Secure Degrees of Freedom of the Gaussian Diamond-Wiretap Channel

Si-Hyeon Lee, *Member, IEEE,* Wanyao Zhao, *Member, IEEE,* and Ashish Khisti, *Member, IEEE*

Abstract—In this paper, we consider the Gaussian diamond-wiretap channel that consists of an orthogonal broadcast channel from a source to two relays and a Gaussian fast-fading multiple access-wiretap channel from the two relays to a legitimate destination and an eavesdropper. For the multiple access part, we consider both the case with full channel state information (CSI) and the case with no eavesdropper's CSI, at the relays and the legitimate destination. For both the cases, we establish the exact secure degrees of freedom and generalize the results for multiple relays.

Our results show (i) how to strike a balance between sending message symbols and common noise symbols from the source to the relays in the broadcast component and (ii) how to combine artificial noise-beamforming and noise-alignment techniques at the relays in the multiple access component. In the case with full CSI, we propose a scheme where the relays simultaneously beamform common noise signals in the null space of the legitimate destination's channel, and align them with the message signals at the eavesdropper. In the case with no eavesdropper's CSI, we present a scheme that efficiently utilizes the broadcast links by incorporating computation between the message and common noise symbols at the source. Finally, most of our achievability and converse techniques can also be adapted to the Gaussian (non-fading) channel model.

Index Terms—Physical layer security, secure degrees of freedom, diamond-wiretap channel, artificial noise-beamforming, artificial noise-alignment

I. INTRODUCTION

A model of wiretap channel was first studied by Wyner [2], where a source wishes to send its message to a legitimate destination while keeping it secret from an eavesdropper. Wyner established the secrecy capacity for the degraded case where the eavesdropper receives a physically degraded version of the channel output at the legitimate destination. Csiszár and Körner generalized his work to general, not necessarily degraded, discrete memoryless wiretap channel [3]. This line of work has been subsequently extended to various multi-user scenarios, see e.g., [4]–[16], however, the characterization of the secrecy capacity remains a challenging open problem in general. In fact, even for the seemingly simple case of the Gaussian multiple access-wiretap channel, the secrecy capacity is only known for the degraded case [9].

Recently, as an alternative but insightful measure, the secure degrees of freedom (d.o.f.) has been actively studied [17]–[20]

for various multi-user wiretap networks. For the Gaussian multiple access-wiretap channel, the sum secure d.o.f. was shown to be $\frac{2}{3}$ for almost all channel gains [18]. For achievability, a cooperative jamming scheme was proposed that incorporates real interference alignment [21] at the legitimate destination and the eavesdropper. In many practical scenarios, however, it is hard for the source and the legitimate destination to know the eavesdropper's channel state information (CSI). In [20], the secure d.o.f. with no eavesdropper's CSI was characterized for some interesting one-hop wiretap channels. For the Gaussian multiple access-wiretap channel, the sum secure d.o.f. was shown in [20] to reduce to $\frac{1}{2}$ with no eavesdropper's CSIT, which is achieved by a blind cooperative jamming scheme. We note that the prior work has focused on one-hop wiretap networks, and to the best of our knowledge, there has been no prior work on the secure d.o.f. for multi-hop wiretap networks.

In this paper, we consider the Gaussian diamond-wiretap channel illustrated in Fig. 1 that consists of an orthogonal broadcast channel from a source to two relays and a Gaussian multiple access-wiretap channel from the two relays to a legitimate destination and an eavesdropper. We consider both the case where the relays and the legitimate destination know the legitimate CSI and the eavesdropper's CSI and the case where they know only the legitimate CSI, which we call the case with full CSI and the case with no eavesdropper's CSI, respectively. As a pessimistic scenario, we assume that the source does not know any of the legitimate CSI and the eavesdropper's CSI and the eavesdropper knows both the CSI's.[1] The proposed setting is a two-hop communication network and involves several new elements not present in the single-hop networks studied previously. Our model introduces a new possibility of utilizing common message and/or common noise for the Gaussian multiple access-wiretap channel. This brings in an interesting tension in the use of the broadcast links regarding whether we send independent messages, common message, common noise, or a function of those across the broadcast part. At one extreme, when the capacities of the orthogonal links in the broadcast part are sufficiently small, the optimal strategy turns out to send independent partial message to each relay and incorporate jamming schemes [18], [20] for the multiple access part. At the other extreme, when the broadcast part has sufficiently high capacity to transmit common message

S.-H. Lee and A. Khisti are with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, Canada (e-mail: sihyeon.lee@utoronto.ca; akhisti@comm.utoronto.ca). W. Zhao was at University of Toronto when this work was done. The material in this paper was presented in part at IEEE ISIT 2016 [1]. This work was supported by QNRF, a member of Qatar Foundation, under NPRP project 5-401-2-161.

---

[1]The source may not know the legitimate CSI when it is apart from the legitimate destination. However, we note that both our converse and achievability results hold when the source knows the legitimate CSI. We also note that the secrecy under the assumption of global CSI at the eavesdropper guarantees secrecy when the eavesdropper has limited knowledge of CSI. Such an assumption of global CSI at the eavesdropper is widely used for wiretap fading channels, e.g., [20], [22].
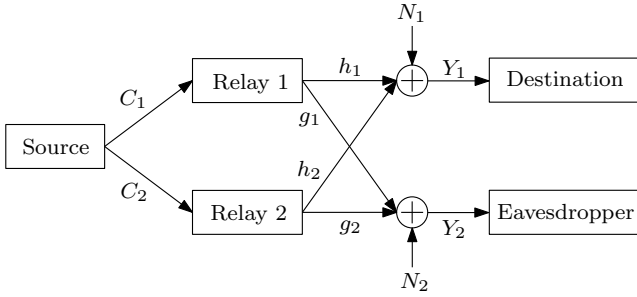
Figure 1. The Gaussian diamond-wiretap channel.

or common noise symbols to the relays, without incurring bottleneck, it follows that the secure d.o.f. equals 1 using the results [23]–[25] for the multiple-input single-output (MISO) wiretap channel. When the link capacities of the broadcast part are moderate, however, the optimal scheme is not immediate. Furthermore, due to the possibility of sending common information across the broadcast part, we cannot assume in proving converse that the channel inputs and outputs at the relays are independent, whereas channel inputs at transmitters are inherently independent in most one-hop wiretap networks.

In the absence of secrecy constraint, our model falls back to the diamond channel introduced by Schein [26], whose capacity is not known in general. For a range of moderate link capacities at the broadcast part, [27]–[30] characterized the capacity of the diamond channel, which is strictly tighter than the cutset bound. For achievability, a coding scheme incorporating multicoding at the source was proposed in [27], [28]. This scheme was generalized in [29], [30] by considering common message sent to the relays. For converse, [28], [29] used a technique from [31] to take into account the correlation between the two relay signals. The converse proof technique used in [28], [29] was refined and tightened in [30] and was generalized in [32] for the scenario where there are two destinations. In the presence of a secrecy constraint, such converse proof techniques need to be adopted carefully by taking into account the stochastic encoding functions introduced to confuse the eavesdropper. Those works [27], [28] were generalized in [33] for the degraded Gaussian diamond-wiretap channel, in which the secrecy capacity was characterized for several ranges of channel parameters. For non-degraded case, however, the coding scheme used in [33] achieves zero secure d.o.f. and structured codes such as interference alignment and beamforming schemes need to be involved to achieve a positive secure d.o.f.

For the Gaussian diamond-wiretap channel in Fig. 1, we establish the exact secure d.o.f. in terms of the link d.o.f.'s at the broadcast part, both for the case with full CSI and for the case with no eavesdropper's CSI. In the converse proof for the case with full CSI, we assume a deterministic model as in [20, Section 4.2.1] and then apply similar steps to the secrecy penalty lemma [18, Lemma 1]. As a result, we encounter a term corresponding to the amount of independent randomness that is injected at each relay to confuse the eavesdropper. Such randomness cannot be too large due to the reliability constraint

at the legitimate receiver. To capture the trade-off between the message rate and the amount of such randomness, we adapt the proof steps of the role of a helper lemma [18, Lemma 2] for our model. For the case with no eavesdropper's CSI, we use one more known result from [20], [34] that the entropy of the channel output sequence at a receiver whose CSI is not available at the transmitters is at least as large as that at a receiver whose CSI is available.

Our achievability part is based on five key constituent schemes. In particular, we propose two new schemes that utilize common noise, in a way that the common noise signals are beam-formed in the null space of the legitimate destination's channel. One of these two schemes is for the case with full CSI and is called a simultaneous alignment and beamforming (S-AB) scheme, which incorporates alignment of the message and the common noise signals at the eavesdropper. The proposed S-AB scheme also extends easily to the case with more than two relays and yields the best achievable secure d.o.f. The other scheme is for the case with no eavesdropper's CSI and is called a computation for jamming (CoJ) scheme, which efficiently utilizes the broadcast links by incorporating computation between the message and the common noise symbols at the source. The remaining three schemes are straightforward extensions of the previously known schemes, i.e., the cooperative jamming scheme [18] and blind cooperative jamming scheme [20] for the Gaussian multiple access-wiretap channel and the message-beamforming scheme [23], [24] for the Gaussian MISO wiretap channel.

As a natural extension, we also consider a generalized Gaussian diamond-wiretap channel with more than two relays. For the brevity of the results, we consider the symmetric case where the link d.o.f.'s of the broadcast part are the same. By generalizing the proof techniques used in the two-relay case, we establish the exact secure d.o.f. for the case with no eavesdropper's CSI and present upper and lower bounds on the secure d.o.f. for the case with full CSI.

The remaining of this paper is organized as follows. In Section II, we formally present the model of the Gaussian diamond-wiretap channel. Our main results on the secure d.o.f. are given in Section III. In Sections IV and V, we prove the converse and the achievability parts, respectively. We extend the results for the case with multiple relays in Section VI. We conclude this paper in Section VII.

