Finite-SNR Regime Analysis of The Gaussian Wiretap Multiple-Access Channel

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

***Abstract*—In this work, we consider a K-user Gaussian wiretap multiple-access channel (GW-MAC) in which each transmitter has an independent confidential message for the receiver. There is also an external eavesdropper who intercepts the communications. The goal is to transmit the messages reliably while keeping them confidential from the eavesdropper. To accomplish this goal, two different approaches have been proposed in prior works, namely, i.i.d. Gaussian random coding and real alignment. However, the former approach fails at moderate and high SNR regimes as its achievable result does not grow with SNR. On the other hand, while the latter approach gives a promising result at the infinite SNR regime, its extension to the finite-SNR regime is a challenging task. To fill the gap between the performance of the existing approaches, in this work, we establish a new scheme in which, at the receiver's side, it utilizes an extension of the compute-and-forward decoding strategy and at the transmitters' side it exploits lattice alignment, cooperative jamming, and i.i.d. random codes. For the proposed scheme, we derive a new achievable bound on sum secure rate which scales with $\log(\mathrm{SNR})$ and hence it outperforms the i.i.d. Gaussian codes in moderate and high SNR regimes. We evaluate the performance of our scheme, both theoretically and numerically. Furthermore, we show that our sum secure rate achieves the optimal sum secure degrees of freedom in the infinite-SNR regime.**

I. Introduction

It has been shown that structured codes outperform the standard random codes in certain communication scenarios with and without security constraints such as [1], [2], [3], and [4]. For instance, a scheme based on real alignment was proposed in [2] for the K-user Gaussian wiretap multiple-access channel (GW-MAC). They used alignment to confuse the eavesdropper and showed that in the infinite SNR regime, their scheme improves over the result achieved by Gaussian i.i.d. random codes in [5]. Also, Xie *et al.* in [3] employed the real alignment technique in conjunction with cooperative jamming for the same channel model and showed improvement over the former scheme in [2]. In particular, the proposed scheme in [3] achieves the optimal sum secure degrees of freedom (s.d.o.f.) for the K-user Gaussian wiretap multiple-access channel. Additionally, using similar schemes, they characterized the exact secure degrees of freedom for Gaussian broadcast channel with multiple helpers as well as sum secure degrees of freedom for the two-user interference channel.

The aforementioned alignment schemes are limited to the infinite SNR regime whereas their extension to the finite-SNR regime is challenging. On the other hand, in [6], Ordentlich *et al.* accommodated the finite-SNR regime analysis for the K-user multiple-access channel (MAC) without security constraints. They proposed a lattice alignment scheme using the compute-and-forward decoding strategy, introduced in [7], and showed that their scheme achieves a sum rate, *without security*, that is within a constant gap from K-user MAC sum capacity and is valid for any finite value of SNR.

Also, very recently, a compute-and-forward based scheme was proposed to handle the finite-SNR regime for the K-user Gaussian wiretap multiple-access channel [8]. A lower bound on the sum secure rate was derived, which achieved $\frac{K-1}{K}$ sum secure degrees of freedom. This was the first scheme on GW-MAC that achieved a positive s.d.o.f and yet it worked at finite-SNR regime.

In this paper, in light of the work in [3], we further improve upon [8] such that our new achievable sum secure rate reaches the optimal sum secure degrees of freedom, i.e., $\frac{K(K-1)}{K(K-1)+1}$, in the infinite-SNR regime and yet improves over i.i.d. Gaussian random codes in the moderate and high SNR regimes. It also surpasses the result in [8] in high SNR regimes. We propose a new scheme which consists of two layers in its encoding strategy: the inner layer and the outer layer. Transmitters incorporate a nested lattice structure as well as cooperative jamming signals in their inner layers and i.i.d. random codes in their outer layers. Also, in our decoding strategy, the receiver exploits a new extension of the compute-and-forward decoding strategy. We characterize a lower bound on the sum secure rate for the K-user Gaussian wiretap multiple access channel which is valid for any finite value of SNR and is in agreement with the result in [3] in the infinite-SNR regime. Moreover, we evaluate the performance of our proposed scheme numerically for a three-user GW-MAC.

The rest of the paper is organized as follows. In Section II the system model is defined. Section III is devoted to our main results. The achievability scheme and analysis of security are presented in Section IV. Section V provides the numerical results. The paper is concluded in Section VI. Finally, complementary proofs are provided in Appendix.

