Preserving Confidentiality in The Gaussian Broadcast Channel Using Compute-and-Forward

Parisa Babaheidarian[1], Somayeh Salimi[2], and Panos Papadimitratos[3]
[1]Boston University, [2]Uppsala University, [3]KTH Royal Institute of Technology

***Abstract*—We study the transmission of confidential messages across a wireless broadcast channel with $K > 2$ receivers and K helpers. The goal is to transmit all messages reliably to their intended receivers while keeping them confidential from the unintended receivers. We design a codebook based on nested lattice structure, cooperative jamming, lattice alignment, and i.i.d. coding. Moreover, we exploit the asymmetric compute-and-forward decoding strategy to handle finite SNR regimes. Unlike previous alignment schemes, our achievable rates are attainable at any finite SNR value. Also, we show that our scheme achieves the optimal sum secure degrees of freedom of 1 for the K-receiver Gaussian broadcast channel with K confidential messages and K helpers.**

I. Introduction

Physical-layer security has been widely studied under different communication scenarios. The encoding strategies have been used to analyze these security scenarios can be grouped in two main categories: i.i.d. random coding and structured coding. Several achievability schemes were proposed within the first category. Csiszar and Korner discussed transmitting a confidential message over a broadcast channel with one legitimate receiver and one passive eavesdropper [1]; capacity results were obtained for a less noisy channel using random i.i.d. codes. Recently, several works in the second category shed lights on the advantage of structured codes in achieving security. In the absence of capacity results for different communication channels in general cases (i.e., no assumption on degradedness or specific channel gains), researchers have studied the secure degrees of freedom (s.d.o.f.) in the infinite SNR regime. Despite the promising performance that Gaussian i.i.d. codes show in maintaining reliability in AWGN channels, studies show that they achieve *zero* sum *secure* degrees of freedom [2] and [3]. In contrast, structured codes attain a positive secure degrees of freedom [4], [5], and [6]. In [5], a collection of one-hop communication scenarios were considered including the wiretap Gaussian broadcast channel with helpers. Xie and Ulukus in [5] and [7] suggested an achievable scheme for the considered security scenarios which was based on real alignment encoding, cooperative jamming, and maximum likelihood decoder which operated in the infinite SNR regime; they showed that following their schemes, optimal sum secure degrees of freedom are achievable. Also, in [8] and [3], a lattice-based scheme was proposed for the Gaussian wiretap channel with one helper which was optimal at infinite SNR for a subset of channel gains.

A lattice-based framework known as the *compute-and-forward* framework [9] was proposed to handle interference which enabled the decoder to decode integer linear combinations of the transmitted codewords. In [6] and [10], we investigated the Gaussian wiretap multiple-access channel and the two-user Gaussian interference channel with confidential messages, respectively. For these models, we introduced achievable schemes which, unlike previous works, could operate at any finite SNR value and for almost all (real) channel gains. Furthermore, we derived constant gap results for the sum secure capacity. In this paper, we study the Gaussian broadcast channel with K receivers and K helpers for $K > 2$. The case of $K = 2$ with one helper was studied in [5] and optimal s.d.o.f. was obtained.

In our model, the transmitter has an independent message for each receiver which needs to be kept confidential from other receivers. A set of K helpers implicitly cooperate with the transmitter by sending out jamming signals with proper beam-forming, to assist the transmitter in preserving the confidentiality of messages at the unintended receivers. We propose an achievability scheme which works at any SNR value and for almost all real-valued channel gains[1]. We offer a set of lower bounds on individual secure rates and show that the sum secure rate is within a constant gap from the sum secure capacity for this channel model. Our achievable scheme combines the idea of jamming signals and beamforming with asymptotic alignment in [7] and a generalization of the compute-and-forward framework in [11]. We extend the nested lattice framework of [11] to ensure security in our scheme.

The rest of the paper is organized as follows: in Sec. II, we formally state the problem, in Sec. III our main results are presented. Sec. IV is devoted to the achievability scheme along with proofs of reliability and security analysis. Finally, The paper is concluded in Sec. V.

II. Problem Statement

We study the K-receiver Gaussian broadcast channel with confidential messages. The transmitter has K confidential messages, $W_1, W_2, \ldots, W_K$, for receivers $1, 2, \ldots, K$, respectively. Each receiver acts as a passive eavesdropper with respect to all messages excluding its own intended message. In addition, there are K helpers sending jamming signals to protect the confidentiality of messages at unintended receivers. The goal is to ensure the reliability of the intended messages

[1]Except for a set of channel gains with small Lebesgue measure.

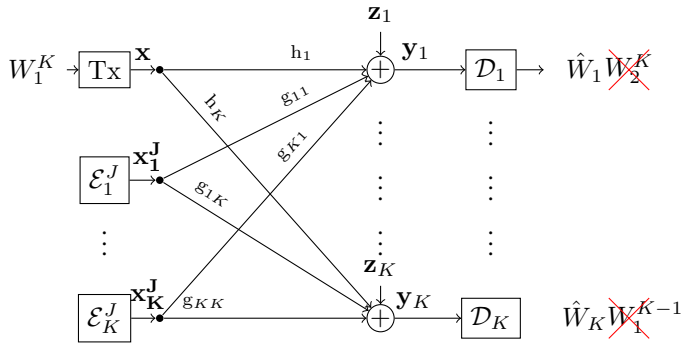

Fig. 1: The K-receiver Gaussian broadcast channel with confidential messages and K helpers.

and the confidentiality of the unintended messages. The relation among the transmitter's and the helpers' inputs and the output of the channel at receiver ℓ is determined as:

$$\mathbf{y}_\ell = h_\ell \mathbf{x} + \sum_{i=1}^{K} g_{i\ell} \mathbf{x}_i^J + \mathbf{z}_\ell \tag{1}$$