II. SYSTEM MODEL

Consider the Gaussian diamond-wiretap channel illustrated in Fig. 1 that consists of a broadcast channel from a source to two relays and a Gaussian multiple access-wiretap channel from the two relays to a legitimate destination and an eavesdropper. For the broadcast part, the source is connected to the two relays through orthogonal links of capacities C_1 and C_2. For the multiple access part, the channel outputs $Y_1(t)$ and $Y_2(t)$ at time t at the legitimate destination and the eavesdropper, respectively, are given as

$$Y_1(t) = h_1(t)X_1(t) + h_2(t)X_2(t) + N_1(t) \qquad (1)$$
$$Y_2(t) = g_1(t)X_1(t) + g_2(t)X_2(t) + N_2(t), \qquad (2)$$

where $X_1(t)$ and $X_2(t)$ are the channel inputs from relays 1 and 2, respectively, $h_k(t)$ and $g_k(t)$ for $k = 1, 2$ are the channel fading coefficients to the legitimate destination and the eavesdropper, respectively, and $N_1(t)$ and $N_2(t)$ are independent Gaussian noise with zero mean and unit variance at the legitimate destination and the eavesdropper, respectively, at time t. The transmit power constraint at relay $k = 1, 2$ is given as $\frac{1}{n} \sum_{t=1}^{n} X_k^2(t) \leq P$, where n denotes the number of channel uses.

We assume a fast fading scenario where $h_1(t)$, $h_2(t)$, $g_1(t)$, and $g_2(t)$ are drawn in an i.i.d. fashion over time according to an arbitrary real-valued joint density function $f(h_1, h_2, g_1, g_2)$, whose all joint and conditional density functions are bounded and whose support set does not include zero and infinity, i.e., there exists a positive finite L such that

$$\frac{1}{L} \leq |h_k(t)|, |g_k(t)| \leq L. \tag{3}$$

We note that (3) is a mild technical condition because by choosing L large enough, the omitted support set can be reduced to a negligible probability that has a vanishing impact on the degrees of freedom. For notational convenience, let $\mathbf{h}^t = [h_1(1)\ h_2(1)\ \cdots\ h_1(t)\ h_2(t)]$ and $\mathbf{g}^t = [g_1(1)\ g_2(1)\ \cdots\ g_1(t)\ g_2(t)]$ denote the legitimate channel state information (CSI) and the eavesdropper's CSI up to time t, respectively.

We assume that the source does not know any of the legitimate CSI and the eavesdropper's CSI and the eavesdropper knows both the CSI's. Two cases are considered regarding the availability of CSI at the relays and the legitimate destination. First, we consider a case where both the legitimate CSI and the eavesdropper's CSI are available at the two relays and the legitimate destination, which we call the case with full CSI. We also consider another case where only the legitimate CSI is available at the two relays and the legitimate destination, which we call a case with no eavesdropper's CSI. We note that our achievability and converse techniques for the case with full CSI and our achievability technique for the case with no eavesdropper's CSI can be adapted for the scenario with fixed channel gains over time and for the scenario with complex channel fading coefficients, as remarked at the end of Section III.

A $(2^{nR}, n)$ secrecy code consists of a message $W \sim \text{Unif}[1 : 2^{nR}]$,[2] a stochastic encoder at the source that (randomly) maps $W \in [1 : 2^{nR}]$ to $(J_1, J_2) \in [1 : 2^{nC_1}] \times [1 : 2^{nC_2}]$, a stochastic encoder at time $t = 1, \ldots, n$ at relay $k = 1, 2$ that (randomly) maps $(J_k, \mathbf{h}^t, \mathbf{g}^t)$ and $(J_k, \mathbf{h}^t)$ for the case with full CSI and for the case with no eavesdropper's CSI, respectively, to $X_k(t) \in \mathcal{X}_k$, and a decoding function at the legitimate destination that maps $(Y_1^n, \mathbf{h}^n, \mathbf{g}^n)$ and $(Y_1^n, \mathbf{h}^n)$ for the case with full CSI and for the case with no eavesdropper's CSI, respectively, to $\hat{W} \in [1 : 2^{nR}]$. The probability of error is given as $P_e^{(n)} = P(\hat{W} \neq W)$. A secrecy rate of R is said to be achievable if there exists a sequence of $(2^{nR}, n)$ codes such that $\lim_{n \to \infty} P_e^{(n)} = 0$ and

$\lim_{n \to \infty} \frac{1}{n} I(W; Y_2^n | \mathbf{h}^n, \mathbf{g}^n) = 0$.[3] The secrecy capacity is the supremum of all achievable secrecy rates.

In this paper, we are interested in asymptotic behavior of the secrecy capacity when P tends to infinity. We say a d.o.f. tuple $(\alpha_1, \alpha_2, d_s)$ is achievable if a rate R with $d_s = \lim_{P \to \infty} \frac{R}{\frac{1}{2} \log P}$ is achievable when C_1 and C_2 satisfy

$$\alpha_1 = \lim_{P \to \infty} \frac{C_1}{\frac{1}{2} \log P}, \quad \alpha_2 = \lim_{P \to \infty} \frac{C_2}{\frac{1}{2} \log P}.$$

A secure d.o.f. $d_s(\alpha_1, \alpha_2)$ is the maximum d_s such that $(\alpha_1, \alpha_2, d_s)$ is achievable. For brevity, d_s denotes $d_s(\alpha_1, \alpha_2)$ according to the context. Without loss of generality, let us assume $C_1 \geq C_2$, which implies $\alpha_1 \geq \alpha_2$.

III. MAIN RESULTS

In this section, we state our main results of this paper. The following two theorems present the secure d.o.f. of the Gaussian diamond-wiretap channel for the case with full CSI and for the case with no eavesdropper's CSI, respectively, whose proofs are in Section IV for the converse parts and in Section V for the achievability parts.

Theorem 1. *The secure d.o.f. of the Gaussian diamond-wiretap channel with full CSI at the relays and the legitimate destination is equal to*

$$d_s = \min\left\{\alpha_1 + \alpha_2, \frac{\alpha_2 + 1}{2}, 1\right\}. \tag{4}$$

Theorem 2. *The secure d.o.f. of the Gaussian diamond-wiretap channel with no eavesdropper's CSI at the relays and the legitimate destination is equal to*

$$d_s = \min\left\{\alpha_1 + \alpha_2, \frac{\alpha_1 + \alpha_2 + 1}{3}, \frac{\alpha_2 + 1}{2}, 1\right\}. \tag{5}$$

We note that the secure d.o.f. of the classical Gaussian wiretap channel is zero. Theorems 1 and 2 show that the secure d.o.f. can be greatly improved by deploying relays. First, note that even if $\alpha_2 = 0$, the secure d.o.f. of $\frac{1}{2}$ is achievable as long as $\alpha_1 \geq \frac{1}{2}$, both for the case with full CSI and for the case with no eavesdropper's CSI. This is because relay 2 can act as a helper [20] that enables to produce a jamming signal in cooperation with relay 1. We also note that when each of α_1 and α_2 is higher than or equal to 1, one secure d.o.f. is achievable for both the cases. For the case with full CSI, this is natural from the known results [23], [24] for the Gaussian multiple-input single-output (MISO) wiretap channel, where the source has two antennas and each of the legitimate destination and the eavesdropper has one antenna. In this Gaussian MISO wiretap channel, one secure d.o.f. is achievable by beamforming the message signal in the null space of the eavesdropper's channel. Similarly, if the source can send the message with d.o.f. 1 to both the relays for our diamond-wiretap channel, the relays are able to beam-form the message signals in the null space of the eavesdropper's channel. However, with no eavesdropper's CSI, this is not immediate from the known results for the Gaussian MISO

---

[2] $[i : j]$ for two integers i and j denotes the set $\{i, i+1, \cdots, j\}$ and $\text{Unif}[S]$ for a set S denotes the uniform distribution over S. When $S = [i : j]$, we use $\text{Unif}[i : j]$ instead of $\text{Unif}[[i : j]]$.

[3]Note that there is no secrecy constraint at the relays.

wiretap channel. The secure d.o.f. of the Gaussian MISO wiretap channel is still 1 with no eavesdropper's CSI [25], but it is achieved by sending an artificial noise signal in the null space of the legitimate destination in addition to the message signal. To translate this scheme to our diamond-wiretap channel, the source needs to send to the relays common artificial noise as well as (partial) messages, which requires $\alpha_1 \geq 1$, $\alpha_2 \geq 1$, and $\alpha_1 + \alpha_2 \geq 3$. To achieve $(\alpha_1, \alpha_2, d_s) = (1, 1, 1)$, we propose a novel scheme that incorporates *computation* of the message and artificial noise symbols at the source. This scheme involves transmitting a judicious function of the message and noise symbols from the source such that we only require $(\alpha_1, \alpha_2) = (1, 1)$, yet accomplish noise-beamforming as discussed above.

For the special case of symmetric link capacities, i.e., $\alpha_1 = \alpha_2 = \alpha$, the secure d.o.f.'s are given as

$$\min\left\{2\alpha, \frac{\alpha+1}{2}, 1\right\}, \min\left\{2\alpha, \frac{2\alpha+1}{3}, 1\right\}$$

for the case with full CSI and for the case with no eavesdropper's CSI, respectively. Note that the secure d.o.f. is 2α up to $\alpha = \frac{1}{3}$ and $\alpha = \frac{1}{4}$ for the case with full CSI and for the case with no eavesdropper's CSI, respectively. In this range, the broadcast part is the bottleneck and hence it is optimal to send independent partial messages to the relays and to incorporate the cooperative jamming [18] and the blind cooperative jamming [20] for the case with full CSI and for the case with no eavesdropper's CSI, respectively. After this threshold value of α, the source needs to send some common information (same message or common artificial noise) to achieve a higher secure d.o.f. and this causes the reduction of the gain in secure d.o.f. with respect to α. In Section VI, we investigate the effect of the absence of the eavesdropper's CSI on the secure d.o.f. for a generalized model with multiple relays.