II. System model

We consider the problem of secure and reliable communication over a multiple-access channel with K users at the presence of an external eavesdropper. The system is modeled by

$$\mathbf{y} = \sum_{\ell=1}^{K} h_\ell \mathbf{x}_\ell + \mathbf{z}, \quad \mathbf{y}_E = \sum_{\ell=1}^{K} g_\ell \mathbf{x}_\ell + \mathbf{z}_E \tag{1}$$

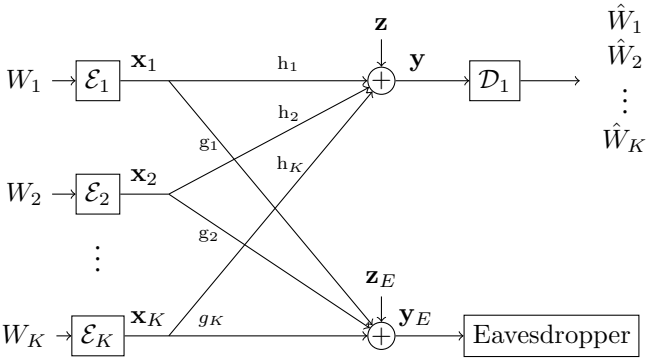

Fig. 1: The Gaussian wiretap multiple-access channel model.

Where $\mathbf{x}_\ell$ is user ℓ's channel input with a block length of N. Vectors $\mathbf{y}$ and $\mathbf{y}_E$ are the channel outputs at the receiver and the eavesdropper sides, respectively. The real-valued elements h_ℓ and g_ℓ are the channel gains from user ℓ to the receiver and the eavesdropper, respectively; thus, vectors $\mathbf{h} \triangleq [h_1, \ldots, h_K]^T$ and $\mathbf{g} \triangleq [g_1, \ldots, g_K]^T$ are the channel gain vectors. We assume that the transmitters[1] know the channel states, i.e., the channel gain vectors, in advance. Finally, the random vectors $\mathbf{z}$ and $\mathbf{z}_E$ are, respectively, the receiver's and the eavesdropper's channel noises which are independent and each is i.i.d. Gaussian with zero mean and normalized variance.

As it is shown in Figure 1, user ℓ has an independent confidential message W_ℓ which is uniformly distributed over the set $\{1, \ldots, 2^{NR_\ell}\}$, for $\ell \in \{1, \ldots, K\}$. User ℓ maps its message to the codeword $\mathbf{x}_\ell$ through a stochastic encoder, i.e., $\mathbf{x}_\ell = \mathcal{E}_\ell(W_\ell)$. Also, there are power constraints on the channel inputs as $\|\mathbf{x}_\ell\|^2 \leq NP$, for all $\ell \in \{1, \ldots, K\}$. There is also a decoder $\mathcal{D}$ at the receiver side that estimates the transmitted messages, i.e., $\mathcal{D}(\mathbf{y}) = \{\hat{W}_\ell\}_{\ell=1}^K$.

Definition 1 (Achievable sum secure rate): For the K-user GW-MAC, a sum secure rate $\sum_{\ell=1}^K R_\ell$ is achievable, if for any $\epsilon > 0$ and sufficiently large N, there exist a sequence of encoders $\{\mathcal{E}_\ell\}_{\ell=1}^K$ and a decoder D such that:

$$\mathrm{Prob}\left(\bigcup_{\ell=1}^K \{\hat{W}_\ell \neq W_\ell\}\right) < \epsilon \tag{2}$$

$$\sum_{\ell=1}^K R_\ell \leq \frac{1}{N} H(W_1, W_2, \ldots, W_K | \mathbf{y}_E) + \epsilon \tag{3}$$

We refer to inequalities (2) and (3) as the *reliability* and the *weak secrecy* constraints, respectively. Note that the sum secure capacity is the supremum over all the achievable sum secure rates.

III. Main results

In our achievability scheme, we develop a new decoding strategy for K-user GW-MAC, which extends the one used in [6], to comply with our encoding strategy. In our setting, the receiver decodes $K(K-1)+1$ equations whose coefficient vectors are integer valued and are linearly independent, then it solves the system of the equations for the transmitted messages. We denote the optimal rates at which the receiver can successfully decode the equations by the set of rates $R_{comb,k}$, $\forall\, k \in \{1, \ldots, K(K-1)+1\}$ and we refer to them as equation rates or integer combination rates. The rates $R_{comb,k}$ are computed in Section IV.

