Adding Common Randomness Can Remove the Secrecy Penalty in GDoF

Fan Li and Jinyuan Chen

***Abstract*—In communication networks secrecy constraints *usually* incur an extra limit in capacity or generalized degrees-of-freedom (GDoF), in the sense that a penalty in capacity or GDoF is incurred due to the secrecy constraints. Over the past decades a significant amount of effort has been made by the researchers to understand the limits of secrecy constraints in communication networks. In this work, we focus on how to remove the secrecy penalty in communication networks, i.e., how to remove the GDoF penalty due to secrecy constraints. We begin with three basic settings: a two-user symmetric Gaussian interference channel with confidential messages, a symmetric Gaussian wiretap channel with a helper, and a two-user symmetric Gaussian multiple access wiretap channel. Interestingly, in this work we show that adding common randomness at the transmitters can *totally* remove the penalty in GDoF or GDoF region of the three settings considered here. The results reveal that adding common randomness at the transmitters is a powerful way to remove the secrecy penalty in communication networks in terms of GDoF performance. Common randomness can be generated offline before the real-time message communication. The role of the common randomness is to jam the information signal at the eavesdroppers, without causing too much interference at the legitimate receivers. To accomplish this role, a new method of Markov chain-based interference neutralization is proposed in the achievability schemes utilizing common randomness. From the practical point of view, we need to minimize the amount of common randomness used for removing the secrecy penalty in terms of GDoF performance. With this motivation, for most of the cases we characterize the minimal GDoF of common randomness to remove secrecy penalty, based on our derived converses and achievability.**

***Index Terms*—Information-theoretic security, generalized degrees-of-freedom (GDoF), common randomness, interference neutralization, interference networks.**

I. Introduction

For the secure communications with secrecy constraints, the confidential messages need to be transmitted reliably to the legitimate receiver(s), without leaking the confidential information to the eavesdroppers (cf. [1], [2]). In communication networks secrecy constraints *usually* impose an extra limit in capacity or generalized degrees-of-freedom (GDoF), in the sense that a penalty in capacity or GDoF is incurred due to secrecy constraints (cf. [2]–[12]). Since Shannon's work of [1] in 1949, a significant amount of effort has been made by the researchers to understand the limits of secrecy constraints in communication networks (cf. [2]–[25] and the references therein). In this work, we focus on how to remove the secrecy penalty in communication networks, i.e., how to remove the GDoF penalty due to secrecy constraints.

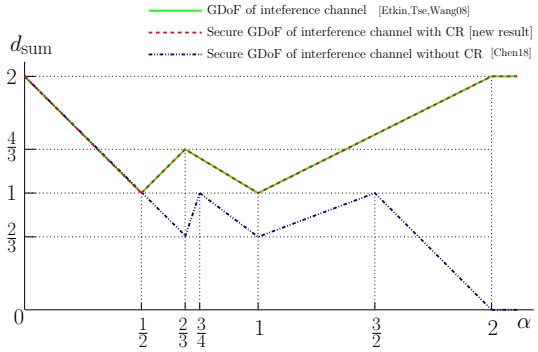

Fig. 1. The optimal secure sum GDoF vs. α, for two-user symmetric Gaussian interference channels without and with common randomness (CR), where α is a channel parameter indicating the interference-to-signal ratio.

In this work we consider three basic settings: a two-user symmetric Gaussian interference channel with secrecy constraints, a symmetric Gaussian wiretap channel with a helper, and a two-user symmetric Gaussian multiple access wiretap channel. Interestingly, we show that adding common randomness at the transmitters can remove the secrecy penalty in these three settings, i.e., it can *totally* remove the penalty in GDoF or GDoF region of the three settings. Let us take a two-user symmetric Gaussian interference channel as an example. For this interference channel *without* secrecy constraints, the GDoF is a "W" curve (see Fig. 1 and [26]). If secrecy constraints are imposed on this channel, then the secure GDoF is significantly reduced, compared to the original "W" curve (see Fig. 1 and [12]). It implies that a GDoF penalty is incurred due to secrecy constraints. Interestingly we show in this work that adding common randomness at the transmitters can totally remove the GDoF penalty due to secrecy constraints (see Fig. 1). The results reveal that adding common randomness at the transmitters is a constructive way to remove the secrecy penalty in terms of GDoF performance in communication networks.

In our settings the common randomness is available at the transmitters but not at the receivers. The role of the common randomness is to jam the information signal at the eavesdroppers, without causing too much interference at the legitimate receivers. By jamming the information signal at the eavesdroppers with common randomness, we seek to remove the penalty in GDoF. However, the jamming signal

Fan Li and Jinyuan Chen are with Louisiana Tech University, Department of Electrical Engineering, Ruston, USA (emails: fli005@latech.edu, jinyuan@latech.edu). This work was presented in part at the 2019 IEEE International Symposium on Information Theory. This work was supported by the NSF EPSCoR-Louisiana Materials Design Alliance (LAMDA) program (grant number #OIA-1946231) and the Louisiana Board of Regents Support Fund (BoRSF) Research Competitiveness Subprogram (grant number #32-4121-40336).

generated from the common randomness needs to be designed carefully so that it must not create too much interference at the legitimate receivers. Otherwise, the interference will incur a new penalty in GDoF. To accomplish the role of the common randomness, a new method of Markov chain-based interference neutralization is proposed in the achievability schemes. The idea of the Markov chain-based interference neutralization method is given as follows: the common randomness is used to generate a certain number of signals with specific directions and powers; one signal is used to jam the information signal at an eavesdropper but it will create an interference at a legitimate receiver; this interference will be neutralized by another signal generated from the same common randomness; the added signal also creates another interference but will be neutralized by the next generated signal; this process repeats until the residual interference is under the noise level. Since one signal is used to neutralize the previous signal and will be neutralized by the next signal, it forms a Markov chain for this interference neutralization process.

In this work we mainly seek to address the two fundamental questions given as: 1) Can we remove the secrecy penalty in GDoF by adding common randomness at the transmitters? 2) What is the minimal amount of common randomness for removing the secrecy penalty in GDoF? In other words, we focus on how to optimally utilize the common randomness that is assumed to be generated already. In one direction of the previous works (e.g., [27]–[43]), the focus is to generate the common randomness (the key) that needs to be shared between the distributed nodes, without leaking information about this common randomness to an eavesdropper. This can be considered as a secret sharing problem, or key generation problem, which is different from the problem studied in this work. This work considers the problem of efficient utilization of the common randomness that has been previously generated.

In the setting considered in this work, common randomness is shared between the transmitters only. This is different from the secret key agreement problem (or cryptography problem) where the common randomness or secret key is normally shared between the transmitter and the receiver. From the practical point of view, sharing common randomness between the transmitters might be more practical than sharing common randomness between the transmitter and the receiver. For example, in the cellular network, if the transmitters are the base stations, the base stations can share the common randomness with high-throughput backhaul cable, as shown in Fig. 2. In the downlink channel, sharing common randomness between base stations (transmitters) is more practical than sharing common randomness between base station (transmitter) and mobile user (receiver). Common randomness can be generated offline when the system is not busy (e.g., during the night-time) before real-time communication. For another example of dense networks, such as microcell network and picocell network, in which the coverage areas of neighboring cells could be highly overlapped and two base stations could send two different messages to one receiver simultaneously. In this scenario, two base stations can share the common randomness in order to improve the secure rates. Again, the common randomness can be generated

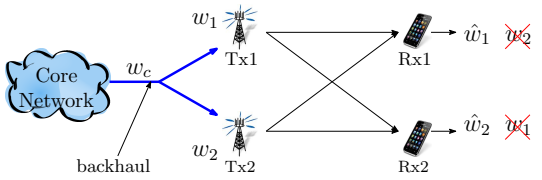

Fig. 2. One example of sharing common randomness in cellular networks.

offline, i.e., when the system is not busy, and can be used later for the real-time communication. Furthermore, in the scenario that the message is sensitive and confidential, the transmitters may not like to share any messages with each other due to the lack of trust between them. In this scenario, the transmitters could share the common randomness only in order to improve the secure rates.

The achievability of this work is based on the pulse amplitude modulation (PAM), rate splitting, signal alignment, distance-outage bounding technique, and Markov chain-based interference neutralization. Note that PAM, rate splitting, signal alignment, and distance-outage bounding technique have been used in the previous works (cf. [12] and [19]), while Markov chain-based interference neutralization is the new technique proposed in this work. While the works in [12] and [19] showed that there is a secrecy penalty in GDoF performance in some settings, this work showed that adding common randomness at the transmitters can totally remove this secrecy penalty.

In terms of the organization of this work, section II describes the system models and section III provides the main results. The converse is described in Section VIII. The achievability is provided in Sections V-VI and some of the appendices, while a scheme example is described in Section IV. The work is concluded in Section IX. Regarding the notations, $\mathbb{I}(\bullet)$, $\mathbb{H}(\bullet)$ and $\mathrm{h}(\bullet)$ denote the mutual information, entropy, and differential entropy, respectively. The notations of $\mathcal{Z}^+$, $\mathcal{R}$ and $\mathcal{N}$ denote the sets of positive integers, real numbers, and nonnegative integers, respectively. We define that $(\bullet)^+ = \max\{\bullet, 0\}$. We consider all the logarithms with base 2. The notation of $f(a) = o(g(a))$ implies that $\lim_{a\to\infty} f(a)/g(a) = 0$.

II. The Three System Models

For this work we focus on three settings: a two-user interference channel with secrecy constraints, a wiretap channel with a helper, and a two-user multiple access wiretap channel (see Fig. 3). These three settings share a common channel input-output relationship, given as

$$y_1(t) = \sqrt{P^{\alpha_{11}}} h_{11} x_1(t) + \sqrt{P^{\alpha_{12}}} h_{12} x_2(t) + z_1(t), \quad (1)$$

$$y_2(t) = \sqrt{P^{\alpha_{21}}} h_{21} x_1(t) + \sqrt{P^{\alpha_{22}}} h_{22} x_2(t) + z_2(t), \quad (2)$$

for $t \in \{1, 2, \cdots, n\}$, where $x_\ell(t)$ represents the transmitted signal of transmitter ℓ at time t, with a normalized power constraint $\mathbb{E}|x_\ell(t)|^2 \le 1$; $y_k(t)$ is the signal received at receiver k; and $z_k(t) \sim \mathcal{N}(0,1)$ is the additive white Gaussian noise, for $k, \ell \in \{1, 2\}$. The term $\sqrt{P^{\alpha_{k\ell}}} h_{k\ell}$ captures the channel gain between receiver k and transmitter ℓ, where $h_{k\ell} \in (1, 2]$ denotes the channel coefficient. The exponent $\alpha_{k\ell}$ represents the *link strength* for the channel between receiver k

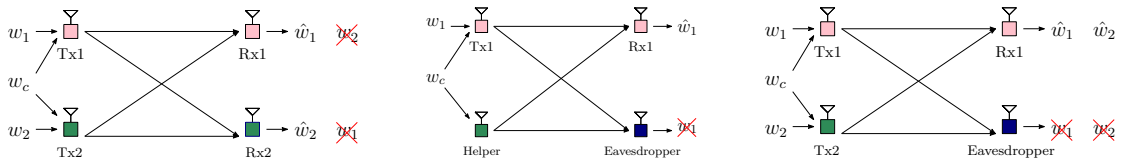

Fig. 3. Three communication settings with common randomness: IC-SC, WTH, and MAC-WT.

and transmitter ℓ. The parameter $P \geq 1$ reflects the base of link strength of all the links. Note that $\sqrt{P^{\alpha_{k\ell}}}h_{k\ell}$ can represent any real channel gain bigger or equal to 1. Thus, the above model in (1) and (2) is able to describe the general channels, in the sense of secure capacity approximation. The channel parameters $\{h_{k\ell}, \alpha_{k\ell}\}_{k\ell}$ are assumed to be available at all the nodes. In this work we focus on the *symmetric* case such that

$$\alpha_{11} = \alpha_{22} = 1, \ \alpha_{12} = \alpha_{21} = \alpha, \ \alpha > 0.$$

The three settings considered here are different, mainly on the number of confidential messages, the intended receivers of the messages, and the secrecy constraints. In what follows, we will present the details of three settings.

A. Interference channel with secrecy constraints (IC-SC)

In the setting of interference channel, transmitter ℓ intends to send the confidential message w_ℓ to receiver ℓ using n channel uses, where the message w_ℓ is independently and uniformly chosen from a set $\mathcal{W}_\ell \triangleq \{1, 2, \cdots, 2^{nR_\ell}\}$, for $\ell \in \{1, 2\}$. To transmit w_ℓ, a function

$$f_\ell : \mathcal{W}_\ell \times \mathcal{W}_c \to \mathcal{R}^n \tag{3}$$

is used to map $w_\ell \in \mathcal{W}_\ell$ to the signal $x_\ell^n = f_\ell(w_\ell, w_c) \in \mathcal{R}^n$, where $w_c \in \mathcal{W}_c$ denotes the *common randomness* that is available at both transmitters but not at the receivers. We assume that w_c is uniformly and independently chosen from a set $\mathcal{W}_c \triangleq \{1, 2, \cdots, 2^{nR_c}\}$. In our setting, w_1, w_2 and w_c are assumed to be mutually independent. We assume that the transmitters are allowed to share the common randomness only, but not the messages. The rate tuple $(R_1(P,\alpha), R_2(P,\alpha), R_c(P,\alpha))$ is said to be achievable if there exists a sequence of n-length codes such that each receiver can decode its desired message reliably, that is,

$$\Pr[\hat{w_k} \neq w_k] \leq \epsilon, \quad \forall k \in \{1, 2\}$$

for any $\epsilon > 0$, and the transmission of the messages is secure, that is,

$$\mathbb{I}(w_1; y_2^n) \leq n\epsilon \quad \text{and} \quad \mathbb{I}(w_2; y_1^n) \leq n\epsilon$$

(known as weak secrecy constraints), as n goes large. The secure capacity region $\bar{C}(P,\alpha)$ represents the collection of all the achievable rate tuples $(R_1(P,\alpha), R_2(P,\alpha), R_c(P,\alpha))$. The secure GDoF region $\bar{\mathcal{D}}(\alpha)$ is defined as

$$\bar{\mathcal{D}}(\alpha) \triangleq \Big\{(d_1, d_2, d_c) : \exists \big(R_1(P,\alpha), R_2(P,\alpha), R_c(P,\alpha)\big) \in \bar{C}(P,\alpha)$$
$$s.t. \ \ d_c = \lim_{P\to\infty} \frac{R_c(P,\alpha)}{\frac{1}{2}\log P}, d_k = \lim_{P\to\infty} \frac{R_k(P,\alpha)}{\frac{1}{2}\log P}, \forall k \in \{1,2\}\Big\}.$$

The secure GDoF region $\mathcal{D}(d_c, \alpha)$ is defined as

$$\mathcal{D}(d_c, \alpha) \triangleq \{(d_1, d_2) : \exists (d_1, d_2, d_c) \in \bar{\mathcal{D}}(\alpha)\}$$

which is a function of d_c and α. The secure sum GDoF is then defined as

$$d_{\text{sum}}(d_c, \alpha) \triangleq \max_{d_1, d_2 : (d_1, d_2) \in \mathcal{D}(d_c, \alpha)} d_1 + d_2.$$

In this setting, for a given α we are interested in the maximal (optimal) secure sum GDoF defined as

$$d_{\text{sum}}^*(\alpha) \triangleq \max_{d_c : d_c \geq 0} d_{\text{sum}}(d_c, \alpha).$$

For a given α, we are also interested in the minimal (optimal) GDoF of the common randomness to achieve the maximal secure sum GDoF, defined as

$$d_c^*(\alpha) \triangleq \min_{d_c : \ d_{\text{sum}}(d_c,\alpha) = d_{\text{sum}}^*(\alpha)} d_c.$$

Note that degrees-of-freedom (DoF) can be treated as a specific case of GDoF by considering $\alpha_{12} = \alpha_{21} = \alpha_{22} = \alpha_{11} = 1$.

B. The wiretap channel with a helper (WTH)

In the setting of wiretap channel with a helper, transmitter 1 wishes to send the confidential message w_1 to receiver 1. This setting is slightly different from the previous interference channel setting, as transmitter 2 will just act as a helper without sending any message in this setting (w_2 can be set as empty). For transmitter 1, the mapping function f_1 is similar as that in the interference channel described in Section II-A. For transmitter 2 (helper), a function $f_2 : \mathcal{W}_c \to \mathcal{R}^n$ maps $w_c \in \mathcal{W}_c$ to the signal $x_2^n = f_2(w_c) \in \mathcal{R}^n$, where $w_c \in \mathcal{W}_c$ denotes the common randomness that is available at both transmitters but not at the receivers. As before, we assume that w_c is uniformly and independently chosen from a set $\mathcal{W}_c = \{1, 2, \cdots, 2^{nR_c}\}$ and w_1 and w_c are mutually independent. We assume that the transmitters are allowed to share the common randomness only, but not the message. A rate pair $(R_1(P,\alpha), R_c(P,\alpha))$ is said to be achievable if there exists a sequence of n-length codes such that receiver 1 can reliably decode its desired message w_1 and the transmission of the message is secure such that $\mathbb{I}(w_1; y_2^n) \leq n\epsilon$ (known as weak secrecy constraints), for any $\epsilon > 0$ as n goes large. The secure capacity region $\bar{C}(P,\alpha)$ denotes the collection of all achievable secure rate pairs $(R_1(P,\alpha), R_c(P,\alpha))$. A secure GDoF region is defined as

$$\bar{\mathcal{D}}(\alpha) \triangleq \Big\{(d, d_c) : \exists \big(R_1(P,\alpha), R_c(P,\alpha)\big) \in \bar{C}(P,\alpha),$$
$$s.t. \ \ d_c = \lim_{P\to\infty} \frac{R_c(P,\alpha)}{\frac{1}{2}\log P}, d = \lim_{P\to\infty} \frac{R_1(P,\alpha)}{\frac{1}{2}\log P}\Big\}.$$

For a given α, we are interested in the maximal (optimal) secure GDoF defined as

$$d^*(\alpha) \triangleq \max_{d,d_c:(d,d_c)\in\bar{\mathcal{D}}(\alpha)} d.$$

For a given α, we are also interested in the minimal (optimal) GDoF of the common randomness to achieve the maximal secure GDoF, defined as

$$d_c^*(\alpha) \triangleq \min_{d_c:(d^*(\alpha),d_c)\in\bar{\mathcal{D}}(\alpha)} d_c.$$

C. Multiple access wiretap channel (MAC-WT)

Let us now consider the two-user Gaussian multiple access wiretap channel. The system model of this channel is similar as that of the interference channel defined in Section II-A. One difference is that both messages w_1 and w_2 are intended to receiver 1 in this setting. Another difference is that receiver 2 now is the eavesdropper. Both messages need to be secure from receiver 2 and the secrecy constraint becomes $\mathbb{I}(w_1, w_2; y_2^n) \leq n\epsilon$. The definitions of the rate tuple $(R_1(P,\alpha), R_2(P,\alpha), R_c(P,\alpha))$, secure capacity region $\bar{C}(P,\alpha)$, and secure GDoF regions $\bar{\mathcal{D}}(\alpha)$ and $\mathcal{D}(d_c,\alpha)$ follow from that in Section II-A. For the multiple access wiretap channel, the secure GDoF region $\mathcal{D}(d_c,\alpha)$ might not be symmetric due to the asymmetric links arriving at receiver 1. In this setting, we will focus on the maximal (optimal) secure GDoF region defined as

$$\mathcal{D}^*(\alpha) \triangleq \{(d_1,d_2) : \exists (d_1,d_2) \in \cup_{d_c} \mathcal{D}(d_c,\alpha)\}.$$

We are also interested in the minimal (optimal) GDoF of the common randomness to achieve any given GDoF pair $(d_1,d_2)\in\mathcal{D}^*(\alpha)$, defined as

$$d_c^*(\alpha,d_1,d_2) \triangleq \min_{d_c:(d_1,d_2)\in\mathcal{D}(d_c,\alpha)} d_c.$$

As mentioned, DoF can be treated as a specific case of GDoF by considering $\alpha = 1$.

III. The main results

We will provide here the main results of the channels defined in Section II. The detailed proofs are provided in Sections V-VIII, as well as the appendices.

A. Removing the secrecy penalty

Theorem 1 (IC-SC)**.** *For almost all the channel coefficients $\{h_{k\ell}\} \in (1,2]^{2\times 2}$ of the symmetric Gaussian IC-SC channel with common randomness (see Section II-A), the optimal characterization of the secure sum GDoF is*

$$d_{sum}^*(\alpha) = \begin{cases} 2(1-\alpha) & \text{for } 0 \leq \alpha \leq \frac{1}{2} \quad (4a) \\ 2\alpha & \text{for } \frac{1}{2} \leq \alpha \leq \frac{2}{3} \quad (4b) \\ 2(1-\alpha/2) & \text{for } \frac{2}{3} \leq \alpha \leq 1 \quad (4c) \\ \alpha & \text{for } 1 \leq \alpha \leq 2 \quad (4d) \\ 2 & \text{for } \alpha \geq 2. \quad (4e) \end{cases}$$

This optimal secure sum GDoF is the same as the optimal sum GDoF of the setting without any secrecy constraint.

Proof. See Section V for the achievability proof. The optimal sum GDoF of the interference channel without common randomness and without secrecy constraint, which is characterized in [26], is serving as the upper bound of the secure sum GDoF of this IC-SC channel with common randomness. Since secrecy constraints will not increase the sum GDoF of a network, the converse derived for the setting without secrecy constraints will server as a converse for the setting with secrecy constraints. Furthermore, we show in Appendix E that adding common randomness at the transmitters will not increase the sum GDoF of a two-user interference channel without secrecy constraints (see Lemma 13 in Appendix E). □

Remark 1. *Note that, without secrecy constraints, the optimal sum GDoF of the interference channel is a "W" curve (see [26] and Fig. 1). With secrecy constraints, the secure sum GDoF of the interference channel is then reduced to a modified "W" curve (see [12]). It implies that there is a penalty in GDoF incurred by the secrecy constraints. Interestingly, Theorem 1 reveals that we can remove this penalty by adding common randomness, in terms of sum GDoF.*

Remark 2. *Our result reveals that in this interference channel adding common randomness at the transmitters can remove the GDoF penalty incurred by the secrecy constraints. However, it remains open if adding common randomness at the transmitters can still remove the capacity penalty incurred by the secrecy constraints. Note that the capacity is unknown in most of the communication networks. Thus, it is challenging to investigate if the capacity penalty can be removed by adding common randomness. In this work, we only focus on the GDoF performance but not the capacity.*

Remark 3. *In this work we just focus on the settings where the transmitters share the common randomness only, but not the messages. In the extreme case where the two transmitters share all of their information including the messages, the interference channel defined in Section II then becomes a two-user MISO channel, in which $\max\{1,\alpha\}$ secure GDoF is achievable for each user. It reveals that, sharing messages provides a secure GDoF gain, compared to the case where only common randomness is shared between the transmitters. However, sharing common randomness is usually more practical than sharing the messages. The common randomness can be generated offline and then used for real-time communication, while the real-time messages might not be feasible to be shared in a timely manner when the system is in the peak time. Furthermore, in the scenario that the message is sensitive and confidential, the transmitters may not like to share any messages with each other due to the lack of trust between them. In this scenario, the transmitters could share the common randomness only in order to improve the secure rates.*

Theorem 2 (WTH)**.** *Given the symmetric Gaussian WTH channel with common randomness (see Section II-B), the optimal secure GDoF is expressed by*

$$d^*(\alpha) = 1, \quad \forall \alpha \in [0,\infty),$$

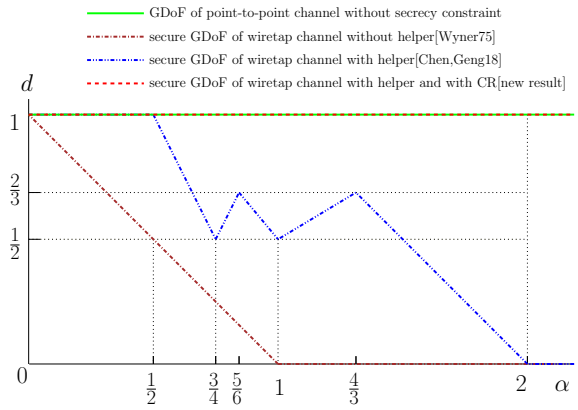

Fig. 4. The optimal secure GDoF vs. α for a wiretap channel with a helper, for the cases with and without common randomness.

