On the Secrecy Capacity of 2-user Gaussian Interference Channel with Independent Secret Keys

Aditya Sinha, Parthajit Mohapatra, Jemin Lee and Tony Q.S. Quek

***Abstract*—This paper considers the problem of secure communication over a 2-user Gaussian interference channel (GIC) with shared key of finite rate between the transmitter-receiver pair with strong secrecy constraint at the receiver. The main contributions of the paper lies in obtaining a novel achievable scheme which uses a combination of *one-time pad*, *stochastic encoding* and *superposition based coding scheme*, and outer bound on the secrecy capacity region of the 2-user GIC. The main novelty of the derivation of the outer bound lies in the selection of the side-information to be provided to the receiver and using the secrecy constraints at the receiver. The results highlight the role of secret key in the encoding of messages to enhance the system performance in interference limited scenarios.**

I. Introduction

The performance of most of the wireless systems is limited by interference rather than by noise. Hence, in an interference limited environment, users may not be able to decode the interference to improve their own performance when there are secrecy constraints at the receivers. This in turn can reduce the performance of the system further. When the users also have shared key between the legitimate parties, the availability/non-availability of the shared key at the non-legitimate receiver can result in different performance of the system. The shared key need to be used in a judicious manner in the encoding of the message to enhance the system performance. This work aims at answering one of the fundamental questions on how to use the secret key in the encoding of the message in an interference limited environment. Here, the problem of secure communication is studied over a 2-user Gaussian interference channel (GIC) where the transmitter-receiver pair have a shared key of finite rate.

The problem of secure communication was studied from an information theoretic point of view for the first time in [1], where the legitimate parties shared a key which is unknown to the eavesdropper. The problem of secure communication over a noisy channel was studied in [2], where it was shown that it is possible to send information securely without using any key between the legitimate parties. The problem of secure communication over wiretap channel with shared secret key has also been studied in [3]–[5]. The problem of secure communication in other settings has been studied in [6]–[9].

Aditya Sinha & Parthajit Mohapatra are with the Indian Institute of Technology Kharagpur, India (e-mail: adityasinha@iitkgp.ac.in, parthajit@gssst.iitkgp.ernet.in).

Jemin Lee is with the Daegu Gyeongbuk Institute of Science and Technology, Daegu, Korea (e-mail: jmnlee@dgist.ac.kr).

Tony Q.S. Quek is with the Singapore University of Technology and Design, Singapore (e-mail: tonyquek@sutd.edu.sg).

It is also important to explore the optimal use of secret keys in multiuser scenarios as the non-availability of key at the non-legitimate nodes can degrade the system performance. The use of secret shared key in multiuser scenarios has been also been explored under different settings [10], [11]. However, the use of secret key in interference limited scenarios for secure communication is far from obvious. Therefore, this work considers the problem of secure communication over 2-user GIC, where the transmitter and receiver share a common key of finite rate. The main contribution of the paper lies in deriving new achievable schemes and outer bounds on the secrecy capacity of 2-user GIC for the weak/moderate interference regime. A new achievable scheme is proposed for the 2-user GIC with shared key using a combination of one-time pad, stochastic encoding and superposition coding. This paper presents a general result and one can obtain the achievable results for either one-time pad or stochastic encoding as special cases. Outer bound on the secrecy capacity region of the 2-user GIC with shared key is also derived. The main novelty of the derivation lies in the careful selection of the side-information to be provided to the receiver as well as using the secrecy constraints at the receivers.

II. System Model

We consider a two-user real Gaussian interference channel (GIC) as in [12], with independent secret key K_i, $i \in \{1,2\}$ being shared between the i^{th} transmitter and receiver pair. In this model, each transmitter wants to communicate with its corresponding receiver, while keeping the information secret from the other receiver. A pictorial representation of the model is shown in Fig. 1. The input-output relation is given by

$$y_1 = h_{11}x_1 + h_{21}x_2 + z_1 \;\&\; y_2 = h_{12}x_1 + h_{22}x_2 + z_2, \quad (1)$$

where $x_i \in \Re$ $(i = 1, 2)$ is subject to average power constraint $E[{x_i}^2] \leq P_i$. The noise processes are i.i.d. over time and are characterized by $z_i \sim \mathcal{N}(0,1)$. It is also assumed that global channel state information is available at all the nodes, where all channel coefficients h_{ij}, $i, j \in \{1,2\}$ are real. In this work, we will consider the weak/moderate interference regime, i.e. $h_{ii} > h_{ij}, i \neq j$.

