Secure Communications with Limited Common Randomness at Transmitters

Fan Li and Jinyuan Chen

***Abstract*—In this work we consider common randomness-aided secure communications, where a limited common randomness is available at the transmitters. Specifically, we focus on a two-user interference channel with secrecy constraints and a wiretap channel with a helper, in the presence of a limited common randomness shared between the transmitters. For both settings, we characterize the optimal secure sum degrees-of-freedom (DoF) or secure DoF as a function of the DoF of common randomness. The results reveal that the secure sum DoF or secure DoF increases as the DoF of common randomness increases, bridging the gap between the extreme DoF point without common randomness and the other extreme DoF point with unlimited common randomness. The proposed scheme is a two-layer coding scheme, in which two sub-schemes are designed in two layers respectively, i.e., at two different power levels, utilizing common randomness in the first layer only. The role of common randomness is to jam partial information signal at the eavesdroppers, without causing interference at the legitimate receivers. To prove the optimality of the proposed scheme, a new converse is also derived in this work.**

I. Introduction

Since Shannon's seminal work "Communication Theory of Secrecy Systems" in 1949 [1], information-theoretic secrecy has been broadly studied in various communication channels, such as wiretap channels [2]–[11], broadcast channels [12]–[17], and other multiuser channels [12], [18]–[48]. In the pioneer work by Wyner in 1975 [2], the notion of secure capacity was introduced via a wiretap channel, where a transmitter seeks to send a message to the legitimate receiver reliably and securely, in the presence of an eavesdropper. For the wiretap channel, it is well known that the secrecy capacity is

$$C = \max[\mathrm{I}(v; y_1) - \mathrm{I}(v; y_2)]$$

(see, e.g., [3]), where the maximum is computed over the auxiliary variable v, the transmitted signal x and the received signals y_1 and y_2 at the legitimate receiver and eavesdropper, respectively, such that $v \to x \to (y_1, y_2)$ forms a Markov chain. This secure capacity can be interpreted as the difference between the capacities of the legitimate channel and the eavesdropping channel, which implies that *secrecy constraint incurs a capacity penalty*. This observation, i.e., secrecy constraint incurs a capacity penalty, has also been revealed later in some other channels (see, e.g., [12], [25], [27], [31], [33], [36]–[38]).

Recently the work in [49] showed an interesting observation that, adding common randomness (CR) at the transmitters can totally remove the penalty in degrees-of-freedom (DoF), as well as in generalized DoF (GDoF), incurred by the secrecy constraints in some communication networks, where DoF is a prelog factor of capacity at the high signal-to-noise ratio (SNR) regime. For example, in a two-user interference channel without secrecy constraints, the maximal sum DoF is 1. With secrecy constraints, the maximal secure sum DoF of the two-user interference channel is $2/3$, which implies that $1/3$ DoF penalty is incurred due to the secrecy constraints. The work in [49] showed that adding $1/2$ DoF of common randomness at the transmitters can achieve 1 secure sum DoF, in the two-user interference channel. As we can see, adding a sufficient amount of common randomness at the transmitters can totally remove the DoF penalty incurred by the secrecy constraints.

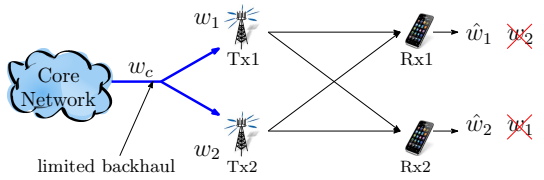

Fig. 1. One example of sharing common randomness in cellular networks, where w_c is the common randomness shared between the transmitters with limited backhaul cable.

This work generalizes the CR-aided secure communications studied in [49], by focusing on the settings with limited common randomness. In the communication systems, sharing common randomness between the transmitters might incur a consumption in resource that is usually limited. For example, in the cellular network, the base stations can share the common randomness with backhaul cable but the rate of backhaul cable is usually limited (see Fig. 1). Given the above motivation, in this work we consider a two-user interference channel with secrecy constraints and a wiretap channel with a helper, in the presence of a limited common randomness.

For the two settings considered here with a limited DoF of common randomness, we characterize the optimal secure sum DoF or secure DoF. Specifically, for the two-user interference channel with secrecy constraints, we show that the optimal secure sum DoF is characterized as $\frac{2\min\{d_c,1/2\}+2}{3}$, where d_c is the DoF of common randomness available at the transmitters. This result reveals that the DoF penalty incurred by the secrecy constraints, i.e., $1-\frac{2\min\{d_c,1/2\}+2}{3}$, decreases as the DoF of common randomness increases, and the DoF penalty is totally removed when the DoF of common randomness reaches the value of $1/2$, matching the result in [49] at a specific point of $d_c = 1/2$. Similar conclusion is also derived in the wiretap channel with a helper and with a limited common randomness.

In this work, the proposed scheme is a two-layer coding

Fan Li and Jinyuan Chen are with Louisiana Tech University, Department of Electrical Engineering, Ruston, USA (emails: fli005@latech.edu, jinyuan@latech.edu).

scheme, in which two sub-schemes are designed respectively in two layers, i.e., at two different power levels. Specifically, the sub-scheme in the first layer is designed by using $\min\{d_c, 1/2\}$ DoF of common randomness. For the sub-scheme in the second layer, however, it is designed without using common randomness. The role of the limited common randomness is to jam partial information signal at the eavesdroppers, without causing interference at the legitimate receivers. To prove the optimality of the proposed scheme, a new converse is also derived in this work.

In this work, system models are detailed in Section II, and the results are presented in Section III. The converse proofs are provided in Sections VI and VII, while the achievability proofs are provided in Sections IV and V. The conclusion is drawn in Section VIII. In this work, $\mathrm{H}(\bullet)$, $\mathrm{h}(\bullet)$ and $\mathrm{I}(\bullet)$ denote the entropy, differential entropy and mutual information, respectively. $\mathcal{Z}$ and $\mathcal{R}$ denote the sets of integers and real numbers, respectively. The notation of $f(a) = o(g(a))$ is defined such that $\lim_{a\to\infty} f(a)/g(a) = 0$.

II. The System Models

We consider a two-user interference channel with secrecy constraints and a wiretap channel with a helper (see Fig. 2). The two settings have a common channel input-output relationship

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

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

for $t = 1, 2, 3, \cdots, n$, where $x_k(t)$ is the transmitted signal of transmitter k at time t, with a normalized power constraint $\mathbb{E}|x_k(t)|^2 \leq 1$; $y_k(t)$ represents the received signal of receiver k; $z_k(t) \sim \mathcal{N}(0,1)$ is the additive white Gaussian noise; and $h_{k\ell}$ represents the channel coefficient between receiver k and transmitter ℓ, for $k, \ell \in \{1, 2\}$. It is assumed that the channel coefficients $\{h_{k\ell}\}_{k,\ell}$ are drawn independently and identically from a continuous distribution, and the absolute value of each channel coefficient is bounded between a finite maximum value and a nonzero minimum value. All the channel coefficients are assumed to be perfectly known to all the nodes. The two settings considered here are slightly different. More details of the two settings are provided in the following subsections.

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

In the interference channel, a confidential message w_ℓ is sent from transmitter ℓ to receiver ℓ, where w_ℓ is independently and uniformly chosen from a set $\mathcal{W}_\ell \triangleq \{1, 2, \cdots, 2^{nR_\ell}\}$, for $\ell \in \{1, 2\}$. At transmitter ℓ, a function

$$f_\ell : \mathcal{W}_\ell \times \mathcal{W}_c \times \mathcal{W}_{\ell,p} \to \mathcal{R}^n \quad (3)$$

is used to map $w_\ell \in \mathcal{W}_\ell$ to the signal $x_\ell^n = f_\ell(w_\ell, w_c, w_{\ell,p}) \in \mathcal{R}^n$, where $w_c \in \mathcal{W}_c$ denotes the *common randomness* that is available at both transmitters but not at the receivers, and $w_{\ell,p} \in \mathcal{W}_{\ell,p}$ represents the *private randomness* that is available at transmitter ℓ only, for $\ell \in \{1, 2\}$. We assume that the common randomness w_c is uniformly and independently chosen from a set $\mathcal{W}_c \triangleq \{1, 2, \cdots, 2^{nR_c}\}$. In our setting, $w_1, w_2, w_{1,p}, w_{2,p}$ and w_c are assumed to be mutually independent. The rate tuple $(R_1(P), R_2(P), R_c(P))$ is said to be achievable if there exists a sequence of n-length codes such that each receiver can decode its desired message reliably, i.e., $\Pr[\hat{w_k} \neq w_k] \leq \epsilon$, $\forall k \in \{1, 2\}$ for any $\epsilon > 0$, satisfying the weak secrecy constraints

$$\mathrm{I}(w_1; y_2^n) \leq n\epsilon \quad \text{and} \quad \mathrm{I}(w_2; y_1^n) \leq n\epsilon \quad (4)$$

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

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

For a given $d_c \in [0, \infty)$, the secure DoF region $\mathcal{D}(d_c)$ is defined as

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

For a given $d_c \in [0, \infty)$, the maximal (optimal) secure sum DoF is then defined as

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

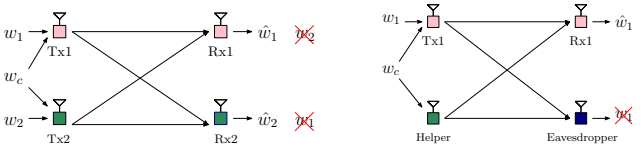

Fig. 2. Two settings with common randomness: IC-SC and WTH.

B. The wiretap channel with a helper (WTH)

In the wiretap channel with a helper, a confidential message w_1 is sent from transmitter 1 to receiver 1. In this setting transmitter 2 will not send any message and will act as a helper (w_2 is treated as an empty term). At transmitter 1, the mapping function f_1 is similar as that in the interference channel (see (3)). At transmitter 2 (helper), a function

$$f_2 : \mathcal{W}_c \times \mathcal{W}_{2,p} \to \mathcal{R}^n$$

is used to generate the signal $x_2^n = f_2(w_c, w_{2,p}) \in \mathcal{R}^n$, where $w_c \in \mathcal{W}_c$ is the common randomness available at both transmitters, and $w_{2,p} \in \mathcal{W}_{2,p}$ is the *private randomness* available at transmitter 2 only. 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 $w_1, w_{1,p}, w_{2,p}$ and w_c are mutually independent. A rate pair $(R_1(P), R_c(P))$ is said to be achievable if there exists a sequence of n-length codes such that receiver 1 can decode its desired message w_1 reliably, satisfying the weak secrecy constraint $\mathrm{I}(w_1; y_2^n) \leq n\epsilon$, for any $\epsilon > 0$, as n goes large. The secure capacity region $\bar{C}(P)$ is the

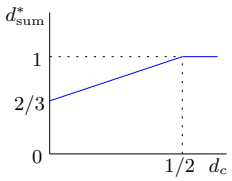

Fig. 3. d^*_{sum} vs d_c, for the interference channel with common randomness.

