t,i}$ from encoder t when $S_{t,i} = t$, whereas eavesdrops the signal $x_{\bar{t},i}$ from the other encoder when $S_{t,i} = \bar{t}$. By assuming that the switch state information is available at the receiver, we have

$$\begin{aligned} p(y_{t,i}|x_{1,i}, x_{2,i}, s_{t,i}) &= p(y_{t,i}|x_{1,i})\mathbf{1}(s_{t,i} = 1) \\ &\quad + p(y_{t,i}|x_{2,i})\mathbf{1}(s_{t,i} = 2) \\ &= p(y_{t,i}|x_{s_{t,i},i}) \end{aligned} \tag{38}$$

where $\mathbf{1}(\cdot)$ is the indicator function.

The switch state information $\{S_{t,i}\}_{i=1}^n$ is an i.i.d. process known at receiver t. In this case, we can view $s_{t,i}$ as a part of channel output, i.e., we set

$$y_{t,i} \triangleq \{z_{t,i},\, s_{t,2}\} \tag{39}$$

where $z_{t,i}$ represents the received signal value at receiver t. Under this setting, we have the following theorem on the secrecy capacity region of the SC-CM.

Theorem 4. *For the switch channel*

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

with confidential messages, the capacity region is

$$\mathbb{C}_{\rm SC} = \mathbb{R}_{\rm IC-I}(\pi_{\rm IC-I})$$

where $\pi_{\rm IC-I}$ and $\mathbb{R}_{\rm IC-I}(\pi_{\rm IC-I})$ are defined in (11) and (15), respectively.

Proof: We provide the proof in Appendix B. □

Remark 3. In the modeled switch channels with confidential messages (SC-CM), receiver t listens to the desired information during time fraction τ_t, and intercepts the other message during the left time fraction $(1-\tau_t)$. When $\tau_1 = \tau_2 = 1$, both receivers only listen to their own messages and thus the SC-CM reduces to two independent parallel channels without the secrecy constraints. When $\tau_1 = 1$ and $\tau_2 = 0$, receiver 2 acts as an eavesdropper only and both Y_1 and Y_2 are independent with respect to the message W_2. Hence the SC-CM reduces to the general wiretap channel [1], [2].

Example 1. (deterministic memoryless switch channel) We assume that the channel is discrete memoryless and that the input-output relationship at each time instant satisfies

$$Y_{t,i} = \begin{cases} X_{1,i}, & S_{t,i} = 1 \\ X_{2,i}, & S_{t,i} = 2 \end{cases} \qquad \text{for} \quad i = 1, \ldots, n \tag{40}$$

where $P(S_{t,i} = t) = \tau_t$ and $\tau_1 + \tau_2 \ge 1$. Theorem 4 implies that the secrecy capacity region of this channel is:

$$\left\{ (R_1, R_2) : \begin{array}{l} R_1 \le (\tau_1 + \tau_2 - 1)H(X_1) \\ R_2 \le (\tau_1 + \tau_2 - 1)H(X_2) \end{array} \right\}. \tag{41}$$

V. Gaussian IC-CM

In this section, we consider Gaussian interference channels (GIC) with confidential message (GIC-CM) where each transmitter (and receiver) employs a single antenna. We assume the channel input and output symbols to be from an alphabet of real numbers. Following the standard form GIC [4], the received symbols are

$$\begin{aligned} y_{1,i} &= x_{1,i} + \alpha_1 x_{2,i} + z_{1,i} \\ y_{2,i} &= \alpha_2 x_{1,i} + x_{2,i} + z_{2,i} \quad i = 1, \ldots, n \end{aligned} \tag{42}$$

where α_1 and α_2 are normalized crossover *channel gains*, $x_{1,i}$ and $x_{1,i}$ are transmitted symbols from encoders 1 and 2 with the average power constraint

$$\sum_{i=1}^{n} \frac{\mathsf{E}[x_{t,i}^2]}{n} \le P_t, \quad \text{for } t = 1, 2,$$

and $\{z_{1,i}\}$ and $\{z_{2,i}\}$ correspond to two independent, zero-mean, unit-variance, Gaussian noise sequences. In the following, we focus on the *weak* interference channel, i.e., $0 \le \alpha_1^2 < 1$ and $0 \le \alpha_2^2 < 1$. We describe three transmission

schemes and their achievable rate regions under the prefect secrecy requirement.