$\mathbf{y}_\ell$ is receiver ℓ's observation from the channel, $\mathbf{x}$ is the N-length input vector transmitted by the transmitter, h_ℓ is the main channel gain from the transmitter to receiver ℓ. Moreover, $\mathbf{x}_i^J$ is the jamming signal transmitted by the i-th helper, $g_{i\ell}$ is the gain of the channel between helper i and receiver ℓ. Note that we consider real-valued channel gains in our model. Finally, $\mathbf{z}_\ell$ is an independent i.i.d. Gaussian noise with zero means and unit variances. The power constraints at the transmitter and the helpers are given as $\|\mathbf{x}\|^2 \leq NP$ and $\sum_{i=1}^{K} \|\mathbf{x}_i^J\|^2 \leq NP$. The confidential message, W_ℓ, is independent of all other messages and is uniformly distributed over the set $\{1, \ldots, 2^{NR_\ell}\}$, for $\ell \in \{1, \ldots, K\}$. The transmitter maps the messages to codeword $\mathbf{x}$ through a stochastic encoder, i.e., $\mathbf{x} = \mathcal{E}(W_1, W_2, \ldots, W_K)$. 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 K-receiver Gaussian broadcast channel with K independent confidential messages, a non-negative rate tuple $(R_1, R_2, \ldots, R_K)$ is achievable, if for any $\epsilon > 0$ and sufficiently large N, there exist encoder $\mathcal{E}$ and decoders $\{\mathcal{D}_\ell\}_{\ell=1}^K$ such that $\forall \ell \in \{1, \ldots, K\}$:

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

$$R_\ell \leq \frac{1}{N} H(W_\ell | \mathbf{y}_1, \ldots, \mathbf{y}_{\ell-1}, \mathbf{y}_{\ell+1}, \ldots, \mathbf{y}_K) + \epsilon \tag{3}$$

Inequalities (2) and (3) capture the reliability and the confidentiality constraints of message W_ℓ, respectively; the confidentiality constraint ensures weak secrecy [12]. The secrecy capacity region is the supremum over all the achievable secure rate tuples.

III. Main Results

We present our main result as a set of lower bounds on the individual secrecy rates of the confidential messages. We also present the sum secure degrees of freedom attainable by our scheme.

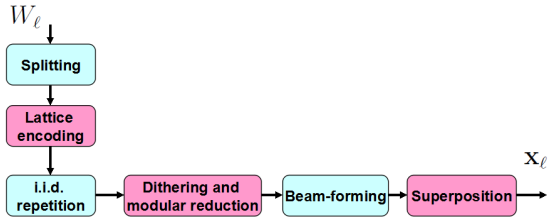

Fig. 2: The encoding steps performed by the transmitter for each confidential message.

Theorem 1: For the K-user Gaussian broadcast channel with K helpers, any non-negative secure rate tuple $(R_1, R_2, \ldots, R_K)$ satisfying the following inequalities is achievable with weak secrecy.

$$R_\ell < R_{comb,K}^{(\ell)} - \frac{1}{2} \max_{\substack{k \in \{1,\ldots,K\} \\ k \neq \ell}} \log\left(\frac{\sum_{m=1}^{M} (h_k^2 P_{m\ell} + g_{\ell k}^2 P_{m\ell}^J)}{g_{\ell k}^2 P_{m'\ell}^J} \right) \tag{4}$$

The rate $R_{comb,K}^{(\ell)}$ is defined as the optimal achievable rate at which receiver ℓ decodes the K-th linear integer combination using the compute-and-forward strategy. Also, M is the number of dimensions used in the beam-forming operation and m is the dimension index. $P_{m\ell}$ is the power allocated to encode the m-th component of the ℓ-th confidential message. $P_{m\ell}^J$ is the power used by helper ℓ to encode the m-th component of its jamming signal. Lastly, $P_{m'\ell}^J$ is the smallest power among the powers used to encode the components of the jamming signal by helper ℓ, in our design this is also smaller than $P_{m\ell}$, $\forall m$. Also, the power allocated to encode helper ℓ's jamming signal is chosen such that $g_{\ell\ell}^2 \sum_m P_{m\ell}^J < 1$.

Remark 1: The set of achievable rates in (4) for all $\ell \in \{1, \ldots, K\}$ can be optimized over the choice of power allocations in the transmitter and the helpers as long as the following conditions are satisfied:

$$g_{\ell\ell}^2 \sum_{m=1}^{M} P_{m\ell}^J < 1, \quad P_{m_1\ell}^J < P_{m_2\ell} \ \forall m_1, m_2 \in [1, M], \forall \ell \in [1, K] \tag{5}$$

$$\sum_{\ell=1}^{K} \sum_{m=1}^{M} P_{m\ell} \leq P \ , \sum_{\ell=1}^{K} \sum_{m=1}^{M} P_{m\ell}^J \leq P. \tag{6}$$

Our achievable scheme is based on rate-splitting, nested lattice coding, i.i.d. repetitions, cooperative jamming, and beam-forming. Figure 2 illustrates the block diagram of the encoding steps at the transmitter. The decoding is performed according to the asymmetric compute-and-forward strategy at the receivers. The detailed description is provided in Sec. IV.

Corollary 1: Following our scheme, at each receiver, a $\frac{1}{K}$ secure degrees of freedom is achievable for the receiver's intended message; hence, the optimal sum secure degrees of freedom of 1 is achievable, i.e.,

$$s.d.o.f. \triangleq \lim_{P \to \infty} \frac{\sum_{\ell=1}^{K} R_\ell}{\frac{1}{2} \log(1 + P)} = 1 \tag{7}$$

Corollary 1 is proven in Sec. IV.

IV. Achievability scheme

We describe our achievable scheme for $K = 3$ receivers and three helpers to better clarify the key ideas in our coding scheme. Then, we generalize our scheme to any arbitrary $K > 2$ receivers with K helpers. We begin with codebook construction at the transmitter and then we describe the codebook construction at the helpers.

A. Codebook construction

The transmitter generates a lattice vector for each independent confidential message. The lattice vectors are drawn from a set of nested lattice sets.

Consider pairs of coarse and fine lattices as $(\Lambda_\ell^m, \Lambda_{f,\ell}^m)$ for each pair $(m,\ell) \in \{1,\dots,T^4\} \times \{1,2,3\}$. Similarly, consider pairs $(\Lambda_{Ji}^m, \Lambda_{f,Ji}^m)$ for $i \in \{1,2,3\}$, and $m \in \{1,\dots,T^4\}$. The subscript f specifies the fine lattice in the pair. T is some large number; let us define $M \triangleq T^4$. Assume that these lattices are nested according to the following chain:

$$\Lambda \subseteq \Lambda_3^m \subseteq \Lambda_2^m \subseteq \Lambda_1^m \subseteq \Lambda_{3J}^m \subseteq \Lambda_{2J}^m \subseteq \Lambda_{1J}^m \subseteq \Lambda_{f,3}^m \dots$$

$$\subseteq \Lambda_{f,2}^m \subseteq \Lambda_{f,1}^m \subseteq \Lambda_{f,3J}^m \subseteq \Lambda_{f,2J}^m \subseteq \Lambda_{f,1J}^m \tag{8}$$

