Optimal Secure GDoF of Symmetric Gaussian Wiretap Channel with a Helper

Jinyuan Chen and Chunhua Geng

***Abstract*—We study a symmetric Gaussian wiretap channel with a helper, where a confidential message is sent from a transmitter to a legitimate receiver, in the presence of a helper and an eavesdropper, under a weak notion of secrecy constraint. For this setting, we characterize the optimal secure generalized degrees-of-freedom (GDoF). The result reveals that, adding a helper can significantly increase the secure GDoF of the wiretap channel. The result is supported by a new converse and a new scheme. In the proposed scheme, the helper sends a cooperative jamming signal at a specific power level and direction. In this way, it minimizes the penalty in GDoF incurred by the secrecy constraint. In the secure rate analysis, the techniques of noise removal and signal separation are used.**

***Index Terms*—Information-theoretic secrecy, wiretap channel, generalized degrees-of-freedom, cooperative jamming, secure capacity.**

I. Introduction

The study of information-theoretic secrecy dates back to Shannon's work of [1] in 1949. Since then, information-theoretic secrecy has been investigated in varying communication channels, e.g., the wiretap channels [2]–[4], multiple access channels with confidential messages and wiretap multiple access channels [5]–[12], the broadcast channels with confidential messages [13]–[18], and the interference channels with confidential messages [13], [19]–[39]. In those settings, the messages are transmitted over the channels with secrecy constraints, which often incur a penalty in capacity (cf. [10], [13], [19], [24], [25], [28], [29], [31], [33], [37], [38], [40]). One way to minimize the capacity penalty incurred by secrecy constraints is to add helper(s) into the channels (see, e.g., [25], [33], [34], [36], [39], [41]–[45]). Specifically, the work in [39] recently showed that adding a helper can *totally* remove the penalty in sum generalized degrees-of-freedom (GDoF), in a two-user symmetric Gaussian interference channel.

In this work, we consider secure communications over a Gaussian wiretap channel with a helper. In this setting, a confidential message sent from a transmitter to a legitimate receiver needs to be secure from an eavesdropper, in the presence of a helper. The wiretap channel and its variations have been considered as the basic channels for the investigation of information-theoretic secrecy. For example, the wiretap channel with a helper can be considered as a specific case of an interference channel with only one confidential message. The insights gained from the former can be very helpful in understanding the fundamental limits of the latter. For the Gaussian wiretap channel with one helper, the work in [45] provided both inner and outer bounds on the achievable secrecy rate at finite SNRs, where the achievability is based on unstructured Gaussian random codes and the derived inner and outer bounds do not match in general. In the wiretap channel with M helpers, the works in [25], [41] showed that the secure degrees-of-freedom (DoF) is $\frac{M}{M+1}$ for almost all channel gains. The result is derived under the assumption that perfect channel state information (CSI) is available at the transmitters. The work in [36], [42] then showed that the same secure DoF of $\frac{M}{M+1}$ is still achievable when the eavesdropper CSI is not available at the transmitters. Another work in [43] studied a Gaussian wiretap channel with a helper, where a single antenna is equipped at each of the transmitter and the legitimate receiver, while multiple antennas are equipped at each of the helper and the eavesdropper. The result in [43] revealed that the secure DoF $1/2$ is achievable irrespective of the number of antennas at the eavesdropper, as long as the number of antennas at the helper is the same as the number of antennas at the eavesdropper. In the setting of wiretap channel with a helper, the previous DoF results were generalized to the multiple-antenna scenario where multiple antennas are equipped at each node [33], [44]. The work in [44] used the assumption that perfect CSI is available at the transmitters, while the work in [33] used the assumption that the eavesdropper CSI is not available at the transmitters. In all of those previous works in [25], [33], [36], [41]–[44] (except for [45], which studied the secrecy rate at finite SNRs), the authors considered the secure DoF performance of the channels. The DoF metric is a form of capacity approximation. Under the DoF metric, all the non-zero channel gains are treated equally strong, at the regime of high signal-to-noise ratio (SNR). However, in the communication channels the capacity is usually affected by different channel strengths of different links. Therefore, it motivates us to go beyond the DoF metric and consider a better form of capacity approximation. GDoF metric is a generalization of DoF, which is able to capture the capacity behavior when different links have different channel strengths and is very helpful in understanding the capacity to within a constant gap (cf. [46]). The work in [34] studied the secure GDoF and secure capacity of the Gaussian wiretap channel with a helper, as well as the Gaussian multiple access wiretap channel, where channel gain from the first transmitter to the eavesdropper is the same as the channel gain from

Jinyuan Chen is with Louisiana Tech University, Department of Electrical Engineering, Ruston, USA (email: jinyuan@latech.edu). Chunhua Geng is with MediaTek USA Inc., Irvine, USA (email: chunhua.geng@mediatek.com).
This work was presented in part at the 2019 IEEE International Symposium on Information Theory. The work of Jinyuan Chen 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).

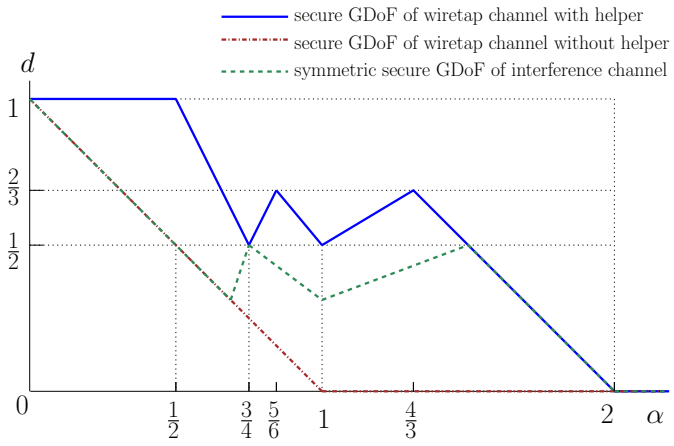

Fig. 1. Optimal secure GDoF vs. α for the symmetric Gaussian wiretap channels with and without a helper, where α denotes the ratio between the direct-links' channel strength (in decibel scale) and the cross-links' channel strength (in decibel scale). The direct-links refers to the link from the transmitter to its legitimate receiver, as well as the link from the helper to the eavesdropper, while the cross-links refers to the other two links, in this symmetric setting. The dash line with green color refers to the optimal symmetric secure GDoF vs. α for the symmetric Gaussian interference channel with confidential messages (cf. [37]).

the second transmitter to the eavesdropper. Note that, the setting considered in [34] has symmetric channel gains at the wiretapper, which is different from our setting considered in this work. Also note that, the secure GDoF upper bound and the lower bound provided in [34] are not matched for a certain range of channel parameters. In this work, we seek to characterize the *optimal* secure GDoF of a wiretap channel with a helper.

Specifically, the main contribution of this work is the *optimal* secure GDoF characterization of a symmetric wiretap channel with a helper, for all the channel parameters. The result reveals that, adding a helper can significantly increase the secure GDoF of the wiretap channel (see Fig. 1). The result is supported by a new converse and a new scheme. The converse is derived for the wiretap channel with a helper under the *general* channel parameters, i.e., the converse holds for the symmetric and asymmetric channels. In the proposed scheme,[1] the helper sends a cooperative jamming signal at a specific power level and direction. In this way, it minimizes the penalty in GDoF incurred by the secrecy constraint. In the proposed scheme, the signal of the transmitter is a superposition of a common signal, a middle signal, and a private signal. The power of private signal is low enough such that this signal arrives at the eavesdropper under the noise level. The power of the common signal and middle signal is above the noise level at the receivers. However, at the eavesdropper each of the common signal and middle signal is aligned at a specific power level and direction with the jamming signal sent from the helper, which minimizes the penalty in GDoF incurred by the secrecy constraint. Here the common signal and middle signal can be considered as the upper and lower parts of the common signal in [38], respectively. Comparing the achievable scheme of this paper with [38], the fundamental difference is that here we split the common signal in [38] into two parts and apply different transmit power levels and different pulse amplitude modulation (PAM) constellation sets to them to achieve the optimal secure GDoF for a certain regime. The optimal secure GDoF is described in different expressions for different interference regimes. For each interference regime, the power and rate levels of the signals in the proposed scheme are set to the optimal values, so as to achieve the optimal secure GDoF. In the secure rate analysis, the techniques of noise removal and signal separation are used (cf. [47], [48]). The secure GDoF result derived in this work can be extended to understand the secure capacity to within a constant gap, which will be investigated in the future work.

We will organize the rest of this work as follows. In Section II we will describe the channel model. In Section III, the main results of this work will be provided. The converse proof will be described in Section IV. The achievability proof will be shown in Section V and Section VI. In Section VII we will provide the conclusion. In terms of notations, we use $\mathbb{H}(\bullet)$ and $\mathbb{I}(\bullet)$ to represent the entropy and mutual information, respectively, and use $\mathrm{h}(\bullet)$ to represent differential entropy. $\mathcal{Z}$ and $\mathcal{Z}^+$ are used to denote the sets of integers and positive integers, respectively, while $\mathcal{R}$ is used to denote the set of real numbers. $(\bullet)^+ = \max\{0, \bullet\}$. When $f(s) = o(g(s))$ is used, it suggests that $\lim_{s\to\infty} f(s)/g(s) = 0$. All the logarithms are considered with base 2.

II. System Model

This work focuses on a Gaussian wiretap channel with a helper (see Fig. 2). In this setting, transmitter 1 sends a *confidential* message to receiver 1 (the legitimate receiver), in the presence of a helper (transmitter 2) and an eavesdropper (receiver 2). By following the common conventions in [37], [38], [48], the channel input-output relationship of this setting is described by

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

$$y_2(t) = \sqrt{P^{\alpha_{21}}} h_{21} x_1(t) + \sqrt{P^{\alpha_{22}}} h_{22} x_2(t) + z_2(t) \quad (1b)$$

where $y_k(t)$ denotes the received signal of receiver k at time t, $x_k(t)$ denotes the transmitted signal of transmitter k with a normalized power constraint $\mathbb{E}|x_k(t)|^2 \le 1$, and $z_k(t) \sim \mathcal{N}(0,1)$ denotes the additive white Gaussian noise. $\sqrt{P^{\alpha_{k\ell}}} h_{k\ell}$ represents the channel gain of the link from transmitter ℓ to receiver k, for $\ell, k = 1, 2$. The nonnegative parameter $\alpha_{k\ell}$ captures the *link strength* of the channel from transmitter ℓ to receiver k. $h_{k\ell} \in (1, 2]$ is a parameter of the channel gain. In this setting, $P \ge 1$ captures the base of signal-to-noise ratio of all the links. Since the form of $\sqrt{P^{\alpha_{k\ell}}} h_{k\ell}$ can describe any real channel gain greater than 1, the above model can describe the general channels (focusing on the cases with channel gains greater than 1) in terms of capacity approximation. In this setting, all the nodes are assumed to know all the channel parameters $\{\alpha_{k\ell}, h_{k\ell}\}_{k,\ell}$.[2] When we consider the *symmetric*

[1] Although in this paper, for illustration simplicity, the achievable scheme is mainly discussed for the symmetric settings, the key ideas could be generalized to asymmetric channels as well.

[2] The availability of the CSI of the eavesdropper links can be justified when the eavesdropper is a legitimate user in the network, as in the case of interference channels with confidential messages [25], [38].

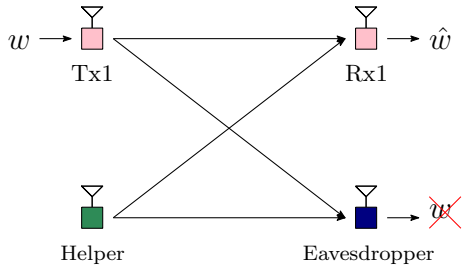

Fig. 2. A Gaussian wiretap channel with a helper, where transmitter 1 sends a *confidential* message w to receiver 1, in the presence of a helper (transmitter 2) and an eavesdropper (receiver 2).

case, we will assume that

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

In this setting, transmitter 1 sends a message w to its legitimate receiver over n channel uses, where w is chosen uniformly from the set $\mathcal{W} \triangleq \{1, 2, 3, \cdots, 2^{nR}\}$. When transmitting the confidential message from transmitter 1, a stochastic function

$$f_1 : \mathcal{W}_0 \times \mathcal{W} \to \mathcal{R}^n$$

maps $w \in \mathcal{W}$ to the signal $x_1^n = f_1(w_0, w) \in \mathcal{R}^n$, where the randomness in this mapping is represented by $w_0 \in \mathcal{W}_0$. We assume that w_0 and w are independent. At the helper (transmitter 2), another function

$$f_2 : \mathcal{W}_h \to \mathcal{R}^n$$

generates a random signal $x_2^n = f_2(w_h) \in \mathcal{R}^n$, where $w_h \in \mathcal{W}_h$ is a random variable that is independent of w_0 and w. We assume that w_0 is available at the first transmitter only, while w_h is available at the second transmitter only. We say a secure rate R is achievable if there exists a sequence of codes with n-length, such that the legitimate receiver can reliably decode the message w, i.e.,

$$\Pr[w \neq \hat{w}] \leq \epsilon \tag{2}$$

for any $\epsilon > 0$, and the message is secure from the eavesdropper, i.e.,

$$\mathbb{I}(w; y_2^n) \leq n\epsilon. \tag{3}$$

The above secrecy constraint is also known as a weak notion of secrecy constraint. We will use $C(\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22}, P)$ to denote the secure capacity, which is defined as the maximal secure rate that is achievable. We will use $d(\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22})$ to denote the secure GDoF, which is defined as

$$d(\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22}) \triangleq \lim_{P \to \infty} \frac{C(\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22}, P)}{\frac{1}{2} \log P}. \tag{4}$$

GDoF is a form of the approximation of capacity. In this setting, DoF is a particular case of GDoF by considering only one point with $\alpha_{12} = \alpha_{21} = \alpha_{22} = \alpha_{11} = 1$.

III. Main result

The main result of this paper is the characterization of the optimal secure GDoF value for the symmetric wiretap channel with a helper defined in Section II.

Theorem 1. *Consider the* symmetric *Gaussian wiretap channel with a helper defined in Section II, with* $\alpha_{12} = \alpha_{21} = \alpha$ *and* $\alpha_{22} = \alpha_{11} = 1$. *For almost all channel coefficients* $\{h_{k\ell}\} \in (1, 2]^{2\times 2}$, *the optimal secure GDoF is characterized as*

$$d(\alpha) = \begin{cases} 1 & \text{for } 0 \leq \alpha \leq 1/2 & \text{(5a)} \\ 2 - 2\alpha & \text{for } 1/2 \leq \alpha \leq 3/4 & \text{(5b)} \\ 2\alpha - 1 & \text{for } 3/4 \leq \alpha \leq 5/6 & \text{(5c)} \\ 3/2 - \alpha & \text{for } 5/6 \leq \alpha \leq 1 & \text{(5d)} \\ \alpha/2 & \text{for } 1 \leq \alpha \leq 4/3 & \text{(5e)} \\ 2 - \alpha & \text{for } 4/3 \leq \alpha \leq 2 & \text{(5f)} \\ 0 & \text{for } 2 \leq \alpha\,. & \text{(5g)} \end{cases}$$

Proof. The converse follows from Lemma 1 and Corollary 2 described in Section IV. Specifically, Lemma 1 provides some upper bounds on the secure *rate* of the Gaussian wiretap channel with a helper, under *general* channel parameters. Corollary 2 is the GDoF result derived from Lemma 1, in the setting of *symmetric* Gaussian wiretap channel with a helper. The achievability based on cooperative jamming is described in Sections V and VI. □

Remark 1. *In Fig. 1, for the wiretap channel* without *a helper (removing transmitter 2), the secure GDoF, denoted by* d_{no}, *is given by*

$$d_{no}(\alpha) = (1 - \alpha)^+ \quad \forall \alpha \in [0, \infty)$$

(see Appendix F for details). Comparing $d_{no}(\alpha)$ *with* $d(\alpha)$ *in Theorem 1, one can find that adding a helper significantly increases the secure GDoF of the wiretap channel.*

Remark 2. *From Fig. 1, it is not hard to verify that for all* α *values, the sum secure GDoF of two-user symmetric interference channels with confidential messages is no less than the secure GDoF of symmetric wiretap channel with a helper (surprisingly, for a large regime of* $\frac{3}{2} \leq \alpha < 2$, *the former is the double of the latter). This indicates that in a two-user symmetric interference channel with confidential messages, acting one of the transmitter as a pure helper (i.e., not sending its own confidential message) does not improve the sum secure GDoF.*

Our achievability scheme is based on pulse amplitude modulation, superposition coding, cooperative jamming, and alignment techniques. Specifically, the transmitted signal of transmitter 1 is a superposition of a *common signal* (denoted by v_c), a *middle signal* (denoted by v_m), and a *private signal* (denoted by v_p). The power of private signal is low enough such that this signal arrives at the eavesdropper under the noise level. The power of the common signal is higher than that of the middle signal, and both signals are above the noise level at the receivers. The transmitted signal of

TABLE I
SIGNAL DESIGN FOR DIFFERENT CASES, WHERE "✓" MEANS THAT THE SIGNAL WILL BE SENT AND "×" MEANS THAT THE SIGNAL WON'T BE SENT.

