On the Secrecy Capacity Region of the Two-User Symmetric Z Interference Channel With Unidirectional Transmitter Cooperation

Parthajit Mohapatra, Chandra R. Murthy, *Senior Member, IEEE*, and Jemin Lee, *Member, IEEE*

***Abstract*— In this paper, the role of unidirectional limited rate transmitter cooperation is studied for the two-user symmetric Z interference channel (Z-IC) with secrecy constraints at the receivers, in achieving two conflicting goals simultaneously: *mitigating interference* and *ensuring secrecy*. First, the problem is studied under the linear deterministic model. A novel scheme for partitioning the encoded messages and outputs based on the relative strengths of the signal and interference is proposed. The partitioning reveals the side information that needs to be provided to the receiver and facilitates the development of tight outer bounds on the secrecy capacity region. The achievable schemes for the deterministic model use a fusion of cooperative precoding and transmission of a jamming signal. The optimality of the proposed scheme is established for the deterministic model for all possible parameter settings. The insights obtained from the deterministic model are used to derive inner and outer bounds on the secrecy capacity region of the two-user Gaussian symmetric Z-IC. The achievable scheme for the Gaussian model uses stochastic encoding in addition to cooperative precoding and transmission of a jamming signal. For the Gaussian case, the secure sum generalized degrees of freedom (GDOF) is characterized and shown to be optimal for the weak/moderate interference regime. It is also shown that the secure sum capacity lies within 2 bits/s/Hz of the outer bound for the weak/moderate interference regime for all values of the capacity of the cooperative link. Interestingly, in the deterministic model, it is found that there is no penalty on the capacity region of the Z-IC due to the secrecy constraints at the receivers in the weak/moderate interference regimes. Similarly, it is found that there is no loss in the secure sum GDOF for the Gaussian case due to the secrecy constraint at the receiver, in the weak/moderate interference regimes. The results highlight the importance of cooperation in facilitating secure communication over the Z-IC.**

***Index Terms*— Z interference channel, information theoretic secrecy, deterministic approximation, cooperation.**

Manuscript received April 12, 2016; revised August 20, 2016; accepted October 2, 2016. Date of publication October 26, 2016; date of current version January 18, 2017. This work was supported in part by the Aerospace Network Research Consortium and in part by the Ministry of Electronics and Information Technology, Government of India. This work was presented in part at the 2015 Proc. ISIT [1]. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Liang Xiao.

P. Mohapatra was with the Department of ECE, Indian Institute of Science, Bengaluru 560012, India. He is now with the G. S. Sanyal School of Telecommunications, IIT Kharagpur, Kharagpur 721302, India (e-mail: parthajit@gssst.iitkgp.ernet.in).

C. R. Murthy is with the ECE Department, Indian Institute of Science, Bengaluru 560012, India (e-mail: cmurthy@ece.iisc.ernet.in).

J. Lee is with the Department of ICE, Daegu Gyeongbuk Institute of Science and Technology, Daegu 42988, South Korea (e-mail: jmnlee@dgist.ac.kr).

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

Digital Object Identifier 10.1109/TIFS.2016.2622007

I. Introduction

THE role of cooperation between the transmitters/receivers in interference limited scenarios has been studied extensively in the context of communication reliability. However, the effect of the cooperation on communication secrecy has not been well explored, and the ability to cooperate can have a very different effect on the achievable rates when there is a secrecy constraint [2], [3]. In a system operating under secrecy constrains at the receivers, the receivers cannot enhance their own rates by decoding and canceling the interference, since this does not preserve the communication secrecy. This leads to the following fundamental questions: (a) how much interference can be mitigated through rate-limited transmitter cooperation, when there are secrecy constraints at receivers? (b) what is the corresponding gain in the rate achieved by the cooperation between transmitters? Answering these questions helps in understanding the role of cooperation in managing interference and ensuring secrecy in multiuser scenarios.

The effect of transmitter cooperation on the secrecy capacity is closely related to the underlying channel model. The channel model considered in this paper is the Z-IC [4], [5]. In the Z-IC, only one of the two transmitters causes interference at the unintended receiver, and is also referred to as a partially connected IC in [6]. As a practical example, the Z-IC can model a 2-tier network, where the macro cell user is close to the edge of the femtocell while the femtocell user is close to the femto base station (BS). Since the macro BS can typically support higher complexity transmission schemes, it could use the side information received from the femto BS to precode its data to improve its own rate and simultaneously ensure secrecy at the femtocell user. At the receivers, the macro cell user could experience significant interference from the femtocell BS, while the femtocell user receives little or no interference from the macro BS, leading to the Z-IC as the appropriate model for the system. Hence, answering the aforementioned questions in the context of the Z-IC can lead to useful insights in the 2-tier cellular network scenario mentioned above.

A. Prior Work

The IC has been studied extensively with and without secrecy constraints at the receivers under different settings [7]–[10]. However, the capacity region of the 2-user Gaussian IC has remained an open problem, even without

secrecy constraint, except for some specific cases like the strong interference regime and the very strong interference regime [11], [12]. The Han-Kobayashi (HK) scheme proposed in [13] is the best known achievable region for the IC.

It has been shown that cooperation between the transmitters or receivers in the case of IC can improve the overall performance of the system, when there is no secrecy constraint at the receivers [14]–[17]. However, the effect of cooperation on managing interference and ensuring secrecy in interference limited scenarios is not well understood. In [2], it has been shown that, with cooperation, it is possible to achieve nonzero secrecy rate, even when the unintended receiver has a better channel compared to the legitimate receiver. The effect of cooperation on the achievable rates for other communication models with secrecy constraints can be found in [18]–[21].

Z-IC Without Secrecy and Without Cooperation: In [4], lower bounds on the capacity region of the Gaussian Z-IC for the weak and moderate interference regimes are derived. In [22], it is shown that superposition encoding with partial decoding is optimal for a certain class of Z-IC. A simple variant of the HK encoding scheme was proposed in [23] for the Gaussian Z-IC and a class of mixed IC.

Z-IC Without Secrecy and With Cooperation: The role of cooperation in the Z-IC without the secrecy constraint has been investigated in [24]–[29]. In [23] and [28], a cognitive Z-IC is considered, where the non-interfering user (primary user) shares its codeword with the interfering user (secondary user). It is shown that a combination of superposition coding and dirty paper coding can achieve capacity over a certain subset of the strong interference regime. The capacity region of the cognitive Z-IC is established in the very strong interference regime in [25]. In [26], both the encoders cooperate through noiseless links with finite capacities and the sum capacity of the channel is characterized to within 2 bits of the outer bound.

Z-IC With Secrecy and Without Cooperation: In [30], the Z-IC model is considered with secrecy constraints at the receivers and achievable schemes are obtained for the deterministic and the Gaussian model in the weak/moderate interference regime. For the deterministic model, the secrecy capacity region is characterized. In [31], it is shown that when the non-interfering transmitter is constrained to use a deterministic encoder, the capacity region can reduce.

B. Contributions

This work considers the 2-user symmetric Z-IC with unidirectional transmitter cooperation via a rate-limited link from transmitter 2 (which causes interference) to transmitter 1 (which does not cause interference), and with secrecy constraints at the receivers. The key challenge here is to devise techniques for simultaneously canceling interference and guaranteeing secrecy. First, the problem is solved under the deterministic approximation of the channel. Using the results in the deterministic model, an achievable scheme and outer bounds are derived for the Gaussian channel model.

One of the key techniques used in the achievable scheme for both the models is *cooperative precoding* performed at transmitter 1, which cancels interference at receiver 1 and thereby simultaneously ensures secrecy. However, the amount of the interference that can be canceled at the receiver is limited by the rate of the cooperative link. In the deterministic model, transmission of a jamming signal along with interference cancelation is required to achieve the capacity. On the other hand, the achievable scheme for the Gaussian model uses stochastic encoding in addition to cooperative precoding and transmission of a jamming signal. Derivation of outer bound requires judicious use of the secrecy constraint at receiver, along with careful selection of the side information to be provided to the receivers. In particular, the cooperation between the transmitters makes the encoded messages dependent, which makes derivation of the outer bounds even more difficult.

The main contributions of the paper are as follows:

1. Outer bounds on the secrecy capacity of the symmetric Z-interference channel with unidirectional transmitter cooperation are derived. The key novelty in deriving the outer bounds is the choice of side information to be provided to the receiver(s) and the use of the secrecy constraints at the receivers in a judicious manner. To elaborate, a novel partitioning of the encoded messages and outputs is proposed for the deterministic model based on the strength of interference and signal. Further, this partitioning also helps to bound or simplify the entropy terms that are difficult to evaluate due to the dependence between the encoded messages.

2. An achievable scheme is proposed for the system under consideration, which uses a combination of transmission of random bits and cooperative precoding to cancel the interference at the unintended receiver. The cooperative precoding offers two benefits simultaneously: it cancels interference and ensures secrecy.

3. It is shown that, for all values C and over all interference regimes, the inner and outer bounds derived on the secrecy capacity region match, thus yielding the capacity of the deterministic symmetric Z-IC with unidirectional transmitter cooperation and secrecy constraints. It is also shown that the capacity region of the deterministic symmetric Z-IC does not enlarge if the perfect secrecy constraint at the receiver is replaced with the weak or strong notion of secrecy.

4. An achievable scheme is proposed for the Gaussian case, which uses a combination of stochastic encoding, interference cancelation and artificial noise transmission. The novelty in the achievable scheme lies in fusing stochastic encoding with interference cancelation. The achievable rate of secure communication is analyzed using the notion of strong secrecy. Interestingly, it is shown that the equivocation computation for the Gaussian case reduces to the equivocation computation for a Gaussian wiretap channel.

5. Tight outer bounds are developed for the Gaussian case by providing appropriate side information and bounding the entropy terms containing both discrete and continuous random variables based on the insights obtained for the deterministic case. The outer bounds derived on the secrecy capacity region of the Gaussian symmetric Z-IC are the best known outer bounds till date with unidirectional transmitter cooperation.

6. In the weak/moderate interference regime, the secure sum generalized degrees of freedom (GDOF) is also characterized and shown to be optimal for all values of the capacity of the

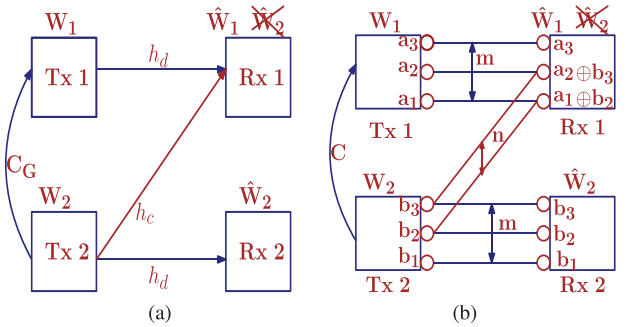


Fig. 1. 2-user symmetric Z-IC with unidirectional transmitter cooperation (from transmitter 2 to transmitter 1): (a) Gaussian model, and (b) Deterministic model.

cooperative link. The secure sum capacity of the symmetric Z-IC is also shown to lie within 2 bits/s/Hz of the outer bound in the weak/moderate interference regime for all possible values of the capacity of the cooperative link.

7. Bounds on the secrecy capacity region of the 2-user symmetric Z-IC *without* cooperation between the transmitters are special cases of the analysis for both models. Note that, prior to this work, the capacity region of the symmetric Z-IC for the deterministic model with secrecy constraints was not fully known even for the non-cooperating case [30].

It is shown that limited-rate transmitter cooperation can greatly facilitate secure communication over the Z-IC in weak/moderate and high interference regimes. In the case of the deterministic model, it is found, surprisingly, that there is no penalty on the capacity region of the Z-IC due to the secrecy constraints at the receivers in the weak/moderate interference regimes. Thus, the proposed scheme allows one to get secure communications for free. Similarly, it is found that there is no loss in the sum GDOF for the Gaussian case due to the secrecy constraint at the receiver, in the weak/moderate interference regimes. For the deterministic model, it is found that for every one bit increase in the capacity of the cooperative link, the secure sum rate can increase by one bit, in the weak, moderate and high interference regimes, until the sum rate is saturated by its maximum possible value.

Notation: Lower case or upper case letters represent scalars, lower case boldface letters represent vectors, and upper case boldface letters represent matrices.

II. System Model

Consider a 2-user Gaussian symmetric Z-IC with unidirectional and rate-limited transmitter cooperation from transmitter 2 to 1, as shown in Fig. 1a.[1] In the Z-IC, only transmitter 2 causes interference to receiver 1. The received signal at receiver i, y_i, is given by

$$y_1 = h_d x_1 + h_c x_2 + z_1; \quad y_2 = h_d x_2 + z_2, \tag{1}$$

where z_j $(j = 1, 2)$ is the additive white Gaussian noise, distributed as $\mathcal{N}(0, 1)$. Here, h_d and h_c are the channel gains of the direct and interfering links, respectively. The input signals (x_i) satisfy the power constraint: $E[|x_i|^2] \leq P$. The unidirectional cooperative link from the interfering transmitter (transmitter 2) to the non-interfering transmitter (transmitter 1) is noiseless, secure, and of finite rate C_G.

The equivalent deterministic model of (1) at high SNR is given by [14], [30]

$$\mathbf{y}_1 = \mathbf{D}^{q-m}\mathbf{x}_1 \oplus \mathbf{D}^{q-n}\mathbf{x}_2; \quad \mathbf{y}_2 = \mathbf{D}^{q-m}\mathbf{x}_2, \tag{2}$$

where $\mathbf{x}_1$ $(\mathbf{x}_2)$ is the binary input vector of the deterministic Z-IC from user 1 (user 2) of length m $(\max\{m, n\})$; $\mathbf{y}_1$ $(\mathbf{y}_2)$ is the binary output vector of length $\max\{m, n\}$ (m); $\mathbf{D}$ is a $q \times q$ downshift matrix with elements $d_{j',j''} = 1$ if $2 \leq j' = j'' + 1 \leq q$ and $d_{j',j''} = 0$ otherwise; and the operator $\oplus$ stands for modulo-2 addition, i.e., the XOR operation. The deterministic model is pictorially illustrated in Fig. 1b.

The deterministic model is a first order approximation of a Gaussian channel, where all the signals are represented by their binary expansions. Here, noise is modeled by truncation, and the superposition of signals at the receiver is modeled by *modulo* 2 addition. Hence, the parameters m, n, and C of the deterministic model are related to the Gaussian symmetric Z-IC as $m = (\lfloor 0.5 \log \mathsf{SNR} \rfloor)^+$, $n = (\lfloor 0.5 \log \mathsf{INR} \rfloor)^+$, and $C = \lfloor C_G \rfloor$. Note that the notation followed for the deterministic model is the same as that presented in [14]. The bits $a_i \in \mathcal{F}_2$ and $b_i \in \mathcal{F}_2$ denote the information bits of transmitters 1 and 2, respectively, sent on the i^{th} level, with the levels numbered starting from the bottom-most entry.