The above coarse lattice sets are scaled such that their second moments are equal to $\sigma_{m3}^2, \sigma_{m2}^2, \sigma_{m1}^2, \sigma_{m,3J}^2, \sigma_{m,2J}^2, \sigma_{m,1J}^2$, respectively. We denote the fundamental Voronoi region of the coarse lattice Λ_ℓ^m as $\mathcal{V}_\ell^m$; similarly, the fundamental Voronoi region of the coarse lattice Λ_{iJ}^m is denoted as $\mathcal{V}_{iJ}^m$. The centers of the cosets of the fine lattice sets $\Lambda_{f,\ell}^m$ and $\Lambda_{f,iJ}^m$ are both n-length lattice words, which are the realizations of the n-length random vector $\mathbf{t}_{m\ell}$ and $\mathbf{u}_{mi}$, respectively. The inner codebook associated with sub-message (m,ℓ) is defined as $\mathcal{L}_{m\ell} \triangleq \{\mathbf{t}_{m\ell} | \mathbf{t}_{m\ell} \in \mathcal{V}_\ell^m\}$. Also, the inner codebook $\mathcal{L}_{m,Ji}$ is similarly defined for the collection of the jamming codewords $\mathbf{u}_{mi}$ and is used by the i-th helper.

Consider a probability distribution $P(\mathbf{t}_{m\ell})$ over the codebook $\mathcal{L}_{m\ell}$. To generate the outer codebooks for sub-message (m,ℓ), the transmitter acts as follows: from codebook $\mathcal{L}_{m\ell}$ and according to distribution $P(\mathbf{t}_{m\ell})$, it draws B i.i.d. copies of codewords $\mathbf{t}_{m\ell}$ and then, it concatenates the drawn vectors. The resulting codeword which has length $N \triangleq n \times B$ is considered as one realization of the outer codeword $\bar{\mathbf{t}}_{m\ell}$. The transmitter generates $2^{NR_{comb3,m}^\ell}$ realizations of random vector $\bar{\mathbf{t}}_{m\ell}$, where $R_{comb3,m}^\ell > 0$ and $R_{comb,3}^\ell \triangleq \sum_{m=1}^M R_{comb3,m}^\ell$. The collection of the generated codewords is termed the outer codebook for sub-message (m,ℓ) and denoted as $\mathcal{C}_{m\ell}$. The outer codebook at helper i, generated in a similar manner, and denoted as $\mathcal{C}_{m,iJ}$. Note that the idea behind the i.i.d. repetitions of the inner codewords is to take advantage of the Packing lemma in the proof of weak secrecy. [2]

Next step in the codebook construction is the random partitioning. For each sub-message codebook $\mathcal{C}_{m\ell}$, the transmitter randomly partitions the outer codewords into $2^{NR_{m\ell}}$ bins of equal sizes. The transmitter chooses the non-negative rates $R_{m\ell}$ such that $R_\ell = \sum_{m=1}^M R_{m\ell}$, where

$$R_\ell \triangleq R_{comb,3}^{(\ell)} - \max_{\substack{k\in\{1,2,3\}\\ k\neq\ell}} \left(\frac{1}{2} \log \left(\frac{\sum_m (h_k^2 P_{m\ell} + g_{\ell k}^2 P_{m\ell}^J)}{g_{\ell k}^2 P_{m'\ell}^J} \right) \right) + \epsilon_\ell, \tag{9}$$

in which term ϵ_ℓ vanishes as the block length increases.
To each partition, an index $w_{m\ell} \in \{1,\dots,2^{NR_{m\ell}}\}$ is randomly assigned. Additionally, for each sub-message $w_{m\ell}$, the transmitter generates a random dither vector $\mathbf{d}_{m\ell}$ drawn from a uniform distribution over the Voronoi region $\mathcal{V}_\ell^m$. The outer dither codewords $\bar{\mathbf{d}}_{m\ell}$ are constructed as described before.

B. Encoding

The transmitter encodes the confidential message w_ℓ by dividing the message into $M = T^4$ independent sub-messages, where T is a large number. It is worth to mention that M is the number of dimensions used in beam-forming the signals. Our ultimate goal is to align codewords at the unintended receivers with the jamming signals in many dimensions. Each sub-message is denoted by indices (m,ℓ), where $m \in \{1,\dots,M\}$ and $\ell \in \{1,\dots,K\}$, and is encoded separately. To encode the sub-message $w_{m\ell}$, the transmitter picks randomly a codeword $\bar{\mathbf{t}}_{m\ell}$ from the corresponding codebook $\mathcal{C}_{m\ell}$. It then dithers the extracted codeword and reduces the sum through a modular operation over the corresponding coarse lattice, i.e.,

$$\tilde{\mathbf{x}}_{m\ell} \triangleq \left[\bar{\mathbf{t}}_{m\ell} + \bar{\mathbf{d}}_{m\ell}\right] \mod \Lambda_\ell^m \tag{10}$$

The modular operation in (10) is done block-wise for each block of length n. Next, we apply beam-forming such that each codeword $\tilde{\mathbf{x}}_{m\ell}$ scaled as $\mathbf{x}_{m\ell} \triangleq \tilde{\mathbf{x}}_{m\ell}.f(m,\ell,\mathbf{h},\mathbf{g}_1,\mathbf{g}_2,\mathbf{g}_3)$, where $\mathbf{h} \triangleq [h_1,h_2,h_3]^T$, $\mathbf{g}_i \triangleq [g_{i1},g_{i2},g_{i3}]^T$, and $f(.)$ is a mapping which takes the indices and the channel gains as inputs and outputs an scalar value. The mapping f, is chosen such that the codewords $\mathbf{x}_{m\ell}$ for all (m,ℓ) are rationally independent for all channel gain vectors, except for a small Lebesgue measure. We will expand on the mapping f shortly. The transmitter sends codeword $\mathbf{x} \triangleq \sum_{\ell=1}^K \mathbf{x}_\ell$, where $\mathbf{x}_\ell \triangleq \sum_{m=1}^M \mathbf{x}_{m\ell}$, across the channel. The power allocated to sub-codeword (m,ℓ) is defined as $P_{m\ell} \triangleq \sigma_{m\ell}^2.|f(m,\ell,\mathbf{h},\mathbf{g}_1,\mathbf{g}_2,\mathbf{g}_3)|^2$. It is worth mentioning that the lattice sets in (8) are scaled such that the power allocations $P_{m\ell}$ and $P_{m\ell}^J$ satisfy the constraints in (5-6).