	$0 \le \alpha \le \frac{1}{2}$	$\frac{1}{2} \le \alpha \le \frac{3}{4}$	$\frac{3}{4} \le \alpha \le \frac{5}{6}$	$\frac{5}{6} \le \alpha \le 1$	$1 \le \alpha \le \frac{4}{3}$	$\frac{4}{3} \le \alpha \le 2$
(v_c, u_c)	×	×	✓	✓	✓	✓
(v_m, u_p)	✓	✓	✓	✓	×	×
v_p	✓	✓	✓	✓	×	×

the helper (transmitter 2) is a superposition of a *common jamming signal* (denoted by u_c) and a *private jamming signal* (denoted by u_p). The common signal v_c is aligned with the common jamming signal u_c at the eavesdropper at a specific power level and direction, while the middle signal v_m is aligned with the private jamming signal u_p at the eavesdropper, again, at a specific power level and direction. One difference between the common and private jamming signals is that, the latter arrives at the legitimate receiver under the noise level. Therefore, the signal u_p will *not* cause much interference at the legitimate receiver, while the signal u_c will create significant interference at the legitimate receiver, which we intend to minimize to improve the achievable secrecy rate. Different from the common and the middle signals, the *private signal* is not required to be aligned with the jamming signal at the eavesdropper, because it arrives at the eavesdropper under the noise level. Depending on different regimes of α, some signals are not needed and are thus set as empty signals. Table I gives a summary of the signal design. Note that (v_c, u_c) is considered as a pair of signals, and (v_m, u_p) is considered as another pair of signals, due to our alignment design. With the above signal design, our scheme achieves the optimal secure GDoF value. More details of the achievability scheme can be found in Sections V and VI.

Remark 3. *Essentially, here the common signal v_c and middle signal v_m can be regarded as the upper and lower parts of the common signal $v_{1,c}$ in [38], respectively. Comparing the achievable scheme of this paper with [38], the fundamental difference is that here we split the common signal $v_{1,c}$ in [38] into two parts, i.e., the* upper *part (or the common signal) v_c and the* lower *part (or the middle signal) v_m, and apply different transmit power levels (depending on β in Section V) and PAM constellation sets (depending on λ in Section V) to them to achieve the optimal secure GDoF for the regime $\frac{3}{4} < \alpha < 1$. See the two columns $\frac{3}{4} \le \alpha \le \frac{5}{6}$ and $\frac{5}{6} \le \alpha \le 1$ in Table II of Section V, where different β (i.e., β_c and β_m) and λ (i.e., λ_c and λ_m) values are applied to common and middle signals, respectively. Notably, the transmit power level of the common signal is larger than that of the middle signal, i.e., $-\beta_c \ge -\beta_m$. This flexible design enables that the helper could use a weaker private jamming signal u_p to align with the middle signal at the eavesdropper and only incur interference that is under the noise floor of the legitimate receiver, which is the key to achieve the optimal secure GDoF. This design is different from the achievable scheme in [38], where sophisticated common signal splitting is not needed and the same power and constellation set is applied to the whole of the common signal $v_{k,c}$ (In each column of Table I in [38], there is only one single value of $\beta_{v_{k,c}}$ and $\lambda_{v_{k,c}}$). Also, it is notable that in the regime of $0 \le \alpha \le \frac{3}{4}$ and $1 \le \alpha \le 2$, a smart splitting of the common signal $v_{1,c}$ in [38] is not needed to achieve the optimal secure GDoF. In the columns of $0 \le \alpha \le \frac{1}{2}$, $\frac{1}{2} \le \alpha \le \frac{3}{4}$, $1 \le \alpha \le \frac{4}{3}$ and $\frac{4}{3} \le \alpha \le 2$ of Table II in Section V, we have either $(\beta_c = \infty, \lambda_c = 0)$ or $(\beta_m = \infty, \lambda_m = 0)$, which means that either the common signal v_c or the middle signal v_m is empty.*

Remark 4. *In this paper, besides the achievability, we also provide an information theoretic upper bound matching the derived lower bound, and fully characterize the secure GDoF for the symmetric Gaussian wiretap channel with a helper. Our converse is based on genie-aided techniques. Specifically, we enhance the setting by using the following two approaches: a) adding noise with a certain power to the observation of eavesdropper; b) adding information to the legitimate receiver. By using these genie-aided techniques, and with careful manipulation, we are able to derive a new converse bound on secure GDoF that are optimal in this wiretap channel with a helper.*

IV. CONVERSE

For the Gaussian wiretap channel with a helper defined in Section II, we provide a general upper bound on the secure rate, which is stated in the following Lemma 1.

Lemma 1. *For the Gaussian wiretap channel with a helper defined in Section II, letting $\phi_1 \triangleq (\alpha_{12} - (\alpha_{22} - \alpha_{21})^+)^+$ and $\phi_3 \triangleq \min\{\alpha_{21}, \alpha_{12}, (\alpha_{11} - \phi_1)^+\}$, the secure rate is upper bounded by*

$$R \le \frac{1}{2}\log\Big(1 + P^{\alpha_{11}-\phi_3}\frac{|h_{11}|^2}{|h_{21}|^2} + P^{\alpha_{12}-(\alpha_{22}-\alpha_{21})^+}\frac{|h_{12}|^2}{|h_{22}|^2}\Big) + \frac{1}{2}\log\big(1 + P^{\phi_3-\phi_1}|h_{22}|^2\big) + 7.3 \tag{6}$$

$$R \le \frac{1}{2}\Big(\frac{1}{2}\log\big(1 + \frac{P^{(\alpha_{11}-\alpha_{21})^+}}{|h_{21}|^2}\big) + \frac{1}{2}\log\big(1 + \frac{P^{(\alpha_{22}-\alpha_{12})^+}}{|h_{12}|^2}\big) + \frac{1}{2}\log\big(1 + P^{\alpha_{11}}|h_{11}|^2 + P^{\alpha_{12}}|h_{12}|^2\big) + \log 9\Big) \tag{7}$$

$$R \le \frac{1}{2}\log\Big(1 + P^{\alpha_{11}-\alpha_{21}}\frac{|h_{11}|^2}{|h_{21}|^2} + P^{\alpha_{22}+\alpha_{11}-\alpha_{21}}\frac{|h_{11}|^2|h_{22}|^2}{|h_{21}|^2}\Big). \tag{8}$$

The proof of Lemma 1 is provided in the following subsections. Our converse is based on genie-aided techniques. Specifically, we enhance the setting by using the following two approaches. a) Adding noise with a certain power to the

observation of eavesdropper. See (23) later on, where $y_2(t)$ becomes $\bar{y}_2(t)$, which is a noisy version of $y_2(t)$. b) Adding information to the legitimate receiver. See (21) and (28) later on. The converse also builds on some bounds on the difference of conditional differential entropy of an interference channel (see Lemmas 3 and 4 later on). More details of the converse proof are provided in the following subsections.

Based on Lemma 1, we provide the secure GDoF upper bound in the following corollary.

Corollary 1. *For the Gaussian wiretap channel with a helper defined in Section II, the secure GDoF is upper bounded by*

$$\begin{aligned} &d(\alpha_{11},\alpha_{12},\alpha_{21},\alpha_{22}) \\ &\le \min\Big\{\underbrace{\max\{\phi_1,(\alpha_{11}-\phi_3)^+\}+(\phi_3-\phi_1)^+}_{Bound\ 1}, \\ &\underbrace{\frac{1}{2}\big((\alpha_{11}-\alpha_{21})^+ + (\alpha_{22}-\alpha_{12})^+ + \max\{\alpha_{11},\alpha_{12}\}\big)}_{Bound\ 2}, \\ &\underbrace{(\alpha_{22}+\alpha_{11}-\alpha_{21})^+}_{Bound\ 3}\Big\}. \end{aligned} \tag{9}$$

Proof. The first bound $d \le \max\{\phi_1,(\alpha_{11}-\phi_3)^+\}+(\phi_3-\phi_1)^+$ follows from the bound in (6). The second bound follows from the bound in (7) and the last bound follows from the bound in (8). □

The following result is a simplified version of Corollary 1 for the symmetric setting with $\alpha_{11}=\alpha_{22}=1, \alpha_{21}=\alpha_{12}=\alpha$.

Corollary 2. *For the symmetric Gaussian wiretap channel with a helper defined in Section II, with $\alpha_{11}=\alpha_{22}=1, \alpha_{21}=\alpha_{12}=\alpha$, the secure GDoF is upper bounded by*

$$d(\alpha) \le \begin{cases} 1 & for\ \ 0\le\alpha\le 1/2 \\ 2-2\alpha & for\ \ 1/2\le\alpha\le 3/4 \\ 2\alpha-1 & for\ \ 3/4\le\alpha\le 5/6 \\ 3/2-\alpha & for\ \ 5/6\le\alpha\le 1 \\ \alpha/2 & for\ \ 1\le\alpha\le 4/3 \\ 2-\alpha & for\ \ 4/3\le\alpha\le 2 \\ 0 & for\ \ 2\le\alpha\ . \end{cases}$$

Proof. See Appendix G. □

In what follows, we provide the proof of Lemma 1. At first, for $k,\ell\in\{1,2\}, k\neq\ell$ we define that

$$\phi_1 \triangleq (\alpha_{12}-(\alpha_{22}-\alpha_{21})^+)^+ \tag{11}$$
$$\phi_2 \triangleq (\alpha_{11}-\phi_1)^+ \tag{12}$$
$$\phi_3 \triangleq \min\{\alpha_{21},\alpha_{12},\phi_2\} \tag{13}$$
$$s_{kk}(t) \triangleq \sqrt{P^{(\alpha_{kk}-\alpha_{k\ell})^+}}h_{kk}x_k(t)+\tilde{z}_k(t) \tag{14}$$
$$s_{\ell k}(t) \triangleq \sqrt{P^{\alpha_{\ell k}}}h_{\ell k}x_k(t)+z_\ell(t) \tag{15}$$
$$\bar{x}_1(t) \triangleq \sqrt{P^{\min\{\alpha_{21},\alpha_{12},\alpha_{11}-\phi_1\}}}h_{21}x_1(t)+\bar{z}_3(t) \tag{16}$$
$$\bar{x}_2(t) \triangleq \sqrt{P^{\phi_3}}\tilde{z}_2(t)+\bar{z}_4(t) \tag{17}$$

and

$$\begin{aligned} \bar{y}_2(t) &\triangleq \sqrt{P^{-(\alpha_{21}-\phi_3)}}y_2(t)+\bar{z}_2(t) \\ &= \sqrt{P^{\phi_3}}h_{21}x_1(t)+\sqrt{P^{\alpha_{22}-(\alpha_{21}-\phi_3)}}h_{22}x_2(t) \\ &\quad +\sqrt{P^{-(\alpha_{21}-\phi_3)}}z_2(t)+\bar{z}_2(t) \end{aligned} \tag{18}$$

where $\tilde{z}_1(t),\tilde{z}_2(t),\bar{z}_2(t),\bar{z}_3(t),\bar{z}_4(t)\sim\mathcal{N}(0,1)$ are i.i.d. noise random variables that are independent of the other noise random variables and transmitted signals $\{x_1(t),x_2(t)\}_t$. Let $s_{kk}^n \triangleq \{s_{kk}(t)\}_{t=1}^n$, $s_{\ell k}^n \triangleq \{s_{\ell k}(t)\}_{t=1}^n$, $\bar{x}_k^n \triangleq \{\bar{x}_k(t)\}_{t=1}^n$ and $\bar{y}_2^n \triangleq \{\bar{y}_2(t)\}_{t=1}^n$.

A. Proof of bound (6)

Let us focus on the proof of bound (6). For the channel defined in Section II, the secure rate is bounded as follows:

$$\begin{aligned} nR &= \mathbb{H}(w) \\ &= \mathbb{I}(w;y_1^n)+\mathbb{H}(w|y_1^n) \\ &\le \mathbb{I}(w;y_1^n)+n\epsilon_{1,n} && (19)\\ &\le \mathbb{I}(w;y_1^n)-\mathbb{I}(w;y_2^n)+n\epsilon_{1,n}+n\epsilon && (20)\\ &\le \mathbb{I}(w;y_1^n,s_{22}^n)-\mathbb{I}(w;y_2^n)+n\epsilon_{1,n}+n\epsilon && (21)\\ &= \underbrace{\mathbb{I}(w;s_{22}^n)}_{=0}+\mathbb{I}(w;y_1^n|s_{22}^n)-\mathbb{I}(w;y_2^n)+n\epsilon_{1,n}+n\epsilon \\ &= \mathbb{I}(w;y_1^n|s_{22}^n)-\mathbb{I}(w;y_2^n)+n\epsilon_{1,n}+n\epsilon && (22)\\ &\le \mathbb{I}(w;y_1^n|s_{22}^n)-\mathbb{I}(w;\bar{y}_2^n)+n\epsilon_{1,n}+n\epsilon && (23) \end{aligned}$$

where (19) follows from Fano's inequality; (20) results from secrecy constraint in (3), i.e., $\mathbb{I}(w;y_2^n)\le n\epsilon$ for an arbitrary small ϵ; (21) uses the fact that adding information will not reduce the mutual information; (22) follows from the fact that w is independent of x_2^n and s_{22}^n (cf. (14)); (23) stems from the fact that $w\to y_2^n\to\bar{y}_2^n$ forms a Markov chain, which implies that $\mathbb{I}(w;y_2^n)\ge\mathbb{I}(w;\bar{y}_2^n)$.

We invoke the following lemma to bound $\mathbb{I}(w;\bar{y}_2^n)$ appeared in (23).

Lemma 2. *For $s_{22}(t)$ and $\bar{y}_2(t)$ defined in* (14) *and* (18)*, the following inequality holds true*

$$\mathbb{I}(w;\bar{y}_2^n) \ge \mathbb{I}(w;\bar{y}_2^n|s_{22}^n)-\frac{n}{2}\log 14. \tag{24}$$

Proof. The proof of this lemma is provided in Appendix A. □

Then, by incorporating the result of Lemma 2 into (23), it gives

$$\begin{aligned} &nR-\frac{n}{2}\log 14-n\epsilon_{1,n}-n\epsilon \\ \le&\mathbb{I}(w;y_1^n|s_{22}^n)-\mathbb{I}(w;\bar{y}_2^n|s_{22}^n) \\ =&\mathrm{h}(y_1^n|s_{22}^n)-\mathrm{h}(\bar{y}_2^n|s_{22}^n)+\mathrm{h}(\bar{y}_2^n|s_{22}^n,w)-\mathrm{h}(y_1^n|s_{22}^n,w) \\ =&\mathrm{h}(y_1^n|s_{22}^n)-\mathrm{h}(\bar{y}_2^n|s_{22}^n)+\mathrm{h}(\bar{y}_2^n,s_{22}^n|w)-\mathrm{h}(y_1^n,s_{22}^n|w) \end{aligned} \tag{25}$$

where (25) uses the identities that $\mathrm{h}(\bar{y}_2^n|s_{22}^n,w) = \mathrm{h}(\bar{y}_2^n,s_{22}^n|w)-\mathrm{h}(s_{22}^n|w)$ and $\mathrm{h}(y_1^n|s_{22}^n,w)=\mathrm{h}(y_1^n,s_{22}^n|w)-\mathrm{h}(s_{22}^n|w)$. For the first two terms in (25), we have an upper bound that is stated in the following lemma.

Lemma 3. *For $s_{22}(t)$ and $\bar{y}_2(t)$ defined in* (14) *and* (18)*, the following inequality holds true*

$$\begin{aligned}&\mathrm{h}(y_1^n|s_{22}^n)-\mathrm{h}(\bar{y}_2^n|s_{22}^n)\\ \le&\frac{n}{2}\log\Big(1+P^{\alpha_{11}-\phi_3}\cdot\frac{|h_{11}|^2}{|h_{21}|^2}+P^{\alpha_{12}-(\alpha_{22}-\alpha_{21})^+}\cdot\frac{|h_{12}|^2}{|h_{22}|^2}\Big)\\ &+\frac{n}{2}\log 10.\end{aligned}$$

Proof. The proof of this lemma is provided in Appendix B. □

For the last two terms in (25), we have an upper bound that is stated in the following lemma.