Transmitter i intends to send independent message $W_i \in \{1, ..., 2^{nR_i}\}$ to the respective receiver in n channel uses over the GIC. Moreover, each transmitter-receiver pair has a shared key K_i of rate R_{K_i}. These keys are independent of each other as well as the messages and are unknown to

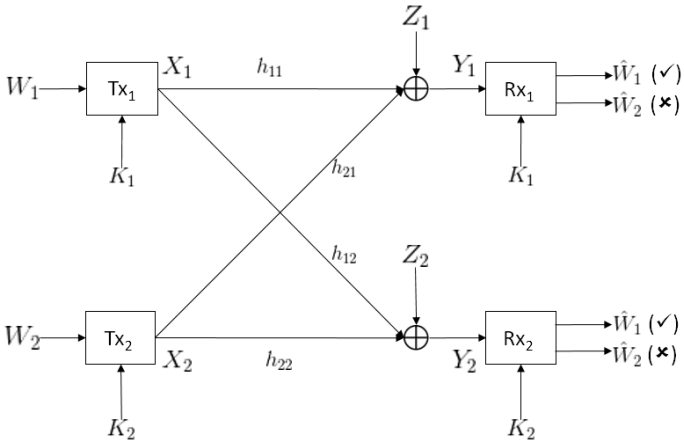


Fig. 1. Two-user GIC with independent keys.

the unintended receiver. The message-key pair (W_i, K_i) is uniformly distributed over $[1 : 2^{nR_i}] \times [1 : 2^{nR_{K_i}}]$.

For information theoretic secrecy, it is required to satisfy the strong secrecy constraint [13], which is defined as: $I(W_i; Y_j^n, K_j) \leq \epsilon_n$ $(i \neq j)$, where $\epsilon_n \to 0$ as $n \to \infty$.

III. Achievable Scheme and Main Result

Due to the secrecy constraint, receiver i is not allowed to decode the message of transmitter j $(i \neq j)$, which in turn can reduce the performance of the system further. When transmitter-receiver pair i share a key a priori, then it is possible to perform encoding at the transmitter i such that some part of the interference can be decoded and hence, canceled at receiver i, and at the same time secrecy can be guaranteed. Apart from this, it may be possible to send another message using stochastic encoding. This motivates us to split the message of transmitter i into two parts: the *common confidential message* (W_{ic}) and the *private message* (W_{ip}). The details of the encoding and decoding process are as follows.

A. Encoding

The message W_i $(i \in \{1, 2\})$ at transmitter i is split into private message $W_{ip} \in \mathcal{W}_{ip} \triangleq \{1, 2, \ldots, 2^{nR_{ip}}\}$ and common confidential message $W_{ic} \in \mathcal{W}_{ic} \triangleq \{1, 2, \ldots, 2^{nR_{ic}}\}$. The total rate corresponding to transmitter i is: $R_i = R_{ip} + R_{ic}$.

We propose the use of secret keys as a part of One Time Pad (OTP) to secure the common messages as follows:

$$W'_{1c} = W_{1c} \otimes K_1 \qquad W'_{2c} = W_{2c} \otimes K_2. \tag{2}$$

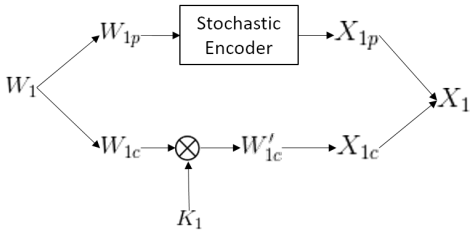


Fig. 2. The encoding scheme.

Here, the modulo-2 sum of the binary expansion of W_{ic} and K_i is used to obtain the encrypted message W'_{ic}. On the other hand, the private message is encoded using stochastic encoding. The details of the encoding process are as follows.

The transmitter i generates the codebooks as follows. For the common confidential message, transmitter i generates a codebook $\mathcal{C}_{ic}$ containing $2^{nR_{ic}}$ i.i.d. sequences of length n and its entries are i.i.d. random variables from $\mathcal{N}(0, P_{ic})$, where P_{ic} is the power used to send the common confidential message. The message $W_{ic} \in \mathcal{W}_{ic}$ is first encrypted using the key of size R_{iK} as described before. The encrypted message is denoted as W'_{ic}. For the private message, it generates $2^{n(R_{ip}+R'_{ip})}$ codewords of length n with i.i.d. $\mathcal{N}(0, P_{ip})$ entries, where P_{ip} is the power used to send the private message. The $2^{n(R_{ip}+R'_{ip})}$ codewords in the codebook $\mathcal{C}_{ip}$ are randomly grouped into $2^{nR_{ip}}$ bins, with each bin containing $2^{nR'_{ip}}$ codewords. To send W_{ip}, the message selects the bin and the transmitter i selects $w'_{ip} \in \mathcal{W}'_{ip} \triangleq \{1, 2, \ldots, 2^{nR'_{ip}}\}$ randomly from the bin, transmitting the codeword $\mathbf{X}_{ip}^N(w_{ip}, w'_{ip})$. Finally, transmitter i sends