Encoding at helper ℓ is performed as follows: for each $m \in \{1,\dots,M\}$, it randomly picks a jamming codeword, $\bar{\mathbf{u}}_{m\ell}$, from codebook $C_{m,\ell J}$. It then dithers the codeword and performs the modular operation using lattice $\Lambda_{\ell J}^m$ to generate $\tilde{\mathbf{x}}_{m\ell}^J$. Next, it constructs codeword $\mathbf{x}_{m\ell}^J$ as $\mathbf{x}_{m\ell}^J \triangleq \tilde{\mathbf{x}}_{m\ell}^J.f(m,\ell,\mathbf{h},\mathbf{g}_1,\mathbf{g}_2,\mathbf{g}_3)$. Eventually, helper ℓ transmits signal $\mathbf{x}_\ell^J = \sum_m \mathbf{x}_{m\ell}^J$ through the channel. We denote the power of the transmitted codeword by helper ℓ as P_ℓ^J which is defined as $P_\ell^J \triangleq \sum_{m=1}^M P_{m\ell}^J$ over index m, where $P_{m\ell}^J$ is defined similar to $P_{m\ell}$. The construction of the beam-forming function f is performed such that the desired alignments are formed. For $K = 3$ receivers, and for a given ℓ, codeword

[2] Packing Lemma is deduced by applying the joint typicality lemma on i.i.d. random sequences [13].

$\mathbf{x}_\ell$ should get aligned with jamming codeword $\mathbf{x}_\ell^J$ at receivers $k \neq \ell$. For instance, codeword $\mathbf{x}_1$ needs to be aligned with jamming codeword $\mathbf{x}_1^J$ at receivers 2 and 3. This requires that the same pairs of codewords get aligned at multiple receivers, simultaneously. To this end, we take advantage of the asymptotic alignment technique, (introduced in [14] and used in [7] for real-alignment), to align the N-dimensional lattice codewords. To do so, consider a one-to-one mapping $\phi^3 : \{1,\dots,M\} \to \{1,\dots,T\} \times \{1,\dots,T\} \times \{1,\dots,T\} \times \{1,\dots,T\}$. We design the beam-forming function, f, for the three-receiver Gaussian broadcast channel with channel gain vectors $\mathbf{h}, \mathbf{g}_1, \mathbf{g}_2, \mathbf{g}_3$ as

$$f(m,1,\mathbf{h},\mathbf{g}_1,\mathbf{g}_2,\mathbf{g}_3) = h_2^{r_1} h_3^{r_2} g_{12}^{r_3} g_{13}^{r_4} \tag{11}$$
$$f(m,2,\mathbf{h},\mathbf{g}_1,\mathbf{g}_2,\mathbf{g}_3) = h_1^{r_1} h_3^{r_2} g_{21}^{r_3} g_{23}^{r_4} \tag{12}$$
$$f(m,3,\mathbf{h},\mathbf{g}_1,\mathbf{g}_2,\mathbf{g}_3) = h_1^{r_1} h_2^{r_2} g_{31}^{r_3} g_{32}^{r_4} \tag{13}$$
$$(r_1,r_2,r_3,r_4) = \phi^3(m),\ m \in \{1,\dots,M\}. \tag{14}$$

Following the results in [14] and [7], it can be shown that for large enough values of M our beam-forming function asymptotically provides the desired alignments at the receivers simultaneously. In other words, the desired alignments between the pair of codewords happen in many dimensions which asymptotically yields perfect alignment.

C. Decoding

We describe decoding at receiver 1; other receivers act in a similar manner. Receiver 1 observes the following sequence from the channel:

$$\mathbf{y}_1 = h_1 \sum_{m=1}^{M} \mathbf{x}_{m1} + \sum_{m=1}^{M} (h_1 \mathbf{x}_{m2} + g_{21} \mathbf{x}_{m2}^J) + \sum_{m=1}^{M} (h_1 \mathbf{x}_{m3} + g_{31} \mathbf{x}_{m3}^J) + \sum_{m=1}^{M} g_{11} \mathbf{x}_{m1}^J + \mathbf{z}_1 \tag{15}$$

Due to beam-forming in (11)-(13), the sub-message codewords associated with confidential message W_2 and the jamming sub-codewords of helper 2 are aligned in the second term of (15). Similarly, the corresponding sub-codewords in the third term of the equation (15) are aligned. Moreover, according to (5), power of the fourth term in (15) falls below noise level; as it carries no useful information regarding the messages, receiver 1 treats the fourth term as noise. Consequently, receiver 1 decodes the following effective 3-user multiple-access channel in which the power of the effective noise $\tilde{\mathbf{z}}_1$ is normalized. We have

$$\tilde{\mathbf{y}}_1 = \frac{h_1}{\sqrt{g_{11}^2 P_1^J + 1}} \sum_{m=1}^{M} \mathbf{x}_{m1} + \frac{1}{\sqrt{g_{11}^2 P_1^J + 1}} \sum_{m=1}^{M} (h_1 \mathbf{x}_{m2} + g_{21} \mathbf{x}_{m2}^J) + \frac{1}{\sqrt{g_{11}^2 P_1^J + 1}} \sum_{m=1}^{M} (h_1 \mathbf{x}_{m3} + g_{31} \mathbf{x}_{m3}^J) + \tilde{\mathbf{z}}_1 \tag{16}$$

Receiver 1 decodes three effective lattice codewords, i.e., $\mathbf{x}_{eff,1} \triangleq \sum_{m=1}^{M} \mathbf{x}_{m1}$, $\mathbf{x}_{eff,2} \triangleq \sum_{m=1}^{M} (h_1 \mathbf{x}_{m2} + g_{21} \mathbf{x}_{m2}^J)$, and $\mathbf{x}_{eff,3} \triangleq \sum_{m=1}^{M} (h_1 \mathbf{x}_{m3} + g_{31} \mathbf{x}_{m3}^J)$. In other words, the effective channel vector $\mathbf{h}_{eff,1}$ at receiver 1 is defined as $\mathbf{h}_{eff,1} \triangleq \left[\frac{h_1}{\sqrt{g_{11}^2 P_1^J + 1}}, \frac{1}{\sqrt{g_{11}^2 P_1^J + 1}}, \frac{1}{\sqrt{g_{11}^2 P_1^J + 1}} \right]^T$, and subsequently, the power scaling factor which determines the ratios of the power of effective codewords with respect to the power constraint is $\mathbf{b}_{eff,1} \triangleq \left[\sqrt{\frac{P_1}{P}}, \sqrt{\frac{h_1^2 P_2 + g_{21}^2 P_2^J}{P}}, \sqrt{\frac{h_1^2 P_3 + g_{31}^2 P_3^J}{P}} \right]^T$. According to the asymmetric compute-and-forward technique and Theorem 7 in [11], receiver 1 finds the optimal set of linearly independent integer-valued coefficient vectors, which maximizes the achievable sum rate, to construct the integer combinations and then it decodes the integer combinations successively. We denote these vectors as $\mathbf{a}_1$, $\mathbf{a}_2$, and $\mathbf{a}_3$. Upon decoding the first integer combination, the codeword belonging to the densest lattice inner codebook is decoded. Let us denote the first integer combination by vector $\mathbf{v}_1 \triangleq \sum_{\ell=1}^{3} \mathbf{a}_1(\ell) \mathbf{x}_{eff,\ell}$. Receiver 1 decodes $\mathbf{v}_1$ as follows:

$$\left[\mathbf{s}_1 \triangleq \beta_1 \tilde{\mathbf{y}}_1 - \sum_{\ell=1}^{3} \mathbf{a}_1(\ell) \bar{\mathbf{d}}_\ell \right] \bmod \Lambda = [\mathbf{v}_1 + \mathbf{z}_{eff,1}] \bmod \Lambda, \tag{17}$$

in which the effective noise of the first integer combination is defined as $\mathbf{z}_{eff,1} \triangleq \sum_{\ell=1}^{3} (\beta_1 \mathbf{h}_{eff,1}(\ell) - \mathbf{a}_1(\ell)) \mathbf{x}_{eff,\ell} + \beta_1 \tilde{\mathbf{z}}_1$. To decode the integer combination $\mathbf{v}_1$, receiver 1 computes the quantization value of $\mathbf{s}_1$ under the densest lattice among the lattice sets used for encoding $\{\mathbf{x}_{eff,\ell}\}_{\ell=1}^3$. Let us denote the index of the corresponding effective codeword with k. Then, according to Theorem 2 in [11] we have: $R_{comb,1}^1 \triangleq \frac{1}{2} \log(\frac{P_{eff,k}}{\sigma_{eff,1}^2})$. $R_{comb,1}^1$ is the optimal achievable rate at which the first integer combination is decoded at receiver 1. Similarly, we can define $R_{comb,2}^1$ and $R_{comb,3}^1$ as the optimal rates of decoding the second and the third integer combinations at receiver 1, respectively. $P_{eff,k}$ is the power of the k-th effective codeword and $\sigma_{eff,1}^2$ is the variance of the effective noise associated with the first integer combination, i.e., $\mathbf{z}_{eff,1}$. Receiver 1 proceeds with decoding the next integer combinations of the effective codewords. However, to maximize the achievable rates, receiver 1 first cancels out the contribution of the previously decoded codewords from the current combination and then the codeword with the highest rate among the remaining codewords in the integer combination gets decoded. Assume that the effective codewords are decoded in the order specified by $\pi^{-1}(1), \pi^{-1}(2), \pi^{-1}(3)$, where $\pi(.)$ is a one-to-one permutation operator over the set $\{1,2,3\}$. Then, following Theorem 2 in [11], the k-th optimal achievable combination rate is given as $R_{comb,k}^1 \triangleq \frac{1}{2} \log\left(\frac{P_{eff,\pi^{-1}(k)}}{\sigma_{eff,k}^2}\right)$, where $\sigma_{eff,k}^2$ is the variance of the effective noise in k-th integer combination. Note that upon decoding each combination, the effective codeword which was constructed using the densest lattice (highest rate) among the participating codewords in the combination is decoded. Therefore, the order among the variances of the effective noises is given as $\sigma_{eff,1}^2 \leq \sigma_{eff,2}^2 \leq \sigma_{eff,3}^2$. Note that the goal is to obtain a lower-bound on the achievable rate of $\mathbf{x}_{eff,1}$. According to the definition of $R_{comb,k}^1$ and the order among the variances, $R_{eff,1} \geq R_{comb,3}^1$. Therefore, receiver 1 can reliably decode its intended codeword so long as it is

generated at a rate $R_{eff,1} \leq \frac{1}{2}\log(\frac{P_1}{\sigma^2_{eff,3}})$. Note that, given the optimal integer-valued coefficient vectors, i.e., $\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3$, the variance $\sigma^2_{eff,3}$ is a function of β_3. It can be shown that the optimal choice for β_3 which minimizes $\sigma^2_{eff,3}$ is the MSE factor [11], i.e, $\beta_3 = \frac{\mathbb{E}\left[\left(\sum_{\ell=1}^{3}\mathbf{a}_3(\ell)\mathbf{x}_{eff,\ell}\right)\tilde{\mathbf{y}}_1\right]}{\mathbb{E}\left[\tilde{\mathbf{y}}_1^2\right]}$. The integer-valued coefficients can be computed using the LLL reduction algorithm in [15] which provides a polynomial-time solution and computes a nearly optimal set of integer-valued coefficient vectors. [3] The proof of reliability at other receivers can be done similarly. So far, we showed that for a confidential message ℓ, any non-negative rate below $R^{\ell}_{comb,3}$ can be decoded reliably at receiver ℓ which ensures the reliability of the rates in Theorem 1. Next section is devoted to the analysis of security.

D. Security analysis

In this section, we show that our achievable scheme provides weak secrecy for all messages at the unintended receivers, i.e.,

$$\frac{1}{nB}I(W_1,...,W_{\ell-1},W_{\ell+1},...,W_K;\mathbf{y}_\ell)\leq\epsilon,\ \forall\ell\in\{1,...,K\} \qquad (18)$$

in which $\epsilon > 0$ tends to zero as n and B approach infinity. For simplicity, we shall prove (18) for $K = 3$ receivers; the extension of the proof to an arbitrary $K > 2$ is straightforward. We proceed the proof by showing the weak secrecy of the joint messages (W_2, W_3) at receiver 1, i.e., $\frac{1}{nB}I(W_2, W_3; \mathbf{y}_1) \leq \epsilon$. We have $\frac{1}{nB}I(W_2, W_3; \mathbf{y}_1) \leq \frac{1}{nB}I(W_2, W_3; \mathbf{y}_1, \bar{\mathbf{t}}_1)$, therefore,

$$\frac{1}{nB}I(W_2, W_3; \mathbf{y}_1) \leq \sum_{\ell=2}^{3} R_\ell - \frac{1}{nB}H(W_2, W_3|\mathbf{y}_1, \bar{\mathbf{t}}_1), \qquad (19)$$

in which $\bar{\mathbf{t}}_\ell \triangleq (\bar{\mathbf{t}}_{1\ell}, \ldots, \bar{\mathbf{t}}_{m\ell}, \ldots, \bar{\mathbf{t}}_{M\ell})$. We proceed by lower bounding the second term in (19):