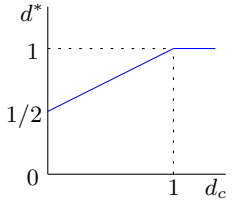

Fig. 4. d^* vs d_c, for wiretap channel with a helper and common randomness.

collection of all achievable secure rate pairs $(R_1(P), R_c(P))$. A secure DoF region is defined as

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

For a given $d_c \in [0, \infty)$, the maximal (optimal) secure DoF is defined as

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

III. The Main Results

The main contribution of this work is the characterization of the optimal secure sum DoF and optimal secure DoF for the IC-SC and WTH settings, respectively.

Theorem 1 (IC-SC)**.** *Considering the IC-SC setting defined in Section II-A, for almost all realizations of the channel coefficients, the optimal secure sum DoF is characterized by*

$$d^*_{sum}(d_c) = \frac{2 \cdot \min\{d_c, 1/2\} + 2}{3}, \quad for \quad d_c \in [0, \infty).$$

Proof. The converse is provided in Section VI. The achievability is a two-layer coding scheme, in which two sub-schemes are designed respectively in two layers. The scheme is provided in Section IV. □

Remark 1. *The result in Theorem 1 matches the existing result of $d^*_{sum} = 2/3$ without common randomness (i.e., when $d_c = 0$, cf. [33]), and the result of $d^*_{sum} = 1$ with full common randomness (i.e., when $d_c = 1/2$, cf. [49]). It can be seen that, without common randomness there is a $1/3$ DoF penalty incurred by the secrecy constraints. Theorem 1 reveals that, the DoF penalty incurred by the secrecy constraints decreases as the DoF of common randomness increases, when $d_c \in [0, 1/2]$. As shown in Fig. 3, the optimal secure sum DoF curve characterized in Theorem 1 bridges the two extreme DoF points with no common randomness and with full common randomness.*

Theorem 2 (WTH)**.** *Considering the WTH setting defined in Section II-B, for almost all the realizations of channel coefficients, the optimal secure DoF is characterized by*

$$d^*(d_c) = \frac{\min\{d_c, 1\} + 1}{2}, \quad for \quad d_c \in [0, \infty).$$

Proof. See Sections V and VII for the proofs. The achievability is also a two-layer coding scheme. □

Remark 2. *The result in Theorem 2 matches the existing result of $d^* = 1/2$ without common randomness (i.e., when $d_c = 0$, cf. [33]), and the result of $d^* = 1$ with full common randomness (i.e., when $d_c = 1$, cf. [49]). It can be seen that, without common randomness there is a $1/2$ DoF penalty incurred by the secrecy constraint. Theorem 2 reveals that, the DoF penalty incurred by the secrecy constraint decreases as the DoF of common randomness increases, when $d_c \in [0, 1]$. As shown in Fig. 4, the optimal secure DoF curve characterized in Theorem 2 bridges the two extreme DoF points with no common randomness and with full common randomness.*

IV. Achievability for Interference Channel

This section provides the achievability proof of Theorem 1, for the IC-SC setting defined in Section II-A. The proposed scheme is a two-layer coding scheme, in which two sub-schemes are designed respectively in two layers, i.e., at two different power levels. Specifically, the sub-scheme in the first layer is designed by using $\min\{d_c, 1/2\}$ DoF of common randomness. For the sub-scheme in the second layer, however, it is designed by using private randomness only, without using common randomness.

This proposed scheme is the extension of the coding scheme proposed in [49] that is able to remove the penalty in DoF, as well as GDoF, incurred by the secrecy constraints in some communication networks. In a two-user interference channel with secrecy constraints, the scheme proposed in [49] is able to achieve 1 secure sum DoF by using $1/2$ DoF of common randomness. Note that, without secrecy constraints, the maximal sum DoF is also 1 for the two user interference channel. In this work we will generalize the scheme in [49] to achieve the optimal secure sum DoF $d^*_{\text{sum}} = \frac{2d_c+2}{3}$ with d_c DoF of common randomness for $d_c \in [0, 1/2]$. Since the maximal sum DoF $d^*_{\text{sum}} = 1$ is achievable by using $d_c = 1/2$ DoF of common randomness, without loss of generality we will consider the case of $d_c \in [0, 1/2]$ in this achievability proof. Before describing the proposed scheme, let us revisit the coding scheme proposed in [49] with full DoF of common randomness ($d_c = 1/2$) for achieving full secure sum DoF ($d^*_{\text{sum}} = 1$) in the interference channel.

A. Coding scheme with full common randomness (cf. [49])

In a two-user interference channel with secrecy constraints, if $d_c = 1/2$ DoF of common randomness is available at the

transmitters, then the transmitters can send the signals in the following forms (removing the time index for simplicity)

$$x_1 = \varepsilon v_1 + \varepsilon \frac{h_{22}h_{12} - h_{12}h_{21}}{h_{11}h_{22} - h_{12}h_{21}} u_c \tag{5}$$

$$x_2 = \varepsilon v_2 + \varepsilon \frac{h_{11}h_{21} - h_{21}h_{12}}{h_{22}h_{11} - h_{21}h_{12}} u_c \tag{6}$$

where ε is a finite constant to regularize the power of the transmitted signals, and u_c is the common randomness. The signals v_1 and v_2 carry the messages of transmitters 1 and 2, respectively. The random variables u_c, v_1 and v_2 are *independently* and *uniformly* drawn from a pulse amplitude modulation (PAM) set

$$v_1, v_2, u_c \in \Omega(\xi = \frac{\gamma}{Q}, \quad Q = P^{\frac{1/2-\epsilon}{2}}) \tag{7}$$

where the parameter $\epsilon > 0$ can be made arbitrarily small, and γ is a finite constant that is used to regularize the power of the signal, for

$$\Omega(\xi, Q) \triangleq \{\xi a : \ a \in [-Q, Q] \cap \mathcal{Z}\}.$$

In this scheme, since $\mathrm{H}(v_k) = \frac{1/2-\epsilon}{2} \log P + o(\log P)$, it implies that the signal v_k carries $1/2$ DoF for $k \in \{1, 2\}$. At the receivers, the received signals then take the following forms

$$y_1 = \varepsilon\sqrt{P}h_{11}v_1 + \varepsilon\sqrt{P}h_{12}\underbrace{(v_2 + u_c)}_{\text{aligned}} + z_1 \tag{8}$$

$$y_2 = \varepsilon\sqrt{P}h_{22}v_2 + \varepsilon\sqrt{P}h_{21}\underbrace{(v_1 + u_c)}_{\text{aligned}} + z_2. \tag{9}$$

The role of the common randomness u_c is to jam the information signal at the eavesdroppers, without causing interference at the legitimate receivers. With a careful design in the signal directions as in (5) and (6), the common randomness u_c jointly sent from both transmitters can jam the information signal v_2 at receiver 1 (the corresponding eavesdropper) and also jam the information signal v_1 at receiver 2, without causing interference.

For this coding scheme with full DoF of common randomness, i.e., with $d_c = 1/2$, it can be proved that the secure rates $R_k = \mathrm{I}(v_k; y_k) - \mathrm{I}(v_k; y_j|v_j) \geq \frac{1/2-\epsilon}{2} \log P + o(\log P)$ for $k \neq j$, $k, j \in \{1, 2\}$, and the optimal secure sum DoF $d^*_{\text{sum}} = 1$, are achievable for almost all the realizations of channel coefficients (cf. [49]).

B. Proposed coding scheme with limited common randomness

The proposed scheme is the extension of the coding scheme proposed in [49]. Specifically, when $d_c \in [0, 1/2]$, the proposed scheme will achieve the optimal secure sum DoF $d^*_{\text{sum}} = \frac{2d_c+2}{3}$ by using d_c DoF of common randomness and some private randomness. In this scheme, the signals

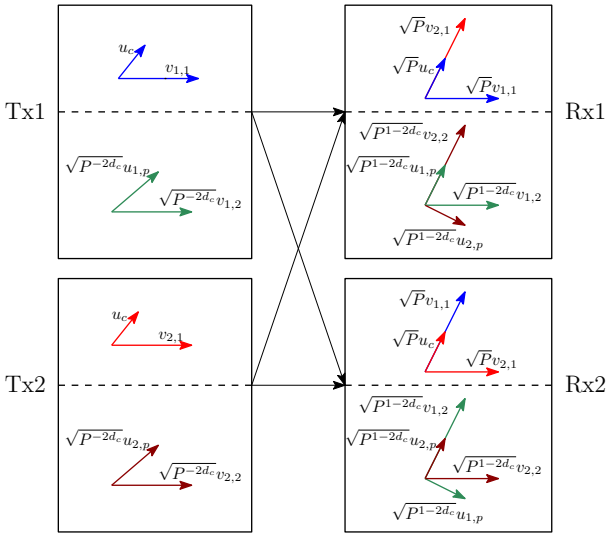

Fig. 5. Illustration of the coding scheme with limited common randomness, by using two-layer coding design.