Lemma 4. *For $y_2(t)$ defined in* (1)*, and $s_{22}(t)$ defined in* (14)*, the following inequality holds true*

$$\begin{aligned}&\mathrm{h}(\bar{y}_2^n,s_{22}^n|w)-\mathrm{h}(y_1^n,s_{22}^n|w)\\ \le&\frac{n}{2}\log\big(1+P^{\phi_3-\phi_1}|h_{22}|^2\big)+\frac{n}{2}\log 168.\end{aligned}\tag{26}$$

Proof. The proof of this lemma is provided in Appendix C. □

Finally, by incorporating the results of Lemmas 3 and 4 into (25), the secure rate is bounded by

$$\begin{aligned}R\le&\frac{1}{2}\log\Big(1+P^{\alpha_{11}-\phi_3}\frac{|h_{11}|^2}{|h_{21}|^2}+P^{\alpha_{12}-(\alpha_{22}-\alpha_{21})^+}\frac{|h_{12}|^2}{|h_{22}|^2}\Big)\\ &+\frac{1}{2}\log\big(1+P^{\phi_3-\phi_1}|h_{22}|^2\big)+7.3+\epsilon_{1,n}+\epsilon.\end{aligned}$$

Letting $n\to\infty,\ \epsilon_{1,n}\to 0,\ \epsilon_{2,n}\to 0$ and $\epsilon\to 0$, we get the desired bound (6).

B. Proof of bound (7)

Let us now prove the bound (7). Let

$$\tilde{x}_k(t)\triangleq\sqrt{P^{\max\{\alpha_{kk},\alpha_{\ell k}\}}}x_k(t)+\tilde{z}_k(t)$$

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

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

for $k,\ell\in\{1,2\},k\neq\ell$ (cf. (15)) Beginning with Fano's inequality, the secure rate is bounded as:

$$\begin{aligned}&nR-n\epsilon_{1,n}\\ \le&\mathbb{I}(w;y_1^n)\\ \le&\mathbb{I}(w;y_1^n)-\mathbb{I}(w;y_2^n)+n\epsilon &(27)\\ \le&\mathbb{I}(w;y_1^n,\tilde{x}_1^n,\tilde{x}_2^n,y_2^n)-\mathbb{I}(w;y_2^n)+n\epsilon &(28)\\ =&\mathrm{h}(\tilde{x}_1^n,\tilde{x}_2^n)-\mathrm{h}(y_2^n)+\mathrm{h}(y_1^n,y_2^n|\tilde{x}_1^n,\tilde{x}_2^n)\\ &-\mathrm{h}(y_1^n,\tilde{x}_1^n,\tilde{x}_2^n|y_2^n,w)+n\epsilon\\ \le&\mathrm{h}(\tilde{x}_1^n,\tilde{x}_2^n)-\mathrm{h}(s_{21}^n)+\mathrm{h}(y_1^n,y_2^n|\tilde{x}_1^n,\tilde{x}_2^n)\\ &-\mathrm{h}(y_1^n,\tilde{x}_1^n,\tilde{x}_2^n|y_2^n,w)+n\epsilon &(29)\end{aligned}$$

where (27) results from a secrecy constraint (cf. (3)); (28) stems from the fact that adding information does not decrease the mutual information; (29) follows from the derivation that $\mathrm{h}(y_2^n)\ge\mathrm{h}(y_2^n|x_2^n)=\mathrm{h}(s_{21}^n)$. Note that $y_2(t)=\sqrt{P^{\alpha_{22}}}h_{22}x_2(t)+s_{21}(t)$. On the other hand, we have

$$\begin{aligned}nR\le&\mathbb{I}(x_1^n;y_1^n)+n\epsilon_{1,n} &(30)\\ =&\mathrm{h}(y_1^n)-\mathrm{h}(s_{12}^n|x_1^n)+n\epsilon_{1,n} &(31)\\ =&\mathrm{h}(y_1^n)-\mathrm{h}(s_{12}^n)+n\epsilon_{1,n} &(32)\end{aligned}$$

where (30) follows from the Markov chain of $w\to x_1^n\to y_1^n$; (31) results from the fact that $y_1(t)=\sqrt{P^{\alpha_{11}}}h_{11}x_1(t)+s_{12}(t)$; (32) follows from the independence between x_1^n and s_{12}^n. Finally, by combining (29) and (32), it gives

$$\begin{aligned}&2nR-2n\epsilon_{1,n}-n\epsilon\\ \le&\mathrm{h}(\tilde{x}_1^n)-\mathrm{h}(s_{21}^n)+\mathrm{h}(\tilde{x}_2^n)-\mathrm{h}(s_{12}^n)+\mathrm{h}(y_1^n)\\ &+\mathrm{h}(y_1^n,y_2^n|\tilde{x}_1^n,\tilde{x}_2^n)-\mathrm{h}(y_1^n,\tilde{x}_1^n,\tilde{x}_2^n|y_2^n,w).\end{aligned}\tag{33}$$

At this point, by following the steps from (171)-(176) in [38], we end up with

$$\begin{aligned}&2R+2\epsilon_{1,n}-\epsilon\\ \le&\frac{1}{2}\log\big(1+\frac{P^{(\alpha_{11}-\alpha_{21})^+}}{|h_{21}|^2}\big)+\frac{1}{2}\log\big(1+\frac{P^{(\alpha_{22}-\alpha_{12})^+}}{|h_{12}|^2}\big)\\ &+\frac{1}{2}\log\big(1+P^{\alpha_{11}}|h_{11}|^2+P^{\alpha_{12}}|h_{12}|^2\big)+\log 9.\end{aligned}$$

By setting $n\to\infty,\ \epsilon_{1,n}\to 0$ and $\epsilon\to 0$, it gives bound (7).

C. Proof of bound (8)

Bound (8) is directly from [38, Lemma 8].

V. Achievability

This section focuses on the *symmetric* Gaussian wiretap channel with a helper defined in Section II. Note that we consider the symmetric channel mainly for illustration simplicity. The key ideas of the achievable scheme presented in this section could be generalized to asymmetric settings as well. For this channel, we will provide a cooperative jamming scheme to achieve the optimal secure GDoF expressed in Theorem 1. The proposed scheme will use PAM modulation and signal alignment. The details of the scheme are described as follows.

1) Codebook: At transmitter 1, a codebook is generated as

$$\begin{aligned}\mathcal{B}\triangleq\big\{&v^n(w,w_0):w\in\{1,2,\cdots,2^{nR}\},\\ &w_0\in\{1,2,\cdots,2^{nR_0}\}\big\}\end{aligned}\tag{34}$$

with v^n being the codewords. All the codewords' elements are independent and identically generated according to a specific distribution. R and R_0 are the rates of the confidential message w and the confusion message w_0, respectively. The purpose of using the confusion message is to guarantee the security of the confidential message. The message will be mapped to a codeword under the following two steps. First, given the message w, a sub-codebook $\mathcal{B}(w)$ is selected, where $\mathcal{B}(w)$ is defined as

$$\mathcal{B}(w)\triangleq\big\{v^n(w,w_0):\ w_0\in\{1,2,\cdots,2^{nR_0}\}\big\}.$$

Second, transmitter 1 *randomly* selects a codeword from the selected sub-codebook based on a uniform distribution. Then,

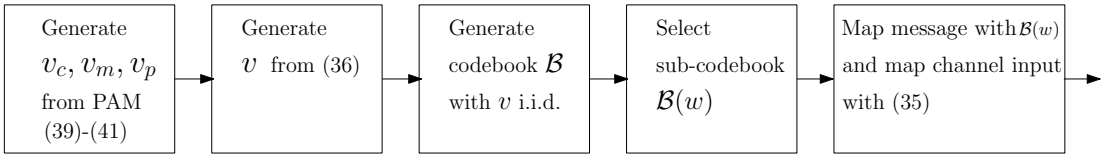

Fig. 3. A schematic representation of the proposed scheme, focusing on transmitter 1.

the channel input is mapped from selected codeword v^n such that

$$x_1(t) = h_{22}v(t) \tag{35}$$

for $t = 1, 2, \cdots, n$, where $v(t)$ denotes the tth element of v^n.

2) Constellation and alignment: In the proposed scheme, each codeword v^n is generated such that each element takes the following form

$$v(t) = \sqrt{P^{-\beta_c}} \cdot v_c(t) + \sqrt{P^{-\beta_m}} \cdot v_m(t) + \sqrt{P^{-\beta_p}} \cdot v_p(t) \tag{36}$$

which suggests that the input x_1 in (35) can be described as

$$x_1 = \sqrt{P^{-\beta_c}} h_{22} v_c + \sqrt{P^{-\beta_m}} h_{22} v_m + \sqrt{P^{-\beta_p}} h_{22} v_p \tag{37}$$

without the time index for simplicity (same for the next signal descriptions). For transmitter 2 (the helper), the transmitted signal is a cooperative jamming signal designed as

$$x_2 = \sqrt{P^{\alpha-1-\beta_c}} h_{21} u_c + \sqrt{P^{\alpha-1-\beta_m}} h_{21} u_p. \tag{38}$$

For the above transmitted signals, the random variables v_c, v_m, v_p, u_c and u_p are *independently* (cross symbols and times) and *uniformly* drawn from the corresponding PAM constellation sets

$$v_c, u_c \in \Omega(\xi = \frac{6\gamma}{Q},\ Q = P^{\frac{\lambda_c}{2}}) \tag{39}$$

$$v_m, u_p \in \Omega(\xi = \frac{2\gamma}{Q},\ Q = P^{\frac{\lambda_m}{2}}) \tag{40}$$

$$v_p \in \Omega(\xi = \frac{\gamma}{Q},\ Q = P^{\frac{\lambda_p}{2}}) \tag{41}$$

where $\Omega(\xi, Q) \triangleq \{\xi \cdot a :\ a \in \mathcal{Z} \cap [-Q, Q]\}$ denotes the PAM constellation set, and γ is a finite constant such that

$$\gamma \in (0, 1/20]. \tag{42}$$

In Table II we provide the parameters $\{\beta_c, \beta_m, \beta_p, \lambda_c, \lambda_m, \lambda_p\}$ under different regimes[3]. If the parameters are set as $\beta_p = \infty$ and $\lambda_p = 0$, we will treat v_p as an empty term in the transmitted signal. Similar implication is applied to $\{v_c, u_c, v_m, u_p\}$. In Fig. 3 we provide a schematic representation of the proposed scheme, focusing on transmitter 1.

[3]Without loss of generality, we assume that $P^{\frac{\lambda_c}{2}}$, $P^{\frac{\lambda_m}{2}}$ and $P^{\frac{\lambda_p}{2}}$ are integers. Consider one example with $\lambda_c = \alpha - 1/2 - \epsilon$ and $P^{\frac{\lambda_c}{2}} = \sqrt{P^{\alpha-1/2-\epsilon}}$. When $\sqrt{P^{\alpha-1/2-\epsilon}}$ is not an integer, we can slightly modify ϵ such that $\sqrt{P^{\alpha-1/2-\epsilon}}$ is an integer, for the regime with large P.

Given our signal design, the power constraints $\mathbb{E}|x_1|^2 \le 1$ and $\mathbb{E}|x_2|^2 \le 1$ are satisfied. Focusing on the first transmitter, we have

$$\begin{aligned}
\mathbb{E}|v_c|^2 &= \frac{2 \times (\frac{6\gamma}{Q})^2}{2Q+1} \sum_{i=1}^{Q} i^2 = \frac{(\frac{6\gamma}{Q})^2 \cdot Q(Q+1)}{3} \le \frac{72\gamma^2}{3} \\
\mathbb{E}|v_m|^2 &\le \frac{8\gamma^2}{3} \\
\mathbb{E}|v_p|^2 &\le \frac{2\gamma^2}{3}
\end{aligned} \tag{43}$$

which suggests that

$$\begin{aligned}
\mathbb{E}|x_1|^2 &\le 4 \times (\frac{72\gamma^2}{3} + \frac{8\gamma^2}{3} + \frac{2\gamma^2}{3}) \\
&= \frac{328}{3}\gamma^2 \le \frac{328}{3} \times \frac{1}{400} < 1.
\end{aligned} \tag{44}$$

Similarly, we have $\mathbb{E}|x_2|^2 \le 1$. Note that, with our parameter design it holds true that $\beta_c \ge \alpha - 1$ and $\beta_m \ge 2\alpha - 1$, which controls the average power of the transmitted signal x_2 to satisfy $\mathbb{E}|x_2|^2 \le 1$.

The above signal design then implies the following forms of the received signals

$$\begin{aligned}
y_1 =& \sqrt{P^{1-\beta_c}} h_{11} h_{22} v_c + \sqrt{P^{1-\beta_m}} h_{11} h_{22} v_m \\
&+ \sqrt{P^{1-\beta_p}} h_{11} h_{22} v_p + \sqrt{P^{2\alpha-1-\beta_c}} h_{12} h_{21} u_c \\
&+ \sqrt{P^{2\alpha-1-\beta_m}} h_{12} h_{21} u_p + z_1
\end{aligned} \tag{45}$$

$$\begin{aligned}
y_2 =& h_{21} h_{22} (\sqrt{P^{\alpha-\beta_c}} (v_c + u_c) + \sqrt{P^{\alpha-\beta_m}} (v_m + u_p)) \\
&+ \sqrt{P^{\alpha-\beta_p}} h_{21} h_{22} v_p + z_2.
\end{aligned} \tag{46}$$

As we can see, at the eavesdropper, the jamming signal u_c (resp. u_p) is aligned at a specific power level and direction with the signal v_c (resp. v_m). In this way, it will minimize the penalty in GDoF incurred by the secrecy constraint, which can be seen later. Note that, with the above parameter design, the power of signal term with v_p is under the noise level at receiver 2, while the power of signal term with u_p is under the noise level at receiver 1.

3) Secure rate analysis: For $\epsilon > 0$, let us define the two rates as

$$R \triangleq \mathbb{I}(v; y_1) - \mathbb{I}(v; y_2) - \epsilon \tag{47}$$

$$R_0 \triangleq \mathbb{I}(v; y_2) - \epsilon. \tag{48}$$

Note that the wiretap channel with a helper can be considered as a specific case of the two-user interference channel with confidential messages, by removing the message of the second transmitter. Therefore, the result of [28, Theorem 2] reveals that the rate R defined in (47) is achievable and the message w is secure, i.e., $\mathbb{I}(w; y_2^n) \le n\epsilon$. The result of [28, Theorem 2]

TABLE II
DESIGNED PARAMETERS FOR DIFFERENT CASES, FOR SOME $\epsilon > 0$.

	$0 \le \alpha \le \frac{1}{2}$	$\frac{1}{2} \le \alpha \le \frac{3}{4}$	$\frac{3}{4} \le \alpha \le \frac{5}{6}$	$\frac{5}{6} \le \alpha \le 1$	$1 \le \alpha \le \frac{4}{3}$	$\frac{4}{3} \le \alpha \le 2$
β_c	∞	∞	0	0	$\alpha - 1$	$\alpha - 1$
β_m	0	$2\alpha - 1$	$2\alpha - 1$	$2\alpha - 1$	∞	∞
β_p	α	α	α	α	∞	∞
λ_c	0	0	$4\alpha - 3 - \epsilon$	$\alpha - 1/2 - \epsilon$	$\alpha/2 - \epsilon$	$2 - \alpha - \epsilon$
λ_m	$\alpha - \epsilon$	$1 - \alpha - \epsilon$	$1 - \alpha - \epsilon$	$1 - \alpha - \epsilon$	0	0
λ_p	$1 - \alpha - \epsilon$	$1 - \alpha - \epsilon$	$1 - \alpha - \epsilon$	$1 - \alpha - \epsilon$	0	0

requires that the random variables $\{v(t)\}_{t=1}^n$ are mutually independent, and that $v \to x_1 \to (y_1, y_2)$ forms a Markov chain, both of which are satisfied based on the design from (34)-(42) in our scheme.

In the following, we will analyze the secure rate for different cases of α. Note that, for the regimes of $0 \le \alpha \le \frac{3}{4}$, we also provide an alternative proof based on the scheme of treating interference as noise for the achievable secure GDoF in Appendix H.