$$\begin{aligned}
&\frac{1}{nB}H(W_2,W_3|\mathbf{y}_1,\bar{\mathbf{t}}_1)=\frac{1}{nB}H(W_2,W_3,\bar{\mathbf{t}}_2,\bar{\mathbf{t}}_3|\mathbf{y}_1,\bar{\mathbf{t}}_1)\\
&-\frac{1}{nB}H(\bar{\mathbf{t}}_2,\bar{\mathbf{t}}_3|\mathbf{y}_1,\bar{\mathbf{t}}_1,W_2,W_3)\\
&\geq \frac{1}{nB}H(\bar{\mathbf{t}}_2,\bar{\mathbf{t}}_3|\mathbf{y}_1,\bar{\mathbf{t}}_1) - \frac{1}{nB}H(\bar{\mathbf{t}}_2,\bar{\mathbf{t}}_3|\mathbf{y}_1,\bar{\mathbf{t}}_1,W_2,W_3)\\
&\overset{(a)}{\geq} \frac{1}{nB}H(\bar{\mathbf{t}}_2,\bar{\mathbf{t}}_3|\mathbf{y}_1,\bar{\mathbf{t}}_1) - 2\epsilon_{23}\\
&\overset{(b)}{\geq} \frac{1}{nB}H(\bar{\mathbf{t}}_2,\bar{\mathbf{t}}_3|\mathbf{y}_1,\bar{\mathbf{t}}_1,D,\mathbf{z}_1) - 2\epsilon_{23}\\
&\overset{(c)}{=}\frac{1}{nB}H\Bigg(\bar{\mathbf{t}}_2,\bar{\mathbf{t}}_3\Big|\sum_{m=1}^{M}(h_1\mathbf{x}_{m2}+g_{21}\mathbf{x}^J_{m2}),\sum_{m=1}^{M}(h_1\mathbf{x}_{m3}+g_{31}\mathbf{x}^J_{m3}),\bar{\mathbf{t}}_1,D,\mathbf{z}_1\Bigg)-2\epsilon_{23}\\
&\overset{(d)}{=}\frac{1}{nB}H\Bigg(\bar{\mathbf{t}}_2,\bar{\mathbf{t}}_3\Big|\sum_{m=1}^{M}(h_1f_{m2}\bar{\mathbf{t}}_{m2}+g_{21}f_{m2}\bar{\mathbf{u}}_{m2}),\\
&\sum_{m=1}^{M}(h_1f_{m3}\bar{\mathbf{t}}_{m3}+g_{31}f_{m3}\bar{\mathbf{u}}_{m3}),\bar{\mathbf{t}}_1,D,\mathbf{z}_1\Bigg)-2\epsilon_{23}\\
&\overset{(e)}{=}\frac{1}{nB}H\Bigg(\bar{\mathbf{t}}_2,\bar{\mathbf{t}}_3\Big|\sum_{m=1}^{M}(\tilde{\mathbf{t}}_{m2}+\tilde{\mathbf{u}}_{m2}),\sum_{m=1}^{M}(\tilde{\mathbf{t}}_{m3}+\tilde{\mathbf{u}}_{m3}),\bar{\mathbf{t}}_1,D,\mathbf{z}_1\Bigg)-2\epsilon_{23} \qquad (20)
\end{aligned}$$

In the above arguments, inequality (a) holds due to Lemma 1 in [6]. Inequality (b) is true since conditioning reduces entropy. Equality (c) is deduced from expression (15) and definition of $\mathbf{x}_{m\ell}$. Equality (d) is deduced from (10) and after subtracting dithers. Also, equality (e) comes from defining the lattice vectors $h_1 f_{m2}\bar{\mathbf{t}}_{m2}$, $g_{21}f_{m2}\bar{\mathbf{u}}_{m2}$, $h_1 f_{m3}\bar{\mathbf{t}}_{m3}$, and $g_{31}f_{m3}\bar{\mathbf{u}}_{m3}$ as lattice vectors $\tilde{\mathbf{t}}_{m2}$, $\tilde{\mathbf{u}}_{m2}$, $\tilde{\mathbf{t}}_{m3}$, and $\tilde{\mathbf{u}}_{m3}$, respectively.

Now, assume that among the nested coarse lattices $\{\Lambda_{m2}\}_{m=1}^{M}$ and $\{\Lambda^J_{m2}\}_{m=1}^{M}$, lattice $\Lambda^J_{m'2}$ is the densest lattice for some $m' \in \{1,\ldots,M\}$ and similarly, assume among the nested coarse lattices $\{\Lambda_{m2}\}_{m=1}^{M}$ and $\{\Lambda^J_{m3}\}_{m=1}^{M}$, lattice $\Lambda^J_{m''3}$ is the densest lattice for some $m'' \in \{1,\ldots,M\}$. Then, following the expression in (20), we have:

$$\begin{aligned}
&\frac{1}{nB}H(W_2,W_3|\mathbf{y}_1,\bar{\mathbf{t}}_1)\geq\frac{1}{nB}H\Bigg(\bar{\mathbf{t}}_2,\bar{\mathbf{t}}_3\Big|\Big[\sum_{m=1}^{M}(\tilde{\mathbf{t}}_{m2}+\tilde{\mathbf{u}}_{m2})\Big]\ \mathrm{mod}\Lambda^J_{m'2},\\
&Q_{\Lambda^J_{m'2}}(\sum_{m=1}^{M}(\tilde{\mathbf{t}}_{m2}+\tilde{\mathbf{u}}_{m2})),\Big[\sum_{m=1}^{M}(\tilde{\mathbf{t}}_{m3}+\tilde{\mathbf{u}}_{m3})\Big]\ \mathrm{mod}\Lambda^J_{m''3},\\
&Q_{\Lambda^J_{m''3}}(\sum_{m=1}^{M}(\tilde{\mathbf{t}}_{m3}+\tilde{\mathbf{u}}_{m3})),\bar{\mathbf{t}}_1,D,\mathbf{z}_1\Bigg)-2\epsilon_{23}\\
&\geq\frac{1}{nB}H\Bigg(\bar{\mathbf{t}}_2,\bar{\mathbf{t}}_3\Big|\Big[\sum_{m=1}^{M}(\tilde{\mathbf{t}}_{m2}+\tilde{\mathbf{u}}_{m2})\Big]\ \mathrm{mod}\Lambda^J_{m'2},\Big[\sum_{m=1}^{M}(\tilde{\mathbf{t}}_{m3}+\tilde{\mathbf{u}}_{m3})\Big]\ \mathrm{mod}\Lambda^J_{m''3}\Bigg)\\
&-\frac{1}{nB}H\Bigg(Q_{\Lambda^J_{m'2}}(\sum_{m=1}^{M}(\tilde{\mathbf{t}}_{m2}+\tilde{\mathbf{u}}_{m2})),\\
&Q_{\Lambda^J_{m''3}}(\sum_{m=1}^{M}(\tilde{\mathbf{t}}_{m3}+\tilde{\mathbf{u}}_{m3}))\Big|\bar{\mathbf{t}}_1,D,\mathbf{z}_1\Bigg)-2\epsilon_{23}\\
&\overset{(f)}{\geq}\frac{1}{nB}H\Bigg(\bar{\mathbf{t}}_2,\bar{\mathbf{t}}_3\Big|\Big[\sum_{m=1}^{M}(\tilde{\mathbf{t}}_{m2}+\tilde{\mathbf{u}}_{m2})\Big]\ \mathrm{mod}\Lambda^J_{m'2},\\
&\Big[\sum_{m=1}^{M}(\tilde{\mathbf{t}}_{m3}+\tilde{\mathbf{u}}_{m3})\Big]\ \mathrm{mod}\Lambda^J_{m''3}\Bigg)-2\epsilon_{23}\\
&-\frac{1}{nB}H\Bigg(Q_{\Lambda^J_{m'2}}(\sum_{m=1}^{M}(\tilde{\mathbf{t}}_{m2}+\tilde{\mathbf{u}}_{m2})),Q_{\Lambda^J_{m''3}}(\sum_{m=1}^{M}(\tilde{\mathbf{t}}_{m3}+\tilde{\mathbf{u}}_{m3}))\Bigg)\\
&\geq\frac{1}{nB}H\Bigg(\bar{\mathbf{t}}_2,\bar{\mathbf{t}}_3\Big|\Big[\sum_{m=1}^{M}(\tilde{\mathbf{t}}_{m2}+\tilde{\mathbf{u}}_{m2})\Big]\ \mathrm{mod}\Lambda^J_{m'2},\Big[\sum_{m=1}^{M}(\tilde{\mathbf{t}}_{m3}+\tilde{\mathbf{u}}_{m3})\Big]\ \mathrm{mod}\Lambda^J_{m''3}\Bigg)\\
&-\frac{1}{nB}H\Bigg(Q_{\Lambda^J_{m'2}}(\sum_{m=1}^{M}(\tilde{\mathbf{t}}_{m2}+\tilde{\mathbf{u}}_{m2}))\Bigg)-2\epsilon_{23}-\frac{1}{nB}H\Bigg(Q_{\Lambda^J_{m''3}}(\sum_{m=1}^{M}(\tilde{\mathbf{t}}_{m3}+\tilde{\mathbf{u}}_{m3}))\Bigg)\\
&\overset{(g)}{\geq}\frac{1}{nB}H\Bigg(\bar{\mathbf{t}}_2,\bar{\mathbf{t}}_3\Big|\Big[\sum_{m=1}^{M}(\tilde{\mathbf{t}}_{m2}+\tilde{\mathbf{u}}_{m2})\Big]\ \mathrm{mod}\Lambda^J_{m'2},\\
&\Big[\sum_{m=1}^{M}(\tilde{\mathbf{t}}_{m3}+\tilde{\mathbf{u}}_{m3})\Big]\ \mathrm{mod}\Lambda^J_{m''3}\Bigg)-\frac{1}{2}\log\Bigg(\frac{\sum_m(h_1^2P_{m2}+g_{21}^2P^J_{m2})}{g_{21}^2P^J_{m'2}}\Bigg)\\
&-\frac{1}{2}\log\Bigg(\frac{\sum_m(h_1^2P_{m3}+g_{31}^2P^J_{m3})}{g_{31}^2P^J_{m''3}}\Bigg)-\delta(\epsilon_2)-\delta(\epsilon_3)-2\epsilon_{23}\\
&\overset{(h)}{=}\frac{1}{nB}H(\bar{\mathbf{t}}_2,\bar{\mathbf{t}}_3)-\frac{1}{2}\log\Bigg(\frac{\sum_m(h_1^2P_{m2}+g_{21}^2P^J_{m2})}{g_{21}^2P^J_{m'2}}\Bigg)\\
&-\frac{1}{2}\log\Bigg(\frac{\sum_m(h_1^2P_{m3}+g_{31}^2P^J_{m3})}{g_{31}^2P^J_{m''3}}\Bigg)-\delta(\epsilon_2)-\delta(\epsilon_3)-2\epsilon_{23}\\
&\overset{(k)}{=}R^{(2)}_{comb,3}+R^{(3)}_{comb,3}-\frac{1}{2}\log\Bigg(\frac{\sum_m(h_1^2P_{m2}+g_{21}^2P^J_{m2})}{g_{21}^2P^J_{m'2}}\Bigg)\\
&-\frac{1}{2}\log\Bigg(\frac{\sum_m(h_1^2P_{m3}+g_{31}^2P^J_{m3})}{g_{31}^2P^J_{m''3}}\Bigg)-\delta(\epsilon_2)-\delta(\epsilon_3)-2\epsilon_{23} \qquad (21)
\end{aligned}$$

In the above inequalities, inequality (f) holds since conditioning reduces entropy. Inequality (g) is deduced by applying Lemma 1 in [16] to lattice codewords $\sum_{m=1}^{M}(\tilde{\mathbf{t}}_{m2} + \tilde{\mathbf{u}}_{m2}))$ and $\sum_{m=1}^{M}(\tilde{\mathbf{t}}_{m3} + \tilde{\mathbf{u}}_{m3}))$. Equality (h) is deduced from Crypto Lemma in [17] and the fact that the lattice sets used for encoding the jamming signals were chosen such that it would be denser than the lattice sets used for encoding the message signals. Finally, equality (k) is resulted from the independence of codewords $\bar{\mathbf{t}}_2$ and $\bar{\mathbf{t}}_3$ and the rates at which they were generated according to the achievable scheme

[3] Due to space limitation, we will include numerical results in the extended version of this paper.