$$\mathbf{X}_i^n(W'_{ic}, W_{ip}, W'_{ip}) = \mathbf{X}_{ic}^n(W'_{ic}) + \mathbf{X}_{ip}^n(W_{ip}, W'_{ip}), \tag{3}$$

where $P_{ip} + P_{ic} \leq P_i$, and $\mathbf{X}_{ic}^n$ and $\mathbf{X}_{ip}^n$ correspond to the codeword of the common confidential and private messages of transmitter i, respectively.

B. Decoding

Due to secrecy constraint, receiver cannot decode the interference to cancel its effect and this in turn can increase the noise floor at the receiver. To overcome this problem, apart from its own message, receiver i is also allowed to decode and remove the common encrypted message of the unintended receiver $W'_{jc}(j \neq i)$, while treating private message W_{jp}, $j \neq i$ as noise. In other words, at receiver 1, X_{1p}, X_{1c} and X_{2c} form a multiple access channel (MAC_1), with X_{2p} being treated as noise. A similar situation at receiver 2 gives rise to MAC_2. The joint typical decoder at receiver i outputs $\hat{W}_{ip}$, $\hat{W}'_{ic}$ and $\hat{W}'_{jc}$ $(j \neq i)$. Using the key K_i, the receiver i decodes the common confidential message $\hat{W}_{ic}$. It is not difficult to see that although receiver i can decode $\hat{W}'_{jc}$, but it cannot determine W_{jc} as the receiver does not have access to key K_j. Note that receiver i cannot decode the private message of transmitter j due to stochastic encoding performed at transmitter j. However, in stochastic encoding, some part of the rate is sacrificed in confusing the unintended receiver. The achievable result is stated in the following theorem.

Theorem 1. *For the GIC with independent shared key between the transmitter i and receiver i, and the secrecy constraint at the receivers, the following secrecy rate region is achievable for the weak/moderate interference regime:*

$$\begin{aligned} R_i &\leq I(X_i; Y_i | X_{jc}) - R'_{ip}, \\ R_i &\leq I(X_i; Y_i | X_{ic}, X_{jc}) + \min\{I(X_{ic}; Y_j | X_j), R_{K_i}\} - R'_{ip}, \\ R_i + R_j &\leq I(X_i; Y_i | X_{ic}, X_{jc}) + I(X_j, X_{ic}; Y_j | X_{jc}) \\ &\quad + \min\{I(X_{jc}; Y_j), R_{K_j}\} - R'_{ip} - R'_{jp}, \end{aligned}$$

$$R_i + R_j \le I(X_i, X_{jc}; Y_i|X_{ic}) + I(X_j, X_{ic}; Y_j|X_{jc}) - R'_{ip} - R'_{jp},$$
$$R_i + 2R_j \le I(X_i, X_{jc}; Y_i|X_{ic}) + I(X_j; Y_j|X_{ic}, X_{jc}) + I(X_j, X_{ic}; Y_j) - R'_{ip} - 2R'_{jp}, \quad (4)$$

where $i \in \{1, 2\}$ and $j \neq i$, with the equivocation rates being bound as

$$R'_{1p} \ge I(X_1; Y_1|X_2, X_{1c}), \;\; R'_{2p} \ge I(X_2; Y_2|X_1, X_{2c}). \quad (5)$$

Proof. The proof involves probability of error analysis and equivocation computation to show the secrecy of the message. The main novelty of the proof lies in combining the independent key with stochastic encoding. The decoding is based on joint typical set decoding. Note that due to symmetry of the problem, it is sufficient to consider only receiver 1. Consider the following event

$$E_{ijkl} = \{(X^n_{1p}(i, j), X^n_{1c}(k), X^n_{2c}(l), Y^n_1) \in A^{(n)}_\epsilon\}, \quad (6)$$

Since codebook construction is symmetric, without loss in generality, we can assume that $(i, j, k, l) = (1, 1, 1, 1)$ was sent. Then, the error probability can be written as follows:

$$P^{(n)}_e = P(E^c_{1111} \bigcup \cup_{(i,j,k,l)\neq(1,1,1,1)} E_{ijkl}). \quad (7)$$

