Scalable Security in Interference Channels With Arbitrary Number of Users

Parisa Babaheidarian
Qualcomm Technologies
pbabahei@qti.qualcomm.com

Somayeh Salimi
Cygate AB
somayeh.salimi@cygate.se

Panos Papadimitratos
KTH Royal Institute of Technology
papadim@kth.se

***Abstract*—In this paper, we present an achievable security scheme for an interference channel with arbitrary number of users. In this model, each receiver should be able to decode its intended message while it should remain ignorant regarding messages intended for other receivers. Our scheme relies on transmitters to collectively ensure the confidentiality of the transmitted messages using a cooperative jamming technique and lattice alignment. The Asymmetric compute-and-forward framework is used to perform the decoding operation. The proposed scheme is the first asymptotically optimal achievable scheme for this security scenario which scales to arbitrary number of users and works for any finite-valued SNR. Also, our scheme achieves the upper bound sum secure degrees of freedom of 1 without using external helpers and thus the achievable rates lie within constant gap from sum secure capacity.**

I. Introduction

Wireless communication channels are susceptible to leakage and interception by illegitimate users. Oftentimes, cryptographic algorithms such as the public key systems (PKI) are used to provide confidentiality. Many of such techniques rely on trapdoor functions whose security are questioned by advances in quantum computers and artificial intelligence. On the other hand, the information theoretic tools such as i.i.d. random codes [1], [2], promise unconditional security. These techniques have been vastly studied in different communication models including interference channels [3]. In the last decade, studies showed that despite promising performance of random codes in achieving reliable transmission, these codes perform poorly in security scenarios specially in high SNR regime. In [4], [5] it was shown that the i.i.d. Gaussian random codes achieve *zero* sum secure degrees of freedom as SNR approaches infinity. To combat this limitation, structured codes have been incorporated in several security scenarios in which they outperformed i.i.d. Gaussian random codes [4], [6], [7]. In [8], Babaheidarian et al., presented an achievable scheme using structured lattice codes which was shown to provide weak secrecy (defined in [9]) in a two-user interference channel with weak or moderately weak interference power levels. The advantage of their scheme compared to prior research on real alignment [4] is that the scheme in [8] maintains security at any finite SNR value and the secure rates linearly scale with $\log(\mathrm{SNR})$. Furthermore, they showed their scheme is asymptotically optimal. However, the scheme in [8] assumed only a two-user scenario and the direct generalization to arbitrary number of users is not straightforward.

In this work, we present a new achievable secure scheme for an interference channel with arbitrary number of users with $K > 2$ users in which interference level is within weak or moderately weak regimes. Inspired by [8], [10], [11], our scheme utilizes the compute-and-forward decoding framework to handle finite SNR values as opposed to real-alignment schemes in [5], [7] which applied a maximum likelihood decoder. Our scheme takes advantage of a two-layer codebook structure in which the inner layer uses a set of nested lattice codebooks and the outer layer uses i.i.d. repeated codes. The novelty of our scheme is that the proposed scheme scales to any number of users ($K > 2$) and works at any finite SNR value. Also, we show that our scheme achieves optimal sum secure degrees of freedom of 1 asymptotically. Thus, our achievable sum secure rate is within constant gap from sum secure capacity in finite SNR regime. It is worth to mention that unlike prior schemes in [4] and [12], in our scheme, transmitters collectively ensure confidentiality of their messages at every unintended receiver without using an external helper.

The rest of the paper is organized as follows: Section II states the problem formulation, Section III presents our achievability results, Section IV provides proof of achievability and finally concluding remarks are made in Section V.