in Section IV. Next, we plug the lower bound in (21) to the second term in (19). Then, following (9) we obtain: $\frac{1}{nB}I(W_2,W_3;\mathbf{y}_1)\leq \delta(\epsilon_2)+\delta(\epsilon_3)+2\epsilon_{23}+\epsilon_2+\epsilon_3$. Now, define $\epsilon' \triangleq \delta(\epsilon_2)+\delta(\epsilon_3)+2\epsilon_{23}+\epsilon_2+\epsilon_3$, which tends to zero as n and B approach infinity. Thus, the analysis of weak secrecy for the joint messages (W_2,W_3) at receiver 1 is completed. Proofs of weak secrecy for the unintended message pairs at receiver 2 and receiver 3 are established similarly. ■

Extension to an arbitrary $K>2$

For the general case of $K>2$, the codebook construction is performed similar to $K=3$ case. However, in this case, each message is divided into $M \triangleq T^{2K-2}$ independent sub-messages where T is some large number. Also, secure rates R_ℓ for $\ell \in \{1,\dots,K\}$ are chosen as $R_\ell = R^{(\ell)}_{comb,K} - \frac{1}{2}\max_{\substack{k\in\{1,\dots,K\}\\ k\neq\ell}}\left(\log\left(\frac{\sum_{m=1}^{M}(h_k^2P_{m\ell}+g_{\ell k}^2P^J_{m\ell})}{g_{\ell k}^2P^J_{m'\ell}}\right)\right)+\epsilon_\ell$, where $\epsilon_\ell>0$ is a small number that vanishes as $N\to\infty$.

Also, the encoding step is performed similar to $K=3$ case. The beam-forming functions used at the transmitter and at helpers are extended as in the following:

$$f(m,\ell,\mathbf{h},\mathbf{g}_1,\mathbf{g}_2,...,\mathbf{g}_K)=h_1^{r_1}h_2^{r_2}...h_{\ell-1}^{r_{\ell-1}}h_{\ell+1}^{r_\ell}...h_K^{r_{K-1}} \times g_{\ell 1}^{r_K}g_{\ell 2}^{r_{K+1}}...g_{\ell\ell-1}^{r_{K+\ell-2}}g_{\ell\ell+1}^{r_{K+\ell-1}}...g_{\ell K}^{r_{2K-2}}, \quad (22)$$

where $(r_1,r_2,\dots,r_{2K-2})=\phi^K(m)$, in which $\phi^K(.)$ is a one-to-one mapping from the set $\{1,\dots,M\}$ to set of tuples with $2K-2$ elements, i.e., $(r_1,r_2,\dots,r_{2K-2})$, whose elements take values from the set $\{1,\dots,T\}$. Also, in (22), vector $\mathbf{g}_\ell$ is defined as $\mathbf{g}_\ell \triangleq [g_{\ell 1},g_{\ell 2},\dots,g_{\ell K}]^T$. Decoding at each receiver is performed using the asymmetric compute-and-forward framework as in the case of $K=3$; the difference here is that each receiver decodes an effective K-user MAC to estimate its intended messages. Also, the the weak secrecy proof is a straightforward extension of $K=3$ case.

Proof of Corollary 1:

The soundness of Corollary 1 is proven in two steps: step 1 is to show that the second term in (4) is constant with respect to power constraint P. Note that $P_{m\ell}$ and $P^J_{m\ell}$ are portions of powers allocated for transmitting the ℓ-th confidential message by the transmitter and the jamming signal by helper ℓ, respectively. Note that the power allocation must be performed in such a way that it satisfies power constraints in (5-6). Hence, we have $P_{m\ell}=\alpha_{m\ell}P$ and $P_{m\ell}=\alpha^J_{m\ell}P$, for some constants $0<\alpha_{m\ell},\alpha^J_{m\ell}<1$. As a result, the second term in (4) can be rewritten as $\frac{1}{2}\max_k\left(\log\left(\frac{P(\sum_m h_k^2\alpha_{m\ell}+g_{\ell k}^2\alpha^J_{m\ell})}{Pg_{\ell k}^2\alpha^J_{m^*\ell}}\right)\right)$. Notice that the factor P would be canceled out from the top and bottom of the fraction and the rest is a constant with respect to power P. In step 2, we show that the first term in (4) provides $\frac{1}{K}$ degrees of freedom. Hence, total secure degrees of freedom provided by all confidential messages is $\sum_{\ell=1}^{K}\frac{1}{K}=1$. Note that in (4), $R^{(\ell)}_{comb,K}$ is the smallest combination rate among the optimal set of K combination rates for the effective K-user MAC that receiver ℓ perceives. It was shown in Corollary 5 in [11] that for almost every channel gain vector, the degrees of freedom provided by each of the K optimal combination rates is $\frac{1}{K}$. Thus, $R^{(\ell)}_{comb,K}$ provides $\frac{1}{K}$ degrees of freedom as well and this holds for all $\ell\in\{1,\dots,K\}$. As a result, total secure degrees of freedom provided in our achievable scheme is equal to 1, this is indeed optimal. Note that for a Gaussian broadcast channel with confidential messages $s.d.o.f.\leq 1$, since the optimal degrees of freedom for a Gaussian broadcast channel without security constraints is 1 which serves as an upper bound in our security scenario [5].

V. Conclusion

We investigated transmitting confidential messages through the Gaussian broadcast channel with $K>2$ receivers and K helpers. We offered an achievable scheme which achieves secure rates that operate within a constant gap from sum secure capacity.

References

[1] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[2] J. Xie and S. Ulukus, "Secure degrees of freedom of the gaussian multiple access wiretap channel," in *Proceedings of the International Symposium on Information Theory Proceedings (ISIT 2013)*, pp. 1337–1341, IEEE, 2013.

[3] X. He and A. Yener, "Providing secrecy with structured codes: Two-user gaussian channels," *IEEE Transactions on Information Theory*, vol. 60, no. 4, pp. 2121–2138, 2014.

[4] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "On the secure degrees-of-freedom of the multiple-access-channel," available online http://arxiv.org/abs/1003.0729.

[5] 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.

[6] 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.

[7] 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.

[8] X. He and A. Yener, "Secure degrees of freedom for gaussian channels with interference: Structured codes outperform gaussian signaling," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, pp. 1–6, IEEE, 2009.

[9] 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.

[10] P. Babaheidarian, S. Salimi, and P. Papadimitratos, "Security in the gaussian interference channel: Weak and moderately weak interference regimes," in *Proceedings of the International Symposium on Information Theory Proceedings (ISIT 2016)*, pp. 2434–2438, 2016.

[11] 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.

[12] 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.

[13] A. El Gamal and Y.-H. Kim, *Network information theory*. Cambridge University Press, 2011.

[14] 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.

[15] A. Lenstra, H. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Math. Ann.*, vol. 261, pp. 515–534, 1982.

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

[17] 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.