Following along a similar analysis as done in [14, Sec. 15.3.1], for receiver 1, we get

$$R_{1c} \le I(X_{1c}; Y_1|X_{1p}, X_{2c}), \qquad R_{2c} \le I(X_{2c}; Y_1|X_{1p}, X_{1c}),$$
$$R_{1c} + R_{2c} \le I(X_{1c}, X_{2c}; Y_1|X_{1p}),$$
$$R_{1p} + R'_{1p} \le I(X_{1p}; Y_1|X_{1c}, X_{2c}),$$
$$R_{1p} + R'_{1p} + R_{1c} \le I(X_{1p}, X_{1c}; Y_1|X_{2c}),$$
$$R_{1p} + R'_{1p} + R_{2c} \le I(X_{1p}, X_{2c}; Y_1|X_{1c}),$$
$$R_{1p} + R'_{1p} + R_{1c} + R_{2c} \le I(X_{1p}, X_{1c}, X_{2c}; Y_1),$$
$$R_{1c} \le R_{K_1}, \qquad R_{2c} \le R_{K_2}, \quad (8)$$

where the last inequality is due to key rate limits. For receiver 2, we simply interchange the indices from 1 to 2 and vice-versa in the above equations. Using the relation $R_i = R_{ip} + R_{ic}$ and Fourier-Motzkin elimination [15], the rate region in (4) is obtained.

To determine R'_{1p}, consider the following:

$$\begin{aligned} I(W_1; Y^n_2, K_2) &\overset{(a)}{=} I(W_{1c}; Y^n_2, K_2) + I(W_{1p}; Y^n_2, K_2|W_{1c}) \\ &\overset{(b)}{=} I(W_{1p}; Y^n_2, K_2|W_{1c}) \\ &\overset{(c)}{\le} H(W_{1p}|W_{1c}) - H(W_{1p}|Y^n_2, K_2, W_{1c}, X^n_2) \\ &\overset{(d)}{=} I(W_{1p}; S^n_2), \end{aligned} \quad (9)$$

where (a) is obtained using the fact that $W_1 = (W_{1p}, W_{1c})$ and chain rule for mutual information; (b) is due to the fact that W_{1c} is independent of (Y^n_2, K_2) due to one-time padding performed at transmitter 1; (c) is due to the fact that conditioning cannot increase the entropy; and (d) is obtained using the fact that W_{1p} is independent of W_{1c}, X^n_2 and K_2 and $S^n_2 \triangleq h_{12}X^n_{1p} + Z^n_2$.

This is effectively reducing the GIC to a hypothetical wiretap channel ($W_{1p} \to Y'^n_1 \to S^n_2$), where Y'^n_1 is the output at receiver 1 after decoding and canceling the message from transmitter 1 and the encrypted message of transmitter 2 and $S^n_2 \triangleq h_{12}X^n_{1p} + Z^n_2$ is the modified output at receiver 2 (which is the eavesdropper in the hypothetical wiretap channel). Using the approach in [13], one can show that $I(W_{1p}; S^n_2) \to 0$ as $n \to \infty$ if the conditions of (5) hold true. □

Using the above result, the following lower bound on the secrecy rate region is obtained. For simplification, we have considered symmetric GIC ($h_{ii} = h_d$ and $h_{ij} = h_c$, $i \neq j$) with following codebook parameters: $P_1 = P_2 = P$, $P_{ic} = P_c$, $P_{ip} = P_p$ and $P_p + P_c \le P$, and $R_{K_1} = R_{K_2} = R_K$.

Corollary 1. *Using the result in Theorem 1, for $h_d \ge h_c$, the following rate region is achievable*

$$R_s = \textit{Convex closure of} \bigcup_{0\le(\beta,\lambda)\le 1} R^{IC}_s(\beta, \lambda), \quad (10)$$