The transmitter i has a message W_i, which should be decodable at the intended receiver i, but needs to be kept secret from the other, i.e., the unintended receiver j $(j \neq i)$, and this is termed as the *secrecy constraint*. Note that, for the Z-IC, the message W_1 is secure as there is no link from transmitter 1 to receiver 2. Hence, the goal is to ensure that W_2 is not decodable at receiver 1. The encoding at transmitter 1 should satisfy the causality constraint, i.e., it cannot depend on the signal to be sent over the cooperative link in the future. The signal sent over the cooperative link from transmitter 2 to transmitter 1 is represented by $\mathbf{v}_{21}$. It is also assumed that the transmitters trust each other completely and they do not deviate from the agreed schemes, for both models.

For the deterministic model, the encoded message at transmitter 1 is a function of its own data bits, the bits received through the cooperative link, and possibly some random bits, whereas the encoded message at transmitter 2 is independent of the other user's data bits. The bits transmitted on the different levels of the deterministic model are chosen to be equiprobable Bernoulli distributed, denoted by $\mathcal{B}(\frac{1}{2})$. The decoding is based on solving the linear equation in (2) at each receiver. For secrecy, it is required to satisfy the perfect secrecy constraint, i.e., $I(W_i; \mathbf{y}_j) = 0, i, j \in \{1, 2\}$ and $i \neq j$ in the case of the deterministic model [32]. In the later part of the sequel, it is shown that replacing the perfect secrecy constraint at receiver with the strong or weak secrecy constraint does not enlarge the capacity region of the deterministic model.

In the Gaussian case, the details of the encoding and decoding schemes can be found in Sec. IV. For the Gaussian model, the notion of strong secrecy is considered, i.e., $I(W_2; \mathbf{y}_1^N) \to 0$ as $N \to \infty$, where N corresponds to the block length [33].

[1]The model is termed as symmetric as the links from transmitter 1 to receiver 1 and transmitter 2 to receiver 2 are of the same strength.

The following interference regimes are considered: weak/moderate interference regime ($0 \leq \alpha \leq 1$), high interference regime ($1 < \alpha \leq 2$) and very high interference regime ($\alpha > 2$), where, with a slight abuse of notation $\alpha \triangleq \frac{n}{m}$ is used for the deterministic model and $\alpha \triangleq \frac{\log \text{INR}}{\log \text{SNR}}$ is used for the Gaussian model. The quantity α captures the amount of coupling between the signal and interference.

III. Linear Deterministic Symmetric Z-IC: Capacity Region

In this section, the secrecy capacity region of the linear deterministic symmetric Z-IC with unidirectional transmitter cooperation is characterized for the different interference regimes through Theorems 1-3. It is shown that the upper bound on the secrecy capacity region matches with the lower bound, and thereby establishes the capacity region for the deterministic model. Due to lack of space, only a high level description of the proofs of the results are provided, and the interested reader is referred to [1], [34], [35] for details.

Note that in all interference regimes, the rate of both users can be trivially upper bounded by m, i.e., $R_1 \leq m$ and $R_2 \leq m$. One of the key techniques used in deriving tight outer bounds is to partition the encoded message, output, or both, depending on the value of α. The partitioning of the encoded messages/outputs gives insights on the side information to be provided to the receiver. This in turn allows one to exploit the secrecy constraint at the receiver to obtain tight and tractable outer bounds on the secrecy capacity region of the Z-IC. This partitioning also helps to simplify the entropy terms as the encoded messages at the transmitters are not independent due to the cooperation between the transmitters.

The following Markov relation is used in the derivation of these outer bounds: conditioned on the cooperating signal ($\mathbf{v}_{21}^N$), the encoded signals and the messages at the two transmitters are independent [14], [36], i.e.,

$$(W_1, \mathbf{x}_1^N) \rightarrow (\mathbf{v}_{21}^N) \rightarrow (W_2, \mathbf{x}_2^N). \tag{3}$$

Outer Bounds in the Weak/Moderate Interference Regime ($0 \leq \alpha \leq 1$): The encoded message $\mathbf{x}_1$ is split into two parts: one part ($\mathbf{x}_{1a}$), which is received without interference at receiver 1, and another part ($\mathbf{x}_{1b}$), which is received with interference at receiver 1. The encoded message of transmitter 2 is also split into two parts: one part ($\mathbf{x}_{2a}$), which causes interference to receiver 1, and another part ($\mathbf{x}_{2b}$), which does not cause any interference to receiver 1. The partitioning of the output and the encoded message is shown in Fig. 2a. In the derivation of this outer bound, the secrecy constraints at the receivers are not used.

Inner Bounds in the Weak/Moderate Interference Regime ($0 \leq \alpha \leq 1$): When there is a high capacity cooperative link from transmitter 2 to transmitter 1, the interference caused at receiver 1 by transmitter 2 can be completely canceled by using the signal received from transmitter 2 via the cooperative link at transmitter 1. This cancelation of interference offers two benefits: it improves the achievable rate, and also ensures secrecy, since the signal sent by transmitter 2 is no longer decodable at receiver 1. When the capacity of the cooperative link is not sufficiently high, it is not possible to design the precoding to completely eliminate the interference caused by transmitter 2 at receiver 1. In this case, the transmission of random bits (i.e., transmission of artificial noise [37], [38]) by transmitter 1 can ensure secrecy of the data bits sent by transmitter 2 at receiver 1, in turn enabling transmitter 2 to achieve a higher secure rate of communication. Thus, the proposed achievable scheme uses a carefully designed combination of interference cancelation and transmission of random bits depending on the capacity of the cooperative link C bits, and the value of α. A pictorial representation of the scheme to achieve the corner points $(R_1, R_2) = (5, 3)$ and $(R_1, R_2) = (3, 5)$ is shown in Figs. 3a and 3b, respectively.

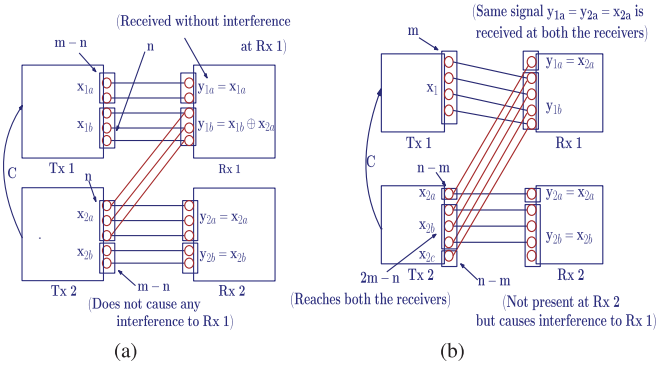


Fig. 2. Deterministic Z-IC: partitioning of encoded messages and outputs: (a) $(m, n) = (5, 3)$, and (b) $(m, n) = (4, 5)$.

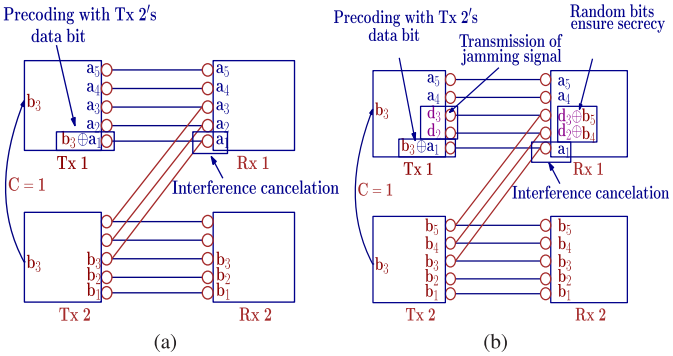


Fig. 3. Deterministic Z-IC with $m = 5$, $n = 3$ and $C = 1$: (a) $(R_1, R_2) = (5, 3)$, and (b) $(R_1, R_2) = (3, 5)$.

Theorem 1: In the weak/moderate interference regime ($0 \leq \alpha \leq 1$, i.e., $n \leq m$), the secrecy capacity region of the 2-user deterministic symmetric Z-IC with unidirectional and rate-limited transmitter cooperation is

$$R_1 \leq m, \quad R_2 \leq m, \quad R_1 + R_2 \leq 2m - n + C. \tag{4}$$

Remarks:

- The derivation of the outer bound [1] does not use the secrecy constraint at the receiver. The proposed schemes can achieve the four corner points of the outer bound, and hence, the secrecy constraints at the receivers do not result in any penalty on the capacity region. Thus, the capacity region of the deterministic Z-IC is characterized with and without secrecy constraints for all values of C.
- When $0 < \alpha \leq 1$, both users can achieve the maximum rate of m simultaneously if $C \geq m$.

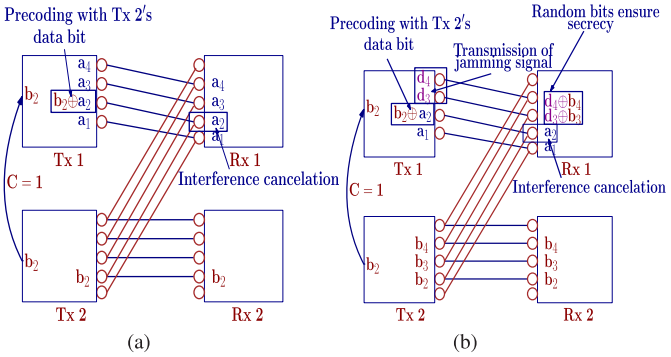


Fig. 4. Deterministic Z-IC with $m = 4$, $n = 5$ and $C = 1$: (a) $(R_1, R_2) = (4, 1)$, and (b) $(R_1, R_2) = (2, 3)$.

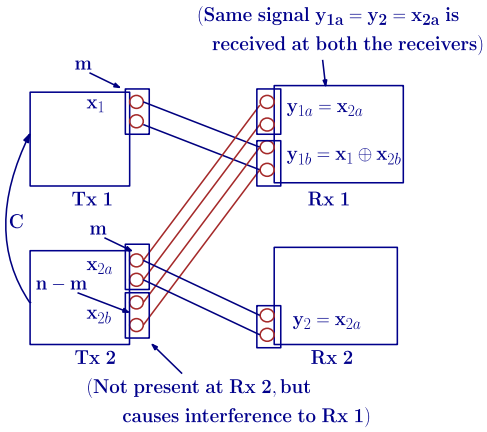


Fig. 5. Deterministic Z-IC with $(m, n) = (2, 4)$: Illustration of partitioning of the message/output.

Outer Bounds in the High Interference Regime ($1 < \alpha < 2$): In this case, it is not difficult to see that the rate of user 1 can be upper bounded by m. To get insights into the outer bounds on R_2 and $R_1 + R_2$, consider Fig. 2b. One can see that transmitter 2 cannot use the levels $[1 : n-m]$ for transmitting its own data as the corresponding links do not exist at the intended receiver. Any data bits transmitted on the levels $[m+1 : n]$, i.e., $\mathbf{x}_{2a}$, will be received without interference at receiver 1. If receiver 2 can decode these data bits, receiver 1 will also be able to decode these data bits. Hence, these data bits $\mathbf{y}_{1a} = \mathbf{x}_{2a}$ will not be secure. Hence, they are provided as side information to receiver 2 to obtain the upper bounds. Then, using the secrecy constraint at receiver 1, the following outer bounds can be obtained.

Inner Bounds in the High Interference Regime ($1 < \alpha < 2$): The achievable scheme proposed here differs from that proposed in the weak/moderate interference regime in terms of the placement of random bits. A high level description of the achievable scheme to achieve the corner points $(R_1, R_2) = (4, 1)$ and $(R_1, R_2) = (2, 3)$ is shown in Figs. 4a and 4b, respectively.

Theorem 2: In the high interference regime ($1 < \alpha < 2$, i.e., $m < n < 2m$), the secrecy capacity region of the 2-user deterministic symmetric Z-IC with unidirectional and rate-limited transmitter cooperation is

$$R_1 \leq m, \quad R_2 \leq 2m - n, \quad R_1 + R_2 \leq m + C. \tag{5}$$

Remarks:

- When $C = 0$ and $1 < \alpha < 2$, if user 1 achieves the maximum rate of m, then user 2 cannot achieve any nonzero secrecy rate. This is in contrast to the weak/moderate interference case, where user 1 achieves the maximum rate of m, while user 2 achieves the rate of $m - n$ even without cooperation.
- When $1 < \alpha < 2$ and $C \geq 2m - n$, transmitters 1 and 2 can simultaneously achieve the maximum rates of m and $2m - n$, respectively.
- In general, the principle behind the schemes to achieve the corner points $(m, m - n + C)$ and (m, C) in the weak/moderate and high interference regimes, respectively, is precoding of data bits at transmitter 1 using the data bits of transmitter 2 received on the cooperative link to cancel interference and ensure secrecy. On the other hand, the achievability of the corner points $(m-n+C, m)$ and $(n - m + C, 2m - n)$ in the weak/moderate and high interference regimes, respectively, requires transmission of random bits by transmitter 1 to ensure that the signal from transmitter 2 remains secure, in addition to precoding data bits received from transmitter 2 with its own data bits.

Outer Bounds in the Very High Interference Regime ($\alpha \geq 2$): In Fig. 5, it can be noticed that only the levels $[n-m+1 : m]$ can be used to send data from transmitter 2 to receiver 2, as the links corresponding to the lower levels $[1 : n-m]$ do not exist at receiver 2. The data bits transmitted on the levels $[n-m+1 : n]$, i.e., $\mathbf{x}_{2a}$, are received without interference at receiver 1. If receiver 2 can decode these data bits, then receiver 1 can also decode these data bits. Hence, transmitter 2 cannot send any data bits securely on these levels. To capture this in the derivation, receiver 2 is provided with the side information of the form $\mathbf{y}_{1a}^N$, which in turn helps to bound the rate by $I(W_2; \mathbf{y}_2^N | \mathbf{y}_{1a}^N)$. It can be noticed that this quantity is zero, as $\mathbf{y}_{1a} = \mathbf{y}_2 = \mathbf{x}_{2a}$. The secrecy capacity region in the very high interference regime ($\alpha \geq 2$) is given in the following theorem.

Theorem 3: In the very high interference regime ($\alpha \geq 2$, i.e., $2m \leq n$), the secrecy capacity region of the 2-user deterministic symmetric Z-IC with unidirectional and rate-limited transmitter cooperation is

$$R_1 \leq m, \quad R_2 = 0. \tag{6}$$

Proof: The outer bound on the rate of user 2 in Theorem 3 shows that user 2 cannot achieve any nonzero secrecy rate irrespective of the capacity of the cooperative link. Thus, transmitter 1 can send data bits on the levels $[1 : m]$, while transmitter 2 remains silent. This characterizes the capacity of the deterministic Z-IC in the very high interference regime. ■

Interestingly, it turns out that the capacity region of the deterministic symmetric Z-IC does not change if the perfect secrecy constraint at the receiver is replaced with the strong or the weak notion of secrecy. This result is stated in the following Theorem.

