Security in The Gaussian Interference Channel: Weak and Moderately Weak Interference Regimes

Parisa Babaheidarian*, Somayeh Salimi**, Panos Papadimitratos**
*Boston University,**KTH Royal Institute of Technology

***Abstract*—We consider a secure communication scenario through the two-user Gaussian interference channel: each transmitter (user) has a confidential message to send reliably to its intended receiver while keeping it secret from the other receiver. Prior work investigated the performance of two different approaches for this scenario; i.i.d. Gaussian random codes and real alignment of structured codes. While the latter achieves the optimal sum secure degrees of freedom (s.d.o.f.), its extension to finite SNR regimes is challenging. In this paper, we propose a new achievability scheme for the weak and the moderately weak interference regimes, in which the reliability as well as the confidentiality of the transmitted messages are maintained at any finite SNR value. Our scheme uses lattice structure, structured jamming codewords, and lattice alignment in the encoding and the asymmetric compute-and-forward strategy in the decoding. We show that our lower bound on the sum secure rates scales linearly with $\log(SNR)$ and hence, it outperforms i.i.d. Gaussian random codes. Furthermore, we show that our achievable result is asymptotically optimal. Finally, we provide a discussion on an extension of our scheme to $K > 2$ users.**

I. Introduction

It has been shown that structured codes along with alignment techniques can improve achievability results over i.i.d. random codes in different secure communication scenarios. For instance, two schemes based on real alignment of structured signals were tested on a multi-user Gaussian interference channel with confidential messages [1], [2]. In [1], a two-user Gaussian interference channel with no helper was considered, in which each user had a message for its intended receiver to be kept confidential from the other receiver. It was shown that the optimal sum secure degrees of freedom can be achieved for this channel through cooperative jamming signals and real alignment [1]. The case with extra nodes serving as helpers was further investigated at infinite SNR in [1]. Also, the scheme proposed in [2] attained the optimal sum s.d.o.f. for the $K > 2$-user Gaussian interference channels with confidential messages and no helper; it was shown that the optimal s.d.o.f. for this general case is equal to $\frac{K(K-1)}{2K-1}$ [2].

Although the aforementioned schemes showed promising performance in the infinite SNR regime, their extension to the finite SNR regimes is challenging due to the difficulty in bounding their decoding error probability at a finite SNR value. In this work, we consider the two-user Gaussian interference channel with no helper in which each transmitter wishes to send a message to its intended receiver while keeping it confidential from the other receiver. For this scenario, we offer an achievability scheme that combines the idea of using cooperative jamming with the Han-Kobayashi achievability scheme [3]. More specifically, in our scheme each transmitter sends out a superposition of lattice codewords, taken from multiple nested lattice sets. The jamming codewords are also constructed using a lattice structure. Using careful alignments, each transmitter helps the other transmitter to keep its confidential message secret from the unintended receiver. This implies cooperation between the transmitters without any connection. To handle the finite SNR regimes, each receiver applies the compute-and-forward decoding strategy in [4], [5]. We investigate the performance of our scheme for any finite SNR value (as long as $\log(SNR) > 0$) and whenever the interference level lies either in the weak or moderately weak interference regimes. Also, we show that our achievable result reaches the optimal sum secure degrees of freedom for the considered model. Moreover, we provide a discussion on the extension of our scheme to the general case of $K > 2$ users.

The rest of the paper is organized as follows. In Section II, we state the considered problem formally. In section III, we present our achievable results. Section IV provides the proposed achievability scheme along with the analysis of security. Section V extends our scheme to the $K > 2$-user case. Finally, the paper is concluded in Section VI.

II. Problem Statement

We consider the problem of reliable transmission over a two-user interference channel in which each transmitter has a confidential message to send to one intended receiver while keeping it secret from the other receiver. The relationships among channel inputs and outputs are described as:

$$\mathbf{y}_1 = h_{11}\mathbf{x}_1 + h_{21}\mathbf{x}_2 + \mathbf{z}_1 \quad (1)$$

$$\mathbf{y}_2 = h_{22}\mathbf{x}_2 + h_{12}\mathbf{x}_1 + \mathbf{z}_2 \quad (2)$$

where $\mathbf{x}_\ell$ is transmitter ℓ's channel input with length N, and $\mathbf{y}_\ell$ is the channel output at receiver ℓ, for $\ell = 1, 2$. The real-valued $h_{\ell\ell}$ is the channel gain from user ℓ to its respective receiver (the direct link gain) and the real-valued $h_{\ell j}$, for $j = 1, 2$ and $j \neq \ell$, is the cross link gain (the leakage link gain). We assume that the transmitters[1] know the channel states, i.e., the channel gains, in advance. Finally, the random vector $\mathbf{z}_\ell$ is an independent channel noise, which is i.i.d. Gaussian with zero mean and normalized variance.

Transmitter ℓ has an independent confidential message W_ℓ, uniformly distributed over the set $\{1, \ldots, 2^{NR_\ell}\}$, for

[1]In our scheme, knowledge of the channel state is not beneficial either to the receiver or to the eavesdropper.