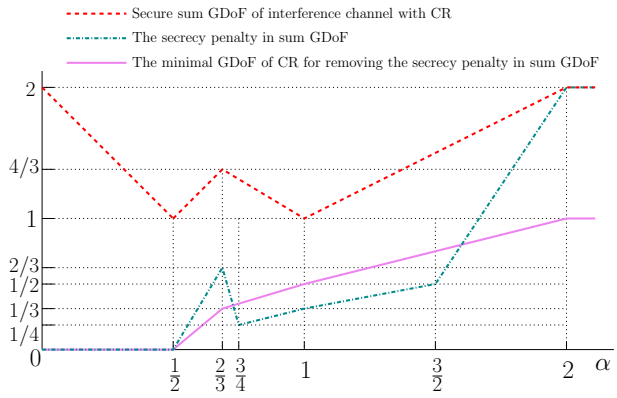

Fig. 5. The secrecy penalty in sum GDoF and the minimal GDoF of CR for removing this penalty for IC-SC setting.

which is the same as the maximal GDoF of the setting without secrecy constraint.

Proof. See Section VI for the achievability proof. Without secrecy constraint, the WTH channel can be enhanced to a point-to-point channel with a helper, and the maximal GDoF of the point-to-point channel with or without a helper is 1. Note that adding common randomness at the transmitters will not increase the GDoF of a point-to-point channel with a helper (see Lemma 14 in Appendix E). □

Remark 4. *For the symmetric Gaussian WTH channel without common randomness, the secure GDoF is another modified "W" curve (see [19] and Fig. 4). Without secrecy constraint, the maximal GDoF of the setting is* 1*. Thus, there is a penalty in GDoF due to secrecy constraint. Theorem 2 reveals that we can remove this GDoF penalty by adding common randomness (see Fig. 4).*

Theorem 3 (MAC-WT)**.** *Given the symmetric Gaussian MAC-WT channel with common randomness (see Section II-C), the optimal secure GDoF region $\mathcal{D}^*(\alpha)$ is the set of all pairs (d_1, d_2) satisfying*

$$d_1 + d_2 \leq \max\{1, \alpha\} \tag{5}$$
$$0 \leq d_1 \leq 1 \tag{6}$$
$$0 \leq d_2 \leq \alpha, \tag{7}$$

which is the same as the optimal GDoF region of the symmetric Gaussian multiple access channel without eavesdropper, i.e., without secrecy constraint.

Proof. The achievability proof is provided in Section VII. The optimal GDoF region of the multiple access channel without secrecy constraint is serving as the outer bound of the optimal secure GDoF region of the MAC-WT channel with common randomness. The optimal GDoF region of the symmetric Gaussian multiple access channel is characterized as in (5)-(7), which can be easily derived from the capacity region of the setting (cf. [44]). Note that adding common randomness at the transmitters will not enlarge the GDoF region of a two-user Gaussian multiple access channel (see Lemma 15 in Appendix E). □

Remark 5. *For the multiple access channel, there is a penalty in GDoF region due to secrecy constraint. For example, considering the case with $\alpha = 1$, the optimal sum GDoF of the multiple access channel without secrecy constraint is* 1*. With secrecy constraint, i.e., with an eavesdropper, the optimal secure sum GDoF of multiple access wiretap channel is reduced to* $2/3$ *(cf. [7]). Therefore, secrecy constraint incurs an extra limit on the GDoF region. Theorem 3 reveals that by adding common randomness we can achieve a secure GDoF region that is the same as the one without secrecy constraint. In other words, with common randomness, secrecy constraint will not incur any penalty in GDoF region of the symmetric multiple access wiretap channel.*

B. How much common randomness is required?

The results in Theorems 1-3 reveal that we can remove the secrecy penalty, i.e., remove the penalty in GDoF, by adding common randomness for each channel considered here. From the practical point of view, we need to minimize the amount of common randomness used for removing the secrecy penalty in terms of GDoF performance. The results on this perspective are given in the following theorems.

Theorem 4 (IC-SC)**.** *For the two-user symmetric Gaussian IC-SC channel, the minimal GDoF of the common randomness to achieve the maximal secure sum GDoF $d^*_{sum}(\alpha)$ is*

$$d^*_c(\alpha) = d^*_{sum}(\alpha)/2 - (1-\alpha)^+ \qquad \alpha \in [0, \infty). \tag{8}$$

Proof. See Section V for the achievability proof and Section VIII-A for the converse proof. □

Remark 6. *For the two-user symmetric Gaussian IC-SC channel, Fig. 5 depicts the secrecy penalty in sum GDoF vs. α, where the secrecy penalty is defined as the difference between the maximal sum GDoF without secrecy constraints and the maximal secure sum GDoF with secrecy constraints but without common randomness. Fig. 5 also depicts the minimal GDoF of common randomness for removing the secrecy penalty in sum GDoF, for $\alpha \in [0, \infty)$, based on the result in Theorem 4. As shown in Fig. 5, it is interesting that at some regime, 1 GDoF of common randomness can remove 2 sum GDoF of secrecy penalty (see the regime when $\alpha \geq 2$).*

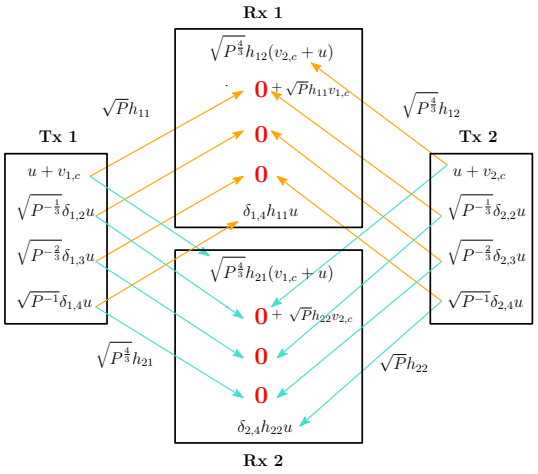

Fig. 6. Markov chain-based interference neutralization at the receivers, for a two-user interference channel with $\alpha = 4/3$.

Theorem 5 (WTH)**.** *For the symmetric Gaussian WTH channel, the minimal GDoF of the common randomness to achieve the maximal secure GDoF $d^*(\alpha)$ is*

$$d_c^*(\alpha) = 1 - (1-\alpha)^+ \qquad \alpha \in [0, \infty).$$

Proof. See Section VI and Section VIII-B for the achievability and converse proofs, respectively. □

For the MAC-WT channel, by focusing on the case of $\alpha = 1$, we were able to characterize the minimal DoF of the common randomness to achieve any given DoF pair (d_1, d_2) in the maximal secure DoF region $\mathcal{D}^*(1)$ expressed in Theorem 3.

Theorem 6 (MAC-WT)**.** *Given the symmetric Gaussian MAC-WT channel, and for $\alpha = 1$, the minimal DoF of the common randomness to achieve any given DoF pair (d_1, d_2) in the maximal secure DoF region $\mathcal{D}^*(1)$ is*

$$d_c^*(1, d_1, d_2) = \max\{d_1, d_2\} \quad \textit{for} \quad (d_1, d_2) \in \mathcal{D}^*(1),\ \alpha = 1.$$

Proof. The achievability and converse proofs are provided in Section VII and Section VIII-C, respectively. □

Remark 7. *When $\alpha = 1$, Theorem 6 reveals that the minimal DoF of the common randomness to achieve the secure DoF pair $(d_1 = 1/2, d_2 = 1/2) \in \mathcal{D}^*(1)$ is 1/2. It implies that 1/2 DoF of common randomness achieves the maximal secure sum DoF 1. Without common randomness, the secure sum DoF cannot be more than $2/3$ for the case with $\alpha = 1$. Note that it is challenging to characterize $d_c^*(\alpha, d_1, d_2)$ for the general case of α. For the general case, the optimal secure GDoF region is non-symmetric in (d_1, d_2) as shown in Theorem 3. For a given GDoF pair in the asymmetric secure GDoF region, it might require several converse bounds on the minimal GDoF of the common randomness for achieving this GDoF pair, which will be studied in our future work.*

IV. Scheme Example

We will here provide a scheme example, focusing on the IC-SC channel with $\alpha = 4/3$ (see Section II-A). Note that for the case of $\alpha = 4/3$, without the consideration of secrecy constraints the sum GDoF is $4/3$ (cf. [26]). With the consideration of secrecy constraints, the secure sum GDoF is reduced to $8/9$ (cf. [12]). In this example, we will show that by adding common randomness the secure sum GDoF can be improved to $4/3$, which matches the sum GDoF for the case *without* secrecy constraints. In our scheme, Markov chain-based interference neutralization will be used in the signal design. In this scheme, the transmitted signals are given as (without time index):

$$x_k = v_{k,c} + \sum_{\ell=1}^{4} \delta_{k,\ell} \sqrt{P^{-\beta_{u_\ell}}} \cdot u$$

for $k \in \{1, 2\}$, where $\beta_{u_\ell} = \frac{1}{3}(\ell - 1)$, for $\ell \in \{1, 2, 3, 4\}$; and

$$\delta_{j,\ell} = \begin{cases} -\frac{h_{ii}}{h_{ij}} \cdot \left(\frac{h_{11}h_{22}}{h_{12}h_{21}}\right)^{\frac{\ell}{2}-1} & \ell \in \{2, 4\} \\ \left(\frac{h_{11}h_{22}}{h_{12}h_{21}}\right)^{\frac{\ell-1}{2}} & \ell \in \{1, 3\} \end{cases} \tag{9}$$

for $i, j \in \{1, 2\}, i \neq j$. u is the common randomness. $v_{1,c}$ and $v_{2,c}$ carry the messages of transmitters 1 and 2, respectively. The random variables $v_{1,c}$, $v_{2,c}$ and u are *independently* and *uniformly* drawn from a PAM set

$$v_{1,c}, v_{2,c}, u \in \Omega(\xi = \frac{\gamma}{Q}, \quad Q = P^{\frac{2/3-\epsilon}{2}})$$

where $\gamma \in \left(0, 1/64\right]$ is a constant, $\Omega(\xi, Q) \triangleq \{\xi a : \ a \in [-Q, Q] \cap \mathcal{Z}\}$, and $\epsilon > 0$ is a parameter that can be made arbitrarily small. With this signal design, $v_{k,c}$ carries $2/3$ GDoF, i.e., $\mathbb{H}(v_{k,c}) = \frac{2/3-\epsilon}{2} \log P + o(\log P)$, with $k \in \{1, 2\}$. One can check that the average power constraints $\mathbb{E}|x_1|^2 \leq 1$ and $\mathbb{E}|x_2|^2 \leq 1$ are satisfied. Then, the received signals are given as (without time index)

$$\begin{aligned} y_k =& \sqrt{P} h_{kk} v_{k,c} + \underbrace{\sqrt{P^{4/3}} h_{kj} v_{j,c} + \sqrt{P^{4/3}} \delta_{j,1} h_{kj} u}_{\text{aligned}} \\ &+ \sum_{\ell=1}^{3} \underbrace{(\sqrt{P^{(4-\ell)/3}} \delta_{k,\ell} h_{kk} + \sqrt{P^{(4-\ell)/3}} \delta_{j,\ell+1} h_{kj}) u}_{\text{interference neutralization}} \\ &+ \delta_{k,4} h_{kk} u + z_k \\ =& \sqrt{P} h_{kk} v_{k,c} + \sqrt{P^{4/3}} h_{kj} (v_{j,c} + u) + \delta_{k,4} h_{kk} u + z_k \end{aligned}$$

for $k \neq j$, $k, j \in \{1, 2\}$. The idea of the Markov chain-based interference neutralization method is given as follows. As shown in Fig. 6, the common randomness u is used to generate a certain number of signals with specific directions and powers, i.e., $\{\delta_{1,\ell}\sqrt{P^{-\beta_{u_\ell}}} u\}_{\ell=1}^4$ at transmitter 1 and $\{\delta_{2,\ell}\sqrt{P^{-\beta_{u_\ell}}} u\}_{\ell=1}^4$ at transmitter 2; the signal $\delta_{2,1}\sqrt{P^{-\beta_{u_1}}} u$ from transmitter 2 is used to jam the information signal $v_{2,c}$ at receiver 1 but it will create an interference at receiver 2; this interference will be neutralized by the signal $\delta_{1,2}\sqrt{P^{-\beta_{u_2}}} u$ from transmitter 1; the added signal $\delta_{1,2}\sqrt{P^{-\beta_{u_2}}} u$ also creates another interference at receiver 1 but will be neutralized by the next generated signal $\delta_{2,3}\sqrt{P^{-\beta_{u_3}}} u$; this process repeats until the residual interference is under the noise level. Since one signal is used to neutralize the previous signal and will be neutralized by the next signal, it forms a Markov chain for this interference neutralization process.

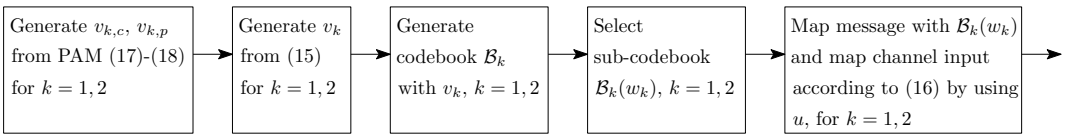

Fig. 7. A schematic diagram of the proposed scheme for the interference channel.

From our signal design, it can be proved that the secure rates $R_k = \mathbb{I}(v_{k,c}; y_k) - \mathbb{I}(v_{k,c}; y_j|v_{j,c}) \geq \frac{2/3-\epsilon}{2}\log P + o(\log P)$, $k \neq j$, $k, j \in \{1,2\}$, and the secure sum GDoF $d_{\text{sum}} = 4/3$, are achievable for almost all the channel coefficients $\{h_{k\ell}\} \in (1,2]^{2\times 2}$, by using $d_c = 2/3$ GDoF of common randomness. More details on the proposed scheme can be found in Section V.

V. Achievability for interference channel

The scheme proposed in this section, as well as the schemes proposed in the next sections, uses PAM modulation, rate splitting, signal alignment, distance-outage bounding technique, and Markov chain-based interference neutralization. In the rate analysis of the proposed schemes, some lemmas regarding error probabilities are provided in this section and the next sections. For each of those lemmas, the proof is based on one of the two methods: a) successive decoding, and b) noise removal and signal separation. Specifically, the proof of Lemma 1 is based on successive decoding, while the proofs of Lemmas 2, 4 and 5 are based on noise removal and signal separation. For the method of noise removal and signal separation, we will use the distance-outage bounding technique. In a nutshell, the distance-outage bounding technique is a tool that can be used to bound the minimum distance of the constellation points of a signal by controlling the outage set of the channel coefficients (cf. [45], [12]). Although the proposed schemes are designed for the symmetric settings, the key ideas could be generalized to asymmetric settings (see the discussion in Section IX-A).

In this section we will provide the achievability scheme for the *symmetric* Gaussian IC-SC channel defined in Section II-A. For the case with $0 \leq \alpha \leq 1/2$, there is no secrecy penalty in sum GDoF performance (cf. [12], [26]). Thus, here we will just focus on the case with $\alpha > 1/2$. The scheme details are given in the following subsections.

1) Codebook generation: Transmitter k, $k = 1, 2$, at first generates a codebook as

$$\mathcal{B}_k \triangleq \left\{ v_k^n(w_k, w_k') : w_k \in \{1, 2, \cdots, 2^{nR_k}\}, w_k' \in \{1, 2, \cdots, 2^{nR_k'}\} \right\} \tag{10}$$

where v_k^n denotes the corresponding codewords. The elements of the codewords are generated independently and identically based on a particular distribution. w_k' is an independent randomness that is used to protect the confidential message, and is uniformly distributed over $\{1, 2, \cdots, 2^{nR_k'}\}$. R_k and R_k' are the rates of w_k and w_k', respectively. To transmit the confidential message w_k, transmitter k *randomly* chooses a codeword v_k^n from a sub-codebook $\mathcal{B}_k(w_k)$ defined by

$$\mathcal{B}_k(w_k) \triangleq \left\{ v_k^n(w_k, w_k') : w_k' \in \{1, 2, \cdots, 2^{nR_k'}\} \right\},\ k = 1, 2 \tag{11}$$

according to a uniform distribution. Then, the selected codeword v_k^n is mapped to the channel input based on the following signal design

$$x_k(t) = \varepsilon v_k(t) + \varepsilon \sum_{\ell=1}^{\tau} \delta_{k,\ell} \sqrt{P^{-\beta_{u_\ell}}} \cdot u(t) \tag{12}$$

for $k = 1, 2$, where $v_k(t)$ denotes the tth element of v_k^n; $\{\delta_{j,\ell}\}_{j,\ell}$ are parameters that will be designed specifically later on for different cases of α, based on the Markov chain-based interference neutralization and alignment technique. ε is a parameter designed as

$$\varepsilon \triangleq \begin{cases} 1 & \text{if } \alpha \neq 1 \\ \frac{h_{11}h_{22} - h_{12}h_{21}}{8} & \text{if } \alpha = 1 \end{cases} \tag{13}$$

which is used to regularize the power of the transmitted signal. τ is a parameter designed as

$$\tau \triangleq \begin{cases} \lceil \frac{\alpha}{1-\alpha} \rceil & \text{if } \alpha < 1 \\ \lceil \frac{\alpha}{\alpha-1} \rceil & \text{if } \alpha > 1 \\ 1 & \text{if } \alpha = 1. \end{cases} \tag{14}$$

u is a random variable *independently* and *uniformly* drawn from a PAM constellation set, which will be specified later on. For the proposed scheme, the common randomness w_c is mapped into the random variables w_1', w_2' and $\{u(t)\}_t$, where w_1', w_2', $\{u(t)\}_t$ are mutually independent[1]. Based on our definition, w_1', w_2' and $\{u(t)\}_t$ are available at the transmitters but not at the receivers.

2) Signal design: For transmitter k, $k = 1, 2$, each element of the codeword is designed to have the following form

$$v_k = v_{k,c} + \sqrt{P^{-\beta_{k,p}}} v_{k,p}. \tag{15}$$

With this, the input signal in (12) can be expressed as

$$x_k = \varepsilon v_{k,c} + \varepsilon \sqrt{P^{-\beta_{k,p}}} \cdot v_{k,p} + \varepsilon \sum_{\ell=1}^{\tau} \delta_{k,\ell} \sqrt{P^{-\beta_{u_\ell}}} \cdot u,\ k = 1, 2 \tag{16}$$

(without time index for simplicity), where random variables $\{v_{k,c}, v_{k,p}, u\}$ are *independently* and *uniformly* drawn from the following PAM constellation sets

$$v_{k,c}, u \in \Omega(\xi = \frac{\gamma}{Q},\ Q = P^{\frac{\lambda_{k,c}}{2}}) \tag{17}$$

$$v_{k,p} \in \Omega(\xi = \frac{\gamma}{2Q},\ Q = P^{\frac{\lambda_{k,p}}{2}}) \tag{18}$$

where γ is a parameter satisfying the constraint $\gamma \in \left(0,\ \frac{1}{\tau \cdot 2^\tau}\right]$. In the proposed scheme, the designed parameters

[1]Note that w_k' is not needed to be part of the common randomness, i.e., it could be the private randomness available at transmitter k only, for $k = 1, 2$. However, as it will be shown later on, the rate of w_k' is relatively small, compared to the rate of the common randomness $\{u(t)\}_t$ used in this proposed scheme.

$\{\beta_{k,p}, \beta_{u_\ell}, \lambda_{k,c}, \lambda_{k,p}, \lambda_u\}_{k,\ell}$ are given in Table I for different regimes[2]. A schematic diagram of the proposed scheme for the interference channel is provided in Fig. 7. Based on the signal design in (17) and (18), we have

$$\mathbb{E}|v_{k,c}|^2 = \frac{2\times(\frac{\gamma}{Q})^2}{2Q+1}\sum_{i=1}^{Q} i^2 \le \frac{2\gamma^2}{3},\ \mathbb{E}|u|^2 \le \frac{2\gamma^2}{3},\ \mathbb{E}|v_{k,p}|^2 \le \frac{\gamma^2}{6}. \tag{19}$$

From (13), (16) and (19), we can verify that the signal x_k satisfies the power constraint, that is

$$\begin{aligned}\mathbb{E}|x_k|^2 &= \varepsilon^2\mathbb{E}|v_{k,c}|^2 + \varepsilon^2 P^{-\beta_{k,p}}\mathbb{E}|v_{k,p}|^2 + \varepsilon^2\big(\sum_{\ell=1}^{\tau}\delta_{k,\ell}P^{-\beta_{u_\ell}}\big)^2\mathbb{E}|u|^2 \\ &\le \frac{2\gamma^2\varepsilon^2}{3} + \frac{\gamma^2\varepsilon^2}{6} + \frac{2\gamma^2\varepsilon^2\tau^2 4^\tau}{3} \\ &\le 1\end{aligned}$$

for $k = 1, 2$, where $\gamma \in \big(0, \frac{1}{\tau\cdot 2^\tau}\big]$, $\varepsilon^2 \le 1$ and $\delta_{k,\ell}$ is designed specifically for different cases of α satisfying the inequality $\varepsilon^2\delta_{k,\ell}^2 \le 4^\tau, \forall k, \ell$, which will be shown later on.

3) Secure rate analysis: We define the rates R_k and R'_k as

$$R_k \triangleq \mathbb{I}(v_k; y_k) - \mathbb{I}(v_k; y_\ell|v_\ell) - \epsilon \tag{20}$$

$$R'_k \triangleq \mathbb{I}(v_k; y_\ell|v_\ell) - \epsilon \tag{21}$$

for some $\epsilon > 0$, and $\ell, k \in \{1, 2\}, \ell \neq k$. With our codebook and signal design, the result of [8, Theorem 2] (or [3, Theorem 2]) suggests that the rate pair (R_1, R_2) defined above is achievable and the transmission of the messages is secure, i.e., $\mathbb{I}(w_1; y_2^n) \le n\epsilon$ and $\mathbb{I}(w_2; y_1^n) \le n\epsilon$. Remind that, based on our codebook design, v_1 and v_2 are independent, since w_1, w_2, w'_1, w'_2 are mutually independent (cf. (10)).

In what follows we will show how to remove the secrecy penalty in terms of GDoF performance by adding common randomness, focusing on the regime of $\alpha > 1/2$. Specifically, we will consider the following five cases: $\frac{1}{2} < \alpha \le \frac{2}{3}$, $\frac{2}{3} \le \alpha < 1$, $\alpha = 1$, $1 < \alpha \le 2$, and $2 \le \alpha$. In the achievability scheme, a Markov chain-based interference neutralization method is proposed to accomplish the role of common randomness.

A. $1/2 < \alpha \le 2/3$

In this case with $1/2 < \alpha \le 2/3$, based on the parameters designed in Table I, by setting

$$\delta_{1,1} = \frac{h_{12}}{h_{11}}, \quad \delta_{2,1} = \frac{h_{21}}{h_{22}}, \quad \delta_{1,2} = \delta_{2,2} = -\frac{h_{12}h_{21}}{h_{11}h_{22}}, \tag{22}$$

[2]Without loss of generality we will take the assumption that $P^{\frac{\lambda_{k,c}}{2}}$ and $P^{\frac{\lambda_{k,p}}{2}}$ are integers, for $k = 1, 2$. For example, when $P^{\frac{\lambda_{2,c}}{2}}$ isn't an integer, the parameter ϵ in Table I can be slightly modified such that $P^{\frac{\lambda_{2,c}}{2}}$ is an integer, for the regime with large P. Similar assumption will also be used in the next channel models later.

TABLE I
PARAMETER DESIGN FOR THE IC-SC CHANNEL.

	$\frac{1}{2}<\alpha\le\frac{2}{3}$	$\frac{2}{3}\le\alpha<1$	$\alpha=1$	$1<\alpha\le 2$	$2\le\alpha$
$\beta_{u_\ell}, \ell\in\{1,2,\cdots,\tau\}$	$(1-\alpha)\ell$	$(1-\alpha)\ell$	0	$(\alpha-1)(\ell-1)$	$(\alpha-1)(\ell-1)$
$\beta_{1,p},\ \beta_{2,p}$	α	α	∞	∞	∞
$\lambda_{1,c},\ \lambda_{2,c}$	$2\alpha-1-\epsilon$	$\alpha/2-\epsilon$	$1/2-\epsilon$	$\alpha/2-\epsilon$	$1-\epsilon$
λ_u	$2\alpha-1-\epsilon$	$\alpha/2-\epsilon$	$1/2-\epsilon$	$\alpha/2-\epsilon$	$1-\epsilon$
$\lambda_{1,p},\ \lambda_{2,p}$	$1-\alpha-\epsilon$	$1-\alpha-\epsilon$	0	0	0

the transmitted signals take the following forms

$$x_1 = v_{1,c} + \sqrt{P^{-\alpha}}\cdot v_{1,p} + \big(\sqrt{P^{\alpha-1}}\cdot\frac{h_{12}}{h_{11}} - \sqrt{P^{2\alpha-2}}\cdot\frac{h_{12}h_{21}}{h_{11}h_{22}}\big)u \tag{23}$$

$$x_2 = v_{2,c} + \sqrt{P^{-\alpha}}\cdot v_{2,p} + \big(\sqrt{P^{\alpha-1}}\cdot\frac{h_{21}}{h_{22}} - \sqrt{P^{2\alpha-2}}\cdot\frac{h_{21}h_{12}}{h_{22}h_{11}}\big)u. \tag{24}$$

Note that in this case, $\tau = 2$ and $\varepsilon = 1$. The received signals then take the following forms

$$\begin{aligned}y_1 =& \sqrt{P}h_{11}v_{1,c} + \sqrt{P^{1-\alpha}}h_{11}v_{1,p} + \sqrt{P^{\alpha}}h_{12}\underbrace{(v_{2,c}+u)}_{\text{aligned}} \\ &+ \underbrace{h_{12}v_{2,p} - \sqrt{P^{3\alpha-2}}\cdot\frac{h_{12}^2h_{21}}{h_{11}h_{22}}u}_{\text{treated as noise}} + z_1\end{aligned} \tag{25}$$

$$\begin{aligned}y_2 =& \sqrt{P}h_{22}v_{2,c} + \sqrt{P^{1-\alpha}}h_{22}v_{2,p} + \sqrt{P^{\alpha}}h_{21}\underbrace{(v_{1,c}+u)}_{\text{aligned}} \\ &+ \underbrace{h_{21}v_{1,p} - \sqrt{P^{3\alpha-2}}\cdot\frac{h_{21}^2h_{12}}{h_{22}h_{11}}u}_{\text{treated as noise}} + z_2.\end{aligned} \tag{26}$$

In the above expressions of y_1 and y_2, the interference is removed by using the Markov chain-based interference neutralization method.