II. Problem Statement

In this paper, we focus on the problem of simultaneous transmission of confidential messages to their intended receivers in a K- user (transmitter-receiver pair) interference channel where K is an arbitrary *even* number and $K > 2$. For the case with odd number of users, one dummy user is added [1]. At Receiver i ($1 \leq i \leq K$), the channel output is denoted as $\mathbf{Y}_i$ and at Transmitter j the input to the channel is denoted as $\mathbf{X}_j$. The channel gain between Transmitter j and Receiver i is denoted as h_{ji}, and lastly, noise $\mathbf{z}_i$ at Receiver i is modeled by an i.i.d. random Gaussian vector with zero mean and identity covariance matrix. The relation between input and output of the channel is defined as

$$\mathbf{Y}_i = h_{ii}\mathbf{X}_i + \sum_{j \neq i} h_{ji}\mathbf{X}_j + \mathbf{z}_i \quad \forall i \in \{1, \ldots, K\} \tag{1}$$

Our assumption is that the channel gains are real valued and

[1] Note that this condition does not reduce the total degrees of freedom since the dummy user can also transmit secure data.

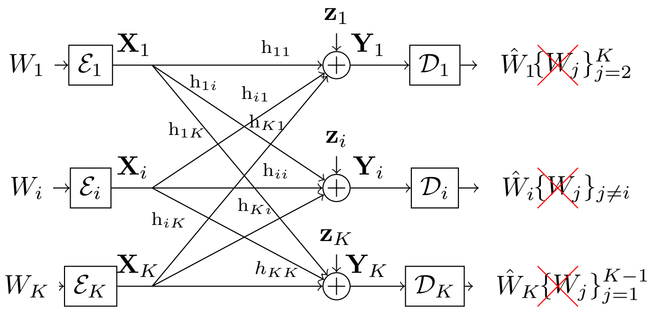

Fig. 1: The K-user Gaussian interference channel model with confidential messages.

known by the transmitters. Fig. 1 illustrates the communication model. We assume that the transmitted and received codewords, i.e., $\mathbf{X}_j$ and $\mathbf{Y}_i$ are of length N, for all $i,j \in \{1,\dots,K\}$. Transmitter j has an independent confidential message for receiver j which is denoted as W_j and is uniformly distributed over the set $\{1,2,\dots,2^{NR_j}\}$. Transmitter j encodes its message to codeword $\mathbf{X}_j$ through a stochastic encoder $\mathcal{E}_j$ subject to a power constraint $\|\mathbf{X}_j\|_2^2 \leq NP$, where P is a positive number. Also, Receiver i is equipped with decoder D_i which maps codeword $\mathbf{Y}_i$ to an estimate of its message: $\hat{W}_i = D_i(\mathbf{Y}_i)$.

Definition 1 (Achievable secure rates): For a K-user Gaussian interference channel with independent confidential messages, a non-negative secure-rate tuple $(R_1, R_2, \dots, R_K)$ is achievable with weak secrecy, if for any $\epsilon > 0$ and sufficiently large N, there exist encoders $\{\mathcal{E}_j\}_{j=1}^K$ and decoders $\{D_i\}_{i=1}^K$ such that $\forall i,j \in \{1,2,\dots,K\}$:

$$\mathrm{Prob}\left(D_i(\mathbf{Y}_i) \neq W_i\right) < \epsilon, \tag{2}$$

$$R_j \leq \frac{1}{N} H(W_j|\mathbf{Y}_1,\dots,\mathbf{Y}_{j-1},\mathbf{Y}_{j+1},\dots,\mathbf{Y}_K) + \epsilon \tag{3}$$

III. Main Results

In this section, we present the achievable secure rates for the interference channel model defined in Section II. We define a few notations to present the secure rates in a closed form. Assume R^ℓ_{comb} is an achievable rate at which confidential message W_ℓ can be reliably decoded at Receiver ℓ without any security constraint. Also, assume $P_{\ell,m} \geq 0$ is the power allocated by Transmitter ℓ to encode the m-th component of confidential message W_ℓ where total number of components is set to a positive integer M. Assume m^* is the index of the component associated with the densest lattice codebook. Additionally, the power allocated by Transmitter ℓ to encode the m-th component of the jamming codeword is denoted by $P^J_{\ell,m}$. Also, assume set $S_M \subset \{1,2,\dots,M\}$ where $\frac{|S_M|}{M} \to 1$ for large enough M. Then, we have