Remark 1. *For the scenario where the channel fading coefficients are fixed during the whole communication, the lower and upper bounds on the secure d.o.f. for the case with full CSI in Theorem 1 and the lower bound on the secure d.o.f. for the case with no eavesdropper's CSI in Theorem 2 continue to hold for almost all channel gains. For an upper bound with no eavesdropper's CSI, a key result from [34] used for the upper bound in Theorem 2, i.e., the entropy of the channel output at the eavesdropper is at least as large as that at the legitimate destination, does not seem to be immediately generalized to the scenario with fixed channel gains.*

Remark 2. *We note that our achievability results can be generalized for complex channel fading coefficients by applying [35, Lemma 7] in our analysis of interference alignment. Also, our converse result for the case with full CSI can be generalized for complex channel fading coefficients in a straightforward manner.*

IV. CONVERSE

For the Gaussian multiple access-wiretap channel, it is shown in [20, Section 4.2.1] that there is no loss of secure d.o.f. if we consider the following deterministic model with

integer-input and integer-output, instead of the model (1)-(2) in Section II:

$$Y_1(t) = \sum_{k=1}^{2} \lfloor h_k(t)X_k(t)\rfloor, \ Y_2(t) = \sum_{k=1}^{2} \lfloor g_k(t)X_k(t)\rfloor \quad (6)$$

with the constraint

$$X_k \in \{0, 1, \ldots, \lfloor\sqrt{P}\rfloor\}, k = 1, 2 \quad (7)$$

where $\lfloor\cdot\rfloor$ denotes the floor function.

Likewise, it can be shown that there is no loss of secure d.o.f. in considering the deterministic model (6) and (7) for the multiple access part in our Gaussian diamond-wiretap channel.[4] Hence, in this section, let us assume that the multiple access part is given as (6) and (7). In this section, c_i's for $i = 1, 2, 3, \ldots$ are used to denote positive constants that do not depend on n and P. We note that $\mathbf{h}^n, \mathbf{g}^n$ are known to the legitimate destination and the eavesdropper for the case with full CSI. For the case with no eavesdropper's CSI, we assume $\mathbf{g}^n$ in addition to $\mathbf{h}^n$ is available at the legitimate destination, which only possibly increases the secure d.o.f. Hence, $\mathbf{h}^n, \mathbf{g}^n$ are conditioned in every entropy and mutual information terms in this section, but are omitted for notational convenience.

A. Proof for the converse part of Theorem 1

From the cut-set bound, we can easily obtain

$$d_s \leq \min\{\alpha_1 + \alpha_2, 1\}. \quad (8)$$

Hence, it remains to show $d_s \leq \frac{\alpha_2+1}{2}$. By applying similar steps used for the secrecy penalty lemma [18, Lemma 1], we have

$$nR \overset{(a)}{\leq} I(W; Y_1^n) + nc_2$$
$$\overset{(b)}{\leq} I(W; Y_1^n) - I(W; Y_2^n) + nc_3$$
$$\leq I(W; Y_1^n, Y_2^n) - I(W; Y_2^n) + nc_3$$
$$= I(W; Y_1^n | Y_2^n) + nc_3$$
$$\leq H(Y_1^n | Y_2^n) + nc_3$$
$$= H(Y_1^n, Y_2^n) - H(Y_2^n) + nc_3$$
$$\leq H(X_1^n, X_2^n, Y_1^n, Y_2^n) - H(Y_2^n) + nc_3$$
$$\leq H(X_1^n, X_2^n) + H(Y_1^n, Y_2^n | X_1^n, X_2^n) - H(Y_2^n) + nc_3$$
$$\overset{(c)}{=} H(X_1^n, X_2^n) - H(Y_2^n) + nc_3, \quad (9)$$

where (a) is from the Fano's inequality, (b) is from the secrecy constraint, and (c) is because a deterministic model in (6) is assumed in this section. To bound $H(Y_2^n)$ in (9), it follows that

$$H(Y_2^n)$$
$$= H\left(\left\{\sum_{i=1}^{2}\lfloor g_i(t)X_i(t)\rfloor\right\}_{t=1}^{n}\right)$$
$$\geq H\left(\left\{\sum_{i=1}^{2}\lfloor g_i(t)X_i(t)\rfloor\right\}_{t=1}^{n}\Big| X_2^n\right)$$

---

[4]We omit a formal proof as it is identical to that in [20, Section 4.2.1].

$$= H\big(\big\{\lfloor g_1(t)X_1(t)\rfloor\big\}_{t=1}^n\big|X_2^n\big)$$
$$= H\big(X_1^n, \big\{\lfloor g_1(t)X_1(t)\rfloor\big\}_{t=1}^n\big|X_2^n\big)$$
$$\quad - H\big(X_1^n\big|\big\{\lfloor g_1(t)X_1(t)\rfloor\big\}_{t=1}^n, X_2^n\big)$$
$$= H(X_1^n|X_2^n) - H\big(X_1^n\big|\big\{\lfloor g_1(t)X_1(t)\rfloor\big\}_{t=1}^n, X_2^n\big)$$
$$\geq H(X_1^n|X_2^n) - \sum_{t=1}^n H(X_1(t)|\lfloor g_1(t)X_1(t)\rfloor)$$
$$\overset{(a)}{\geq} H(X_1^n|X_2^n) - nc_4, \tag{10}$$

where (a) is from [20, Lemma 2].[5]

Now continuing (9) with (10) substituted, we have

$$nR \leq H(X_2^n) + nc_5$$
$$\leq H(X_2^n, J_2) + nc_5$$
$$= H(J_2) + H(X_2^n|J_2) + nc_5. \tag{11}$$

Note that the term $H(X_2^n|J_2)$ signifies the amount of independent randomness injected at relay 2 to confuse the eavesdropper. Such randomness cannot be too large because of the reliability constraint at the receiver. To capture the trade-off between the rate R and $H(X_2^n|J_2)$, we apply similar steps to the role of a helper lemma [18, Lemma 2]. We start from the Fano's inequality to get

$$nR \leq I(W; Y_1^n) + nc_2$$
$$\leq I(J_1, J_2; Y_1^n) + nc_2$$
$$= H(Y_1^n) - H(Y_1^n|J_1, J_2) + nc_2. \tag{12}$$

For the term $H(Y_1^n|J_1, J_2)$, we have

$$H(Y_1^n|J_1, J_2)$$
$$= H\big(\big\{\sum_{i=1}^2 \lfloor h_i(t)X_i(t)\rfloor\big\}_{t=1}^n\big|J_1, J_2\big)$$
$$\geq H\big(\big\{\sum_{i=1}^2 \lfloor h_i(t)X_i(t)\rfloor\big\}_{t=1}^n\big|J_1, J_2, X_1^n\big)$$
$$= H\big(\big\{\lfloor h_2(t)X_2(t)\rfloor\big\}_{t=1}^n\big|J_1, J_2, X_1^n\big)$$
$$= H\big(X_2^n, \big\{\lfloor h_2(t)X_2(t)\rfloor\big\}_{t=1}^n\big|J_1, J_2, X_1^n\big)$$
$$\quad - H\big(X_2^n\big|\big\{\lfloor h_2(t)X_2(t)\rfloor\big\}_{t=1}^n, J_1, J_2, X_1^n\big)$$
$$= H(X_2^n|J_1, J_2, X_1^n)$$
$$\quad - H\big(X_2^n\big|\big\{\lfloor h_2(t)X_2(t)\rfloor\big\}_{t=1}^n, J_1, J_2, X_1^n\big)$$
$$\geq H(X_2^n|J_1, J_2, X_1^n) - \sum_{t=1}^n H(X_2(t)|\lfloor h_2(t)X_2(t)\rfloor)$$
$$\overset{(a)}{\geq} H(X_2^n|J_1, J_2, X_1^n) - nc_6$$
$$\overset{(b)}{=} H(X_2^n|J_2) - nc_6, \tag{13}$$

where (a) is from Lemma 2 in [20] and (b) is due to the Markov chain $X_2^n - J_2 - (X_1^n, J_1)$. Therefore, by substituting (13) in (12), we obtain

$$nR \leq H(Y_1^n) - H(X_2^n|J_2) + nc_7. \tag{14}$$

[5]We note that the constraint in [20, Lemma 2] is satisfied under our channel model.

Combining (11) and (14), we have

$$2nR \leq H(J_2) + H(Y_1^n) + nc_8.$$

Hence, we have

$$R \leq \frac{1}{2}\left(\frac{1}{2}\log P + C_2\right) + c_9,$$

and, in turn,

$$d_s \leq \frac{1}{2}(1 + \alpha_2).$$

Combining with (8), we finish the proof for the converse part of Theorem 1. ∎

B. Proof for the converse part of Theorem 2

Note that (9) continue to hold for the case with no eavesdropper's CSI. Continuing with (9), it follows that

$$nR \leq H(X_1^n, X_2^n) - H(Y_2^n) + nc_{10}$$
$$\leq H(X_1^n, X_2^n, J_1, J_2) - H(Y_2^n) + nc_{10}$$
$$= H(J_1, J_2) + H(X_1^n, X_2^n|J_1, J_2) - H(Y_2^n) + nc_{10}$$
$$\leq H(J_1) + H(J_2) + H(X_1^n|J_1)$$
$$\quad + H(X_2^n|J_2) - H(Y_2^n) + nc_{10}. \tag{15}$$

By applying similar steps as those to derive (14), we can obtain

$$nR \leq H(Y_1^n) - H(X_k^n|J_k) + nc_{11}, \ k = 1, 2. \tag{16}$$

Continuing with (15) substituted by (16) for $k = 1, 2$, we have

$$3nR \leq H(J_1) + H(J_2) + 2H(Y_1^n) - H(Y_2^n) + nc_{12}$$

For the case with no eavesdropper's CSI, it is shown in [34, Section 5] that the difference $H(Y_1^n) - H(Y_2^n)$ can not be larger than $n \cdot o(\log P)$.[6] Therefore, we have

$$3nR \leq H(J_1) + H(J_2) + H(Y_1^n) + nc_{12} + n \cdot o(\log P)$$

which derives that

$$d_s \leq \frac{\alpha_1 + \alpha_2 + 1}{3}.$$

Since the bound on d_s for the case with full CSI continues to hold for the case with no eavesdropper's CSI, we finish the proof for the converse part of Theorem 2. ∎

V. ACHIEVABILITY

The direct parts of Theorems 1 and 2 are proved by first identifying a few key constituent schemes and then time-sharing among them appropriately. Let us first provide a high-level description of those schemes and then give a detailed one. First, the following three schemes require the eavesdropper's CSI at the relays and the legitimate destination and their operations are illustrated in Fig. 2.