978-1-5090-1806-2/16/$31.00 ©2016 IEEE

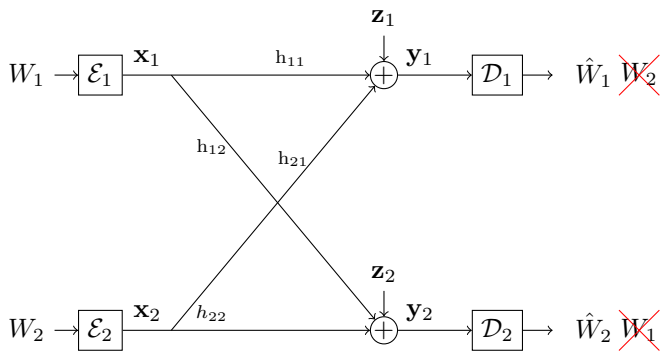

Fig. 1: The two-user Gaussian interference channel model with confidential messages.

$\ell \in \{1,2\}$. Transmitter ℓ maps its message to codeword $\mathbf{x}_\ell$ through a stochastic encoder, i.e., $\mathbf{x}_\ell = \mathcal{E}_\ell(W_\ell)$. Moreover, there is a power constraint on the channel input as $\|\mathbf{x}_\ell\|^2 \leq NP$, for $\ell = 1, 2$. At receiver ℓ, decoder $\mathcal{D}_\ell$ estimates the respective transmitted message as $\hat{W}_\ell = \mathcal{D}_\ell(\mathbf{y}_\ell)$. Figure 1 illustrates the communication model.

Definition 1 (Achievable secure rates): For the two-user Gaussian interference channel with independent confidential messages, a non-negative rate pair (R_1, R_2) is achievable, if for any $\epsilon > 0$ and sufficiently large N, there exist encoders $\{\mathcal{E}_\ell\}_{\ell=1}^2$ and decoders $\{\mathcal{D}_\ell\}_{\ell=1}^2$ such that:

$$\text{Prob}\left(D_\ell(\mathbf{y}_\ell) \neq W_\ell\right) < \epsilon \quad \ell = 1, 2 \tag{3}$$

$$R_1 \leq \frac{1}{N} H(W_1|\mathbf{y}_2) + \epsilon, \quad R_2 \leq \frac{1}{N} H(W_2|\mathbf{y}_1) + \epsilon \tag{4}$$

Inequalities in (3) capture the reliability constraints for both receivers and the constraints in (4) ensure the confidentiality of each message from the unintended receiver according to the notion of weak secrecy [6]. The secrecy capacity region is the supremum over all the achievable secure rate pairs.

Definition 2 (Weak and moderately weak interference regimes): In our model, the interference to noise ratio (INR) for receivers 1 and 2 is defined as[2]

$$INR_1 \triangleq h_{21}^2 P, \quad INR_2 \triangleq h_{12}^2 P \tag{5}$$

Then, the *weak interference regime* includes all channel gains such that

$$\frac{1}{2} \leq \left(\frac{\log(h_{21}^2 P)}{\log(h_{11}^2 P)}\right) < \frac{2}{3}, \quad \frac{1}{2} \leq \left(\frac{\log(h_{12}^2 P)}{\log(h_{22}^2 P)}\right) < \frac{2}{3} \tag{6}$$

Furthermore, the *moderately weak interference regime* includes all channel gains such that

$$\frac{2}{3} \leq \left(\frac{\log(h_{21}^2 P)}{\log(h_{11}^2 P)}\right) < 1, \quad \frac{2}{3} \leq \left(\frac{\log(h_{12}^2 P)}{\log(h_{22}^2 P)}\right) < 1 \tag{7}$$

Note that Definition 2 is aligned with the common notions of weak and moderately weak interference regimes in the literature, e.g., as in [4].

[2]We assume that $\log(h_{11}^2 P) > 0$ and $\log(h_{22}^2 P) > 0$ which are consistent with the assumption that users operate above noise level.

III. Main Results

Consider $P_{t1}, P_{u1}, P_{t2}, P_{u2}$ as non-negative scalar variables such that $P_{t1} + \left(\frac{h_{21}}{h_{11}}\right)^2 P_{u1} \leq P$ and $P_{t2} + \left(\frac{h_{12}}{h_{22}}\right)^2 P_{u2} \leq P$. Then, the following theorem provides a lower bound on the achievable secure rates.

Theorem 1: A rate pair (R_1, R_2) which satisfies the following inequalities is an achievable secure rate pair for the weak and moderately weak interference regimes.

$$R_1 < R_{comb,2}^{(1)} - \frac{1}{2}\log\left(\frac{P_{u2} + P_{t1}}{P_{u2}}\right) \tag{8}$$

$$R_2 < R_{comb,2}^{(2)} - \frac{1}{2}\log\left(\frac{P_{u1} + P_{t2}}{P_{u1}}\right) \tag{9}$$

In which, $R_{comb,2}^{(1)}$ is a lower bound on the optimal combination rate at which transmitter 1's message can be reliably decoded by receiver 1 using the asymmetric compute-and-forward decoding strategy. The achievable combination rate $R_{comb,2}^{(1)}$ is mathematically computed in (20). The combination rate $R_{comb,2}^{(2)}$ is similarly defined for receiver 2. The proof of Theorem 1 is shown in Section IV.