Theorem 1 (Achievable secure rates): A non-negative rate tuple $(R_1, R_2, \dots, R_K)$ which satisfies the following inequality for all $\ell \in \{1,\dots,K\}$, is achievable with weak secrecy for the defined interference channel model:

$$R_\ell < R^\ell_{comb} - \max_{\substack{i\\ i\neq\ell}} \left[\log\left(\sum_{\substack{m\in S_M\\ \frac{|S_M|}{M}\to 1}}^{M} \frac{h^2_{\ell,i}P_{\ell,m} + h^2_{K-\ell+1,i}P^J_{K-\ell+1,m}}{h^2_{K-\ell+1,i}P^J_{K-\ell+1,m^*}}\right)\right] \tag{4}$$

Note that the supremum of all such rates over power allocations $P_{\ell,m}$ and $P^J_{\ell,m}$, for all (ℓ,m), are also achievable so long as the power the power constraints given in Section IV are satisfied. Our achievable scheme utilizes nested lattice codebooks and random i.i.d. repetitions to generate two-layered lattice codewords. Transmitters apply beam-forming operation on message codewords as well as jamming codewords to ensure the security of the confidential messages at every unintended receiver. Note that despite the cooperative jamming scheme, no online communication among the transmitters is required.

Corollary 1: Following our scheme, the optimal sum secure degrees of freedom (s.s.d.f.) of 1 is achievable for an interference channel featuring *weak or moderately weak interference power level* with arbitrary $K > 2$ users, i.e.,

$$s.s.d.f = \frac{\sum_{\ell=1}^K R_\ell}{\frac{1}{2}\log(1+P)} \leq 1 \tag{5}$$

Proof of Corollary 1 is presented in Subsection IV-E of the extended version in [13].

IV. Achievability Scheme

We prove the achievability result presented in Theorem 1 by describing the codebook construction followed by the encoding and decoding operations. Due to space limitation, proof of weak secrecy is provided in Subsection IV-D of the extended version in [13].

A. Codebook construction

Our codebook and encoding process is based on the idea of passive cooperation among the transmitters. The passive cooperation happens when each transmitter is a sender of its own message but also acts as a helper to protect the confidentiality of another user's message at the illegitimate receivers. For instance, in the K-user setting, Transmitter 1 helps protecting Transmitter K's message at every receiver except receiver K, and Transmitter 2 does the same job for Transmitter $K-1$ and so forth. The reason we call this cooperation passive is that it does not require transmitters to exchange online messages so long as they know the channel state and the index of the transmitter they need to help which can be agreed on in the initial acquisition and prior to the connected mode. Broadly speaking, Transmitter i protects its confidential message with the help of Transmitter $K-i+1$ which generates a random jamming codeword that is beam-formed to align with the components of the i-th message codeword at every receiver, except Receiver i, simultaneously.

Since the same pair of codewords needs to be simultaneously aligned at multiple receivers with different channel gains, perfect alignment between the two codewords is not possible. However, partial alignment across multiple components can still happen. It can be shown that if the messages are encoded across sufficiently large number of independent components, partial alignment approaches perfect alignment, asymptotically [14]. Hence, the confidential messages and the jamming signals are split into M independent components where M is a large number. Each component is encoded separately and the superposition of all components are transmitted over the channel. The codebooks used for encoding confidential messages and the jamming signals form a nested lattice structure in which the jamming codewords are selected from finer lattice codebooks compared to message codebooks. The reason is that the jamming signal needs to get aligned with any possible realization of the confidential message codeword at unintended receivers. A pair of a coarse and a fine lattice sets are used to encode each individual confidential message and jamming signal. Assume that the pair used to encode the m-th component of the confidential message j at Transmitter j is denoted as $(\Lambda_j^m, \Lambda_{f,j}^m)$. Also, the associated lattice pair used for protecting the m-th component of confidential message $K-j+1$ is denoted as $(\Lambda_{J,j}^m, \Lambda_{fJ,j}^m)$. For each component $m \in \{1,\ldots,M\}$ the following nested lattice relation holds amongst all the participating lattice sets:

$$\Lambda \subseteq \Lambda_K^m \subseteq \Lambda_{K-1}^m \subseteq \ldots \Lambda_1^m \subseteq \Lambda_{J,K}^m \subseteq \ldots \Lambda_{J,1}^m \subseteq \Lambda_{f,K}^m \subseteq \ldots \Lambda_{f,1}^m \subseteq \Lambda_{Jf,K}^m \subseteq \ldots \Lambda_{Jf,1}^m \tag{6}$$