- [Scheme 1 achieving $(\alpha_1, \alpha_2, d_s) = (\frac{1}{3}, \frac{1}{3}, \frac{2}{3})$. Incorporation of cooperative jamming [18]]:
  The message with d.o.f. $\frac{2}{3}$ is split into two independent partial messages each with d.o.f. $\frac{1}{3}$. The source sends a

[6]The channel assumption in [34] is satisfied under our channel model.

partial message to each relay in a way that each relay has a different partial message, which requires $\alpha_1 = \alpha_2 = \frac{1}{3}$. Then, the relays operate according to the cooperative jamming scheme [18] for the Gaussian multiple access-wiretap channel, which is briefly explained in the following. Each relay sends independent partial message (d.o.f. $\frac{1}{3}$) together with its own noise (d.o.f. $\frac{1}{3}$) in a way that the noise signals are aligned at the legitimate destination and a partial message signal sent from a relay is aligned with and is perfectly masked by the noise signal sent from the other relay at the eavesdropper.

- [Scheme 2 achieving $(\alpha_1, \alpha_2, d_s) = (1, 1, 1)$. Incorporation of message-beamforming [23], [24]]:
  The source sends the message with d.o.f. 1 to both the relays, which requires $\alpha_1 = \alpha_2 = 1$. Both the relays send the message cooperatively in a way that the message signals are beam-formed in the null space of the eavesdropper's channel.

- [Scheme 3 achieving $(\alpha_1, \alpha_2, d_s) = (1, 1, 1)$. Simultaneous alignment and beamforming (S-AB)]:
  The message with d.o.f. 1 is split into two independent partial messages each with d.o.f. $\frac{1}{2}$. The source sends a partial message together with a common noise with d.o.f. $\frac{1}{2}$ to each relay, which requires $\alpha_1 = \alpha_2 = 1$. Then, each relay sends independent partial message (d.o.f. $\frac{1}{2}$) and common noise (d.o.f. $\frac{1}{2}$) in a way that the common noise signals are beam-formed in the null space of the legitimate destination's channel and the partial message signals are aligned with and are perfectly masked by the common noise signal at the eavesdropper. Although this scheme achieves the same d.o.f. tuple as for Scheme 2, it outperforms Scheme 2 for more than two relays as remarked in Section VI.

Next, the following two schemes operate with no eavesdropper's CSI at the relays and the legitimate destination, which are illustrated in Fig. 3.

- [Scheme 4 achieving $(\alpha_1, \alpha_2, d_s) = (\frac{1}{2}, 0, \frac{1}{2})$. Incorporation of blind cooperative jamming [20]]:
  The source sends the message with d.o.f. $\frac{1}{2}$ only to relay 1, which requires $\alpha_1 = \frac{1}{2}$. Then, the relays operate according to the blind cooperative jamming scheme [20] for the wiretap channel with helpers. Relay 1 sends the message (d.o.f. $\frac{1}{2}$) together with its own noise (d.o.f. $\frac{1}{2}$) and relay 2 sends its own noise (d.o.f. $\frac{1}{2}$) in a way that the noise signals are aligned at the legitimate destination. Since the noise signals occupy the entire space at the eavesdropper, the messages can be shown to be secure.

- [Scheme 5 achieving $(\alpha_1, \alpha_2, d_s) = (1, 1, 1)$. Computation for jamming (CoJ)]:
  The source adds a noise sequence with d.o.f. 1 to the message codeword with d.o.f. 1 and sends the resultant sequence, which also has d.o.f. 1, to relay 1. To relay 2, the source sends the noise sequence used for the addition. This requires $\alpha_1 = \alpha_2 = 1$. Then, relays 1 and 2 send what they have received in a way that the common noise signals are canceled out at the legitimate destination. Because the common noise signals occupy
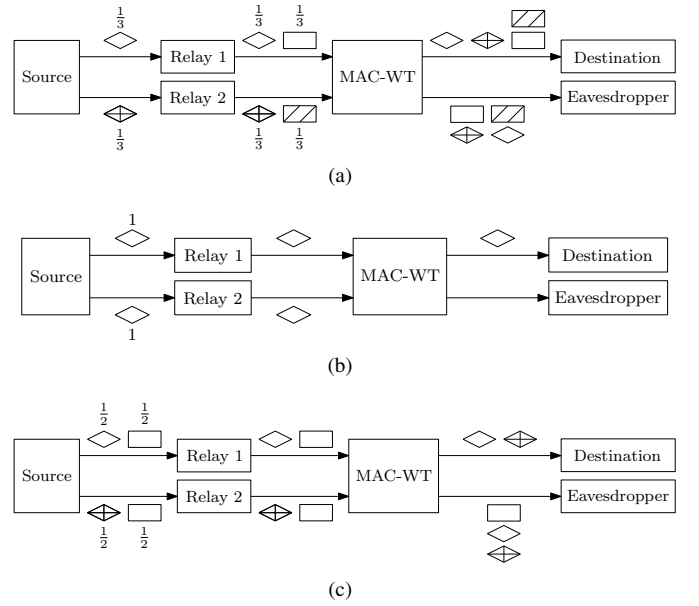

Figure 2. Schemes for the case with full CSI: (a) Incorporation of cooperative jamming, (b) Incorporation of message-beamforming, and (c) Simultaneous alignment and beamforming. Diamond shapes and rectangular shapes illustrate (partial) messages and noises, respectively, and the number above or below each shape represents its corresponding d.o.f. Same shapes with same patterns mean the same information. Otherwise, different shapes and/or different patterns represent independent informations.
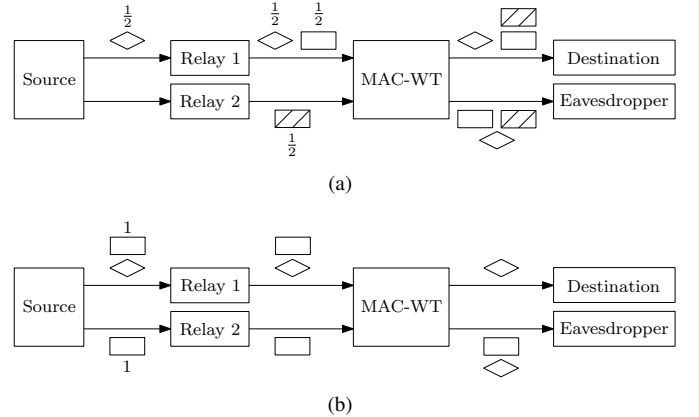

Figure 3. Schemes for the case with no eavesdropper's CSI: (a) Incorporation of blind cooperative jamming and (b) Computation for jamming. Similarly as in Fig. 2, diamond shapes and rectangular shapes represent (partial) messages and noises, respectively, with the number above or below each shape corresponding to its d.o.f. Same shapes with same patterns represent the same information, and otherwise independent informations.

the entire space at the eavesdropper, the message can be shown to be secure.

To show the achievability part of Theorem 1, we perform time-sharing among Scheme 1, Scheme 4, and any of Schemes 2, 3, and 5. For the achievability part of Theorem 2, we time-share between Schemes 4 and 5. Because Schemes 1, 2, and 4 are straightforward extensions of the previously proposed schemes in [18], [20], [23], [24], we give a detailed description only for Schemes 3 and 5. To that end, we first present some achievability results for the Gaussian multiple access-wiretap channel, which corresponds to the multiple access part of our model where each relay acts as a source having its

own message. In particular, to take into account the possible transmission of common noise from the source to the relays in our model, we assume that a common noise sequence is available at the sources of the Gaussian multiple-access wiretap channel. In such a Gaussian multiple access-wiretap channel, source $k = 1, 2$ wishes to send message W_k of rate R_k to the legitimate destination while keeping it secret from the eavesdropper. A secrecy rate tuple (R_1, R_2) is said to be achievable if there exists a sequence of codes with block length n such that $\lim_{n\to\infty} P(\hat{W}_1 \neq W_1 \text{ or } \hat{W}_2 \neq W_2) = 0$ and $\lim_{n\to\infty} \frac{1}{n} I(W_1, W_2; Y_2^n | \mathbf{h}^n, \mathbf{g}^n) = 0$. The following two theorems give achievable secrecy rate regions for the Gaussian multiple access-wiretap channel for the case with full CSI at the sources and the legitimate destination and for the case with no eavesdropper's CSI at the sources and the legitimate destination, respectively. Since these theorems are direct consequences of the achievablility result in [10], their proofs are omitted in this paper.

Theorem 3. *For the Gaussian multiple access-wiretap channel with full CSI at the sources and the legitimate destination and with common i.i.d. noise $U \sim p(u)$ available at the sources, a secrecy rate tuple (R_1, R_2) is achievable if*

$$\sum_{k \in S} R_k \leq I(V_S; Y_1 | V_{S^c}, \mathbf{h}, \mathbf{g}) - I(V_S; Y_2 | \mathbf{h}, \mathbf{g})$$

for all $S \subseteq [1 : 2]$ for some $\prod_{k \in [1:2]} p(v_k) p(x_k | u, v_k, \mathbf{h}, \mathbf{g})$ such that $\mathrm{E}[X_k^2] \leq P$ for $k = 1, 2$.[7]

Theorem 4. *For the Gaussian multiple access-wiretap channel with no eavesdropper's CSI at the sources and the legitimate destination and with common i.i.d. noise $U \sim p(u)$ available at the sources, a secrecy rate tuple (R_1, R_2) is achievable if*

$$\sum_{k \in S} R_k \leq I(V_S; Y_1 | V_{S^c}, \mathbf{h}) - I(V_S; Y_2 | \mathbf{h}, \mathbf{g})$$

for all $S \subseteq [1 : 2]$ for some $\prod_{k \in [1:2]} p(v_k) p(x_k | u, v_k, \mathbf{h})$ such that $\mathrm{E}[X_k^2] \leq P$ for $k = 1, 2$.