Based on our signal design, we will prove that the secure rates satisfy $R_k = \mathbb{I}(v_k; y_k) - \mathbb{I}(v_k; y_\ell|v_\ell) \ge \frac{\alpha-2\epsilon}{2}\log P + o(\log P)$, for $k, \ell \in \{1, 2\}$, $k \neq \ell$, and the secure sum GDoF $d_{\text{sum}} = 2\alpha$ is achievable. For the secure rates described in (20), letting $\epsilon \to 0$ gives

$$R_1 = \mathbb{I}(v_1; y_1) - \mathbb{I}(v_1; y_2|v_2) \tag{27}$$

$$R_2 = \mathbb{I}(v_2; y_2) - \mathbb{I}(v_2; y_1|v_1). \tag{28}$$

Due to the symmetry we will focus on bounding the secure rate R_1 (see (27)). We will use $\hat{v}_{1,c}$ and $\hat{v}_{1,p}$ to denote the estimates for $v_{1,c}$ and $v_{1,p}$ respectively from y_1, and use $\Pr[\{v_{1,c} \neq \hat{v}_{1,c}\}\cup\{v_{1,p} \neq \hat{v}_{1,p}\}]$ to represent the error probability of this estimation. Then the term $\mathbb{I}(v_1; y_1)$ can be lower bounded by

$$\mathbb{I}(v_1; y_1) \ge \mathbb{I}(v_1; \hat{v}_{1,c}, \hat{v}_{1,p}) \tag{29}$$

$$= \mathbb{H}(v_1) - \mathbb{H}(v_1|\hat{v}_{1,c}, \hat{v}_{1,p})$$

$$\ge \mathbb{H}(v_1) - \big(1 + \Pr[\{v_{1,c} \neq \hat{v}_{1,c}\}\cup\{v_{1,p} \neq \hat{v}_{1,p}\}]\cdot\mathbb{H}(v_1)\big) \tag{30}$$

$$= \big(1 - \Pr[\{v_{1,c} \neq \hat{v}_{1,c}\}\cup\{v_{1,p} \neq \hat{v}_{1,p}\}]\big)\cdot\mathbb{H}(v_1) - 1 \tag{31}$$

where (29) results from the Markov chain $v_1 \to y_1 \to \{\hat{v}_{1,c}, \hat{v}_{1,p}\}$; (30) uses Fano's inequality. The rates of $v_{1,c}$, $v_{1,p}$ and $v_1 = v_{1,c} + \sqrt{P^{-\alpha}} \cdot v_{1,p}$ are computed as

$$\mathbb{H}(v_{1,c}) = \log(2 \cdot P^{\frac{2\alpha-1-\epsilon}{2}} + 1) \tag{32}$$

$$\mathbb{H}(v_{1,p}) = \log(2 \cdot P^{\frac{1-\alpha-\epsilon}{2}} + 1) \tag{33}$$

$$\mathbb{H}(v_1) = \frac{\alpha - 2\epsilon}{2} \log P + o(\log P) \tag{34}$$

where $v_{1,p} \in \Omega(\xi = \frac{\gamma}{2Q},\ Q = P^{\frac{1-\alpha-\epsilon}{2}})$ and $v_{1,c} \in \Omega(\xi = \frac{\gamma}{Q},\ Q = P^{\frac{2\alpha-1-\epsilon}{2}})$. Based on our signal design, with v_k we can reconstruct $\{v_{k,c}, v_{k,p}\}$, and vice versa, for $k = 1, 2$. To derive the lower bound of $\mathbb{I}(v_1; y_1)$, we provide a result below.

Lemma 1. *With* (16)-(18) *and* (23)-(24) *and for* $1/2 < \alpha \leq 2/3$*, the error probability of decoding* $\{v_{k,c}, v_{k,p}\}$ *from* y_k *is vanishing when* P *goes large, that is,*

$$Pr[\{v_{k,c} \neq \hat{v}_{k,c}\} \cup \{v_{k,p} \neq \hat{v}_{k,p}\}] \to 0 \quad as \quad P \to \infty,\ k = 1, 2. \tag{35}$$

Proof. See Appendix A. The proof is based on successive decoding method. □

By incorporating the results of (34) and Lemma 1 into (31), the term $\mathbb{I}(v_1; y_1)$ in (27) can be lower bounded by

$$\mathbb{I}(v_1; y_1) \geq \frac{\alpha - 2\epsilon}{2} \log P + o(\log P). \tag{36}$$

For the term $\mathbb{I}(v_1; y_2|v_2)$ in (27), we can treat it as a rate penalty. This penalty can be bounded by

$$\begin{aligned}
&\mathbb{I}(v_1; y_2|v_2) \\
\leq &\mathbb{I}(v_1; y_2, v_{1,c} + u|v_2) && (37)\\
= &\mathbb{I}(v_1; v_{1,c}+u) + \mathbb{I}(v_1; h_{21}v_{1,p} - \sqrt{P^{3\alpha-2}} \cdot \frac{h_{21}^2 h_{12}}{h_{22} h_{11}} u + z_2 | v_2, v_{1,c}+u) && (38)\\
\leq &\mathbb{H}(v_{1,c}+u) - \mathbb{H}(u) + \mathrm{h}(h_{21}v_{1,p} - \sqrt{P^{3\alpha-2}} \cdot \frac{h_{21}^2 h_{12}}{h_{22} h_{11}} u + z_2) - \mathrm{h}(z_2) && (39)\\
\leq &\underbrace{\log(4P^{\frac{2\alpha-1-\epsilon}{2}}+1) - \log(2P^{\frac{2\alpha-1-\epsilon}{2}}+1)}_{\leq 1} + \frac{1}{2}\log(2\pi e \cdot 69) - \frac{1}{2}\log(2\pi e) && (40)\\
\leq &\log(2\sqrt{69}) && (41)
\end{aligned}$$

where (38) follows from the fact that v_1, v_2, u are mutually independent; (39) stems from the fact that $\{v_{k,p}, v_{k,c}\}$ can be reconstructed from v_k for $k = 1, 2$, and the identity that adding a condition will not increase the differential entropy; (40) results from the derivations that $\mathbb{H}(v_{1,c}+u) \leq \log(4P^{\frac{2\alpha-1-\epsilon}{2}}+1)$, and that $\mathrm{h}(h_{21}v_{1,p} - \sqrt{P^{3\alpha-2}} \cdot \frac{h_{21}^2 h_{12}}{h_{22} h_{11}} u + z_2) \leq \frac{1}{2}\log(2\pi e(|h_{21}|^2 \cdot \mathbb{E}|v_{1,p}|^2 + P^{3\alpha-2} \cdot |h_{21}|^4 |h_{12}|^2 \cdot \mathbb{E}|u|^2 + 1)) \leq \frac{1}{2}\log(2\pi e \cdot 69)$. With (36) and (41), we have

$$R_1 = \mathbb{I}(v_1; y_1) - \mathbb{I}(v_1; y_2|v_2) \geq \frac{\alpha - 2\epsilon}{2} \log P + o(\log P)$$

and also $R_2 \geq \frac{\alpha-2\epsilon}{2} \log P + o(\log P)$ resulting from symmetry. It suggests that the proposed scheme achieves $d_{\text{sum}} = 2\alpha$ by using $d_c = 2\alpha - 1$ GDoF of common randomness. Note that in our scheme the common randomness is mapped into some random variables, i.e., w_1', w_2' and $\{u(t)\}_t$. In this case, the rate of w_1' is $R_1' = \mathbb{I}(v_1; y_2|v_2) - \epsilon \leq o(\log P) - \epsilon$ (see (21) and (41)); the rate of w_2' is $R_2' = \mathbb{I}(v_2; y_1|v_1) - \epsilon \leq o(\log P) - \epsilon$; and the rate of u is $\mathbb{H}(u) = \log(2 \cdot P^{\frac{\lambda_u}{2}} + 1) = \frac{\lambda_u}{2} \log P + o(\log P)$, which gives $d_c = \lambda_u = 2\alpha - 1$ when $\epsilon \to 0$. In this case, the GDoF of w_1' and w_2' are both 0, while the GDoF of u is $d_c = 2\alpha - 1$. Therefore, the effects of w_1' and w_2' in terms of GDoF counted for the common randomness can be ignored.

B. $2/3 \leq \alpha < 1$

In this case with $2/3 \leq \alpha < 1$, based on the parameters designed in Table I, the transmitted signals take the following forms

$$x_1 = v_{1,c} + \sqrt{P^{-\alpha}} \cdot v_{1,p} + \sum_{\ell=1}^{\tau} \delta_{1,\ell} \sqrt{P^{-\beta_{u_\ell}}} \cdot u \tag{42}$$

$$x_2 = v_{2,c} + \sqrt{P^{-\alpha}} \cdot v_{2,p} + \sum_{\ell=1}^{\tau} \delta_{2,\ell} \sqrt{P^{-\beta_{u_\ell}}} \cdot u \tag{43}$$

where the parameters $\{\delta_{j,\ell}\}_{j,\ell}$ are designed by

$$\delta_{j,\ell} = \begin{cases} -\left(\frac{h_{12}h_{21}}{h_{11}h_{22}}\right)^{\frac{\ell}{2}} & \ell \in \{2k : 2k \leq \tau, k \in \mathcal{Z}^+\} \\ \frac{h_{ji}}{h_{jj}} \cdot \left(\frac{h_{12}h_{21}}{h_{11}h_{22}}\right)^{\frac{\ell-1}{2}} & \ell \in \{2k\text{–}1 : 2k-1 \leq \tau, k \in \mathcal{Z}^+\} \end{cases} \tag{44}$$

for $i, j \in \{1, 2\}, i \neq j$. Note that the common randomness u is used to generate a certain number of signals with specific directions and powers, i.e., $\{\delta_{1,\ell}\sqrt{P^{-\beta_{u_\ell}}}u\}_{\ell=1}^{\tau}$ at transmitter 1 and $\{\delta_{2,\ell}\sqrt{P^{-\beta_{u_\ell}}}u\}_{\ell=1}^{\tau}$ at transmitter 2. Then, the received signals are expressed as

$$\begin{aligned}
y_1 = &\sqrt{P}h_{11}v_{1,c} + \sqrt{P^{1-\alpha}}h_{11}v_{1,p} + \sqrt{P^{\alpha}}h_{12}(v_{2,c} + u) \\
&+ \sqrt{P^{(\tau+1)\alpha-\tau}}\delta_{2,\tau}h_{12}u + h_{12}v_{2,p} + z_1 && (45)\\
y_2 = &\sqrt{P}h_{22}v_{2,c} + \sqrt{P^{1-\alpha}}h_{22}v_{2,p} + \sqrt{P^{\alpha}}h_{21}(v_{1,c} + u) \\
&+ \sqrt{P^{(\tau+1)\alpha-\tau}}\delta_{1,\tau}h_{21}u + h_{21}v_{1,p} + z_2. && (46)
\end{aligned}$$

As can be seen from (45) and (46), the interference is removed by using the Markov chain-based interference neutralization method. We will focus on bounding the secure rate R_1. By following the derivations in (29)-(31), the term $\mathbb{I}(v_1; y_1)$ can be lower bounded by

$$\mathbb{I}(v_1; y_1) \geq \left(1 - \Pr[\{v_{1,c} \neq \hat{v}_{1,c}\} \cup \{v_{1,p} \neq \hat{v}_{1,p}\}]\right) \cdot \mathbb{H}(v_1) - 1 \tag{47}$$

where the rate of v_1 in (47) is

$$\mathbb{H}(v_1) = \mathbb{H}(v_{1,c}) + \mathbb{H}(v_{1,p}) = \frac{1 - \alpha/2 - 2\epsilon}{2} \log P + o(\log P) \tag{48}$$

and the error probability in (47) is vanishing (see the following lemma).

Lemma 2. *Consider the signal design in* (16)-(18) *and* (42)-(44) *for the case with* $2/3 \leq \alpha < 1$*. For almost all the channel*

realizations, the error probability of decoding $\{v_{k,c}, v_{k,p}\}$ *from* y_k *is vanishing when* P *goes large, that is*

$$Pr[\{v_{k,c} \neq \hat{v}_{k,c}\} \cup \{v_{k,p} \neq \hat{v}_{k,p}\}] \to 0 \quad as \quad P \to \infty, \ k = 1, 2. \tag{49}$$

Proof. See Appendix B. The proof is based on noise removal and signal separation. The distance-outage bounding technique is also used in the proof. □

From (47), (48) and Lemma 2, the term $\mathbb{I}(v_1; y_1)$ can be lower bounded by

$$\mathbb{I}(v_1; y_1) \geq \frac{1 - \alpha/2 - 2\epsilon}{2} \log P + o(\log P) \tag{50}$$

for almost all the channel coefficients $\{h_{k\ell}\} \in (1, 2]^{2\times 2}$. From the derivations in (37)-(41), the term $\mathbb{I}(v_1; y_2|v_2)$ in (27) is bounded by

$$\mathbb{I}(v_1; y_2|v_2) \leq o(\log P). \tag{51}$$

With (50) and (51), we conclude that

$$R_1 = \mathbb{I}(v_1; y_1) - \mathbb{I}(v_1; y_2|v_2) \geq \frac{1-\alpha/2-2\epsilon}{2} \log P + o(\log P) \tag{52}$$

and also $R_2 \geq \frac{1-\alpha/2-2\epsilon}{2} \log P + o(\log P)$, for almost all the channel realizations. It imply that the proposed scheme achieves $d_{\text{sum}} = 2(1 - \alpha/2)$ for almost all the channel realizations, by using $d_c = \alpha/2$ GDoF of common randomness.

C. $\alpha = 1$

In this case with $\alpha = 1$, based on the parameters designed in Table I, and by setting

$$\delta_{1,1} = \frac{h_{22}h_{12} - h_{12}h_{21}}{h_{11}h_{22} - h_{12}h_{21}}, \quad \delta_{2,1} = \frac{h_{11}h_{21} - h_{21}h_{12}}{h_{22}h_{11} - h_{21}h_{12}}, \tag{53}$$

the transmitted signals take the following forms

$$x_1 = \varepsilon v_{1,c} + \varepsilon \frac{h_{22}h_{12} - h_{12}h_{21}}{h_{11}h_{22} - h_{12}h_{21}} \cdot u \tag{54}$$

$$x_2 = \varepsilon v_{2,c} + \varepsilon \frac{h_{11}h_{21} - h_{21}h_{12}}{h_{22}h_{11} - h_{21}h_{12}} \cdot u. \tag{55}$$

Note that in this case, $\tau = 1$ and $\varepsilon = \frac{h_{11}h_{22}-h_{12}h_{21}}{8}$. Then, the received signals are simplified as

$$y_1 = \varepsilon\sqrt{P}h_{11}v_{1,c} + \varepsilon\sqrt{P}h_{12}(v_{2,c} + u) + z_1 \tag{56}$$

$$y_2 = \varepsilon\sqrt{P}h_{22}v_{2,c} + \varepsilon\sqrt{P}h_{21}(v_{1,c} + u) + z_2. \tag{57}$$

From the previous steps in (29)-(34) and Lemma 2, one can prove that $\mathbb{I}(v_1; y_1) \geq \frac{1/2-\epsilon}{2} \log P + o(\log P)$ which holds for almost all realizations of the channel coefficients. From (37)-(41), one can also prove that $\mathbb{I}(v_1; y_2|v_2) \leq o(\log P)$. As a result, the secure rates can be bounded as

$$R_1 = \mathbb{I}(v_1; y_1) - \mathbb{I}(v_1; y_2|v_2) \geq \frac{1/2 - \epsilon}{2} \log P + o(\log P) \tag{58}$$

and $R_2 \geq \frac{1/2-\epsilon}{2} \log P + o(\log P)$ due to the symmetry, for almost all channel realizations. The proposed scheme then achieves $d_{\text{sum}} = 1$ for almost all channel realizations by using $d_c = 1/2$ GDoF of common randomness.

D. $1 < \alpha \leq 2$

In this case with $1 < \alpha \leq 2$, the transmitted signals take the following forms

$$x_j = v_{j,c} + \sum_{\ell=1}^{\tau} \delta_{j,\ell} \sqrt{P^{-\beta_{u_\ell}}} \cdot u$$

for $j = 1, 2$, where in this case the parameters $\{\delta_{j,\ell}\}_{j,\ell}$ are designed by

$$\delta_{j,\ell} = \begin{cases} -\frac{h_{ii}}{h_{ij}} \cdot \left(\frac{h_{11}h_{22}}{h_{12}h_{21}}\right)^{\frac{\ell}{2}-1} & \ell \in \{2k : 2k \leq \tau, k \in \mathcal{Z}^+\} \\ \left(\frac{h_{11}h_{22}}{h_{12}h_{21}}\right)^{\frac{\ell-1}{2}} & \ell \in \{2k\text{–}1 : 2k-1 \leq \tau, k \in \mathcal{Z}^+\} \end{cases} \tag{59}$$

for $i, j \in \{1, 2\}, i \neq j$. Then, the received signals become

$$y_1 = \sqrt{P}h_{11}v_{1,c} + \sqrt{P^{\alpha}}h_{12}(v_{2,c} + u) + \sqrt{P^{\tau-(\tau-1)\alpha}}\delta_{1,\tau}h_{11}u + z_1 \tag{60}$$

$$y_2 = \sqrt{P}h_{22}v_{2,c} + \sqrt{P^{\alpha}}h_{21}(v_{1,c} + u) + \sqrt{P^{\tau-(\tau-1)\alpha}}\delta_{2,\tau}h_{22}u + z_2. \tag{61}$$

By following the proof steps in (29)-(34) and Lemma 2, in this case one can prove that $\mathbb{I}(v_1; y_1) \geq \frac{\alpha/2-\epsilon}{2} \log P + o(\log P)$ for almost all the realizations of the channel coefficients. Also, it is easy to prove that $\mathbb{I}(v_1; y_2|v_2) \leq o(\log P)$. Therefore, the proposed scheme achieves $d_{\text{sum}} = \alpha$ for almost all channel realizations by using $d_c = \alpha/2$ GDoF of common randomness.

E. $\alpha \geq 2$

When $\alpha \geq 2$, the transmitted signals take the following forms

$$x_1 = v_{1,c} + \left(1 - \sqrt{P^{1-\alpha}} \cdot \frac{h_{22}}{h_{21}}\right)u, \quad x_2 = v_{2,c} + \left(1 - \sqrt{P^{1-\alpha}} \cdot \frac{h_{11}}{h_{12}}\right)u \tag{62}$$

and the received signals can be simplified as

$$y_1 = \sqrt{P}h_{11}v_{1,c} + \sqrt{P^{\alpha}}h_{12}(v_{2,c} + u) - \sqrt{P^{2-\alpha}} \cdot \frac{h_{22}h_{11}}{h_{21}}u + z_1 \tag{63}$$

$$y_2 = \sqrt{P}h_{22}v_{2,c} + \sqrt{P^{\alpha}}h_{21}(v_{1,c} + u) - \sqrt{P^{2-\alpha}} \cdot \frac{h_{11}h_{22}}{h_{12}}u + z_2. \tag{64}$$

For this case, by following the proof steps in (29)-(34) and Lemma 1, we have $\mathbb{I}(v_1; y_1) \geq \frac{1-\epsilon}{2} \log P + o(\log P)$. One can also prove that $\mathbb{I}(v_1; y_2|v_2) \leq o(\log P)$ for this case. It implies that the proposed scheme achieves $d_{\text{sum}} = 2$ by using $d_c = 1$ GDoF of common randomness.

VI. Achievability for wiretap channel with a helper

In this section, we will provide the achievability scheme for the WTH setting defined in Section II-B. Similarly to the scheme for the previous IC-SC setting, the proposed scheme for this WTH setting also uses PAM modulation, rate splitting, signal alignment, distance-outage bounding technique, and Markov chain-based interference neutralization. For the case

with $0 \leq \alpha \leq 1/2$, there is no secrecy penalty in GDoF performance (cf. [19]). Therefore, here we will just focus on the case with $\alpha > 1/2$ and prove that $d(\alpha) = 1$ is achievable. The scheme details are given as follows.

1) Codebook generation: The codebook generation is similar to the previous case for the interference channel with confidential messages, with one difference being that only transmitter 1 is required to generate the codebook in this channel. Note that in this channel transmitter 2 will act as a helper without sending message. For transmitter 1, it generates a codebook as in (10). To transmit the confidential message w_1, transmitter 1 chooses a codeword v^n *randomly* from a sub-codebook as in (11). Then the selected codeword is mapped to the channel input under the following signal design

$$x_1(t) = \varepsilon v(t) + \varepsilon \sum_{\ell=0}^{\tau} \delta_{1,\ell} \sqrt{P^{-\beta_{u_\ell}}} \cdot u(t) \tag{65}$$

where $\{\delta_{k,\ell}\}_{k,\ell}$ are the parameters, which will be specified later by using the Markov chain-based interference neutralization and alignment technique. ε is a parameter designed as

$$\varepsilon \triangleq \begin{cases} 1 & \text{if } \alpha \neq 1 \\ \frac{h_{11}h_{22}-h_{12}h_{21}}{8} & \text{if } \alpha = 1. \end{cases} \tag{66}$$

τ is another parameter designed as

$$\tau \triangleq \begin{cases} 1 & \text{if } \alpha = 1 \\ \lceil \frac{1}{2(1-\alpha)} \rceil & \text{if } \alpha < 1 \\ \lceil \frac{1}{2(\alpha-1)} \rceil & \text{if } \alpha > 1. \end{cases} \tag{67}$$

u is a random variable *independently* and *uniformly* drawn from a PAM constellation set which will be specified later on. In this channel, the common randomness w_c is mapped into two random variables, i.e., w_1' and u, and w_1' and u are mutually independent. Based on our definition, w_1' and u are available at the transmitters but not at the receivers.

2) Signal design: In the scheme, each element of the codeword v^n is designed as

$$v(t) = v_c(t) + \sqrt{P^{-\beta_p}} \cdot v_p(t). \tag{68}$$

With this, the channel input in (65) is expressed as

$$x_1 = \varepsilon v_c + \varepsilon \sqrt{P^{-\beta_p}} \cdot v_p + \varepsilon \sum_{\ell=0}^{\tau} \delta_{1,\ell} \sqrt{P^{-\beta_{u_\ell}}} \cdot u \tag{69}$$

(removing the time index). In this setting, the helper (transmitter 2) sends a jamming signal designed as

$$x_2 = \varepsilon \sum_{\ell=1}^{\tau} \delta_{2,\ell} \sqrt{P^{-\beta'_{u_\ell}}} \cdot u \tag{70}$$

where the random variables u, v_c and v_p are *independently* and *uniformly* drawn from the corresponding PAM constellation sets

$$v_c, u \in \Omega(\xi = \frac{\gamma}{Q},\ Q = P^{\frac{\lambda_c}{2}}) \tag{71}$$

$$v_p \in \Omega(\xi = \frac{\gamma}{2Q},\ Q = P^{\frac{\lambda_p}{2}}) \tag{72}$$

and γ is a parameter satisfying the constraint $\gamma \in \big(0,\ \frac{1}{(\tau+2)\cdot 4^\tau}\big]$. Table II provides the designed parameters $\{\beta_p, \beta_{u_\ell}, \beta'_{u_\ell}, \lambda_c, \lambda_p, \lambda_u\}$ under different regimes. In this setting by following the step in (19) one can check that the power constraints $\mathbb{E}|x_1|^2 \leq 1$ and $\mathbb{E}|x_2|^2 \leq 1$ are satisfied.