The coarse lattice sets are scaled such that their second moments are equal to $\sigma_{m,K}^2, \ldots, \sigma_{m,1}^2, \sigma_{Jm,K}^2, \ldots, \sigma_{Jm,1}^2$, respectively. Also, the fundamental Voronoi region of the coarse lattice associated with the m-th component of message i denoted as $\mathcal{V}_i^m$ and the one associated with the m-th component of the jamming signal generated at Transmitter i is denoted as $\mathcal{V}_{J,i}^m$. The center of a corset of the fine lattice $\Lambda_{f,i}^m$ is an n-length random vector (lattice word) and is denoted by $\mathbf{t}_{m,i}$. The inner codebook used for encoding the m-th component of message i is defined as the union of all realizations of this vector, i.e., $\mathcal{L}_{m,i} \triangleq \{\mathbf{t}_{m,i} | \mathbf{t}_{m,i} \in \mathcal{V}_i^m\}$. Similarly, the inner codebook for the jamming signal is defined as $\mathcal{L}_{Jm,i} \triangleq \{\mathbf{u}_{m,i} | \mathbf{u}_{m,i} \in \mathcal{V}_{J,i}^m\}$, where $\mathbf{u}_{m,i}$ is also an n-length lattice word associated with the center of a corset of fine lattice $\Lambda_{Jf,i}^m$. To construct an outer codeword, we use i.i.d. random repetition of the inner codeword. This step is done to take advantage of Packing Lemma [15] in the proof of secrecy. Consider a probability distribution $P(\mathbf{t}_{m,i})$ over the elements of codebook $\mathcal{L}_{m,i}$. Transmitter i draws B independent realizations of the inner codeword $\mathbf{t}_{m,i}$ according to distribution $P(\mathbf{t}_{m,i})$. These n-length lattice words are concatenated to form an $N \triangleq n \times B$ length vector which is a realization of the outer codeword $\bar{\mathbf{t}}_{m,i}$. To construct the corresponding outer codebook, Transmitter i generates $2^{NR_{comb,m}^i}$ realizations of the outer codeword $\bar{\mathbf{t}}_{m,i}$. This outer codebook is denoted as $\mathcal{C}_{m,i}$. Similarly, the outer codebook generated to encode the m-th component of the jamming signal at Transmitter i is denoted as $\mathcal{C}_{Jm,i}$ and the random vector representing its outer codeword is denoted as $\bar{\mathbf{u}}_{m,i}$.

The constructed outer codebooks are partitioned to emulate the wiretap code [2]. To do this, Transmitter i randomly partitions codebook $\mathcal{C}_{m,i}$ into $2^{NR_{m,i}}$ bins of equal sizes. Each bin (m,i) is given an index $w_{m,i}$ where $w_{m,i} \in \{1,\ldots,2^{NR_{m,i}}\}$. These indices are essentially independent sub-messages of the confidential message W_i. The transmitter chooses the non-negative rates $R_{m,i}$ such that $R_i = \sum_{m=1}^M R_{m,i}$, where the secure rate R_i is set to

$$R_i \triangleq R_{comb}^i - \max_{\substack{\ell \\ \ell \neq i}} \left[\log \left(\sum_{\substack{m \in S \\ \frac{|S|}{M} \to 1}}^{M} \frac{h_{i\ell}^2 P_{i,m} + h_{K-i+1,\ell}^2 P_{K-i+1,m}^J}{h_{K-i+1,\ell}^2 P_{K-i+1,m^*}^J} \right) \right] \tag{7}$$

where for all $m, m^* \in M$, and $i \in \{1,2,\ldots,K\}$ and set S_M (as defined in Section III), quantities $P_{i,m}$ and $P_{i,m}^J$ are positive values and they represent the power allocations among the corresponding confidential message and jamming signal components, respectively. These quantities are formulated in Subsection IV-B. Also, $R_{comb}^i \triangleq \sum_{m=1}^M R_{comb,m}^i$.