Remark 3. *Theorems 3 and 4 can be obtained from [10] by applying the technique of adding prefix channels introduced in [3]. We add prefix channel $p(u, x_k | v_k, \mathbf{h}, \mathbf{g}) = p(u) p(x_k | u, v_k, \mathbf{h}, \mathbf{g})$ for the case with full CSI and add prefix channel $p(u, x_k | v_k, \mathbf{h}) = p(u) p(x_k | u, v_k, \mathbf{h})$ for the case with no eavesdropper's CSI.*

Now, let us describe Schemes 3 and 5.

Scheme 3 achieving $(\alpha_1, \alpha_2, d_s) = (1, 1, 1)$. Simultaneous alignment and beamforming scheme: The message W of rate R is split into W_1 and W_2 each of which having rate $R/2$. Then, the source sends W_k to relay k together with a common noise sequence U^n generated in an i.i.d. manner according to $\mathrm{Unif}[C(a, Q)]$, where

$$C(a, Q) = a\{-Q, -Q + 1, \cdots, 0, \cdots, Q - 1, Q\}$$

for some positive real number a and positive integer Q which will be specified later. This transmission from the source to

[7]In Theorems 3 and 4, $\mathbf{h} = (h_1, h_2)$ and $\mathbf{g} = (g_1, g_2)$ denote the random channel fading coefficients generated by $f(h_1, h_2, g_1, g_2)$.

the relays imposes the following constraints:

$$\frac{R}{2} + \log(2Q + 1) \leq C_1 \tag{17}$$

$$\frac{R}{2} + \log(2Q + 1) \leq C_2. \tag{18}$$

Now, we apply Theorem 3 for the multiple access part with the following choices of R_1, R_2, and $p(v_1) p(v_2) p(x_1 | u, v_1, \mathbf{h}, \mathbf{g}) p(x_2 | u, v_2, \mathbf{h}, \mathbf{g})$:

$$R_1 = R/2, \; R_2 = R/2$$

$$V_1 \sim \mathrm{Unif}[C(a, Q)], \; V_2 \sim \mathrm{Unif}[C(a, Q)]$$

$$X_1 = \left(h_2 - \frac{g_2}{g_1} h_1 \right) V_1 + h_2 U$$

$$X_2 = \left(\frac{g_1}{g_2} h_2 - h_1 \right) V_2 - h_1 U.$$

Then, the channel outputs at the legitimate destination and the eavesdropper are given as

$$Y_1 = \left(h_1 h_2 - \frac{g_2}{g_1} h_1^2 \right) V_1 + \left(\frac{g_1}{g_2} h_2^2 - h_1 h_2 \right) V_2 + N_1$$

$$Y_2 = (g_1 h_2 - g_2 h_1)(V_1 + V_2 + U) + N_2,$$

respectively. According to Theorem 3, the secrecy rate of R is achievable if

$$R \leq I(V_1, V_2; Y_1 | \mathbf{h}, \mathbf{g}) - I(V_1, V_2; Y_2 | \mathbf{h}, \mathbf{g}) \tag{19}$$

$$\frac{R}{2} \leq I(V_1; Y_1 | V_2, \mathbf{h}, \mathbf{g}) - I(V_1; Y_2 | \mathbf{h}, \mathbf{g}) \tag{20}$$

$$\frac{R}{2} \leq I(V_2; Y_1 | V_1, \mathbf{h}, \mathbf{g}) - I(V_2; Y_2 | \mathbf{h}, \mathbf{g}) \tag{21}$$

are satisfied.

Let us bound the first term in the RHS of (19). The constellation at the legitimate destination consists of $(2Q+1)^2$ points and the minimum distance $d_{\min}$ of which can be bounded using the Khintchine-Groshev theorem of Diophantine approximation [21] as follows: for any $\delta > 0$, there exists a constant k_δ such that

$$d_{\min} \geq \frac{a k_\delta}{Q^{1+\delta}} \tag{22}$$

for almost all channel fading coefficients except a set of Lebesque measure zero. Since the probability that a realization of channel fading coefficients does not satisfy (22) is negligible, for the sake of brevity, let us assume that channel fading coefficients satisfy (22) in the subsequent analysis.

Let $(\hat{V}_1, \hat{V}_2)$ denote the estimate of (V_1, V_2) which is chosen as the closest point to Y_1 in the constellation. Then, we have

$$P((\hat{V}_1, \hat{V}_2) \neq (V_1, V_2)) \leq \exp\left(-\frac{d_{\min}^2}{8} \right)$$

$$\leq \exp\left(-\frac{a^2 k_\delta^2}{8 Q^{2(1+\delta)}} \right).$$

By choosing $Q = P^{\frac{1-\delta}{2(2+\delta)}}$ and $a = \frac{\gamma P^{1/2}}{Q}$ for some $\gamma > 0$, we have

$$P((\hat{V}_1, \hat{V}_2) \neq (V_1, V_2)) \leq \exp\left(-\frac{\gamma^2 k_\delta^2 P^\delta}{8} \right).$$

To meet the power constraints, we choose γ as follows:

$$\gamma = \frac{1}{\sqrt{5}L^3}$$

$$\leq \min\left\{\frac{1}{\sqrt{(h_2 - \frac{g_2}{g_1}h_1)^2 + h_2^2}}, \frac{1}{\sqrt{(\frac{g_1}{g_2}h_2 - h_1)^2 + h_1^2}}\right\}.$$

According to the Fano's inequality, it follows that

$$\begin{aligned}
&H(V_1, V_2 | Y_1, \mathbf{h}, \mathbf{g}) \\
&\leq H(V_1, V_2 | \hat{V}_1, \hat{V}_2) \\
&\leq 1 + P((\hat{V}_1, \hat{V}_2) \neq (V_1, V_2)) \log(|(V_1, V_2)| - 1) \\
&\leq 1 + \exp\left(-\frac{k_\delta^2 P^\delta}{40 L^6}\right) \log(2Q+1)^2 \\
&= o(\log P).
\end{aligned}$$

Therefore, the first term in the RHS of (19) can be bounded as

$$\begin{aligned}
&I(V_1, V_2; Y_1 | \mathbf{h}, \mathbf{g}) \\
&= H(V_1, V_2 | \mathbf{h}, \mathbf{g}) - H(V_1, V_2 | Y_1, \mathbf{h}, \mathbf{g}) \\
&\geq \log(2Q+1)^2 - o(\log P) \\
&= \frac{1-\delta}{2+\delta} \log P - o(\log P). \quad (23)
\end{aligned}$$

For the second term in the RHS of (19), it follows that

$$\begin{aligned}
&I(V_1, V_2; Y_2 | \mathbf{h}, \mathbf{g}) \\
&\stackrel{(a)}{\leq} I(V_1, V_2; (g_1 h_2 - g_2 h_1)(V_1 + V_2 + U) | \mathbf{h}, \mathbf{g}) \\
&\stackrel{(b)}{=} I(V_1, V_2; V_1 + V_2 + U) \\
&= H(V_1 + V_2 + U) - H(U) \\
&\leq \log(6Q+1) - \log(2Q+1) \\
&= \log\left(\frac{6Q+1}{2Q+1}\right) \\
&= o(\log P), \quad (24)
\end{aligned}$$

where (a) is due to the Markov chain $(V_1, V_2) - ((g_1 h_2 - g_2 h_1)(V_1 + V_2 + U), \mathbf{h}, \mathbf{g}) - Y_2$ and (b) is because $P(g_1 h_2 - g_2 h_1 = 0) = 0$ for our channel model.

Next, for the first term in the RHS of (20), we have

$$\begin{aligned}
&I(V_1; Y_1 | V_2, \mathbf{h}, \mathbf{g}) \\
&= I(V_1; Y_1' | \mathbf{h}, \mathbf{g}) \\
&= H(V_1) - H(V_1 | Y_1', \mathbf{h}, \mathbf{g}) \\
&\stackrel{(a)}{=} H(V_1) - h(N_1 | Y_1', \mathbf{h}, \mathbf{g}) \\
&\geq H(V_1) - h(N_1) \\
&= \log(2Q+1) - \frac{1}{2}\log 2\pi e \\
&\geq \frac{1-\delta}{2(2+\delta)} \log P - o(\log P) \quad (25)
\end{aligned}$$

for $Y_1' \triangleq h_{\text{eff}} V_1 + N_1$ and $h_{\text{eff}} \triangleq h_1 h_2 - \frac{g_2}{g_1} h_1^2$, where (a) is because $P(h_{\text{eff}} = 0) = 0$ for our channel model and for given $Y_1', \mathbf{h}, \mathbf{g}$ with $h_{\text{eff}} \neq 0$, V and N_1 have a one-to-one relationship. For the second term in the RHS of (20), we have

$$I(V_1; Y_2 | \mathbf{h}, \mathbf{g}) \leq I(V_1, V_2; Y_2 | \mathbf{h}, \mathbf{g})$$

$$\stackrel{(a)}{\leq} o(\log P), \quad (26)$$

where (a) is from (24).

Similarly, for the terms in the RHS of (21), we can show

$$I(V_2; Y_1 | V_1, \mathbf{h}, \mathbf{g}) \geq \frac{1-\delta}{2(2+\delta)} \log P - o(\log P) \quad (27)$$

$$I(V_2; Y_2 | \mathbf{h}, \mathbf{g}) \leq o(\log P). \quad (28)$$

By substituting (19)-(21) with (23)-(28) and then choosing δ sufficiently small, we have

$$R \leq \frac{1}{2}\log P - o(\log P) \quad (29)$$

for the multiple access part. From (17), (18), and (29), we conclude that $(\alpha_1, \alpha_2, d_s) = (1, 1, 1)$ is achievable.

Scheme 5 achieving $(\alpha_1, \alpha_2, d_s) = (1, 1, 1)$. Computation for jamming scheme: In this scheme, we wish to apply Theorem 4 for the multiple access part with the following choices of R_1, R_2, and $p(v_1)p(v_2)p(x_1|u, v_1, \mathbf{h})p(x_2|u, v_2, \mathbf{h})$:

$$R_1 = R, \ R_2 = 0$$
$$V_1 \sim \text{Unif}[C(a, Q)], \ V_2 = \emptyset$$
$$X_1 = \frac{1}{h_1}(V_1 + U), \ X_2 = -\frac{1}{h_2}U,$$

where $U \sim \text{Unif}[C(a, Q)]$, $C(a, Q) = a\{-Q, -Q+1, \cdots, 0, \cdots, Q-1, Q\}$, $Q = P^{\frac{1-\delta}{2}}$, and $a = \frac{1}{\sqrt{2}L}P^{\frac{\delta}{2}}$ for $\delta > 0$. Note that the power constraints at the relays are satisfied since $\frac{1}{\sqrt{2}L} \leq \min\left\{\frac{|h_1|}{\sqrt{2}}, |h_2|\right\}$.