Theorem 4: The secrecy capacity region of the deterministic symmetric Z-IC with unidirectional transmitter cooperation

satisfies the following

$$\mathcal{C}^{\text{perfect}} = \mathcal{C}^{\text{strong}} = \mathcal{C}^{\text{weak}}, \tag{7}$$

where $\mathcal{C}^{\text{perfect}}$, $\mathcal{C}^{\text{strong}}$ and $\mathcal{C}^{\text{weak}}$ correspond to the capacity regions of the 2-user deterministic Z-IC with unidirectional transmitter cooperation guaranteeing the perfect, strong and weak secrecy constraints at the receivers, respectively.

Proof: In the literature, three notions of secrecy have been used: *perfect*, *strong*, and *weak secrecy*. Mathematically, perfect secrecy is defined as $I(W_i; \mathbf{y}_j^N) = 0, i, j \in \{1, 2\}$ and $i \neq j$ [32]. Strong secrecy is defined as: $\lim_{N\to\infty} I(W_i; \mathbf{y}_j^N) = 0, i, j \in \{1, 2\}$ and $i \neq j$ [33]. Weak secrecy is defined as: $\lim_{N\to\infty} \frac{1}{N} I(W_i; \mathbf{y}_j^N) = 0, i, j \in \{1, 2\}$ and $i \neq j$ [33].

Any communication scheme satisfying the perfect secrecy condition will automatically satisfy the strong and weak secrecy conditions. Similarly, a communication scheme satisfying strong secrecy will automatically satisfy the weak secrecy condition. Hence, the following holds

$$\mathcal{C}^{\text{perfect}} \subseteq \mathcal{C}^{\text{strong}} \subseteq \mathcal{C}^{\text{weak}} \subseteq \mathcal{C}^{\text{weak}}_{\text{outer}}, \tag{8}$$

where $\mathcal{C}^{\text{weak}}_{\text{outer}}$ corresponds to the outer bound on the capacity region of the Z-IC with unidirectional transmitter cooperation and weak secrecy constraints at the receivers. The achievable results in Sec. III are obtained under the perfect secrecy constraints at the receivers. On the other hand, it is not difficult to show that the upper bounds on the capacity region in [1] do not change if the perfect secrecy constraint is replaced with the weak secrecy constraint.[2] As the achievable rate regions (i.e., $\mathcal{C}^{\text{perfect}}$) match with the upper bounds on the capacity region (i.e., $\mathcal{C}^{\text{weak}}_{\text{outer}}$), the relation in (7) holds. ■

IV. Gaussian Symmetric Z-IC: Achievable Scheme

For the Gaussian case, a unified achievable scheme is proposed, which is applicable in the weak, moderate and high interference regimes. The achievable scheme is based on the cooperative precoding performed at the transmitters to cancel the interference at the unintended receiver, along with stochastic encoding and transmission of artificial noise. When the capacity of the cooperative link is not sufficiently high, it is not possible to share the entire message of transmitter 2 with transmitter 1 through the cooperative link. Hence, the interference caused at receiver 1 by transmitter 2 cannot be completely eliminated. Thus, stochastic encoding performed at transmitter 2 and artificial noise transmission by transmitter 1 can provide additional randomness to increase the secrecy rate of user 2.

The achievable scheme for the deterministic model is extended to the Gaussian model as follows. Since there is no cooperative link from transmitter 1 to transmitter 2, transmitter 1 cannot share its message with transmitter 2 for cooperation. The message of transmitter 1 intended to receiver 1 is inherently secure, as there is no link from transmitter 1 to receiver 2. This translates to having a non-cooperative private message $w_{p1} \in \mathcal{W}_{p1} = \{1, 2, \ldots, 2^{NR_1}\}$ at transmitter 1, and for each message, it transmits a codeword from a Gaussian codebook of size 2^{NR_1}. Next, for the transmission of data by transmitter 2, recall that, in the deterministic case, the data bits sent by transmitter 2 on the lower levels $[1 : m - n]$ are inherently secure in the weak/moderate interference regime (See Fig. 3a). To enable secure transmission of data bits on the higher levels (specifically, levels $[m - n + 1 : m]$ in the weak/moderate interference regime and levels $[n - m + 1 : n]$ in the high interference regime), transmitter 2 needs the assistance of transmitter 1. That is, transmitter 1 needs to precode the data bits received through the cooperative link, or needs to send a jamming signal, so that the other user's data bits remain undecodable at receiver 1. To translate this scheme to the Gaussian case, the message at transmitter 2 is split into two parts: a non-cooperative private message $w_{p2} \in \mathcal{W}_{p2} = \{1, 2, \ldots, 2^{NR_{p2}}\}$ and a cooperative private message $w_{cp2} \in \mathcal{W}_{cp2} = \{1, 2, \ldots, 2^{NR_{cp2}}\}$. Transmitter 2 encodes the non-cooperative private message into $\mathbf{x}_{p2}^N$ using stochastic encoding. A stochastic encoder is specified by a matrix of conditional probability $f_{p2}(x_{p2,k}|w_{p2})$, where $x_{p2,k} \in \mathcal{X}_{p2}$ and $w_{p2} \in \mathcal{W}_{p2}$.

For the cooperative private message, transmitters 1 and 2 precode the message w_{cp2} cooperatively such that the codeword carrying the cooperative private message is completely canceled at the non-intended receiver. This cooperative precoding also helps ensure secrecy for the cooperative private message. The details of the encoding and decoding process of the achievable scheme are presented in the following subsection.

A. Encoding and Decoding

For the non-cooperative private part, transmitter 1 generates a codebook $\mathcal{C}_{p1}$ containing 2^{NR_1} codewords of length N with i.i.d. $\mathcal{N}(0, P_{p1})$ entries. Transmitter 2 generates two codebooks as follows. For the non-cooperative private message, it generates a codebook $\mathcal{C}_{cp2}$ containing $2^{N(R_{p2}+R'_{p2})}$ codewords of length N with i.i.d. $\mathcal{N}(0, P_{p2})$ entries. The $2^{N(R_{p2}+R'_{p2})}$ codewords in the codebook $\mathcal{C}_{p2}$ are randomly grouped into $2^{NR_{p2}}$ bins, with each bin containing $2^{NR'_{p2}}$ codewords. Any codeword in $\mathcal{C}_{p2}$ is indexed as $\mathbf{x}_{p2}^N(w_{p2}, w'_{p2})$ for $w_{p2} \in \mathcal{W}_{p2}$ and $w'_{p2} \in \mathcal{W}'_{p2} = \{1, 2, \ldots, 2^{NR'_{p2}}\}$. To send w_{p2}, transmitter 2 selects w'_{p2} uniformly at random from the set $\mathcal{W}'_{p2}$ and transmits the codeword $\mathbf{x}_{p2}^N(w_{p2}, w'_{p2})$. For the cooperative private message, transmitter 2 generates a codebook $\mathcal{C}_{cp2}$ consisting of $2^{NR_{cp2}}$ codewords of length N with i.i.d. $\mathcal{N}(0, P_{cp2})$ entries. This codebook is made available at transmitter 1.

To send a message (w_{p2}, w_{cp2}), transmitter 2 superimposes the cooperative codeword $\mathbf{x}_{cp2}(w_{p2})$ with the non-cooperative codeword $\mathbf{x}_{p2}^N(w_{p2}, w'_{p2})$ as

$$\mathbf{x}_2^N(w_{p2}, w'_{p2}, w_{cp2}) = \mathbf{x}_{p2}^N(w_{p2}, w'_{p2}) + h_d \mathbf{x}_{cp2}^N(w_{cp2}). \tag{9}$$

The following power constraint is required to be satisfied at transmitter 2: $P_{p2} + h_d^2 P_{cp2} \leq P$, where P_{p2} and P_{cp2} are parameters to be chosen later.

[2]This can be shown by using $\frac{1}{N} I(W_i; \mathbf{y}_j^N) \leq \epsilon$, $i \neq j$, (weak secrecy) as a measure of secrecy in the derivation of the outer bounds, instead of $I(W_i, \mathbf{y}_j) = 0$ (perfect secrecy).

Transmitter 1 performs precoding as mentioned in (10), so that the codeword carrying the cooperative private message of transmitter 2 is canceled at receiver 1. This is termed as *cooperative precoding*. Transmitter 1 also adds artificial Gaussian noise ($\mathbf{x}_{a1}^N$) to increase the achievable secrecy rate for transmitter 2. Thus, transmitter 1 sends

$$\mathbf{x}_1^N(w_{p1}, w_{cp2}) = \mathbf{x}_{p1}^N(w_{p1}) - h_c\mathbf{x}_{cp2}^N(w_{cp2}) + \mathbf{x}_{a1}^N. \quad (10)$$

The power constraint at transmitter 1 reads: $P_{p1} + h_c^2 P_{cp2} + P_{a1} \leq P$, where P_{p1} and P_{a1} are parameters to be chosen later.

The decoding at the receivers is performed as follows. Receiver 1 looks for a unique index $\hat{w}_{p1}$ such that $(\mathbf{y}_1^N, \mathbf{x}_1^N(\hat{w}_{p1}))$ is jointly typical. Receiver 2 looks for a unique tuple $(\hat{w}_{p2}, \hat{w}'_{p2}, \hat{w}_{cp2})$ such that $(\mathbf{y}_2^N, \mathbf{x}_{p2}^N(\hat{w}_{p2}, \hat{w}'_{p2}), \mathbf{x}_{cp2}^N(\hat{w}_{cp2}))$ is jointly typical. Decoding errors at the receivers can occur in one of two ways. First, the receiver may not be able to find any codeword that is jointly typical with the received sequence. Second, a wrong codeword is jointly typical with the received sequence.

Based on the above encoding and decoding strategy, the following theorem gives a lower bound on the secrecy capacity region of the Z-IC with unidirectional transmitter cooperation.

Theorem 5: For the Gaussian symmetric Z-IC with unidirectional transmitter cooperation and secrecy constraints at the receivers, the achievable rate region is given by

$$\begin{aligned} R_1 &\leq I(\mathbf{x}_{p1}; \mathbf{y}_1), \\ R_2 &\leq \min\big\{I(\mathbf{x}_{p2}, \mathbf{x}_{cp2}; \mathbf{y}_2), I(\mathbf{x}_{p2}; \mathbf{y}_2|\mathbf{x}_{cp2}) \\ &\qquad + \min\{C_G, I(\mathbf{x}_{cp2}; \mathbf{y}_2|\mathbf{x}_{p2})\}\big\} - R'_{p2}, \end{aligned} \quad (11)$$

where $R'_{p2} = I(\mathbf{x}_{p2}; \mathbf{y}_1|\mathbf{x}_{p1})$.

Proof: See Appendix A. ∎

Remarks:

1) The term R'_{p2} in Theorem 5 accounts for the rate sacrificed by transmitter 2 in confusing receiver 1 to keep the non-cooperative message of transmitter 2 secret. As the capacity of the cooperative link increases, the loss in rate due to the stochastic encoding decreases, as more power can be assigned to the cooperative private message.
2) When $C_G = 0$ and $\alpha \geq 1$, the transmission of artificial noise by transmitter 1 is required along with stochastic encoding for user 2 to achieve a non-zero secrecy rate.

By evaluating the mutual information terms in (5) and taking convex closure of the union of the set of regions obtained over different codebook parameters (P_{p1}, P_{a1}, P_{p2}, P_{cp2}), the following lower bound on the secrecy capacity region is obtained.

Corollary 1: Using the result in Theorem 5, the following rate region is achievable

$$\mathcal{R}_s \triangleq \text{convex closure of} \bigcup_{0\leq(\theta_i,\beta_i,\lambda_i)\leq 1,\, i=1,2} \mathcal{R}_{\text{Z-IC}}^s(\theta_i, \beta_i, \lambda_i), \quad (12)$$

where

$$\begin{aligned} \mathcal{R}_{\text{Z-IC}}^s(\theta_i, \beta_i, \lambda_i) \triangleq \{&(R_1, R_2) : R_1 \geq 0, R_2 \geq 0, \\ &R_1 \leq 0.5\log\left(1 + \frac{h_d^2 P_{p1}}{1 + h_d^2 P_{a1} + h_c^2 P_{p2}}\right), \\ &R_2 \leq 0.5\log(1 + h_d^2 P_{p2} + h_d^4 P_{cp2}) - R'_{p2}, \\ &R_2 \leq 0.5\log(1 + h_d^2 P_{p2}) + \min\{C_G, \\ &0.5\log(1 + h_d^4 P_{cp2})\} - R'_{p2}\}, \end{aligned} \quad (13)$$

where $R'_{p2} \triangleq 0.5\log\left(1 + \frac{h_c^2 P_{p2}}{1 + h_d^2 P_{a1}}\right)$, $P_{cp2} \triangleq \frac{\lambda_2}{(\lambda_1+\lambda_2)h_d^2} P_2$, $P_{p2} \triangleq \frac{\lambda_1}{\lambda_1+\lambda_2} P_2$, $P_{p1} \triangleq \frac{\theta_1}{\theta_1+\theta_2} P'$, $P_{a1} \triangleq \frac{\theta_2}{\theta_1+\theta_2} P'$, $P' \triangleq (P_1 - h_c^2 P_{cp2})^+$, $P_1 \triangleq \beta_1 P$, and $P_2 \triangleq \beta_2 P$.

Proof: See Appendix B. ∎

Remarks:

1) In Corollary 1, the parameter β_i ($0 \leq \beta_i \leq 1$) acts as a power control parameter for transmitter i ($i = 1, 2$). The parameters θ_i and λ_i act as rate splitting parameters for transmitter i.
2) When $C = 0$ (or $C_G = 0$), the system reduces to the 2-user Z-IC (Gaussian Z-IC) without cooperation, which was studied in [30]. The achievable results in Theorem 2 (Theorem 3) in [30] can be obtained as a special case of achievable results for the deterministic model (Gaussian model) in Theorem 1 (Theorem 5), by setting $C = 0$ ($C_G = 0$) and $0 \leq \alpha \leq 1$. Note that, for both the deterministic and Gaussian models, achievable schemes on the secrecy capacity region have not been addressed in the literature for the high interference regime ($\alpha > 1$), even when $C = 0$ ($C_G = 0$).
3) It is straightforward to extend the result in Corollary 1 by using time-division multiplexing [31, Lemma 2] and allowing transmitter 1 to transmit over a different subband [31, Lemma 3] to obtain the corresponding results in [31], by setting $C_G = 0$ and $P_{a1} = 0$, for the weak/moderate interference regime.