The following theorem is our main result.

Theorem 1: A sum secure rate $\sum_{\ell=1}^K R_\ell$ is achievable if it satisfies the following inequality

$$\sum_{\ell=1}^K R_\ell < \sum_{k=2}^{K(K-1)+1} R_{comb,k} - \frac{1}{2}\sum_{\ell=1}^K \log\left(\frac{\sum_{j=1, j\neq\ell}^K \gamma_{j,\ell}^2 P_{j,\ell} + \gamma_{\ell,\ell}^2 P_{\ell,\ell}}{\gamma_{\ell,\ell}^2 P_{\ell,\ell}}\right) \tag{4}$$

such that, for all $\ell \in \{1, \ldots, K\}$, the following holds.

$$\gamma_{(\ell,i)} = \frac{g_\ell h_i}{g_i} \quad \forall i \neq \ell, \tag{5}$$

$$\gamma_{(\ell,\ell)} = h_\ell \tag{6}$$

and

$$\sum_{i=1}^K P_{\ell,i} \leq P, \;\; P_{\ell,i} > 0 \;\; \forall i \in \{1, \ldots, K\} \tag{7}$$

Note that the achievable bound in (4) is a function of coefficients $P_{\ell,i}$, hence the supremum over all choices of $P_{\ell,i}$ satisfying (7) is also achievable.

Remark 1: The sum rate $\sum_{k=1}^{K(K-1)+1} R_{comb,k}$ in our scheme is different from the sum rate achieved by [6] for the K-user Gaussian MAC capacity[2]. However, we show that our achievable sum rate reaches the performance of the compute-and-forward framework in [6], asymptotically. In other words, we show that $\sum_{k=1}^{K(K-1)+1} R_{comb,k}$ is within a constant gap from K-user Gaussian MAC capacity. The proof is provided in Appendix-A. Also, we will verify this claim by a numerical experiment in Section V.

Corollary 1: The achievable sum secure rate in (4) grows with $\log(\mathrm{SNR})$, i.e.,

$$\sum_{\ell=1}^K R_\ell \propto \log(\mathrm{P}) \tag{8}$$

Remark 2: The importance of Corollary 1 becomes clear when its result is compared with the performance of sum secure rate provided by i.i.d. Gaussian random codes in [5]. Recall that the latter achieves a sum secure rate of $\frac{1}{2}\log(\frac{1+\|\mathbf{h}\|^2 P}{1+\|\mathbf{g}\|^2 P})$ for the K-user GW-MAC. Hence, the security performance of the scheme in [5] does not grow by increasing the power[3].

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

[2] We refer to the sum of non-secure rate as sum rate.

[3] Assuming the channel gain vector norms are of similar orders.

Corollary 2: The sum secure degrees of freedom (s.d.o.f.) achieved by our scheme is

$$\lim_{P\to\infty} \frac{\sum_\ell R_\ell}{\frac{1}{2}\log(1+P)} = \frac{K(K-1)}{K(K-1)+1} \tag{9}$$

Remark 3: Recall that in [3] it is shown that the optimal sum secure degrees of freedom for the K-user Gaussian wiretap MAC is $\frac{K(K-1)}{K(K-1)+1}$. Hence, our achievable result in (4) is asymptotically optimal.

Next section provides the achievability scheme and the security analysis.

IV. The achievability scheme and analysis of security

In this section, we introduce our new scheme. First, we describe the codebook construction and encoding strategy applied by the transmitters and then we unfold the decoding strategy used by the receiver. Finally, the proof of weak secrecy of the proposed scheme is presented. (Note: Proofs for Corollary 1 and 2 are given in Appendix.

Codebook construction and encoding strategy

In order to send the confidential messages $\{W_\ell\}_{\ell=1}^K$, each user (transmitter) utilizes $(K-1)$ sub-codewords to encode its own confidential message. Moreover, each user employs an additional sub-codeword as a jamming signal which does not carry any information regarding the confidential messages. We proceed with describing the operations done by user ℓ, other users perform similarly.