To that end, one naive approach is to let the source send the message W to relay 1 and send a common noise sequence U^n to both relays 1 and 2, which requires

$$R + \log(2Q+1) \leq C_1$$
$$\log(2Q+1) \leq C_2.$$

However, there is a cleverer way to enable the aforementioned relay operations, in which the source *computes* $V_1^n(W) + U^n$ and sends the sum to relay 1. To relay 2, the source sends U^n. This transmission from the source to the relays is possible if the following constraints are satisfied:

$$\log(4Q+1) \leq C_1 \quad (30)$$
$$\log(2Q+1) \leq C_2. \quad (31)$$

Now, the channel outputs at the legitimate destination and the eavesdropper are given as

$$Y_1 = V_1 + N_1$$
$$Y_2 = \frac{g_1}{h_1}V_1 + \left(\frac{g_1}{h_1} - \frac{g_2}{h_2}\right)U + N_2,$$

respectively. According to Theorem 4, the following secrecy rate can be achieved.

$$R \leq I(V_1; Y_1 | \mathbf{h}) - I(V_1; Y_2 | \mathbf{h}, \mathbf{g}). \quad (32)$$

Let us bound the first term in the RHS of (32). We have

$$\begin{aligned}
I(V_1; Y_1 | \mathbf{h}) &= I(V_1; V_1 + N_1) \\
&= H(V_1) - H(V_1 | V_1 + N_1) \\
&= H(V_1) - h(N_1 | V_1 + N_1)
\end{aligned}$$

$$\geq H(V_1) - h(N_1)$$
$$= \log(2Q+1) - \frac{1}{2}\log(2\pi e)$$
$$\geq \frac{1-\delta}{2}\log P - o(\log P). \tag{33}$$

For the second term in the RHS of (32), it follows that

$$I(V_1; Y_2|\mathbf{h}, \mathbf{g})$$
$$= I(V_1, U; Y_2|\mathbf{h}, \mathbf{g}) - I(U; Y_2|V_1, \mathbf{h}, \mathbf{g})$$
$$\overset{(a)}{\leq} I(V_1, U; Y_2|\mathbf{h}, \mathbf{g}) - \frac{1-\delta}{2}\log P + o(\log P)$$
$$= h(Y_2|\mathbf{h}, \mathbf{g}) - h(Y_2|V_1, U, \mathbf{h}, \mathbf{g}) - \frac{1-\delta}{2}\log P + o(\log P)$$
$$= h(Y_2|\mathbf{h}, \mathbf{g}) - h(N_2) - \frac{1-\delta}{2}\log P + o(\log P)$$
$$\overset{(b)}{\leq} \frac{1}{2}\log P - \frac{1}{2}\log 2\pi e - \frac{1-\delta}{2}\log P + o(\log P)$$
$$= \frac{\delta}{2}\log P + o(\log P), \tag{34}$$

where (a) is by applying similar steps as those used for obtaining (25) and (b) is because all channel fading coefficients are assumed to be bounded away from zero and infinity.

By substituting (32) with (33) and (34) and by choosing δ sufficiently small, we have

$$R \leq \frac{1}{2}\log P + o(\log P) \tag{35}$$

for the multiple access part. From (30), (31), and (35), we conclude that $(\alpha_1, \alpha_2, d_s) = (1, 1, 1)$ is achievable.

Now, we are ready to prove the achievability parts of Theorems 1 and 2.

A. Proof for the achievability part of Theorem 1

Note that $\alpha_1 \geq \alpha_2$ without loss of generality in our model. First, consider the case where the minimum of (4) is equal to $\alpha_1 + \alpha_2$, which implies $2\alpha_1 + \alpha_2 \leq 1$. We use time-sharing technique as follows: use Scheme 1 for $3\alpha_2$ fraction of time, use Scheme 4 for $2(\alpha_1 - \alpha_2)$ fraction of time, and keep silent for the remaining fraction.[8] Then, it can be easily shown $d_s = \alpha_1 + \alpha_2$ is achievable. Next, consider the case where the minimum of (4) is given as $\frac{1}{2}(1+\alpha_2)$. If $\alpha_2 \leq \frac{1}{3}$, by using Scheme 1 for $3\alpha_2$ fraction of time and using Scheme 4 for $1 - 3\alpha_2$ fraction of time, $\frac{1}{2}(1 + \alpha_2)$ is achievable. If $\frac{1}{3} < \alpha_2 \leq 1$, by using Scheme 1 for $\frac{3}{2}(1 - \alpha_2)$ fraction of time and using any of Schemes 2, 3, and 5 for the remaining fraction of time, $\frac{1}{2}(1+\alpha_2)$ is achievable. Finally, consider the case where the minimum of (4) is 1, which implies $\alpha_1 \geq 1$ and $\alpha_2 \geq 1$. By using any of Schemes 2, 3, and 5, $d_s = 1$ is trivially achievable. ∎

B. Proof for the achievability part of Theorem 2

We note that a variant of Scheme 4 where the roles of relays 1 and 2 are swapped can achieve $(\alpha_1, \alpha_2, d_s) = (0, \frac{1}{2}, \frac{1}{2})$, and let us call this scheme as Scheme 4*. First, consider the case where the minimum of (5) is equal to $\alpha_1 + \alpha_2$, which implies

[8]Note that $3\alpha_2 + 2(\alpha_1 - \alpha_2) = 2\alpha_1 + \alpha_2 \leq 1$.

$2\alpha_1 + 2\alpha_2 \leq 1$. By using Scheme 4 for $2\alpha_1$ fraction of time and Scheme 4* for $2\alpha_2$ fraction of time and keeping silent for the remaining fraction, $d_s = \alpha_1 + \alpha_2$ can be shown to be achievable. Next, consider the case where the minimum of (5) is given as $\frac{1}{3}(1 + \alpha_1 + \alpha_2)$. By using Scheme 4 for $\frac{2(\alpha_1 - 2\alpha_2 + 1)}{3}$ fraction, Scheme 4* for $\frac{2(\alpha_2 - 2\alpha_1 + 1)}{3}$ fraction, and Scheme 5 for the remaining fraction of time, it can be shown that $d_s = \frac{1}{3}(1 + \alpha_1 + \alpha_2)$ is achievable. Now, consider the case where the minimum of (5) is given as $\frac{1}{2}(1 + \alpha_2)$. We use Scheme 4 for $(1 - \alpha_2)$ fraction of time and use Scheme 5 for α_2 fraction of time, which achieves $d_s = \frac{1}{2}(1 + \alpha_2)$. Finally, consider the case where the minimum of (5) is 1, which implies $\alpha_1 \geq 1$ and $\alpha_2 \geq 1$. By using Scheme 5, $d_s = 1$ is trivially achievable. ∎

VI. Generalization to M Relays

In this section, we consider a generalized Gaussian diamond-wiretap channel where there are arbitrary number of relays. Assume that there are $M \geq 2$ relays with transmit power constraint of P. For the broadcast part, the source is connected to M relays through orthogonal links, where the link capacity to relay $k = 1, \ldots, M$ is C_k such that $\lim_{P \to \infty} \frac{C_k}{\frac{1}{2}\log P} = \alpha_k$. For the multiple access part, the channel outputs $Y_1(t)$ and $Y_2(t)$ at time t at the legitimate destination and the eavesdropper, respectively, are given as

$$Y_1(t) = \sum_{k=1}^{M} h_k(t)X_k(t) + N_1(t) \tag{36}$$
$$Y_2(t) = \sum_{k=1}^{M} g_k(t)X_k(t) + N_2(t), \tag{37}$$

in which $X_k(t)$ is the channel input at relay k, $h_k(t)$'s and $g_k(t)$'s are channel fading coefficients to the legitimate destination and the eavesdropper, respectively, and $N_1(t)$ and $N_2(t)$ are independent Gaussian noise with zero mean and unit variance at the legitimate destination and the eavesdropper, respectively, at time t. Similarly as in Section II, we assume fast fading[9], no CSI at the source, and full CSI at the eavesdropper, and consider the two cases regarding the availability of CSI at the relays and the legitimate destination, i.e., the case with full CSI and the case with no eavesdropper's CSI. A secrecy code, secrecy capacity, and secure d.o.f. are defined by a straightforward generalization from Section II. For the brevity of the results, we focus on the symmetric case with $C_1 = \cdots = C_M = C$, which implies $\alpha_1 = \cdots = \alpha_M = \alpha$.

The following two theorems present our results on the secure d.o.f. for the case with full CSI and for the case with no eavesdropper's CSI, respectively.