- **[time sharing]** Here, the transmission period is divided into two non-overlapping slots with time fractions τ_1 and τ_2, where $\tau_1 + \tau_2 = 1$. Transmitter t sends confidential message W_t in slot t with time fraction τ_t, $t = 1, 2$. We refer to this technique as the time sharing scheme. We note that, in each slot, the channel reduces to a Gaussian wire-tap channel [8]. Let $\mathbb{R}_{\mathrm{GIC}}^{[\mathrm{T}]}$ denote the set of (R_1, R_2) satisfying

$$\begin{aligned} 0 \le R_1 &\le \tau_1[\log(1+P_1) - \log(1+\alpha_2^2 P_1)]/2 \\ 0 \le R_2 &\le \tau_2[\log(1+P_2) - \log(1+\alpha_1^2 P_2)]/2 \end{aligned} \quad (43)$$

  for all time fraction τ_1, τ_2 pairs. Following [8], we can show that any rate pair

$$(R_1, R_2) \in \mathbb{R}_{\mathrm{GIC}}^{[\mathrm{TS}]}$$

  is achievable for GIC-CM.
- **[multiplexed transmission]** In the multiplexed transmission scheme, we allow communication links to share the same degrees of freedom. Since we require perfect security for confidential messages, no partial decoding of the other transmitter's message is allowed at a receiver. Hence, the interference results in increasing to the noise floor. Let

$$0 \le \beta_t \le 1 \quad \text{for } t = 1, 2.$$

  By choosing $V_t = X_t \sim \mathcal{N}[0, \beta_t P_t]$ independently and U as a time-sharing random variable, Theorem 2 implies that any rate pair

$$(R_1, R_2) \in \mathbb{R}_{\mathrm{GIC}}^{[\mathrm{M}]}$$

  is achievable for GIC-CM, where $\mathbb{R}_{\mathrm{GIC}}^{[\mathrm{M}]}$ denotes the convex set of (R_1, R_2) satisfying

$$\begin{aligned} 0 \le R_1 &\le \frac{1}{2}\log\left(1 + \frac{\beta_1 P_1}{1+\alpha_1^2\beta_2 P_2}\right) - \frac{1}{2}\log(1+\alpha_2^2\beta_1 P_1) \\ 0 \le R_2 &\le \frac{1}{2}\log\left(1 + \frac{\beta_2 P_2}{1+\alpha_2^2\beta_1 P_1}\right) - \frac{1}{2}\log(1+\alpha_2^2\beta_1 P_2) \end{aligned} \quad (44)$$

  for all β_1, β_2 pairs.
- **[artificial noise]** Here, we propose a new scheme which allows one of the transmitters (e.g., transmitter 2) generate artificial noise. This strategy involves splitting the transmission power of transmitter 2 into two parts $P_{2,M}$ and $P_{2,A}$, where

$$\begin{aligned} P_{2,M} &= (1-\lambda)\beta_2 P_2 \\ P_{2,A} &= \lambda\beta_2 P_2, \quad \text{for } 0 \le \lambda \le 1, \end{aligned}$$

  so that transmitter 2 encodes the confidential message with power $P_{2,M}$ and generates artificial noise with power $P_{2,A}$. The artificial noise can spoil the received signal of receiver 2 and, hence, protect the confidential message of transmitter 1. Let U be a time-sharing random variable,

$$X_1 = V_1 \quad \text{and} \quad X_2 = V_2 + A_2 \quad (45)$$

where V_1, V_2, and A_2 are independent Gaussian random variables:

$$\begin{aligned} &V_1 \sim \mathcal{N}[0, \beta_1 P_1], \quad V_2 \sim \mathcal{N}[0, (1-\lambda)\beta_2 P_1], \\ &A_2 \sim \mathcal{N}[0, \lambda\beta_2 P_2] \end{aligned}$$

Applying Theorem 2, we can prove that any rate pair

$$(R_1, R_2) \in \mathbb{R}_{\mathrm{GIC}}^{[\mathrm{A}]}$$

is achievable for GIC-CM, where $\mathbb{R}_{\mathrm{GIC}}^{[\mathrm{A}]}$ denotes the convex set of (R_1, R_2) satisfying

$$\begin{aligned} 0 \le R_1 &\le \log\frac{1}{2}\left(1 + \frac{\beta_1 P_1}{1+\alpha_1^2\beta_2 P_2}\right) \\ &\quad - \frac{1}{2}\log\left(1 + \frac{\alpha_2^2\beta_1 P_1}{1+\lambda\beta_2 P_2}\right) \\ 0 \le R_2 &\le \frac{1}{2}\log\left[1 + \frac{(1-\lambda)\beta_2 P_2}{1+\alpha_2^2\beta_1 P_1 + \lambda\beta_2 P_2}\right] \\ &\quad - \frac{1}{2}\log[1 + (1-\lambda)\alpha_1^2\beta_2 P_2] \end{aligned} \quad (46)$$

for all β_1, β_2 pairs and power splitting parameter λ. Furthermore, the achievable region can be increased by reversing the roles of transmitters 1 and 2.