Additionally, for each component of the confidential message i and the jamming signal, Transmitter i generates a random dither outer codeword $\bar{\mathbf{d}}_{m,i}$ and $\bar{\mathbf{d}}_{Jm,i}$, respectively. Dithers are drawn uniformly random from the corresponding Voronoi regions, $\mathcal{V}_{m,i}$ and $\mathcal{V}_{Jm,i}$. Dithers are public information and after selection are provided to all parties. In the following, we present the encoding operation at Transmitter i which also protects Transmitter $K-i+1$'s confidential message at receivers $1,2,\ldots,K-1$. Encoding at the other transmitters is performed in a similar fashion.

B. Encoding

Transmitter i splits the confidential message $w_i \in \{1,\ldots 2^{NR_i}\}$ into $M \triangleq T^{2K-2}$ independent sub-messages, where T is a large number. The m-th sub-message is denoted as $w_{m,i} \in \{1,\ldots,2^{NR_{m,i}}\}$. To encode this sub-message, Transmitter i randomly picks an outer codeword $\bar{\mathbf{t}}_{m,i}$ from the corresponding outer codebook $\mathcal{C}_{m,i}$. Next, the selected codeword is mixed with a random dither $\bar{\mathbf{d}}_{m,i}$ according to the following equation $\tilde{\mathbf{x}}_{m,i} \triangleq [\bar{\mathbf{t}}_{m,i} + \bar{\mathbf{d}}_{m,i}] \mod \Lambda_i^m$. The modular operation in dithering step is done blockwise over each n-length block, separately. Similarly, the jamming codeword $\tilde{\mathbf{x}}_{m,i}^J$ is defined. Note that the lattice set associated with the jamming codewords are denser than the message codewords. In the next step, the beam-forming operation is performed over each component codeword. Note that each component is sent over a different beam-forming dimension where the total number of the dimensions is M. The idea is to align the jamming signal and the confidential message codeword across many such dimensions at unintended receivers. The precoder applied to codeword $\tilde{\mathbf{x}}_{m,i}$ is denoted as $f(m,i,K-i+1,\mathbf{H})$, where $\mathbf{H} = (\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_K)$ is the matrix of channel gains. The precoder f is a mapping that takes sub-message indices (m,i) and channel gain matrix $\mathbf{H}$ as inputs and outputs a scalar value. This mapping ensures that the resulting codewords are rationally independent for all channel gains expect for a small Lebesgue measure. Transmitter i applies the individual precoders over each component codeword and forms the superposition codeword $\mathbf{x}_i$ over the channel, where

$$\mathbf{x}_i \triangleq \sum_{m=1}^{M} \tilde{\mathbf{x}}_{m,i} f(m, i, K-i+1, \mathbf{H}) \tag{8}$$

Similarly, a precoder is applied to the jamming codeword to protect the confidential message of Transmitter $K-i+1$, i.e.,

$$\mathbf{x}_i^J \triangleq \sum_{m=1}^{M} \tilde{\mathbf{x}}_{m,i}^J g(m, i, K-i+1, \mathbf{H}) \tag{9}$$

The superimposed transmitted codeword $\mathbf{X}_i \triangleq \mathbf{x}_i + \mathbf{x}_i^J$ satisfies the power constraint, i.e., $\|\mathbf{X}_i\|_2^2 \leq NP$. Let us define $P_{m,i} \triangleq \sigma_{m,i}^2 |f(m,i,K-i+1,\mathbf{H})|^2$ and $P_i = \sum_{m=1}^{M} P_{m,i}$. Similarly, for the jamming codeword, define $P_{m,i}^J \triangleq \sigma_{Jm,i}^2 |g(m,i,K-i+1,\mathbf{H})|^2$ and $P_i^J = \sum_{m=1}^{M} P_{m,i}^J$. Transmitter i allocates power between jamming power and message power such that $P_i + P_i^J \leq P$. Additionally, the coarse lattice sets associated with every jamming codeword is scaled such that for $\forall i \in \{1, \ldots, K\}$, we have