V. Gaussian Symmetric Z-IC: Outer Bounds

In this section, the outer bounds on the secrecy capacity region for the Z-IC with unidirectional transmitter cooperation are stated as Theorems 6-8. In addition to the differences between the deterministic model and the Gaussian model (noise modeled by truncation and carry-overs ignored in the module-2 addition), the derivation of outer bounds for the Gaussian case requires the bounding of differential entropy terms containing continuous as well as discrete random variables, due to the unidirectional cooperation between the transmitters. The partitioning of the encoded messages or outputs used in the derivation of the outer bounds for the deterministic case cannot be directly applied to the Gaussian case. To overcome this problem, either analogous quantities that serve as side information at receiver need to be found to mimic the partitioning of the encoded messages/outputs, or the bounding steps need to be modified taking cue from the deterministic model. This helps to obtain tractable outer bounds on the secrecy capacity region, which are presented in the following subsections.

A. Weak/Moderate Interference Regime ($0 \le \alpha \le 1$)

The outer bound derived in Theorem 1 involved providing the side information $(\mathbf{x}_{2a}, \mathbf{v}_{21})$ to receiver 2 by a genie. The quantity $\mathbf{x}_{2a}$ corresponds to the part of the encoded message $\mathbf{x}_2$ of transmitter 2 which causes interference at receiver 1 (See Fig. 2a). In the Gaussian case, to mimic the approach used for the deterministic case, receiver 2 is provided with side information $(\mathbf{s}_2 \triangleq h_c\mathbf{x}_2 + \mathbf{z}_1, \mathbf{v}_{21})$. Note that an outer bound based on this idea was presented in [26], which considered the Gaussian Z-IC with unidirectional transmitter cooperation, but without secrecy constraints at the receivers. For the sake of completeness, the result is stated as Theorem 6 for the symmetric case. The outer bound in Theorem 1 for the weak/moderate interference regime can be considered as a deterministic equivalent of the outer bound presented below.

Theorem 6 [26]: The capacity region of the 2-user Gaussian symmetric Z-IC with unidirectional transmitter cooperation is upper bounded as

$$\begin{aligned} &R_1 \le 0.5\log(1+\text{SNR}),\ R_2 \le 0.5\log(1+\text{SNR}),\\ &R_1+R_2 \le 0.5\log(1+\text{SNR}+\text{INR}+2\sqrt{\text{SNR}\cdot\text{INR}})\\ &\qquad +0.5\log\left(1+\frac{\text{SNR}}{1+\text{INR}}\right)+C_G, \end{aligned} \tag{14}$$

where $\text{SNR} \triangleq h_d^2 P$ and $\text{INR} \triangleq h_c^2 P$.

Note that the outer bound stated in Theorem 6 does not use the secrecy constraint at receiver. In the weak/moderate interference regime, the data bits transmitted on the lower levels $[1 : m-n]$ of transmitter 2 are inherently secure in the deterministic case as shown in Fig. 3a. However, in the Gaussian case, there is no one-to-one correspondence of this as noise cannot be modeled by truncation. The secrecy constraint at the receiver may lead to a nonzero penalty in rate for the Gaussian case. Hence, outer bounds are derived on the rate of user 2 and the sum rate using the secrecy constraint at receiver 1, which is stated as the theorem below.

Theorem 7: The secrecy capacity region of the 2-user Gaussian symmetric Z-IC with unidirectional transmitter cooperation in the weak/moderate interference regime is upper bounded as

$$\begin{aligned} &R_1 \le 0.5\log(1+\text{SNR}),\\ &R_2 \le \max_{-1\le\rho\le 1} 0.5\log\left(1+\text{SNR}\right.\\ &\qquad\left.-\frac{(\rho\text{SNR}+\sqrt{\text{SNR}\cdot\text{INR}})^2}{1+\text{SNR}+\text{INR}+2\rho\sqrt{\text{SNR}\cdot\text{INR}}}\right),\\ &R_1+R_2 \le \log(1+\text{SNR})-0.5\log(1+\text{INR})+C_G. \end{aligned} \tag{15}$$

Proof: See Appendix C. ∎

Remarks:

- It is easy to show that the outer bound on the sum rate in Theorem 7 is tighter than the outer bound in Theorem 6 for all values of SNR, INR and C_G. Thus, the outer bound in Theorem 7 improves over Theorem 6. From the outer bound on the rate of user 2 in Theorems 6 and 7, it can be observed that outer bound obtained with the secrecy constraint is tighter than the outer bound obtained without using the secrecy constraint.
- When $C_G = 0$, the outer bound on the rate of user 2 reduces to $0.5\log\left(1+\text{SNR}-\frac{\text{SNR}\cdot\text{INR}}{1+\text{SNR}+\text{INR}}\right)$, as the only possible value ρ can take is 0. Hence, this outer bound indicates that user 2 cannot achieve the maximum possible rate of $0.5\log(1+\text{SNR})$. This is in contrast to the deterministic case, where user 2 can achieve the maximum rate of m, as observed from Theorem 1.
- The outer bound on the sum rate in Theorem 6 is applicable in all interference regimes whereas the outer bound in Theorem 7 is applicable only in the weak/moderate interference regime.

B. High Interference Regime ($1 < \alpha < 2$)

The derivation of the outer bound in this regime is based on the outer bound in Theorem 2 obtained for the deterministic model. In the proof of Theorem 2, to upper bound the rate of user 2, a part of the output at receiver 1 which does not contain the signal sent by transmitter 1 is provided as side information to receiver 2, i.e., $\mathbf{y}_{1a}^N$. In the Gaussian case, it is not possible to partition the encoded message as was done for the deterministic model (See Fig. 2b). To overcome this problem, the output at receiver 1, i.e., $\mathbf{y}_1^N$, is provided as side information to receiver 2. Providing side information in this way creates a degraded channel from transmitter 2 to receiver 1 with respect to the channel from transmitter 2 to receiver 2. In the deterministic case, to upper bound the sum rate, the output at receiver 1 $(\mathbf{y}_1^N)$ is partitioned into two parts: $\mathbf{y}_{1a}^N$ and $\mathbf{y}_{1b}^N$, and receiver 2 is provided with side information of the form $\mathbf{y}_{1a}^N$. To mimic this in the Gaussian case, the output of receiver 2, i.e., $\mathbf{y}_2^N$, is provided as side information to receiver 1 and $(W_1, \mathbf{y}_1^N)$ is provided as side information to receiver 2. The outer bound on the secrecy capacity region is stated in the following theorem.

Theorem 8: The secrecy capacity region of the 2-user Gaussian symmetric Z-IC with unidirectional transmitter cooperation is upper bounded as

$$\begin{aligned} &R_1 \le 0.5\log(1+\text{SNR}),\\ &R_2 \le \max_{-1\le\rho\le 1} 0.5\log\left(1+\text{SNR}\right.\\ &\qquad\left.-\frac{(\rho\text{SNR}+\sqrt{\text{SNR}\cdot\text{INR}})^2}{1+\text{SNR}+\text{INR}+2\rho\sqrt{\text{SNR}\cdot\text{INR}}}\right),\\ &R_1+R_2 \le \max_{-1\le\rho\le 1} 0.5\log\left(1+\text{SNR}+\text{INR}\right.\\ &\qquad\left.+2\rho\sqrt{\text{SNR}\cdot\text{INR}}-\frac{(\rho\text{SNR}+\sqrt{\text{SNR}\cdot\text{INR}})^2}{1+\text{SNR}}\right)\\ &\qquad +0.5\log\Sigma_{\mathbf{y}_2|\mathbf{s}}+C_G, \end{aligned} \tag{16}$$

where $\Sigma_{\mathbf{y}_2|\mathbf{s}} \triangleq 1+\text{SNR}-\Sigma_{\mathbf{y}_2,\mathbf{s}}\Sigma_{\mathbf{s},\mathbf{s}}^{-1}\Sigma_{\mathbf{y}_2,\mathbf{s}}^T$, $\Sigma_{\mathbf{y}_2,\mathbf{s}} \triangleq \begin{bmatrix}\rho\text{SNR} & \rho\text{SNR}+\sqrt{\text{SNR}\cdot\text{INR}}\end{bmatrix}$ and $\Sigma_{\mathbf{s},\mathbf{s}} \triangleq \begin{bmatrix}1+\text{SNR} & \text{SNR}+\rho\sqrt{\text{SNR}\cdot\text{INR}}\\ \text{SNR}+\rho\sqrt{\text{SNR}\cdot\text{INR}} & 1+\text{SNR}+\text{INR}+2\rho\sqrt{\text{SNR}\cdot\text{INR}}\end{bmatrix}$.

Proof: See Appendix D. ∎

Remarks:

- When there is no cooperation between the transmitters, the encoded messages at the two transmitters are independent of each other. Hence, for the non-cooperating case, the outer bound on the rate is obtained by setting $\rho = 0$ in Theorem 8.
- The outer bound in Theorem 8 is applicable over all the interference regimes. Note that the outer bound in Theorem 6 is also applicable to the high interference regime. In the later part of the paper, it is demonstrated that the outer bound in Theorem 8 is tighter than the outer bound in Theorem 6 in this interference regime.

C. Relation Between the Outer Bounds for the Deterministic and Gaussian Models

In the following, it is shown that, for high SNR and INR, the outer bounds for the Gaussian case in Theorems 7 and 8 are approximately equal to the outer bounds for the deterministic model. For ease of presentation, it is assumed that $0.5\log\text{SNR}$, $0.5\log\text{INR}$, and C_G are integers. Recall that, the parameters m, n and C of the deterministic model are related to the Gaussian model as $m = (\lfloor 0.5\log\text{SNR}\rfloor)^+$, $n = (\lfloor 0.5\log\text{INR}\rfloor)^+$ and $C = \lfloor C_G \rfloor$, respectively.

1) Weak/Moderate Interference Regime ($0 \le \alpha \le 1$): It is easy to see that for high SNR and INR (i.e., SNR, INR $\gg 1$), the upper bounds on the individual rates in Theorem 6 can be approximated as

$$\begin{aligned} R_1 &\le 0.5\log(1+\text{SNR}) \approx m, \quad \text{and} \\ R_2 &\le 0.5\log(1+\text{SNR}) \approx m. \end{aligned} \tag{17}$$

When SNR > INR (i.e., $0 \le \alpha \le 1$), the outer bound on the sum rate in Theorem 6 is approximated as

$$\begin{aligned} R_1 + R_2 &\le 0.5\log\left(1+\text{SNR}+\text{INR}+2\sqrt{\text{SNR}\cdot\text{INR}}\right) \\ &\quad + 0.5\log\left(1+\frac{\text{SNR}}{1+\text{INR}}\right) + C_G, \\ &\approx 2m - n + C. \end{aligned} \tag{18}$$

From (17) and (18), the outer bound derived for the Gaussian case matches with the corresponding outer bound for the deterministic model stated in Theorem 1.

In Theorem 7, due to the maximization involved in the outer bound on R_2 over ρ, $C_G = 0$ is considered to simplify the exposition. For the non-cooperating case, the outer bound is optimized by setting $\rho = 0$. The outer bound on the rate of user 2 is approximated as

$$R_2 \le 0.5\log\left(1+\text{SNR}-\frac{\text{SNR}\cdot\text{INR}}{1+\text{SNR}+\text{INR}}\right) \approx m. \tag{19}$$

Hence, the outer bound on the rate of user 2 is approximately equal to m for high SNR and INR.

It is also easy to see that, for high SNR and INR, the outer bound on the sum rate in Theorem 7 can be approximated as

$$R_1 + R_2 \approx 2m - n + C. \tag{20}$$

It can be noticed that the outer bound derived for the Gaussian case corresponds to the outer bound for the deterministic model stated in Theorem 1. It is interesting to note that both the outer bounds on the sum rate in Theorems 6 and 7 correspond to the outer bound for the deterministic model stated in Theorem 1 for high SNR and INR. As mentioned earlier in the remark to Theorem 7, the outer bound in Theorem 7 is tighter than Theorem 6. However, for high values of SNR and INR, the gap between these two outer bounds decreases and these two outer bounds are approximately equal to each other.

2) High Interference Regime ($1 < \alpha < 2$): In Theorem 8, due to the maximization involved in the upper bounds on R_2 and $R_1 + R_2$ over ρ, $C_G = 0$ is considered in the following analysis to simplify the exposition. For the non-cooperating case, the outer bound is optimized by setting $\rho = 0$. First, the outer bound on the rate of user 1 is approximated as

$$R_1 \le 0.5\log(1+\text{SNR}) \approx m. \tag{21}$$

The outer bound on the rate of user 2 is also approximated as

$$R_2 \le 0.5\log\left(1+\text{SNR}-\frac{\text{SNR}\cdot\text{INR}}{1+\text{SNR}+\text{INR}}\right) \approx 2m-n. \tag{22}$$

The outer bound on the sum rate becomes

$$\begin{aligned} R_1 + R_2 \le\ & 0.5\log\left(1+\text{SNR}+\text{INR}-\frac{\text{SNR}\cdot\text{INR}}{1+\text{SNR}}\right) \\ & + 0.5\log\Sigma_{\mathbf{y}_2|\mathbf{s}}, \end{aligned} \tag{23}$$

where with some algebraic manipulation it can be shown that $\Sigma_{\mathbf{y}_2|\mathbf{s}} = 1 + \text{SNR} - \Sigma_{\mathbf{y}_2,\mathbf{s}}\Sigma_{\mathbf{s},\mathbf{s}}^{-1}\Sigma_{\mathbf{y}_2,\mathbf{s}}^T \approx 1$. Hence, the sum rate outer bound in (23) reduces to

$$R_1 + R_2 \le m. \tag{24}$$

From (21), (22), and (24), it can be observed that the approximated outer bound of Gaussian case in Theorem 8 matches with the outer bound of deterministic case in Theorem 2 for the high interference regime.

This validates that the approaches used in obtaining outer bounds in the two models are consistent with each other.