Corollary 1: The secure rates in (8) and (9) scale linearly with $\log(P)$.
The proof of Corollary 1 is provided in Section IV.

Corollary 2: The optimal sum secure degrees of freedom of $\frac{2}{3}$ is achievable using our proposed scheme, i.e.,

$$\lim_{P\to\infty} \frac{R_1 + R_2}{\frac{1}{2}\log(1+P)} = \frac{2}{3} \tag{10}$$

The achievability proof of Corollary 2 is deduced by applying Corollary 5 in [4] to $R_{comb,2}^{(1)}$ and $R_{comb,2}^{(2)}$ and the fact that the second terms in (8) and (9) are constant with respect to power P. Also, the upper bound was shown in [1].

Remark 1: Recall that the performance of i.i.d. Gaussian random codes was investigated in [7] under three different schemes including time-sharing, multiplexed transmission, and incorporation of artificial noise. According to the results in [7], i.i.d. Gaussian random codes achieve *zero* sum secure degrees of freedom for the two-user Gaussian interference channel in all the three schemes.

IV. Achievability Scheme

We begin the achievabiliy proof of Theorem 1 by describing our codebook construction, encoding, decoding strategies, and analysis of security.

A. Codebook construction

Our codebook construction is motivated by the Han-Kobayashi scheme in which each user transmits a superposition of codewords taken from two nested lattice codebooks. However, the difference here is that the second lattice codebook is used to encode the jamming signal. Therefore, each transmitter encodes its message as well as a cooperative jamming signal that masks the other transmitter's message at the unintended receiver. We describe the codebook construction for transmitter 1; transmitter 2 builds its codebook similarly.

The transmitter picks two n-dimensional pairs of coarse and fine lattice sets $(\Lambda_{t,1}, \Lambda_{t,f,1})$ and $(\Lambda_{u,1}, \Lambda_{u,f,1})$. The former coarse and fine lattice pair, indexed by t, is used for encoding transmitter's message and the latter pair indexed by u is used for encoding the transmitter's jamming signal. Assume that the lattice sets chosen by both transmitters form a nested structure as[3]

$$\Lambda \subseteq \Lambda_{t,2} \subseteq \Lambda_{t,1} \subseteq \Lambda_{u,2} \subseteq \Lambda_{u,1} \subseteq \Lambda_{t,f,2} \subseteq \Lambda_{t,f,1} \subseteq \Lambda_{u,f,2} \subseteq \Lambda_{u,f,1} \tag{11}$$

We scale the coarse lattice sets such that the second moments of $\Lambda_{t,2}, \Lambda_{t,1}, \Lambda_{u,2}, \Lambda_{u,1}$ are determined by $P_{t,2}, P_{t,1}, P_{u,2}, P_{u,1}$, respectively. We denote the fundamental Voronoi region of the coarse lattice $\Lambda_{t,1}$ as $\mathcal{V}_{t,1}$. The centers of the cosets of the fine lattice $\Lambda_{t,f,1}$ are n-length lattice words which are considered as the realizations of the n-length random vector $\mathbf{t}_1$. Then, the lattice codebook of transmitter 1 is constructed as $\mathcal{L}_{t,1} \triangleq \{\mathbf{t}_1 | \mathbf{t}_1 \in \mathcal{V}_{t,1}\}$ and is dubbed as the *inner* codebook. Assume a probability distribution $P(\mathbf{t}_1)$ over the inner codebook $\mathcal{L}_{t,1}$. Then, transmitter 1 constructs a realization of an N-length random vector $\bar{\mathbf{t}}_1$, where $N \triangleq n \times B$, by generating B i.i.d. copies of $\mathbf{t}_1$ according to the distribution $P(\mathbf{t}_1)$. This process is repeated for $2^{NR^{(1)}_{comb,2}}$ times. The collection of the generated vectors are called as the *outer* codebook and is denoted by $\mathcal{C}_{t,1}$. Also, vector $\bar{\mathbf{t}}_1$ represents the random vector for the *outer* lattice codewords of transmitter 1. Note that $R^{(1)}_{comb,2} \triangleq \frac{1}{n}\log(|\mathcal{L}_{t,1}|)$ is the rate at which the inner codewords of transmitter 1 are generated.