TABLE II
PARAMETER DESIGN FOR THE WTH CHANNEL.

	$1/2 < \alpha < 1$	$\alpha = 1$	$\alpha > 1$
β_{u_0}	∞	∞	0
$\beta_{u_\ell},\ \ell \in \{1, 2, \cdots, \tau-1\}$	$2\ell(1-\alpha)$	0	$2\ell(\alpha-1)$
β_{u_τ}	∞	0	$2\tau(\alpha-1)$
$\beta'_{u_\ell},\ \ell \in \{1, 2, \cdots, \tau\}$	$(2\ell-1)(1-\alpha)$	0	$(2\ell-1)(\alpha-1)$
β_p	α	∞	∞
λ_c	$\alpha-\epsilon$	$1-\epsilon$	$1-\epsilon$
λ_p	$1-\alpha-\epsilon$	0	0
λ_u	$\alpha-\epsilon$	$1-\epsilon$	$1-\epsilon$

3) Secure rate analysis: We define the rates R_1 and R_1' as

$$R_1 \triangleq \mathbb{I}(v; y_1) - \mathbb{I}(v; y_2) - \epsilon \tag{73}$$

$$R_1' \triangleq \mathbb{I}(v; y_2) - \epsilon. \tag{74}$$

With our codebook and signal design, the result of [8, Theorem 2] (or [3, Theorem 2]) suggests that the rate R_1 defined in (73) is achievable and the transmission of the message w_1 is secure. For this WTH channel, it can be treated as a particular case of the IC-SC channel if we remove the second transmitter's message (or set it empty). Thus, the result of [8, Theorem 2] (or [3, Theorem 2]) derived for the IC-SC channel reveals that the secure rate R_1 defined in (73) is achievable in this WTH channel.

In what follows we will provide the rate analysis, focusing on the regime of $\alpha > 1/2$. Specifically, we will consider the following three cases: $\frac{1}{2} < \alpha < 1$, $\alpha = 1$ and $\alpha > 1$. The achievability scheme also uses the Markov chain-based interference neutralization.

A. $1/2 < \alpha < 1$

When $1/2 < \alpha < 1$, the parameters $\{\delta_{k,\ell}\}_{k,\ell}$ are designed by

$$\delta_{1,\ell} = -\big(\frac{h_{12}h_{21}}{h_{11}h_{22}}\big)^\ell \qquad \ell \in \{1, 2, \cdots, \tau-1\}$$

$$\delta_{2,\ell} = \frac{h_{21}}{h_{22}} \cdot \big(\frac{h_{12}h_{21}}{h_{11}h_{22}}\big)^{\ell-1} \qquad \ell \in \{1, 2, \cdots, \tau\}.$$

In this case, the transmitted signals take the following forms

$$x_1 = v_c + \sqrt{P^{-\alpha}} \cdot v_p + \sum_{\ell=1}^{\tau-1} \delta_{1,\ell} \sqrt{P^{-\beta_{u_\ell}}} \cdot u,\ \ x_2 = \sum_{\ell=1}^{\tau} \delta_{2,\ell} \sqrt{P^{-\beta'_{u_\ell}}} \cdot u.$$

Then, the received signals are expressed as

$$y_1 = \sqrt{P} h_{11} v_c + \sqrt{P^{1-\alpha}} h_{11} v_p + \sqrt{P^{2\tau\alpha+1-2\tau}} \delta_{2,\tau} h_{12} u + z_1$$

$$y_2 = \sqrt{P^{\alpha}} h_{21} (v_c + u) + h_{21} v_p + z_2.$$

For this case, by following the proof steps in (29)-(34) and Lemma 1, one can prove that $\mathbb{I}(v; y_1) \geq \frac{1-2\epsilon}{2} \log P + o(\log P)$.

From (37)-(41), one can prove that $\mathbb{I}(v;y_2) \leq o(\log P)$ for this case. By inserting the above results into (73), the achievable rate can be bounded by $R_1 \geq \frac{1-2\epsilon}{2}\log P + o(\log P)$, which reveals that the proposed scheme achieves $d(\alpha)=1$ by using $d_c = \alpha$ GDoF of common randomness (note that $d_c = \lambda_u = \alpha - \epsilon$).

B. $\alpha = 1$

In this case by setting $\delta_{1,1} = -\frac{h_{12}h_{21}}{h_{11}h_{22}-h_{12}h_{21}}$ and $\delta_{2,1} = \frac{h_{11}h_{21}}{h_{11}h_{22}-h_{12}h_{21}}$, the transmitted signals take the following forms

$$x_1 = \varepsilon v_c - \varepsilon\frac{h_{12}h_{21}}{h_{11}h_{22}-h_{12}h_{21}}u, \quad x_2 = \varepsilon\frac{h_{11}h_{21}}{h_{11}h_{22}-h_{12}h_{21}}u.$$

Note that in this case, $\tau = 1$ and $\varepsilon = \frac{h_{11}h_{22}-h_{12}h_{21}}{8}$. Then, the received signals are expressed as

$$y_1 = \varepsilon\sqrt{P}h_{11}v_c + z_1, \qquad y_2 = \varepsilon\sqrt{P}h_{21}(v_c+u) + z_2.$$

From the previous steps in (29)-(34) and Lemma 1, one can prove that $\mathbb{I}(v;y_1) \geq \frac{1-\epsilon}{2}\log P + o(\log P)$ for this case. One can also prove that $\mathbb{I}(v;y_2) \leq o(\log P)$. As a result, the achievable secure rate can be bounded as $R_1 \geq \frac{1-\epsilon}{2}\log P + o(\log P)$. This bound suggests that, when $\alpha = 1$, the proposed scheme achieves $d(\alpha) = 1$ by using $d_c = 1$ GDoF of common randomness.

C. $\alpha > 1$

In this case the parameters $\{\delta_{k,\ell}\}_{k,\ell}$ are designed by

$$\delta_{1,\ell} = \big(\frac{h_{11}h_{22}}{h_{12}h_{21}}\big)^{\ell} \qquad \ell \in \{0,1,\cdots,\tau\}$$
$$\delta_{2,\ell} = -\frac{h_{11}}{h_{12}}\cdot\big(\frac{h_{11}h_{22}}{h_{12}h_{21}}\big)^{\ell-1} \qquad \ell \in \{1,2,\cdots,\tau\}.$$

The transmitted signals in this case have the following expressions

$$x_1 = v_c + \sum_{\ell=0}^{\tau}\delta_{1,\ell}\sqrt{P^{-\beta_{u_\ell}}}\cdot u, \quad x_2 = \sum_{\ell=1}^{\tau}\delta_{2,\ell}\sqrt{P^{-\beta'_{u_\ell}}}\cdot u.$$

Then, the received signals are expressed as

$$y_1 = \sqrt{P}h_{11}v_c + \sqrt{P^{-2\tau\alpha+2\tau+1}}\delta_{1,\tau}h_{11}u + z_1$$
$$y_2 = \sqrt{P^{\alpha}}h_{21}(v_c+u) + z_2.$$

By following the proof steps in (29)-(34), (37)-(41), and Lemma 1, one can bound the rate R_1 expressed in (73) as

$$R_1 = \mathbb{I}(v;y_1) - \mathbb{I}(v;y_2) \geq \frac{1-\epsilon}{2}\log P + o(\log P).$$

This suggests that in this case the proposed scheme achieves $d(\alpha) = 1$ by using $d_c = 1$ GDoF of common randomness.

VII. Achievability for multiple access wiretap channel

In this section, we will provide the achievability proof of Theorem 3 for MAC-WT channel defined in Section II-C. The following lemma will be used in the proof.

Lemma 3. *Given the symmetric Gaussian MAC-WT channel defined in Section II-C, for any tuple (d_1', d_2', d_c') such that $(d_1', d_2', d_c') \in \bar{\mathcal{D}}(\alpha)$, then*

$$(\frac{1}{\alpha}d_2', \frac{1}{\alpha}d_1', \frac{1}{\alpha}d_c') \in \bar{\mathcal{D}}(\frac{1}{\alpha}). \tag{75}$$

Proof. See Appendix C. □

In what follows, we will first focus on the case of $0 \leq \alpha \leq 1$ and prove that the optimal secure GDoF region $\mathcal{D}^*(\alpha) = \{(d_1,d_2)|d_1+d_2 \leq \max\{1,\alpha\}, 0 \leq d_1 \leq 1, 0 \leq d_2 \leq \alpha\}$ is achievable for the $0 \leq \alpha \leq 1$ case[3]. In Section VII-C, we will prove that $\mathcal{D}^*(\alpha)$ is achievable for $\alpha > 1$ by using the result of Lemma 3. The proposed scheme for this MAC-WT setting also uses PAM modulation, rate splitting, signal alignment, distance-outage bounding technique, and Markov chain-based interference neutralization. The details of the proposed scheme are given as follows.

1) Codebook: The codebook generation is the same as that of the interference channel in Section V (see (10) and (11)). In this setting, the channel input takes the following form

$$\begin{aligned} x_k(t) =& \varepsilon v_k(t) + \varepsilon\sum_{\ell=1}^{\tau/2}\delta_{k,\ell}\sqrt{P^{-\beta_{1,k,\ell}}}\cdot u_1(t) \\ &+ \varepsilon\sum_{\ell=1}^{\tau/2}\delta_{k,\ell}\sqrt{P^{-\beta_{2,k,\ell}}}\cdot u_2(t) \end{aligned} \tag{76}$$

for $k = 1,2$, where $v_k(t)$ denotes the tth element of codeword; $\{\delta_{k,\ell}\}_{k,\ell}$ and τ are parameters that will be designed specifically later on for different cases of α; ε is a parameter designed as

$$\varepsilon \triangleq \begin{cases} 1 & \text{if } \alpha \neq 1 \\ \frac{h_{11}h_{22}-h_{12}h_{21}}{8} & \text{if } \alpha = 1. \end{cases} \tag{77}$$

2) PAM constellation and signal alignment: In this setting, all the elements of the codewords are designed to take the following forms (without time index) for transmitter 1 and transmitter 2, respectively,

$$v_1 = v_{1,c} + \sqrt{P^{-\beta_{1,p}}}v_{1,p}, \; v_2 = \sqrt{P^{-\beta_{2,c}}}\frac{h_{21}}{h_{22}}v_{2,c} + \sqrt{P^{-\beta_{2,m}}}\frac{h_{21}}{h_{22}}v_{2,m}.$$

Then, we can rewrite the channel input in (76) as

$$\begin{aligned} x_1 =& \varepsilon v_{1,c} + \varepsilon\sqrt{P^{-\beta_{1,p}}}v_{1,p} + \varepsilon\sum_{\ell=1}^{\tau/2}\delta_{1,\ell}\sqrt{P^{-\beta_{1,1,\ell}}}\cdot u_1 \\ &+ \varepsilon\sum_{\ell=1}^{\tau/2}\delta_{1,\ell}\sqrt{P^{-\beta_{2,1,\ell}}}\cdot u_2 \end{aligned} \tag{78}$$

$$\begin{aligned} x_2 =& \varepsilon\sqrt{P^{-\beta_{2,c}}}\frac{h_{21}}{h_{22}}v_{2,c} + \varepsilon\sqrt{P^{-\beta_{2,m}}}\frac{h_{21}}{h_{22}}v_{2,m} \\ &+ \varepsilon\sum_{\ell=1}^{\tau/2}\delta_{2,\ell}\sqrt{P^{-\beta_{1,2,\ell}}}\cdot u_1 + \varepsilon\sum_{\ell=1}^{\tau/2}\delta_{2,\ell}\sqrt{P^{-\beta_{2,2,\ell}}}\cdot u_2 \end{aligned} \tag{79}$$

[3]When $\alpha = 0$, $\mathcal{D}(0) = \{(d_1,d_2)|0 \leq d_1 \leq 1, d_2 = 0\}$ is achievable by using a single-user transmission scheme. Therefore, without loss of generality, we will focus on the case with $\alpha > 0$.

TABLE III
DESIGNED PARAMETERS FOR MAC-WT CHANNEL WHEN $\alpha \leq 1$. THE LAST TWO ROWS CORRESPOND TO THE DESIGN OF THE PARAMETERS $\beta_{1,k,\ell}$ AND $\beta_{2,k,\ell}$, FOR $k \in \{1,2\}$ AND $\ell \in \{1,2,\cdots,\frac{\tau}{2}\}$.

	$0 \leq \alpha \leq \frac{2}{3}$		$\frac{2}{3} \leq \alpha < 1$		$\alpha = 1$
	$0 \leq B \leq (2\alpha-1)^+$	$(2\alpha-1)^+ < B \leq \alpha$	$0 \leq B \leq 2\alpha-1$	$2\alpha-1 < B \leq \alpha$	$(d_1', d_2') \in \mathcal{D}^*(1)$
$\beta_{2,c}$	$1-\alpha$	$1-\alpha$	$1-\alpha$	$1-\alpha$	0
$\beta_{2,m}$	∞	$\alpha - B$	∞	$\alpha - B$	∞
$\beta_{1,p}$	α	α	α	∞	∞
$\lambda_{2,c}$	$B-\epsilon$	$(2\alpha-1)^+ - \epsilon$	$B-\epsilon$	$2\alpha-1-\epsilon$	$d_2' - \epsilon$
$\lambda_{2,m}$	0	$B-(2\alpha-1)^+ - \epsilon$	0	$B-2\alpha+1-\epsilon$	0
$\lambda_{1,p}$	$1-\alpha-B-\epsilon$	$(\max\{B, 1-\alpha\}-B-\epsilon)^+$	$\min\{1-\alpha, 2\alpha-1-B\}-\epsilon$	0	0
$\lambda_{1,c}$	$\alpha - \epsilon$	$(1-B-\lambda_{1,p})^+ - 2\epsilon$	$(1-B-\lambda_{1,p})^+ - 2\epsilon$	$1-B-\epsilon$	$d_1' - \epsilon$
$\beta_{2,k,\ell}$	∞	$\beta_{1,k,\ell}-(1+B-2\alpha)$	∞	$\beta_{1,k,\ell}-(1+B-2\alpha)$	∞
$\beta_{1,k,\ell}$	$(2\ell-k+1)(1-\alpha)$				0

where the random variables $\{v_{k,c}, v_{1,p}, v_{2,m}, u_k\}_{k=1,2}$ are *independent* and *uniformly* drawn from the PAM constellation sets

$$v_{1,c} \in \Omega(\xi = \frac{\eta_{1,c}\gamma}{Q},\ Q = P^{\frac{\lambda_{1,c}}{2}}) \tag{80}$$

$$v_{1,p} \in \Omega(\xi = \frac{\gamma}{2Q},\ Q = P^{\frac{\lambda_{1,p}}{2}}) \tag{81}$$

$$v_{2,c} \in \Omega(\xi = \frac{\eta_{2,c}\gamma}{Q},\ Q = P^{\frac{\lambda_{2,c}}{2}}) \tag{82}$$

$$u_1 \in \Omega(\xi = \frac{\gamma}{Q},\ Q = P^{\frac{\max\{\lambda_{1,c},\lambda_{2,c}\}}{2}}) \tag{83}$$

$$v_{2,m}, u_2 \in \Omega(\xi = \frac{\gamma}{2Q},\ Q = P^{\frac{\lambda_{2,m}}{2}}) \tag{84}$$

respectively, where $\gamma \in \big(0, \frac{1}{\tau \cdot 2^\tau}\big]$. The parameters $\{\lambda_{k,c}, \lambda_{1,p}, \lambda_{2,m}, \beta_{2,c}, \beta_{1,p}, \beta_{2,m}, \beta_{1,k,\ell}, \beta_{2,k,\ell}\}_{k,\ell}$ are designed as in Table III. Note that B is a parameter within a specific range, which will be specified later on for different cases of α. The parameters $\eta_{1,c}$ and $\eta_{2,c}$ are designed to ensure that $v_{1,c}$ and $v_{2,c}$ have a certain integer relationship on the minimum distances of their PAM constellation sets[4]. Specifically, $\eta_{1,c}$ and $\eta_{2,c}$ are designed as

$$\eta_{i_m,c} = 1, \quad \eta_{i_n,c} = \left\lceil \sqrt{P^{\lambda_{i_m,c}-\lambda_{i_n,c}}} \right\rceil \Big/ \sqrt{P^{\lambda_{i_m,c}-\lambda_{i_n,c}}} \tag{85}$$

$$\text{where} \quad i_m = \arg\max_{i \in \{1,2\}} \lambda_{i,c}, \qquad i_n \neq i_m, \quad i_m, i_n \in \{1,2\}. \tag{86}$$

With this design, the ratio of the minimum distance of the constellation for $v_{i_n,c}$ and the minimum distance of the constellation for $v_{i_m,c}$, i.e., $\frac{\eta_{i_n,c}\gamma}{P^{\frac{\lambda_{i_n,c}}{2}}} \Big/ \frac{\eta_{i_m,c}\gamma}{P^{\frac{\lambda_{i_m,c}}{2}}}$, is an integer, where $1 \leq \eta_{i_n,c} < 2$. By following the step in (19), it is easy to check that the average power constraints $\mathbb{E}|x_1|^2 \leq 1$ and $\mathbb{E}|x_2|^2 \leq 1$ are satisfied. In our scheme, the parameter τ is designed as

$$\tau \triangleq \begin{cases} 2\left\lceil \max\left\{ \left\lceil \frac{\alpha}{1-\alpha} \right\rceil, \left\lceil \frac{1-\alpha+B}{1-\alpha} \right\rceil \right\}/2 \right\rceil & \text{if } \alpha \neq 1 \\ 2 & \text{if } \alpha = 1. \end{cases} \tag{87}$$

The parameters $\{\delta_{k,\ell}\}_{k,\ell}$ are designed as

$$\delta_{1,\ell} \triangleq \begin{cases} -\left(\frac{h_{12}h_{21}}{h_{11}h_{22}}\right)^\ell & \text{if } \alpha \neq 1 \\ -\frac{h_{12}h_{21}}{h_{11}h_{22}-h_{12}h_{21}} & \text{if } \alpha = 1 \end{cases} \tag{88}$$

and

$$\delta_{2,\ell} \triangleq \begin{cases} \frac{h_{21}}{h_{22}} \cdot \left(\frac{h_{12}h_{21}}{h_{11}h_{22}}\right)^{\ell-1} & \text{if } \alpha \neq 1 \\ \frac{h_{11}h_{21}}{h_{11}h_{22}-h_{12}h_{21}} & \text{if } \alpha = 1 \end{cases} \tag{89}$$

for $\ell \in \{1, 2, \cdots \tau/2\}$.

3) Secure rate analysis: Given the codebook design and signal mapping, the result of [46, Theorem 1] implies that we can achieve the following secure rate region

$$\Big\{(R_1, R_2) : \sum_{k=1}^{2} R_k \leq \big(\mathbb{I}(v_1, v_2; y_1) - \mathbb{I}(v_1, v_2; y_2)\big)^+, \\ R_1 \leq \mathbb{I}(v_1; y_1|v_2),\ R_2 \leq \mathbb{I}(v_2; y_1|v_1)\Big\}. \tag{90}$$

In the following subsections we will provide the analysis of the rate region under three different cases, i.e., $0 \leq \alpha \leq \frac{2}{3}$, $\frac{2}{3} \leq \alpha < 1$ and $\alpha = 1$. In the proposed scheme, a Markov chain-based interference neutralization method is used.

A. $0 \leq \alpha \leq \frac{2}{3}$

For this case of $0 \leq \alpha \leq \frac{2}{3}$, we will divide the analysis into two cases and show that the secure GDoF region $\mathcal{D}^*(\alpha)$ is achievable.

[4]For a PAM constellation set defined as $\Omega(\xi, Q) \triangleq \{\xi a :\ a \in [-Q, Q] \cap \mathcal{Z}\}$, the minimum distance of the constellation is ξ.

1) $0 \leq B \leq (2\alpha-1)^+$*:* In the case with $0 \leq \alpha \leq \frac{2}{3}$ and $0 \leq B \leq (2\alpha-1)^+$, based on the parameter design in (78)-(89) and Table III, the transmitted signals take the following forms

$$x_1 = v_{1,c} + \sqrt{P^{-\alpha}} v_{1,p} + \sum_{\ell=1}^{\tau/2} \delta_{1,\ell} \sqrt{P^{-\beta_{1,1,\ell}}} \cdot u_1 \tag{91}$$

$$x_2 = \sqrt{P^{\alpha-1}} \frac{h_{21}}{h_{22}} v_{2,c} + \sum_{\ell=1}^{\tau/2} \delta_{2,\ell} \sqrt{P^{-\beta_{1,2,\ell}}} \cdot u_1. \tag{92}$$

Then the received signals take the forms as

$$y_1 = \sqrt{P} h_{11} v_{1,c} + \sqrt{P^{2\alpha-1}} \frac{h_{12} h_{21}}{h_{22}} v_{2,c} + \sqrt{P^{1-\alpha}} h_{11} v_{1,p} + z_1, \tag{93}$$

$$y_2 = \sqrt{P^{\alpha}} h_{21} (v_{1,c} + v_{2,c} + u_1) + \sqrt{P^{\alpha-\beta_{1,1,\tau/2}}} \delta_{1,\tau/2} h_{21} u_1 + h_{12} v_{1,p} + z_2. \tag{94}$$

In the above expressions of y_1 and y_2, the interference is removed by using the Markov chain-based interference neutralization method. For the secure rate region in (90), we will prove that $\mathbb{I}(v_1, v_2; y_1) - \mathbb{I}(v_1, v_2; y_2) \geq \frac{1-3\epsilon}{2} \log P + o(\log P)$, $\mathbb{I}(v_1; y_1|v_2) \geq \frac{1-B-2\epsilon}{2} \log P + o(\log P)$ and $\mathbb{I}(v_2; y_1|v_1) \geq \frac{B-\epsilon}{2} \log P + o(\log P)$, which will imply that the GDoF region $\{(d_1, d_2) | d_1 + d_2 \leq 1, 0 \leq d_1 \leq 1-B, 0 \leq d_2 \leq B\}$ is achievable, for almost all the channel coefficients $\{h_{k\ell}\} \in (1,2]^{2\times 2}$.

First we focus on the lower bound of $\mathbb{I}(v_1, v_2; y_1) - \mathbb{I}(v_1, v_2; y_2)$. Let $\hat{v}_{1,c}, \hat{v}_{2,c}$ and $\hat{v}_{1,p}$ be the estimates of $v_{1,c}, v_{2,c}$ and $v_{1,p}$ from y_1, respectively. Let $\Pr[\{v_{1,c} \neq \hat{v}_{1,c}\} \cup \{v_{1,p} \neq \hat{v}_{1,p}\} \cup \{v_{2,c} \neq \hat{v}_{2,c}\}]$ denote the corresponding error probability of this estimation. Then the term $\mathbb{I}(v_1, v_2; y_1)$ can be lower bounded by

$$\begin{aligned}
&\mathbb{I}(v_1, v_2; y_1) \\
\geq &\mathbb{I}(v_1, v_2; \hat{v}_{1,c}, \hat{v}_{1,p}, \hat{v}_{2,c}) \qquad (95)\\
= &\mathbb{H}(v_1, v_2) - \mathbb{H}(v_1, v_2 | \hat{v}_{1,c}, \hat{v}_{1,p}, \hat{v}_{2,c}) \\
\geq &\big(1 - \Pr[\{v_{1,c} \neq \hat{v}_{1,c}\} \cup \{v_{1,p} \neq \hat{v}_{1,p}\} \cup \{v_{2,c} \neq \hat{v}_{2,c}\}]\big) \cdot \mathbb{H}(v_1, v_2) - 1. \qquad (96)
\end{aligned}$$

For the term $\mathbb{H}(v_1, v_2)$ appeared in (96) we have

$$\mathbb{H}(v_1, v_2) = \mathbb{H}(v_{1,c}) + \mathbb{H}(v_{1,p}) + \mathbb{H}(v_{2,c}) = \frac{1-3\epsilon}{2} \log P + o(\log P). \tag{97}$$

Below we provide a result on the error probability appeared in (96).