A. Rate analysis when $0 \le \alpha \le 1/2$

For the first case with $0 \le \alpha \le 1/2$, the parameter design in Table II gives the following forms of the transmitted signals

$$x_1 = h_{22} v_m + \sqrt{P^{-\alpha}} h_{22} v_p \tag{49}$$

$$x_2 = \sqrt{P^{\alpha - 1}} h_{21} u_p. \tag{50}$$

Then, the received signals become

$$y_1 = \sqrt{P} h_{11} h_{22} v_m + \sqrt{P^{1-\alpha}} h_{11} h_{22} v_p + \sqrt{P^{2\alpha - 1}} h_{12} h_{21} u_p + z_1 \tag{51}$$

$$y_2 = \sqrt{P^{\alpha}} h_{21} h_{22} (v_m + u_p) + h_{21} h_{22} v_p + z_2. \tag{52}$$

Let us now analyze the achievable secure rate expressed in (47), i.e.,

$$R = \mathbb{I}(v; y_1) - \mathbb{I}(v; y_2) \tag{53}$$

by setting $\epsilon \to 0$. We will begin with the first term in the right-hand side of (53). With our signal design, v is now expressed as $v = v_m + \sqrt{P^{-\alpha}} v_p$. In this case, the two random variables v_m and v_p can be estimated from y_1, with error probability denoted by $\Pr[\{v_m \neq \hat{v}_m\} \cup \{v_p \neq \hat{v}_p\}]$. For the first term in the right-hand side of (53), we have the following bound

$$\begin{aligned}
\mathbb{I}(v; y_1) &\ge \mathbb{I}(v; \hat{v}_m, \hat{v}_p) && (54)\\
&= \mathbb{H}(v) - \mathbb{H}(v | \hat{v}_m, \hat{v}_p) \\
&\ge \mathbb{H}(v) - \big(1 + \Pr[\{v_m \neq \hat{v}_m\} \cup \{v_p \neq \hat{v}_p\}] \cdot \mathbb{H}(v)\big) && (55)\\
&= \big(1 - \Pr[\{v_m \neq \hat{v}_m\} \cup \{v_p \neq \hat{v}_p\}]\big) \cdot \mathbb{H}(v) - 1 && (56)
\end{aligned}$$

where (54) uses the Markov property of $v \to y_1 \to \{\hat{v}_m, \hat{v}_p\}$; and (55) follows from Fano's inequality. The entropy $\mathbb{H}(v)$ in (56) can be computed as

$$\begin{aligned}
\mathbb{H}(v) &= \mathbb{H}(v_m) + \mathbb{H}(v_p) \\
&= \log(2 \cdot P^{\frac{\alpha - \epsilon}{2}} + 1) + \log(2 \cdot P^{\frac{1 - \alpha - \epsilon}{2}} + 1) \\
&= \frac{1 - 2\epsilon}{2} \log P + o(\log P)
\end{aligned} \tag{57}$$

using the facts that $v_m \in \Omega(\xi = 2\gamma \cdot \frac{1}{Q},\ Q = P^{\frac{\alpha - \epsilon}{2}})$ and $v_p \in \Omega(\xi = \gamma \cdot \frac{1}{Q},\ Q = P^{\frac{1 - \alpha - \epsilon}{2}})$, and that $\{v_p, v_m\}$ can be reconstructed from v, and vice versa. For the error probability appeared in (56), we have the following result.

Lemma 5. *Consider the case with $0 \le \alpha \le 1/2$, and consider the signal design in* (37)-(42) *and Table II. Then, the error probability of the estimation of $\{v_m, v_p\}$ from y_1 is*

$$Pr[\{v_m \neq \hat{v}_m\} \cup \{v_p \neq \hat{v}_p\}] \to 0 \quad as \quad P \to \infty. \tag{58}$$

Proof. The proof is described in Appendix D. In the proof, a successive decoding method is used in the estimation of $\{v_m, v_p\}$ from y_1. □

By combining the results of (56), (57) and (58), it produces the following bound

$$\mathbb{I}(v; y_1) \ge \frac{1 - 2\epsilon}{2} \log P + o(\log P). \tag{59}$$

Note that the term $\mathbb{I}(v; y_2)$ in the right-hand side of (53) can be considered as a penalty term in the secure rate, incurred by the secrecy constraint. We will show that, with our scheme design using signal alignment, this penalty will be minimized to a small value that can be ignored in terms of GDoF. It can be seen from the received signal of the eavesdropper that, the jamming signal is aligned at a specific power level and direction with the signal sent from transmitter 1 (see (46)). Let us now bound the penalty term $\mathbb{I}(v; y_2)$ as follows:

$$\begin{aligned}
&\mathbb{I}(v; y_2) \\
\le &\mathbb{I}(v; y_2, v_m + u_p) \\
= &\mathbb{I}(v; v_m + u_p) + \mathbb{I}(v; h_{21} h_{22} v_p + z_2 | v_m + u_p) \\
= &\mathbb{H}(v_m + u_p) - \mathbb{H}(u_p) + \mathrm{h}(h_{21} h_{22} v_p + z_2) - \mathrm{h}(z_2) \\
\le &\underbrace{\log(4 \cdot P^{\frac{\alpha - \epsilon}{2}} + 1) - \log(2 \cdot P^{\frac{\alpha - \epsilon}{2}} + 1)}_{\le 1}
\end{aligned}$$

$$+\frac{1}{2}\log(2\pi e(\underbrace{|h_{21}|^2|h_{22}|^2+1}_{\leq 17}))-\frac{1}{2}\log(2\pi e) \quad (60)$$

$$\leq \log(2\sqrt{17}) \quad (61)$$

where (60) results from the identity that Gaussian input maximizes the differential entropy and the fact that $v_m+u_p \in \Omega(\xi = 2\gamma \cdot P^{-\frac{\alpha-\epsilon}{2}},\ Q = 2P^{\frac{\alpha-\epsilon}{2}})$. Note that uniform distribution maximizes the entropy. At the final step, we incorporate the results of (59) and (61) into (53) and then get the following bound on the secure rate

$$R \geq \frac{1-2\epsilon}{2}\log P + o(\log P). \quad (62)$$

It implies that the secure GDoF $d = 1$ is achievable for this case with $0 \leq \alpha \leq 1/2$.

B. Rate analysis when $1/2 \leq \alpha \leq 3/4$

Given the parameter design in Table II, in this case the transmitted signals are simplified as

$$x_1 = \sqrt{P^{-(2\alpha-1)}}h_{22}v_m + \sqrt{P^{-\alpha}}h_{22}v_p \quad (63)$$

$$x_2 = \sqrt{P^{-\alpha}}h_{21}u_p \quad (64)$$

which gives the following forms of the received signals

$$y_1 = \sqrt{P^{2-2\alpha}}h_{11}h_{22}v_m + \sqrt{P^{1-\alpha}}h_{11}h_{22}v_p + h_{12}h_{21}u_p + z_1 \quad (65)$$

$$y_2 = \sqrt{P^{1-\alpha}}h_{21}h_{22}(v_m+u_p) + h_{21}h_{22}v_p + z_2. \quad (66)$$

In this case, we can prove that the secure rate $R \geq \frac{2-2\alpha-2\epsilon}{2}\log P + o(\log P)$ is achievable. The rate analysis for this case follows from the steps in the previous case (cf. (53)-(62)). To avoid the repetition, we will just provide the outline of the proof for this case. In the first step, it can be proved that

$$\mathbb{I}(v; y_1) \geq \frac{2-2\alpha-2\epsilon}{2}\log P + o(\log P) \quad (67)$$

by following the derivations in (53)-(59). In this case $v = \sqrt{P^{-(2\alpha-1)}}v_m + \sqrt{P^{-\alpha}}v_p$ and $\mathbb{H}(v) = \mathbb{H}(v_m) + \mathbb{H}(v_p) = \frac{2-2\alpha-2\epsilon}{2}\log P + o(\log P)$. Similarly to the conclusion in Lemma 5 for the previous case, in this case it is also true that the error probability of the estimation of $\{v_m, v_p\}$ from y_1 vanishes as $P \to \infty$. A successive decoding method is also used in this estimation. In the second step, by following the derivations related to (60) and (61), it can be proved that

$$\mathbb{I}(v; y_2) \leq o(\log P), \quad (68)$$

which, together with (67), gives the lower bound on the secure rate $R \geq \frac{2-2\alpha-2\epsilon}{2}\log P + o(\log P)$. It implies that the secure GDoF $d = 2-2\alpha$ is achievable for this case.

C. Rate analysis when $3/4 \leq \alpha \leq 5/6$

Given the parameter design in Table II, in this case the transmitted signals are simplified as

$$x_1 = h_{22}v_c + \sqrt{P^{-(2\alpha-1)}}h_{22}v_m + \sqrt{P^{-\alpha}}h_{22}v_p \quad (69)$$

$$x_2 = \sqrt{P^{\alpha-1}}h_{21}u_c + \sqrt{P^{-\alpha}}h_{21}u_p. \quad (70)$$

The received signals are given by

$$y_1 = \sqrt{P}h_{11}h_{22}v_c + \sqrt{P^{2\alpha-1}}h_{12}h_{21}u_c + \sqrt{P^{2-2\alpha}}h_{11}h_{22}v_m + \sqrt{P^{1-\alpha}}h_{11}h_{22}v_p + h_{12}h_{21}u_p + z_1 \quad (71)$$

$$y_2 = h_{21}h_{22}(\sqrt{P^{\alpha}}(v_c+u_c) + \sqrt{P^{1-\alpha}}(v_m+u_p)) + h_{21}h_{22}v_p + z_2. \quad (72)$$

The rate analysis also follows (53)-(62). In this case, we can prove that the secure rate $R \geq \frac{2\alpha-1-3\epsilon}{2}\log P + o(\log P)$ is achievable. Again, to avoid the repetition we will just provide the outline of the proof. In the first step, it can be proved that

$$\mathbb{I}(v; y_1) \geq \frac{2\alpha-1-3\epsilon}{2}\log P + o(\log P) \quad (73)$$

by following the derivations in (53)-(59). Here we have $v = v_c + \sqrt{P^{-(2\alpha-1)}}v_m + \sqrt{P^{-\alpha}}v_p$ and $\mathbb{H}(v) = \mathbb{H}(v_c) + \mathbb{H}(v_m) + \mathbb{H}(v_p) = \frac{2\alpha-1-3\epsilon}{2}\log P + o(\log P)$. It is true that the error probability of the estimation of $\{v_c, v_m, v_p\}$ from y_1 vanishes as $P \to \infty$. A successive decoding method is also used in this estimation. In the second step, by following the derivations related to (60) and (61), we can prove that

$$\mathbb{I}(v; y_2) \leq o(\log P). \quad (74)$$

Therefore, the secure rate is bounded by $R \geq \frac{2\alpha-1-3\epsilon}{2}\log P + o(\log P)$, implying that the secure GDoF $d = 2\alpha-1$ is achievable.

D. Rate analysis when $5/6 \leq \alpha \leq 1$

In this case, the transmitted signals take the same forms as in (69) and (70), and the received signals are expressed as in (71) and (72). However, in the rate analysis, the estimation approach is different, where noise removal and signal separation will be used. By following the previous derivations in (54)-(56), we have the following bound

$$\mathbb{I}(v; y_1) \geq \big(1 - \Pr[\{v_c \neq \hat{v}_c\} \cup \{v_m \neq \hat{v}_m\} \cup \{v_p \neq \hat{v}_p\}]\big) \cdot \mathbb{H}(v) - 1 \quad (75)$$

where the entropy $\mathbb{H}(v)$ in (75) can be computed as

$$\mathbb{H}(v) = \mathbb{H}(v_c) + \mathbb{H}(v_m) + \mathbb{H}(v_p) = \frac{3/2-\alpha-3\epsilon}{2}\log P + o(\log P). \quad (76)$$

The following lemma shows that the error probability $\Pr[\{v_c \neq \hat{v}_c\} \cup \{v_m \neq \hat{v}_m\} \cup \{v_p \neq \hat{v}_p\}]$ in (75) vanishes as P approaches infinity.

Lemma 6. *Consider the case with* $5/6 \leq \alpha \leq 1$*, and consider the signal design in* (37)-(42) *and Table II. Then, for almost all the channel realizations* $\{h_{k\ell}\} \in (1,2]^{2\times 2}$*, the error probability of the estimation of* $\{v_c, v_m, v_p\}$ *from* y_1 *is*

$$Pr[\{v_c \neq \hat{v}_c\} \cup \{v_m \neq \hat{v}_m\} \cup \{v_p \neq \hat{v}_p\}] \to 0 \ \ as\ P \to \infty. \quad (77)$$

Proof. The proof is described in Section VI. In the proof, noise removal and signal separation are used in the estimation of $\{v_c, v_m, v_p\}$ from y_1. □

The results of (75), (76) and (77) imply that the bound

$$\mathbb{I}(v;y_1) \geq \frac{3/2-\alpha-3\epsilon}{2}\log P + o(\log P) \tag{78}$$

holds true for almost all the channel realizations $\{h_{k\ell}\} \in (1,2]^{2\times 2}$. Next, by following the derivations related to (60) and (61), it can be proved that

$$\mathbb{I}(v;y_2) \leq o(\log P). \tag{79}$$

Thus, we have $R \geq \frac{3/2-\alpha-3\epsilon}{2}\log P + o(\log P)$, implying that the secure GDoF $d = 3/2-\alpha$ is achievable, for almost all the channel realizations in this case.

E. Rate analysis when $1 \leq \alpha \leq 4/3$

In this case, the transmitted signals are simplified as

$$x_1 = \sqrt{P^{-(\alpha-1)}}h_{22}v_c \tag{80}$$

$$x_2 = h_{21}u_c \tag{81}$$

and the received signals are expressed as

$$y_1 = \sqrt{P^{2-\alpha}}h_{11}h_{22}v_c + \sqrt{P^{\alpha}}h_{12}h_{21}u_c + z_1 \tag{82}$$

$$y_2 = \sqrt{P}h_{21}h_{22}(v_c+u_c) + z_2. \tag{83}$$

As in the previous case, the estimation approaches of noise removal and signal separation are also used here for the rate analysis. In this case, the entropy $\mathbb{H}(v)$ is computed as $\mathbb{H}(v) = \mathbb{H}(v_c) = \frac{\alpha/2-\epsilon}{2}\log P + o(\log P)$. Following the previous derivations in (54)-(56), we have

$$\begin{aligned}\mathbb{I}(v;y_1) &\geq \big(1-\Pr[\{v_c \neq \hat{v}_c\}]\big)\cdot\mathbb{H}(v) - 1\\ &= \big(1-\Pr[\{v_c \neq \hat{v}_c\}]\big)\cdot\frac{\alpha/2-\epsilon}{2}\log P + o(\log P).\end{aligned} \tag{84}$$

The lemma below provides the result on the error probability $\Pr[v_c \neq \hat{v}_c]$.

Lemma 7. *Consider the case with* $1 \leq \alpha \leq 4/3$*, and consider the signal design in* (37)-(42) *and Table II. Then, for almost all the channel realizations* $\{h_{k\ell}\} \in (1,2]^{2\times 2}$*, the error probability of the estimation of* v_c *from* y_1 *is*

$$Pr[v_c \neq \hat{v}_c] \to 0 \quad as \quad P \to \infty. \tag{85}$$

Proof. The proof is described in Appendix E. In the proof, noise removal and signal separation are used in the estimation of v_c from y_1. □

The results of (84) and (85) implies that the following bound

$$\mathbb{I}(v;y_1) \geq \frac{\alpha/2-\epsilon}{2}\log P + o(\log P) \tag{86}$$

holds true for almost all the channel realizations $\{h_{k\ell}\} \in (1,2]^{2\times 2}$. Again, it is not hard to prove that $\mathbb{I}(v;y_2) \leq o(\log P)$. Together with (86), it reveals that $R \geq \frac{\alpha/2-\epsilon}{2}\log P + o(\log P)$, and that the secure GDoF $d = \alpha/2$ is achievable, for almost all the channel realizations in this case.

F. Rate analysis when $4/3 \leq \alpha \leq 2$

In this case, the transmitted signals take the same forms as in (80) and (81), and the received signals are expressed as in (82) and (83). Here the entropy $\mathbb{H}(v)$ is computed as $\mathbb{H}(v) = \mathbb{H}(v_c) = \frac{2-\alpha-\epsilon}{2}\log P + o(\log P)$. Similar to the previous cases, we can prove that

$$\mathbb{I}(v;y_1) \geq \big(1-\Pr[v_c \neq \hat{v}_c]\big)\cdot\frac{2-\alpha-\epsilon}{2}\log P + o(\log P) \tag{87}$$

(cf. (84)). The probability $\Pr[v_c \neq \hat{v}_c]$ in (87) is the error probability of the estimation of v_c from y_1. In this case, it can be proved that u_c and v_c can be estimated from y_1 in a successive way and the error probability of this estimation vanishes as $P \to \infty$. The proof of this step is similar to that of Lemma 5, and hence it is omitted here to avoid the repetition. Then, we have

$$\mathbb{I}(v;y_1) \geq \frac{2-\alpha-\epsilon}{2}\log P + o(\log P). \tag{88}$$

As in the previous cases, it can be proved that $\mathbb{I}(v;y_2) \leq o(\log P)$. Finally we have a lower bound on the secure rate $R \geq \frac{2-\alpha-\epsilon}{2}\log P + o(\log P)$, which implies that the secure GDoF $d = 2-\alpha$ is achievable in this case.