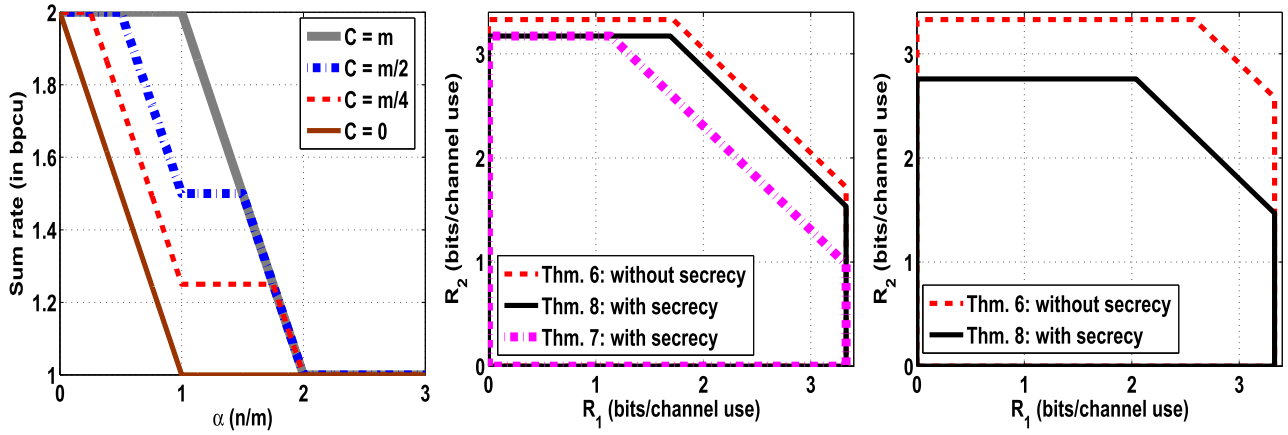
VI. Approximate Secure Sum Capacity Characterization of the Gaussian Symmetric Z-IC in the Weak/Moderate Interference Regime

A. Secure Sum Generalized Degrees of Freedom (GDOF)

As mentioned earlier, the capacity region for many multiuser scenarios has remained an open problem, even without secrecy constraints at the receivers. Due to this, there has been an active research interest in approximate characterizations of the capacity. In this context, the notion of *generalized degrees of freedom (GDOF)* has been used as a proxy for the capacity at high SNR and INR, for the IC, *without secrecy constraint* [7]. A natural extension of this is the secure sum GDOF given by

$$d_{\text{sum}}(\kappa,\gamma) = \lim_{\text{SNR}\to\infty} \frac{C_{\text{sum}}(\text{SNR},\text{INR})}{0.5\log\text{SNR}}, \tag{25}$$

where $\kappa \triangleq \lim_{\text{SNR}\to\infty} \frac{\log\text{INR}}{\log\text{SNR}}$, $\gamma \triangleq \lim_{\text{SNR}\to\infty} \frac{C_G}{0.5\log\text{SNR}}$ and C_{sum} is the secure sum capacity of the 2-user Gaussian Z-IC with unidirectional transmitter cooperation. To characterize the



(a) (b) (c)

Fig. 6. (a) Sum rate capacity for the deterministic symmetric Z-IC with $m = 4$, $n = 5$ and $C = 1$; (b) Comparison of the outer bounds on the secrecy capacity region for the Gaussian symmetric Z-IC: $P = 100$, $h_d = 1$, $h_c = 0.5$, $\alpha = 0.69$, and $C_G = 0$, and (c) Comparison of the outer bounds on the secrecy capacity region for the Gaussian symmetric Z-IC: $P = 100$, $h_d = 1$, $h_c = 1.5$, $\alpha = 1.17$, and $C_G = 1$.

sum GDOF, $h_d = 1$ is assumed without loss of generality, and the following power allocation is used.

$$P_{p1} = \frac{P}{2}, \quad P_{p2} = \frac{1}{h_c^2}, \quad P_{cp2} = \frac{1}{2}\left(P - \frac{1}{h_c^2}\right) \text{ and } P_{a1} = 0. \tag{26}$$

It is also assumed that $h_c^2 P > 1$, so that the above power allocation is always feasible. The motivation for this power allocation is as follows. The power for the message of transmitter 1 is set as $\frac{P}{2}$ to ensure that user 1 achieves the maximum GDOF of 1. Recall that, in the weak/moderate interference regime, transmitter 2 can send data bits securely on the lower levels $[1 : m - n]$, as the links corresponding to these levels are not present at receiver 1. In other words, the data bits transmitted on the lower levels $[1 : m - n]$ of transmitter 2 are received at or below the noise floor of receiver 1. Hence, in the Gaussian case, the power for the non-cooperative private message is chosen such that it is received at the noise floor of the receiver 1. Due to this power allocation, the loss in rate of user 2 due to stochastic encoding is $R'_{p1} = 0.5$ bits/s/Hz. Hence, the loss in achievable secrecy rate due to stochastic encoding does not scale with SNR and INR. The cooperative private message of transmitter 2 is assigned a power of $\frac{1}{2}\left(P - \frac{1}{h_c^2}\right)$.

In the following theorem, the secure sum GDOF is characterized using the power allocation in (26) for all values of C_G in the weak/moderate interference regime.

Theorem 9: The optimal secure sum GDOF of the 2 user Gaussian symmetric Z-IC with unidirectional transmitter cooperation in the weak/moderate interference regime is

$$d_{\text{sum}}(\kappa, \gamma) = \min\{2, 2 - \kappa + \min(\gamma, 1)\}. \tag{27}$$

Proof: See Appendix E. ∎

Remarks:

1) The outer bound on the sum rate in Theorems 6 and 7 are used to obtain outer bound on the sum GDOF. Both the bounds give the same results in terms of the GDOF. Note that the derivation of the outer bound in Theorem 6 does not use the secrecy constraint at receiver 1 [26]. Hence, there is no penalty in the sum GDOF due to the secrecy constraint at receiver in the weak/moderate interference regime for all values of C_G.
2) When $\gamma = \kappa$, $d_{\text{sum}}(\kappa, \gamma) = 2$. Hence, both users can achieve the maximum GDOF of 1 simultaneously. Similarly, in the deterministic model, when $C = n$ (or $\frac{C}{m} = \alpha$), both users can simultaneously achieve a maximum rate of m.

As the proposed scheme with the power allocation in (26) can achieve the optimal sum GDOF, the achievable sum rate will be within a finite number of bits from the outer bound. In the following subsection, the gap between the achievable sum rate and outer bound is characterized.

B. Finite Bit Gap Result on the Sum Rate Capacity

In this section, the sum rate capacity of the 2-user Gaussian Z-IC with unidirectional transmitter cooperation is shown to lie within 2 bits/s/Hz of the outer bound in the weak/moderate interference regime (INR < SNR) for all values of C_G. Note that this gap is the worst case gap. To show the finite gap result, the power allocation in (26) is used in Corollary 1 to obtain a lower bound on the secure sum capacity. This result is stated in the following theorem.

Theorem 10: The secure sum rate capacity (C_{sum}) of the 2-user Gaussian symmetric Z-IC with unidirectional transmitter cooperation is bounded from above by the outer bound, which in turn is within 2 bits/s/Hz of the inner bound in the weak/moderate interference regime for all values of C_G, i.e.,

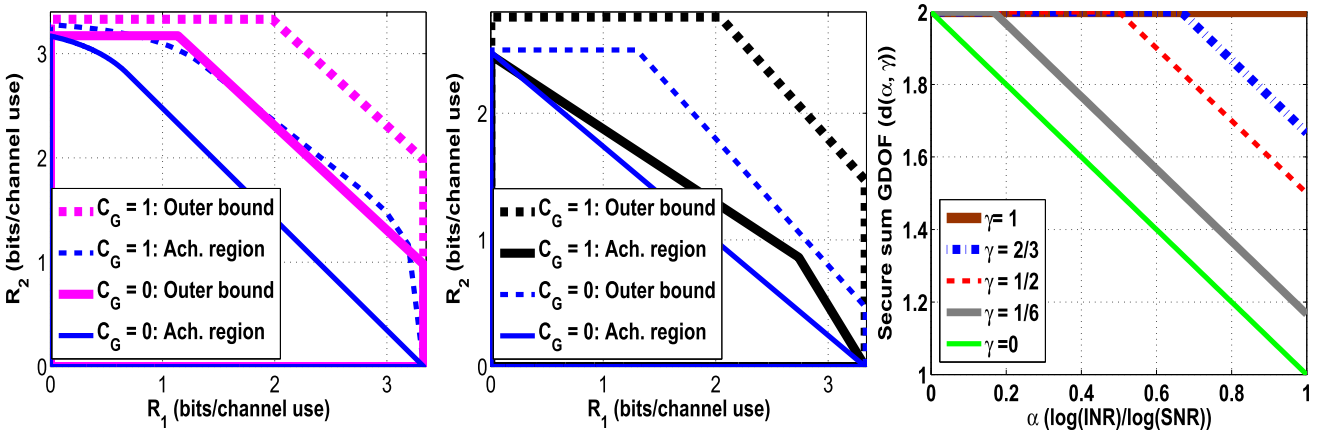
$$R_{\text{sum}} \le C_{\text{sum}} \le C_{\text{sum}}^{\text{outer}} \le R_{\text{sum}} + 2, \tag{28}$$

where R_{sum} and $C_{\text{sum}}^{\text{outer}}$ correspond to the lower bound and upper bound on the secure sum capacity, respectively.

Proof: See Appendix F. ∎

VII. Numerical Results and Discussion

In Fig. 6a, the secure sum capacity of the deterministic Z-IC is plotted against α for different values of C using the result in Sec. III. In this case, the secure sum capacity is normalized by m. When $C = 0$, as α increases, the sum



(a) (b) (c)

Fig. 7. (a) Achievable rate region for the Gaussian model in the weak/moderate interference regime: $P = 100$, $h_d = 1$, $h_c = 0.5$ and $\alpha = 0.69$; (b) Achievable rate region for the Gaussian model in the high interference regime: $P = 100$, $h_d = 1$, $h_c = 1.5$ and $\alpha = 1.17$; and (c) Secure sum GDOF in the weak/moderate interference regime for the Gaussian model. In the plot, γ corresponds to the scaling of the capacity of the cooperative link with respect to 0.5 log SNR.

capacity decreases and becomes constant for $\alpha > 1$. As the value of the cooperative link increases, in the initial part of the weak interference regime, both users can achieve the maximum rate, i.e., m. This is due to the fact that the capacity of the cooperative link is sufficient to cancel the interference at receiver 1. However, with further increase in the value of C, the secure sum capacity starts decreasing. In the very high interference regime, user 2 cannot achieve any nonzero secrecy rate irrespective of the value of C.

In Fig. 6b, the upper bounds on the secrecy capacity region of the Z-IC in Theorems 6, 7 and 8 are compared for the weak/moderate interference regime. The outer bound in Theorem 7 is tighter than the outer bounds in Theorems 6 and 8 except for the corner points for transmitter 2. Recall that, the outer bound in Theorem 6 does not use the secrecy constraint at the receiver in its derivation. The outer bound in Theorem 8 is derived using the intuitions obtained from the high interference regime case considered in the deterministic model for Theorem 2. This is reflected in the plot as explained above.

In Fig. 6c, the outer bound on the secrecy capacity region of the Z-IC in Theorems 6 and 8 are compared for the high interference regime. The proposed outer bound is tighter than the outer bound in Theorem 6.

In Figs. 7a and 7b, the achievable results in Corollary 1 are plotted along with the outer bounds obtained in Sec. V for different values of C_G, in the weak and high interference regimes, respectively. When $C_G > 0$, a part of the interference can be canceled at the unintended receiver, which leads to a gain in the rate due to cooperation. In particular, the improvement in the sum rate performance for both the cases can be observed from these figures. As the capacity of the cooperative link increases, less power is assigned to send the non-cooperative private message of transmitter 2, which in turn also reduces the loss in rate due to stochastic encoding.

In Fig. 7c, the secure sum GDOF stated in Theorem 9 is plotted against α for various values of γ. From the figure, it can be noticed that with cooperation it is possible for both users to achieve the maximum GDOF, i.e., 1, in the initial part of the weak/moderate interference regime, if the capacity of the cooperative link scales with SNR. In these cases, there is no loss in terms of GDOF due to the secrecy constraint at the receiver.

VIII. Conclusions

This work explored the role of limited-rate unidirectional transmitter cooperation in facilitating secure communication over the 2-user symmetric Z-IC. For the deterministic case, the achievable scheme used a combination of interference cancelation and transmission of random bits. The secrecy capacity region of the deterministic model was characterized over all interference regimes and for all values of C. The study of the deterministic model gave useful insights for the Gaussian case. The proposed scheme for the Gaussian model used a fusion of cooperative precoding for interference cancelation, stochastic encoding and artificial noise transmission for ensuring secrecy of the unintended message at the receiver. The secure sum GDOF of the Gaussian symmetric Z-IC was characterized in the weak/moderate interference regimes. The sum rate capacity was also shown to lie within 2 bits of the outer bound in the weak/moderate interference regime for all values of the capacity of the cooperative link, C_G. The results showed that cooperation between the users can facilitate secure communication over Z-IC except for the very high interference regime. It is also found that secrecy constraint at the receiver does not hurt the capacity in the weak/moderate interference regime for the deterministic model. Similarly, it was found that there is no loss in the secure sum GDOF in the weak/moderate interference regime due to the secrecy constraint at the receiver.

Appendix

A. Proof of Theorem 5

The proof involves analyzing the error probability at the decoders for the proposed encoding scheme, along with equivocation computation. The equivocation computation is necessary to choose how much of its own rate transmitter 2 must sacrifice to keep the non-cooperative private message

secret. The main novelty in the proof lies in precoding of the cooperative private message of transmitter 2 at transmitter 1, which cancels the interference at receiver 1 and at the same time ensures secrecy of the cooperative private message.

1) Error Probability Analysis: For receivers 1 and 2, define the following events: $E_i \triangleq \{(\mathbf{y}_1^N, \mathbf{x}_{p1}^N(i)) \in T_\epsilon^N(P_{Y_1X_{p1}})\}$, and $F_{ijk} \triangleq \{(\mathbf{y}_2^N, \mathbf{x}_{p2}^N(i,j), \mathbf{x}_{cp2}^N(k)) \in T_\epsilon^N(P_{Y_2X_{p2}X_{cp2}})\}$, where $T_\epsilon^N(P_{Y_1X_{p1}})$ denotes the set of jointly typical sequences $\mathbf{y}_1$ and $\mathbf{x}_{p1}$ with respect to $P(\mathbf{y}_1, \mathbf{x}_{p1})$ and $T_\epsilon^N(P_{Y_2X_{p2}X_{cp2}})$ denotes the set of jointly typical sequences $\mathbf{y}_2$, $\mathbf{x}_{p2}$ and $\mathbf{x}_{cp2}$ with respect to $P(\mathbf{y}_2, \mathbf{x}_{p2}, \mathbf{x}_{cp2})$. Without loss of generality, assume that transmitters 1 and 2 send $\mathbf{x}_1^N(1,1)$ and $\mathbf{x}_2^N(1,1,1)$, respectively. An error occurs if the transmitted and received sequences are not jointly typical, or a wrong codeword is jointly typical with the received sequences. Using the union of events bound and asymptotic equipartition property (AEP), it can be shown that $\lambda_{e1}^N = P(E_1^c \bigcup \cup_{i\neq 1} E_i) \leq P(E_1^c) + \sum_{i\neq 1} P(E_i) \to 0$ as $N \to \infty$ provided

$$R_1 \leq I(\mathbf{x}_{p1}; \mathbf{y}_1). \tag{29}$$

Similarly, the probability of error at receiver 2, i.e., $\lambda_{e2}^N = P(F_{111}^c \bigcup \cup_{(i,j,k)\neq(1,1,1)} F_{ijk}) \leq P(F_{111}^c) + \sum_{(i,j,k)\neq(1,1,1)} P(F_{ijk}) \to 0$ as $N \to \infty$ provided

$$\begin{aligned} &R_{p2} + R'_{p2} \leq I(\mathbf{x}_{p2}; \mathbf{y}_2|\mathbf{x}_{cp2}),\ R_{cp2} \leq I(\mathbf{x}_{cp2}; \mathbf{y}_2|\mathbf{x}_{p2}), \\ &R_{p2} + R'_{p2} + R_{cp2} \leq I(\mathbf{x}_{p2}, \mathbf{x}_{cp2}; \mathbf{y}_2). \end{aligned} \tag{30}$$

Due to the rate-limited cooperation, the following condition is required to be satisfied for the cooperative private message

$$R_{cp2} \leq C_G. \tag{31}$$

Hence, using (29), (30), (31), and $R_2 = R_{p2} + R_{cp2}$, (5) is obtained.