Theorem 5. *For the generalized Gaussian diamond-wiretap channel with $M \geq 2$ relays with full CSI at the relays and the legitimate destination, the secure d.o.f. satisfies*

$$d_{s,-} \leq d_s \leq d_{s,+},$$

[9]Similarly as for the two-relay case in Section II, we assume that the channel fading coefficients are generated from a real-valued joint density function whose all joint and conditional density functions are bounded and whose support set does not contain zero and infinity.
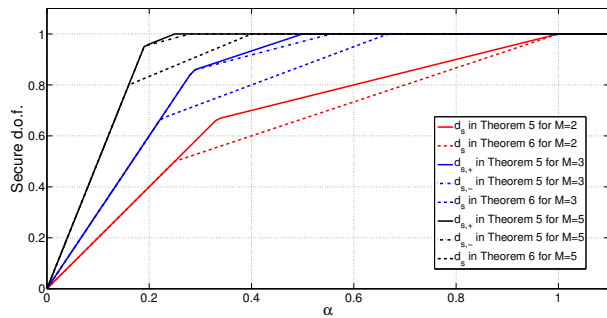
Figure 4. Secure d.o.f. of the generalized Gaussian diamond-wiretap channel with M relays

where

$$d_{s,+} = \min\left\{M\alpha, \frac{M-1}{M}(1+\alpha), 1\right\},$$

$$d_{s,-} = \min\left\{M\alpha, \frac{2M(M-1)+M^2\alpha}{2M^2-M+2}, 1\right\}.$$

Theorem 6. *For the generalized Gaussian diamond-wiretap channel with $M \geq 2$ relays with no eavesdropper's CSI at the relays and the legitimate destination, the secure d.o.f. is equal to*

$$d_s = \min\left\{M\alpha, \frac{M\alpha + M - 1}{M+1}, 1\right\}.$$

In Fig. 4, the results in Theorems 5 and 6 are illustrated for $M = 2, 3, 5$. For the case with full CSI with $M > 2$, there exists a gap between the lower and upper bounds on the secure d.o.f., which decreases as M increases. We note that up to the threshold value $\frac{M-1}{M(M-1)+1}$ (resp., $\frac{M-1}{M^2}$) of α for the case with full CSI (resp., for the case with no eavesdropper's CSI), the secure d.o.f. is linear in M and α. In this regime, the broadcast part becomes the bottleneck and hence it is optimal to send independent partial messages to the relays and to incorporate the cooperative jamming scheme [18] (resp., the blind cooperative jamming scheme [20]) for the multiple access part. After this threshold value of α, the source needs to send some common information to the relays to achieve a higher secure d.o.f. and hence the slope of secure d.o.f. in α becomes lower. If α is $\frac{1}{M} + \frac{2}{M^2}$ for the case with full CSI (resp., $\frac{2}{M}$ for the case with no eavesdropper's CSI), one secure d.o.f. can be achieved by generalizing the S-AB scheme (resp., the CoJ scheme) in Section V. We note that there is a gap between the secure d.o.f.'s with and without eavesdropper's CSI for $\alpha \in \left(\frac{M-1}{M^2}, \frac{2}{M}\right)$, and there is no loss in secure d.o.f. for other ranges of α.

Theorems 5 and 6 can be proved by generalizing the proof techniques in Sections IV and V. In the following, we provide brief proofs for these theorems.

A. Converse

Similarly as in Section IV, there is no loss of secure d.o.f. in considering the following deterministic model with integer-input and integer-output for the multiple access part, instead of the original channel (36) and (37):

$$Y_1(t) = \sum_{k=1}^{M} \lfloor h_k(t)X_k(t)\rfloor, \ \ Y_2(t) = \sum_{k=1}^{M} \lfloor g_k(t)X_k(t)\rfloor \quad (38)$$

with the constraint

$$X_k \in \{0, 1, \ldots, \lfloor\sqrt{P}\rfloor\}, k = 1, \ldots, M. \quad (39)$$

Hence, in this subsection, let us assume that the multiple access part is given as (38) and (39). In addition, the channel fading coefficients are conditioned in every entropy and mutual information terms in this subsection due to the same reason as in Section IV, but are omitted for notational convenience. c_i''s for $i = 1, 2, 3, \ldots$ are used to denote positive constants that do not depend on n and P.

1) Proof for the converse part of Theorem 5: We generalize the converse proof technique in Section IV-A for multiple relays. We can obtain the following inequality by applying similar techniques used to obtain (11):

$$nR \leq \sum_{k=2}^{M} H(J_k) + \sum_{k=2}^{M} H(X_k^n|J_k) + nc_1'. \quad (40)$$

On the other hand, we can generalize (14) for multiple relays as follows:

$$nR \leq H(Y_1^n) - H(X_k^n|J_k) + nc_2', \ \ k = 2, \cdots, M. \quad (41)$$

By combining (40) and (41), we have

$$MnR \leq \sum_{k=2}^{M} H(J_k) + (M-1)H(Y_1^n) + nc_3'$$
$$\leq (M-1)nC + (M-1)H(Y_1^n) + nc_3'.$$

It follows that

$$R \leq \frac{M-1}{M}\left(\frac{1}{2}\log P + C\right) + c_4'$$

or

$$d_s \leq \frac{M-1}{M}(1+\alpha).$$

Together with the following bound from the cutset bound, this completes the proof,

$$d_s \leq \min\{M\alpha, 1\}. \quad (42)$$

∎

2) Proof for the converse part of Theorem 6: We extend the converse proof technique in Section IV-B for multiple relays. First, we can generalize (15) for multiple relays as follows:

$$nR \leq \sum_{k=1}^{M} H(J_k) + \sum_{k=1}^{M} H(X_k^n|J_k) - H(Y_2^n) + nc_5'. \quad (43)$$

Next, the following inequality can be obtained by applying similar techniques used in deriving (16):

$$nR \leq H(Y_1^n) - H(X_k^n|J_k) + nc_6', \ \ k = 1, \ldots, M \quad (44)$$

Combining (43) and (44), we have

$$(M+1)nR$$

$$\leq \sum_{k=1}^{M} H(J_k) + MH(Y_1^n) - H(Y_2^n) + nc_7'$$

$$\leq MnC + (M-1)H(Y_1^n) + H(Y_1^n) - H(Y_2^n) + nc_7'$$

$$\overset{(a)}{\leq} MnC + (M-1)H(Y_1^n) + n \cdot o(\log P) + nc_7',$$

where (a) is because the difference $H(Y_1^n) - H(Y_2^n)$ can not be larger than $n \cdot o(\log P)$ for the case with no eavesdropper's CSI from [34, Section 6].[10] In terms of d.o.f., equivalently, we have

$$d_s \leq \frac{M\alpha + M - 1}{M + 1}.$$

Combining with the bound (42) from the cutset bound, we finish the proof. ∎

B. Achievability

1) Proof for the achievability part of Theorem 5: Note that it is sufficient to show that the following two corner points are achievable: $(\alpha, d_s) = \left(\frac{M-1}{M(M-1)+1}, \frac{M(M-1)}{M(M-1)+1} \right)$ and $(\alpha, d_s) = \left(\frac{1}{M} + \frac{2}{M^2}, 1 \right)$. For the first corner point, the message with d.o.f. $\frac{M(M-1)}{M(M-1)+1}$ is split into M independent partial messages each with d.o.f. $\frac{M-1}{M(M-1)+1}$. The source sends each partial message to each different relay, which requires $\alpha = \frac{M-1}{M(M-1)+1}$. Then, the relays operate according to the cooperative jamming scheme in [18] for the Gaussian multiple access-wiretap channel.

To show $(\alpha, d_s) = \left(\frac{1}{M} + \frac{2}{M^2}, 1 \right)$ is achievable, we propose $\frac{M(M-1)}{2}$ sub-schemes, where the (i,j)-th sub-scheme for $i \in [1 : M]$ and $j \in [1 : M]$ such that $j > i$ achieves $\alpha_i = \alpha_j = \frac{2}{M}$, $\alpha_k = \frac{1}{M}$ for $k \notin \{i,j\}$, and $d_s = 1$. By time-sharing among these sub-schemes uniformly, we can prove that $(\alpha, d_s) = \left(\frac{1}{M} + \frac{2}{M^2}, 1 \right)$ is achievable. Each sub-scheme is generalized from the S-AB scheme proposed in Section V. In Fig. 5-(b), the (1,2)-th subscheme is illustrated for $M = 4$. The message with d.o.f. 1 is split into M independent partial messages each with d.o.f. $\frac{1}{M}$. In the (i,j)-th sub-scheme, the source sends each partial message to each different relay and sends a common noise with d.o.f. $\frac{1}{M}$ to relays i and j in addition to the partial messages, which requires $\alpha_i = \alpha_j = \frac{2}{M}$ and $\alpha_k = \frac{1}{M}$ for $k \notin \{i,j\}$. Then, each relay transmits what it has received in a way that the common noise signals are beam-formed in the null space of the legitimate destination's channel and the partial message signals are aligned with and are perfectly masked by the common noise signal at the eavesdropper. ∎

2) Proof for the achievability part of Theorem 6: Note that it is sufficient to show that the following two corner points are achievable: $(\alpha, d_s) = \left(\frac{M-1}{M^2}, \frac{M-1}{M} \right)$ and $(\alpha, d_s) = \left(\frac{2}{M}, 1 \right)$. First, $(\alpha, d_s) = \left(\frac{M-1}{M^2}, \frac{M-1}{M} \right)$ can be shown to be achievable by uniformly time-sharing M sub-schemes, where the k-th sub-scheme for $k \in [1 : M]$ achieves $\alpha_k = \frac{M-1}{M}$, $\alpha_j = 0$ for $j \neq k$, and $d_s = \frac{M-1}{M}$. Each sub-scheme is a direct extension of the blind cooperative jamming scheme [20] for the wiretap channel with helpers, i.e., for the k-th sub-scheme, the source

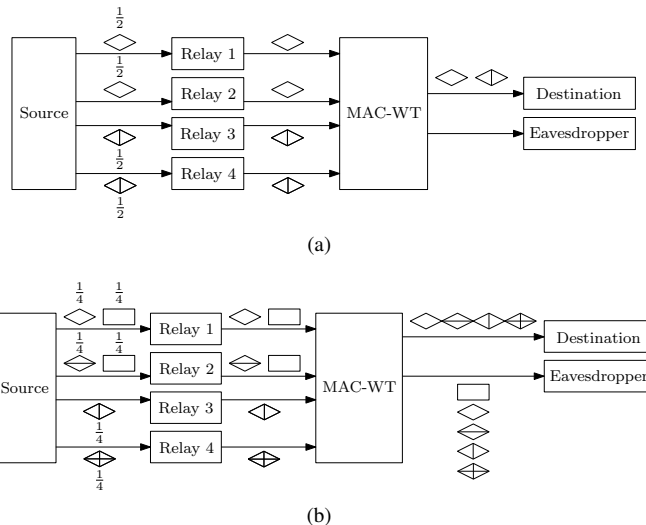[10]The channel assumption in [34] is satisfied under our channel model.