In addition to the codebooks for the confidential message, the transmitter constructs an inner codebook $\mathcal{L}_{u,1}$ and an outer codebook $\mathcal{C}_{u,1}$ for the *jamming* signal, in a similar manner. The random vector assigned to the jamming inner lattice codewords is denoted by $\mathbf{u}_1$, and $\bar{\mathbf{u}}_1$ represents the random vector for the jamming outer codewords. In the next step, codebook $\mathcal{C}_{t,1}$ is randomly partitioned into 2^{NR_1} bins of equal size. The random variable representing the bin index is denoted by W_1 and its realization w_1 takes values from the set $\{1, \ldots, 2^{NR_1}\}$. $\mathcal{C}_{t,1}(w_1)$ is the set of outer codewords belong to bin w_1.

Finally, a set of random N-length vectors $\bar{\mathbf{d}}_{t,1}$ and $\bar{\mathbf{d}}_{u,1}$ are generated for dithering. Assume that each n-length block of dither $\bar{\mathbf{d}}_{t,1}$ has a uniform distribution over $\mathcal{V}_{t,1}$, and similarly, each n-length block of dither $\bar{\mathbf{d}}_{u,1}$ has a uniform distribution over the corresponding Voronoi region $\mathcal{V}_{u,1}$. Dithers are public and hence they don't add to secrecy. Note that transmitter 2 constructs its codebooks similarly.

B. Encoding

We describe the encoding procedure for transmitter 1; similar arguments hold for encoding at transmitter 2. To encode the confidential message w_1, transmitter 1 randomly picks a codeword $\bar{\mathbf{t}}_1$ from the bin set $\mathcal{C}_{t,1}(w_1)$. Then, it dithers the codeword using a randomly generated N-length vector $\bar{\mathbf{d}}_{t,1}$. The result is reduced to the Voronoi region $\mathcal{V}_{t,1}$ using the modular operation. Also, $\bar{\mathbf{u}}_1$ is chosen at random. We have:

$$\bar{\mathbf{t}}_{1,d} \triangleq \big[\bar{\mathbf{t}}_1 + \bar{\mathbf{d}}_{t,1}\big] \bmod \Lambda_{t,1},\ \bar{\mathbf{u}}_{1,d} \triangleq \big[\bar{\mathbf{u}}_1 + \bar{\mathbf{d}}_{u,1}\big] \bmod \Lambda_{u,1} \tag{12}$$

Next step in the encoding procedure is scaling the jamming codeword such that it aligns with the confidential codeword of transmitter 2 at receiver 1. The superposition of the confidential codeword with the scaled jamming codeword is sent through the channel as the transmitter 1 input, i.e., $\mathbf{x}_1 = \bar{\mathbf{t}}_{1,d} + \frac{h_{21}}{h_{11}}\bar{\mathbf{u}}_{1,d}$. Note that $\mathbf{x}_1$ satisfies the channel input power constraint, thus, $P_{t1} + \left(\frac{h_{21}}{h_{11}}\right)^2 P_{u1} \leq P$.

C. Decoding

As in the previous steps, we describe the decoding procedure at receiver 1; receiver 2 acts similarly. The decoding procedure is based on the asymmetric compute-and-forward strategy, introduced in [4] and [5]. In our model, receiver 1 observes sequence $\mathbf{y}_1$ from the channel as

$$\mathbf{y}_1 = h_{11}\bar{\mathbf{t}}_{1,d} + h_{21}(\bar{\mathbf{t}}_{2,d} + \bar{\mathbf{u}}_{1,d}) + \frac{h_{21}h_{12}}{h_{22}}\bar{\mathbf{u}}_{2,d} + \mathbf{z}_1 \tag{13}$$

Assume that the powers of codewords $\bar{\mathbf{u}}_{1,d}$ and $\bar{\mathbf{u}}_{2,d}$ are set such that the codewords $\frac{h_{12}h_{21}}{h_{11}}\bar{\mathbf{u}}_{1,d}$ and $\frac{h_{21}h_{12}}{h_{22}}\bar{\mathbf{u}}_{2,d}$ are below the noise power level. As jamming codewords do not carry useful information about the confidential signals, receiver 1 treats the third term in (13) as noise. Therefore, receiver 1 observes an effective two-user Gaussian multiple-access channel (GMAC) as $\mathbf{y}_1 = h_{11}\bar{\mathbf{t}}_{1,d} + h_{21}(\bar{\mathbf{t}}_{2,d} + \bar{\mathbf{u}}_{1,d}) + \tilde{\mathbf{z}}_1$, in which $\tilde{\mathbf{z}}_1$ is the effective noise seen by receiver 1. Now, let us normalize the noise power to form a standard effective MAC as in [4]. We have:

$$\tilde{\mathbf{y}}_1 = \frac{h_{11}}{\sqrt{1+\alpha_1^2 P_{u2}}}\bar{\mathbf{t}}_{1,d} + \frac{h_{21}}{\sqrt{1+\alpha_1^2 P_{u2}}}(\bar{\mathbf{t}}_{2,d} + \bar{\mathbf{u}}_{1,d}) + \tilde{\mathbf{z}}_{eff,1} \tag{14}$$

where $\tilde{\mathbf{z}}_{eff,1}$ is the normalized-power effective noise; the factor α_1 is defined as $\alpha_1 \triangleq \frac{h_{12}h_{21}}{h_{22}}$; finally, $\tilde{\mathbf{y}}_1$ is the scaled sequence observed at receiver 1.