In the following, R'_{p2} is determined for ensuring secrecy of the non-cooperative private message of transmitter 2 at receiver 1.

2) Equivocation Computation: For ensuring strong secrecy, the following condition is required to be satisfied[3]

$$\lim_{N\to\infty} I(W_2; \mathbf{y}_1^N) = 0. \tag{32}$$

Consider the following

$$\begin{aligned} I(W_2; \mathbf{y}_1^N) &= I(W_{p2}, W_{cp2}; \mathbf{y}_1^N), \\ &= I(W_{p2}; \mathbf{y}_1^N) + I(W_{cp2}; \mathbf{y}_1^N|W_{p2}). \end{aligned} \tag{33}$$

Note that $H(W_{cp2}|\mathbf{y}_1^N, W_{p2}) = H(W_{cp2})$ because the codeword carrying the cooperative private message is completely canceled at receiver 1 and the cooperative private message is chosen independent of the non-cooperative private message at transmitter 2. Hence, $\lim_{N\to\infty} I(W_{cp2}; \mathbf{y}_1^N|W_{p2}) = 0$. Now, it is required to show that strong secrecy condition is satisfied for the non-cooperative private message of transmitter 2 at receiver 1. First, consider the following:

$$\begin{aligned} I(W_{p2}; \mathbf{y}_1^N) \leq I(W_{p2}; \mathbf{y}_1^N, \mathbf{x}_{p1}^N) &\overset{(a)}{=} I(W_{p2}; \mathbf{y}_1^N|\mathbf{x}_{p1}^N), \\ &\overset{(b)}{=} I(W_{p2}; \mathbf{y}_1'^N), \end{aligned} \tag{34}$$

where (a) is obtained using the fact that W_{p2} is independent of $\mathbf{x}_{p1}^N$ and (b) is obtained using the fact that $\mathbf{x}_{p1}^N$ and $\mathbf{x}_{p2}^N$ are chosen independent of each other during code construction and $\mathbf{y}_1'^N \triangleq h_c\mathbf{x}_{p2}^N + \mathbf{z}_1^N$.

It is not difficult to see that transmitter 2 forms a hypothetical Gaussian wiretap channel with receiver 2 (legitimate user) and receiver 1 (eavesdropper) with outputs $\mathbf{y}_2^N$ and $\mathbf{y}_1'^N$, respectively. Using the result in [39, Corollary 2], one can ensure that $I(W_{p2}; \mathbf{y}_1'^N) \to 0$ as $N \to \infty$ provided

$$R'_{p2} = I(\mathbf{x}_{p2}; \mathbf{y}'_1) + \epsilon_n = I(\mathbf{x}_{p2}; \mathbf{y}_1|\mathbf{x}_{p1}) + \epsilon_n. \tag{35}$$

Note that, although [39, Corollary 2] is stated for the memoryless wiretap channel with additive cost function, the result is applicable in the Gaussian case also, as the approach can be directly generalized from the discrete case to the continuous case [40, Chapter 6].

B. Proof of Corollary 1

The first term in (5) is evaluated as follows

$$R_1 \leq 0.5\log\left(1 + \frac{h_d^2 P_{p1}}{1 + h_d^2 P_{a1} + h_c^2 P_{p2}}\right) \tag{36}$$

where the power allocations are as mentioned in the statement of the theorem. The second term in (5) is simplified as follows

$$R_2 \leq 0.5\log(1 + h_d^2 P_{p2} + h_d^4 P_{cp2}) - R'_{p2}, \tag{37}$$

where $R'_{p2} = 0.5\log\left(1 + \frac{h_c^2 P_{p2}}{1+h_d^2 P_{a1}}\right)$.

The last term in (5) is simplified as follows

$$\begin{aligned} R_2 \leq\ & 0.5\log(1 + h_d^2 P_{p2}) + \min\left\{C_G, 0.5\log(1 + h_d^4 P_{cp2})\right\} \\ & - R'_{p2}. \end{aligned} \tag{38}$$

Taking convex closure of (36) and the minimum of (37) and (38) over different values of θ_i, β_i and λ_i, the achievable secrecy rate in (12) is obtained. The parameters θ_i, β_i and λ_i are defined in the statement of the Corollary. This completes the proof.

C. Proof of Theorem 7

It is easy to see that the rate of transmitter 1 is upper bounded by $0.5\log(1 + \text{SNR})$. Hence, it is required to prove the upper bounds on the rate of transmitter 2 and the sum rate. Using Fano's inequality, the rate of transmitter 2 is upper bounded as follows

$$\begin{aligned} NR_2 &\leq I(W_2; \mathbf{y}_2^N) + N\epsilon_N, \\ &\leq I(W_2; \mathbf{y}_2^N, \mathbf{y}_1^N) + N\epsilon_N, \\ &= I(W_2; \mathbf{y}_1^N) + I(W_2; \mathbf{y}_2^N|\mathbf{y}_1^N) + N\epsilon_N, \\ &\overset{(a)}{\leq} h(\mathbf{y}_2^N|\mathbf{y}_1^N) - h(\mathbf{y}_2^N|\mathbf{y}_1^N, W_2) + N\epsilon_N, \end{aligned}$$

[3]In the equivocation computation, it is assumed for ease of presentation that transmitter 1 does not send any artificial noise. However, the derivation holds even when transmitter 1 sends artificial noise.

or

$$R_2 \overset{(b)}{\leq} \max_{0\leq|\rho|\leq 1} 0.5\log\left(1+\text{SNR} - \frac{(\rho\text{SNR}+\sqrt{\text{SNR}\cdot\text{INR}})^2}{1+\text{SNR}+\text{INR}+2\rho\sqrt{\text{SNR}\cdot\text{INR}}}\right), \tag{39}$$

where (a) is obtained using the secrecy constraint at the receiver 1; (b) is obtained using the approach in [6] and [40].

In the following, the sum rate is upper bounded using Fano's inequality, secrecy constraint at receiver 1 and chain rule of mutual information.

$$\begin{aligned} N[R_1+R_2] &\leq I(W_1;\mathbf{y}_1^N)+I(W_2;\mathbf{y}_2^N)-I(W_2;\mathbf{y}_1^N)+N\epsilon_N,\\ &= I(W_1;\mathbf{y}_1^N)+I(W_2;\mathbf{y}_2^N)-I(W_2;\mathbf{y}_1^N,\mathbf{s}_2^N)\\ &\quad +I(W_2;\mathbf{s}_2^N|\mathbf{y}_1^N)+N\epsilon_N, \end{aligned} \tag{40}$$

where $\mathbf{s}_2^N \triangleq h_c\mathbf{x}_2^N+\mathbf{z}_1^N$.

The main novelty in the proof lies in bounding these mutual information terms. To upper bound the sum rate further, consider the following term of (40), where the cooperative signal $\mathbf{v}_{21}^N$ is provided as side information to both the receivers.

$$\begin{aligned} &I(W_1;\mathbf{y}_1^N)+I(W_2;\mathbf{s}_2^N|\mathbf{y}_1^N)\\ &\overset{(a)}{\leq} I(W_1;\mathbf{y}_1^N|\mathbf{v}_{21}^N)+I(W_2;\mathbf{v}_{21}^N|\mathbf{y}_1^N)+I(W_2;\mathbf{s}_2^N|\mathbf{y}_1^N,\mathbf{v}_{21}^N),\\ &\leq I(W_1,\mathbf{x}_1^N;\mathbf{y}_1^N|\mathbf{v}_{21}^N)+I(W_2;\mathbf{v}_{21}^N|\mathbf{y}_1^N)\\ &\quad +I(W_2;\mathbf{s}_2^N|\mathbf{y}_1^N,\mathbf{v}_{21}^N),\\ &\overset{(b)}{=} I(\mathbf{x}_1^N;\mathbf{y}_1^N|\mathbf{v}_{21}^N)+I(W_2;\mathbf{v}_{21}^N|\mathbf{y}_1^N)+I(W_2;\mathbf{s}_2^N|\mathbf{y}_1^N,\mathbf{v}_{21}^N),\\ &= I(\mathbf{x}_1^N;\mathbf{y}_1^N|\mathbf{v}_{21}^N)+H(\mathbf{v}_{21}^N|\mathbf{y}_1^N)-H(\mathbf{v}_{21}^N|\mathbf{y}_1^N,W_2)\\ &\quad +h(\mathbf{s}_2^N|\mathbf{y}_1^N,\mathbf{v}_{21}^N)-h(\mathbf{s}_2^N|\mathbf{y}_1^N,\mathbf{v}_{21}^N,W_2),\\ &\overset{(c)}{\leq} I(\mathbf{x}_1^N;\mathbf{y}_1^N|\mathbf{v}_{21}^N)+H(\mathbf{v}_{21}^N)+h(\mathbf{s}_2^N,\mathbf{y}_1^N|\mathbf{v}_{21}^N)-h(\mathbf{y}_1^N|\mathbf{v}_{21}^N)\\ &\quad -h(\mathbf{s}_2^N|\mathbf{y}_1^N,\mathbf{v}_{21}^N,W_2),\\ &= I(\mathbf{x}_1^N;\mathbf{y}_1^N|\mathbf{v}_{21}^N)+H(\mathbf{v}_{21}^N)+h(\mathbf{s}_2^N|\mathbf{v}_{21}^N)+h(\mathbf{y}_1^N|\mathbf{s}_2^N,\mathbf{v}_{21}^N)\\ &\quad -h(\mathbf{y}_1^N|\mathbf{v}_{21}^N)-h(\mathbf{s}_2^N|\mathbf{y}_1^N,\mathbf{v}_{21}^N,W_2), \end{aligned} \tag{41}$$

where (a) is obtained using the chain rule for mutual information and the fact that $\mathbf{v}_{21}$ is not a function of W_1; (b) is obtained using the Markov chain relation: $W_1 \rightarrow (\mathbf{v}_{21},\mathbf{x}_1) \rightarrow \mathbf{y}_1$, which can shown using the signal flow graph (SFG) approach in [42]; (c) follows because removing conditioning cannot decrease entropy and $h(\mathbf{s}_2^N,\mathbf{y}_1^N|\mathbf{v}_{21}^N)=h(\mathbf{y}_1^N|\mathbf{v}_{21}^N)+h(\mathbf{s}_2^N|\mathbf{y}_1^N,\mathbf{v}_{21}^N)$.

Note that bounding the differential entropy terms above is difficult as it involves continuous and discrete random variables. To overcome this problem, using relation in (3), it can be shown that $h(\mathbf{s}_2^N|\mathbf{v}_{21}^N)=h(\mathbf{s}_2^N|\mathbf{v}_{21}^N,\mathbf{x}_1^N)$. This also implies that $h(\mathbf{s}_2^N|\mathbf{v}_{21}^N,\mathbf{x}_1^N)=h(\mathbf{y}_1^N|\mathbf{v}_{21}^N,\mathbf{x}_1^N)$. This is one of the key steps in the derivation as it leads to cancelation of $I(\mathbf{x}_1^N;\mathbf{y}_1^N|\mathbf{v}_{21}^N)$ as shown below.

$$\begin{aligned} &I(W_1;\mathbf{y}_1^N)+I(W_2;\mathbf{s}_2^N|\mathbf{y}_1^N)\\ &\leq I(\mathbf{x}_1^N;\mathbf{y}_1^N|\mathbf{v}_{21}^N)+H(\mathbf{v}_{21}^N)+h(\mathbf{s}_2^N|\mathbf{v}_{21}^N,\mathbf{x}_1^N)\\ &\quad +h(\mathbf{y}_1^N|\mathbf{s}_2^N,\mathbf{v}_{21}^N)-h(\mathbf{y}_1^N|\mathbf{v}_{21}^N)-h(\mathbf{s}_2^N|\mathbf{y}_1^N,\mathbf{v}_{21}^N,W_2),\\ &= I(\mathbf{x}_1^N;\mathbf{y}_1^N|\mathbf{v}_{21}^N)+H(\mathbf{v}_{21}^N)+h(\mathbf{y}_1^N|\mathbf{v}_{21}^N,\mathbf{x}_1^N)\\ &\quad +h(\mathbf{y}_1^N|\mathbf{s}_2^N,\mathbf{v}_{21}^N)-h(\mathbf{y}_1^N|\mathbf{v}_{21}^N)-h(\mathbf{s}_2^N|\mathbf{y}_1^N,\mathbf{v}_{21}^N,W_2),\\ &\overset{(a)}{\leq} I(\mathbf{x}_1^N;\mathbf{y}_1^N|\mathbf{v}_{21}^N)+NC_G-I(\mathbf{x}_1^N;\mathbf{y}_1^N|\mathbf{v}_{21}^N)\\ &\quad +h(\mathbf{y}_1^N|\mathbf{s}_2^N,\mathbf{v}_{21}^N)-h(\mathbf{s}_2^N|\mathbf{y}_1^N,\mathbf{v}_{21}^N,W_2,\mathbf{x}_2^N),\\ &\overset{(b)}{=} NC_G+h(\mathbf{y}_1^N|\mathbf{s}_2^N,\mathbf{v}_{21}^N)-h(\mathbf{s}_2^N|\mathbf{y}_1^N,\mathbf{v}_{21}^N,\mathbf{x}_2^N),\\ &= NC_G+h(\mathbf{y}_1^N|\mathbf{s}_2^N,\mathbf{v}_{21}^N)-h(\mathbf{s}_2^N,\mathbf{y}_1^N|\mathbf{v}_{21}^N,\mathbf{x}_2^N)\\ &\quad +h(\mathbf{y}_1^N|\mathbf{v}_{21}^N,\mathbf{x}_2^N),\\ &= h(\mathbf{y}_1^N|\mathbf{s}_2^N,\mathbf{v}_{21}^N)-h(\mathbf{s}_2^N|\mathbf{x}_2^N,\mathbf{v}_{21}^N)-h(\mathbf{y}_1^N|\mathbf{s}_2^N,\mathbf{x}_2^N,\mathbf{v}_{21}^N)\\ &\quad +h(\mathbf{y}_1^N|\mathbf{x}_2^N,\mathbf{v}_{21}^N)+NC_G,\\ &\overset{(c)}{\leq} h(\mathbf{s}_1^N)-h(\mathbf{z}_1^N)+NC_G, \end{aligned} \tag{42}$$

where $\mathbf{s}_1^N \triangleq h_d\mathbf{x}_1^N+\mathbf{z}_1^N$; (a) is obtained using the fact that conditioning cannot increase the differential entropy and $H(\mathbf{v}_{21}^N) \leq NC_G$; (b) is obtained using the fact that $I(W_2;\mathbf{s}_2^N|\mathbf{y}_1^N,\mathbf{v}_{21}^N,\mathbf{x}_2^N)=0$, which can again be shown with the help of an SFG [42]; and (c) is obtained by noticing that first and third term cancel with each other using the relation in (3) and using the fact that conditioning cannot increase the differential entropy.