User ℓ picks K n-dimensional coarse and fine lattice pairs as $(\Lambda_{f,(\ell,i)}, \Lambda_{(\ell,i)})$ for all $i \in \{1,\dots,K\}$. The set of lattices used by all users form a nested structure in which the following two conditions hold.

$$\Lambda_{(j,\ell)} \subseteq \Lambda_{(\ell,\ell)}, \quad \Lambda_{f,(j,\ell)} \subseteq \Lambda_{f,(\ell,\ell)} \quad \forall\, j \neq \ell \tag{10}$$

The fundamental Voronoi region of the coarse lattice $\Lambda_{(\ell,i)}$ is denoted by $\mathcal{V}_{(\ell,i)}$. For each i, the centers of the translations of the fine lattice $\Lambda_{f,(\ell,i)}$ (cosets) lying in $\mathcal{V}_{(\ell,i)}$ are considered as the realizations of the random vector $\mathbf{t}_{\ell,i}$. The second moment of the coarse lattice $\Lambda_{(\ell,i)}$ is set as $\gamma^2_{(\ell,i)}P_{\ell,i}$.

Define the set $\mathcal{L}_{(\ell,i)} \triangleq \{\mathbf{t}_{\ell,i} | \mathbf{t}_{\ell,i} \in \mathcal{V}_{(\ell,i)}\}$. Assume that vectors $\mathbf{t}_{\ell,i}$ have a probability distribution $P(\mathbf{t}_{\ell,i})$ over the set $\mathcal{L}_{(\ell,i)}$. The set $\mathcal{L}_{(\ell,i)}$ is termed the *inner* sub-codebook i used by user ℓ.

Consider a one-to-one mapping $\phi : \{1,\dots,K\} \times \{1,\dots,K\}\backslash\{(\ell,\ell)|\ell \in [1,K]\} \to \{2,\dots,K(K-1)+1\}$. Then, the ratio between the coarse lattice $\Lambda_{(\ell,i)}$ and its associated fine lattice is set such that $R_{comb,k} = \frac{1}{n}\log(|\mathcal{L}_{(\ell,i)}|)$ where $k = \phi(\ell,i)$ for all $i \neq \ell$ and $k = 1$ for $i = \ell$.

Next, user ℓ generates B independent copies of vectors $\mathbf{t}_{\ell,i}$ according to distribution $P(\mathbf{t}_{\ell,i})$ to make one *realization* of the outer codewords $\bar{\mathbf{t}}_{\ell,i}$. As a result, the block length of the generated outer codeword is $N \triangleq n \times B$. User ℓ performs this procedure $2^{NR_{comb,(\ell,i)}}$ times to construct its outer sub-codebook i, i.e., $\mathcal{C}_{(\ell,i)}$. User ℓ generates all its other sub-codebooks, similarly. It is worth to mention that the i.i.d. repetition of the inner codebook is added to the scheme so that we can benefit from Packing Lemma in the proof of weak secrecy[4].

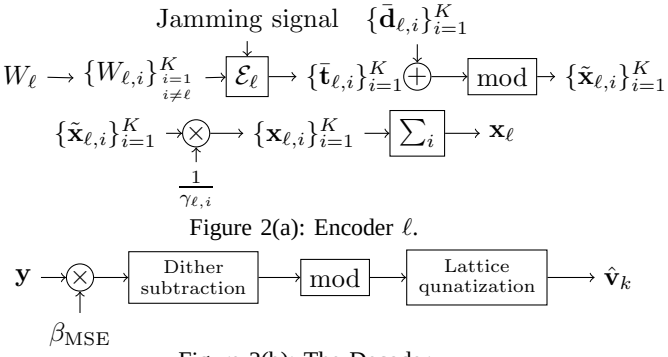

Fig. 2: Our achievable scheme.