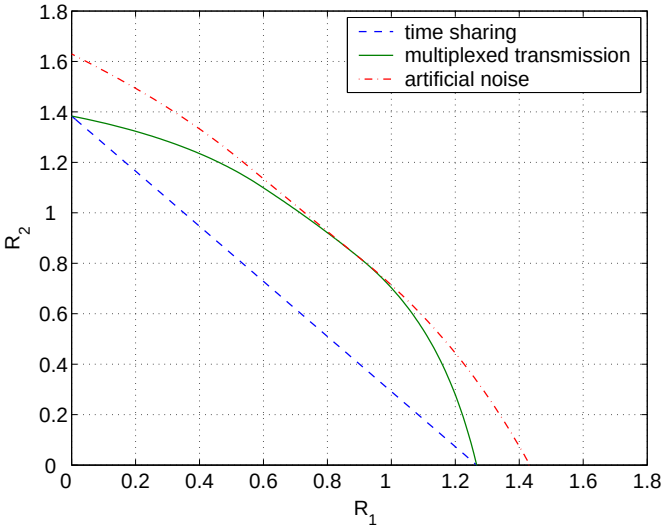

Fig. 4. achievability regions for the GIC-CM ($P_1 = 10$, $P_2 = 15$, and $\alpha_1 = \alpha_2 = 0.3$)

As shown in Figures 4 and 5, we compare the achievable region $\mathbb{R}_{\mathrm{GIC}}^{[\mathrm{T}]}$, $\mathbb{R}_{\mathrm{GIC}}^{[\mathrm{M}]}$, and $\mathbb{R}_{\mathrm{GIC}}^{[\mathrm{A}]}$ by numerical calculation, where we set

$$P_1 = 10, \ P_2 = 15, \ \alpha_1 = \alpha_2 = 0.3$$

for Figure 4 and

$$P_1 = 100, \ P_2 = 100, \ \alpha_1 = \alpha_2 = 0.2$$

for Figure 5. Both numerical computation results illustrate that that the artificial noise strategy allows communicating at a larger rate region compared with the time sharing and multiplexed transmission schemes.

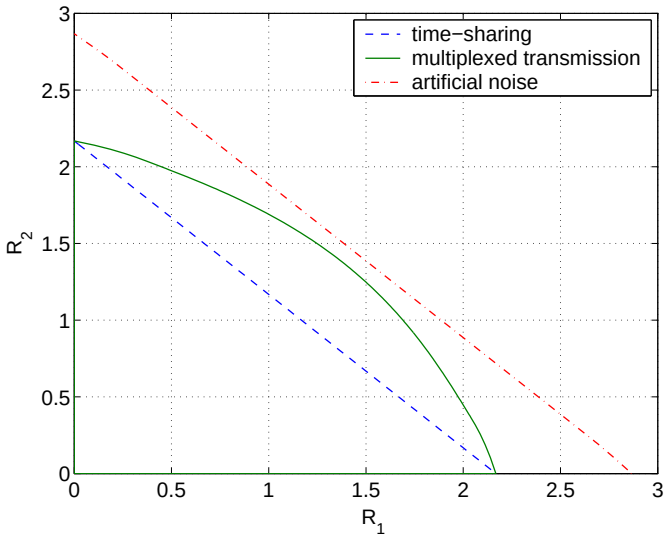

Fig. 5. achievability regions for the GIC-CM ($P_1 = 100$, $P_2 = 100$, and $\alpha_1 = \alpha_2 = 0.2$)

APPENDIX

A. Proof of Lemma 1

Proof: **(Lemma 1)** By the definition of Δ_1, we have

$$\begin{aligned}\Delta_1 &= I(V_1;Y_1|U) - I(V_1;Y_2|U)\\ &= I(V_1,V_2;Y_1|U) - I(V_2;Y_1|V_1,U) - I(V_1,V_2;Y_2|U)\\ &\quad + I(V_2;Y_2|V_1,U). \end{aligned} \tag{47}$$

Similarly,

$$\begin{aligned}\Delta_2 &= I(V_2;Y_2|U) - I(V_2;Y_1|U)\\ &= I(V_1,V_2;Y_2|U) - I(V_1;Y_2|V_2,U) - I(V_1,V_2;Y_2|U)\\ &\quad + I(V_1;Y_1|V_2,U). \end{aligned} \tag{48}$$

(47) and (48) imply that

$$\begin{aligned}\Delta_1 + \Delta_2 &= -I(V_2;Y_1|V_1,U) + I(V_2;Y_2|V_1,U)\\ &\quad - I(V_1;Y_2|V_2,U) + I(V_1;Y_1|V_2,U)\\ &= \Delta_4 + \Delta_3. \end{aligned} \tag{49}$$