Consider the effective channel vector, $\mathbf{h}_{eff,1}$, and the power scaling vector, $\mathbf{b}_{eff,1}$, defined as $\mathbf{h}_{eff,1} \triangleq \left(\frac{h_{11}}{\sqrt{1+\alpha_1^2 P_{u2}}}, \frac{h_{21}}{\sqrt{1+\alpha_1^2 P_{u2}}}\right)^T$ and $\mathbf{b}_{eff,1} \triangleq \left(\sqrt{\frac{P_{t1}}{P}}, \sqrt{\frac{P_{t2}+P_{u1}}{P}}\right)^T$, respectively. Then, according to Theorem 7 in [4], the sum of the optimal combination rates for the above effective two-user GMAC seen by receiver 1 is lower-bounded as

$$\sum_{\ell=1}^{2} R^{(1)}_{comb,\ell} \geq \frac{1}{2}\log\left(\frac{1+P\sum_{\ell=1}^{2}\mathbf{h}^2_{eff,1}(\ell)\mathbf{b}^2_{eff,1}(\ell)}{\mathbf{b}^2_{eff,1}(1)\mathbf{b}^2_{eff,1}(2)}\right) - 1 \tag{15}$$

Next, assume the optimal combination rates for the aforementioned effective GMAC are sorted in a descending order, i.e., $R^{(1)}_{comb,1} \geq R^{(1)}_{comb,2}$. Then, based on Theorem 9 in [4], it is guaranteed that transmitter 1's confidential message can be decoded reliably by receiver 1 for all rates not bigger than

[3] Λ is the common coarsest lattice set.

$R^{(1)}_{comb,2}$ unless the effective channel gains are rational[4]. As a result, it remains to find a lower bound on the achievable rate $R^{(1)}_{comb,2}$, i.e.,

$$R^{(1)}_{comb,2} = \sum_{\ell=1}^{2} R^{(1)}_{comb,\ell} - R^{(1)}_{comb,1} \tag{16}$$

which is equivalent to finding an upper bound on the achievable rate $R^{(1)}_{comb,1}$, which maps to the decoding rate of the aligned codewords $\bar{\mathbf{t}}_{2,d} + \bar{\mathbf{u}}_{1,d}$. Therefore, the computation rate for $R^{(1)}_{comb,1}$ is given as $R^{(1)}_{comb,1} = \frac{1}{2}\log(P_{t2} + P_{u1}) - \frac{1}{2}\log(\sigma^2_{eff,1})$, in which $\sigma^2_{eff,1}$ is the variance of the effective noise in *the first integer linear combination of the codewords decoded at receiver 1*. Let us denote the first integer linear combination as $\mathbf{v}_1$. Assume it is determined by the integer-valued 2×1 vector $\mathbf{a}_1$, i.e., $\mathbf{v}_1 \triangleq \mathbf{a}_1(1)(\bar{\mathbf{t}}_2 + \bar{\mathbf{u}}_1) + \mathbf{a}_1(2)\bar{\mathbf{t}}_1$. Recall that according to the compute-and-forward strategy in [8], the receiver decodes an estimate of $\mathbf{v}_1$ as follows:

$$\mathbf{s}_1 = \left[\beta\tilde{\mathbf{y}}_1 - \mathbf{a}_1(1)(\bar{\mathbf{d}}_{t,2} + \bar{\mathbf{d}}_{u,1}) - \mathbf{a}_1(2)\bar{\mathbf{d}}_{t,1}\right] \bmod \Lambda \tag{17}$$

$$= \left[\mathbf{v}_1 + \mathbf{z}_{eff,1}\right] \bmod \Lambda \tag{18}$$

in which $\beta \in \mathbb{R}$ is a scaling factor. To estimate $\mathbf{v}_1$ from (18), the receiver quantizes (18) with respect to the finest participating lattice, i.e., $\hat{\mathbf{v}} \triangleq Q_{\Lambda_{u,f,1}}(\mathbf{s}_1)$. Note that the modular operation as well as the quantization are done block-wise.

To upper-bound the combination rate $R^{(1)}_{comb,1}$, it is sufficient to lower bound $\sigma^2_{eff,1}$; which is computed as

$$\sigma^2_{eff,1} \triangleq \Big(\beta^2 + P\Big(\mathbf{b}^2_{eff,1}(1)(\beta\mathbf{h}_{eff,1}(1) - \mathbf{a}_1(1))^2 + \mathbf{b}^2_{eff,1}(2)(\beta\mathbf{h}_{eff,1}(2) - \mathbf{a}_1(2))^2\Big)\Big) \tag{19}$$

Finally, the effective variance is minimized over β and $\mathbf{a}_1$ and it is denoted by $\sigma^{*2}_{eff,1}$, i.e., $\sigma^{*2}_{eff,1} \triangleq \min_{\beta,\mathbf{a}} \sigma^2_{eff,1}$. As a result, a lower bound on the achievable rate $R^{(1)}_{comb,2}$ is obtained as

$$R^{(1)}_{comb,2} \geq \frac{1}{2}\log\left(1 + \mathbf{h}^2_{eff,1}(1)P_{t1} + \mathbf{h}^2_{eff,2}(2)\left(P_{t2} + P_{u1}\right)\right) + \log(P) + \frac{1}{2}\log(\sigma^{*2}_{eff,1}) - \frac{1}{2}\log(P_{t1}) - \log(P_{t2} + P_{u1}) - 1 \tag{20}$$

Prior to security analysis, we show that the rates in (8) and (9) scale with power as it was claimed in Corollary 1.