Lemma 4. *When* $0 \leq \alpha \leq \frac{2}{3}$ *and* $0 \leq B \leq (2\alpha-1)^+$*, given the signal design in Table III,* (80)-(84) *and* (91)-(92)*, for almost all the channel realizations the error probability of decoding* $\{v_{1,c}, v_{1,p}, v_{2,c}\}$ *from* y_1 *is vanishing when* P *goes large, i.e.,*

$$Pr[\{v_{1,c} \neq \hat{v}_{1,c}\} \cup \{v_{1,p} \neq \hat{v}_{1,p}\} \cup \{v_{2,c} \neq \hat{v}_{2,c}\}] \to 0 \quad as \ P \to \infty. \tag{98}$$

Proof. This proof follows from the key steps of the proofs of Lemma 1 and Lemma 2. Specifically, in this setting one can first estimate $v_{1,c}$ from y_1 expressed in (93) based on successive decoding method (see Lemma 1), and then estimate $v_{2,c}$ and $v_{1,p}$ simultaneously based on noise removal and signal separation methods (see Lemma 2). One can follow the proof steps of Lemma 1 and Lemma 2 to show that this error probability is vanishing as P goes large. In order to avoid the repetition we skip the details in this proof. □

With the results of (96), (97) and Lemma 4, we can bound the term $\mathbb{I}(v_1, v_2; y_1)$ as

$$\mathbb{I}(v_1, v_2; y_1) \geq \frac{1-3\epsilon}{2} \log P + o(\log P) \tag{99}$$

for almost all the channel coefficients $\{h_{k\ell}\} \in (1,2]^{2\times 2}$. For the term $\mathbb{I}(v_1, v_2; y_2)$, we can bound it as

$$\begin{aligned}
&\mathbb{I}(v_1, v_2; y_2) \\
\leq &\mathbb{I}(v_1, v_2; y_2, v_{1,c} + v_{2,c} + u_1) \qquad (100)\\
= &\mathbb{I}(v_1, v_2; v_{1,c} + v_{2,c} + u_1) + \mathbb{I}(v_1, v_2; y_2 | v_{1,c} + v_{2,c} + u_1) \\
\leq &\mathbb{H}(v_{1,c} + v_{2,c} + u_1) - \mathbb{H}(u_1) \\
&+ \mathrm{h}(\sqrt{P^{\alpha-\beta_{1,1,\tau/2}}} \delta_{1,\tau/2} h_{21} u_1 + h_{12} v_{1,p} + z_2) - \mathrm{h}(z_2) \qquad (101)\\
\leq &\log(6Q'+1) - \log(2Q'+1) \\
&+ \frac{1}{2} \log\big(2\pi e (\frac{8}{3\tau^2} + \frac{2}{3\tau^2 \cdot 4^\tau} + 1)\big) - \frac{1}{2} \log(2\pi e) \qquad (102)\\
\leq &\log\left(3\sqrt{\frac{8}{3\tau^2} + \frac{2}{3\tau^2 \cdot 4^\tau} + 1}\right) \qquad (103)
\end{aligned}$$

where (102) stems from the derivation that $\mathbb{H}(v_{1,c} + v_{2,c} + u_1) \leq \log(6Q'+1)$ and $\mathbb{H}(u_1) = \log(2Q'+1)$, where $Q' \triangleq P^{\frac{\max\{\lambda_{1,c}, \lambda_{2,c}\}}{2}}$. Due to our design in (85)-(86), the ratio between the minimum distance of the constellation for $v_{2,c}$ and the minimum distance of the constellation for $v_{1,c}$ is an integer. This integer relationship allows us to minimize the value of $\mathbb{H}(v_{1,c} + v_{2,c} + u_1)$, which can be treated as a GDoF penalty.

Given the results of (99) and (103), it reveals that

$$\mathbb{I}(v_1, v_2; y_1) - \mathbb{I}(v_1, v_2; y_2) \geq \frac{1-3\epsilon}{2} \log P + o(\log P) \tag{104}$$

for almost all the channel realizations. Now we consider the bound of $\mathbb{I}(v_1; y_1|v_2)$. Let

$$y_1' = \sqrt{P} h_{11} v_{1,c} + \sqrt{P^{1-\alpha}} h_{11} v_{1,p} + z_1 \tag{105}$$

and let $\{\hat{v}_{1,c}', \hat{v}_{1,p}'\}$ be the estimates of $\{v_{1,c}, v_{1,p}\}$ from y_1'. Then we have

$$\begin{aligned}
&\mathbb{I}(v_1; y_1|v_2) \\
= &\mathbb{I}(v_1, y_1') \qquad (106)\\
\geq &\big(1 - \Pr[\{v_{1,c} \neq \hat{v}_{1,c}'\} \cup \{v_{1,p} \neq \hat{v}_{1,p}'\}]\big) \cdot \mathbb{H}(v_1) - 1 \qquad (107)
\end{aligned}$$

where (106) follows from the independence between v_2 and v_1; (107) follows from the steps in (95) and (96). For the term $\mathbb{H}(v_1)$ appeared in (107), we have

$$\mathbb{H}(v_1) = \frac{1-B-2\epsilon}{2} \log P + o(\log P). \tag{108}$$

By following the proof steps of Lemma 1, one can easily prove that error probability of estimating $v_{1,c}$ and $v_{1,p}$ based on y_1' is vanishing when P goes large, that is,

$$\Pr[\{v_{1,c} \neq \hat{v}_{1,c}'\} \cup \{v_{1,p} \neq \hat{v}_{1,p}'\}] \to 0 \quad \text{as} \quad P \to \infty. \tag{109}$$

With (107), (108) and (109), it suggests that

$$\mathbb{I}(v_1; y_1|v_2) \geq \frac{1-B-2\epsilon}{2}\log P + o(\log P). \tag{110}$$

Similarly, $\mathbb{I}(v_2; y_1|v_1)$ can be bounded by

$$\mathbb{I}(v_2; y_1|v_1) \geq \frac{B-\epsilon}{2}\log P + o(\log P). \tag{111}$$

By combining the results of (90), (104), (110) and (111), it implies that the GDoF region $\{(d_1, d_2)|d_1+d_2 \leq 1, 0 \leq d_1 \leq 1-B, 0 \leq d_2 \leq B\}$ is achievable for almost all the channel coefficients, for this case with $0 \leq \alpha \leq \frac{2}{3}$ and $0 \leq B \leq (2\alpha-1)^+$.

2) $(2\alpha-1)^+ < B \leq \alpha$*:* In the case with $0 \leq \alpha \leq \frac{2}{3}$ and $(2\alpha-1)^+ < B \leq \alpha$, by following the steps in the previous case one can prove that the GDoF region $\{(d_1, d_2)|d_1+d_2 \leq 1, 0 \leq d_1 \leq 1-B, 0 \leq d_2 \leq B\}$ is achievable.

Finally, by combining the results of the above two cases and by moving B from 0 to α, it reveals that for almost all the channel realizations the proposed scheme achieves $\mathcal{D}^*(\alpha)$ in this case of $0 \leq \alpha \leq \frac{2}{3}$.

B. $\frac{2}{3} \leq \alpha < 1$

When $\frac{2}{3} \leq \alpha < 1$, we will also divide the analysis into two cases.

1) $0 \leq B \leq 2\alpha-1$*:* In the case with $\frac{2}{3} \leq \alpha < 1$ and $B \leq 2\alpha-1$, the signals of the transmitters have the same forms as in (91) and (92), and the signals of the receivers take the same forms as in (93) and (94). In this case, we have

$$\begin{aligned}
&\mathbb{I}(v_1, v_2; y_1) \\
&\geq \big(1\text{–}\Pr[\{v_{1,c} \neq \hat{v}_{1,c}\} \cup \{v_{1,p} \neq \hat{v}_{1,p}\} \cup \{v_{2,c} \neq \hat{v}_{2,c}\}]\big) \cdot \mathbb{H}(v_1, v_2) \text{–} 1 \qquad (112)\\
&= \frac{1-3\epsilon}{2}\log P + o(\log P) \qquad (113)
\end{aligned}$$

for almost all the channel coefficients, where (112) follows from the steps in (95)-(96); the last step stems from Lemma 5 (see below) and the derivation that $\mathbb{H}(v_1, v_2) = \mathbb{H}(v_{1,c}) + \mathbb{H}(v_{1,p}) + \mathbb{H}(v_{2,c}) = \frac{1-3\epsilon}{2}\log P + o(\log P)$.

Lemma 5. *When* $\frac{2}{3} \leq \alpha < 1$ *and* $0 \leq B \leq 2\alpha-1$*, given the signal design in Table III,* (80)-(84) *and* (91)-(92)*, for almost all the channel coefficients* $\{h_{k\ell}\} \in (1, 2]^{2\times 2}$*, the error probability of decoding* $\{v_{1,c}, v_{1,p}, v_{2,c}\}$ *from* y_1 *is vanishing when* P *is large, i.e.,*

$$Pr[\{v_{1,c} \neq \hat{v}_{1,c}\} \cup \{v_{1,p} \neq \hat{v}_{1,p}\} \cup \{v_{2,c} \neq \hat{v}_{2,c}\}] \to 0 \quad as \ P \to \infty. \tag{114}$$

Proof. See Appendix D. □

From the steps in (100)-(103), one can easily show that $\mathbb{I}(v_1, v_2; y_2) \leq o(\log P)$, which, together with (113), implies that

$$\mathbb{I}(v_1, v_2; y_1) - \mathbb{I}(v_1, v_2; y_2) \geq \frac{1-3\epsilon}{2}\log P + o(\log P) \tag{115}$$

for almost all the channel coefficients. From the steps in (105)-(111), the following two inequalities can be easily derived

$$\mathbb{I}(v_1; y_1|v_2) \geq \frac{1-B-2\epsilon}{2}\log P + o(\log P), \tag{116}$$

$$\mathbb{I}(v_2; y_1|v_1) \geq \frac{B-\epsilon}{2}\log P + o(\log P). \tag{117}$$

From (90) and (115)–(117) we can conclude that the secure GDoF region $\{(d_1, d_2)|d_1+d_2 \leq 1, 0 \leq d_1 \leq 1-B, 0 \leq d_2 \leq B\}$ is achievable for almost all the channel coefficients, for this case with $0 \leq \alpha \leq \frac{2}{3}$ and $0 \leq B \leq 2\alpha-1$.

2) $2\alpha-1 < B \leq \alpha$*:* In the case with $\frac{2}{3} \leq \alpha < 1$ and $2\alpha-1 < B \leq \alpha$, by following the steps in the previous case one can prove that the GDoF region $\{(d_1, d_2)|d_1+d_2 \leq 1, 0 \leq d_1 \leq 1-B, 0 \leq d_2 \leq B\}$ is achievable.

Finally, by combining the results of the above two cases and by moving B from 0 to α, it reveals that for almost all the channel realizations the proposed scheme achieves $\mathcal{D}^*(\alpha)$ in this case of $0 \leq \alpha \leq \frac{2}{3}$.

C. $\alpha = 1$

In the case with $\alpha = 1$, for any GDoF pair $(d_1^{'}, d_2^{'})$ such that $(d_1^{'}, d_2^{'}) \in \mathcal{D}^*(1)$, we will provide the following scheme and show that the GDoF pair $(d_1^{'}, d_2^{'})$ is achievable with $d_c^{'} = \max\{d_1^{'}, d_2^{'}\}$ GDoF common randomness. Based on the parameter design in (78)-(89) and Table III, then the transmitted signals are designed as

$$x_1 = \varepsilon v_{1,c} - \varepsilon\frac{h_{12}h_{21}}{h_{11}h_{22}-h_{12}h_{21}} \cdot u_1 \tag{118}$$

$$x_2 = \varepsilon\frac{h_{21}}{h_{22}} \cdot v_{2,c} + \varepsilon\frac{h_{11}h_{21}}{h_{11}h_{22}-h_{12}h_{21}} \cdot u_1. \tag{119}$$

In terms of the signals at the receivers, we have

$$y_1 = \varepsilon\sqrt{P}h_{11}v_{1,c} + \varepsilon\sqrt{P}\frac{h_{12}h_{21}}{h_{22}} \cdot v_{2,c} + z_1 \tag{120}$$

$$y_2 = \varepsilon\sqrt{P}h_{21}(v_{1,c} + v_{2,c} + u_1) + z_2. \tag{121}$$

From the derivations in (95)-(97), (100)-(103), and Lemma 2, the term $\mathbb{I}(v_1, v_2; y_1) - \mathbb{I}(v_1, v_2; y_2)$ in (90) can be bounded by

$$\mathbb{I}(v_1, v_2; y_1) - \mathbb{I}(v_1, v_2; y_2) \geq \frac{d_1^{'} + d_2^{'} - 2\epsilon}{2}\log P + o(\log P) \tag{122}$$

for almost all the channel coefficients. By following the steps in (105)-(111), we have

$$\mathbb{I}(v_1; y_1|v_2) \geq \frac{d_1^{'} - \epsilon}{2}\log P + o(\log P). \tag{123}$$

$$\mathbb{I}(v_2; y_1|v_1) \geq \frac{d_2^{'} - \epsilon}{2}\log P + o(\log P). \tag{124}$$

Finally, by incorporating the results of (122)-(124) into (90), it suggests that the secure GDoF pair $(d_1^{'}, d_2^{'})$ is achievable by using $d_c^{'} = \max\{d_1^{'}, d_2^{'}\}$ GDoF of common randomness (mainly due to u_1), for almost all the channel coefficients $\{h_{k\ell}\} \in (1, 2]^{2\times 2}$. By moving $d_1^{'}$ from 0 to $1-d_2^{'}$ and moving $d_2^{'}$ from 0 to 1, then we can conclude that any GDoF pair $(d_1^{'}, d_2^{'}) \in \mathcal{D}^*(1)$ is achievable by using $d_c^{'} = \max\{d_1^{'}, d_2^{'}\}$ GDoF of common randomness for almost all the channel coefficients, in this case with $\alpha = 1$.

D. $\alpha > 1$

We have proved in Sections VII-A-VII-C that the optimal secure GDoF region $\mathcal{D}^*(\alpha)$ is achievable by the proposed scheme when $\alpha \leq 1$, where $\mathcal{D}^*(\alpha) = \{(d_1, d_2) | d_1 + d_2 \leq \max\{1, \alpha\}, 0 \leq d_1 \leq 1, 0 \leq d_2 \leq \alpha\}$.

Let us consider a secure GDoF pair $(d_1^{'}, d_2^{'})$ such that $(d_1^{'}, d_2^{'}) \in \mathcal{D}^*(\alpha)$, with conditions $0 \leq d_1^{'} \leq 1 - d_2^{'}$ and $0 \leq d_2^{'} \leq \alpha$, for $\alpha \leq 1$. From Sections VII-A-VII-C, it reveals that the proposed scheme is able to achieve this secure GDoF pair $(d_1^{'}, d_2^{'})$ with a certain amount of GDoF common randomness. For notationally convenience let us use $d_c^{'}$ to denote that amount of GDoF common randomness for achieving the corresponding GDoF pair $(d_1^{'}, d_2^{'})$ in the proposed scheme. For this secure GDoF tuple $(d_1^{'}, d_2^{'}, d_c^{'})$, it holds true that

$$(d_1^{'}, d_2^{'}, d_c^{'}) \in \bar{\mathcal{D}}(\alpha) \tag{125}$$

since it is achievable by the proposed scheme, for $\alpha \leq 1$. From the result of Lemma 3, it also holds true that

$$\left(d_2^{'}/\alpha,\ d_1^{'}/\alpha,\ d_c^{'}/\alpha\right) \in \bar{\mathcal{D}}(1/\alpha). \tag{126}$$

In other words, the secure GDoF tuple $(d_2^{'}/\alpha,\ d_1^{'}/\alpha,\ d_c^{'}/\alpha)$ is included in the region $\bar{\mathcal{D}}(1/\alpha)$ and the secure GDoF pair $(d_2^{'}/\alpha,\ d_1^{'}/\alpha)$ is included in the region $\mathcal{D}^*(\frac{1}{\alpha})$, for $\alpha \leq 1$. Then, by moving $d_2^{'}$ from 0 to α and moving $d_1^{'}$ from 0 to $1 - d_2^{'}$, it implies that any point in $\mathcal{D}^*(\frac{1}{\alpha}) = \{(d_1, d_2) | d_1 + d_2 \leq \frac{1}{\alpha}, 0 \leq d_1 \leq 1, 0 \leq d_2 \leq \frac{1}{\alpha}\}$ is achievable for $\alpha \leq 1$. Let $\alpha^{'} = 1/\alpha$, we finally conclude that the optimal secure GDoF region $\mathcal{D}^*(\alpha^{'}) = \{(d_1, d_2) | d_1 + d_2 \leq \alpha^{'}, 0 \leq d_1 \leq 1, 0 \leq d_2 \leq \alpha^{'}\}$ is achievable for $\alpha^{'} > 1$.

VIII. Converse

In this section we will provide the converse proofs for Theorems 4-6, regarding the minimal GDoF of the common randomness to achieve the maximal secure sum GDoF, secure GDoF, and the maximal secure GDoF region for interference channel, wiretap channel with a helper, and multiple access wiretap channel, respectively. Let us define that

$$s_{k\ell}(t) \triangleq \sqrt{P^{\alpha_{k\ell}}} h_{k\ell} x_\ell(t) + z_k(t)$$

for $k, \ell \in \{1, 2\}, k \neq \ell$. Let $s_{k\ell}^n \triangleq \{s_{k\ell}(t)\}_{t=1}^n$.

A. Converse for two-user interference channel

We begin with the converse proof of Theorem 4, for the two-user interference channel defined in Section II-A. The following lemma reveals a bound on the minimal GDoF of common randomness $d_c^*(\alpha)$, for achieving the maximal secure sum GDoF $d_{\text{sum}}^*(\alpha)$.

Lemma 6. *Given the two-user symmetric Gaussian IC-SC channel (see Section II-A), the minimal GDoF of the common randomness $d_c^*(\alpha)$ for achieving the maximal secure sum GDoF $d_{sum}^*(\alpha)$ satisfies the following inequality*

$$d_c^*(\alpha) \geq d_{sum}^*(\alpha)/2 - (1 - \alpha)^+ \qquad \alpha \in [0, \infty). \tag{127}$$

In what follows, we will prove Lemma 6. This proof will use the secrecy constraints and Fano's inequality. Starting with the secrecy constraint $\mathbb{I}(w_1; y_2^n) \leq n\epsilon$, and with the identity of $\mathbb{I}(w_1; y_2^n) = \mathbb{I}(w_1; w_c, w_2, y_2^n) - \mathbb{I}(w_1; w_c, w_2 | y_2^n)$, we have

$$\mathbb{I}(w_1; w_c, w_2, y_2^n) \leq \mathbb{I}(w_1; w_c, w_2 | y_2^n) + n\epsilon. \tag{128}$$

The first term in the right-hand side of (128) is bounded as

$$\begin{aligned}
\mathbb{I}(w_1; w_c, w_2 | y_2^n) &= \mathbb{H}(w_c, w_2 | y_2^n) - \mathbb{H}(w_c, w_2 | y_2^n, w_1) \\
&\leq \mathbb{H}(w_c) + \mathbb{H}(w_2 | y_2^n) && (129) \\
&\leq \mathbb{H}(w_c) + n\epsilon_n && (130)
\end{aligned}$$

where (129) uses the fact that conditioning reduces entropy; and (130) follows from Fano's inequality. On the other hand, the term in the left-hand side of (128) can be rewritten as

$$\begin{aligned}
\mathbb{I}(w_1; w_c, w_2, y_2^n) &= \mathbb{I}(w_1; y_2^n | w_c, w_2) \\
&= \mathbb{H}(w_1) - \mathbb{H}(w_1 | w_c, w_2, y_2^n) && (131)
\end{aligned}$$

using the independence between w_1, w_c and w_2. By incorporating (130) and (131) into (128), it gives

$$\mathbb{H}(w_1) \leq \mathbb{H}(w_c) + \mathbb{H}(w_1 | w_c, w_2, y_2^n) + n\epsilon_n + n\epsilon. \tag{132}$$

For the second term in the right-hand side of (132), we have

$$\begin{aligned}
&\mathbb{H}(w_1 | w_c, w_2, y_2^n) \\
=&\mathbb{H}(w_1 | w_c, w_2, y_2^n, s_{21}^n) && (133) \\
\leq&\mathbb{H}(w_1 | w_c, w_2, y_2^n, s_{21}^n) - \mathbb{H}(w_1 | y_1^n) + n\epsilon_n && (134) \\
\leq&\mathbb{H}(w_1 | w_c, w_2, s_{21}^n) - \mathbb{H}(w_1 | y_1^n, w_c, w_2, s_{21}^n) + n\epsilon_n \\
=&\mathbb{I}(w_1; y_1^n | w_c, w_2, s_{21}^n) + n\epsilon_n \\
=&\mathbb{I}(w_1; \{y_1(t) - \sqrt{P^{1-\alpha}} \cdot \frac{h_{11}}{h_{21}} s_{21}(t) \\
&- \sqrt{P^\alpha} h_{12} x_2(t)\}_{t=1}^n | w_c, w_2, s_{21}^n) + n\epsilon_n && (135) \\
=&\mathbb{I}(w_1; \{-\sqrt{P^{1-\alpha}} \cdot \frac{h_{11}}{h_{21}} z_2(t) + z_1(t)\}_{t=1}^n | w_c, w_2, s_{21}^n) + n\epsilon_n \\
=&\mathrm{h}(\{-\sqrt{P^{1-\alpha}} \cdot \frac{h_{11}}{h_{21}} z_2(t) + z_1(t)\}^n | w_c, w_2, s_{21}^n) \\
&- \mathrm{h}(\{-\sqrt{P^{1-\alpha}} \cdot \frac{h_{11}}{h_{21}} z_2(t) + z_1(t)\}^n | w_1, w_c, w_2, s_{21}^n) + n\epsilon_n \\
=&\mathrm{h}(\{-\sqrt{P^{1-\alpha}} \cdot \frac{h_{11}}{h_{21}} z_2(t) + z_1(t)\}^n | w_c, w_2, s_{21}^n) - \mathrm{h}(z_1^n) + n\epsilon_n && (136) \\
\leq&\frac{n}{2} \log(1 + P^{1-\alpha} \cdot \frac{|h_{11}|^2}{|h_{21}|^2}) + n\epsilon_n && (137)
\end{aligned}$$

where (133) follows from the fact that s_{21}^n can be reconstructed by $\{w_c, w_2, y_2^n\}$; (134) is from Fano's inequality; (135) uses the fact that x_2^n is a function of (w_c, w_2); (136) results from the fact that z_2^n can be reconstructed from $\{w_1, w_c, w_2, s_{21}^n\}$; (137) follows from the identity that conditioning reduces differential entropy and the identity that $\mathrm{h}(z_1^n) = \frac{n}{2} \log(2\pi e)$. Finally, given that $\mathbb{H}(w_1) = nR_1$ and $\mathbb{H}(w_c) = nR_c$, combining the results of (132) and (137) gives the following inequality

$$nR_1 - \frac{n}{2} \log(1 + P^{1-\alpha} \cdot \frac{|h_{11}|^2}{|h_{21}|^2}) - n\epsilon_n' \leq nR_c \tag{138}$$

for $\epsilon_n' = 2\epsilon_n + \epsilon$. Due to the symmetry, by exchanging the roles of user 1 and user 2, we also have

$$nR_2 - \frac{n}{2} \log(1 + P^{1-\alpha} \cdot \frac{|h_{22}|^2}{|h_{12}|^2}) - n\epsilon_n' \leq nR_c. \tag{139}$$

Based on the definitions of $d_c^*(\alpha)$ and $d_{\text{sum}}^*(\alpha)$ in Section II-A, combining the results of (138) and (139) produces the following bound

$$d_{\text{sum}}^*(\alpha)/2-(1-\alpha)^+\leq d_c^*(\alpha),\qquad \forall\alpha\in[0,\infty) \tag{140}$$

which completes the proof of Lemma 6.

B. Converse for the wiretap channel with a helper

Let us now focus on the converse proof of Theorem 5 for the wiretap channel with a helper. The following lemma reveals a bound on the minimal GDoF of common randomness $d_c^*(\alpha)$, for achieving the maximal secure GDoF, i.e., $d^*(\alpha)=1$ for any $\alpha\in[0,\infty)$ (see Theorem 2).

Lemma 7. *Given the* symmetric *Gaussian WTH channel (see Section II-B), the minimal GDoF of the common randomness $d_c^*(\alpha)$ for achieving the maximal secure GDoF satisfies the following inequality*

$$d_c^*(\alpha)\geq 1-(1-\alpha)^+\qquad \alpha\in[0,\infty). \tag{141}$$

The proof of Lemma 7 follows closely from that of Lemma 6. One difference is that in this setting w_2 is kept as an empty term. By following the steps in (128)-(132) we have the following bound for this setting

$$\mathbb{H}(w_1)\leq\mathbb{H}(w_c)+\mathbb{H}(w_1|w_c,y_2^n)+n\epsilon. \tag{142}$$

By following the steps in (133)-(137) we have the following bound for this setting

$$\mathbb{H}(w_1|w_c,y_2^n)\leq\frac{n}{2}\log(1+P^{1-\alpha}\cdot\frac{|h_{11}|^2}{|h_{21}|^2})+n\epsilon_n. \tag{143}$$

The results of (142) and (143) imply that

$$nR_1-\frac{n}{2}\log(1+P^{1-\alpha}\cdot\frac{|h_{11}|^2}{|h_{21}|^2})-n\epsilon_n'\leq nR_c \tag{144}$$

for $\epsilon_n'=\epsilon_n+\epsilon$. Based on the definitions of $d_c^*(\alpha)$ and $d^*(\alpha)$ in Section II-B, and given the result of Theorem 2, i.e., $d^*(\alpha)=1,\forall\alpha\in[0,\infty)$, the result of (144) gives the following bound

$$1-(1-\alpha)^+\leq d_c^*(\alpha),\qquad \forall\alpha\in[0,\infty) \tag{145}$$

which completes the proof of Lemma 7.