transmitted by the two transmitters take the following forms (without time index)

$$x_1 = \underbrace{\varepsilon v_{1,1} + \varepsilon \frac{h_{22}h_{12} - h_{12}h_{21}}{h_{11}h_{22} - h_{12}h_{21}} \cdot u_c}_{\text{signals in Layer 1}} + \underbrace{\varepsilon\sqrt{P^{-2d_c}}v_{1,2} + \varepsilon\sqrt{P^{-2d_c}}\frac{h_{12}}{h_{11}} \cdot u_{1,p}}_{\text{signals in Layer 2}} \tag{10}$$

$$x_2 = \underbrace{\varepsilon v_{2,1} + \varepsilon \frac{h_{11}h_{21} - h_{21}h_{12}}{h_{22}h_{11} - h_{21}h_{12}} \cdot u_c}_{\text{signals in Layer 1}} + \underbrace{\varepsilon\sqrt{P^{-2d_c}}v_{2,2} + \varepsilon\sqrt{P^{-2d_c}}\frac{h_{21}}{h_{22}} \cdot u_{2,p}}_{\text{signals in Layer 2}} \tag{11}$$

where ε is a finite constant for regularizing the signal power; u_c is the common randomness; $u_{k,p}$ is a private randomness available at transmitter k only; and $v_{k,1}$ and $v_{k,2}$ are two signals carrying the message of transmitters k, for $k = 1, 2$. As shown in (10) and (11), at transmitter k the signals $v_{k,1}$ and u_c are transmitted at a higher power level, while the signals $v_{k,2}$ and $u_{k,p}$ are transmitted at a lower power level. In this scheme, the random variables u_c, $u_{1,p}$, $u_{2,p}$, $v_{1,1}$, $v_{1,2}$, $v_{2,1}$ and $v_{2,2}$ are *independently* (cross symbols and times) and *uniformly* drawn from their corresponding PAM constellation sets, such as

$$v_{k,1}, u_c \in \Omega(\xi = \frac{\gamma}{Q}, \ Q = P^{\frac{d_c-\epsilon}{2}}) \tag{12}$$

$$v_{k,2}, u_{k,p} \in \Omega(\xi = \frac{\gamma}{2Q}, \ Q = P^{\frac{\frac{1}{3}(1-2d_c)-\epsilon}{2}}) \tag{13}$$

for $k = 1, 2$, where $\epsilon > 0$ can be set arbitrarily small, and γ is a finite constant. Based on the above coding design, the received signals are expressed as

$$y_1 = \underbrace{\varepsilon\sqrt{P}h_{11}v_{1,1} + \varepsilon\sqrt{P}h_{12}(v_{2,1} + u_c)}_{\text{signals in Layer 1}}$$

$$+\varepsilon\sqrt{P^{1-2d_c}}h_{11}v_{1,2}+\varepsilon\sqrt{P^{1-2d_c}}h_{12}(v_{2,2}+u_{1,p})$$
$$+\varepsilon\sqrt{P^{1-2d_c}}\frac{h_{12}h_{21}}{h_{22}}u_{2,p}+z_1 \tag{14}$$

$$y_2=\underbrace{\varepsilon\sqrt{P}h_{22}v_{2,1}+\varepsilon\sqrt{P}h_{21}(v_{1,1}+u_c)}_{\text{signals in Layer 1}}$$
$$+\varepsilon\sqrt{P^{1-2d_c}}h_{22}v_{2,2}+\varepsilon\sqrt{P^{1-2d_c}}h_{21}(v_{1,2}+u_{2,p})+$$
$$\varepsilon\sqrt{P^{1-2d_c}}\frac{h_{21}h_{12}}{h_{11}}u_{1,p}+z_2. \tag{15}$$

As we can see in Fig. 5, the signals sent with higher power arrive at the receivers at a higher power level, while the signals sent with lower power arrive at the receivers at a lower power level. Since the DoF of common randomness is limited, we use the common randomness u_c to jam partial information signals ($v_{1,1}$ and $v_{2,1}$) at the eavesdroppers, in Layer 1 only. In Layer 2, we use private randomness $u_{1,p}$ and $u_{2,p}$ to jam the rest of the information signals ($v_{2,2}$ and $v_{1,2}$) at the eavesdroppers. In this scheme, the common randomness will not generate interference at the receivers, while the private randomness will generate interference at the receivers.

1) Rate analysis: Let us now analyze the secure rate of the proposed two-layer coding scheme. Before analyzing the secure rate of the scheme, let us first discuss the codebook generation and signal mapping of the scheme.

For transmitter k, $k=1,2$, it generates a codebook as

$$\mathcal{B}_k\triangleq\Big\{v_k^n(w_k,w_k'):w_k\in\{1,2,\cdots,2^{nR_k}\},\ w_k'\in\{1,2,\cdots,2^{nR_k'}\}\Big\} \tag{16}$$

which includes a set of codewords v_k^n with labels. The elements of the codewords are independently and identically generated by using a particular distribution. Specifically, the elements of the codewords are independently and identically generated based on the following structure

$$v_k(t)=v_{k,1}(t)+\sqrt{P^{-2d_c}}v_{k,2}(t) \tag{17}$$

where $v_k(t)$ denotes the tth element of v_k^n, and $v_{k,1}(t)$ and $v_{k,2}(t)$ are generated based on (12) and (13). Once a new codeword v_k^n is generated, it will be labeled with a new value of (w_k,w_k'). In the expression of (16), w_k is the confidential message and w_k' is a private randomness available at transmitter k only. The private randomness w_k' is used to protect the confidential message, and is uniformly distributed over $\{1,2,\cdots,2^{nR_k'}\}$. R_k and R_k' represent the rates of w_k and w_k', respectively. To send the message w_k, transmitter k chooses a codeword v_k^n *randomly* from a sub-codebook $\mathcal{B}_k(w_k)$ defined by

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

for $k\in\{1,2\}$. Then, the selected codeword v_k^n is mapped to the channel inputs $\{x_k(t)\}_{t=1}^n$ based on the following relationship

$$x_k(t)=\varepsilon v_k(t)+\varepsilon\frac{h_{jj}h_{kj}-h_{kj}h_{jk}}{h_{kk}h_{jj}-h_{kj}h_{jk}}u_c(t)+\varepsilon\sqrt{P^{-2d_c}}\frac{h_{kj}}{h_{kk}}u_{k,p}(t)$$

for $t\in\{1,2,\cdots,n\}$ and $k,j\in\{1,2\},j\neq k$, where $v_k(t)$ denotes the tth element of v_k^n. The randomness $u_c(t)$ and $u_{k,p}(t)$ are independently generated based on (12) and (13). As a result, the channel inputs take the forms as in (10) and (11). In the proposed scheme, $\{u_c(t)\}_t$ refer to the common randomness available at both transmitters, while w_k' and $\{u_{k,p}(t)\}_t$ refer to the private randomness available at transmitter k only. In our setting, w_1', w_2', $\{u_{1,p}(t)\}_t$, $\{u_{2,p}(t)\}_t$ and $\{u_c(t)\}_t$ are mutually independent.

Let us set the rates R_k and R_k' appeared in (16) as

$$R_k\triangleq\mathrm{I}(v_k;y_k)-\mathrm{I}(v_k;y_\ell|v_\ell)-\epsilon \tag{18}$$
$$R_k'\triangleq\mathrm{I}(v_k;y_\ell|v_\ell)-\epsilon \tag{19}$$

for some $\epsilon>0$, and $\ell,k\in\{1,2\},\ell\neq k$. With our codebook design and signal mapping, the result of [36, Theorem 2] (or [12, Theorem 2]) reveals that the rate pair (R_1,R_2) defined in (18) is achievable under the secrecy constraints (cf. (4)). In the following we will derive the low bound of R_1 expressed in (18), as the lower bound of R_2 can be easily derived due to the symmetry. At first, we have a bound on $\mathrm{I}(v_1;y_1)$ appeared in (18), given as

$$\begin{aligned}&\mathrm{I}(v_1;y_1)\\ \geq&\mathrm{I}(v_1;\hat{v}_{1,1},\hat{v}_{1,2}) &(20)\\ =&\mathrm{H}(v_1)-\mathrm{H}(v_1|\hat{v}_{1,1},\hat{v}_{1,2})\\ \geq&\mathrm{H}(v_1)-\big(1+\Pr[\{v_{1,1}\neq\hat{v}_{1,1}\}\cup\{v_{1,2}\neq\hat{v}_{1,2}\}]\cdot\mathrm{H}(v_1)\big) &(21)\\ =&\big(1-\Pr[\{v_{1,1}\neq\hat{v}_{1,1}\}\cup\{v_{1,2}\neq\hat{v}_{1,2}\}]\big)\cdot\frac{\frac{1+d_c}{3}-2\epsilon}{2}\log P\\ &+o(\log P) &(22)\end{aligned}$$

where $\hat{v}_{1,1}$ and $\hat{v}_{1,2}$ denote the estimates of $v_{1,1}$ and $v_{1,2}$ respectively from y_1, and $\Pr[\{v_{1,1}\neq\hat{v}_{1,1}\}\cup\{v_{1,2}\neq\hat{v}_{1,2}\}]$ denotes the error probability of this estimation; recall that $v_1=v_{1,1}+\sqrt{P^{-2d_c}}v_{1,2}$ (see (17)); the step in (20) follows from the Markov chain $v_1\to y_1\to\{\hat{v}_{1,1},\hat{v}_{1,2}\}$; and the step in (21) stems from Fano's inequality. The step in (22) follows from the following derivations

$$\begin{aligned}\mathrm{H}(v_1)&=\mathrm{H}(v_{1,1})+\mathrm{H}(v_{1,2})\\ &=\log(2\cdot P^{\frac{d_c-\epsilon}{2}}+1)+\log(2\cdot P^{\frac{(1-2d_c)/3-\epsilon}{2}}+1)\\ &=\frac{(1+d_c)/3-2\epsilon}{2}\log P+o(\log P)\end{aligned}$$

where $v_{1,1}\in\Omega(\xi=\frac{\gamma}{Q},\ Q=P^{\frac{d_c-\epsilon}{2}})$ and $v_{1,2}\in\Omega(\xi=\frac{\gamma}{2Q},\ Q=P^{\frac{(1-2d_c)/3-\epsilon}{2}})$ (see (12) and (13)). Note that $v_{1,1}$ and $v_{1,2}$ can be reconstructed from v_1, and vice versa, given that $v_1=v_{1,1}+\sqrt{P^{-2d_c}}v_{1,2}$. To get a desired bound on $\mathrm{I}(v_1;y_1)$, a result on the error probability is provided below.

Lemma 1. *Given the signal design in* (10)-(17)*, and for almost all realizations of channel coefficients, the error probability of decoding $\{v_{k,1},v_{k,2}\}$ from y_k is vanishing when P goes large, for $k=1,2$, i.e.,*

$$Pr[\{v_{k,1}\neq\hat{v}_{k,1}\}\cup\{v_{k,2}\neq\hat{v}_{k,2}\}]\to 0\quad as\quad P\to\infty. \tag{23}$$

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

By incorporating the result of Lemma 1 into (22), it gives a lower bound on $\mathrm{I}(v_1; y_1)$, given as

$$\mathrm{I}(v_1; y_1) \geq \frac{(1+d_c)/3 - 2\epsilon}{2} \log P + o(\log P) \tag{24}$$

for almost all realizations of channel coefficients. Let us now focus on bounding the term $\mathrm{I}(v_1; y_2|v_2)$ in (18), which can be treated as a rate penalty. The following lemma provides a result on bounding this penalty.