(a)

(b)

Figure 5. Comparison between (a) the message-beamforming scheme and (b) the S-AB scheme for $M = 4$. Similarly as in Fig. 2 and Fig. 3, diamond shapes and rectangular shapes represent (partial) messages and noises, respectively, with the number above or below each shape corresponding to its d.o.f. Same shapes with same patterns represent the same information, and otherwise independent informations.

sends the message with d.o.f. $\frac{M-1}{M}$ to relay k and the relays operate according to the blind cooperative jamming scheme [20] as if relay k is the source and the other relays are the helpers.

Next, $(\alpha, d_s) = \left(\frac{2}{M}, 1 \right)$ can be shown to be achievable by uniformly time-sharing $\frac{M(M-1)}{2}$ sub-schemes, where the (i,j)-th sub-scheme for $i \in [1 : M]$ and $j \in [1 : M]$ such that $j > i$ achieves $\alpha_i = \alpha_j = 1$, $\alpha_k = 0$ for $k \notin \{i,j\}$, and $d_s = 1$. Each sub-scheme is the same as the CoJ scheme proposed in Section V, i.e., in the (i,j)-th scheme, we use the CoJ scheme as if there are only two relays i and j. ∎

Remark 4. *We note that a generalization of the message-beamforming scheme in Section V for the case with M-relays achieves $(\alpha, d_s) = \left(\frac{2}{M}, 1 \right)$. Hence, the S-AB scheme outperforms the message-beamforming scheme for $M > 2$. To see the intuition behind this, we illustrate some instances of using these two schemes for $M = 4$ in Fig. 5, where both the schemes achieve one secure d.o.f. but the S-AB scheme uses less link d.o.f.'s at the broadcast part. For the message-beamforming scheme, every pair of two relays has to send a common partial message to beam-form each partial message. For the S-AB scheme, once two relays have common noise and independent partial messages as in the two-relay case, the other relays can send independent partial messages without common noise since the same common noise can be used to mask all the partial messages simultaneously. Hence, the S-AB scheme requires less 'common' information and thus is more efficient in the use of the broadcast links.*

VII. Conclusion

In this paper, we established the exact secure d.o.f. of the Gaussian diamond-wiretap channel and generalized the results for multiple relays. We considered both the case with full CSI

and the case with no eavesdropper's CSI, at the relays and the legitimate destination. Our results show that the absence of the eavesdropper's CSI reduces the secure d.o.f. for some range of moderate link d.o.f.'s of the broadcast part, but its effect decreases as the number of relays increases. For the converse part, we introduced a technique of capturing the trade-off between the message rate and the amount of independent randomness injected at each relay. For the achievability part, we newly proposed a simultaneous alignment and beamforming (S-AB) scheme and a computation for jamming (CoJ) scheme for the case with full CSI and for the case with no eavesdropper's CSI, respectively. Both the schemes incorporate transmitting common noise from the source to the relays and beamforming of common noise signals in the null space of the legitimate destination's channel. The S-AB scheme involves aligning the message and the common noise signals at the eavesdropper simultaneously with the beamforming of the common noise signals. By doing so, it utilizes common information more efficiently than the message-beamforming scheme for more than two relays. The CoJ scheme involves computation between the message and the common noise symbols at the source, which requires less link d.o.f.'s at the broadcast part than naively sending the message and the common noise separately.

We note that our proposed schemes utilize the common information sent from the source to the two relays. If the relays are allowed to conference, such common information can be shared at the relays by conferencing among them. In the recent work [36], the exact secure d.o.f. was established for such a conferencing scenario for the case with full CSI. For achievability, a modified S-AB scheme was proposed where the relays share the common noise via conferencing (instead of the transmission from the source) and hence less link d.o.f.'s are required. As a final remark, we note that our CoJ scheme can be useful in keeping the message secret from the relays. Exploiting such a feature can be an interesting further work for the scenario where the source has common and confidential messages to each of the relays and the legitimate destination.

REFERENCES

[1] S.-H. Lee, W. Zhao, and A. Khisti, "Secure degrees of freedom of the Gaussian diamond-wiretap channel," in *2016 IEEE International Symposium on Information Theory (ISIT)*, July 2016, pp. 2819–2823.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, 1975.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, pp. 339–348, May 1978.

[4] O. O. Koyluoglu, C. E. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, vol. 58, pp. 3000–3015, May 2012.

[5] M. Yuksel and E. Erkip, "The relay channel with a wiretapper," in *Annual Conference on Information Sciences and Systems*, Baltimore,MD, Mar. 2007.

[6] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, pp. 976–1002, Mar. 2008.

[7] M. Bloch and A. Thangaraj, "Confidential messages to a cooperative relay," in *IEEE Information Theory Workshop*, Porto, Portugal, May 2008.

[8] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4005–4019, Sep. 2008.

[9] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, pp. 5747–5755, Dec. 2008.

[10] ——, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2735–2751, June 2008.

[11] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180–2189, Jun. 2008.

[12] E. Perron, "Information-theoretic secrecy for wireless networks," Ph.D. dissertation, École Polytechnique Fédérale de Lausanne, 2009.

[13] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, pp. 3807–3827, Aug. 2010.

[14] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Inf. Theory*, vol. 57, pp. 137–155, Jan. 2011.

[15] M. H. Yassaee, M. R. Aref, and A. Gohari, "Achievability proof via output statistics of random binning," *IEEE Trans. Inf. Theory*, vol. 60, pp. 6760–6786, Nov. 2014.

[16] S. E. J. Richter, C. Scheunert and E. A. Jorswieck, "Weak secrecy in the multiway untrusted relay channel with compute-and-forward." *IEEE Trans. Inf. Forens. and Sec*, vol. 10, pp. 1262–1273, Jun. 2015.

[17] X. He and A. Yener, "Providing secrecy with structured codes: Two-user Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 60, pp. 2121–2138, Apr. 2014.

[18] J. Xie and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," *IEEE Trans. Inf. Theory*, vol. 60, pp. 3359–3378, Jun. 2014.

[19] ——, "Secure degrees of freedom of K-user Gaussian interference channel: A unified view," *IEEE Trans. Inf. Theory*, vol. 61, pp. 2647–2661, May 2015.

[20] P. Mukherjee, J. Xie, and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks with no eavesdropper CSIT," *IEEE Trans. Inf. Theory*, submitted for publication. [Online]. Available: http://arxiv.org/abs/1506.06114.

[21] A. S. Motahari, S. Oveis-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, pp. 4799–4810, Aug. 2014.

[22] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4687–4698, Oct. 2008.

[23] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, pp. 3088–3104, Jul. 2010.

[24] 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, pp. 4215–4227, Sep. 2010.

[25] P. Mukherjee, R. Tandon, and S. Ulukus, "Secrecy for MISO broadcast channels with heterogeneous CSIT," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, Hong Kong, 2015, pp. 1966 – 1970.

[26] B. E. Schein, "Distributed coordination in network information theory," Ph.D. dissertation, Massachusetts Institute of Technology, 2001.

[27] D. Traskov and G. Kramer, "Reliable communication in networks with multi-access interference," in *Proc. IEEE Information Theory Workshop (ITW)*, 2007, pp. 343–348.

[28] W. Kang and N. Liu, "The Gaussian multiple access diamond channel," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, Jul.-Aug. 2011, pp. 1499–1503.

[29] W. Kang, N. Liu, and W. Chong, "The Gaussian multiple access diamond channel," *IEEE Transactions on Information Theory*, vol. 61, no. 11, pp. 6049–6059, Nov 2015.

[30] S. Saeedi Bidokhti and G. Kramer, "Capacity bounds for diamond networks with an orthogonal broadcast channel," [Online]. Available: http://arxiv.org/abs/1510.00994.

[31] L. H. Ozarow, "On a source-coding problem with two channels and three receivers," *Bell Syst. Tech. J.*, vol. 59, pp. 1909–1921, 1980.

[32] T. Yang, N. Liu, W. Kang, and S. Shamai, "An upper bound on the sum capacity of the downlink multicell processing with finite backhaul capacity," [Online]. Available: http://arxiv.org/abs/1609.00833.

[33] S.-H. Lee and A. Khisti, "Degraded Gaussian diamond-wiretap channel," *IEEE Trans. Commun.*, vol. 63, pp. 5027–5038, Dec. 2015.

[34] A. G. Davoodi and S. A. Jafar, "Aligned image sets under channel uncertainty: Settling a conjecture by Lapidoth, Shamai and Wigger on the collapse of degrees of freedom under finite precision CSIT," 2014. [Online]. Available: http://arxiv.org/abs/1403.1541.

[35] M. A. Maddah-Ali, "On the degrees of freedom of the compound MIMO broadcast channels with finite states," 2014. [Online]. Available: http://arxiv.org/abs/0909.5006.

[36] S.-H. Lee and A. Khisti, "The Gaussian diamond-wiretap channel with conferencing relays," *IEEE Communications Letters*, vol. 20, no. 7, pp. 1393–1396, July 2016.

Si-Hyeon Lee (S'08-M'13) received the B.S. (summa cum laude) and Ph.D. degrees in electrical engineering from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea, in 2007 and 2013, respectively. She is now a Postdoctoral Fellow at the Department of Electrical and Computer Engineering, University of Toronto. Her research interests include network information theory, physical layer security, and wireless communication systems.

Wanyao Zhao (S'14-M'15) finished his M.A.Sc.degree at University of Toronto in 2015 and his B.Eng. degree at Beijing Institute of Technology in 2013. He is now working at Bank of China Limited. His research interest includes information theory, physical layer security and wireless communication.

Ashish Khisti (S'02-M'08) received his BASc Degree in Engineering Sciences (Electrical Option) from University of Toronto, and his S.M and Ph.D. Degrees in Electrical Engineering from the Massachusetts Institute of Technology. Between 2009-2015, he was an assistant professor in the Electrical and Computer Engineering department at the University of Toronto. He is presently an associate professor, and holds a Canada Research Chair in the same department. He is a recipient of an Ontario Early Researcher Award, the Hewlett-Packard Innovation Research Award and the Harold H. Hazen teaching assistant award from MIT. He presently serves as an associate editor for IEEE Transactions on Information Theory and is also a guest editor for the Proceedings of the IEEE (Special Issue on Secure Communications via Physical-Layer and Information-Theoretic Techniques).