VI. Proof of Lemma 6

Given the observation y_1 in (71), and with $5/6 \leq \alpha \leq 1$, we will show that v_c, u_c, v_m and v_p can be estimated with vanishing error probability, for almost all the channel realizations. Our focus is to prove that v_c, u_c and v_m can be estimated from y_1 simultaneously with vanishing error probability, for almost all the channel realizations. This proof is motivated by the proof of [38, Lemma 4], in which the noise removal and signal separation techniques will be used. Once v_c, u_c and v_m are estimated correctly from y_1, we can remove v_c, u_c and v_m from y_1 and then estimate v_p with vanishing error probability.

Recall that $v_c, u_c \in \Omega(\xi = \frac{6\gamma}{Q},\ Q = P^{\frac{\alpha-1/2-\epsilon}{2}})$, $v_m, u_p \in \Omega(\xi = \frac{2\gamma}{Q},\ Q = P^{\frac{1-\alpha-\epsilon}{2}})$ and $v_p \in \Omega(\xi = \frac{\gamma}{Q},\ Q = P^{\frac{1-\alpha-\epsilon}{2}})$, for some parameters $\gamma \in (0, 1/20]$ and $\epsilon \to 0$. Let us describe y_1 in the following form

$$\begin{aligned}y_1 =& \sqrt{P}h_{11}h_{22}v_c + \sqrt{P^{2\alpha-1}}h_{12}h_{21}u_c + \sqrt{P^{2-2\alpha}}h_{11}h_{22}v_m\\ &+ \sqrt{P^{1-\alpha}}h_{11}h_{22}v_p + h_{12}h_{21}u_p + z_1\\ =& \sqrt{P^{1-\alpha+\epsilon}}2\gamma\underbrace{\big(3\sqrt{P^{1/2}}g_2q_2 + 3\sqrt{P^{2\alpha-3/2}}g_1q_1 + g_0q_0\big)}_{\triangleq\,\tilde{s}}\\ &+ \sqrt{P^{1-\alpha}}\underbrace{\big(h_{11}h_{22}v_p + \sqrt{P^{\alpha-1}}h_{12}h_{21}u_p\big)}_{\triangleq\,\tilde{e}} + z_1\\ =& \sqrt{P^{1-\alpha+\epsilon}}\cdot 2\gamma\tilde{s} + \sqrt{P^{1-\alpha}}\tilde{e} + z_1\end{aligned} \tag{89}$$

where $g_2 \triangleq g_0 \triangleq h_{11}h_{22}$, $g_1 \triangleq h_{12}h_{21}$, $\tilde{e} \triangleq h_{11}h_{22}v_p + \frac{1}{\sqrt{P^{1-\alpha}}}h_{12}h_{21}u_p$, $\tilde{s} \triangleq g_0q_0 + 3\sqrt{P^{2\alpha-3/2}}g_1q_1 + 3\sqrt{P^{1/2}}g_2q_2$ and

$$q_2 \triangleq \frac{Q_2}{6\gamma}\cdot v_c, \quad q_1 \triangleq \frac{Q_1}{6\gamma}\cdot u_c, \quad q_0 \triangleq \frac{Q_0}{2\gamma}\cdot v_m,$$
$$Q_2 \triangleq Q_1 \triangleq P^{\frac{\alpha-1/2-\epsilon}{2}}, \quad Q_0 \triangleq P^{\frac{1-\alpha-\epsilon}{2}}.$$

In this scenario, the following conditions are always satisfied: $q_k \in \mathcal{Z}$ and $|q_k| \le Q_k$ for $k = 0, 1, 2$. Let

$$A_2 \triangleq 3\sqrt{P^{1/2}}, \quad A_1 \triangleq 3\sqrt{P^{2\alpha-3/2}}, \quad A_0 \triangleq 1.$$

In this scenario with $5/6 \le \alpha \le 1$, without loss of generality we will consider the case that[4] $Q_0, Q_1, Q_2, A_1, A_2 \in \mathcal{Z}^+$.

For the observation y_1 in (89), the goal is to estimate the sum $\tilde{s} = g_0(q_0 + 3\sqrt{P^{1/2}}q_2) + 3\sqrt{P^{2\alpha-3/2}}g_1q_1$ by considering the other signals as noise (noise removal). After decoding $\tilde{s}$ correctly, the three symbols q_0, q_1, q_2 can be estimated, based on the fact that $\{g_0, g_1\}$ are rationally independent (signal separation, cf. [47]), as well as the fact that q_0 and q_2 can be reconstructed from $q_0 + 3\sqrt{P^{1/2}}q_2$. Note that the minimum distance of $3\sqrt{P^{1/2}}q_2$, i.e., $\min_{q_2, \bar{q}_2 \in \mathcal{Z} \cap [-Q_2, Q_2],\ q_2 \neq \bar{q}_2} 3\sqrt{P^{1/2}}\cdot|q_2 - \bar{q}_2|$, is no less than the maximum of $2q_0$. To estimate $\tilde{s}$ from y_1, we will show that the minimum distance of $\tilde{s}$ is sufficiently large, in order to make the error probability vanishing. Let us define the minimum distance of $\tilde{s}$ as

$$d_{\min}(g_0, g_1, g_2) \triangleq \min_{\substack{q_1, q_2, \tilde{q}_1, \tilde{q}_2 \in \mathcal{Z} \cap [-Q_2, Q_2] \\ q_0, \tilde{q}_0 \in \mathcal{Z} \cap [-Q_0, Q_0] \\ (q_0, q_1, q_2) \neq (\tilde{q}_0, \tilde{q}_1, \tilde{q}_2)}} \Big| g_0(q_0 - \tilde{q}_0) + 3\sqrt{P^{2\alpha-3/2}}g_1(q_1 - \tilde{q}_1) + 3\sqrt{P^{1/2}}g_2(q_2 - \tilde{q}_2) \Big|. \quad (90)$$

The following lemma provides a result on the minimum distance.

Lemma 8. *For the case with $5/6 \le \alpha \le 1$, and for some constants $\delta \in (0, 1]$ and $\epsilon > 0$, the following bound on the minimum distance $d_{\min}$ holds true*

$$d_{\min} \ge \delta \quad (91)$$

for all the channel realizations $\{h_{11}, h_{12}, h_{22}, h_{21}\} \in (1, 2]^{2\times 2} \setminus \mathcal{H}_{out}$, where $\mathcal{H}_{out} \subseteq (1, 2]^{2\times 2}$ is an outage set whose Lebesgue measure, denoted by $\mathcal{L}(\mathcal{H}_{out})$, has the following bound

$$\mathcal{L}(\mathcal{H}_{out}) \le 12096\delta \cdot P^{-\frac{\epsilon}{2}}. \quad (92)$$

Proof. For $\beta \triangleq \delta \in (0, 1]$, we define an event as

$$B(q_2, q_1, q_0) \triangleq \{(g_2, g_1, g_0) \in (1, 4]^3 : |A_2 g_2 q_2 + A_1 g_1 q_1 + g_0 q_0| < \beta\}. \quad (93)$$

Also define

$$B \triangleq \bigcup_{\substack{q_0, q_1, q_2 \in \mathcal{Z}: \\ |q_k| \le 2Q_k \ \forall k \\ (q_0, q_1, q_2) \neq 0}} B(q_2, q_1, q_0). \quad (94)$$

[4]The result of Lemma 6 still holds for the case when any of $\{Q_0, Q_1, Q_2, A_1, A_2\}$ is not integer. The proof just needs some minor modifications. For example, when A_2 is not an integer, we can modify v_c and u_c as $v_c = \eta_c v_c'$ and $u_c = \eta_c u_c'$, where $v_c', u_c' \in \Omega(\xi = \frac{6\gamma}{Q}, Q = P^{\frac{\lambda_c}{2}})$, and η_c is a selected parameter such that $0 < \eta_c < 1$ and $A_2\eta_c$ is an integer.

For $5/6 \le \alpha \le 1$, by [48, Lemma 14] we have the following bound on the Lebesgue measure of B (i.e., $\mathcal{L}(B)$)

$$\begin{aligned}
&\mathcal{L}(B) \\
\le& 504\beta \cdot 4\Big(2\min\{\frac{Q_0}{A_2}, Q_2\} + \tilde{Q}_2 \min\{Q_1, \frac{Q_0}{A_1}, \frac{A_2\tilde{Q}_2}{A_1}\} \\
&\quad + 2\min\{\frac{Q_0}{A_1}, Q_1\} + \tilde{Q}_1 \min\{Q_2, \frac{Q_0}{A_2}, \frac{A_1\tilde{Q}_1}{A_2}\}\Big) \\
\le& 504\beta \cdot 4\Big(\frac{2Q_0}{A_2} + \tilde{Q}_2 \cdot \frac{Q_0}{A_1} + \frac{2Q_0}{A_1} + \tilde{Q}_1 \cdot \frac{Q_0}{A_2}\Big) \\
\le& 504\beta \cdot 4\Big(Q_1 \cdot \frac{9Q_0}{A_2} + \frac{4Q_0}{A_1}\Big) \\
\le& 504\beta \cdot 8Q_0 \max\{\frac{9Q_1}{A_2}, \frac{4}{A_1}\} \\
\le& 504\beta \cdot 8Q_0 \cdot 3P^{\frac{\alpha-1}{2}} \\
=& 12096\delta \cdot P^{-\frac{\epsilon}{2}}
\end{aligned} \quad (95)$$

where $\tilde{Q}_1 = \min\{Q_1, 8\frac{\max\{Q_0, A_2Q_2\}}{A_1}\} = Q_1$ and $\tilde{Q}_2 = \min\{Q_2, 8\frac{\max\{Q_0, A_1Q_1\}}{A_2}\} = Q_1 \cdot \min\{1, \frac{8A_1}{A_2}\}$. In this scenario, we can treat B as an outage set. When $(g_0, g_1, g_2) \notin B$, by definition we have $d_{\min}(g_0, g_1, g_2) \ge \delta$. Recall that $g_2 \triangleq g_0 \triangleq h_{11}h_{22}$ and $g_1 \triangleq h_{12}h_{21}$. At this point, we define a new set $\mathcal{H}_{\text{out}}$ as

$$\mathcal{H}_{\text{out}} \triangleq \{(h_{11}, h_{22}, h_{12}, h_{21}) \in (1, 2]^{2\times 2} : (g_2 = g_0, g_1, g_0) \in B\}.$$

We define $\mathbb{1}_{\mathcal{H}_{\text{out}}}(h_{11}, h_{22}, h_{12}, h_{21}) = 1$ if $(h_{11}, h_{22}, h_{12}, h_{21}) \in \mathcal{H}_{\text{out}}$, else $\mathbb{1}_{\mathcal{H}_{\text{out}}}(h_{11}, h_{22}, h_{12}, h_{21}) = 0$. Similarly, we define $\mathbb{1}_B(g_1, g_0) = 1$ if $(g_2 = g_0, g_1, g_0) \in B$, else $\mathbb{1}_B(g_1, g_0) = 0$. Then we can bound the Lebesgue measure of $\mathcal{H}_{\text{out}}$ as

$$\begin{aligned}
&\mathcal{L}(\mathcal{H}_{\text{out}}) \\
=& \int_{h_{11}=1}^{2}\int_{h_{12}=1}^{2}\int_{h_{21}=1}^{2}\int_{h_{22}=1}^{2} \mathbb{1}_{\mathcal{H}_{\text{out}}}(h_{11}, h_{22}, h_{12}, h_{21}) dh_{22} \cdot dh_{21}dh_{12}dh_{11} \\
=& \int_{h_{11}=1}^{2}\int_{h_{12}=1}^{2}\int_{h_{21}=1}^{2}\int_{h_{22}=1}^{2} \mathbb{1}_B(h_{12}h_{21}, h_{11}h_{22}) dh_{22}dh_{21} \cdot dh_{12}dh_{11} \\
\le& \int_{h_{11}=1}^{2}\int_{h_{12}=1}^{2}\int_{g_1=1}^{4}\int_{g_0=1}^{4} \mathbb{1}_B(g_1, g_0) h_{11}^{-1}h_{12}^{-1} dg_0dg_1 \cdot dh_{12}dh_{11} \\
\le& \int_{h_{11}=1}^{2}\int_{h_{12}=1}^{2} \mathcal{L}(B) dh_{12}dh_{11} \\
\le& 12096\delta \cdot P^{-\frac{\epsilon}{2}}
\end{aligned} \quad (96)$$

where the last step uses the result in (95). □

In the rest of this section, we will consider the channel realizations $(h_{11}, h_{22}, h_{12}, h_{21}) \in (1, 2]^{2\times 2}$ that are not in the outage set $\mathcal{H}_{\text{out}}$. The result of Lemma 8 reveals that

$$\mathcal{L}(\mathcal{H}_{\text{out}}) \to 0, \quad \text{for} \quad P \to \infty.$$

When the channel realizations satisfy the condition $(h_{11}, h_{22}, h_{12}, h_{21}) \notin \mathcal{H}_{\text{out}}$, we have the following property on the minimum distance defined in (90): $d_{\min} \ge \delta$ for a

given constant $\delta \in (0,1]$. With this result, we can estimate $\tilde{s}$ from y_1 expressed in (89). For the random variable $\tilde{e} = h_{11}h_{22}v_p + \frac{1}{\sqrt{P^{1-\alpha}}}h_{12}h_{21}u_p$ appeared in (89), it is true that

$$|\tilde{e}| \le \tilde{e}_{\max} \triangleq 3/5 \quad \forall \tilde{e}.$$

At this point, we have the following bound on the error probability of the estimation of $\tilde{s}$ from y_1

$$\begin{aligned}\Pr[\tilde{s} \neq \hat{\tilde{s}}] &\le \Pr\Big[|z_1 + \sqrt{P^{1-\alpha}}\tilde{e}| > \sqrt{P^{1-\alpha+\epsilon}} \cdot 2\gamma \cdot \frac{d_{\min}}{2}\Big] \\ &\le 2 \cdot \mathbf{Q}\big(P^{\frac{1-\alpha+\epsilon}{2}} \cdot 2\gamma \cdot \frac{d_{\min}}{2} - P^{\frac{1-\alpha}{2}}\tilde{e}_{\max}\big) \\ &\le 2 \cdot \mathbf{Q}\big(P^{\frac{1-\alpha}{2}}(\gamma\delta P^{\frac{\epsilon}{2}} - 3/5)\big) \end{aligned} \tag{97}$$

where $\hat{\tilde{s}}$ denotes the estimate of $\tilde{s}$; $\mathbf{Q}(\tau) \triangleq \frac{1}{\sqrt{2\pi}}\int_\tau^\infty \exp(-\frac{z^2}{2})dz$; the last step stems from the result that $d_{\min} \ge \delta$. By following the fact that $\mathbf{Q}(\tau) \le \frac{1}{2}\exp(-\tau^2/2),\ \forall \tau \ge 0$, the result in (97) implies the following conclusion

$$\Pr[\tilde{s} \neq \hat{\tilde{s}}] \to 0 \quad \text{for} \quad P \to \infty. \tag{98}$$

After decoding $\tilde{s} = g_0(q_0 + 3\sqrt{P^{1/2}}q_2) + 3\sqrt{P^{2\alpha-3/2}}g_1q_1$ correctly, the three symbols q_0, q_1, q_2 can be recovered, as illustrated before in this section.

Next, we remove $\tilde{s}$ from y_1, which leads to

$$y_1 - \sqrt{P^{1-\alpha+\epsilon}} \cdot 2\gamma\tilde{s} = \sqrt{P^{1-\alpha}}h_{11}h_{22}v_p + h_{12}h_{21}u_p + z_1. \tag{99}$$

Since the interference term $h_{12}h_{21}u_p$ in (99) is under the noise level, i.e., $h_{12}h_{21}u_p \le 8\gamma \le 2/5$, one can easily prove that the the error probability for decoding v_p from the observation in (99) is

$$\Pr[v_p \neq \hat{v}_p] \to 0 \quad \text{for} \quad P \to \infty. \tag{100}$$

Therefore, the error probability $\Pr[\{v_c \neq \hat{v}_c\} \cup \{v_m \neq \hat{v}_m\} \cup \{v_p \neq \hat{v}_p\}]$ vanishes as P approaches infinity, for almost all the channel realizations $(h_{11}, h_{22}, h_{12}, h_{21}) \in (1,2]^{2\times 2}$.

VII. Conclusion

In this work, we characterized the optimal secure GDoF of a symmetric Gaussian wiretap channel with a helper, under a weak notion of secrecy constraint. The result reveals that, adding a helper can significantly increase the secure GDoF of the wiretap channel. A new converse and a new scheme are provided in this work. The converse derived in this work holds for the symmetric and asymmetric channels. In the proposed scheme, the helper sends a cooperative jamming signal at a specific power level and direction, which allows to minimize the penalty in GDoF incurred by the secrecy constraint. Notably, a smart splitting of the common signal into a new common signal (or upper common signal) and middle signal (or lower common signal) is one of the key technique ingredients in the proposed scheme. In the secure rate analysis, the techniques of noise removal and signal separation are used. The optimal secure GDoF is described in different expressions for different interference regimes. For the regimes of $0 \le \alpha \le 5/6$ and $4/3 \le \alpha \le 2$, the achievable secure GDoF result holds for all the channel realizations under our channel model. For the regime of $5/6 < \alpha < 4/3$, the achievable secure GDoF result holds for almost all the channel realizations when P is large, under our channel model. In the future work, we will generalize our secure GDoF result to understand the constant-gap secure capacity.