Lemma 2. *Given the signal design in* (10)-(17)*, it holds true that*

$$\mathrm{I}(v_1; y_2|v_2) \leq o(\log P). \tag{25}$$

Proof. See Appendix B. □

Based on the results of (24) and (25), it reveals that the achievable secure rate R_1 expressed in (18) is lower bounded by

$$R_1 \geq \frac{(1+d_c)/3 - 2\epsilon}{2} \log P + o(\log P) \tag{26}$$

for almost all realizations of channel coefficients. Due to the symmetry, the achievable secure rate R_2 expressed in (18) is also lower bounded by $R_2 \geq \frac{(1+d_c)/3-2\epsilon}{2} \log P + o(\log P)$. Therefore, the proposed scheme achieves the secure sum DoF $d_1 + d_2 = 2(1+d_c)/3$ for almost all realizations of channel coefficients.

Recall that, in the proposed scheme the common randomness u_c is *independently* and *uniformly* drawn from the PAM constellation set such as $u_c \in \Omega(\xi = \frac{\gamma}{Q},\ Q = P^{\frac{d_c-\epsilon}{2}})$. In this case we have $\mathrm{H}(u) = \log(2 \cdot P^{\frac{d_c-\epsilon}{2}} + 1) = \frac{d_c-\epsilon}{2} \log P + o(\log P)$, which implies that the amount of DoF of the common randomness used in the proposed scheme is d_c when $\epsilon \to 0$.

V. Achievability for wiretap channel with a helper

This section provides the achievability proof of Theorem 2, for the wiretap channel with a helper defined in Section II-B. The proposed scheme is also a two-layer coding scheme, which is similar to the scheme described in the previous section. Considering the case of $d_c \in [0, 1]$, the proposed scheme will be shown to achieve the optimal secure DoF $d^* = \frac{d_c+1}{2}$ by using d_c DoF of common randomness and some private randomness. In order to avoid the repetition, we will just provide the highlights of the scheme.

For the scheme proposed for the wiretap channel with a helper, the signals transmitted by the two transmitters take the following forms (without time index)

$$x_1 = \underbrace{\varepsilon v_{1,1} - \varepsilon \frac{h_{12}h_{21}}{h_{11}h_{22} - h_{12}h_{21}} u_c}_{\text{signals in Layer 1}} + \underbrace{\varepsilon \sqrt{P^{-d_c}} \frac{1}{h_{21}} v_{1,2}}_{\text{signal in Layer 2}} \tag{27}$$

$$x_2 = \underbrace{\varepsilon \frac{h_{11}h_{21}}{h_{22}h_{11} - h_{21}h_{12}} u_c}_{\text{signal in Layer 1}} + \underbrace{\varepsilon \sqrt{P^{-d_c}} \frac{1}{h_{22}} u_{2,p}}_{\text{signal in Layer 2}} \tag{28}$$

where ε is a finite constant for regularizing the signal power; u_c is the common randomness; $u_{2,p}$ is a private randomness available at transmitter 2 only; and $v_{1,1}$ and $v_{1,2}$ are two signals carrying the message of transmitters 1. As shown in (27) and (28), the signals $v_{1,1}$ and u_c are transmitted at a higher power level, while the signals $v_{1,2}$ and $u_{2,p}$ are transmitted at a lower power level. In this scheme, the random variables u_c, $u_{2,p}$, $v_{1,1}$ and $v_{1,2}$ are *independently* (cross symbols and times) and *uniformly* drawn from their corresponding PAM constellation sets, such as

$$v_{1,1}, u_c \in \Omega(\xi = \frac{\gamma}{Q},\ Q = P^{\frac{d_c-\epsilon}{2}}) \tag{29}$$

$$v_{1,2}, u_{2,p} \in \Omega(\xi = \frac{\gamma}{2Q},\ Q = P^{\frac{(1-d_c)/2-\epsilon}{2}}) \tag{30}$$

where $\epsilon > 0$ can be set arbitrarily small, and γ is a finite constant. Based on the above coding design, the received signals are expressed as

$$y_1 = \underbrace{\varepsilon \sqrt{P} h_{11} v_{1,1}}_{\text{signal in Layer 1}} + \underbrace{\varepsilon \sqrt{P^{1-d_c}} \frac{h_{11}}{h_{21}} v_{1,2} + \varepsilon \sqrt{P^{1-d_c}} \frac{h_{12}}{h_{22}} u_{2,p}}_{\text{signals in Layer 2}} + z_1 \tag{31}$$

$$y_2 = \underbrace{\varepsilon \sqrt{P} h_{21} (v_{1,1} + u_c)}_{\text{signal in Layer 1}} + \underbrace{\varepsilon \sqrt{P^{1-d_c}} (v_{1,2} + u_{2,p})}_{\text{signal in Layer 2}} + z_2. \tag{32}$$

As we can see in (31) and (32), the signals sent with higher power arrive at the receivers at a higher power level, while the signals sent with lower power arrive at the receivers at a lower power level. Since the DoF of common randomness is limited, we use the common randomness u_c to jam the information signal $v_{1,1}$ at the eavesdropper, in Layer 1. In Layer 2, we use private randomness $u_{2,p}$ to jam the rest of the information signal (i.e., $v_{1,2}$) at the eavesdropper. In this scheme, the common randomness will not generate interference at the legitimate receiver, while the private randomness will generate interference at the legitimate receiver.

By following the rate analysis in the previous section (cf. (16)-(26)), one can show that the proposed scheme achieves the secure rate R_1 that is bounded by $R_1 \geq \frac{\frac{d_c+1}{2}-2\epsilon}{2} \log P + o(\log P)$, for almost all the realizations of channel coefficients. The analysis is also based on successive decoding (cf. Lemma 1). Note that the wiretap channel with a helper can be considered as a specific case of the IC-SC setting by removing the message of the second transmitter. Therefore, the results in (18) and (19), as well as the analysis provided for the IC-SC setting, can be extended to this WTH setting. Thus, it implies that the optimal secure DoF $d^* = \frac{d_c+1}{2}$ is achievable for almost all the realizations of channel coefficients, by using $d_c \in [0, 1]$ DoF of common randomness.

VI. Converse for the interference channel

For the Gaussian interference channel defined in Section II-A, we provide an upper bound on the secure sum DoF, which is stated in the following lemma. The result of this lemma serves as the converse of Theorem 1.

Lemma 3. *For the two-user Gaussian interference channel defined in Section II-A, the following bound holds true*

$$d_1 + d_2 \le \min\Big\{1,\ \frac{2d_c+2}{3}\Big\}. \tag{33}$$

In the following we will first prove

$$2d_1 + d_2 \le d_c + 1 \tag{34}$$
$$2d_2 + d_1 \le d_c + 1 \tag{35}$$

which will produce the desired bound $d_1+d_2 \le \frac{2d_c+2}{3}$. Later on we will prove the other bound

$$d_1 + d_2 \le 1$$

which will complete the proof for Lemma 3. Let us define that

$$s_{\ell k}(t) \triangleq \sqrt{P}h_{\ell k}x_k(t) + z_\ell(t) \tag{36}$$
$$\tilde{x}_k(t) \triangleq \sqrt{P}x_k(t) + \tilde{z}_k(t) \tag{37}$$

for $k,\ell \in \{1,2\}, k \ne \ell$, where $\tilde{z}_k(t) \sim \mathcal{N}(0,1)$ is a virtual noise that is independent of the other noise and transmitted signals x_1^n and x_2^n. Let $s_{\ell k}^n \triangleq \{s_{\ell k}(t)\}_{t=1}^n$ and $\tilde{x}_k^n \triangleq \{\tilde{x}_k(t)\}_{t=1}^n$.

A. Proof of bounds (34) and (35)

Beginning with Fano's inequality, the rate of user 1 is bounded as

$$\begin{aligned}
&nR_1 - n\epsilon_{1,n} \\
\le&\mathrm{I}(w_1; y_1^n) && (38)\\
\le&\mathrm{I}(w_1; y_1^n) - \mathrm{I}(w_1; y_2^n) + n\epsilon && (39)\\
\le&\mathrm{I}(w_1; y_1^n, \tilde{x}_1^n, \tilde{x}_2^n, y_2^n, w_c) - \mathrm{I}(w_1; y_2^n) + n\epsilon && (40)\\
=&\mathrm{I}(w_1; y_1^n, \tilde{x}_1^n, \tilde{x}_2^n, w_c|y_2^n) + n\epsilon \\
=&\underbrace{\mathrm{I}(w_1; w_c|y_2^n)}_{\le nR_c} + \mathrm{I}(w_1; y_1^n, \tilde{x}_1^n, \tilde{x}_2^n|y_2^n, w_c) + n\epsilon \\
\le&nR_c + \mathrm{I}(w_1; y_1^n, \tilde{x}_1^n, \tilde{x}_2^n|y_2^n, w_c) + n\epsilon && (41)\\
=&nR_c + \mathrm{h}(y_1^n, \tilde{x}_1^n, \tilde{x}_2^n|y_2^n, w_c) - \mathrm{h}(y_1^n, \tilde{x}_1^n, \tilde{x}_2^n|y_2^n, w_1, w_c) + n\epsilon \\
=&nR_c + \mathrm{h}(\tilde{x}_1^n, \tilde{x}_2^n|w_c) + \mathrm{h}(y_1^n, y_2^n|\tilde{x}_1^n, \tilde{x}_2^n, w_c) - \mathrm{h}(y_2^n|w_c) \\
&- \mathrm{h}(y_1^n, \tilde{x}_1^n, \tilde{x}_2^n|y_2^n, w_1, w_c) + n\epsilon \\
\le&nR_c + \mathrm{h}(\tilde{x}_1^n|w_c) + \mathrm{h}(\tilde{x}_2^n|w_c) + \mathrm{h}(y_1^n, y_2^n|\tilde{x}_1^n, \tilde{x}_2^n, w_c) \\
&- \mathrm{h}(y_2^n|w_c) - \mathrm{h}(y_1^n, \tilde{x}_1^n, \tilde{x}_2^n|y_2^n, w_1, w_c) + n\epsilon && (42)
\end{aligned}$$

where (38) results from Fano's inequality, with $\lim_{n\to\infty}\epsilon_{1,n} = 0$; (39) follows from the secrecy constraint; (40) stems from the fact that adding information does not decrease the mutual information; (41) holds true because $\mathrm{I}(w_1; w_c|y_2^n) \le \mathrm{H}(w_c) = nR_c$; (42) uses chain rule and the fact that conditioning reduces differential entropy. We also have another bound on the rate of user 1 as

$$\begin{aligned}
nR_1 \le& \mathrm{I}(w_1; y_1^n) + n\epsilon_{1,n} \\
\le& \mathrm{I}(w_1; y_1^n, w_c) + n\epsilon_{1,n} && (43)\\
=& \mathrm{I}(w_1; y_1^n|w_c) + n\epsilon_{1,n} && (44)\\
=& \mathrm{h}(y_1^n|w_c) - \mathrm{h}(y_1^n|w_1, w_c) + n\epsilon_{1,n} \\
\le& \mathrm{h}(y_1^n|w_c) - \mathrm{h}(y_1^n|x_1^n, w_1, w_c) + n\epsilon_{1,n} && (45)\\
=& \mathrm{h}(y_1^n|w_c) - \mathrm{h}(s_{12}^n|x_1^n, w_1, w_c) + n\epsilon_{1,n} && (46)\\
=& \mathrm{h}(y_1^n|w_c) - \mathrm{h}(s_{12}^n|w_c) + n\epsilon_{1,n} && (47)
\end{aligned}$$

where (43) uses the fact that adding information does not decrease the mutual information; (44) stems from the independence between w_c and w_1; (45) uses the fact that conditioning reduces differential entropy; (46) results from the fact that $y_1(t) = \sqrt{P}h_{11}x_1(t) + s_{12}(t)$; (47) follows from the Markov chain of $\{x_1^n, w_1\} \to w_c \to s_{12}^n$. In a similar way, we have

$$nR_2 \le \mathrm{h}(y_2^n|w_c) - \mathrm{h}(s_{21}^n|w_c) + n\epsilon_{2,n}. \tag{48}$$