Note that

$$\begin{aligned}2(\Delta_1 + \Delta_2) &= 2(\Delta_3 + \Delta_4)\\ &= (\Delta_1 + \Delta_4) + (\Delta_2 + \Delta_3)\end{aligned}$$

Hence,

$$\min[\Delta_1 + \Delta_4,\ \Delta_2 + \Delta_3] \le \Delta_1 + \Delta_2$$

and

$$\min[\Delta_1 + \Delta_4,\ \Delta_2 + \Delta_3] \le \Delta_3 + \Delta_4. \qquad \square$$

B. Proof of Theorem 4

Proof: **(Theorem 4)** Note that the switch channel is a special case of the interference channel. Hence, we prove that

$$\mathbb{R}_{\rm O}(\pi_{\rm IC-O}) = \mathbb{R}_{\rm IC-I}(\pi_{\rm IC-I})$$

for the SC-CM case. Comparing the outer bound (25) with the inner bound (15) and the distribution $\pi_{\rm IC-O}$ with $\pi_{\rm IC-I}$, we need to show that

$$I(W_1;W_2|U_i) = 0 \tag{50}$$

$$I(W_1;W_2|U_i,Y_{2,i}) = 0 \tag{51}$$

where $U_i = \{\mathbf{Y}_1^{i-1}, \tilde{\mathbf{Y}}_2^{i+1}\}$. We first prove the equality (50). Following the switch output definition (39), we have

$$\begin{aligned}&I(W_1;W_2|U_i)\\ &= I(W_1;W_2|\mathbf{Y}_1^{i-1},\tilde{\mathbf{Y}}_2^{i+1})\\ &= I(W_1;W_2|\mathbf{Y}_1^{i-1},\tilde{\mathbf{Y}}_2^{i+1},\mathbf{S}_1^{i-1},\tilde{\mathbf{S}}_2^{i+1})\\ &= \sum_{\mathbf{s}_1^{i-1}}\sum_{\tilde{\mathbf{s}}_2^{i+1}} P(\mathbf{S}_1^{i-1}=\mathbf{s}_1^{i-1},\ \tilde{\mathbf{S}}_2^{i+1}=\tilde{\mathbf{s}}_2^{i+1})\\ &\qquad \cdot I(W_1;W_2|\mathbf{Y}_1^{i-1},\tilde{\mathbf{Y}}_2^{i+1},\mathbf{s}_1^{i-1},\tilde{\mathbf{s}}_2^{i+1})\\ &= \sum_{\mathbf{s}_1^{i-1}}\sum_{\tilde{\mathbf{s}}_2^{i+1}} \left[\prod_{j=1}^{i-1} P(S_{1,j}=s_{1,j}) \prod_{k=i+1}^{n} P(S_{2,k}=s_{2,k})\right]\\ &\qquad \cdot I(W_1;W_2|\mathbf{Y}_1^{i-1},\tilde{\mathbf{Y}}_2^{i+1},\mathbf{s}_1^{i-1},\tilde{\mathbf{s}}_2^{i+1}). \end{aligned} \tag{52}$$

Now, for given $s_{t,i}$, the switch channel model (38) implies that $y_{t,i}$ only depend on the channel input $x_{s_{t,i},i}$. By using functional dependence graphs [9], we can easily verify that

$$I(W_1;W_2|\mathbf{Y}_1^{i-1},\tilde{\mathbf{Y}}_2^{i+1},\mathbf{s}_1^{i-1},\tilde{\mathbf{s}}_2^{i+1}) = 0$$

for fixed switch state information $\mathbf{s}_1^{i-1}$ and $\tilde{\mathbf{s}}_2^{i+1}$. Hence, (52) implies that $I(W_1;W_2|U_i)$. Following the same approach, we can prove the equality (51). Therefore, we have the desired result. $\square$

ACKNOWLEDGMENT

The authors would like to thank Shlomo Shamai (Shitz) and Gerhard Kramer for their useful comments about the proof.

REFERENCES

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

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

[3] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages," in *Proc. Allerton Conference on Commun. Contr. Computing*, Urbana, IL, USA, Sept 2006.

[4] A. B. Carleial, "Interference channels," *IEEE Trans. on Inf. Theory*, vol. 24, no. 1, p. 60, Jan. 1978.

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

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

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

[8] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. on Inf. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.
[9] G. Kramer, "Capacity results for the discrete memoryless network," *IEEE Trans. on Inf. Theory*, vol. 49, pp. 4–21, Jan. 2003.