Now, consider the bounding of the remaining two terms in (40). As it involves the difference of two mutual information terms, it is not straightforward to upper bound these terms. In the weak/moderate interference regime, the channel from transmitter 2 to receiver 1 is weaker than the channel from transmitter 2 to receiver 2. Hence, $\mathbf{x}_2$, $\mathbf{y}_2$ and $\mathbf{s}_2$ satisfy the following Markov chain: $\mathbf{x}_2 \rightarrow \mathbf{y}_2 \rightarrow \mathbf{s}_2$ and this channel can be viewed as a degraded broadcast channel. Using the result in [29] and [42], the following bound is obtained.

$$\begin{aligned} &I(W_2;\mathbf{y}_2^N)-I(W_2;\mathbf{y}_1^N,\mathbf{s}_2^N)\\ &\quad = I(W_2;\mathbf{y}_2^N)-I(W_2;\mathbf{s}_2^N)-I(W_2,\mathbf{y}_1^N|\mathbf{s}_2^N),\\ &\quad \leq I(W_2;\mathbf{y}_2^N)-I(W_2;\mathbf{s}_2^N) \leq N[I(\mathbf{x}_2;\mathbf{y}_2)-I(\mathbf{x}_2;\mathbf{s}_2)]. \end{aligned} \tag{43}$$

Finally, using (42) and (43), (40) becomes

$$R_1+R_2 \leq \log(1+\text{SNR})-0.5\log(1+\text{INR})+C_G. \tag{44}$$

This completes the proof.

D. Proof of Theorem 8

As mentioned earlier, the rate of transmitter 1 is upper bounded by $0.5\log(1+\text{SNR})$. Hence, it is required to prove the upper bounds on the rate of transmitter 2 and the sum rate. Using the steps used to obtain outer bound on the rate of user 2 in the proof of Theorem 7, the following bound is obtained

$$NR_2 \leq \max_{0\leq|\rho|\leq 1} 0.5\log\left(1+\text{SNR} - \frac{(\rho\text{SNR}+\sqrt{\text{SNR}\cdot\text{INR}})^2}{1+\text{SNR}+\text{INR}+2\rho\sqrt{\text{SNR}\cdot\text{INR}}}\right). \tag{45}$$

The derivation of the outer bound on the sum rate goes as follows. First, an outer bound on the rate of user 1 is obtained. Then, an outer bound on the rate of user 2 is derived. Adding these two outer bounds leads to cancelation of negative

differential entropy terms, which in turn allows one to obtain a single letter characterization of the sum rate outer bound.

In the following, an outer bound on the rate of user 1 is obtained by providing $\mathbf{y}_2^N$ as side information to receiver 1.

$$\begin{aligned} NR_1 &\leq I(W_1; \mathbf{y}_1^N, \mathbf{y}_2^N) + N\epsilon_N, \\ &\overset{(a)}{=} I(W_1; \mathbf{y}_1^N | \mathbf{y}_2^N) + N\epsilon_N, \\ &\overset{(b)}{\leq} h(\mathbf{y}_1^N | \mathbf{y}_2^N) - h(\mathbf{s}_1^N | \mathbf{y}_2^N, W_1, \mathbf{x}_2^N, \mathbf{v}_{21}^N) + N\epsilon_N, \\ &\quad \text{where } \mathbf{s}_1^N \triangleq h_d \mathbf{x}_1^N + \mathbf{z}_1^N \\ &\overset{(c)}{=} h(\mathbf{y}_1^N | \mathbf{y}_2^N) - h(\tilde{\mathbf{s}}_1^N | \mathbf{y}_2^N, W_1, \mathbf{x}_2^N, \mathbf{v}_{21}^N) + N\epsilon_N, \\ &\quad \text{where } \tilde{\mathbf{s}}_1^N \triangleq h_d \mathbf{x}_1^N + \tilde{\mathbf{z}}_1^N, \\ &\overset{(d)}{=} h(\mathbf{y}_1^N | \mathbf{y}_2^N) - h(\tilde{\mathbf{s}}_1^N | W_1, \mathbf{v}_{21}^N) + N\epsilon_N, \end{aligned} \tag{46}$$

where (a) is obtained using the fact that $\mathbf{y}_2^N$ is independent of W_1; (b) is obtained using the fact that conditioning cannot increase the differential entropy; (c) is obtained using the fact that the secrecy capacity region of the Z-IC with confidential messages is invariant under any joint channel noise distribution $P(\mathbf{z}_1^N, \mathbf{z}_2^N)$ that leads to the same marginal distributions $P(\mathbf{z}_1^N)$ and $P(\mathbf{z}_2^N)$ [44]. Although this invariance property is stated for the Gaussian IC in [44], it holds for the Z-IC with limited-rate transmitter cooperation also. The need for replacing $\mathbf{z}_1^N$ with $\tilde{\mathbf{z}}_1^N$ will become clear later in the proof. Finally, (d) is obtained using the relation in (3).

Next, to bound the rate of user 2, starting from Fano's inequality, one proceeds as follows. The genie provides $(\mathbf{y}_1^N, W_1)$ as side information to receiver 2 and the rate of user 2 is further upper bounded as follows

$$NR_2 \leq I(W_2; \mathbf{y}_1^N, W_1) + I(W_2; \mathbf{y}_2^N | \mathbf{y}_1^N, W_1) + N\epsilon_N. \tag{47}$$

Consider the first term in (47)

$$\begin{aligned} I(W_2; \mathbf{y}_1^N, W_1) &\overset{(a)}{\leq} N\epsilon_N + H(W_1 | \mathbf{y}_1^N) - H(W_1 | \mathbf{y}_1^N, W_2), \\ &\overset{(b)}{\leq} N\epsilon_N, \end{aligned} \tag{48}$$

where (a) is obtained using the secrecy constraint at receiver 1, i.e., $I(W_2; \mathbf{y}_1^N) \leq N\epsilon_N$ and (b) is obtained from the reliability condition for message W_1, i.e., $H(W_1 | \mathbf{y}_1^N) \leq N\delta_N$ and dropping the negative entropy term. In the above, for notational simplicity, δ_N is absorbed into ϵ_N. Using (48), (47) reduces to

$$\begin{aligned} NR_2 &\leq I(W_2; \mathbf{y}_2^N, \mathbf{v}_{21}^N | \mathbf{y}_1^N, W_1) + N\epsilon_N, \\ &= I(W_2; \mathbf{v}_{21}^N | \mathbf{y}_1^N, W_1) + I(W_2; \mathbf{y}_2^N | \mathbf{v}_{21}^N, \mathbf{y}_1^N, W_1) + N\epsilon_N. \end{aligned} \tag{49}$$

To bound the rate of user 2 further, $\tilde{\mathbf{s}}_1^N$ is included in the second mutual information term. In the following, it can be noticed that working with $\tilde{\mathbf{s}}_1^N$ instead of $\mathbf{s}_1^N$ leads to $-h(\tilde{\mathbf{z}}_1^N)$ instead of 0. Thus, replacing the noise in $\mathbf{s}_1^N$ with an independent noise leads to a tighter outer bound. Hence, the outer bound on R_2 becomes

$$\begin{aligned} R_2 &\leq H(\mathbf{v}_{21}^N | \mathbf{y}_1^N, W_1) - H(\mathbf{v}_{21}^N | \mathbf{y}_1^N, W_1, W_2) \\ &\quad + I(W_2; \mathbf{y}_2^N, \tilde{\mathbf{s}}_1^N | \mathbf{v}_{21}^N, \mathbf{y}_1^N, W_1) + N\epsilon_N, \\ &\overset{(a)}{\leq} H(\mathbf{v}_{21}^N) + I(W_2; \tilde{\mathbf{s}}_1^N | \mathbf{v}_{21}^N, \mathbf{y}_1^N, W_1) \\ &\quad + I(W_2; \mathbf{y}_2^N | \mathbf{v}_{21}^N, \mathbf{y}_1^N, W_1, \tilde{\mathbf{s}}_1^N) + N\epsilon_N, \\ &\overset{(b)}{\leq} H(\mathbf{v}_{21}^N) + h(\tilde{\mathbf{s}}_1^N | \mathbf{v}_{21}^N, W_1) \\ &\quad - h(\tilde{\mathbf{s}}_1^N | \mathbf{v}_{21}^N, \mathbf{y}_1^N, W_1, W_2, \mathbf{x}_1^N, \mathbf{x}_2^N) + h(\mathbf{y}_2^N | \mathbf{y}_1^N, \tilde{\mathbf{s}}_1^N) \\ &\quad - h(\mathbf{y}_2^N | \mathbf{v}_{21}^N, \mathbf{y}_1^N, W_1, \tilde{\mathbf{s}}_1^N, W_2, \mathbf{x}_2^N) + N\epsilon_N, \\ &= H(\mathbf{v}_{21}^N) + h(\tilde{\mathbf{s}}_1^N | \mathbf{v}_{21}^N, W_1) - h(\tilde{\mathbf{z}}_1^N) + h(\mathbf{y}_2^N | \mathbf{y}_1^N, \tilde{\mathbf{s}}_1^N) \\ &\quad - h(\mathbf{z}_2^N) + N\epsilon_N, \end{aligned} \tag{50}$$

where (a) and (b) are obtained using the fact that removing (or adding) conditioning cannot decrease (or cannot increase) the differential entropy.

Adding (46) and (50), the following is obtained

$$\begin{aligned} &R_1 + R_2 \\ &\leq H(\mathbf{v}_{21}) + h(\mathbf{y}_1 | \mathbf{y}_2) + h(\mathbf{y}_2 | \mathbf{y}_1, \tilde{\mathbf{s}}_1) - h(\tilde{\mathbf{z}}_1) - h(\mathbf{z}_2), \\ &\leq \max_{0 \leq |\rho| \leq 1} C_G + 0.5 \log \Bigg[1 + \mathrm{SNR} + \mathrm{INR} + 2\rho\sqrt{\mathrm{SNR} \cdot \mathrm{INR}} \\ &\qquad - \frac{(\rho \mathrm{SNR} + \sqrt{\mathrm{SNR} \cdot \mathrm{INR}})^2}{1 + \mathrm{SNR}} \Bigg] \\ &\quad + 0.5 \log \Sigma_{y_2|s}, \end{aligned} \tag{51}$$

where $\Sigma_{\mathbf{y}_2|\mathbf{s}}$ is as defined in the statement of the theorem. The above inequality is obtained using the approach in [6] and [40]. The individual terms in the above equations are obtained as follows: $h(\mathbf{y}_1|\mathbf{y}_2) = 0.5 \log 2\pi e \Sigma_{\mathbf{y}_1|\mathbf{y}_2}$, where $\Sigma_{\mathbf{y}_1|\mathbf{y}_2} = E[\mathbf{y}_1^2] - \frac{E[\mathbf{y}_1\mathbf{y}_2]^2}{E[\mathbf{y}_2^2]} = 1 + \mathrm{SNR} + \mathrm{INR} + 2\rho\sqrt{\mathrm{SNR} \cdot \mathrm{INR}} - \frac{(\rho \mathrm{SNR} + \sqrt{\mathrm{SNR} \cdot \mathrm{INR}})^2}{1 + \mathrm{SNR}}$. The term $\Sigma_{\mathbf{y}_2|\mathbf{s}}$ is obtained as follows: $\Sigma_{\mathbf{y}_2|\mathbf{s}} = E[\mathbf{y}_2^2] - E[\mathbf{y}_2\mathbf{s}^T] E[\mathbf{s}\mathbf{s}^T]^{-1} E[\mathbf{s}\mathbf{y}_2] = 1 + \mathrm{SNR} - \Sigma_{\mathbf{y}_2,\mathbf{s}} \Sigma_{\mathbf{s},\mathbf{s}}^{-1} \Sigma_{\mathbf{y}_2,\mathbf{s}}^T$, where $\mathbf{s} \triangleq [\tilde{\mathbf{s}}_1 \ \ \mathbf{y}_1]^T$. In the above equation, the terms $\Sigma_{\mathbf{y}_2,\mathbf{s}}$ and $\Sigma_{\mathbf{s},\mathbf{s}}$ are as defined in the statement of the theorem. This completes the proof.

E. Proof of Theorem 9

Using Corollary 1 and the power allocation in (26), the lower bound on the sum rate reduces to

$$\begin{aligned} &R_1 + R_2 \\ &\leq 0.5 \log \left(1 + \frac{P}{4}\right) + \min \left\{ 0.5 \log \left(1 + \frac{1}{2h_c^2} + \frac{P}{2}\right), \right. \\ &\quad \left. 0.5 \log \left(1 + \frac{1}{h_c^2}\right) + \min \left\{ C_G, 0.5 \log \left(1 + \right.\right.\right. \\ &\qquad \left.\left.\left. \frac{1}{2} \left(P - \frac{1}{h_c^2} \right) \right) \right\} \right\} - 0.5 \log 2, \\ &= 0.5 \log \mathrm{SNR} + \min \left\{ 0.5 \log \mathrm{SNR}, 0.5 \log \frac{\mathrm{SNR}}{\mathrm{INR}} \right. \\ &\qquad \left. + \min \left\{ C_G, 0.5 \log \mathrm{SNR} \right\} \right\} + \mathcal{O}(1), \end{aligned}$$

or

$$d_{\mathrm{sum}}(\kappa, \gamma) = \min\{2, 2 - \kappa + \min(1, \gamma)\}. \tag{52}$$

Hence, the achievable sum GDOF becomes

$$d_{\mathrm{sum}}(\kappa, \gamma) = \min\{2, 2 - \kappa + \gamma\}. \tag{53}$$

To establish the GDOF optimality of the proposed scheme, consider the following trivial outer bound on the sum rate, i.e., $R_1 + R_2 \leq \log(1 + \text{SNR})$. Hence, the outer bound on the secure sum GDOF becomes $d_{\text{sum}}(\kappa, \gamma) \leq 2$.