Proof of Corollary 1: We show that R_1 scales linearly with $\log(P)$; the same result can be shown for R_2, using similar arguments. To this end, let us assume a power allocation among the users' jamming powers and confidential-messages powers as $P_{t1} = P_{t2} = (1-\gamma^2)P$ and $(\frac{h_{21}}{h_{11}})^2 P_{u1} = (\frac{h_{12}}{h_{22}})^2 P_{u2} = \gamma^2 P$, for some $0 < \gamma^2 < 1$. This is a valid choice as it satisfies the power constraint. Substituting these power values in (8), we observe that the second term in (8) is constant with respect to P for any valid choice of γ. Therefore, it is enough to show that $R^{(1)}_{comb,2}$ grows linearly with $\log(P)$. Now assume $\gamma^2 = \frac{1}{h^2_{21}P}$, which may be a sub-optimal choice.

[4]The Lebesgue measure of such event is small [4]

The validity of this choice can be checked easily for the weak and the moderately weak interference regimes. Note that this choice for γ^2 makes the power of the third term in (13) to be within noise level. Having chosen γ^2 as mentioned, we can compute P_{u2}, P_{t1} accordingly. As a result, we observe that the first and fourth terms in (20) can be rewritten as $\frac{1}{2}\log(P) + c_1$ and $\frac{1}{2}\log(P) + c_2$ for some constants (with respect to P) c_1, c_2, respectively; additionally, the fifth term can be simplified as $\log(P) + c_3$ for a constant c_3. As a result, we have $R^{(1)}_{comb,2} \geq \frac{1}{2}\log(\sigma^{*2}_{eff,1}) + c_1 + c_2 + c_3$. Now, consider the expression in (19); note that it can be rewritten as $\sigma^2_{eff,1} = (\beta^2 + c_4(\mathbf{a}, \beta)P)$ in which $c_4(.)$ is a positive number. Since the latter holds for any choice of β and integer coefficient vector $\mathbf{a}$, it is also true for the the infimum and as a result, $\log(\sigma^{*2}_{eff,1}) \propto \log(P)$. This completes the proof of Corollary 1.

D. Analysis of Security

In this subsection we show that our scheme provides weak secrecy for each transmitter's confidential message. Specifically, we prove weak secrecy for transmitter 1's confidential message W_1; the proof of weak secrecy for transmitter 2's message is deduced similarly. We have

$$\frac{1}{N}I(W_1;\mathbf{y}_2) \leq \frac{1}{N}I(W_1;\mathbf{y}_2,\bar{\mathbf{t}}_2) = R_1 - \frac{1}{N}H(W_1|\mathbf{y}_2,\bar{\mathbf{t}}_2) \tag{21}$$

Next, we find a lower bound on the second term in (21) as follows:

$$\begin{aligned}
&\frac{1}{N}H(W_1|\mathbf{y}_2,\bar{\mathbf{t}}_2) = \frac{1}{N}H(\bar{\mathbf{t}}_1, W_1|\mathbf{y}_2,\bar{\mathbf{t}}_2) - \frac{1}{N}H(\bar{\mathbf{t}}_1|\mathbf{y}_2,\bar{\mathbf{t}}_2,W_1)\\
&\geq \frac{1}{N}H(\bar{\mathbf{t}}_1|\mathbf{y}_2,\bar{\mathbf{t}}_2) - \frac{1}{N}H(\bar{\mathbf{t}}_1|\mathbf{y}_2,\bar{\mathbf{t}}_2,W_1)\\
&\overset{(a)}{\geq} \frac{1}{N}H(\bar{\mathbf{t}}_1|\mathbf{y}_2,\bar{\mathbf{t}}_2) - 2\epsilon_2 \overset{(b)}{\geq} \frac{1}{N}H(\bar{\mathbf{t}}_1|\mathbf{y}_2,\bar{\mathbf{t}}_2,\bar{\mathbf{u}}_1,\mathbf{z}_2,D) - 2\epsilon_2
\end{aligned} \tag{22}$$