C. Converse for two-user multiple access wiretap channel

Let us consider the converse proof of Theorem 6 for the two-user multiple access wiretap channel. The following lemma gives a bound on the minimal GDoF of common randomness $d_c^*(\alpha,d_1,d_2)$, for achieving any given GDoF pair (d_1,d_2) in the maximal secure GDoF region $\mathcal{D}^*(\alpha)$.

Lemma 8. *For the* symmetric *Gaussian MAC-WT channel with common randomness (see Section II-C), the minimal GDoF of the common randomness $d_c^*(\alpha,d_1,d_2)$, for achieving any given GDoF pair (d_1,d_2) in the maximal secure GDoF region $\mathcal{D}^*(\alpha)$, satisfies the following inequality*

$$d_c^*(\alpha,d_1,d_2)\geq\max\{d_1-(1-\alpha)^+,d_2-(\alpha-1)^+\}$$

for $(d_1,d_2)\in\mathcal{D}^*(\alpha)$.

The following corollary is directly from Lemma 8 by considering the specific case with $\alpha=1$.

Corollary 1. *For the* symmetric *Gaussian MAC-WT channel with common randomness defined in Section II-C, and for $\alpha=1$, the minimal GDoF of the common randomness $d_c^*(1,d_1,d_2)$, for achieving any given GDoF pair (d_1,d_2) in the maximal secure GDoF region $\mathcal{D}^*(1)$, satisfies the following inequality*

$$d_c^*(1,d_1,d_2)\geq\max\{d_1,d_2\}\quad \textit{for}\quad (d_1,d_2)\in\mathcal{D}^*(1),\ \alpha=1.$$

Let us now prove Lemma 8. This proof will also use the secrecy constraints and Fano's inequality. However, in this setting some steps in the proof are slightly different from that in the previous proofs. Note that in this setting, the confidential messages are intended to receiver 1.

Starting with the secrecy constraint $\mathbb{I}(w_1,w_2;y_2^n)\leq n\epsilon$, and with the identity of $\mathbb{I}(w_1,w_2;y_2^n)=\mathbb{I}(w_1,w_2;w_c,y_2^n)-\mathbb{I}(w_1,w_2;w_c|y_2^n)$, we have

$$\mathbb{I}(w_1,w_2;w_c,y_2^n)\leq\mathbb{I}(w_1,w_2;w_c|y_2^n)+n\epsilon. \tag{146}$$

The first term in the right-hand side of (146) is bounded as

$$\begin{aligned}\mathbb{I}(w_1,w_2;w_c|y_2^n)&=\mathbb{H}(w_c|y_2^n)-\mathbb{H}(w_c|y_2^n,w_1,w_2)\\&\leq\mathbb{H}(w_c).\end{aligned} \tag{147}$$

On the other hand, the term in the left-hand side of (146) can be rewritten as

$$\begin{aligned}\mathbb{I}(w_1,w_2;w_c,y_2^n)&=\mathbb{I}(w_1,w_2;y_2^n|w_c)\\&=\mathbb{H}(w_1,w_2)-\mathbb{H}(w_1,w_2|w_c,y_2^n)\\&=\mathbb{H}(w_1)+\mathbb{H}(w_2)-\mathbb{H}(w_1,w_2|w_c,y_2^n)\end{aligned} \tag{148}$$

using the independence between w_1, w_c and w_2. By incorporating (147) and (148) into (146), it gives

$$\begin{aligned}\mathbb{H}(w_2)\leq&\mathbb{H}(w_c)-\mathbb{H}(w_1)+\mathbb{H}(w_1,w_2|w_c,y_2^n)+n\epsilon\\\leq&\mathbb{H}(w_c)-\mathbb{H}(w_1)+\mathbb{H}(w_1,w_2|w_c,y_2^n)\\&-\mathbb{H}(w_1,w_2|y_1^n)+n\epsilon_n+n\epsilon \qquad (149)\\=&\mathbb{H}(w_c)\underbrace{-\mathbb{H}(w_1)+\mathbb{H}(w_1|w_c,y_2^n)}_{\leq 0}+\mathbb{H}(w_2|w_1,w_c,y_2^n)\\&\underbrace{-\mathbb{H}(w_1|y_1^n)}_{\leq 0}-\mathbb{H}(w_2|w_1,y_1^n)+n\epsilon_n'\\\leq&\mathbb{H}(w_c)+\mathbb{H}(w_2|w_1,w_c,y_2^n)-\mathbb{H}(w_2|w_1,y_1^n)+n\epsilon_n' \qquad (150)\end{aligned}$$

for $\epsilon_n'\triangleq\epsilon_n+\epsilon$, where (149) stems from Fano's equality. For the second and third terms in the right-hand side of (150), we have

$$\begin{aligned}&\mathbb{H}(w_2|w_1,w_c,y_2^n)-\mathbb{H}(w_2|w_1,y_1^n)\\\leq&\mathbb{H}(w_2|\{\sqrt{P}h_{22}x_2(t)+z_2(t)\}_{t=1}^n,w_1,w_c,y_2^n)\\&-\mathbb{H}(w_2|\{\sqrt{P}h_{22}x_2(t)+z_2(t)\}_{t=1}^n,w_1,w_c,y_1^n) \qquad (151)\\\leq&\mathbb{H}(w_2|\{\sqrt{P}h_{22}x_2(t)+z_2(t)\}_{t=1}^n,w_1,w_c)\\&-\mathbb{H}(w_2|\{\sqrt{P}h_{22}x_2(t)+z_2(t)\}_{t=1}^n,w_1,w_c,y_1^n) \qquad (152)\\=&\mathbb{I}(w_2;y_1^n|\{\sqrt{P}h_{22}x_2(t)+z_2(t)\}_{t=1}^n,w_1,w_c)\end{aligned}$$

$$=\mathbb{I}(w_2;\{y_1(t)-\sqrt{P^{\alpha-1}}\cdot\frac{h_{12}}{h_{22}}(\sqrt{P}h_{22}x_2(t)+z_2(t)) - \sqrt{P}h_{11}x_1(t)\}_{t=1}^n|w_c,w_1,\{\sqrt{P}h_{22}x_2(t)+z_2(t)\}_{t=1}^n) \quad (153)$$

$$=\mathbb{I}(w_2;\{-\sqrt{P^{\alpha-1}}\cdot\frac{h_{12}}{h_{22}}z_2(t)+z_1(t)\}_{t=1}^n|w_c,w_1,\{\sqrt{P}h_{22}x_2(t) +z_2(t)\}_{t=1}^n)$$

$$\leq\frac{n}{2}\log(1+P^{\alpha-1}\cdot\frac{|h_{12}|^2}{|h_{22}|^2}) \quad (154)$$

where (151) follows from the fact that $\{\sqrt{P}h_{22}x_2(t)+z_2(t)\}_{t=1}^n$ can be reconstructed by $\{w_1,w_c,y_2^n\}$ and the fact that conditioning reduces entropy; (152) results from the fact that conditioning reduces entropy; (153) uses the fact that x_1^n is a function of (w_c,w_1); (154) follows from the identity that conditioning reduces differential entropy. Combining the results of (150) and (154), it gives the following inequality

$$\mathbb{H}(w_2)-\frac{n}{2}\log(1+P^{\alpha-1}\cdot\frac{|h_{12}|^2}{|h_{22}|^2})-n\epsilon_n'\leq\mathbb{H}(w_c). \quad (155)$$

Finally, given that $\mathbb{H}(w_2)=nR_2$ and $\mathbb{H}(w_c)=nR_c$, (155) implies the following inequality

$$nR_2-\frac{n}{2}\log(1+P^{\alpha-1}\cdot\frac{|h_{12}|^2}{|h_{22}|^2})-n\epsilon_n'\leq nR_c. \quad (156)$$

On the other hand, by interchanging the roles of transmitter 1 and transmitter 2, we also have

$$nR_1-\frac{n}{2}\log(1+P^{1-\alpha}\cdot\frac{|h_{11}|^2}{|h_{21}|^2})-n\epsilon_n'\leq nR_c. \quad (157)$$

Based on the definition of $d_c^*(\alpha,d_1,d_2)$ in Section II-C, the results of (156) and (157) give the following bound

$$\max\{d_1-(1-\alpha)^+,d_2-(\alpha-1)^+\}\leq d_c^*(\alpha,d_1,d_2), \quad (158)$$

for $(d_1,d_2)\in\mathcal{D}^*(\alpha)$, which completes the proof of Lemma 8.

IX. Discussion and Conclusion

In this work we showed that adding common randomness at the transmitters *totally* removes the penalty in sum GDoF or GDoF region of three basic channels. The results reveal that adding common randomness at the transmitters is a constructive way to remove the secrecy constraints in communication networks in terms of GDoF performance. Another contribution of this work is the characterization on the minimal amount of common randomness for removing the secrecy penalty.

For our settings, a common randomness is considered to be available at the transmitters. In the proposed schemes the signals are designed with common randomness, which achieve the maximal secure GDoF performance as if without secrecy constraints. To get the results for the settings without common randomness, one might need to modify the schemes accordingly, e.g., remove the common randomness and add the private randomness. Similarly, for the converse, one might need to modify the proofs in order to derive the results for the setting without common randomness. In one direction of the future work, we will focus on the setting with limited common randomness, which covers the extreme case without common randomness and the other extreme case with unlimited common randomness.

As mentioned, one of the contributions of our work is the characterization on the minimal amount of common randomness for achieving the maximal secure GDoF as if without secrecy constraints. In general there is a tradeoff between the secure GDoF and the amount of the common randomness. For example, considering the two-user symmetric interference channel with $\alpha=1$, for the extreme case without common randomness the maximal secure sum GDoF is $2/3$, while for the case with $1/2$ GDoF of common randomness the maximal secure sum GDoF is 1. It implies that there is a tradeoff between the secure GDoF and the amount of the common randomness for this example. In one direction of the future work, we will investigate the tradeoff between secure GDoF and the amount of common randomness in secure communication networks.

This work specifically considers the weak secrecy constraints (see the statements in Section II), like many other works in the references, e.g., [7]–[16]. Our converse results hold for the settings with strong secrecy constraints, just with a minor modification in the proofs, i.e., by replacing $n\epsilon$ with ϵ in the secrecy constraint terms accordingly. Based on the result in [25] by Wang et al., our achievability results on the interference channel and the wiretap channel with a helper could be extended to the settings with strong secrecy constraints as well.

Although we focus on the symmetric settings in this work, our results could be extended to the asymmetric setting. A discussion on the extension to the asymmetric setting is provided in the following subsection.

A. The extension to the asymmetric setting

Let us first consider an example of asymmetric setting by focusing on the wiretap channel with helper, given the parameters of $(\alpha_{11}=\alpha_{22}=1,\alpha_{12}=1/2,\alpha_{21}=2/3)$. For this example, the scheme originally proposed for the symmetric setting, described in Section VI, can be generalized to achieve the secure GDoF $d=1$ by using $d_c=2/3$ GDoF of common randomness, which will be shown to be optimal. Specifically, by following the scheme described in Section VI-A, we set $\beta_{u_0}=\infty$, $\beta_{u_1}=5/6$, $\beta'_{u_1}=1/3$, $\beta_p=\alpha_{21}=2/3$, $\lambda_c=\lambda_u=2/3-\epsilon$, and $\lambda_p=1/3-\epsilon$, and design the signals at the transmitters as

$$x_1=v_c+\sqrt{P^{-\alpha_{21}}}v_p-\sqrt{P^{-\beta_{u_1}}}\frac{h_{12}h_{21}}{h_{11}h_{22}}u,\quad x_2=\sqrt{P^{-\beta'_{u_1}}}\frac{h_{21}}{h_{22}}u.$$

Then, the received signals take the following forms

$$y_1=\sqrt{P}h_{11}v_c+\sqrt{P^{\frac{1}{3}}}h_{11}v_p+z_1$$
$$y_2=\sqrt{P^{\frac{2}{3}}}h_{21}(v_c+u)+h_{21}v_p-\sqrt{P^{-\frac{1}{6}}}\frac{h_{12}h_{21}^2}{h_{11}h_{22}}u+z_2.$$

At this point, by following the rate analysis in Section VI-A one can show that the secure GDoF value $d=1$ is achievable by using $d_c=2/3$ GDoF of common randomness. Note that $d=1$ is the maximal GDoF value for this setting, even without secrecy constraint.

By following the converse proof in Section VIII-B, we will show that $d_c = 2/3$ is the minimal GDoF of common randomness for achieving the maximal secure GDoF for this asymmetric setting. Specifically, the step in (142) still holds for this asymmetric setting, that is,

$$\mathbb{H}(w_1) \leq \mathbb{H}(w_c) + \mathbb{H}(w_1|w_c, y_2^n) + n\epsilon.$$

From the steps in (133)-(137), in this setting we have

$$\mathbb{H}(w_1|w_c, y_2^n) \leq \frac{n}{2}\log(1 + P^{\alpha_{11}-\alpha_{21}} \cdot \frac{|h_{11}|^2}{|h_{21}|^2}) + n\epsilon_n.$$

Then, the result of (145) in Section VIII-B will be generalized as

$$d^* - (\alpha_{11} - \alpha_{21})^+ \leq d_c^*$$

where d^* is the maximal secure GDoF and d_c^* is the minimal GDoF of common randomness for achieving the maximal secure GDoF d^*. For this example with $\alpha_{11} = 1$ and $\alpha_{21} = 2/3$, and given $d^* = 1$, the above result implies that $d_c^* \geq 1 - (1 - 2/3)^+ = 2/3$. Thus, the proposed scheme is optimal, i.e., it achieves the minimal secure GDoF $d^* = 1$ by using a minimal amount of common randomness, that is, $d_c^* = 2/3$.

Appendix A
Proof of Lemma 1

We here prove Lemma 1. Let us first provide [12, Lemma 1] that will be used in the proof.

Lemma 9. *[12, Lemma 1] Consider a specific channel model $y' = \sqrt{P^{\alpha_1}}h'x' + \sqrt{P^{\alpha_2}}g' + z'$, where $x' \in \Omega(\xi, Q)$, and $z' \sim \mathcal{N}(0, \sigma^2)$. $g' \in \mathcal{S}_{g'}$ is a discrete random variable with a condition*

$$|g'| \leq g_{\max}, \quad \forall g' \in \mathcal{S}_{g'}$$

for $\mathcal{S}_{g'} \subset \mathcal{R}$. h', $g_{\max}$, σ, α_2 and α_1 are finite and positive constants that are independent of P. Also consider the condition $\alpha_1 - \alpha_2 > 0$. Let $\gamma' > 0$ be a finite parameter. If we set Q and ξ by

$$Q = \frac{P^{\frac{\alpha'}{2}}h'\gamma'}{2g_{\max}}, \qquad \xi = \frac{\gamma'}{Q}, \qquad \forall \alpha' \in (0, \alpha_1 - \alpha_2) \quad (159)$$

then the probability of error for decoding x' from y' satisfies

$$Pr(e) \to 0 \quad as \quad P \to \infty.$$

Due to the symmetry, we only focus on the case of $k = 1$. In this setting with $1/2 < \alpha \leq 2/3$, successive decoding method will be used. For the observation y_1 described in (25), it can be expressed in the following form

$$y_1 = \sqrt{P}h_{11}v_{1,c} + \sqrt{P^{\alpha}}g + z_1 \quad (160)$$

where

$$g \triangleq h_{12}(v_{2,c} + u) + \sqrt{P^{1-2\alpha}}h_{11}v_{1,p} + \sqrt{P^{-\alpha}}h_{12}v_{2,p} - \sqrt{P^{2\alpha-2}} \cdot \frac{h_{12}^2 h_{21}}{h_{11}h_{22}}u.$$

One can check that $|g| \leq \frac{14}{\tau \cdot 2^{\tau}}$ holds true for any realization of g. Then, Lemma 9 reveals that the error probability of the estimation of $v_{1,c}$ is

$$\Pr[v_{1,c} \neq \hat{v}_{1,c}] \to 0, \quad \text{as} \quad P \to \infty. \quad (161)$$

After that, $v_{2,c} + u$ can be estimated from the observation below

$$y_1 - \sqrt{P}h_{11}v_{1,c} = \sqrt{P^{\alpha}}h_{12}(v_{2,c} + u) + \sqrt{P^{1-\alpha}}g' + z_1 \quad (162)$$

where $g' \triangleq h_{11}v_{1,p} + \sqrt{P^{\alpha-1}}h_{12}v_{2,p} - \sqrt{P^{4\alpha-3}} \cdot \frac{h_{12}^2 h_{21}}{h_{11}h_{22}}u$. Note that $v_{2,c} + u \in 2\Omega(\xi = \frac{\gamma}{Q}, Q = P^{\frac{2\alpha-1-\epsilon}{2}})$. One can also check that $|g'| \leq \frac{10}{\tau \cdot 2^{\tau}}$. Let $\hat{s}_{vu}$ be an estimate of $s_{vu} \triangleq v_{2,c} + u$. Then, Lemma 9 suggests

$$\Pr[s_{vu} \neq \hat{s}_{vu}] \to 0, \quad \text{as} \quad P \to \infty. \quad (163)$$

Similarly, after decoding $v_{2,c} + u$ we can decode $v_{1,p} \in \Omega(\xi = \frac{\gamma}{Q},\ Q = P^{\frac{1-\alpha-\epsilon}{2}})$ with

$$\Pr[v_{1,p} \neq \hat{v}_{1,p}] \to 0 \quad \text{as} \quad P \to \infty. \quad (164)$$

With results (161) and (164), then we have

$$\Pr[\{v_{1,c} \neq \hat{v}_{1,c}\} \cup \{v_{1,p} \neq \hat{v}_{1,p}\}] \to 0 \quad \text{as} \quad P \to \infty.$$

The case with $k = 2$ is also proved using the same way due the symmetry.

Appendix B
Proof of Lemma 2

We now prove Lemma 2. In the proof we will use the technique of noise removal and signal separation. The distance-outage bounding technique proposed in [45] is used in the proof. In the proof we will also use [12, Lemma 1] (see Lemma 9 in the previous section).

In this proof we will first estimate $v_{1,c}$ and $v_{2,c} + u$ from the observation y_1 expressed in (45) with noise removal and signal separation methods, and then estimate $v_{1,p}$. Note that $v_{1,c} \in \Omega(\xi = \frac{\gamma}{Q},\ Q = P^{\frac{\alpha/2-\epsilon}{2}})$, $v_{2,c} + u \in 2\Omega(\xi = \frac{\gamma}{Q},\ Q = P^{\frac{\alpha/2-\epsilon}{2}})$, and $v_{1,p}, v_{2,p} \in \Omega(\xi = \frac{\gamma}{2Q},\ Q = P^{\frac{1-\alpha-\epsilon}{2}})$, where $2 \cdot \Omega(\xi, Q) \triangleq \{\xi \cdot a :\ a \in \mathcal{Z} \cap [-2Q, 2Q]\}$. For the observation y_1 in (45), it can be expressed as

$$\begin{aligned} y_1 &= \sqrt{P}h_{11}v_{1,c} + \sqrt{P^{\alpha}}h_{12}(v_{2,c} + u) + \tilde{z}_1 \\ &= P^{\frac{\alpha/2+\epsilon}{2}} \cdot \gamma \cdot (\sqrt{P^{1-\alpha}}g_0 q_0 + g_1 q_1) + \tilde{z}_1 \end{aligned} \quad (165)$$

where $\tilde{z}_1 \triangleq \sqrt{P^{1-\alpha}}h_{11}v_{1,p} + \sqrt{P^{(\tau+1)\alpha-\tau}}\delta_{2,\tau}h_{12}u + h_{12}v_{2,p} + z_1$ and

$$g_0 \triangleq h_{11}, \qquad g_1 \triangleq h_{12}, \qquad q_0 \triangleq \frac{Q_{\max}}{\gamma} \cdot v_{1,c}$$

$$q_1 \triangleq \frac{Q_{\max}}{\gamma} \cdot (v_{2,c} + u), \qquad Q_{\max} \triangleq P^{\frac{\alpha/2-\epsilon}{2}}$$

for $\gamma \in \left(0, \frac{1}{\tau \cdot 2^{\tau}}\right]$. It is true that $q_0, q_1 \in \mathcal{Z}$, $|q_1| \leq 2Q_{\max}$ and $|q_0| \leq Q_{\max}$.

Let us consider $\hat{q}_1$ and $\hat{q}_0$ as the corresponding estimates of q_1 and q_0 from y_1 (see (165)). For this estimation we specifically consider an estimator that seeks to minimize

$$|y_1 - P^{\frac{\alpha/2+\epsilon}{2}} \cdot \gamma \cdot (\sqrt{P^{1-\alpha}} g_0 \hat{q}_0 + g_1 \hat{q}_1)|.$$

The minimum distance defined below will be used in the error probability analysis for this estimation

$$d_{\min}(g_0, g_1) \triangleq \min_{\substack{q_0, q_0' \in \mathcal{Z} \cap [-Q_{\max}, Q_{\max}] \\ q_1, q_1' \in \mathcal{Z} \cap [-2Q_{\max}, 2Q_{\max}] \\ (q_0, q_1) \neq (q_0', q_1')}} \Big| \sqrt{P^{1-\alpha}} g_0 (q_0 - q_0') + g_1 (q_1 - q_1') \Big|. \tag{166}$$

Lemma 11 (see below) will reveal that, for almost all channel realizations, this minimum distance is sufficiently large when P is large. In the proof of Lemma 11, we will use a result of [47, Lemma 1] or [48, Lemma 8], which is a generalization of [45, Lemma 14].