With the results of (42), (47) and (48), we have

$$\begin{aligned}
&2nR_1 + nR_2 - nR_c - 2n\epsilon_{1,n} - n\epsilon_{2,n} - n\epsilon \\
\le&\mathrm{h}(\tilde{x}_1^n|w_c) - \mathrm{h}(s_{21}^n|w_c) + \mathrm{h}(\tilde{x}_2^n|w_c) - \mathrm{h}(s_{12}^n|w_c) + \mathrm{h}(y_1^n|w_c) \\
&+ \mathrm{h}(y_1^n, y_2^n|\tilde{x}_1^n, \tilde{x}_2^n, w_c) - \mathrm{h}(y_1^n, \tilde{x}_1^n, \tilde{x}_2^n|y_2^n, w_1, w_c) && (49)\\
\le&\frac{n}{2}\log\big(1 + \frac{1}{|h_{21}|^2}\big) + \frac{n}{2}\log\big(1 + \frac{1}{|h_{12}|^2}\big) \\
&+ \frac{n}{2}\log\big(1 + P|h_{11}|^2 + P|h_{12}|^2\big) \\
&+ \frac{n}{2}\log\big(1 + |h_{11}|^2 + |h_{12}|^2\big) \\
&+ \frac{n}{2}\log\big(1 + |h_{22}|^2 + |h_{21}|^2\big) && (50)\\
=&\frac{n}{2}\log P + n\cdot o(\log P) && (51)
\end{aligned}$$

where (49) stems from the results of (42), (47) and (48); and (50) follows from Lemma 4. At this point, by dividing each side of (51) with $\frac{n}{2}\log P$, and setting $n\to\infty$, $P\to\infty$ and $\epsilon \to 0$, it then gives the bound in (34). By interchanging the roles of user 1 and user 2, the bound in (35) can be proved in a similar way. The lemma used in the proof is provided below.

Lemma 4. *It holds true that*

$$\mathrm{h}(\tilde{x}_1^n|w_c) - \mathrm{h}(s_{21}^n|w_c) \le \frac{n}{2}\log\big(1 + \frac{1}{|h_{21}|^2}\big) \tag{52}$$
$$\mathrm{h}(\tilde{x}_2^n|w_c) - \mathrm{h}(s_{12}^n|w_c) \le \frac{n}{2}\log\big(1 + \frac{1}{|h_{12}|^2}\big) \tag{53}$$
$$\begin{aligned}
\mathrm{h}(y_1^n, y_2^n|\tilde{x}_1^n, \tilde{x}_2^n, w_c) \le& \frac{n}{2}\log\big(2\pi e\big(1 + |h_{11}|^2 + |h_{12}|^2\big)\big) \\
&+ \frac{n}{2}\log\big(2\pi e\big(1 + |h_{22}|^2 + |h_{21}|^2\big)\big)
\end{aligned} \tag{54}$$
$$\mathrm{h}(y_1^n|w_c) \le \frac{n}{2}\log\big(2\pi e(1 + P|h_{11}|^2 + P|h_{12}|^2)\big) \tag{55}$$
$$\mathrm{h}(y_1^n, \tilde{x}_1^n, \tilde{x}_2^n|y_2^n, w_1, w_c) \ge \frac{3n}{2}\log(2\pi e). \tag{56}$$

Proof. See Appendix C. □

B. Proof of the bound $d_1 + d_2 \le 1$

Beginning with Fano's inequality, the sum rate can be bounded as

$$\begin{aligned}
&nR_1 + nR_2 \\
\le&\mathrm{I}(w_1; y_1^n) + \mathrm{I}(w_2; y_2^n) + n\epsilon_n \\
\le&\mathrm{I}(w_1; y_1^n, y_2^n, x_2^n) + \mathrm{I}(x_2^n; y_2^n) + n\epsilon_n && (57)\\
=&\mathrm{I}(w_1; y_1^n, y_2^n|x_2^n) + \mathrm{I}(x_2^n; y_2^n) + n\epsilon_n && (58)\\
=&\mathrm{I}(w_1; y_2^n|x_2^n) + \mathrm{I}(x_2^n; y_2^n) + \mathrm{I}(w_1; y_1^n|y_2^n, x_2^n) + n\epsilon_n \\
=&\underbrace{\mathrm{I}(w_1, x_2^n; y_2^n)}_{\le \frac{n}{2}\log P + no(\log P)} + \underbrace{\mathrm{I}(w_1; y_1^n|y_2^n, x_2^n)}_{\le no(\log P)} + n\epsilon_n
\end{aligned}$$

$$\leq \frac{n}{2}\log P + no(\log P) + n\epsilon_n \tag{59}$$

where (57) follows from the Markov chain of $w_2 \to x_2^n \to y_2^n$ and the fact that adding information does not decrease the mutual information; (58) uses chain rule and the independence between w_1 and x_2^n; (59) follows from the derivations that $\mathrm{I}(w_1, x_2^n; y_2^n) \leq \mathrm{h}(y_2^n) - \mathrm{h}(z_2^n) \leq \frac{n}{2}\log P + no(\log P)$ and that $\mathrm{I}(w_1; y_1^n | y_2^n, x_2^n) = \mathrm{I}(w_1; \{z_1(t) - \frac{h_{11}}{h_{21}} z_2(t)\}_{t=1}^n | y_2^n, x_2^n) \leq no(\log P)$. By dividing each side of (59) with $\frac{n}{2}\log P$, and setting $n \to \infty$ and $P \to \infty$, then the bound $d_1 + d_2 \leq 1$ is proved. At this point we complete the proof of Lemma 3.

VII. Converse for the wiretap channel

For the Gaussian wiretap channel with a helper defined in Section II-B, we provide an upper bound on the secure DoF, which is stated in the following lemma. The result of this lemma serves as the converse of Theorem 2.

Lemma 5. *For the WTH setting defined in Section II-B, the following bound holds true*

$$d \leq \min\{1, \ \frac{d_c + 1}{2}\}. \tag{60}$$

In what follows, we will prove Lemma 5. At first we will prove

$$d \leq \frac{d_c + 1}{2}. \tag{61}$$

Later on we will prove the other bound

$$d \leq 1 \tag{62}$$

which will complete the proof for Lemma 5.

A. Proof of bound (61)

In the proof we will use the same definitions of $s_{\ell k}(t)$ and $\tilde{x}_k(t)$ as in (36) and (37). Beginning with Fano's inequality, we have the following bound on the secure rate

$$\begin{aligned}
&nR_1 - n\epsilon_{1,n} \\
\leq& \mathrm{I}(w_1; y_1^n) \\
\leq& \mathrm{I}(w_1; y_1^n) - \mathrm{I}(w_1; y_2^n) + n\epsilon && (63)\\
\leq& \mathrm{I}(w_1; y_1^n, \tilde{x}_1^n, \tilde{x}_2^n, y_2^n, w_c) - \mathrm{I}(w_1; y_2^n) + n\epsilon \\
=& \mathrm{I}(w_1; y_1^n, \tilde{x}_1^n, \tilde{x}_2^n, w_c | y_2^n) + n\epsilon \\
=& \underbrace{\mathrm{I}(w_1; w_c | y_2^n)}_{\leq nR_c} + \mathrm{I}(w_1; y_1^n, \tilde{x}_1^n, \tilde{x}_2^n | y_2^n, w_c) + n\epsilon \\
\leq& nR_c + \mathrm{I}(w_1; y_1^n, \tilde{x}_1^n, \tilde{x}_2^n | y_2^n, w_c) + n\epsilon && (64)\\
=& nR_c + \mathrm{h}(\tilde{x}_1^n, \tilde{x}_2^n | w_c) + \mathrm{h}(y_1^n, y_2^n | \tilde{x}_1^n, \tilde{x}_2^n, w_c) - \mathrm{h}(y_2^n | w_c) \\
&- \mathrm{h}(y_1^n, \tilde{x}_1^n, \tilde{x}_2^n | y_2^n, w_1, w_c) + n\epsilon \\
\leq& nR_c + \mathrm{h}(\tilde{x}_1^n | w_c) + \mathrm{h}(\tilde{x}_2^n | w_c) + \mathrm{h}(y_1^n, y_2^n | \tilde{x}_1^n, \tilde{x}_2^n, w_c) \\
&- \mathrm{h}(s_{21}^n | w_c) - \mathrm{h}(y_1^n, \tilde{x}_1^n, \tilde{x}_2^n | y_2^n, w_1, w_c) + n\epsilon && (65)
\end{aligned}$$

where (63) results from the secrecy constraint; (41) follows from the result that $\mathrm{I}(w_1; w_c | y_2^n) \leq \mathrm{H}(w_c) = nR_c$; (65) holds true because $\mathrm{h}(y_2^n | w_c) \geq \mathrm{h}(y_2^n | x_2^n, w_c) = \mathrm{h}(s_{21}^n | x_2^n, w_c) = \mathrm{h}(s_{21}^n | w_c)$, due to the equality of $y_2(t) = \sqrt{P} h_{22} x_2(t) + s_{21}(t)$ and the Markov chain of $x_2^n \to w_c \to s_{21}^n$.