Appendix A
Proof of Lemma 2

Recall that $\bar{y}_2(t)$ is a nosy version of $y_2(t)$, defined in (18). From chain rule, we have

$$\begin{aligned}\mathbb{I}(w;\bar{y}_2^n) &= \mathbb{I}(w;\bar{y}_2^n|s_{22}^n) + \mathbb{I}(w;s_{22}^n) - \mathbb{I}(w;s_{22}^n|\bar{y}_2^n) \\ &= \mathbb{I}(w;\bar{y}_2^n|s_{22}^n) - \mathbb{I}(w;s_{22}^n|\bar{y}_2^n) \end{aligned} \tag{101}$$

where (101) follows from the independence between w and s_{22}^n. For the term $\mathbb{I}(w;s_{22}^n|\bar{y}_2^n)$ in (101), it can be bounded by

$$\begin{aligned}&\mathbb{I}(w;s_{22}^n|\bar{y}_2^n) \\ =&\mathrm{h}(s_{22}^n|\bar{y}_2^n) - \mathrm{h}(s_{22}^n|\bar{y}_2^n, w) \\ \le&\sum_{t=1}^n \mathrm{h}(s_{22}(t)|\bar{y}_2(t)) - \mathrm{h}(s_{22}^n|\bar{y}_2^n, w, x_2^n) \qquad (102) \\ =&\sum_{t=1}^n \mathrm{h}(s_{22}(t) - \sqrt{P^{-\phi_3}}\bar{y}_2(t)|\bar{y}_2(t)) - \underbrace{\mathrm{h}(\tilde{z}_2^n)}_{=\frac{n}{2}\log(2\pi e)} \\ =&\sum_{t=1}^n \mathrm{h}\Big(\tilde{z}_2(t) - h_{21}x_1(t) - \sqrt{P^{-\alpha_{21}}}h_{22}z_2(t) - \sqrt{P^{-\phi_3}}\bar{z}_2(t) \\ &\qquad + (\sqrt{P^{(\alpha_{22}-\alpha_{21})^+}} - \sqrt{P^{\alpha_{22}-\alpha_{21}}})h_{22}x_2(t)|\bar{y}_2(t)\Big) \\ &- \frac{n}{2}\log(2\pi e) \qquad (103) \\ \le&\frac{n}{2}\log\Big(\underbrace{1 + |h_{21}|^2 + P^{-\alpha_{21}}|h_{22}|^2 + P^{-\phi_3}}_{\le 10} \\ &\qquad + \underbrace{(\sqrt{P^{(\alpha_{22}-\alpha_{21})^+}} - \sqrt{P^{\alpha_{22}-\alpha_{21}}})^2}_{\le 1} \cdot \underbrace{|h_{22}|^2}_{\le 4}\Big) \qquad (104) \\ \le&\frac{n}{2}\log 14 \qquad (105)\end{aligned}$$

where (102) follows from chain rule and the fact that conditioning reduces differential entropy; (103) uses the identity that $\mathrm{h}(\tilde{z}_2^n) = \frac{n}{2}\log(2\pi e)$; (104) results from the fact that Gaussian input maximizes the differential entropy, and that conditioning reduces differential entropy. At this point, we complete the proof of Lemma 2.

Appendix B
Proof of Lemma 3

For $s_{22}(t)$ and $\bar{y}_2(t)$ defined in (14) and (18), we have

$$\begin{aligned}&\mathrm{h}(y_1^n|s_{22}^n) - \mathrm{h}(\bar{y}_2^n|s_{22}^n) \\ \le&\mathrm{h}(y_1^n|s_{22}^n) - \mathrm{h}(\bar{y}_2^n|s_{22}^n, z_2^n) \qquad (106) \\ =&\mathrm{h}(y_1^n|s_{22}^n) - \mathrm{h}(\{\bar{y}_2(t) - \sqrt{P^{-(\alpha_{21}-\phi_3)}}z_2(t)\}_{t=1}^n|s_{22}^n, z_2^n) \\ =&\mathrm{h}(y_1^n|s_{22}^n) - \mathrm{h}\Big(\{\sqrt{P^{\phi_3}}h_{21}x_1(t) \\ &+ \sqrt{P^{\alpha_{22}-(\alpha_{21}-\phi_3)}}h_{22}x_2(t) + \bar{z}_2(t)\}_{t=1}^n|s_{22}^n, z_2^n\Big)\end{aligned}$$

$$
\begin{aligned}
&=\mathrm{h}(y_1^n|s_{22}^n)-\mathrm{h}\Big(\{\sqrt{P^{\phi_3}}h_{21}x_1(t)\\
&\quad+\sqrt{P^{\alpha_{22}-(\alpha_{21}-\phi_3)}}h_{22}x_2(t)+\bar{z}_2(t)\}_{t=1}^n|s_{22}^n\Big) \qquad (107)\\
&=\mathrm{h}(y_1^n|\{\sqrt{P^{(\alpha_{22}-\alpha_{21})^+}}h_{22}x_2(t)+z_2'(t)\}_{t=1}^n)\\
&\quad-\mathrm{h}\Big(\{\sqrt{P^{\phi_3}}h_{21}x_1(t)+\sqrt{P^{\alpha_{22}-(\alpha_{21}-\phi_3)}}h_{22}x_2(t)\\
&\quad+\bar{z}_2(t)\}_{t=1}^n|\{\sqrt{P^{(\alpha_{22}-\alpha_{21})^+}}h_{22}x_2(t)+z_2'(t)\}_{t=1}^n\Big) \qquad (108)
\end{aligned}
$$

where (106) uses the fact that conditioning reduces differential entropy; (107) follows from the fact that z_2^n is independent of $\{\sqrt{P^{-\phi_3}}h_{21}x_1(t)+\sqrt{P^{\alpha_{22}-(\alpha_{21}-\phi_3)}}h_{22}x_2(t)+\bar{z}_2(t)\}_{t=1}^n$ and $s_{22}^n=\{\sqrt{P^{(\alpha_{22}-\alpha_{21})^+}}h_{22}x_2(t)+\tilde{z}_2(t)\}_{t=1}^n$; in (108) we replace $\tilde{z}_2(t)$ with a new noise random variable $z_2'(t)\sim\mathcal{N}(0,1)$ that is independent of the other noise random variables and transmitted signals $\{x_1(t),x_2(t)\}_t$; note that replacing $\tilde{z}_2(t)\sim\mathcal{N}(0,1)$ with $z_2'(t)\sim\mathcal{N}(0,1)$ will not change the differential entropies in (107), due to the fact that differential entropy depends on distributions. To bound the right-hand side of (108), we will use the result of [38, Lemma 9] that is described below.

Lemma 9. *[38, Lemma 9] Let $y_1(t)=\sqrt{P^{\alpha_{11}}}h_{11}x_1(t)+\sqrt{P^{\alpha_{12}}}h_{12}x_2(t)+z_1(t)$ and $y_2(t)=\sqrt{P^{\alpha_{21}}}h_{21}x_1(t)+\sqrt{P^{\alpha_{22}}}h_{22}x_2(t)+z_2(t)$, as defined in* (1)*. Consider a random variable (or a set of random variables), $\bar{w}_1$, that is independent of $\{x_2^n,z_1^n,z_2^n,\tilde{z}_1^n,\tilde{z}_2^n,\bar{z}_2^n,\bar{z}_3^n,\bar{z}_4^n\}$; and consider another random variable (or another set of random variables), $\bar{w}_2$, that is independent of $\{x_1^n,z_1^n,z_2^n,\tilde{z}_1^n,\tilde{z}_2^n,\bar{z}_2^n,\bar{z}_3^n,\bar{z}_4^n\}$. Then, we have*

$$
\begin{aligned}
&\mathrm{h}(y_2^n|\bar{w}_1)-\mathrm{h}(y_1^n|\bar{w}_1)\\
&\le\frac{n}{2}\log\Big(1+P^{\alpha_{22}-\alpha_{12}}\cdot\frac{|h_{22}|^2}{|h_{12}|^2}+P^{\alpha_{21}-(\alpha_{11}-\alpha_{12})^+}\cdot\frac{|h_{21}|^2}{|h_{11}|^2}\Big)\\
&\quad+\frac{n}{2}\log 10, \qquad (109)\\
&\mathrm{h}(y_1^n|\bar{w}_2)-\mathrm{h}(y_2^n|\bar{w}_2)\\
&\le\frac{n}{2}\log\Big(1+P^{\alpha_{11}-\alpha_{21}}\cdot\frac{|h_{11}|^2}{|h_{21}|^2}+P^{\alpha_{12}-(\alpha_{22}-\alpha_{21})^+}\cdot\frac{|h_{12}|^2}{|h_{22}|^2}\Big)\\
&\quad+\frac{n}{2}\log 10. \qquad (110)
\end{aligned}
$$

Note that the result in (110) holds true when $\bar{w}_2$ is set as $\bar{w}_2\triangleq\{\sqrt{P^{(\alpha_{22}-\alpha_{21})^+}}h_{22}x_2(t)+z_2'(t)\}_{t=1}^n$. Let us define $\alpha_{21}'\triangleq\phi_3$, $\alpha_{22}'\triangleq\alpha_{22}-(\alpha_{21}-\phi_3)$ and $y_2(t)'\triangleq\sqrt{P^{\alpha_{21}'}}h_{21}x_1(t)+\sqrt{P^{\alpha_{22}'}}h_{22}x_2(t)+\bar{z}_2(t)$. Then, by incorporating the result of (110) into (108), we have

$$
\begin{aligned}
&\mathrm{h}(y_1^n|s_{22}^n)-\mathrm{h}(\bar{y}_2^n|s_{22}^n)\\
&\le\mathrm{h}(y_1^n|\bar{w}_2)-\mathrm{h}(y_2'^n|\bar{w}_2) \qquad (111)\\
&\le\frac{n}{2}\log\Big(1+P^{\alpha_{11}-\alpha_{21}'}\cdot\frac{|h_{11}|^2}{|h_{21}|^2}+P^{\alpha_{12}-(\alpha_{22}'-\alpha_{21}')^+}\cdot\frac{|h_{12}|^2}{|h_{22}|^2}\Big)\\
&\quad+\frac{n}{2}\log 10 \qquad (112)\\
&=\frac{n}{2}\log\Big(1+P^{\alpha_{11}-\phi_3}\cdot\frac{|h_{11}|^2}{|h_{21}|^2}+P^{\alpha_{12}-(\alpha_{22}-\alpha_{21})^+}\cdot\frac{|h_{12}|^2}{|h_{22}|^2}\Big)\\
&\quad+\frac{n}{2}\log 10 \qquad (113)
\end{aligned}
$$

where (111) is from (108); and (112) follows from (110). Then, we complete the proof of Lemma 3.

Appendix C
Proof of Lemma 4

In this section we provide the proof of Lemma 4. Recall that $y_2(t)$, $s_{22}(t)$, $\bar{x}_1(t)$ and $\bar{x}_2(t)$ are defined in (1), (14), (16), and (17), respectively. In this setting, we have

$$
\begin{aligned}
&\mathrm{h}(\bar{y}_2^n,s_{22}^n|w)-\mathrm{h}(y_1^n,s_{22}^n|w)\\
&=\mathrm{h}(\bar{y}_2^n,s_{22}^n|w)-\mathrm{h}(y_1^n,s_{22}^n,\bar{x}_1^n|w)+\underbrace{\mathrm{h}(\bar{x}_1^n|w,y_1^n,s_{22}^n)}_{\triangleq J_{11}}\\
&=\mathrm{h}(\bar{y}_2^n,s_{22}^n,s_{12}^n,\bar{x}_2^n,\bar{x}_1^n|w)-\underbrace{\mathrm{h}(s_{12}^n,\bar{x}_2^n,\bar{x}_1^n|w,\bar{y}_2^n,s_{22}^n)}_{\triangleq J_{22}}\\
&\quad-\mathrm{h}(y_1^n,s_{22}^n,\bar{x}_1^n|w)+J_{11}\\
&=\mathrm{h}(s_{22}^n,s_{12}^n,\bar{x}_2^n,\bar{x}_1^n|w)+\underbrace{\mathrm{h}(\bar{y}_2^n|w,s_{22}^n,s_{12}^n,\bar{x}_2^n,\bar{x}_1^n)}_{\triangleq J_{33}}\\
&\quad-\mathrm{h}(y_1^n,s_{22}^n,\bar{x}_1^n|w)+J_{11}-J_{22}\\
&=\mathrm{h}(\bar{x}_1^n|w)+\mathrm{h}(s_{22}^n,s_{12}^n|\bar{x}_1^n,w)+\mathrm{h}(\bar{x}_2^n|s_{22}^n,s_{12}^n,\bar{x}_1^n,w)\\
&\quad-\mathrm{h}(\bar{x}_1^n|w)-\mathrm{h}(y_1^n,s_{22}^n|\bar{x}_1^n,w)+J_{11}-J_{22}+J_{33}\\
&=\underbrace{\mathrm{h}(s_{22}^n,s_{12}^n|\bar{x}_1^n,w)}_{=\mathrm{h}(y_1^n,s_{22}^n|\bar{x}_1^n,w,x_1^n)}-\mathrm{h}(y_1^n,s_{22}^n|\bar{x}_1^n,w)\\
&\quad+\mathrm{h}(\bar{x}_2^n|s_{22}^n,s_{12}^n,\bar{x}_1^n,w)+J_{11}-J_{22}+J_{33}\\
&=\underbrace{\mathrm{h}(y_1^n,s_{22}^n|\bar{x}_1^n,w,x_1^n)-\mathrm{h}(y_1^n,s_{22}^n|\bar{x}_1^n,w)}_{=-\mathbb{I}(x_1^n;y_1^n,s_{22}^n|\bar{x}_1^n,w)\le 0}\\
&\quad+\underbrace{\mathrm{h}(\bar{x}_2^n|s_{22}^n,s_{12}^n,\bar{x}_1^n,w)}_{\triangleq J_{44}}+J_{11}-J_{22}+J_{33} \qquad (114)\\
&\le J_{11}-J_{22}+J_{33}+J_{44}. \qquad (115)
\end{aligned}
$$

In the above steps, chain rules are used in the derivations. In addition, (115) uses the fact that mutual information cannot be negative, and (114) follows from the following derivations

$$
\begin{aligned}
&\mathrm{h}(s_{22}^n,s_{12}^n|\bar{x}_1^n,w)\\
&=\mathrm{h}(s_{22}^n,s_{12}^n)\\
&=\mathrm{h}(s_{22}^n,s_{12}^n|\bar{x}_1^n,w,x_1^n)\\
&=\mathrm{h}(s_{22}^n,\{s_{12}(t)+\sqrt{P^{\alpha_{11}}}h_{11}x_1(t)\}_{t=1}^n|\bar{x}_1^n,w,x_1^n)\\
&=\mathrm{h}(s_{22}^n,y_1^n|\bar{x}_1^n,w,x_1^n) \qquad (116)
\end{aligned}
$$

which use the independence between $\{s_{22}^n,s_{12}^n\}$ and $\{\bar{x}_1^n,w,x_1^n\}$, as well as the identity $y_1(t)=\sqrt{P^{\alpha_{11}}}h_{11}x_1(t)+s_{12}(t)$. To complete this proof, we invoke the following lemma.

Lemma 10. *For J_{11}, J_{22}, J_{33}, and J_{44} defined in this section, we have*

$$
\begin{aligned}
J_{11}&\le\frac{n}{2}\log(42\pi e) \qquad (117)\\
J_{22}&\ge\frac{3n}{2}\log(2\pi e) \qquad (118)\\
J_{33}&\le\frac{n}{2}\log(16\pi e) \qquad (119)\\
J_{44}&\le\frac{n}{2}\log\big(2\pi e\big(1+P^{\phi_3-\phi_1}|h_{22}|^2\big)\big) \qquad (120)
\end{aligned}
$$

where $\phi_3 \triangleq \min\{\alpha_{21}, \alpha_{12}, (\alpha_{11} - \phi_1)^+\}$ *and* $\phi_1 \triangleq (\alpha_{12} - (\alpha_{22} - \alpha_{21})^+)^+$.

The proof of Lemma 10 is given in the following subsection. By incorporating the results of Lemma 10 into (115), we have

$$\begin{aligned}
&\mathrm{h}(\bar{y}_2^n, s_{22}^n|w) - \mathrm{h}(y_1^n, s_{22}^n|w) \\
\le& J_{11} - J_{22} + J_{33} + J_{44} \\
\le& \frac{n}{2}\log\big(1 + P^{\phi_3-\phi_1}|h_{22}|^2\big) + \frac{n}{2}\log 168 \qquad (121)
\end{aligned}$$

which completes the proof of Lemma 4.