$$h_{K-i+1,i}^2 P_{K-i+1}^J \leq 1 \tag{10}$$

Note that the above condition is essential to achieve sum secure degrees of freedom of 1 and without this condition, the achievable sum secure degrees of freedom would reach $\frac{K}{K+1}$. The precoder mapping $f(m, i, K-i+1, \mathbf{H})$ is a product of powers of channel gains between both Transmitters i and $K-i+1$ and the receivers, i.e.,

$$f(m,i,K-i+1,\mathbf{H}) = (h_{i1}^{r_1} h_{i2}^{r_2} \ldots h_{i,i-1}^{r_{i-1}} h_{i,i+1}^{r_i} \ldots h_{iK}^{r_{K-1}}) \times$$
$$(h_{K-i+1,1}^{r_K} h_{K-i+1,2}^{r_{K+1}} \ldots h_{K-i+1,i-1}^{r_{K+i-1}} h_{K-i+1,i+1}^{r_{K+i}} \ldots h_{K-i+1,K}^{r_{2K-2}}) \tag{11}$$

and

$$g(m,i,K-i+1,\mathbf{H}) = (h_{i1}^{r_1} \ldots h_{i,K-i}^{r_{K-i}} h_{i,K-i+2}^{r_{K-i+1}} \ldots h_{iK}^{r_{K-1}}) \times$$
$$(h_{K-i+1,1}^{r_K} h_{K-i+1,2}^{r_{K+1}} \ldots h_{K-i+1,K-i}^{r_{K-i}} h_{K-i+1,K-i+2}^{r_{K-i+1}} \ldots h_{K-i+1,K}^{r_{2K-2}}) \tag{12}$$

The exponents $(r_1, r_2, \ldots, r_{2K-2})$ are computed using a one-to-one mapping $\phi(m)$ that takes the m-th beam-forming dimension to the $2K-2$-length tuple exponent where each exponent is one of the possible T dimensions. In other words, we have: $\phi(m) : \{1, \ldots, M\} \to \{1, \ldots, T\} \times \{1, \ldots, T\} \times \cdots \times \{1, \ldots, T\}$, and for every $m \in \{1, \ldots, M\}$ there exists a non-negative $2K-2$ length tuple such that $(r_1, r_2, \ldots, r_{2K-2}) = \phi(m)$, where $r_j \in \{1, 2, \ldots, T\}$.

C. Decoding

Decoding at each receiver follows asymmetric compute-and-forward technique used in [12]. In the following, we describe the decoding process at Receiver i. Other receivers act in a similar manner.

Receiver i observes the scaled lattice codeword associated with its own message plus a set of unintended codewords aligned with jamming codewords plus effective noise as

$$\mathbf{Y}_i = h_{ii}\mathbf{x}_i + \sum_{\substack{\ell=1 \\ \ell \neq i}}^{K} (h_{\ell i}\mathbf{x}_\ell + h_{K-\ell+1,i}\mathbf{x}_{K-\ell+1}^J)$$
$$+ h_{K-i+1,i}\mathbf{x}_{K-i+1}^J + \mathbf{z}_i \tag{13}$$

Due to asymptotic alignment [14] along many beam-forming dimensions, the collections of the confidential and the jamming codewords participating in the second term in (13) are mutually aligned. Also, note that due to the constraint in (10), the power of the third term falls below noise power (assuming all noise powers are normalized). Also, this term includes only a jamming signal which is of no use to Receiver i. Note that the condition in (10) is aligned with weakly and moderately weak interference definition in [8]. Therefore, Receiver i treats the third term as an additional noise term and the normalized effective noise term $\tilde{\mathbf{z_i}}$ is defined as

$$\tilde{\mathbf{z_i}} \triangleq \frac{1}{\sqrt{1 + h_{K-i+1,i}^2 P_{K-i+1}^J}} (h_{K-i+1,i}\mathbf{x}_{K-i+1}^J + \mathbf{z_i}) \tag{14}$$