Lemma 10. *[48, Lemma 8] or [47, Lemma 1] Let us consider a parameter η such that $\eta > 1$ and $\eta \in \mathcal{Z}^+$, and consider $\beta \in (0, 1]$ and $Q_0, A_0, Q_1, A_1 \in \mathcal{Z}^+$. Also define two events as*

$$\tilde{B}(q_0, q_1) \triangleq \{(g_0, g_1) \in (1, \eta]^2 : |A_1 g_1 q_1 + A_0 g_0 q_0| < \beta\} \tag{167}$$

and

$$\tilde{B} \triangleq \bigcup_{\substack{q_0, q_1 \in \mathcal{Z}: \\ (q_0, q_1) \neq 0, \\ |q_k| \leq Q_k \ \forall k}} \tilde{B}(q_0, q_1). \tag{168}$$

For $\mathcal{L}(\tilde{B})$ denoting the Lebesgue measure of $\tilde{B}$, then this measure is bounded as

$$\mathcal{L}(\tilde{B}) \leq 8\beta(\eta - 1) \min\Big\{ \frac{Q_0 Q_1}{A_1}, \frac{Q_1 Q_0}{A_0}, \frac{Q_0 \eta}{A_1}, \frac{Q_1 \eta}{A_0} \Big\}.$$

Lemma 11. *For $\epsilon > 0$ and $\kappa \in (0, 1]$ and consider the design in* (16)-(18) *and* (42)-(43) *when $\alpha \in [2/3, 1)$. Then the following inequality holds true for the minimum distance $d_{\min}$ defined in* (166)

$$d_{\min} \geq \kappa P^{-\frac{3\alpha/2-1}{2}} \tag{169}$$

for all channel realizations $\{h_{k\ell}\} \in (1, 2]^{2\times 2} \setminus \mathcal{H}_{out}$, where the Lebesgue measure of $\mathcal{H}_{out} \subseteq (1, 2]^{2\times 2}$ satisfies

$$\mathcal{L}(\mathcal{H}_{out}) \leq 64\kappa \cdot P^{-\frac{\epsilon}{2}}. \tag{170}$$

Proof. For this case we set $\eta \triangleq 2$ and define

$$\beta \triangleq \kappa P^{-\frac{3\alpha/2-1}{2}}, \quad A_0 \triangleq \sqrt{P^{1-\alpha}}, \quad A_1 \triangleq 1,$$
$$Q_0 \triangleq 2Q_{\max}, \quad Q_1 \triangleq 4Q_{\max}, \quad Q_{\max} \triangleq P^{\frac{\alpha/2-\epsilon}{2}}.$$

From the previous definitions, $g_0 = h_{11}$ and $g_1 = h_{12}$. Without loss of generality (WLOG) we will consider the case that[5] $A_0, Q_0, A_1, Q_1 \in \mathcal{Z}^+$. Let us define

$$\tilde{B}(q_0, q_1) \triangleq \{(g_0, g_1) \in (1, \eta]^2 : |A_1 g_1 q_1 + A_0 g_0 q_0| < \beta\} \tag{171}$$

and

$$\tilde{B} \triangleq \bigcup_{\substack{q_0, q_1 \in \mathcal{Z}: \\ (q_0, q_1) \neq 0, \\ |q_k| \leq Q_k \ \forall k}} \tilde{B}(q_0, q_1). \tag{172}$$

From Lemma 10, the Lebesgue measure of $\tilde{B}$ can be bounded by

$$\mathcal{L}(\tilde{B}) \leq 8\beta(\eta-1) \min\{\frac{8Q^2_{\max}}{1}, \frac{8Q^2_{\max}}{\sqrt{P^{1-\alpha}}}, \frac{2Q_{\max}\eta}{1}, \frac{4Q_{\max}\eta}{\sqrt{P^{1-\alpha}}}\} \tag{173}$$

$$\begin{aligned}
&= 8\beta(\eta-1) \cdot Q_{\max} \cdot \min\{8Q_{\max}, \frac{8Q_{\max}}{\sqrt{P^{1-\alpha}}}, 2\eta, \frac{4\eta}{\sqrt{P^{1-\alpha}}}\} \\
&\leq 8\beta(\eta-1) \cdot Q_{\max} \cdot P^{\frac{\alpha-1}{2}} \cdot \min\{8Q_{\max}, 4\eta\} \\
&\leq 8\beta(\eta-1) \cdot Q_{\max} \cdot P^{\frac{\alpha-1}{2}} \cdot 4\eta \\
&= 32\beta\eta(\eta-1) \cdot P^{\frac{3\alpha/2-1-\epsilon}{2}} \\
&= 32\eta(\eta-1)\kappa P^{-\frac{\epsilon}{2}} \\
&= 64\kappa P^{-\frac{\epsilon}{2}}.
\end{aligned} \tag{174}$$

Based on the definition in (172), $\tilde{B}$ is a set of (g_0, g_1), where $(g_0, g_1) \in (1, \eta]^2$. For any $(g_0, g_1) \in \tilde{B}$, there exists at least one pair (q_0, q_1) such that $|A_1 g_1 q_1 + A_0 g_0 q_0| < \kappa P^{-\frac{3\alpha/2-1}{2}}$. Thus, $\tilde{B}$ can be treated as the outage set and we have the following conclusion:

$$d_{\min}(g_0, g_1) \geq \kappa P^{-\frac{3\alpha/2-1}{2}}, \quad \text{for} \quad (g_0, g_1) \notin \tilde{B}.$$

Let us now define $\mathcal{H}_{\text{out}}$ as a set of $(h_{22}, h_{21}, h_{12}, h_{11}) \in (1, 2]^{2\times 2}$ such that the corresponding pairs (g_0, g_1) appear in $\tilde{B}$ (outage set), that is,

$$\mathcal{H}_{\text{out}} \triangleq \{(h_{22}, h_{21}, h_{12}, h_{11}) \in (1, 2]^{2\times 2} : (g_0, g_1) \in \tilde{B}\}. \tag{175}$$

[5]Our result also holds true for the scenario when any of the four parameters $\{A_0, Q_0, A_1, Q_1\}$ isn't an integer. It just requires some minor modifications in the proof. Let us consider one example when A_0 isn't an integer. For this example, the parameters A_0 and g_0 can be replaced with $A_0' \triangleq \omega_0 A_0$ and $g_0' \triangleq \frac{1}{\omega_0} g_0$, respectively, where $\omega_0 \triangleq \lceil A_0 \rceil / A_0$. From the definition, ω_0 is bounded, i.e., $1/2 < 1/\omega_0 < 1$, and $A_0' = \omega_0 A_0$ is an integer. Let us consider another example when $Q_0 = 2\sqrt{P^{\alpha/2-\epsilon}}$ isn't an integer. For this example, the parameter ϵ can be slightly modified such that $Q_0 = 2\sqrt{P^{\alpha/2-\epsilon}}$ is an integer and ϵ can still be very small when P is large. Therefore, throughout this work, WLOG we will consider those parameters to be integers, i.e., $A_0, Q_0, A_1, Q_1 \in \mathcal{Z}^+$.

From the relationship between $\tilde{B}$ and $\mathcal{H}_{\text{out}}$, the Lebesgue measure of $\mathcal{H}_{\text{out}}$ can be bounded by

$$\begin{aligned}
&\mathcal{L}(\mathcal{H}_{\text{out}}) \\
=&\int_{h_{22}=1}^{2}\int_{h_{21}=1}^{2}\int_{h_{12}=1}^{2}\int_{h_{11}=1}^{2}\mathbb{1}_{\mathcal{H}_{\text{out}}}(h_{22},h_{21},h_{12},h_{11})dh_{11} \\
&\qquad\cdot dh_{12}dh_{21}dh_{22} \qquad (176)\\
=&\int_{h_{22}=1}^{2}\int_{h_{21}=1}^{2}\int_{h_{12}=1}^{2}\int_{h_{11}=1}^{2}\mathbb{1}_{\tilde{B}}(h_{11},h_{12})dh_{11}dh_{12}dh_{21}dh_{22} \\
\leq&\int_{h_{22}=1}^{2}\int_{h_{21}=1}^{2}\int_{g_1=1}^{\eta}\int_{g_0=1}^{\eta}\mathbb{1}_{\tilde{B}}(g_0,g_1)dg_0dg_1dh_{21}dh_{22} \\
=&\int_{h_{22}=1}^{2}\int_{h_{21}=1}^{2}\mathcal{L}(\tilde{B})dh_{21}dh_{22} \\
\leq&\int_{h_{22}=1}^{2}\int_{h_{21}=1}^{2}64\kappa\cdot P^{-\frac{\epsilon}{2}}dh_{21}dh_{22} \qquad (177)\\
=&64\kappa\cdot P^{-\frac{\epsilon}{2}} \qquad (178)
\end{aligned}$$

where

$$\mathbb{1}_{\mathcal{H}_{\text{out}}}(h_{22},h_{21},h_{12},h_{11})=\begin{cases}1 & \text{if } (h_{22},h_{21},h_{12},h_{11})\in\mathcal{H}_{\text{out}}\\ 0 & \text{if } (h_{22},h_{21},h_{12},h_{11})\notin\mathcal{H}_{\text{out}}\end{cases}$$

and

$$\mathbb{1}_{\tilde{B}}(g_0,g_1)=\begin{cases}1 & \text{if } (g_0,g_1)\in\tilde{B}\\ 0 & \text{if } (g_0,g_1)\notin\tilde{B}\end{cases}$$

and (177) is from (174). □

Lemma 11 suggests that, the minimum distance $d_{\min}$ defined in (166) is sufficiently large for almost all the channel coefficients when P is large. Let us focus on the channel coefficients not in the outage set $\mathcal{H}_{\text{out}}$ and rewrite the observation y_1 in (165) as

$$y_1 = P^{\frac{\alpha/2+\epsilon}{2}}\cdot\gamma\cdot x_s+\sqrt{P^{1-\alpha}}\tilde{g}+z_1 \qquad (181)$$

where $x_s\triangleq\sqrt{P^{1-\alpha}}g_0q_0+g_1q_1$ and $\tilde{g}\triangleq h_{11}v_{1,p}+\sqrt{P^{(\tau+2)\alpha-\tau-1}}\delta_{2,\tau}h_{12}u+\sqrt{P^{\alpha-1}}h_{12}v_{2,p}$. It is true that

$$|\tilde{g}|\leq\tilde{g}_{\max}\triangleq\frac{1}{\tau\cdot2^{\tau-1}}+\frac{2}{\tau},\quad\forall\tilde{g}.$$

For the observation in (181), we will decode x_s by considering other signals as noise (called as noise removal) and then recover q_0 and q_1 from x_s by using the rational independence between g_0 and g_1 (called as signal separation, see [49]). Given the channel coefficients outside the outage set $\mathcal{H}_{\text{out}}$, Lemma 11 suggests that, the minimum distance for x_s satisfies $d_{\min}\geq\kappa P^{-\frac{3\alpha/2-1}{2}}$. With this result, the probability of error for the estimation of x_s from y_1 is bounded by

$$\begin{aligned}
\Pr[x_s\neq\hat{x}_s]\leq&\Pr\Big[|z_1+P^{\frac{1-\alpha}{2}}\tilde{g}|>P^{\frac{\alpha/2+\epsilon}{2}}\cdot\gamma\cdot\frac{d_{\min}}{2}\Big]\\
\leq&2\cdot\mathbf{Q}\big(P^{\frac{\alpha/2+\epsilon}{2}}\cdot\gamma\cdot\frac{d_{\min}}{2}-P^{\frac{1-\alpha}{2}}\tilde{g}_{\max}\big) \qquad (182)\\
\leq&2\cdot\mathbf{Q}\big(P^{\frac{1-\alpha}{2}}(\frac{\gamma\kappa P^{\frac{\epsilon}{2}}}{2}-\frac{1}{\tau\cdot2^{\tau-1}}-\frac{2}{\tau})\big) \qquad (183)
\end{aligned}$$

where $\mathbf{Q}(c)\triangleq\frac{1}{\sqrt{2\pi}}\int_c^\infty\exp(-\frac{u^2}{2})du$ and (182) use the fact that $|\tilde{g}|\leq\tilde{g}_{\max}\triangleq\frac{1}{\tau\cdot2^{\tau-1}}+\frac{2}{\tau},\forall\tilde{g}$; and the last step uses the result of $d_{\min}\geq\kappa P^{-\frac{3\alpha/2-1}{2}}$. From the step in (183), it implies that

$$\Pr[x_s\neq\hat{x}_s]\to0\quad\text{as}\quad P\to\infty. \qquad (184)$$

Note that q_0 and q_1 (and consequently $v_{1,c}$ and $v_{2,c}+u$) can be recovered from x_s due to rational independence.

After decoding x_s we can estimate $v_{1,p}$ from the following observation

$$\begin{aligned}
&y_1-P^{\frac{\alpha/2+\epsilon}{2}}\cdot\gamma\cdot x_s\\
=&\sqrt{P^{1-\alpha}}h_{11}v_{1,p}+\sqrt{P^{(\tau+1)\alpha-\tau}}\delta_{2,\tau}h_{12}u+h_{12}v_{2,p}+z_1.
\end{aligned}$$

Given that $v_{1,p},v_{2,p}\in\Omega(\xi=\frac{\gamma}{2Q},\ Q=P^{\frac{1-\alpha-\epsilon}{2}})$ and $\sqrt{P^{(\tau+1)\alpha-\tau}}\delta_{2,\tau}h_{12}u+h_{12}v_{2,p}\leq\frac{2}{\tau}+\frac{1}{\tau\cdot2^\tau}$, from Lemma 9 we can conclude that the probability of error for the estimation of $v_{1,p}$ satisfies

$$\Pr[\hat{v}_{1,p}\neq v_{1,p}]\to0\quad\text{as}\quad P\to\infty. \qquad (185)$$

With (184) and (185) we can conclude that

$$\Pr[\{v_{1,c}\neq\hat{v}_{1,c}\}\cup\{v_{1,p}\neq\hat{v}_{1,p}\}]\to0\quad\text{as}\quad P\to\infty \qquad (186)$$

for almost all the channel realizations. For the case with $k=2$, it is proved with the same way using the symmetry property.

Appendix C
Proof of Lemma 3

Lemma 3 is proved here. For a MAC-WT channel, the channel input-output relationship can be described as (see (1) and (2))

$$\begin{aligned}
y_1(t)&=\sqrt{P}h_{11}x_1(t)+\sqrt{P^\alpha}h_{12}x_2(t)+z_1(t)\\
y_2(t)&=\sqrt{P^\alpha}h_{21}x_1(t)+\sqrt{P}h_{22}x_2(t)+z_2(t).
\end{aligned} \qquad (187)$$

By interchanging the role of transmitter 1 and transmitter 2 in the MAC-WT channel, the channel input-output relationship can be alternately represented as

$$\begin{aligned}
y_1(t)&=\sqrt{P'^{\alpha'}}h_{12}'x_2'(t)+\sqrt{P'}h_{11}'x_1'(t)+z_1(t)\\
y_2(t)&=\sqrt{P'}h_{22}'x_2'(t)+\sqrt{P'^{\alpha'}}h_{21}'x_1'(t)+z_2(t)
\end{aligned} \qquad (188)$$

where

$$\begin{aligned}
&h_{11}'=h_{12},\quad h_{12}'=h_{11},\quad h_{21}'=h_{22},\quad h_{22}'=h_{21}\\
&x_1'(t)=x_2(t),\quad x_2'(t)=x_1(t),\quad P'=P^\alpha,\quad \alpha'=\frac{1}{\alpha}.
\end{aligned} \qquad (189)$$

Note that the secure capacity region and the secure GDoF region of the MAC-WT channel expressed in (188) are $\bar{C}(P',\alpha')$ and $\bar{\mathcal{D}}(\alpha')$, respectively. Assume a scheme Γ achieves a rate tuple (R_1',R_2',R_c') in the channel expressed in (187), i.e., transmitter 1 achieves a rate $R_1=R_1'$ and transmitter 2 achieves a rate $R_2=R_2'$ by using common randomness rate $R_c=R_c'$. Then the same scheme Γ achieves rates $R_1=R_2',R_2=R_1'$, by using common randomness rate $R_c=R_c'$ in the channel expressed in (188), because the channel expressed in (188) can be reverted back to the channel expressed in (187) by interchanging the role of transmitters.

For any tuple $(d_1^{'}, d_2^{'}, d_c^{'})$ such that $(d_1^{'}, d_2^{'}, d_c^{'}) \in \bar{\mathcal{D}}(\alpha)$ in the channel expressed in (187), there exists a scheme Γ that achieves a rate tuple in the form of

$$\big(R_1 = \frac{d_1^{'}}{2}\log P + o(\log P),\ R_2 = \frac{d_2^{'}}{2}\log P + o(\log P),$$
$$R_c = \frac{d_c^{'}}{2}\log P + o(\log P)\big). \tag{190}$$

Based on the above argument, by interchanging the role of transmitter 1 and transmitter 2 in the channel expressed in (187), the same scheme Γ achieves a rate tuple in the form of

$$\big(R_1 = \frac{d_2^{'}}{2}\log P + o(\log P),\ R_2 = \frac{d_1^{'}}{2}\log P + o(\log P),$$
$$R_c = \frac{d_c^{'}}{2}\log P + o(\log P)\big) \tag{191}$$

in the channel expressed in (188). Then the following GDoF tuple

$$\begin{pmatrix} d_1 \\ d_2 \\ d_c \end{pmatrix} = \begin{pmatrix} \lim\limits_{P^{'}\to\infty} \frac{\frac{d_2^{'}}{2}\log P + o(\log P)}{\frac{1}{2}\log P^{'}} \\ \lim\limits_{P^{'}\to\infty} \frac{\frac{d_1^{'}}{2}\log P + o(\log P)}{\frac{1}{2}\log P^{'}} \\ \lim\limits_{P^{'}\to\infty} \frac{\frac{d_c^{'}}{2}\log P + o(\log P)}{\frac{1}{2}\log P^{'}} \end{pmatrix}$$
$$= \begin{pmatrix} \lim\limits_{P^{'}\to\infty} \frac{\frac{1}{\alpha}\left(\frac{d_2^{'}}{2}\log P^{'} + \alpha o(\frac{\log P^{'}}{\alpha})\right)}{\frac{1}{2}\log P^{'}} \\ \lim\limits_{P^{'}\to\infty} \frac{\frac{1}{\alpha}\left(\frac{d_1^{'}}{2}\log P^{'} + \alpha o(\frac{\log P^{'}}{\alpha})\right)}{\frac{1}{2}\log P^{'}} \\ \lim\limits_{P^{'}\to\infty} \frac{\frac{1}{\alpha}\left(\frac{d_c^{'}}{2}\log P^{'} + \alpha o(\frac{\log P^{'}}{\alpha})\right)}{\frac{1}{2}\log P^{'}} \end{pmatrix}$$
$$= \begin{pmatrix} \frac{1}{\alpha}d_2^{'} \\ \frac{1}{\alpha}d_1^{'} \\ \frac{1}{\alpha}d_c^{'} \end{pmatrix}$$

is achievable in the channel expressed in (188), which implies $\big(\frac{1}{\alpha}d_2^{'}, \frac{1}{\alpha}d_1^{'}, \frac{1}{\alpha}d_c^{'}\big) \in \bar{\mathcal{D}}(\alpha^{'})$. Since $\alpha^{'} = \frac{1}{\alpha}$, then we get

$$\big(\frac{1}{\alpha}d_2^{'}, \frac{1}{\alpha}d_1^{'}, \frac{1}{\alpha}d_c^{'}\big) \in \bar{\mathcal{D}}(\frac{1}{\alpha})$$

which completes the proof.

Appendix D
Proof of Lemma 5

We provide the proof of Lemma 5 in this section for the case of $\frac{2}{3} \le \alpha \le 1$ and $0 \le B \le 2\alpha - 1$. The proof is divided into two sub-cases, i.e., $0 \le B \le 3\alpha - 2$ and $3\alpha - 2 \le B \le 2\alpha - 1$.

A. $0 \le B \le 3\alpha - 2$

For the case of $\frac{2}{3} \le \alpha \le 1$ and $0 \le B \le 3\alpha - 2$, the observation y_1 expressed in (93) can be rewritten in the following form

$$y_1 = \sqrt{P^{1-\alpha}}h_{11}v_{1,p} + \sqrt{P}h_{11}v_{1,c} + \sqrt{P^{2\alpha-1}}\frac{h_{12}h_{21}}{h_{22}}v_{2,c} + z_1$$
$$= 2\gamma\sqrt{P^{\epsilon}}(g_0q_0 + \sqrt{P^{1-\alpha+B}}g_1q_1 + \sqrt{P^{2\alpha-1-B}}g_2q_2) + z_1 \tag{192}$$

where

$$g_0 \triangleq \frac{h_{11}}{4}, \qquad g_1 \triangleq \frac{\eta_{1,c}h_{11}}{2}, \qquad g_2 \triangleq \frac{\eta_{2,c}h_{12}h_{21}}{2h_{22}},$$
$$q_0 \triangleq \frac{2\sqrt{P^{1-\alpha-\epsilon}}}{\gamma}\cdot v_{1,p},\ q_1 \triangleq \frac{\sqrt{P^{\alpha-B-\epsilon}}}{\eta_{1,c}\gamma}\cdot v_{1,c},\ q_2 \triangleq \frac{\sqrt{P^{B-\epsilon}}}{\eta_{2,c}\gamma}\cdot v_{2,c}$$

for $\gamma \in (0, \frac{1}{\tau\cdot 2^{\tau}}]$, $1 \le \eta_{1,c} < 2$, $1 \le \eta_{2,c} < 2$, $v_{1,p} \in \Omega(\xi = \frac{\gamma}{2Q},\ Q = P^{\frac{1-\alpha-\epsilon}{2}})$, $v_{1,c} \in \Omega(\xi = \frac{\eta_{1,c}\gamma}{Q},\ Q = P^{\frac{\alpha-B-\epsilon}{2}})$ and $v_{2,c} \in \Omega(\xi = \frac{\eta_{2,c}\gamma}{Q},\ Q = P^{\frac{B-\epsilon}{2}})$. Based on our definition, it implies that $q_0, q_1, q_2 \in \mathcal{Z}$, $|q_0| \le \sqrt{P^{1-\alpha-\epsilon}}$, $|q_1| \le \sqrt{P^{\alpha-B-\epsilon}}$, and $|q_2| \le \sqrt{P^{B-\epsilon}}$. Let us define the following minimum distance

$$d_{\min}(g_0,g_1,g_2) \triangleq \min_{\substack{q_0,q_0^{'},\in\mathcal{Z}\cap[-\sqrt{P^{1-\alpha-\epsilon}},\sqrt{P^{1-\alpha-\epsilon}}] \\ q_1,q_1^{'},\in\mathcal{Z}\cap[-\sqrt{P^{\alpha-B-\epsilon}},\sqrt{P^{\alpha-B-\epsilon}}] \\ q_2,q_2^{'}\in\mathcal{Z}\cap[-\sqrt{P^{B-\epsilon}},\sqrt{P^{B-\epsilon}}] \\ (q_0,q_1,q_2)\neq(q_0^{'},q_1^{'},q_2^{'})}} \Big| g_0(q_0 - q_0^{'})$$
$$+ \sqrt{P^{1-\alpha+B}}g_1(q_1 - q_1^{'}) + \sqrt{P^{2\alpha-1-B}}g_2(q_2 - q_2^{'})\Big| \tag{193}$$

which will be used for the analysis of the estimation of q_0, q_1 and q_2 from the observation in (192). The lemma below states a result on bounding this minimum distance.

Lemma 12. *Consider the parameters $\kappa \in (0, 1]$ and $\epsilon > 0$, and consider the signal design in Table III,* (80)-(84) *and* (91)-(92) *for the case of $\frac{2}{3} \le \alpha < 1$ and $0 \le B \le 3\alpha - 2$. Then the minimum distance $d_{\min}$ defined in* (193) *satisfies the following inequality*

$$d_{\min} \ge \kappa P^{\frac{\epsilon}{2}} \tag{194}$$

for all the channel coefficients $\{h_{k\ell}\} \in (1, 2]^{2\times 2} \setminus \mathcal{H}_{out}$, where the Lebesgue measure of the outage set $\mathcal{H}_{out} \subseteq (1, 2]^{2\times 2}$ satisfies the following inequality

$$\mathcal{L}(\mathcal{H}_{out}) \le 193536\kappa P^{-\frac{\epsilon}{2}}. \tag{195}$$

Proof. In this case we let

$$\beta \triangleq \kappa P^{\frac{\epsilon}{2}}, \qquad A_1 \triangleq \sqrt{P^{1-\alpha+B}}, \quad A_2 \triangleq \sqrt{P^{2\alpha-1-B}},$$
$$Q_0 \triangleq 2\sqrt{P^{1-\alpha-\epsilon}},\ Q_1 \triangleq 2\sqrt{P^{\alpha-B-\epsilon}},\ Q_2 \triangleq 2\sqrt{P^{B-\epsilon}},$$

for some $\epsilon > 0$, $\kappa \in (0, 1]$, $1 \le \eta_{1,c} < 2$ and $1 \le \eta_{2,c} < 2$. Recall that $g_0 = \frac{h_{11}}{4}$, $g_1 = \frac{\eta_{1,c}h_{11}}{2}$, and $g_2 = \frac{\eta_{2,c}h_{12}h_{21}}{2h_{22}}$. We also define the following two sets

$$B^{\prime}(q_0, q_1, q_2) \triangleq \{(g_0, g_1, g_2) \in (1, 4]^3 : |g_0q_0 + A_1g_1q_1 + A_2g_2q_2| < \beta\}$$

and

$$B^{\prime} \triangleq \bigcup_{\substack{q_0,q_1,q_2\in\mathcal{Z}: \\ (q_0,q_1,q_2)\neq 0, \\ |q_k|\le Q_k\ \forall k}} B^{\prime}(q_0, q_1, q_2). \tag{196}$$

With the result of [45, Lemma 14] we can bound the Lebesgue measure of $B^{\prime}$ as

$$\mathcal{L}(B^{\prime}) \le 504\beta\Big(\frac{2Q_0}{A_2} + \frac{Q_0\tilde{Q}_2}{A_1} + \frac{2Q_0}{A_1} + \frac{Q_0\tilde{Q}_1}{A_2}\Big) \tag{197}$$

where $\tilde{Q}_1 = \min\Big\{Q_1, 8\cdot\frac{\max\{Q_0, A_2Q_2\}}{A_1}\Big\} = 16\sqrt{P^{3\alpha-2-B-\epsilon}}$ and $\tilde{Q}_2 = \min\Big\{Q_2, 8\cdot\frac{\max\{Q_0, A_1Q_1\}}{A_2}\Big\} = 2\sqrt{P^{B-\epsilon}}$. By

plugging the values of the parameters into (197), we can easily bound $\mathcal{L}(B')$ as

$$\mathcal{L}(B') \leq 24192\kappa P^{-\frac{\epsilon}{2}}. \tag{198}$$

With our definition, B' is a collection of (g_0, g_1, g_2) and can be treated as an outage set. Let us define $\mathcal{H}_{\text{out}} \triangleq \{(h_{22}, h_{21}, h_{12}, h_{11}) \in (1,2]^{2\times 2} : (g_0, g_1, g_2) \in B'\}$ as a set of $(h_{22}, h_{21}, h_{12}, h_{11}) \in (1,2]^{2\times 2}$ such that the corresponding pairs (g_0, g_1) are in the outage set B'. Let us also define the indicator function $\mathbb{1}_{\mathcal{H}_{\text{out}}}(h_{22}, h_{21}, h_{12}, h_{11}) = 1$ if $(h_{22}, h_{21}, h_{12}, h_{11}) \in \mathcal{H}_{\text{out}}$, else $\mathbb{1}_{\mathcal{H}_{\text{out}}}(h_{22}, h_{21}, h_{12}, h_{11}) = 0$; and define another indicator function $\mathbb{1}_{B'}(g_1, g_2) = 1$ if $(g_0 = \frac{g_1}{2\eta_{1,c}}, g_1, g_2) \in B'$, else $\mathbb{1}_{B'}(g_1, g_2) = 0$. Then by following the steps in (176)-(178), the Lebesgue measure of $\mathcal{H}_{\text{out}}$ can be bounded as

$$\mathcal{L}(\mathcal{H}_{\text{out}}) \leq 193536\kappa P^{-\frac{\epsilon}{2}}. \tag{199}$$

□

Lemma 12 suggests that, the minimum distance $d_{\min}$ defined in (193) is sufficiently large, i.e., $d_{\min} \geq \kappa P^{\frac{\epsilon}{2}}$, for almost all the channel coefficients when P is large. Let us focus on the channel coefficients not in the outage set $\mathcal{H}_{\text{out}}$. Let $x_s \triangleq g_0 q_0 + \sqrt{P^{1-\alpha+B}} g_1 q_1 + \sqrt{P^{2\alpha-1-B}} g_2 q_2$. Then it is easy to show that the error probability for the estimation of x_s from the observation in (192) is

$$\Pr[x_s \neq \hat{x}_s] \to 0 \quad \text{as} \quad P \to \infty. \tag{200}$$

Note that q_0, q_1, q_2 can be recovered due to the fact that g_0, g_1, g_2 are rationally independent. At this point we can conclude that

$$\Pr[\{v_{1,c} \neq \hat{v}_{1,c}\} \cup \{v_{1,p} \neq \hat{v}_{1,p}\} \cup \{v_{2,c} \neq \hat{v}_{2,c}\}] \to 0 \text{ as } P \to \infty \tag{201}$$

for almost all the channel coefficients.