In the next step, similar to the Wyner random partitioning in [9], the outer codewords of each sub-codebook (ℓ,i), for all $\ell \in \{1,\dots,K\}$ and $i \neq \ell$, are randomly partitioned into $2^{NR_{\ell,i}}$ bins of equal sizes. Note that the non-negative rates $R_{\ell,i}$ are chosen by user ℓ such that $\sum_{i\neq\ell} R_{\ell,i} = R_\ell$. The partition index is characterized by a random variable $W_{\ell,i}$ in the corresponding sub-codebook. To encode the confidential message W_ℓ with its realizations $w_\ell \in \{1,\dots,2^{NR_\ell}\}$, user ℓ divides its message into $(K-1)$ mutually independent sub-messages $W_{\ell,i}$ with the corresponding realizations $w_{\ell,i}$. For the sub-message i, $i \in \{1,\dots,K\}\backslash\ell$, the user picks randomly a codeword $\bar{\mathbf{t}}_{\ell,i}$ from the partition $w_{\ell,i}$ in the sub-codebook $\mathcal{C}_{(\ell,i)}$[5]. Then, it adds a random dither vector $\bar{\mathbf{d}}_{\ell,i}$ to the selected codeword[6] and reduces the sum modulo the coarse lattice $\Lambda_{(\ell,i)}$. Keep in mind that dithers are independent of all other variables and are public.

The modular operation is done for each block of size n and the outcomes of all B blocks are concatenated together. We have:

$$\tilde{\mathbf{x}}_{\ell,i} \triangleq \left(\left[\bar{\mathbf{t}}_{\ell,i} + \bar{\mathbf{d}}_{\ell,i}\right] \bmod \Lambda_{(\ell,i)}\right) \tag{11}$$

At the end, the resulting codeword is scaled by $\frac{1}{\gamma_{(\ell,i)}}$. In short, the N-length codeword $\mathbf{x}_{\ell,i}$ is constructed as

$$\mathbf{x}_{\ell,i} \triangleq \frac{1}{\gamma_{(\ell,i)}}\left(\left[\bar{\mathbf{t}}_{\ell,i} + \bar{\mathbf{d}}_{\ell,i}\right] \bmod \Lambda_{(\ell,i)}\right) \tag{12}$$

The scaling factors $\gamma_{(\ell,i)}$ are defined in (5) and (6).

In addition, the jamming codeword $\bar{\mathbf{t}}_{\ell,\ell}$ is chosen uniformly at random from the sub-codebook $\mathcal{C}_{(\ell,\ell)}$. The codeword $\mathbf{x}_{\ell,\ell}$ is constructed similarly. Eventually, the superposition codeword $\mathbf{x}_\ell \triangleq \sum_{i=1}^K \mathbf{x}_{\ell,i}$ is transmitted through the channel by user ℓ. This procedure is displayed in Figure 2(a).

[4]Recall that proof of Packing Lemma is followed from jointly typicality lemma on i.i.d. random sequences.

[5]Once the assignment of the sub-messages to codewords is done, it will be fixed and provided to all parties.

[6]Each n-length block of the dither $\bar{\mathbf{d}}_{(\ell,i)}$ is uniformly distributed over $\mathcal{V}_{(\ell,i)}$.

Decoding strategy

Recall that the scaling factors $\gamma_{\ell,\ell},\ \forall \ell$, are chosen such that the users' jamming codewords $\tilde{\mathbf{x}}_{\ell,\ell}$ get aligned at the receiver's side and form a single lattice codeword $\sum_\ell \tilde{\mathbf{x}}_{\ell,\ell}$. Thus, the receiver observes

$$\mathbf{y} = \sum_{\ell} \sum_{\substack{i \\ i\neq \ell}} \frac{h_\ell g_i}{g_\ell h_i} \left(\left[\bar{\mathbf{t}}_{\ell,i} + \bar{\mathbf{d}}_{\ell,i} \right] \bmod \Lambda_{(\ell,i)} \right) + \sum_{\ell} \left[\bar{\mathbf{t}}_{\ell,\ell} + \bar{\mathbf{d}}_{\ell,\ell} \right] \bmod \Lambda_{(\ell,\ell)}, \tag{13}$$

Extending the compute-and-forward decoding strategy in [7] to $K(K-1)+1$ integer combinations, the receiver estimates the sub-messages codewords $\bar{\mathbf{t}}_{\ell,i}$ by decoding $K(K-1)+1$ linearly independent equations whose coefficients are integer valued. Equation k is denoted by $\mathbf{v}_k$ and it's defined as

$$\mathbf{v}_k \triangleq \left[a_1^{(k)} \sum_{\ell} \bar{\mathbf{t}}_{\ell,\ell} + \sum_{\substack{(\ell,i) \\ (\ell\neq i)}} a_{\ell,i}^{(k)} \bar{\mathbf{t}}_{\ell,i} \right] \bmod \Lambda, \tag{14}$$

for all $k \in \{1,\ldots,K(K-1)+1\}$. Thus, the integer coefficients vector for equation k is a $(K(K-1)+1)\times 1$ vector $\mathbf{a}^{(k)}$.