A. Proof of Lemma 10

Recall that $s_{11}(t) = \sqrt{P^{\alpha_{11}-\alpha_{12}}}h_{11}x_1(t) + \tilde{z}_1(t)$, $s_{22}(t) = \sqrt{P^{(\alpha_{22}-\alpha_{21})^+}}h_{22}x_2(t) + \tilde{z}_2(t)$, $s_{12}(t) = \sqrt{P^{\alpha_{12}}}h_{12}x_2(t) + z_1(t)$, $\bar{x}_1(t) \triangleq \sqrt{P^{\min\{\alpha_{21},\alpha_{12},\alpha_{11}-\phi_1\}}}h_{21}x_1(t) + \bar{z}_3(t)$, $\bar{x}_2(t) \triangleq \sqrt{P^{\phi_3}}\tilde{z}_2(t) + \bar{z}_4(t)$, $\bar{y}_2(t) \triangleq \sqrt{P^{-(\alpha_{21}-\phi_3)}}y_2(t) + \bar{z}_2(t)$, $\phi_3 \triangleq \min\{\alpha_{21}, \alpha_{12}, \phi_2\}$, $\phi_2 \triangleq (\alpha_{11} - \phi_1)^+$ and $\phi_1 \triangleq (\alpha_{12} - (\alpha_{22} - \alpha_{21})^+)^+$.

At first we focus on the bound of J_{11}:

$$\begin{aligned}
&J_{11} \\
=&\mathrm{h}(\bar{x}_1^n|w, y_1^n, s_{22}^n) \\
\le&\sum_{t=1}^{n}\mathrm{h}(\bar{x}_1(t)|y_1(t), s_{22}(t)) \qquad (122) \\
=&\sum_{t=1}^{n}\mathrm{h}\Big(\bar{x}_1(t) - \sqrt{P^{\min\{\alpha_{21},\alpha_{12},\alpha_{11}-\phi_1\}-\alpha_{11}}}\frac{h_{21}}{h_{11}}\big(y_1(t) \\
&- \sqrt{P^{\alpha_{12}-(\alpha_{22}-\alpha_{21})^+}}\frac{h_{12}}{h_{22}}s_{22}(t)\big)\big|y_1(t), s_{22}(t)\Big) \qquad (123) \\
=&\sum_{t=1}^{n}\mathrm{h}\Big(\bar{z}_3(t) - \sqrt{P^{\min\{\alpha_{21},\alpha_{12},\alpha_{11}-\phi_1\}-\alpha_{11}}}\frac{h_{21}}{h_{11}}z_1(t) \\
&+ \sqrt{P^{\min\{\alpha_{21},\alpha_{12},\alpha_{11}-\phi_1\}-\alpha_{11}+\alpha_{12}-(\alpha_{22}-\alpha_{21})^+}}\frac{h_{21}h_{12}}{h_{11}h_{22}}\tilde{z}_2(t) \\
&\Big|y_1(t), s_{22}(t)\Big) \\
\le&\frac{n}{2}\log\Big(2\pi e\big(1 + \underbrace{P^{\min\{\alpha_{21},\alpha_{12},\alpha_{11}-\phi_1\}-\alpha_{11}}}_{\le 1}\cdot\underbrace{\frac{|h_{21}|^2}{|h_{11}|^2}}_{\le 4} \\
&+ \underbrace{P^{\min\{\alpha_{21},\alpha_{12},\alpha_{11}-\phi_1\}-\alpha_{11}+\alpha_{12}-(\alpha_{22}-\alpha_{21})^+}}_{\le 1}\underbrace{\frac{|h_{21}|^2|h_{12}|^2}{|h_{11}|^2|h_{22}|^2}}_{\le 16}\big)\Big) \qquad (124) \\
\le&\frac{n}{2}\log(42\pi e) \qquad (125)
\end{aligned}$$

where (122) follows from chain rule and the fact that conditioning reduces differential entropy; (123) uses the fact that $\mathrm{h}(a|b) = \mathrm{h}(a - \beta b|b)$ for a constant β and two continuous random variables a and b; (124) follows from the fact that Gaussian input maximizes the differential entropy and that conditioning reduces differential entropy; (125) uses the identities $\min\{\alpha_{21}, \alpha_{12}, \alpha_{11} - \phi_1\} - \alpha_{11} \le 0$ and $\min\{\alpha_{21}, \alpha_{12}, \alpha_{11} - \phi_1\} - \alpha_{11} + \alpha_{12} - (\alpha_{22} - \alpha_{21})^+ \le 0$, where $\phi_1 = (\alpha_{12} - (\alpha_{22} - \alpha_{21})^+)^+$.

For J_{22}, it can be bounded by

$$\begin{aligned}
J_{22} &= \mathrm{h}(s_{12}^n, \bar{x}_2^n, \bar{x}_1^n|w, \bar{y}_2^n, s_{22}^n) \\
&\ge \mathrm{h}(s_{12}^n, \bar{x}_2^n, \bar{x}_1^n|w, \bar{y}_2^n, s_{22}^n, x_2^n, x_1^n, \tilde{z}_2^n) \qquad (126) \\
&= \mathrm{h}(z_1^n, \bar{z}_4^n, \bar{z}_3^n) \\
&= \frac{3n}{2}\log(2\pi e) \qquad (127)
\end{aligned}$$

where (126) follows from the fact that conditioning reduces differential entropy.

For J_{33}, we have the following bound:

$$\begin{aligned}
&J_{33} \\
=&\mathrm{h}(\bar{y}_2^n|w, s_{22}^n, s_{12}^n, \bar{x}_2^n, \bar{x}_1^n) \\
\le&\sum_{t=1}^{n}\mathrm{h}(\bar{y}_2(t)|s_{22}(t), \bar{x}_2(t), \bar{x}_1(t)) \qquad (128) \\
=&\sum_{t=1}^{n}\mathrm{h}\Big(\bar{y}_2(t) - \sqrt{P^{-(\alpha_{22}-\alpha_{21})^+ + (\alpha_{22}-\alpha_{21})}}\big(\sqrt{P^{\phi_3}}s_{22}(t) \\
&- \bar{x}_2(t)\big) - \bar{x}_1(t)\Big|s_{22}(t), \bar{x}_2(t), \bar{x}_1(t)\Big) \\
=&\sum_{t=1}^{n}\mathrm{h}\Big(\big(\sqrt{P^{\phi_3}} - \sqrt{P^{\min\{\alpha_{21},\alpha_{12},\alpha_{11}-\phi_1\}}}\big)h_{21}x_1(t) + \bar{z}_2(t) \\
&+ \sqrt{P^{\phi_3-\alpha_{21}}}z_2(t) - \bar{z}_3(t) \\
&+ \sqrt{P^{-(\alpha_{22}-\alpha_{21})^+ + (\alpha_{22}-\alpha_{21})}}\bar{z}_4(t)\Big|s_{22}(t), \bar{x}_2(t), \bar{x}_1(t)\Big) \\
\le&\frac{n}{2}\log\Big(2\pi e\big(\underbrace{\big(\sqrt{P^{\phi_3}} - \sqrt{P^{\min\{\alpha_{21},\alpha_{12},\alpha_{11}-\phi_1\}}}\big)^2}_{\le 1}|h_{21}|^2 + 1 \\
&+ \underbrace{P^{\phi_3-\alpha_{21}}}_{\le 1} + 1 + \underbrace{P^{-(\alpha_{22}-\alpha_{21})^+ + (\alpha_{22}-\alpha_{21})}}_{\le 1}\big)\Big) \qquad (129) \\
\le&\frac{n}{2}\log(16\pi e) \qquad (130)
\end{aligned}$$

where (128) results from chain rule and the fact that conditioning reduces differential entropy; (129) follows from the fact that Gaussian input maximizes the differential entropy and that conditioning reduces differential entropy; (130) uses the identity that $(\sqrt{P^{\min\{\alpha_{21},\alpha_{12},(\alpha_{11}-\phi_1)^+\}}} - \sqrt{P^{\min\{\alpha_{21},\alpha_{12},\alpha_{11}-\phi_1\}}})^2 \le 1$ and the definition that $\phi_3 \triangleq \min\{\alpha_{21}, \alpha_{12}, \phi_2\}$.

For the term J_{44}, we have two different bounds. One bound is given as

$$\begin{aligned}
&J_{44} \\
=&\mathrm{h}(\bar{x}_2^n|s_{22}^n, s_{12}^n, \bar{x}_1^n, w) \\
\le&\sum_{t=1}^{n}\mathrm{h}(\bar{x}_2(t)|s_{22}(t), s_{12}(t)) \qquad (131) \\
=&\sum_{t=1}^{n}\mathrm{h}\Big(\bar{x}_2(t) - \sqrt{P^{\phi_3}}\big(s_{22}(t) \\
&- \sqrt{P^{-\alpha_{12}+(\alpha_{22}-\alpha_{21})^+}}\frac{h_{22}}{h_{12}}s_{12}(t)\big)\big|s_{22}(t), s_{12}(t)\Big) \\
=&\sum_{t=1}^{n}\mathrm{h}\Big(\bar{z}_4(t) \\
&+ \sqrt{P^{\phi_3-\alpha_{12}+(\alpha_{22}-\alpha_{21})^+}}\frac{h_{22}}{h_{12}}z_1(t)\big|s_{22}(t), s_{12}(t)\Big)
\end{aligned}$$

$$\leq \frac{n}{2}\log\Big(2\pi e\Big(1+P^{\phi_3-(\alpha_{12}-(\alpha_{22}-\alpha_{21})^+)}\cdot\frac{|h_{22}|^2}{|h_{12}|^2}\Big)\Big) \quad (132)$$

where (131) results from chain rule and the fact that conditioning reduces differential entropy; (132) follows from the fact that Gaussian input maximizes the differential entropy and that conditioning reduces differential entropy. The other bound is given as

$$J_{44} \leq \sum_{t=1}^{n} \mathrm{h}(\bar{x}_2(t)) \quad (133)$$

$$= \frac{n}{2}\log\big(2\pi e\big(1+P^{\phi_3}\big)\big) \quad (134)$$

where (133) uses the fact that conditioning reduces differential entropy. By combining the bounds in (132) and (134), we finally have

$$\begin{aligned}
&J_{44}\\
&\leq \frac{n}{2}\log\big(2\pi e\big(1+\min\big\{P^{\phi_3},\ P^{\phi_3-(\alpha_{12}-(\alpha_{22}-\alpha_{21})^+)}\frac{|h_{22}|^2}{|h_{12}|^2}\big\}\big)\big)\\
&\leq \frac{n}{2}\log\Big(2\pi e\Big(1\\
&\quad +\min\Big\{P^{\phi_3}|h_{22}|^2,\ P^{\phi_3-(\alpha_{12}-(\alpha_{22}-\alpha_{21})^+)}|h_{22}|^2\Big\}\Big)\Big)\\
&= \frac{n}{2}\log\Big(2\pi e\Big(1+P^{\phi_3-(\alpha_{12}-(\alpha_{22}-\alpha_{21})^+)^+}|h_{22}|^2\Big)\Big) \quad (135)
\end{aligned}$$

which completes the proof of Lemma 10.

Appendix D
Proof of Lemma 5

Before showing the proof of Lemma 5, we describe the result of [38, Lemma 1] below, which will be used later.

Lemma 11. *[38, Lemma 1] Let $y' = \sqrt{P^{\alpha_1}}hx + \sqrt{P^{\alpha_2}}e + z$, with three random variables $z \sim \mathcal{N}(0,\sigma^2)$, $x \in \Omega(\xi, Q)$, and $e \in \mathcal{S}_e$, for a given discrete set $\mathcal{S}_e$, under the condition of*

$$|e| \leq e_{\max}, \quad \forall e \in \mathcal{S}_e.$$

In this model, $e_{\max}$, h, σ, α_1 and α_2 are positive constants independent of P, with a constraint that $\alpha_1 > \alpha_2$. Let $\gamma' > 0$ be a finite constant independent of P. If the parameters Q and ξ are set as

$$Q = \frac{P^{\frac{\alpha'}{2}}\cdot h\gamma'}{2e_{\max}}, \qquad \xi = \gamma'\cdot\frac{1}{Q}, \quad \textit{for} \quad 0<\alpha'<\alpha_1-\alpha_2$$

then the error probability of the estimation of x from y' is

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

Let us now prove Lemma 5. Given the observation y_1 expressed in (51), we will show that v_m and v_p can be estimated from y_1 with vanishing error probability. In this case, y_1 can be described as

$$y_1 = \sqrt{P}h_{11}h_{22}v_m + \sqrt{P^{1-\alpha}}e' + z_1$$

where $e' \triangleq h_{11}h_{22}v_p + \sqrt{P^{3\alpha-2}}h_{12}h_{21}u_p$. In this scenario with $0 \leq \alpha \leq 1/2$, we have

$$|e'| \leq 7/5$$

for any realizations of e'. Note that, $v_m, u_p \in \Omega(\xi = \frac{2\gamma}{Q},\ Q = P^{\frac{\alpha-\epsilon}{2}})$ and $v_p \in \Omega(\xi = \frac{\gamma}{Q},\ Q = P^{\frac{1-\alpha-\epsilon}{2}})$, for some parameters $\gamma \in (0, 1/20]$ and $\epsilon \to 0$. Then, by Lemma 11, it holds true that the error probability of the estimation of v_m from y_1 is

$$\Pr[v_m \neq \hat{v}_m] \to 0, \quad \text{as} \quad P\to\infty. \quad (136)$$

In the next step, we remove v_m from y_1 and then estimate v_p from the following observation

$$y_1' = \sqrt{P^{1-\alpha}}h_{11}h_{22}v_p + \sqrt{P^{2\alpha-1}}h_{12}h_{21}u_p + z_1. \quad (137)$$

For the second term in the right-hand side of (137), the following condition is always satisfied

$$|h_{12}h_{21}u_p| \leq 4\times 2\gamma \leq 2/5.$$

Therefore, by Lemma 11, it is also true that the error probability of the estimation of v_p from y_1' expressed in (137) is

$$\Pr[v_p \neq \hat{v}_p | v_m = \hat{v}_m] \to 0, \quad \text{as} \quad P\to\infty. \quad (138)$$

At this point, by combining the results of (136) and (138), it gives

$$\Pr[\{v_m \neq \hat{v}_m\}\cup\{v_p \neq \hat{v}_p\}] \to 0 \quad \text{as} \quad P\to\infty.$$

Appendix E
Proof of Lemma 7

Given the case with $1 \leq \alpha \leq 4/3$, we will show that v_c and u_c can be estimated from y_1 with vanishing error probability, for almost all the channel realizations. Recall that $v_c, u_c \in \Omega(\xi = \frac{6\gamma}{Q},\ Q = P^{\frac{\alpha/2-\epsilon}{2}})$, for some parameters $\gamma \in (0, 1/20]$ and $\epsilon \to 0$. Let us describe y_1 in the following form

$$\begin{aligned}
y_1 &= \sqrt{P^{2-\alpha}}h_{11}h_{22}v_c + \sqrt{P^{\alpha}}h_{12}h_{21}u_c + z_1\\
&= 6\gamma P^{\epsilon/2}\underbrace{(A_0'g_0'q_0' + A_1'g_1'q_1')}_{\triangleq \tilde{s}'} + z_1\\
&= 6\gamma P^{\epsilon/2}\tilde{s}' + z_1 \quad (139)
\end{aligned}$$

where $g_0' \triangleq h_{11}h_{22}$, $g_1' \triangleq h_{12}h_{21}$, $A_0' \triangleq \sqrt{P^{2-3\alpha/2}}$, $A_1' \triangleq \sqrt{P^{\alpha/2}}$, $\tilde{s}' \triangleq A_0'g_0'q_0' + A_1'g_1'q_1'$ and

$$q_0' \triangleq \frac{Q_0'}{6\gamma}\cdot v_c, \quad q_1' \triangleq \frac{Q_1'}{6\gamma}\cdot u_c, \quad Q_1' \triangleq Q_0' \triangleq P^{\frac{\alpha/2-\epsilon}{2}}.$$

In this scenario, the following conditions are always satisfied: $q_0', q_1' \in \mathcal{Z}$, $|q_0'| \leq Q_0'$ and $|q_1'| \leq Q_0'$. Similar to the proof of Lemma 6, without loss of generality we will consider the case that $Q_0', A_0', A_1' \in \mathcal{Z}^+$.