Inequality (a) is deduced by applying Lemma 1 in [9] to outer codewords $\bar{\mathbf{t}}_1$. Inequality (b) holds since conditioning reduces entropy. In (22), D denotes the collection of all the dither vectors. Note that receiver 2 observes $\mathbf{y}_2 = h_{22}\bar{\mathbf{t}}_{2,d} + h_{12}(\bar{\mathbf{t}}_{1,d} + \bar{\mathbf{u}}_{2,d}) + \frac{h_{12}h_{21}}{h_{11}}\bar{\mathbf{u}}_{1,d} + \mathbf{z}_2$. Hence, if the receiver 2 had the information of the random vectors D, $\mathbf{z}_2$, and $\bar{\mathbf{t}}_2$, it could decode the aligned lattice codeword $\bar{\mathbf{t}}_{1,d} + \bar{\mathbf{u}}_{2,d}$. As a result, based on (22), we have

$$\begin{aligned}
&\frac{1}{N}H(W_1|\mathbf{y}_2,\bar{\mathbf{t}}_2) \geq \frac{1}{N}H(\bar{\mathbf{t}}_1|\bar{\mathbf{t}}_{1,d}+\bar{\mathbf{u}}_{2,d},\bar{\mathbf{t}}_2,\bar{\mathbf{u}}_1,\mathbf{z}_2,D) - 2\epsilon_2\\
&= \frac{1}{N}H\Big(\bar{\mathbf{t}}_1\Big|[\bar{\mathbf{t}}_{1,d}+\bar{\mathbf{u}}_{2,d}] \bmod \Lambda_{u,2}, Q_{\Lambda_{u,2}}(\bar{\mathbf{t}}_{1,d}+\bar{\mathbf{u}}_{2,d}),\bar{\mathbf{t}}_2,\bar{\mathbf{u}}_1,\mathbf{z}_2,D\Big) - 2\epsilon_2\\
&\geq \frac{1}{N}H\Big(\bar{\mathbf{t}}_1\Big|[\bar{\mathbf{t}}_{1,d}+\bar{\mathbf{u}}_{2,d}] \bmod \Lambda_{u,2},\bar{\mathbf{t}}_2,\bar{\mathbf{u}}_1,\mathbf{z}_2,D\Big)\\
&\quad - \frac{1}{N}H(Q_{\Lambda_{u,2}}(\bar{\mathbf{t}}_{1,d}+\bar{\mathbf{u}}_{2,d})\big|\bar{\mathbf{t}}_2,\bar{\mathbf{u}}_1,\mathbf{z}_2,D) - 2\epsilon_2\\
&\overset{(a)}{=} \frac{1}{N}H\Big(\bar{\mathbf{t}}_1\Big|[\bar{\mathbf{t}}_1+\bar{\mathbf{u}}_2] \bmod \Lambda_{u,2}\Big)
\end{aligned}$$

$$
\begin{aligned}
&-\frac{1}{N}H\Big(Q_{\Lambda_{u,2}}(\bar{\mathbf{t}}_{1,d}+\bar{\mathbf{u}}_{2,d})\Big|\bar{\mathbf{t}}_2,\bar{\mathbf{u}}_1,\mathbf{z}_2,D\Big)-2\epsilon_2\\
&\overset{(b)}{=}\frac{1}{N}H(\bar{\mathbf{t}}_1)-\frac{1}{N}H(Q_{\Lambda_{u,2}}(\bar{\mathbf{t}}_{1,d}+\bar{\mathbf{u}}_{2,d})\big|\bar{\mathbf{t}}_2,\bar{\mathbf{u}}_1,\mathbf{z}_2,D)-2\epsilon_2\\
&\geq\frac{1}{N}H(\bar{\mathbf{t}}_1)-\frac{1}{N}H(Q_{\Lambda_{u,2}}(\bar{\mathbf{t}}_{1,d}+\bar{\mathbf{u}}_{2,d}))-2\epsilon_2\\
&\overset{(c)}{\geq}\frac{1}{N}H(\bar{\mathbf{t}}_1)-\frac{1}{2}\log\left(\frac{P_{u2}+P_{t1}}{P_{u2}}\right)-\delta(\epsilon)-2\epsilon_2\\
&=R_{comb,2}^{(1)}-\frac{1}{2}\log\left(\frac{P_{u2}+P_{t1}}{P_{u2}}\right)-\delta(\epsilon)-2\epsilon_2 \qquad (23)
\end{aligned}
$$

in which equality (a) is due to the fact that the random vectors $\bar{\mathbf{t}}_1, \bar{\mathbf{u}}_2$ are independent from the dithers, the noise and random vectors $\bar{\mathbf{u}}_1, \bar{\mathbf{t}}_2$. Equality (b) follows from Crypto Lemma, Lemma 2 in [10], which states that the lattice codeword $[\bar{\mathbf{t}}_1 + \bar{\mathbf{u}}_2] \bmod \Lambda_{u,2}$ belongs to the codebook $\mathcal{L}_{u,2}$ (operation mod is done for each n-length block) and is independent of codeword $\bar{\mathbf{t}}_1$. Finally, inequality (c) is deduced from Lemma 1 in [11], which bounds the discrete entropy of the quantized vector. Eventually, from (8), (23), and (21), the weak secrecy proof for transmitter 1's confidential message is concluded.