Next, consider the outer bound on the sum rate in Theorem 6

$$\begin{aligned} R_1 + R_2 &\leq 0.5\log(1 + \text{SNR} + \text{INR} + 2\sqrt{\text{SNR}\cdot\text{INR}}) \\ &\quad + 0.5\log\left(1 + \frac{\text{SNR}}{1+\text{INR}}\right) + C_G, \\ &\leq 0.5\log(1 + 3\text{SNR} + \text{INR}) + 0.5\log(1 + \text{SNR} + \text{INR}) \\ &\quad - 0.5\log(1 + \text{INR}) + C_G, \\ &= \log\text{SNR} - 0.5\log\text{INR} + C_G + \mathcal{O}(1), \end{aligned}$$

or

$$d_{\text{sum}}(\kappa, \gamma) \leq 2 - \kappa + \gamma. \tag{54}$$

Next, starting from the sum rate bound in Theorem 7 and using a similar procedure as the above, it can be shown that $d_{\text{sum}}(\kappa, \gamma) \leq 2 - \kappa + \gamma$. Hence, although (unlike Theorem 6) Theorem 7 was derived accounting for the secrecy constraint, both the theorems lead to the same outer bound on the GDOF:

$$d_{\text{sum}}(\kappa, \gamma) \leq \min\{2, 2 - \kappa + \gamma\}. \tag{55}$$

It can be verified that the outer bound in (55) coincides with the achievable GDOF in (53). Hence, the proposed scheme is GDOF optimal, and this completes the proof.

F. Proof of Theorem 10

Using Corollary 1 and the power allocation in (26), the lower bound on the sum rate reduces to

$$\begin{aligned} &R_1 + R_2 \\ &\geq 0.5\log\left(1 + \frac{P_{p1}}{1 + h_c^2 P_{p2}}\right) + \min\{\underbrace{0.5\log(1 + P_{p2} + P_{cp2})}_{I_1}, \\ &\quad \underbrace{0.5\log(1 + P_{p2}) + \min\{C_G, 0.5\log(1 + P_{cp2})\}}_{I_2}\} \\ &\qquad - 0.5\log(1 + h_c^2 P_{p2}). \end{aligned} \tag{56}$$

To bound the gap, consider the following exhaustive cases:

1) When $I_1 \leq I_2$: In this case, (56) reduces to

$$\begin{aligned} &R_1 + R_2 \\ &\geq 0.5\log\left(1 + \frac{P}{4}\right) + 0.5\log\left(1 + \frac{1}{2h_c^2} + \frac{P}{2}\right) - 0.5\log 2, \end{aligned} \tag{57}$$

$$> 0.5\log(1 + \text{SNR}) + 0.5\log(1 + \text{SNR}) - 2. \tag{58}$$

A trivial outer bound on the sum rate is $R_1 + R_2 < \log(1 + \text{SNR})$. Hence, comparing this outer bound on the sum rate with (58), the gap is at most 2 bits/s/Hz.

2) When $I_1 > I_2$ and $0.5\log(1 + P_{cp2}) > C_G$: In this case, the lower bound on the sum rate in (56) reduces to

$$\begin{aligned} R_1 + R_2 &\geq 0.5\log\left(1 + \frac{\text{SNR}}{4}\right) + 0.5\log\left(1 + \frac{\text{SNR}}{\text{INR}}\right) + C_G \\ &\quad - 0.5\log(1 + h_c^2 P_{p2}), \\ &> 0.5\log(1+\text{SNR}) + 0.5\log\left(1 + \frac{\text{SNR}}{\text{INR}}\right) + C_G - 1.5. \end{aligned} \tag{59}$$

To calculate the gap, the following outer bound on the sum rate in Theorem 7 is used.

$$R_1 + R_2 \leq \log(1 + \text{SNR}) - 0.5\log(1 + \text{INR}) + C_G. \tag{60}$$

Subtracting (59) from the sum rate outer bound in (60), it can be seen that the gap is at most 2 bits/s/Hz.

3) When $I_1 > I_2$ and $0.5\log(1 + P_{cp2}) \leq C_G$: In this case, the lower bound on the sum rate reduces to (57), for which the gap is shown to be at most 2 bits/s/Hz.

Hence, the sum rate capacity of the Z-IC with unidirectional transmitter cooperation and the secrecy constraints at the receivers is within 2 bits/s/Hz of the outer bound. This completes the proof.

REFERENCES

[1] P. Mohapatra and C. R. Murthy, "Capacity of the deterministic Z-interference channel with unidirectional transmitter cooperation and secrecy constraints," in *Proc. ISIT*, Jun. 2015, pp. 944–948.

[2] P. Mohapatra and C. R. Murthy, "On the capacity of the two-user symmetric interference channel with transmitter cooperation and secrecy constraints," *IEEE Trans. Inf. Theory*, vol. 62, no. 10, pp. 5664–5689, Oct. 2016.

[3] P. Mohapatra and C. R. Murthy, "Secrecy in the 2-user symmetric deterministic interference channel with transmitter cooperation," in *Proc. SPAWC*, Jun. 2013, pp. 270–274.

[4] N. Liu and S. Ulukus, "On the capacity region of the Gaussian Z-channel," in *Proc. GLOBECOM*, vol. 1. Nov./Dec. 2004, pp. 415–419.

[5] N. Liu, D. Gündüz, and W. Kang, "Capacity results for a class of deterministic Z-interference channels with unidirectional receiver conferencing," in *Proc. 6th Int. ICST Conf. Commun. Netw. China*, Aug. 2011, pp. 580–584.

[6] S. A. Jafar, "Topological interference management through index coding," *IEEE Trans. Inf. Theory*, vol. 60, no. 1, pp. 529–568, Jan. 2014.

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

[8] R. Liu, I. Maric, P. Spasojević, 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.

[9] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3323–3332, Jun. 2011.

[10] C. Geng, R. Tandon, and S. A. Jafar, "On the symmetric 2-user deterministic interference channel with confidential messages," in *Proc. GLOBECOM*, Dec. 2015, pp. 1–6.

[11] A. B. Carleial, "A case where interference does not reduce capacity (corresp.)," *IEEE Trans. Inf. Theory*, vol. 21, no. 5, pp. 569–570, Sep. 1975.

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

[13] 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.

[14] I.-H. Wang and D. N. C. Tse, "Interference mitigation through limited transmitter cooperation," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2941–2965, May 2011.

[15] I.-H. Wang and D. N. C. Tse, "Interference mitigation through limited receiver cooperation," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2913–2940, May 2011.

[16] V. Prabhakaran and P. Viswanath, "Interference channels with source cooperation," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 156–186, Jan. 2011.
[17] A. Jovicic and P. Viswanath, "Cognitive radio: An information-theoretic perspective," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 3945–3958, Sep. 2009.
[18] E. Ekrem and S. Ulukus, "Effects of cooperation on the secrecy of multiple access channels with generalized feedback," in *Proc. CISS*, Mar. 2008, pp. 791–796.
[19] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 137–155, Jan. 2011.
[20] Z. H. Awan, A. Zaidi, and L. Vandendorpe, "Multiaccess channel with partially cooperating encoders and security constraints," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 7, pp. 1243–1254, Jul. 2013.
[21] O. O. Koyluoglu and H. El Gamal, "Cooperative encoding for secrecy in interference channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 5682–5694, Sep. 2011.
[22] N. Liu and A. J. Goldsmith, "Capacity regions and bounds for a class of Z-interference channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 11, pp. 4986–4994, Nov. 2009.
[23] M. Vaezi and H. V. Poor, "Simplified Han–Kobayashi region for one-sided and mixed Gaussian interference channels," in *Proc. ICC*, May 2016, pp. 1–6.
[24] J. Jiang, I. Maric, A. Goldsmith, S. Shamai (Shitz), and S. Cui, "On the capacity of a class of cognitive Z-interference channels," in *Proc. ICC*, Jun. 2011, pp. 1–6.
[25] M. Vaezi and M. Vu, "On the capacity of the cognitive Z-interference channel," in *Proc. 12th Can. Workshop Inf. Theory (CWIT)*, May 2011, pp. 30–33.
[26] H. Bagheri, A. S. Motahari, and A. K. Khandani, "The approximate capacity region of the Gaussian Z-interference channel with conferencing encoders," *CoRR*, vol. abs/1005.1635, 2010.
[27] L. Zhou and W. Yu, "Gaussian Z-interference channel with a relay link: Achievability region and asymptotic sum capacity," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2413–2426, Apr. 2012.
[28] H. T. Do, T. J. Oechtering, and M. Skoglund, "An achievable rate region for the Gaussian Z-interference channel with conferencing," in *Proc. Allerton*, Sep./Oct. 2009, pp. 75–81.
[29] S. Rini, D. Tuninetti, and N. Devroye, "New results on the capacity of the Gaussian cognitive interference channel," in *Proc. Allerton*, Sep./Oct. 2010, pp. 637–644.
[30] Z. Li, R. D. Yates, and W. Trappe, "Secrecy capacity region of a class of one-sided interference channel," in *Proc. ISIT*, Jul. 2008, pp. 379–383.
[31] R. Bustin, M. Vaezi, R. F. Schaefer, and H. V. Poor, "On the secrecy capacity of the Z-interference channel," in *Proc. Int. Zurich Seminar Commun.*, 2016, p. 190.
[32] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[33] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.
[34] P. Mohapatra, C. R. Murthy, and J. Lee. (Apr. 2016). "Outer bounds on the secrecy capacity region of the 2-user Z interference channel with unidirectional transmitter cooperation." [Online]. Available: https://arxiv.org/abs/1604.02468
[35] P. Mohapatra, C. R. Murthy, and J. Lee. (Apr. 2016). "On the secrecy capacity region of the 2-user Z interference channel with unidirectional transmitter cooperation." [Online]. Available: https://arxiv.org/abs/1604.02442
[36] F. M. J. Willems, "The discrete memoryless multiple access channel with partially cooperating encoders (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 29, no. 3, pp. 441–445, May 1983.
[37] R. D. Yates, D. Tse, and Z. Li, "Secret communication on interference channels," in *Proc. ISIT*, Jul. 2008, pp. 374–378.
[38] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.
[39] M. R. Bloch and J. N. Laneman, "Strong secrecy from channel resolvability," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8077–8098, Dec. 2013.
[40] T. S. Han, *Information-Spectrum Methods in Information Theory*. Springer-Verlag, 2003.
[41] C. Suh and D. N. C. Tse, "Feedback capacity of the Gaussian interference channel to within 2 bits," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2667–2685, May 2011.
[42] G. Kramer, *Topics in Multi-User Information Theory*. Boston, MA, USA: NOW Publishers Inc., 2008.
[43] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
[44] X. He and A. Yener, "A new outer bound for the Gaussian interference channel with confidential messages," in *Proc. CISS*, Mar. 2009, pp. 318–323.

Parthajit Mohapatra received the B.E. degree in electronics and communication engineering from the Biju Patnaik University of Technology, Odisha, India, in 2003, the M.Tech. degree in electronic systems and communications from the National Institute of Technology, Rourkela, India, in 2006, and the Ph.D. degree in electrical communication engineering from the Indian Institute of Science, Bengaluru, India, in 2015. He was a Post-Doctoral Research Fellow with the iTrust, center for research in cyber security, Singapore University of Technology and Design, Singapore, from 2015 to 2016.

He is currently an Assistant Professor with the G. S. Sanyal School of Telecommunications, IIT Kharagpur, Kharagpur, India. His research interests are in the areas of information theoretic secrecy, advanced communication techniques for wireless communication, and union of networking and information theory.

Chandra R. Murthy (S'03–M'06–SM'11) received the B.Tech. degree in electrical engineering from IIT Madras, Chennai, India, in 1998, the M.S. degree in electrical and computer engineering from Purdue University, in 2000, and the Ph.D. degree in electrical and computer engineering from the University of California at San Diego, San Diego, CA, USA, in 2006. From 2000 to 2002, he was an Engineer with Qualcomm Inc., where he worked on WCDMA baseband transceiver design and 802.11b baseband receivers. From 2006 to 2007, he was a Staff Engineer with Beceem Communications Inc., where he worked on advanced receiver architectures for the 802.16e Mobile WiMAX standard. In 2007, he joined the Department of Electrical Communication Engineering, Indian Institute of Science, Bengaluru, India, where he is currently an Associate Professor.

His research interests are in the areas of energy harvesting communications, multiuser MIMO systems, and sparse signal recovery techniques applied to wireless communications. His paper won the best paper award in the Communications Track in the National Conference on Communications 2014. He was an Associate Editor of the IEEE SIGNAL PROCESSING LETTERS from 2012 to 2016. He is an elected member of the IEEE SPCOM Technical Committee from 2014 to 2016. He is currently serving as the Chair of the IEEE Signal Processing Society, Bangalore Chapter, and as an Associate Editor of the IEEE TRANSACTIONS ON SIGNAL PROCESSING.

Jemin Lee (S'06–M'11) received the B.S. (Hons.), M.S., and Ph.D. degrees in electrical and electronic engineering from Yonsei University, Seoul, South Korea, in 2004, 2007, and 2010, respectively. She was a Temasek Research Fellow with the iTrust, Centre for Research in Cyber Security, Singapore University of Technology and Design, Singapore, from 2014 to 2016, and was a Post-Doctoral Fellow with the Massachusetts Institute of Technology, Cambridge, MA, USA, from 2010 to 2013. She is currently an Assistant Professor with the Department of Information and Communication Engineering, Daegu Gyeongbuk Institute of Science and Technology. Her current research interests include physical layer security, wireless security, heterogeneous networks, cognitive radio networks, and cooperative communications.

Dr. Lee received the IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award in 2014, the Temasek Research Fellowship in 2013, the Chun-Gang Outstanding Research Award in 2011, and the IEEE WCSP Best Paper Award in 2014. She is currently an Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and the IEEE COMMUNICATIONS LETTERS, and served as a Guest Editor of the IEEE WIRELESS COMMUNICATIONS, Special Issue on LTE in Unlicensed Spectrum, 2016, and the *Elsevier Physical Communication*, Special Issues on Physical Layer Security in 2016 and Heterogeneous and Small Cell Networks in 2014.