For the secure rate, we also have another bound given as

$$\begin{aligned}
nR_1 \leq& \mathrm{I}(w_1; y_1^n) + n\epsilon_{1,n} \\
\leq& \mathrm{I}(w_1; w_c, y_1^n) + n\epsilon_{1,n} \\
=& \mathrm{I}(w_1; y_1^n | w_c) + n\epsilon_{1,n} && (66)\\
\leq& \mathrm{I}(x_1^n; y_1^n | w_c) + n\epsilon_{1,n} && (67)\\
=& \mathrm{h}(y_1^n | w_c) - \mathrm{h}(s_{12}^n | x_1^n, w_c) + n\epsilon_{1,n} && (68)\\
=& \mathrm{h}(y_1^n | w_c) - \mathrm{h}(s_{12}^n | w_c) + n\epsilon_{1,n} && (69)
\end{aligned}$$

where (66) results from the independence between w_1 and w_c; (67) follows from the Markov chain of $w_1 \to \{w_c, x_1^n\} \to y_1^n$; (68) uses the fact that $y_1(t) = \sqrt{P} h_{11} x_1(t) + s_{12}(t)$; (69) is true because $x_1^n \to w_c \to s_{12}^n$ forms a Markov chain.

By merging the results of (65) and (69) together, it produces the following bound

$$\begin{aligned}
&2nR_1 - nR_c - 2n\epsilon_{1,n} - n\epsilon \\
\leq& \mathrm{h}(\tilde{x}_1^n | w_c) - \mathrm{h}(s_{21}^n | w_c) + \mathrm{h}(\tilde{x}_2^n | w_c) - \mathrm{h}(s_{12}^n | w_c) + \mathrm{h}(y_1^n | w_c) \\
&+ \mathrm{h}(y_1^n, y_2^n | \tilde{x}_1^n, \tilde{x}_2^n, w_c) - \mathrm{h}(y_1^n, \tilde{x}_1^n, \tilde{x}_2^n | y_2^n, w_1, w_c). \quad (70)
\end{aligned}$$

At this point, by using the result of Lemma 4 (see Section VI) that is also true for this WTH setting, the bound in (70) can be further bounded as

$$\begin{aligned}
&2R_1 - nR_c + 2\epsilon_{1,n} - \epsilon \\
\leq& \frac{n}{2}\log\big(1 + \frac{1}{|h_{21}|^2}\big) + \frac{n}{2}\log\big(1 + \frac{1}{|h_{12}|^2}\big) \\
&+ \frac{n}{2}\log\big(1 + P|h_{11}|^2 + P|h_{12}|^2\big) \\
&+ \frac{n}{2}\log\big(1 + |h_{11}|^2 + |h_{12}|^2\big) \\
&+ \frac{n}{2}\log\big(1 + |h_{22}|^2 + |h_{21}|^2\big) \\
=& \frac{n}{2}\log P + n \cdot o(\log P) && (71)
\end{aligned}$$

Finally, by dividing each side of (71) with $\frac{n}{2}\log P$, and setting $n \to \infty$, $P \to \infty$ and $\epsilon \to 0$, it then gives the desired bound of $d \leq \frac{d_c+1}{2}$.

B. Proof of bound (62)

Beginning with Fano's inequality, the rate is bounded as

$$\begin{aligned}
nR_1 \leq& \mathrm{I}(w_1; y_1^n) + n\epsilon_n \\
\leq& \mathrm{I}(w_1; y_1^n, x_2^n, w_c) + n\epsilon_n && (72)\\
=& \mathrm{I}(w_1; y_1^n | x_2^n, w_c) + n\epsilon_n && (73)\\
\leq& \mathrm{h}(\{\sqrt{P} h_{11} x_1(t) + z_1(t)\}_{t=1}^n) - \mathrm{h}(z_1^n) + n\epsilon_n && (74)\\
\leq& \frac{n}{2}\log(2\pi e(1 + P|h_{11}|^2)) - \frac{n}{2}\log(2\pi e) + n\epsilon_n && (75)\\
=& \frac{n}{2}\log P + n \cdot o(\log P) && (76)
\end{aligned}$$

where (72) follows from the fact that adding information does not decrease the mutual information; (73) uses chain rule and the independence between w_1 and (x_2^n, w_c); (74) uses the fact that conditioning reduces the differential entropy; (75) follows from the fact that Gaussian input maximizes the differential entropy. The result in (76) reveals that the bound $d \leq 1$ is true, which completes the proof of Lemma 5.

VIII. Conclusion

This work considered a two-user interference channel with secrecy constraints and a wiretap channel with a helper, both with a limited common randomness at the transmitters. This work shows that, the common randomness is helpful in increasing the secure sum DoF or secure DoF, even the common randomness is limited. When the DoF of common randomness is increased to a certain value, the secure sum DoF or secure DoF can be increased to the maximum value as if no secrecy constraints are imposed. The two-layer coding scheme proposed in this work achieves the optimal secure sum DoF or secure DoF by utilizing limited common randomness.

Appendix A
Proof of Lemma 1

In this section we will prove Lemma 1. Specifically we will prove that, given the the signal design in (10)-(17) and for almost all realizations of channel coefficients, the error probability of decoding $\{v_{k,1}, v_{k,2}\}$ from y_k is vanishing when P goes large, i.e.,

$$\Pr[\{v_{k,1} \neq \hat{v}_{k,1}\} \cup \{v_{k,2} \neq \hat{v}_{k,2}\}] \to 0 \quad \text{as} \quad P \to \infty$$

for $k = 1, 2$, where $\hat{v}_{k,1}$ and $\hat{v}_{k,2}$ denote the estimates of $v_{k,1}$ and $v_{k,2}$ respectively from y_k, and $\Pr[\{v_{1,1} \neq \hat{v}_{1,1}\} \cup \{v_{1,2} \neq \hat{v}_{1,2}\}]$ denotes the error probability of this estimation. The estimation is based on successive decoding. Due to the symmetry, we will focus on the proof for the case with $k = 1$. Recall that y_1 is expressed as

$$\begin{aligned} y_1 =& \underbrace{\varepsilon\sqrt{P}h_{11}v_{1,1} + \varepsilon\sqrt{P}h_{12}(v_{2,1} + u_c)}_{\text{signals in Layer 1}} \\ &+ \varepsilon\sqrt{P^{1-2d_c}}h_{11}v_{1,2} + \varepsilon\sqrt{P^{1-2d_c}}h_{12}(v_{2,2} + u_{1,p}) \\ &+ \varepsilon\sqrt{P^{1-2d_c}}\frac{h_{12}h_{21}}{h_{22}}u_{2,p} + z_1 \end{aligned} \tag{77}$$

(see (14)).

In the first step, we estimate the signals $v_{1,1}$ and $(v_{2,1}+u_c)$ in the first layer by treating the signals in the second layer as noise. Recall that

$$v_{1,1}, v_{2,1}, u_c \in \Omega(\xi = \frac{\gamma}{P^{\frac{d_c-\epsilon}{2}}},\ Q = P^{\frac{d_c-\epsilon}{2}}) \tag{78}$$

$$v_{1,2}, v_{2,2}, u_{1,p}, u_{2,p} \in \Omega(\xi = \frac{\gamma}{2P^{\frac{\frac{1-2d_c}{3}-\epsilon}{2}}},\ Q = P^{\frac{\frac{1-2d_c}{3}-\epsilon}{2}}) \tag{79}$$

which imply that

$$v_{2,1} + u_c \in \Omega(\xi = \frac{\gamma}{P^{\frac{d_c-\epsilon}{2}}},\ Q = 2P^{\frac{d_c-\epsilon}{2}}) \tag{80}$$

$$v_{2,2} + u_{1,p} \in \Omega(\xi = \frac{\gamma}{2P^{\frac{\frac{1-2d_c}{3}-\epsilon}{2}}},\ Q = 2P^{\frac{\frac{1-2d_c}{3}-\epsilon}{2}}). \tag{81}$$

For the observation y_1 expressed in (77), it can be transformed into the following form

$$\begin{aligned} y_1' \triangleq& y_1/(\varepsilon\sqrt{P^{1-2d_c}}) \\ =& \sqrt{P^{2d_c}}h_{11}v_{1,1} + \sqrt{P^{2d_c}}h_{12}(v_{2,1} + u_c) + g + z_1' \\ =& \gamma P^{\frac{d_c+\epsilon}{2}}h_{11}q_1 + \gamma P^{\frac{d_c+\epsilon}{2}}h_{12}q_2 + g + z_1' \end{aligned} \tag{82}$$

for

$$\begin{aligned} &q_1 \triangleq \frac{Q_{\max}}{\gamma}v_{1,1}, \quad q_2 \triangleq \frac{Q_{\max}}{\gamma}(v_{2,1} + u_c), \quad Q_{\max} \triangleq P^{\frac{d_c-\epsilon}{2}} \\ &z_1' \triangleq z_1/(\varepsilon\sqrt{P^{1-2d_c}}) \\ &g \triangleq h_{11}v_{1,2} + h_{12}(v_{2,2} + u_{1,p}) + \frac{h_{12}h_{21}}{h_{22}}u_{2,p}. \end{aligned}$$

Based on our definitions, it is true that $q_1 \in \mathcal{Z} \cap [-Q_{\max}, Q_{\max}]$ and $q_2 \in \mathcal{Z} \cap [-2Q_{\max}, 2Q_{\max}]$. The notation g can be considered as a signal in the second layer, which is bounded. Specifically, based on (78)-(81), it is true that

$$\begin{aligned} |v_{1,2}| \leq& \gamma/2 \\ |u_{2,p}| \leq& \gamma/2 \\ |v_{2,2} + u_{1,p}| \leq& \gamma \end{aligned} \tag{83}$$

which imply that there exists a finite constant $g_{\max}$ such that

$$|g| \leq g_{\max}.$$

For the observation y_1' expressed in (82), we will show that q_1 and q_2 can be decoded from y_1' by treating g as noise, with vanishing error probability as P goes large. To do that, let us define the minimum distance of the constellation for the signal $\gamma P^{\frac{d_c+\epsilon}{2}}h_{11}q_1 + \gamma P^{\frac{d_c+\epsilon}{2}}h_{12}q_2$, which is defined by

$$d_{\min} \triangleq \min_{\substack{q_1, q_1' \in \mathcal{Z} \cap [-Q_{\max}, Q_{\max}] \\ q_2, q_2' \in \mathcal{Z} \cap [-2Q_{\max}, 2Q_{\max}] \\ (q_1, q_2) \neq (q_1', q_2')}} \gamma P^{\frac{d_c+\epsilon}{2}} \left| h_{11}(q_1 - q_1') + h_{12}(q_2 - q_2') \right|. \tag{84}$$

For the minimum distance $d_{\min}$ defined in (84), a result on the lower bound is provided in the following lemma.