where $R^{IC}_s(\beta, \lambda) = \{(R_1, R_2) : R_1 \ge 0, R_2 \ge 0,$

$$R_i \le 0.5 \log\left(1 + \frac{h^2_d \beta P}{1 + h^2_c P_p}\right) - R'_p,$$
$$R_i \le 0.5 \log\left(1 + \frac{h^2_d P_p}{1 + h^2_c P_p}\right) + \min\left\{R_K, 0.5 \log\left(1 + \frac{h^2_c P_c}{1 + h^2_c P_p}\right)\right\} - R'_p,$$
$$R_i + R_j \le \min\left\{0.5 \log\left(1 + \frac{h^2_d P_c}{1 + h^2_d P_p + h^2_c \beta P}\right), R_K\right\} + 0.5 \log\left(1 + \frac{h^2_d P_p}{1 + h^2_c P_p}\right) + 0.5 \log\left(1 + \frac{h^2_d P_p + h^2_c P_c}{1 + h^2_c P_p}\right) - 2R'_p,$$
$$R_i + R_j \le \log\left(1 + \frac{h^2_d P_p + h^2_c P_c}{1 + h^2_c P_p}\right) - 2R'_p,$$
$$R_i + 2R_j \le 0.5 \log\left(1 + \frac{h^2_d P_p + h^2_c P_c}{1 + h^2_c P_p}\right) + 0.5 \log\left(1 + \frac{h^2_d P_p}{1 + h^2_c P_p}\right) + 0.5 \log\left(1 + \frac{h^2_d P + h^2_c P_c}{1 + h^2_c P_p}\right) - 3R'_p\}, \quad (11)$$

where $i \in \{1, 2\}$ and $j \neq i$, $R'_p = 0.5 \log(1 + h^2_c P_p)$, $P_p \triangleq \lambda\beta P$ and $P_c \triangleq (1 - \lambda)\beta P$.

In the following, the achievable result using one-time pad (without decoding the other user's message) and wiretap coding when key is used as a fictitious message are presented in the following theorems.

Theorem 2. *The achievable rate region for symmetric GIC with full decoding using One Time Pad, for $h_d \ge h_c$, is given by*

$$R_s = \textit{Convex closure of} \bigcup_{0\le\beta\le 1} R^{IC}_s(\beta),$$
$$\textit{where } R^{IC}_s(\beta) = \{\, (R_1, R_2) : R_i \ge 0, \; i \in \{1, 2\}$$

$$R_i \leq \min\left\{0.5\log\left(1+\frac{h_d^2\beta P_i}{1+h_c^2\beta P_j}\right), R_{K_i}\right\}, j\neq i\} \quad (12)$$

Proof. The above result is obtained using the result in [15, Theorem 22.3], where legitimate parties share a secret key and the communication takes place over a noisy channel. Although the receiver and eavesdropper receive the same output, it's not difficult to show that one can use this as an achievable result for the system model considered in this paper. □

Theorem 3. *The achievable rate region for symmetric GIC with use of key as a fictitious message, for $h_d \geq h_c$, is given by*

$$R_s = \textit{Convex closure of} \bigcup_{0\leq(\beta,\rho)\leq 1} R_s^{IC}(\beta),$$

$$\textit{where } R_s^{IC}(\beta) = \{(R_1,R_2): R_1\geq 0, R_2\geq 0,$$
$$R_i \leq \frac{\rho_i}{2}\min\left\{\log\left(1+\frac{h_d^2\beta P_i}{\rho_i}\right), \log\left(1+\frac{h_d^2\beta P_i}{\rho_i}\right) - \log\left(1+\frac{h_c^2\beta P_i}{\rho_i}\right)+R_{K_i}\right\}, \quad i\in\{1,2\}\} \quad (13)$$

where $\rho_1=\rho$, $\rho_2=1-\rho$ and $0<\rho<1$.

Proof. This result is an extension of [7] to the symmetric GIC and the proof has been omitted for brevity. □

IV. Outer Bound

In this section, an outer bound on the symmetric secrecy capacity of the 2-user Gaussian symmetric IC with shared secret key between transmitter i and receiver i is obtained. One of the novelties of the proof lies in the choice of the side information that needs to be provided to the receivers as well as in the judicious use of the secrecy constraints at the receivers. The outer bound is stated in the following theorem.

Theorem 4. *The symmetric secrecy capacity of the 2-user GIC with independent secret keys is upper bounded as:*

$$R \leq \frac{0.5}{3}\log\left(1+SNR+INR\right)+\frac{0.5}{3}\log\det\left(\Sigma_{\bar{y}|\bar{s}}\right)+\frac{R_{K1}}{3},$$

where $\Sigma_{\bar{y}|\bar{s}} \triangleq \Sigma_{\bar{y}} - \Sigma_{\bar{y},\bar{s}}\Sigma_{\bar{s}}^{-1}\Sigma_{\bar{y},\bar{s}}^T$, $\Sigma_{\bar{s}} \triangleq \begin{bmatrix} 1+INR & 0 \\ 0 & 1+INR \end{bmatrix}$,
$\Sigma_{\bar{y}} \triangleq \begin{bmatrix} 1+SNR+INR & 2\sqrt{SNRINR} \\ 2\sqrt{SNRINR} & 1+SNR+INR \end{bmatrix}$,
$\Sigma_{\bar{y},\bar{s}} \triangleq \begin{bmatrix} \sqrt{SNRINR} & INR \\ INR & \sqrt{SNRINR} \end{bmatrix}$, $SNR \triangleq h_d^2P$, $INR \triangleq h_c^2P$.