As a result, Receiver i effectively observes a K-user Multiple Access Channel (MAC) at its end, i.e.,

$$\tilde{\mathbf{y}}_i \triangleq \frac{h_{ii}}{\sqrt{1 + h_{K-i+1,i}^2 P_{K-i+1}^J}} \mathbf{x}_i + \tilde{\mathbf{z_i}}$$
$$+ \frac{1}{\sqrt{1 + h_{K-i+1,i}^2 P_{K-i+1}^J}} \sum_{\substack{\ell=1 \\ \ell \neq i}}^{K} (h_{\ell i}\mathbf{x}_\ell + h_{K-\ell+1,i}\mathbf{x}_{K-\ell+1}^J) \tag{15}$$

The effective MAC channel gain vector at Receiver i is denoted as $\mathbf{h}_{eff,i}$ and it is defined as $\mathbf{h}_{eff,i} \triangleq \left(\frac{h_{ii}}{\sqrt{1+h_{K-i+1,i}^2 P_{K-i+1}^J}}, \frac{1}{\sqrt{1+h_{K-i+1,i}^2 P_{K-i+1}^J}}, \ldots, \frac{1}{\sqrt{1+h_{K-i+1,i}^2 P_{K-i+1}^J}} \right)^T$.
The ratio between the power of each effective codeword in the effective MAC equation (15) and the power constraint P is defined as power scaling vector $\mathbf{b}_{eff,i}$ and $\mathbf{b}_{eff,i} \triangleq \left(\sqrt{\frac{P_i}{P}}, \sqrt{\frac{h_{1i}^2 P_1 + h_{Ki}^2 P_K^J}{P}}, \ldots, \sqrt{\frac{h_{Ki}^2 P_K + h_{1i}^2 P_1^J}{P}} \right)^T$
Now, Receiver i applies the compute-and-forward technique used for a MAC channel in [10]. Following this technique, Receiver i finds the nearly optimal set of linearly independent integer-valued coefficient vectors which maximize the achievable MAC sum-rate for that Receiver. The receiver constructs K-linearly independent equations using these integer-valued coefficient vectors and decode each equation successively. The first equation is to aim to decode the effective lattice codeword associated with the densest lattice codebook. Upon decoding this codeword, it is canceled out from the second equation and so forth. Therefore, the least achievable equation rate is associated with the K-th combination equation.

Let us denote the optimal set of integer-valued coefficient vectors that construct the K combination equations with $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_K$. Also, let us denote the rates at which the K combination equations are decoded at Receiver i as $R^i_{comb,1}, R^i_{comb,2}, \ldots, R^i_{comb,K}$. The set of coefficient vectors is computed such that the rate at which combination equations are decoded is non-increasing, i.e., $R^i_{comb,1} \geq R^i_{comb,2} \geq \cdots \geq R^i_{comb,K}$. Basically, the effective codeword with the highest achievable rate is decoded first and canceled out and then the second highest rate effective codeword is decoded and so forth. Let us denote the first combination equation as $\mathbf{v}_1 \triangleq \mathbf{a}_1(\ell)\mathbf{x}_{eff,\ell}$. For instance, the effective codewords at Receiver i are defined as $\mathbf{x}_{eff,1} \triangleq \mathbf{x}_i$, $\mathbf{x}_{eff,2} \triangleq h_{1i}\mathbf{x}_1 + h_{Ki}\mathbf{x}^J_K$ and so forth so it would match the corresponding gain order in the effective MAC observed by Receive i. Decoding equation $\mathbf{v}_1$ is performed using the compute-and-forward technique [10], [16] by scaling the noisy observation and canceling out the public dithers as $\beta_1\tilde{\mathbf{y}}_i - \sum_{\ell=1}^{K} \mathbf{a}_1(\ell)\bar{\mathbf{d}}_{eff,\ell} = \mathbf{v}_1 + \mathbf{z}_{eff,i,1}$, where

$$\mathbf{z}_{eff,i,1} \triangleq \sum_{\ell=1}^{K}(\beta_1\mathbf{h}_{eff}(\ell) - \mathbf{a}_1(\ell))\mathbf{x}_{eff,\ell} + \beta_1\tilde{\mathbf{z}}_i \qquad (16)$$