B. $3\alpha - 2 \leq B \leq 2\alpha - 1$

For this case with $\frac{2}{3} \leq \alpha \leq 1$ and $3\alpha - 2 \leq B \leq 2\alpha - 1$, the proof is similar to that of Lemma 4. We will just provide the outline of the proof in order to avoid the repetition. In this case, we will first estimate $v_{1,c}$ from y_1 expressed in (93) based on successive decoding method, and then we will estimate $v_{2,c}$ and $v_{1,p}$ simultaneously based on noise removal and signal separation methods.

In the first step, we rewrite y_1 from (93) to the following form

$$y_1 = \sqrt{P} h_{11} v_{1,c} + \sqrt{P^{2\alpha-1}} \bar{g} + z_1. \tag{202}$$

where $\bar{g} \triangleq \frac{h_{12}h_{21}}{h_{22}} v_{2,c} + \sqrt{P^{2-3\alpha}} h_{11} v_{1,p}$. Since $\bar{g}$ is bounded, i.e., $|\bar{g}| \leq \frac{9}{\tau \cdot 2^{\tau}}$, from Lemma 9 we can conclude that $v_{1,c}$ can be estimated from y_1 with vanishing error probability:

$$\Pr[v_{1,c} \neq \hat{v}_{1,c}] \to 0, \quad \text{as} \quad P \to \infty. \tag{203}$$

In the second step $v_{2,c}$ and $v_{1,p}$ will be estimated simultaneously from the following observation

$$\begin{aligned} y_1 - \sqrt{P} h_{11} v_{1,c} &= \sqrt{P^{2\alpha-1}} \frac{h_{12}h_{21}}{h_{22}} v_{2,c} + \sqrt{P^{1-\alpha}} h_{11} v_{1,p} + z_1 \\ &= \gamma(A_0 g_0 q_0 + A_1 g_1 q_1) + z_1 \end{aligned} \tag{204}$$

where $g_0 \triangleq \frac{\eta_{2,c} h_{12} h_{21}}{h_{22}}$, $g_1 \triangleq \frac{1}{2} h_{11}$, $A_0 \triangleq \sqrt{P^{2\alpha-1-B+\epsilon}}$, $A_1 \triangleq \sqrt{P^{2-3\alpha+B+\epsilon}}$, $q_0 \triangleq \frac{\sqrt{P^{B-\epsilon}}}{\eta_{2,c}\gamma} v_{2,c}$, $q_1 \triangleq \frac{2\sqrt{P^{2\alpha-1-B-\epsilon}}}{\gamma} v_{1,p}$. By following the steps in (165)-(184), one can show that the $v_{2,c}$ and $v_{1,p}$ can be estimated simultaneously from the observation in (204) with vanishing error probability for almost all the channel coefficients. At this point, we can conclude that

$$\Pr[\{v_{1,c} \neq \hat{v}_{1,c}\} \cup \{v_{1,p} \neq \hat{v}_{1,p}\} \cup \{v_{2,c} \neq \hat{v}_{2,c}\}] \to 0 \text{ as } P \to \infty \tag{205}$$

for almost all the channel coefficients.

APPENDIX E
ADDING COMMON RANDOMNESS WILL NOT INCREASE THE GDOF IN THE CONSIDERED SETTINGS

In this section we will prove that adding common randomness at the transmitters will not increase the sum GDoF, GDoF, and GDoF region, of a two-user interference channel, a point-to-point channel with a helper, and a two-user multiple access channel, respectively, as described in the following lemmas. The three settings are simply the enhanced settings of that defined in Section II by removing the secrecy constraints. Since secrecy constraints will not enlarge the GDoF or GDoF region of the networks, the converse derived for the setting without secrecy constraints will server as a converse for the setting with secrecy constraints.

Lemma 13 (IC-SC)**.** *For a two-user symmetric Gaussian interference channel with common randomness at the transmitters (the enhanced setting of that defined in Section II by removing secrecy constraints), the sum GDoF is upper bounded by*

$$d_1 + d_2 \leq d^*_{sum}(\alpha)$$

where $d^*_{sum}(\alpha)$ is characterized in Theorem 1.

Lemma 14 (WTH)**.** *For a point-to-point Gaussian channel with a helper and with common randomness at the transmitters (the enhanced setting of that defined in Section II-B by removing secrecy constraint), the GDoF is upper bounded by*

$$d(\alpha) \leq 1, \quad \forall \alpha \in [0, \infty).$$

Lemma 15 (MAC-WT)**.** *For a two-user symmetric Gaussian multiple access channel with common randomness at the transmitters (the enhanced setting of that defined in Section II-C by removing secrecy constraint), the optimal GDoF region is outer bounded by*

$$d_1 + d_2 \leq \max\{1, \alpha\}, \quad d_1 \leq 1, \quad d_2 \leq \alpha.$$

The proofs of the above three lemmas are proved in the following sections.

A. Proof of Lemma 13

Let us now prove Lemma 13, focusing on the two-user symmetric Gaussian interference channel with common randomness at the transmitters. At first we will follow the footsteps of the converse proof in [26], by taking the additional consideration of the common randomness at the transmitters.

We will consider the genie-aided channel where a genie provides s_{21}^n and w_c to receiver 1, and provides s_{12}^n and w_c to receiver 2, where $s_{21}(t) \triangleq \sqrt{P^{\alpha_{21}}} h_{21} x_1(t) + z_2(t)$ and $s_{12}(t) \triangleq \sqrt{P^{\alpha_{12}}} h_{12} x_2(t) + z_1(t)$. For this genie-aided channel, the sum rate is upper bounded by

$$\begin{aligned}
&nR_1 + nR_2 - n\epsilon_n \\
\le& \mathbb{I}(w_1; y_1^n, s_{21}^n, w_c) + \mathbb{I}(w_2; y_2^n, s_{12}^n, w_c) \\
=& \mathbb{I}(w_1; y_1^n, s_{21}^n | w_c) + \mathbb{I}(w_2; y_2^n, s_{12}^n | w_c) \qquad (206) \\
=& \mathbb{I}(w_1; s_{21}^n | w_c) + \mathbb{I}(w_1; y_1^n | s_{21}^n, w_c) \\
&+ \mathbb{I}(w_2; s_{12}^n | w_c) + \mathbb{I}(w_2; y_2^n | s_{12}^n, w_c) \\
=& \mathrm{h}(s_{21}^n|w_c) - \mathrm{h}(s_{21}^n|w_1, w_c) + \mathrm{h}(y_1^n|s_{21}^n, w_c) - \mathrm{h}(y_1^n|s_{21}^n, w_1, w_c) \\
&+ \mathrm{h}(s_{12}^n|w_c) - \mathrm{h}(s_{12}^n|w_2, w_c) + \mathrm{h}(y_2^n|s_{12}^n, w_c) - \mathrm{h}(y_2^n|s_{12}^n, w_2, w_c) \\
=& \mathrm{h}(s_{21}^n|w_c) - \mathrm{h}(z_2^n) + \mathrm{h}(y_1^n|s_{21}^n, w_c) - \mathrm{h}(s_{12}^n|w_c) + \mathrm{h}(s_{12}^n|w_c) \\
&- \mathrm{h}(z_1^n) + \mathrm{h}(y_2^n|s_{12}^n, w_c) - \mathrm{h}(s_{21}^n|w_c) \qquad (207) \\
\le& \sum_{t=1}^{n} \big(\mathrm{h}(y_1(t)|s_{21}(t), w_c) + \mathrm{h}(y_2(t)|s_{12}(t), w_c) \big) - \mathrm{h}(z_1^n) - \mathrm{h}(z_2^n) \qquad (208)
\end{aligned}$$

where (206) uses the fact that w_1, w_2 and w_c are mutually independent; (207) follows from the fact that, (s_{21}^n, w_1) and (s_{12}^n, w_2) are conditionally independent given w_c; note that x_i^n is a deterministic function of (w_c, w_i) for $i = 1, 2$. For the term $\mathrm{h}(y_1(t)|s_{21}(t), w_c)$ in (208), we have

$$\begin{aligned}
&\mathrm{h}(y_1(t)|s_{21}(t), w_c) \\
=& \mathbb{E}_{w_c}[\mathrm{h}(y_1(t)|s_{21}(t), w_c = \mathrm{w_c})] \\
\le& \frac{1}{2}\log(2\pi e) + \mathbb{E}_{w_c}\big[\frac{1}{2}\log(\mathbb{E}[\mathrm{var}[y_1(t)|s_{21}(t), w_c = \mathrm{w_c}]])\big] \qquad (209) \\
\le& \frac{1}{2}\log(2\pi e) + \mathbb{E}_{w_c}\Big[\frac{1}{2}\log\big(\mathbb{E}[|y_1(t)|^2|w_c = \mathrm{w_c}] \\
&- \frac{|\mathbb{E}[y_1(t)s_{21}(t)|w_c = \mathrm{w_c}]|^2}{\mathbb{E}[|s_{21}(t)|^2|w_c = \mathrm{w_c}]}\big)\Big] \qquad (210) \\
\le& \frac{1}{2}\log(2\pi e) + \frac{1}{2}\log\Big(1 + P^{\alpha_{12}}|h_{12}|^2\mathbb{E}[|x_2(t)|^2|] \\
&+ \frac{P^{\alpha_{11}}|h_{11}|^2 \cdot \mathbb{E}[|x_1(t)|^2|]}{1 + P^{\alpha_{21}}|h_{21}|^2 \cdot \mathbb{E}[|x_1(t)|^2|]}\Big) \qquad (211) \\
\le& \frac{1}{2}\log(2\pi e) + \frac{1}{2}\log\Big(1 + P^{\alpha_{12}}|h_{12}|^2 + \frac{P^{\alpha_{11}}|h_{11}|^2}{1 + P^{\alpha_{21}}|h_{21}|^2}\Big) \qquad (212)
\end{aligned}$$

where (209) follows from the fact that Gaussian input maximizes the conditional differential entropy for a given variance constraint $\mathbb{E}[\mathrm{var}[y_1(t)|s_{21}(t), w_c = \mathrm{w_c}]]$; (210) uses the result that $\mathbb{E}[\mathrm{var}[y|x]] \le \mathbb{E}|y|^2 - \frac{|\mathbb{E}[xy]|^2}{\mathbb{E}[|x|^2]}$ (cf. [50, Lemma 1]); (211) applies Jensen's inequality to the concave functions of $f_1(x) = \log(1+x)$ and $f_2(x) = \frac{ax}{1+bx}$ for $a > 0, b > 0$ and $x \ge 0$; (212) uses the identity that the function $f_3(x, y) = \log(1+cx+\frac{ay}{1+by})$ is increasing with x and y for $a > 0, b > 0, c > 0$. Similarly, we have

$$\begin{aligned}
&\mathrm{h}(y_2(t)|s_{12}(t), w_c) \\
\le& \frac{1}{2}\log(2\pi e) + \frac{1}{2}\log(1 + P^{\alpha_{21}}|h_{21}|^2 + \frac{P^{\alpha_{22}}|h_{22}|^2}{1 + P^{\alpha_{12}}|h_{12}|^2}). \qquad (213)
\end{aligned}$$

By inserting (212) and (213) into (208), and dividing each side of (208) with $\frac{n}{2}\log P$ and letting $P, n \to \infty$, it gives the sum GDoF bound $d_1 + d_2 \le \max\{\alpha_{12}, \alpha_{11} - \alpha_{21}\} + \max\{\alpha_{21}, \alpha_{22} - \alpha_{12}\}$. By focusing on the symmetric case with $(\alpha_{11} = \alpha_{22} = 1, \alpha_{12} = \alpha_{21} = \alpha)$, we have

$$d_1 + d_2 \le 2\max\{\alpha, 1 - \alpha\}. \qquad (214)$$

The above bound is derived by following the footsteps of the converse proof in [26], and by adapting the common randomness w_c term into the derivations.

We can also derive a bound on the sum GDoF by considering the one-sided interference channel where a genie provides w_2 and w_c to receiver 1 and provides w_c to receiver 2. In this one-sided interference channel, by following the footsteps of the converse proof in [51] (or [26]), one can prove that

$$d_1 + d_2 \le 2(1 - \alpha/2) \quad \text{for} \quad \alpha \le 1. \qquad (215)$$

For the one-sided interference channel, by following the footsteps of the converse proof in [52], one can also prove that

$$d_1 + d_2 \le \alpha \quad \text{for} \quad \alpha \ge 1. \qquad (216)$$

Finally, the bounds $d_1 \le \alpha_{11}$ and $d_2 \le \alpha_{22}$ can be easily proved (see next subsection for the similar proof). These two bounds give the sum GDoF bound for the symmetric case: $d_1 + d_2 \le 2$, which, together with (214), (215) and (216), complete the proof of Lemma 13.

B. Proof of Lemma 14

The proof of Lemma 14 is straightforward. For a point-to-point Gaussian channel with a helper and with common randomness at the transmitters, we enhance the setting by providing an information w_c to the receiver. Then, the rate is bounded as

$$\begin{aligned}
&nR_1 - n\epsilon_{1,n} \\
\le& \mathbb{I}(w_1; y_1^n, w_c) \\
=& \mathbb{I}(w_1; y_1^n | w_c) \qquad (217) \\
\le& \sum_t \mathrm{h}(y_1(t)|w_c) - \mathrm{h}(y_1^n|w_c, w_1) \\
=& \sum_t \mathrm{h}(\sqrt{P^{\alpha_{11}}} h_{11} x_1(t) + z_1(t)|w_c) - \mathrm{h}(z_1^n) \qquad (218) \\
\le& \sum_t \mathrm{h}(\sqrt{P^{\alpha_{11}}} h_{11} x_1(t) + z_1(t)) - \mathrm{h}(z_1^n) \\
\le& \frac{n}{2}\log(1 + P^{\alpha_{11}}|h_{11}|^2) \qquad (219)
\end{aligned}$$

where (217) uses the independence between w_1 and w_c; (218) uses the definition that $x_2(t)$ is a deterministic function of w_c; (219) follows from the fact that Gaussian input maximizes the differential entropy. From (219) it implies that $d \le \alpha_{11}$, which completes the proof of Lemma 14 by focusing on the case with $\alpha_{11} = 1$ and $\alpha_{12} = \alpha$.

C. Proof of Lemma 15

Let us now consider the two-user symmetric Gaussian multiple access channel with common randomness at the transmitters. From the proof in the previous subsection, one

can easily prove the $d_1 \leq \alpha_{11}$ and $d_2 \leq \alpha_{12}$. In this setting, the sum rate can be bounded as

$$\begin{aligned} & nR_1 + nR_2 - n\epsilon_n \\ \leq & \mathbb{I}(w_1, w_2; y_1^n) \\ \leq & \sum_t \mathrm{h}(y_1(t)) - \mathrm{h}(y_1^n | w_1, w_2, x_1^n, x_2^n) \\ = & \sum_t \mathrm{h}(y_1(t)) - \mathrm{h}(z_1^n) \\ \leq & \frac{n}{2} \log(1 + P^{\alpha_{11}} |h_{11}|^2 + P^{\alpha_{12}} |h_{12}|^2) \end{aligned} \tag{220}$$

where (220) follows from the fact that Gaussian input maximizes the differential entropy. The result in (220) gives the sum GDoF bound as $d_1 + d_2 \leq \max\{\alpha_{11}, \alpha_{12}\}$. At this point, we complete the proof of Lemma 15 by focusing on the case with $(\alpha_{11} = 1, \alpha_{12} = \alpha)$.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1378, Jan. 1975.

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

[4] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdu, "Capacity of cognitive interference channels with and without secrecy," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 604–619, Feb. 2009.

[5] 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.

[6] X. He, A. Khisti, and A. Yener, "MIMO multiple access channel with an arbitrarily varying eavesdropper: Secrecy degrees of freedom," *IEEE Trans. Inf. Theory*, vol. 59, no. 8, pp. 4733–4745, Aug. 2013.

[7] J. Xie and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3359–3378, Jun. 2014.

[8] ——, "Secure degrees of freedom of K-user Gaussian interference channels: A unified view," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2647–2661, May 2015.

[9] C. Geng, R. Tandon, and S. A. Jafar, "On the symmetric 2-user deterministic interference channel with confidential messages," in *Proc. IEEE Global Conf. Communications (GLOBECOM)*, Dec. 2015.

[10] 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.

[11] P. Mukherjee and S. Ulukus, "MIMO one hop networks with no eve CSIT," in *Proc. Allerton Conf. Communication, Control and Computing*, Sep. 2016.

[12] J. Chen, "Secure communication over interference channel: To jam or not to jam?" *IEEE Trans. Inf. Theory*, vol. 66, no. 5, pp. 2819–2841, May 2020.

[13] R. D. Yates, D. Tse, and Z. Li, "Secret communication on interference channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2008.

[14] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215–4227, Sep. 2010.

[15] R. Liu, Y. Liang, and H. V. Poor, "Fading cognitive multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4992–5005, Aug. 2011.

[16] C. Geng and S. A. Jafar, "Secure GDoF of K-user Gaussian interference channels: When secrecy incurs no penalty," *IEEE Communications Letters*, vol. 19, no. 8, pp. 1287–1290, Aug. 2015.

[17] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[18] S. Karmakar and A. Ghosh, "Approximate secrecy capacity region of an asymmetric MAC wiretap channel within 1/2 bits," in *IEEE 14th Canadian Workshop on Information Theory*, Jul. 2015.

[19] J. Chen and C. Geng, "Optimal secure GDoF of symmetric Gaussian wiretap channel with a helper," to appear in *IEEE Trans. Inf. Theory*, 2020.

[20] P. Babaheidarian, S. Salimi, and P. Papadimitratos, "Finite-SNR regime analysis of the Gaussian wiretap multiple-access channel," in *Proc. Allerton Conf. Communication, Control and Computing*, Sep. 2015.

[21] Z. Li, R. D. Yates, and W. Trappe, "Secrecy capacity region of a class of one-sided interference channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2008.

[22] Y. Liang and H. V. Poor, "Multiple access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[23] R. Fritschek and G. Wunder, "Towards a constant-gap sum-capacity result for the Gaussian wiretap channel with a helper," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2016, pp. 2978–2982.

[24] P. Mukherjee, J. Xie, and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks with no eavesdropper CSIT," *IEEE Trans. Inf. Theory*, vol. 63, no. 3, pp. 1898–1922, Mar. 2017.

[25] Z. Wang, R. Schaefer, M. Skoglund, M. Xiao, and H. V. Poor, "Strong secrecy for interference channels based on channel resolvability," *IEEE Trans. Inf. Theory*, vol. 64, no. 7, pp. 5110–5130, Jul. 2018.

[26] 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.

[27] A. Wyner, "The common information of two dependent random variables," *IEEE Trans. Inf. Theory*, vol. 21, no. 2, pp. 163–179, Mar. 1975.

[28] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[29] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. I. secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[30] ——, "Common randomness in information theory and cryptography. II. CR capacity," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 225–240, Jan. 1998.

[31] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 344–366, Mar. 2000.

[32] S. Venkatesan and V. Anantharam, "The common randomness capacity of a network of discrete memoryless channels," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 367–387, Mar. 2000.

[33] I. Csiszar and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.

[34] L. Zhao and Y. Chia, "The efficiency of common randomness generation," in *Proc. Allerton Conf. Communication, Control and Computing*, Sep. 2011.

[35] H. Tyagi, "Common information and secret key capacity," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5627–5640, Sep. 2013.

[36] C. Zenger, M. Chur, J. Posielek, C. Paar, and G. Wunder, "A novel key generating architecture for wireless low-resource devices," in *International Workshop on Secure Internet of Things*, Mar. 2014.

[37] K. Krentz and G. Wunder, "6doku: Towards secure over-the-air preloading of 6LoWPAN nodes using PHY key generation," in *Smart SysTech 2015; European Conference on Smart Objects, Systems and Technologies*, Jul. 2015.

[38] J. Liu, P. Cuff, and S. Verdú, "Secret key generation with one communicator and a one-shot converse via hypercontractivity," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2015.

[39] ——, "Secret key generation with limited interaction," *IEEE Trans. Inf. Theory*, vol. 63, no. 11, pp. 7358–7381, Nov. 2017.

[40] R. Fritschek and G. Wunder, "On full-duplex secure key generation with deterministic models," in *IEEE Conference on Communications and Network Security (CNS)*, Oct. 2017.

[41] ——, "On-the-fly secure key generation with deterministic models," in *Proc. IEEE Int. Conf. Communications (ICC)*, May 2017.

[42] B. Ghazi and T. Jayram, "Resource-efficient common randomness and secret-key schemes," in *ACM-SIAM Symposium on Discrete Algorithms (SODA)*, Jan. 2018.

[43] M. Bafna, B. Ghazi, N. Golowich, and M. Sudan, "Communication-rounds tradeoffs for common randomness and secret key generation," in *ACM-SIAM Symposium on Discrete Algorithms (SODA)*, Jan. 2019.

[44] T. Cover and J. Thomas, *Elements of Information Theory*, 2nd ed. New York: Wiley-Interscience, 2006.

[45] U. Niesen and M. A. Maddah-Ali, "Interference alignment: From degrees of freedom to constant-gap capacity approximations," *IEEE Trans. Inf. Theory*, vol. 59, no. 8, pp. 4855–4888, Aug. 2013.

[46] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "On the secure degrees-of-freedom of the multiple-access-channel," Mar. 2010, *arXiv:1003.0729.* [Online]. Available: https://arxiv.org/abs/1003.0729
[47] J. Chen and F. Li, "Adding a helper can totally remove the secrecy constraints in two-user interference channel," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 12, pp. 3126–3139, Dec. 2019.
[48] R. Fritschek and G. Wunder, "On multiuser gain and the constant-gap sum capacity of the Gaussian interfering multiple access channel," May 2017, *arXiv:1705.04514.* [Online]. Available: https://arxiv.org/abs/1705.04514
[49] A. S. Motahari, S. O. Gharan, M. A. Maddah-Ali, and A. K. Khandani, "Real interference alignment: Exploiting the potential of single antenna systems," *IEEE Trans. Inf. Theory*, vol. 60, no. 8, pp. 4799–4810, Aug. 2014.
[50] A. Host-Madsen and A. Nosratinia, "The multiplexing gain of wireless networks," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Sep. 2005.
[51] I. Sason, "On achievable rate regions for the Gaussian interference channel," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1345–1356, Jun. 2004.
[52] M. H. M. Costa, "On the Gaussian interference channel," *IEEE Trans. Inf. Theory*, vol. 31, no. 5, pp. 607–615, Sep. 1985.

Fan Li is currently pursuing the Ph.D. degree with the Electrical Engineering Department of Louisiana Tech University. She received the B.Sc. degree from Shandong Technology and Business University in 2012, and the M.Sc. degree from University of Shanghai for Science and Technology in 2015. Her research interests include information theory, distributed consensus, and machine learning.

Jinyuan Chen is an assistant professor in the Electrical Engineering Department at Louisiana Tech University. Before joining Louisiana Tech, he was a postdoctoral scholar at Stanford University from 2014 to 2016. He received the B.Sc. degree from Tianjin University in 2007, the M.Sc. degree from Beijing University of Posts and Telecommunications in 2010, and the Ph.D. degree from Télécom ParisTech in 2014. His research interests include information theory, distributed consensus, blockchain, and machine learning.