Lemma 6. *Consider the minimum distance $d_{\min}$ defined in (84). For almost all realizations of channel coefficients, and for any small enough $\epsilon' > 0$, there exists a positive constant κ' such that*

$$d_{\min} \geq \kappa' P^{\epsilon'}.$$

Proof. See Appendix A-A, at the end of this section. □

Lemma 6 reveals that the minimum distance of the constellation for the signal $\gamma P^{\frac{d_c+\epsilon}{2}}h_{11}q_1 + \gamma P^{\frac{d_c+\epsilon}{2}}h_{12}q_2$ is large enough, compared to the interference g that is upper bounded by a finite constant. Thus, one can easily show that q_1 and q_2 (equivalently, $v_{1,1}$ and $v_{2,1} + u_c$) can be decoded from y_1' (cf. (82)) by treating g as noise, with vanishing error probability when P is sufficiently large. At this point, it can be concluded that for almost all realizations of channel coefficients the error probability of estimating $v_{1,1}$ from y_1 is

$$\Pr[v_{1,1} \neq \hat{v}_{1,1}] \to 0, \quad \text{as} \quad P \to \infty. \tag{85}$$

In the second step, after estimating the signals $v_{1,1}$ and $v_{2,1} + u_c$ in the first layer, we remove them from y_1 and then

estimate signals in the second layer. Specifically, we seek to estimate $v_{1,2}$ from the following observation

$$\begin{aligned} y_1'' \triangleq & y_1 - \varepsilon\sqrt{P}h_{11}v_{1,1} + \varepsilon\sqrt{P}h_{12}(v_{2,1}+u_c) \\ =& \varepsilon\sqrt{P^{1-2d_c}}\big(h_{11}v_{1,2}+h_{12}(v_{2,2}+u_{1,p})+\frac{h_{12}h_{21}}{h_{22}}u_{2,p}\big)+z_1 \\ =& \frac{\varepsilon\gamma}{2}P^{\frac{2(1-2d_c)/3+\epsilon}{2}}\big(h_{11}\bar{q}_1+h_{12}\bar{q}_2+\frac{h_{12}h_{21}}{h_{22}}\bar{q}_3\big)+z_1 \quad (86) \end{aligned}$$

for

$$\bar{q}_1 \triangleq \frac{2\bar{Q}_{\max}}{\gamma}v_{1,2}, \quad \bar{q}_2 \triangleq \frac{2\bar{Q}_{\max}}{\gamma}(v_{2,2}+u_{1,p})$$
$$\bar{q}_3 \triangleq \frac{2\bar{Q}_{\max}}{\gamma}u_{2,p}, \quad \bar{Q}_{\max} \triangleq P^{\frac{\frac{1-2d_c}{3}-\epsilon}{2}}.$$

It holds true that $\bar{q}_1, \bar{q}_3 \in \mathcal{Z} \cap [-\bar{Q}_{\max}, \bar{Q}_{\max}]$ and $q_2 \in \mathcal{Z} \cap [-2\bar{Q}_{\max}, 2\bar{Q}_{\max}]$. By following the analysis in the first step (cf. (82)-(85)), one can show that the minimum distance of the constellation for the signal $\frac{\varepsilon\gamma}{2}P^{\frac{2(1-2d_c)/3+\epsilon}{2}}\big(h_{11}\bar{q}_1 + h_{12}\bar{q}_2+\frac{h_{12}h_{21}}{h_{22}}\bar{q}_3\big)$ appeared in (86) is lower bounded by $\kappa''P^{\epsilon''}$ for some $\epsilon'' > 0$ and positive constant κ'', for almost all realizations of channel coefficients. Thus, one can easily show that $\bar{q}_1$, $\bar{q}_2$ and $\bar{q}_3$ can be decoded from y_1'' with vanishing error probability when P is sufficiently large. At this point, it can be concluded that for almost all realizations of channel coefficients the error probability of estimating $v_{1,2}$ from y_1 is

$$\Pr[v_{1,2} \neq \hat{v}_{1,2}] \to 0, \quad \text{as} \quad P \to \infty. \quad (87)$$

With (85) and (87), it implies that for almost all realizations of channel coefficients the error probability of estimating $v_{1,1}$ and $v_{1,2}$ from y_1 is

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

This completes the proof of Lemma 1 for the case of $k = 1$. Due to the symmetry, Lemma 1 also holds true for the case of $k = 2$.

A. Proof of Lemma 6

To prove Lemma 6, we will use the Khintchine-Groshev Theorem for Monomials[1], that is stated below, as in [50].

Theorem 3 (Khintchine-Groshev Theorem for Monomials)**.** *Let $\boldsymbol{h} = (h_1, h_2, \cdots, h_N) \in \mathcal{R}^N$, and $p_1, p_2, \cdots, p_M$ be distinct monomials generated by $\boldsymbol{h}$, for $N \leq M$. Then, for any $\epsilon > 0$ and almost all $\boldsymbol{h}$, there exists a positive constant κ such that*

$$\big|\sum_{i=1}^{M} p_i q_i\big| > \frac{\kappa}{\max_i |q_i|^{M-1+\epsilon}} \quad (88)$$

holds for all $(q_1, q_2, \cdots, q_M) \neq \mathbf{0} \in \mathcal{Z}^M$.

From the Khintchine-Groshev Theorem for Monomials, it implies that for any small enough $\epsilon > 0$, and for almost all realizations of channel coefficients, there exists a positive constant κ such that the minimum distance $d_{\min}$ defined in (84) is bounded by

$$\begin{aligned} d_{\min} \geq & \gamma P^{\frac{d_c+\epsilon}{2}} \frac{\kappa}{(4Q_{\max})^{2-1+\epsilon}} \\ = & \gamma P^{\frac{d_c+\epsilon}{2}} \frac{\kappa}{(4P^{\frac{d_c-\epsilon}{2}})^{1+\epsilon}} \\ = & \frac{\kappa\gamma}{4\times 4^{\epsilon}} \cdot P^{\epsilon(1-(d_c-\epsilon)/2)} \\ = & \kappa' P^{\epsilon'} \end{aligned} \quad (89)$$

where $Q_{\max} = P^{\frac{d_c-\epsilon}{2}}$, and ϵ' and κ' are defined as

$$\epsilon' \triangleq \epsilon(1-(d_c-\epsilon)/2), \quad \kappa' \triangleq \frac{\kappa\gamma}{4\times 4^{\epsilon}}.$$

In this setting, κ' is a finite constant and ϵ' is positive, given that $d_c \in [0, 1/2]$ and $\epsilon > 0$.

Appendix B
Proof of Lemma 2

In this section we provide the proof of Lemma 2. The term $\mathrm{I}(v_1; y_2|v_2)$ in (18) can be treated as a rate penalty, which can be bounded as

$$\begin{aligned} & \mathrm{I}(v_1; y_2|v_2) \\ \leq & \mathrm{I}(v_1; y_2, v_{1,1}+u_c, v_{1,2}+u_{2,p}|v_2) \quad (90) \\ = & \mathrm{I}(v_1; v_{1,1}+u_c, v_{1,2}+u_{2,p}) \\ & + \mathrm{I}(v_1; y_2|v_2, v_{1,1}+u_c, v_{1,2}+u_{2,p}) \quad (91) \\ = & \mathrm{I}(v_1; v_{1,1}+u_c, v_{1,2}+u_{2,p}) \\ & + \underbrace{\mathrm{I}(v_1; \varepsilon\sqrt{P^{1-2d_c}}\frac{h_{21}h_{12}}{h_{11}}u_{1,p}+z_2|v_2, v_{1,1}+u_c, v_{1,2}+u_{2,p})}_{=0} \\ = & \mathrm{I}(v_1; v_{1,1}+u_c, v_{1,2}+u_{2,p}) \quad (92) \\ = & \mathrm{H}(v_{1,1}+u_c, v_{1,2}+u_{2,p}) - \mathrm{H}(v_{1,1}+u_c, v_{1,2}+u_{2,p}|v_1) \\ = & \mathrm{H}(v_{1,1}+u_c) + \mathrm{H}(v_{1,2}+u_{2,p}) - \mathrm{H}(u_c) - \mathrm{H}(u_{2,p}) \quad (93) \\ \leq & \underbrace{\log(4\cdot P^{\frac{d_c-\epsilon}{2}}+1) - \log(2\cdot P^{\frac{d_c-\epsilon}{2}}+1)}_{\leq 1} \\ & + \underbrace{\log(4\cdot P^{\frac{(1-2d_c)/3-\epsilon}{2}}+1) - \log(2\cdot P^{\frac{(1-2d_c)/3-\epsilon}{2}}+1)}_{\leq 1} \quad (94) \\ \leq & 2 \quad (95) \end{aligned}$$

where (90) uses the fact that adding information does not decrease the mutual information; (91) and (93) follow from the facts that the random variables $v_{1,1}, v_{1,2}, v_2, u_c, u_{1,p}, u_{2,p}$ are mutually independent, and that $\{v_{k,p}, v_{k,c}\}$ can be reconstructed from v_k for $k = 1, 2$. The step in (92) uses the fact that both $u_{1,p}$ and z_2 are independent of the random variables $v_1, v_2, v_{1,1}+u_c$ and $v_{1,2}+u_{2,p}$. The step in (94) results from the derivations that

$$\begin{aligned} \mathrm{H}(u_c) = & \log(2\cdot P^{\frac{d_c-\epsilon}{2}}+1) \\ \mathrm{H}(u_{2,p}) = & \log(2\cdot P^{\frac{(1-2d_c)/3-\epsilon}{2}}+1) \\ \mathrm{H}(v_{1,1}+u_c) \leq & \log(4\cdot P^{\frac{d_c-\epsilon}{2}}+1) \\ \mathrm{H}(v_{1,2}+u_{2,p}) \leq & \log(4\cdot P^{\frac{(1-2d_c)/3-\epsilon}{2}}+1) \end{aligned}$$

[1]A function $f(\boldsymbol{h})$ is a monomial generated by $\boldsymbol{h} = (h_1, h_2, \cdots, h_N) \in \mathcal{R}^N$ if this function can be written as $f(\boldsymbol{h}) = \prod_{i=1}^{N} h_i^{\beta_i}$, for $\beta_i \in \mathbb{N}, \forall i \in [1:N]$.

given that

$$v_{1,1}, v_{2,1}, u_c \in \Omega(\xi = \frac{\gamma}{Q},\ Q = P^{\frac{d_c-\epsilon}{2}})$$

$$v_{2,2}, v_{2,2}, u_{1,p}, u_{2,p} \in \Omega(\xi = \frac{\gamma}{2Q},\ Q = P^{\frac{\frac{1}{3}(1-2d_c)-\epsilon}{2}})$$

(see (12) and (13)). The step in (95) follows from the identity that $\log(1+2a) - \log(1+a) \leq 1$ for $a > 0$. At this point we complete the proof of Lemma 2.