Proof. Using Fano's inequality, rate of user 1 is upper bounded as follows:

$$\begin{aligned} nR_1 &\leq I(W_1;\mathbf{y}_1^n,K_1)+n\epsilon_n \overset{(a)}{=} I(W_1;\mathbf{y}_1^n|K_1)+n\epsilon_n,\\ &\overset{(b)}{\leq} h(\mathbf{y}_1^n)-h(\mathbf{y}_1^n|K_1,W_1,\mathbf{X}_1^n)+n\epsilon_n,\\ &= h(\mathbf{y}_1^n)-h(h_c\mathbf{X}_2^n+\mathbf{z}_1^n)+n\epsilon_n,\\ &\overset{(c)}{=} h(\mathbf{y}_1^n)-h(h_c\mathbf{X}_2^n+\tilde{\mathbf{z}}_1^n)+n\epsilon_n,\\ \text{or } h(\tilde{\mathbf{s}}_2^n) &\leq h(\mathbf{y}_1^n)-nR_1+n\epsilon_n, \tilde{\mathbf{s}}_2^n \triangleq h_c\mathbf{X}_2^n+\tilde{\mathbf{z}}_1^n, \end{aligned} \quad (14)$$

where (a) is obtained using chain rule for mutual information and the fact that the key K_1 is independent of the message W_1; (b) is obtained using the fact that conditioning (removing conditioning) can not increase (decrease) the differential entropy; and (c) is obtained using the fact that the secrecy capacity region of an IC with confidential messages is invariant under any joint channel noise distribution $P(z_1,z_2)$ that leads to the same marginal distributions $P(z_1)$ and $P(z_2)$.

Similarly, one can show that

$$h(\tilde{\mathbf{s}}_1^n) \leq h(\mathbf{y}_2^n)-nR_2+n\epsilon_n, \tilde{\mathbf{s}}_1^n \triangleq h_c\mathbf{X}_1^n+\tilde{\mathbf{z}}_2^n, \quad (15)$$

Above equations are obtained without using the secrecy constraints at the receiver. In the following outer bound, secrecy constraint at receiver has also been used. Consider the following:

$$\begin{aligned} nR_1 &\leq I(W_1;\mathbf{y}_1^n,K_1)+n\epsilon_n \leq I(W_1;\mathbf{y}_1^n,K_1,\mathbf{y}_2^n)+n\epsilon_n,\\ &\overset{(a)}{\leq} I(W_1;\mathbf{y}_1^n,K_1|\mathbf{y}_2^n)+n\epsilon_n,\\ &= h(\mathbf{y}_1^n|\mathbf{y}_2^n)-h(\mathbf{y}_1^n|\mathbf{y}_2^n,W_1)+I(W_1;K_1|\mathbf{y}_1^n,\mathbf{y}_2^n)+n\epsilon_n,\\ &\overset{(b)}{=} h(\mathbf{y}_1^n,\mathbf{y}_2^n)-h(\mathbf{y}_2^n)-h(\mathbf{y}_1^n|\mathbf{y}_2^n,W_1)+\\ &\qquad I(W_1;K_1|\mathbf{y}_1^n,\mathbf{y}_2^n)+n\epsilon_n,\\ &\overset{(c)}{=} h(\mathbf{y}_1^n,\mathbf{y}_2^n,\tilde{\mathbf{s}}_1^n,\tilde{\mathbf{s}}_2^n)-h(\tilde{\mathbf{s}}_1^n,\tilde{\mathbf{s}}_2^n|\mathbf{y}_1^n,\mathbf{y}_2^n)-h(\mathbf{y}_2^n)-\\ &\qquad h(\mathbf{y}_1^n|\mathbf{y}_2^n,W_1)+I(W_1;K_1|\mathbf{y}_1^n,\mathbf{y}_2^n)+n\epsilon_n,\\ &= I(\tilde{\mathbf{s}}_1^n,\tilde{\mathbf{s}}_2^n;\mathbf{y}_1^n,\mathbf{y}_2^n)+h(\mathbf{y}_1^n,\mathbf{y}_2^n|\tilde{\mathbf{s}}_1^n,\tilde{\mathbf{s}}_2^n)-h(\mathbf{y}_2^n)-\\ &\qquad h(\mathbf{y}_1^n|\mathbf{y}_2^n,W_1)+I(W_1;K_1|\mathbf{y}_1^n,\mathbf{y}_2^n)+n\epsilon_n,\\ &\overset{(d)}{\leq} h(\tilde{\mathbf{s}}_1^n,\tilde{\mathbf{s}}_2^n)-h(\tilde{\mathbf{s}}_1^n,\tilde{\mathbf{s}}_2^n|\mathbf{y}_1^n,\mathbf{y}_2^n,\mathbf{X}_1^n,\mathbf{X}_2^n)+h(\mathbf{y}_1^n,\mathbf{y}_2^n|\tilde{\mathbf{s}}_1^n,\tilde{\mathbf{s}}_2^n)\\ &\quad -h(\mathbf{y}_2^n)-h(\mathbf{y}_1^n|\mathbf{y}_2^n,W_1)+I(W_1;K_1|\mathbf{y}_1^n,\mathbf{y}_2^n)+n\epsilon_n,\\ &\overset{(e)}{\leq} h(\tilde{\mathbf{s}}_1^n)+h(\tilde{\mathbf{s}}_2^n)-h(\tilde{\mathbf{z}}_1^n,\tilde{\mathbf{z}}_2^n)+h(\mathbf{y}_1^n,\mathbf{y}_2^n|\tilde{\mathbf{s}}_1^n,\tilde{\mathbf{s}}_2^n)\\ &\quad -h(\mathbf{y}_2^n)-h(\mathbf{y}_1^n|\mathbf{y}_2^n,W_1)+H(K_1)+n\epsilon_n, \end{aligned} \quad (16)$$