V. The general case: The Gaussian Interference Channel with $K > 2$ users

Our scheme in Section IV can be modified to preserve the confidentiality of all the messages from the unintended receivers when there are $K > 2$ users. Recall that in our scheme, each jamming signal was designed to protect one confidential message at one receiver. For the case of $K > 2$ users, we divide each confidential message into $K - 1$ independent random sub-messages and assign each of them a lattice codebook. For transmitter ℓ, the sub-messages outer codewords are denoted by $\{\bar{\mathbf{t}}_{\ell,i}\}_{i=1,i\neq\ell}^{K}$; for $\ell \in \{1, \ldots, K\}$. Now, each jamming codeword protects a portion of all sub-messages at all the required receivers simultaneously. For instance, the jamming codeword of transmitter ℓ, i.e., $\bar{\mathbf{u}}_\ell$ conceals all codewords $\{\bar{\mathbf{t}}_{i,\ell}\}_{i=1,i\neq\ell,i\neq j}^{K}$ at receiver j. However, this requires that $\bar{\mathbf{u}}_\ell$ get aligned with the same codeword at multiple receiver even though the channel link gains are not the same for different receivers. As an example, consider the case of $K = 3$: $\bar{\mathbf{u}}_1$ needs to align with $\bar{\mathbf{t}}_{2,1}$ at receivers 1 and 2; additionally, it should protect $\bar{\mathbf{t}}_{3,1}$ at receivers 1 and 3. Clearly, perfect alignment would not be achieved given that channel link gains are not the same. To remedy this alignment issue, we incorporate a generalization of the asymptotic *real* alignment proposed in [12] and used in [2], [13]. Using this technique, we further split each sub-message inner codeword into large number of components each of which is an n-dimensional lattice vector. Next, using a proper beamforming of the transmitted signals, we can show that a subset of components of each codeword gets aligned with a subset of components of a jamming codeword. Hence, even though a perfect alignment between two desired codewords cannot be achieved at more than one receiver, a partial alignment among their corresponding components can occur at all the required receivers, simultaneously. It can be shown that for a large number of components, the desired alignments happen at all the receivers asymptotically. We aim to further elaborate our scheme for this general case in the extended version of this paper.

VI. Conclusion

In this paper, we considered a reliable and secure communication scenario through the two-user Gaussian interference channel when the interference level is either weak or moderately weak. We showed that our achievable result scales linearly with $\log(SNR)$, when $\log(SNR) > 0$, and reaches the optimal sum secure degrees of freedom at infinite SNR. We also argued how our scheme could be extended to the $K > 2$-user case.

References

[1] J. Xie and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," *IEEE Transactions on Information Theory*, vol. 60, no. 6, pp. 3359–3378, 2014.

[2] J. Xie and S. Ulukus, "Secure degrees of freedom of-user gaussian interference channels: A unified view," *Information Theory, IEEE Transactions on*, vol. 61, no. 5, pp. 2647–2661, 2015.

[3] H. Te Sun and K. Kobayashi, "A new achievable rate region for the interference channel," *IEEE transactions on information theory*, vol. 27, no. 1, pp. 49–60, 1981.

[4] O. Ordentlich, U. Erez, and B. Nazer, "The approximate sum capacity of the symmetric gaussian-user interference channel," *IEEE Transactions on Information Theory*, vol. 60, no. 6, pp. 3450–3482, 2014.

[5] V. Ntranos, V. R. Cadambe, B. Nazer, and G. Caire, "Asymmetric compute-and-forward," in *51th Annual Allerton Conference on Communications, Control, and Computing*, Monticello, IL, September 2013.

[6] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Advances in CryptologyEUROCRYPT 2000*, pp. 351–368, Springer, 2000.

[7] R. Liu, I. Marić, P. Spasojević, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2493–2507, 2008.

[8] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6463–6486, 2011.

[9] P. Babaheidarian, S. Salimi, and P. Papadimitratos, "Finite-SNR regime analysis of the gaussian wiretap multiple-access channel," in *53th Annual Allerton Conference on Communications, Control, and Computing*, Monticello, IL, September 2015.

[10] G. D. Forney, "On the role of mmse estimation in approaching the information-theoretic limits of linear gaussian channels: Shannon meets wiener," in *41th Annual Allerton Conference on Communications, Control, and Computing*, Monticello, IL, September 2003.

[11] P. Babaheidarian and S. Salimi, "Compute-and-forward can buy secrecy cheap," in *in Proceedings of the International Symposium on Information Theory Proceedings (ISIT 2015)*, pp. 2475–2479, 2015.

[12] A. S. Motahari and S. Oveis-Gharan, "Real interference alignment: Exploiting the potential of single antenna systems," *IEEE Transactions on Information Theory*, vol. 60, no. 8, pp. 4799–4810, 2014.

[13] A. Khisti, "Interference alignment for the multiantenna compound wiretap channel," *Information Theory, IEEE Transactions on*, vol. 57, no. 5, pp. 2976–2993, 2011.