Appendix C
Proof of Lemma 4

In this section we provide the proof of Lemma 4.

A. Proof of bounds (52) and (53)

The bound in (52) is proved as follows

$$\begin{aligned}
&\mathrm{h}(\tilde{x}_1^n|w_c) - \mathrm{h}(s_{21}^n|w_c)\\
=&\mathrm{h}(\tilde{x}_1^n|w_c) - \mathrm{h}(\tilde{z}_1^n|w_c) + \mathrm{h}(z_2^n|w_c) - \mathrm{h}(s_{21}^n|w_c)\\
=&\mathrm{I}(\tilde{x}_1^n; x_1^n|w_c) - \mathrm{I}(s_{21}^n; x_1^n|w_c)\\
\leq&\mathrm{I}(\tilde{x}_1^n, s_{21}^n; x_1^n|w_c) - \mathrm{I}(s_{21}^n; x_1^n|w_c) \qquad (96)\\
=&\mathrm{I}(\tilde{x}_1^n; x_1^n|s_{21}^n, w_c)\\
=&\mathrm{h}(\tilde{x}_1^n|s_{21}^n, w_c) - \underbrace{\mathrm{h}(\tilde{x}_1^n|x_1^n, s_{21}^n, w_c)}_{=\mathrm{h}(\tilde{z}_1^n)}\\
=&\mathrm{h}(\tilde{x}_1^n|s_{21}^n, w_c) - \frac{n}{2}\log(2\pi e) \qquad (97)\\
\leq&\sum_{t=1}^{n}\mathrm{h}(\tilde{x}_1(t)|s_{21}(t)) - \frac{n}{2}\log(2\pi e) \qquad (98)\\
=&\sum_{t=1}^{n}\mathrm{h}\Big(\tilde{x}_1(t) - \frac{s_{21}(t)}{h_{21}}\big|s_{21}(t)\Big) - \frac{n}{2}\log(2\pi e)\\
\leq&\sum_{t=1}^{n}\mathrm{h}\Big(\tilde{z}_1(t) - \frac{z_2(t)}{h_{21}}\Big) - \frac{n}{2}\log(2\pi e) \qquad (99)\\
=&\frac{n}{2}\log\big(1 + \frac{1}{|h_{21}|^2}\big)
\end{aligned}$$

where (96) uses the fact that adding information does not decrease the mutual information; (97) follows from the derivation that $\mathrm{h}(\tilde{x}_1^n|x_1^n, s_{21}^n, w_c) = \mathrm{h}(\tilde{z}_1^n|x_1^n, s_{21}^n, w_c) = \mathrm{h}(\tilde{z}_1^n) = \frac{n}{2}\log(2\pi e)$; (98) and (99) hold true because conditioning reduces differential entropy. At this point, the bound in (52) is proved. Due to the symmetry, the bound in (53) can be proved in a similar way.

B. Proof of bound (54)

The bound in (54) is proved as follows

$$\begin{aligned}
&\mathrm{h}(y_1^n, y_2^n|\tilde{x}_1^n, \tilde{x}_2^n, w_c)\\
=&\mathrm{h}\Big(\{y_1(t) - h_{11}\tilde{x}_1(t) - h_{12}\tilde{x}_2(t)\}_{t=1}^n,\\
&\quad\{y_2(t) - h_{22}\tilde{x}_2(t) - h_{21}\tilde{x}_1(t)\}_{t=1}^n\big|\tilde{x}_1^n, \tilde{x}_2^n, w_c\Big)\\
\leq&\sum_{t=1}^{n}\mathrm{h}\big(z_1(t) - h_{11}\tilde{z}_1(t) - h_{12}\tilde{z}_2(t)\big)\\
&+\sum_{t=1}^{n}\mathrm{h}\big(z_2(t) - h_{22}\tilde{z}_2(t) - h_{21}\tilde{z}_1(t)\big) \qquad (100)\\
=&\frac{n}{2}\log\big(2\pi e\big(1 + |h_{11}|^2 + |h_{12}|^2\big)\big)\\
&+\frac{n}{2}\log\big(2\pi e\big(1 + |h_{22}|^2 + |h_{21}|^2\big)\big)
\end{aligned}$$

where (100) uses the fact that conditioning reduces differential entropy.

C. Proof of bounds (55) and (56)

For the bound in (55), the proof is given as

$$\begin{aligned}
\mathrm{h}(y_1^n|w_c) =&\sum_{t=1}^{n}\mathrm{h}(y_1(t)|y_1^{t-1}, w_c)\\
\leq&\sum_{t=1}^{n}\mathrm{h}(y_1(t)) \qquad (101)\\
\leq&\frac{n}{2}\log\big(2\pi e(1+P|h_{11}|^2+P|h_{12}|^2)\big) \qquad (102)
\end{aligned}$$

where (101) results from the fact that conditioning reduces differential entropy; and (102) holds true because Gaussian input maximizes the differential entropy.

For the bound in (56), it is proved as

$$\begin{aligned}
\mathrm{h}(y_1^n, \tilde{x}_1^n, \tilde{x}_2^n|y_2^n, w_1, w_c) \geq&\mathrm{h}(y_1^n, \tilde{x}_1^n, \tilde{x}_2^n|y_2^n, w_1, w_c, x_1^n, x_2^n) \qquad (103)\\
=&\mathrm{h}(z_1^n, \tilde{z}_1^n, \tilde{z}_2^n)\\
=&\frac{3n}{2}\log(2\pi e).
\end{aligned}$$

where (103) follows from the fact that conditioning reduces differential entropy. Now we complete the proof of Lemma 4.

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

[4] S. K. Leung-Yan-Cheong and M. E. Hellman, "Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451 – 456, Jul. 1978.

[5] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153 – 3167, May 2011.

[6] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian wiretap channel with helpers," in *Proc. Allerton Conf. Communication, Control and Computing*, Oct. 2012.

[7] ——, "Secure degrees of freedom of the Gaussian wiretap channel with helpers and no eavesdropper CSI: Blind cooperative jamming," in *47th Annual Conference on Information Sciences and Systems (CISS)*, Mar. 2013.

[8] M. Nafea and A. Yener, "Degrees of freedom of the single antenna Gaussian wiretap channel with a helper irrespective of the number of antennas at the eavesdropper," in *2013 IEEE Global Conference on Signal and Information Processing*, Dec. 2013.

[9] ——, "Secure degrees of freedom for the MIMO wiretap channel with a multiantenna cooperative jammer," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Nov. 2014.

[10] S.-H. Lee and A. Khisti, "The wiretapped diamond-relay channel," *IEEE Trans. Inf. Theory*, vol. 64, no. 11, pp. 7194 – 7207, Nov. 2018.

[11] J. Chen and C. Geng, "Optimal secure GDoF of symmetric Gaussian wiretap channel with a helper," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019.

[12] 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.

[13] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453 – 2469, Jun. 2008.

[14] J. Xu, Y. Cao, and B. Chen, "Capacity bounds for broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4529 – 4542, Oct. 2009.

[15] 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.

[16] Y. K. Chia and A. El Gamal, "Three-receiver broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 2748 – 2765, May 2012.

[17] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "The secrecy capacity region of the Gaussian MIMO broadcast channel," *IEEE Trans. Inf. Theory*, vol. 59, no. 5, pp. 2673 – 2682, May 2013.

[18] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735 – 2751, Jun. 2008.

[19] 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.

[20] 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.

[21] X. He and A. Yener, "A new outer bound for the Gaussian interference channel with confidential messages," in *Proc. 43rd Annu. Conf. Inf. Sci. Syst.*, Mar. 2009.

[22] ——, "Interference channels with strong secrecy," in *Proc. Allerton Conf. Communication, Control and Computing*, Sep. 2009.

[23] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "On the secure degrees-of-freedom of the multiple-access-channel," 2010, available on ArXiv: https://arxiv.org/pdf/1003.0729.pdf.

[24] 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.

[25] 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.

[26] X. He and A. Yener, "The Gaussian many-to-one interference channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2730 – 2745, May 2011.

[27] 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.

[28] E. Perron, S. Diggavi, and E. Telatar, "On noise insertion strategies for wireless network secrecy," in *Proc. Inf. Theory and App. Workshop (ITA)*, Feb. 2009.

[29] 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.

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

[31] 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.

[32] 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.

[33] 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.

[34] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550 – 1573, Aug. 2014.

[35] P. Mohapatra and C. R. Murthy, "Outer bounds on the secrecy rate of the 2-user symmetric deterministic interference channel with transmitter cooperation," in *Proc. 20th National Conference on Communications (NCC)*, 2014.

[36] J. Xie and S. Ulukus, "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.

[37] 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.

[38] 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.

[39] 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.

[40] C. Geng, N. Naderializadeh, A. S. Avestimehr, and S. A. Jafar, "On the optimality of treating interference as noise," *IEEE Trans. Inf. Theory*, vol. 61, no. 4, pp. 1753 – 1767, Apr. 2015.

[41] J. Chen, "New results on the secure capacity of symmetric two-user interference channels," in *Proc. Allerton Conf. Communication, Control and Computing*, Sep. 2016.

[42] 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.

[43] 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.

[44] J. Chen, "Secure communication over interference channel: To jam or not to jam?" in *Proc. Allerton Conf. Communication, Control and Computing*, Oct. 2018.

[45] R. Fritschek and G. Wunder, "On multiuser gain and the constant-gap sum capacity of the Gaussian interfering multiple access channel," 2017, available on ArXiv: https://arxiv.org/abs/1705.04514.

[46] F. Li and J. Chen, "How to break the limits of secrecy constraints in communication networks?" in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019.

[47] 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.

[48] J. Chen, "Secure communication over interference channel: To jam or not to jam?" Dec. 2019, to appear in *IEEE Trans. Inf. Theory*.

[49] F. Li and J. Chen, "Adding common randomness can remove the secrecy constraints in communication networks," available on ArXiv: https://arxiv.org/abs/1907.04599.

[50] 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.