where (a) is obtained using the secrecy constraint at receiver 2, i.e., $I(W_1;\mathbf{y}_2^n) \leq I(W_1;\mathbf{y}_2^n,K_2) \leq n\epsilon_n$; (b) and (c) are obtained using the chain rule for joint entropy; (d) is obtained using the fact that conditioning cannot increase the conditional entropy; and (e) is obtained using the fact that removing conditioning cannot decrease the conditional entropy.

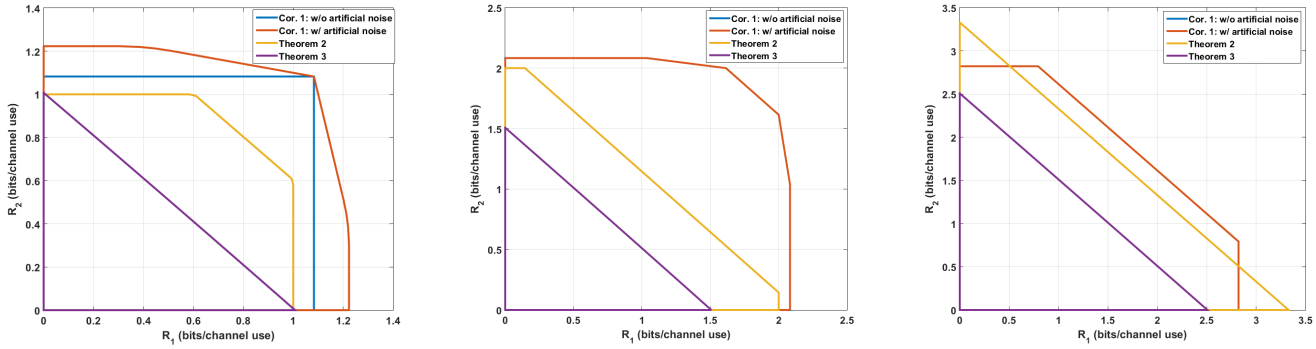
Using (14) and (15) in (16), following bound is obtained

$$\begin{aligned} n(2R_1+R_2) \leq\ & h(\mathbf{y}_1^n)+h(\mathbf{y}_1^n,\mathbf{y}_2^n|\tilde{\mathbf{s}}_1^n,\tilde{\mathbf{s}}_2^n)+nR_{K_1}-h(\tilde{\mathbf{z}}_1^n)\\ &-h(\tilde{\mathbf{z}}_2^n)-h(\mathbf{z}_1^n)+n\epsilon_n, \end{aligned}$$

Using the approach used in [12], the outer bound can be obtained from the above equation. □

V. Results & Discussion

In Fig. 3, the symmetric rate region in Corollary 1 is plotted with and without transmission of artificial noise. Note that the artificial noise transmission scheme is similar to that in [9]. The achievable result in Theorems 2 and 3 are also plotted. It can be noticed that the proposed scheme in Corollary 1 performs the best compared to other schemes when R_K=1 and R_K=2. This gain in rate is due to the fact that receiver can decode some part of interference without violating the secrecy constraint and stochastic encoding also allows to send



(a) (b) (c)

Fig. 3. Rate regions with $P = 100$, $h_d = 1$, $h_c = 0.7$; (a) $R_K = 1$, (b) $R_K = 2$ & (c) $R_K = 4$.

the private message securely. In this case, the performance is primarily limited by the key-rate. When R_K=4, the achievable scheme in Theorem 2 perform better when one of the users achieve low rate. In this case, the performance of the system is primarily limited by interference. It can also be noticed that transmission of artificial noise is useful when the key size is relatively small.