For the observation y_1 in (139), our focus is to estimate the sum $\tilde{s}' = A_0'g_0'q_0' + A_1'g_1'q_1'$. After decoding $\tilde{s}'$ correctly, q_0' and q_1' can be recovered, because $\{g_0', g_1'\}$ are rationally independent. We define the minimum distance of $\tilde{s}'$ as

$$d'_{\min}(g_0', g_1') \triangleq \min_{\substack{q_0',q_1',\tilde{q}_0',\tilde{q}_1' \in \mathcal{Z}\cap[-Q_0', Q_0']\\ (q_0',q_1')\neq(\tilde{q}_0',\tilde{q}_1')}} |A_0'g_0'(q_0'-\tilde{q}_0') + A_1'g_1'(q_1'-\tilde{q}_1')|. \quad (140)$$

The following lemma provides a result on the minimum distance.

Lemma 12. *For the case with $1 \le \alpha \le 4/3$, and for some constants $\delta \in (0,1]$ and $\epsilon > 0$, the following bound on the minimum distance $d'_{\min}$ defined in* (140) *holds true*

$$d'_{\min} \ge \delta \tag{141}$$

for all the channel realizations $\{h_{11}, h_{12}, h_{22}, h_{21}\} \in (1,2]^{2\times 2} \backslash \mathcal{H}'_{out}$, where $\mathcal{H}'_{out} \subseteq (1,2]^{2\times 2}$ is an outage set whose Lebesgue measure, denoted by $\mathcal{L}(\mathcal{H}'_{out})$, has the following bound

$$\mathcal{L}(\mathcal{H}'_{out}) \le 192\delta \cdot P^{-\frac{\epsilon}{2}}. \tag{142}$$

Proof. For $\beta \triangleq \delta \in (0,1]$, we define an event as

$$B'(q'_1, q'_0) \triangleq \{(g'_1, g'_0) \in (1,4]^2 : |A'_1 g'_1 q'_1 + A'_0 g'_0 q'_0| < \beta\} \tag{143}$$

and define

$$B' \triangleq \bigcup_{\substack{q'_0, q'_1 \in \mathcal{Z}: \\ |q'_k| \le 2Q'_0 \ \forall k \\ (q'_0, q'_1) \ne 0}} B'(q'_1, q'_0). \tag{144}$$

For this case with $1 \le \alpha \le 4/3$, by [39, Lemma 1] we have a bound on the Lebesgue measure of B', given as

$$\begin{aligned}\mathcal{L}(B') &\le 24\beta \min\Big\{\frac{4Q'_1Q'_0}{A'_1}, \frac{4Q'_0Q'_1}{A'_0}, \frac{8Q'_0}{A'_1}, \frac{8Q'_1}{A'_0}\Big\} \\ &\le 24\beta \cdot \frac{8Q'_0}{A'_1} \\ &= 192\delta \cdot P^{-\frac{\epsilon}{2}}.\end{aligned} \tag{145}$$

At this point, we define a new set $\mathcal{H}'_{\text{out}}$ as

$$\mathcal{H}'_{\text{out}} \triangleq \{(h_{11}, h_{22}, h_{12}, h_{21}) \in (1,2]^{2\times 2} : (g'_1, g'_0) \in B'\}.$$

By following the steps related to (96), we have the following bound on the Lebesgue measure of $\mathcal{H}'_{\text{out}}$

$$\mathcal{L}(\mathcal{H}'_{\text{out}}) \le \mathcal{L}(B') \le 192\delta \cdot P^{-\frac{\epsilon}{2}}. \tag{146}$$

□

Lemma 12 reveals that the Lebesgue measure of the outage set $\mathcal{H}'_{\text{out}}$ is vanishing when P is large, i.e.,

$$\mathcal{L}(\mathcal{H}'_{\text{out}}) \to 0, \quad \text{for} \quad P \to \infty.$$

Let us now consider the channel condition that $(h_{11}, h_{22}, h_{12}, h_{21}) \notin \mathcal{H}'_{\text{out}}$, in which the minimum distance of $\tilde{s}'$, defined in (90), satisfies the inequality of $d'_{\min} \ge \delta$ (see (141)). With this result, we can conclude that the error probability for decoding $\tilde{s}'$ from $y_1 = 6\gamma P^{\epsilon/2}\tilde{s}' + z_1$ (see (139)), denoted by $\Pr[\tilde{s}' \ne \hat{\tilde{s}}]$, is

$$\Pr[\tilde{s}' \ne \hat{\tilde{s}}'] \to 0 \quad \text{for} \quad P \to \infty$$

for almost all the channel realizations in the regime of large P. After decoding $\tilde{s}'$ correctly, q'_0 and q'_1 can be recovered, based on the fact that $\{g'_0, g'_1\}$ are rationally independent. Then, we complete the proof.

APPENDIX F
SECURE GDOF OF THE GAUSSIAN WIRETAP CHANNEL *without* A HELPER

This section focuses on the wiretap channel *without* a helper (removing transmitter 2). For this channel, the goal is to understand the GDoF based on the capacity result of [2], [3], which will be used for the GDoF comparison of the wiretap channels with and without a helper. For the wiretap channel *without* a helper, the secure capacity, denoted by C_{no}, is given by:

$$C_{no} = \max_{v \to x_1 \to y_1, y_2} \mathbb{I}(v; y_1) - \mathbb{I}(v; y_2) \tag{147}$$

(cf. [2], [3]), where the maximum is computed over all random variables v, x_1, y_1, y_2 such that $v \to x_1 \to y_1, y_2$ forms a Markov chain, and $y_k = \sqrt{P^{\alpha_{k1}}} h_{k1} x_1 + z_k$ for $k = 1, 2$. Let us focus on the upper bound on the following difference:

$$\begin{aligned}&\mathbb{I}(v; y_1) - \mathbb{I}(v; y_2) \\ \le& \mathbb{I}(v; y_1, y_2) - \mathbb{I}(v; y_2) \\ =& \mathrm{h}(y_1|y_2) - \mathrm{h}(y_1|y_2, v) \\ \le& \mathrm{h}(y_1|y_2) - \mathrm{h}(y_1|y_2, v, x_1) &(148)\\ =& \mathrm{h}(y_1|y_2) - \frac{1}{2}\log(2\pi e) &(149)\\ =& \mathrm{h}(y_1 - \sqrt{P^{\alpha_{11}-\alpha_{21}}}\frac{h_{11}}{h_{21}} y_2|y_2) - \frac{1}{2}\log(2\pi e) \\ =& \mathrm{h}(z_1 - \sqrt{P^{\alpha_{11}-\alpha_{21}}}\frac{h_{11}}{h_{21}} z_2|y_2) - \frac{1}{2}\log(2\pi e) \\ \le& \mathrm{h}(z_1 - \sqrt{P^{\alpha_{11}-\alpha_{21}}}\frac{h_{11}}{h_{21}} z_2) - \frac{1}{2}\log(2\pi e) &(150)\\ =& \frac{1}{2}\log(1 + P^{\alpha_{11}-\alpha_{21}}\frac{|h_{11}|^2}{|h_{21}|^2}) &(151)\end{aligned}$$

where (148) and (150) use the identity that conditioning reduces differential entropy; (149) results from the fact that $\mathrm{h}(y_1|y_2, v, x_1) = \mathrm{h}(z_1) = \frac{1}{2}\log(2\pi e)$. By combining (147) and (151), the secure GDoF, denoted by d_{no}, is upper bounded by

$$d_{no} \le (\alpha_{11} - \alpha_{21})^+. \tag{152}$$

On the other hand, since the secure capacity is optimized over the random variables v and x_1, by setting $x_1 = v \sim \mathcal{N}(0,1)$ we have the lower bound on the secure capacity:

$$\begin{aligned}C_{no} \ge& \mathbb{I}(v; y_1) - \mathbb{I}(v; y_2) \\ =& \mathrm{h}(\sqrt{P^{\alpha_{11}}} h_{11} x_1 + z_1) - \mathrm{h}(z_1) \\ &- \mathrm{h}(\sqrt{P^{\alpha_{21}}} h_{21} x_1 + z_2) + \mathrm{h}(z_2) \\ =& \frac{1}{2}\log(1 + P^{\alpha_{11}}|h_{11}|^2) - \frac{1}{2}\log(1 + P^{\alpha_{21}}|h_{21}|^2).\end{aligned} \tag{153}$$

The bound in (153) reveals that the secure GDoF is lower bounded by

$$d_{no} \ge (\alpha_{11} - \alpha_{21})^+ \tag{154}$$

which, together with (152), gives the optimal secure GDoF

$$d_{no} = (\alpha_{11} - \alpha_{21})^+. \tag{155}$$

For the symmetric case of notation with $\alpha_{11}=1$ and $\alpha_{12}=\alpha$, this secure GDoF becomes

$$d_{no}=(1-\alpha)^+ \quad \forall \alpha\in[0,\infty).$$

Appendix G
Proof of Corollary 2

For the symmetric setting with $\alpha_{11}=\alpha_{22}=1, \alpha_{21}=\alpha_{12}=\alpha$, ϕ_1 and ϕ_3 take the following forms:

$$\phi_1=(\alpha-(1-\alpha)^+)^+$$
$$\phi_3=\min\{\alpha,(1-(\alpha-(1-\alpha)^+)^+)^+\}.$$

In this symmetric case, the three bounds in Corollary 1 then become

$$d\le \max\{\phi_1,(1-\phi_3)^+\}+(\phi_3-\phi_1)^+ \tag{156}$$
$$d\le (1-\alpha)^+ +\frac{\max\{1,\alpha\}}{2} \tag{157}$$
$$d\le (2-\alpha)^+. \tag{158}$$

When $0\le\alpha\le 1/2$, it reveals that $\phi_1=0$ and $\phi_3=\alpha$, and the bounds in (156)-(158) can be simplified as

$$d\le 1$$
$$d\le 3/2-\alpha$$
$$d\le 2-\alpha$$

which implies that

$$d\le \min\{1,3/2-\alpha,2-\alpha\}=1, \quad \forall\alpha\in[0,1/2].$$

When $1/2\le\alpha\le 1$, it suggests that $\phi_1=2\alpha-1$ and $\phi_3=\min\{\alpha,2(1-\alpha)\}$. Then, the bounds in (156)-(158) can be simplified as

$$d\le \max\{2\alpha-1,1-\alpha\}+\min\{1-\alpha,(3-4\alpha)^+\}$$
$$d\le 3/2-\alpha$$
$$d\le 2-\alpha.$$

From the above results, the GDoF d can be bounded as

$$d\le\min\{2-2\alpha,3/2-\alpha,2-\alpha\}=2-2\alpha,\ \forall\alpha\in[\frac{1}{2},\frac{3}{4}]$$
$$d\le\min\{2\alpha-1,3/2-\alpha,2-\alpha\}=2\alpha-1,\ \forall\alpha\in[\frac{3}{4},\frac{5}{6}]$$
$$d\le\min\{2\alpha-1,3/2-\alpha,2-\alpha\}=3/2-\alpha,\forall\alpha\in[\frac{5}{6},1].$$

When $1\le\alpha$, then $\phi_1=(\alpha-(1-\alpha)^+)^+=\alpha$ and $\phi_3=0$, and the bounds in (156)-(158) can be simplified as

$$d\le\alpha$$
$$d\le\alpha/2$$
$$d\le(2-\alpha)^+.$$

The above results imply that

$$d\le\min\{(2-\alpha)^+,\ \alpha/2\}=\alpha/2, \qquad \forall\alpha\in[1,4/3]$$
$$d\le\min\{(2-\alpha)^+,\ \alpha/2\}=2-\alpha, \qquad \forall\alpha\in[4/3,2]$$
$$d\le\min\{(2-\alpha)^+,\ \alpha/2\}=0, \qquad \forall\alpha\in[2,+\infty].$$

At this point we complete the proof.

Appendix H
Alternative proof on the achievable secure GDoF in the regimes of $0\le\alpha\le 3/4$

In this section we provide an alternative proof on the achievable secure GDoF in the regimes of $0\le\alpha\le 3/4$ based on a scheme of treating interference as noise.

In the previous work of [38], the author considered a two-user Gaussian interference channel with confidential messages and proposed a scheme in which, each transmitter simply employs a Gaussian wiretap codebook (GWC) to guarantee the secrecy, while each receiver simply treats interference as noise (TIN) when decoding its desired message. This scheme is called as a GWC-TIN scheme (see Section II-B in [38]). Note that the wiretap channel with a helper can be considered as a specific case of the two-user interference channel with confidential messages, by setting the second transmitter's the message empty. Therefore, by treating the message of the second transmitter as a random noise in the GWC-TIN scheme, one can conclude that in the wiretap channel with a helper the following secure rate of the message sent from transmitter 1 to receiver 1 is achievable

$$R\triangleq\big[\mathbb{I}(v_1;y_1)-\mathbb{I}(v_1;y_2)-\epsilon\big]^+ \tag{159}$$

for some $\epsilon>0$, where $y_1=\sqrt{P^{\alpha_{11}}}h_{11}v_1+\sqrt{P^{\alpha_{12}}}h_{12}v_2+z_1$, $y_2=\sqrt{P^{\alpha_{22}}}h_{22}v_2+\sqrt{P^{\alpha_{21}}}h_{21}v_1+z_2$, $v_1\sim\mathcal{N}(0,P^{-\beta_1})$ and $v_2\sim\mathcal{N}(0,P^{-\beta_2})$ for some $\beta_1,\beta_2\ge 0$ (cf. (9)-(15) in [38]). By setting $\epsilon\to 0$, the above secure rate R can be expressed as

$$R=\Big[\underbrace{\frac{1}{2}\log\big(1+\frac{|h_{11}|^2P^{\alpha_{11}-\beta_1}}{1+|h_{12}|^2P^{\alpha_{12}-\beta_2}}\big)}_{=\mathbb{I}(v_1;y_1)} - \underbrace{\frac{1}{2}\log(1+\frac{|h_{21}|^2P^{\alpha_{21}-\beta_1}}{1+|h_{22}|^2P^{\alpha_{22}-\beta_2}})}_{=\mathbb{I}(v_1;y_2)}\Big]^+. \tag{160}$$

Let us focus on the symmetric wiretap channel with a helper considered here, with $(\alpha_{12}=\alpha_{21}=\alpha,\alpha_{22}=\alpha_{11}=1)$. For the regime of $0\le\alpha\le 3/4$, by setting the parameters β_1 and β_2 as $\beta_1=0$ and $\beta_2=\alpha$, the rate in (160) becomes

$$\begin{aligned}R&=\Big[\frac{1}{2}\log\big(\frac{(1+|h_{12}|^2P^{\alpha-\beta_2}+|h_{11}|^2P^{1-\beta_1})(1+|h_{22}|^2P^{1-\beta_2})}{(1+|h_{12}|^2P^{\alpha-\beta_2})(1+|h_{22}|^2P^{1-\beta_2}+|h_{21}|^2P^{\alpha-\beta_1})}\big)\Big]^+\\&=\Big[\frac{1}{2}\log\Big(\frac{(1+|h_{12}|^2+|h_{11}|^2P)(1+|h_{22}|^2P^{1-\alpha})}{(1+|h_{12}|^2)(1+|h_{22}|^2P^{1-\alpha}+|h_{21}|^2P^{\alpha})}\Big)\Big]^+\end{aligned} \tag{161}$$

which implies that the following secure GDoF is achievable

$$d=[2-\alpha-\max\{1-\alpha,\alpha\}]^+=\begin{cases}1 & \text{for } 0\le\alpha\le 1/2\\ 2-2\alpha & \text{for } 1/2\le\alpha\le 3/4\end{cases}.$$

This achievable secure GDoF matches the achievable secure GDoF described in Section V for the regimes of $0\le\alpha\le 3/4$, which is optimal.

Acknowledgement

We wish to thank the Associate Editor and the anonymous reviewers for their helpful comments.

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] 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.

[6] ——, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[7] 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.

[8] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "On the secure DoF of the single-antenna MAC," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2010.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

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

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

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

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

[34] 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.

[35] J. Chen. (Jun. 2017). "On the optimality of secure communication without using cooperative jamming." [Online]. Available: http://arxiv.org/abs/1706.06220.

[36] 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.

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

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

[39] 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.

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

[41] 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.

[42] ——, "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.

[43] 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.

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

[45] 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.

[46] 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.

[47] 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.

[48] 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.

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.

Chunhua Geng (S'12-M'16) received his B.E. degree in Communication Engineering from Beijing Jiaotong University, Beijing, China, in 2007, M.S. degree in Electronic Engineering from Tsinghua University, Beijing, China, in 2010, and Ph.D. degree in Electrical Engineering from University of California Irvine, Irvine, CA, USA, in 2016. Currently, he is with MediaTek USA Inc., Irvine, CA, USA. From 2016 to 2020, he was a research scientist in Nokia Bell Labs, Murray Hill, NJ, USA. Dr. Geng was a recipient of the Exemplary Reviewer for IEEE Transactions on Communications in 2015. His research interests include network information theory, wireless communications, localization and sensing, and physical layer security.