Let us denote the second moment of the effective noise term associated with combination equation 1 in (16) as $\sigma^2_{eff,i,1}$. Following Theorem 2 in [16] equation $\mathbf{v}_1$ can be decoded at an achievable rate $R^i_{comb,1} = \frac{1}{2}\log(\frac{P_{eff,j}}{\sigma^2_{eff,i,1}})$, where j is the index of the effective lattice codeword with densest lattice sets among participating codewords in combination equation $\mathbf{v}_1$. Similarly, combination equations $\mathbf{v}_2, \ldots, \mathbf{v}_K$ are constructed and decoded. Assume that the mapping between effective codeword indices and the order at which they get decoded at Receiver i is determined by a one-to-one permutation function $\pi^i(.) : \{1, 2, \ldots, K\} \rightarrow \{1, 2, \ldots, K\}$. Therefore, the achievable combination rates are derived as $R^i_{comb,\ell} = \frac{1}{2}\log\left(\frac{P_{eff,\pi^i(\ell)}}{\sigma^2_{eff,i,\ell}}\right)$. We already established that the combination equations are constructed such that the codeword with the densest lattice set gets decoded first therefore $\sigma^2_{eff,1} \leq \sigma^2_{eff,2} \leq \ldots \sigma^2_{eff,K}$. As a result, the lowest achievable rate to decode effective codeword $\mathbf{x}_{eff,1}$ at Receiver i, i.e., $\mathbf{x}_i$ is

$$R^i_{comb} \triangleq \frac{1}{2}\log\left(\frac{P_{eff,1}}{\sigma^2_{eff,i,K}}\right) = \frac{1}{2}\log\left(\frac{P_i}{\sigma^2_{eff,i,K}}\right) \qquad (17)$$

Similarly, the achievable combination rates are determined at the other receivers. Since in (4) $R_i \leq R^i_{comb}$ for $i \in \{1, \ldots, K\}$, the proof of reliable decoding is completed. Due to space limitation, Analysis of weak secrecy is provided in [13].

V. Conclusion

We introduced an efficient achievable secure coding framework to transmit confidential messages over an asymmetric interference channel with arbitrary number of users ($K > 2$) provided that the interference level lies in the weak and moderately weak interference regimes. Our achievable scheme utilizes a two-layered codebook comprised of nested lattice codebooks and i.i.d. repetitive codes. We applied a novel approach of cooperative jamming and superposition coding to ensure security of the confidential messages without using external helpers. Also, we utilized the asymmetric compute-and-forward decoding strategy to handle finite SNR regime. We showed that following our scheme, users achieve secure rates which scale linearly with $\log(\text{SNR})$ and a sum secure rate that is within constant gap of sum capacity is attainable. Furthermore, our cooperative scheme achieves the optimal sum secure degrees of freedom of 1 for the defined security model.

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] A. D. Wyner, "The wire-tap channel," *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] Y. Liang, H. V. Poor, S. Shamai, *et al.*, "Information theoretic security," *Foundations and Trends® in Communications and Information Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.

[4] 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.

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

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

[7] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "On the secure degrees-of-freedom of the multiple-access-channel," *arXiv preprint arXiv:1003.0729*, 2010.

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

[9] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 351–368, Springer, 2000.

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

[11] P. Babaheidarian, S. Salimi, and P. Papadimitratos, "Finite-snr regime analysis of the gaussian wiretap multiple-access channel," in *2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 307–314, IEEE, 2015.

[12] P. Babaheidarian, S. Salimi, and P. Papadimitratos, "Preserving confidentiality in the gaussian broadcast channel using compute-and-forward," in *2017 51st Annual Conference on Information Sciences and Systems (CISS)*, pp. 1–6, IEEE, 2017.

[13] P. Babaheidarian, S. Salimi, and P. Papadimitratos, "Towards scalable security in interference channels with arbitrary number of users," *arXiv preprint cs/2004.06588*, 2020.

[14] 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 Transactions on Information Theory*, vol. 60, no. 8, pp. 4799–4810, 2014.

[15] A. El Gamal and Y.-H. Kim, *Network information theory*. Cambridge university press, 2011.

[16] 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.