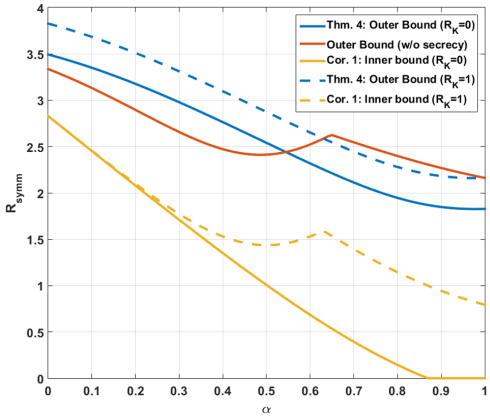


Fig. 4. Comparison of bounds on the symmetric secrecy capacity if the 2-user GIC with $P = 200$ & $h_d = 1$ for different key rates.

In Fig. 4, the symmetric secrecy rate in Corollary 1 is plotted against $\alpha \triangleq \frac{\log \text{INR}}{\log \text{SNR}}$ for different values of R_K. The outer bound in Theorem 4 is plotted along with the outer bound for GIC without secrecy constraint [12, Theorem 3]. One can see that with increase in the key rate, the performance improves in the later part of the weak interference regime ($0 \leq \alpha \leq 0.5$) and moderate interference regime. The proposed outer bound is found to be tight in the moderate interference regime when the key size is small.

VI. Conclusion

This work considered the problem of managing interference and ensuring secrecy in 2-user GIC, when the transmitter-receiver pair shared a key of finite rate. The paper proposed a novel achievable scheme which uses a combination of one-time pad, superposition coding and stochastic encoding. The paper also derives an outer bound on the symmetric secrecy capacity using the secrecy constraint at the receiver and providing side-information to the receiver in a careful manner. It is found that, in the moderate interference regime ($0.5 \leq \alpha \leq 1$), increase in the key rate can improve the performance of the system significantly. However, when the key rate is arbitrarily high, the performance of the system is limited by interference. Developing achievable schemes and outer bounds for other interference regimes is an interesting avenue for future work.

References

[1] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[2] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1334–1387, Oct. 1975.

[3] H. Yamamoto, "Rate-distortion theory for the shannon cipher system," *IEEE Transactions on Information Theory*, vol. 43, no. 3, pp. 827–835, May 1997.

[4] N. Merhav, "Shannon's secrecy system with informed receivers and its application to systematic coding for wiretapped channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2723–2734, June 2008.

[5] W. Kang and N. Liu, "Wiretap channel with shared key," in *2010 IEEE Information Theory Workshop*, Aug 2010, pp. 1–5.

[6] D. Gunduz, D. R. Brown, and H. V. Poor, "Secret communication with feedback," in *2008 International Symposium on Information Theory and Its Applications*, Dec 2008, pp. 1–6.

[7] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y. H. Kim, "Wiretap channel with secure rate-limited feedback," *IEEE Transactions on Information Theory*, vol. 55, no. 12, pp. 5353–5361, Dec 2009.

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

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

[10] R. F. Schaefer, A. Khisti, and H. Boche, "On the use of secret keys in broadcast channels with receiver side information," in *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, May 2014, pp. 1582–1586.

[11] R. F. Schaefer, A. Khisti, and H. V. Poor, "How to use independent secret keys for secure broadcasting of common messages," in *2015 IEEE International Symposium on Information Theory (ISIT)*, June 2015, pp. 1971–1975.

[12] R. H. Etkin, D. N. C. Tse, and H. Wang, "Gaussian interference channel capacity to within one bit," *IEEE Transactions on Information Theory*, vol. 54, no. 12, pp. 5534–5562, Dec 2008.

[13] M. R. Bloch and J. N. Laneman, "Strong secrecy from channel resolvability," *IEEE Transactions on Information Theory*, vol. 59, no. 12, pp. 8077–8098, Dec 2013.

[14] T. M. Cover and J. A. Thomas, *Elements of Information Theory 2nd Edition (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience, July 2006.

[15] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge University Press, 2011.