To decode equation $\mathbf{v}_k$, the receiver scales its observation $\mathbf{y}$ by a factor of β and then it subtracts the dithers off, finally it reduces the result modulo lattice Λ. It is worth mentioning that Λ is the coarsest lattice among all the previously defined lattice sets. The decoding procedure is depicted in Figure 2(b). We have

$$\begin{aligned}
\mathbf{s}_k &= \left[\beta \mathbf{y} - \sum_{\substack{(\ell,i) \\ i\neq \ell}} a_{\ell,i}^{(k)} \bar{\mathbf{d}}_{\ell,i} - a_1^{(k)} \sum_{\ell} \bar{\mathbf{d}}_{\ell,\ell} \right] \bmod \Lambda \\
&= \Bigg[\sum_{\substack{(\ell,i) \\ i\neq \ell}} a_{\ell,i}^{(k)} \gamma_{\ell,i} \mathbf{x}_{\ell,i} + a_1^{(k)} \sum_{\ell} \gamma_{\ell,\ell} \mathbf{x}_{\ell,\ell} - \sum_{\substack{(\ell,i) \\ i\neq \ell}} a_{\ell,i}^{(k)} \bar{\mathbf{d}}_{\ell,i} \\
&\qquad - a_1^{(k)} \sum_{\ell} \bar{\mathbf{d}}_{\ell,\ell} + \mathbf{z}_{\text{eff},k}(\mathbf{h}, \vec{\gamma}, \mathbf{a}^{(k)}, \beta) \Bigg] \bmod \Lambda \\
&= \left[\mathbf{v}_k + \mathbf{z}_{\text{eff},k}(\mathbf{h}, \vec{\gamma}, \mathbf{a}^{(k)}, \beta) \right] \bmod \Lambda
\end{aligned} \tag{15}$$

Where $\vec{\gamma}$ is the vector of the scaling factors and $\mathbf{z}_{\text{eff},k}$ represents the effective noise defined as

$$\mathbf{z}_{\text{eff},k}(\mathbf{h}, \vec{\gamma}, \mathbf{a}^{(k)}, \beta) \triangleq (\beta - a_1^{(k)}) \sum_{\ell} \gamma_{\ell,\ell} \mathbf{x}_{\ell,\ell} + \sum_{\substack{(\ell,i) \\ i\neq \ell}} (\beta h_\ell - a_{\ell,i}^{(k)} \gamma_{\ell,i}) \mathbf{x}_{\ell,i} + \beta \mathbf{z} \tag{16}$$

Thus, the effective noise variance is given as

$$\sigma^2_{\text{eff},k} = \| \beta \tilde{\mathbf{h}} - \Gamma . \mathbf{a}^{(k)} \|^2 P + \beta^2 \tag{17}$$

$\tilde{\mathbf{h}}$ is a $(K(K-1)+1)\times 1$ vector defined as

$$\tilde{\mathbf{h}} \triangleq [1, \underbrace{h_1, \ldots, h_1}_{K-1}, \underbrace{h_2, \ldots, h_2}_{K-1}, \ldots\ldots, \underbrace{h_K, \ldots, h_K}_{K-1}]^T \tag{18}$$

Γ is a $(K(K-1)+1)\times(K(K-1)+1)$ diagonal matrix such that:

$$\Gamma(1,1) = \sqrt{\frac{\sum_{\ell=1}^{K} \gamma_{\ell,\ell}^2 P_{\ell,\ell}}{P}} \tag{19}$$

and for $k > 2$

$$\Gamma(k,k) = \sqrt{\frac{\gamma_{\ell,i}^2 P_{\ell,i}}{P}} \quad s.t.\ k = \phi(\ell,i) \tag{20}$$

It can be shown that the minimizer of the effective noise variance with respect to β is the MSE factor in linear estimation of $a_1^{(k)} \sum_\ell \gamma_{\ell,\ell} \mathbf{x}_{\ell,\ell} + \sum_{\substack{(\ell,i) \\ i\neq\ell}} a_{\ell,i}^{(k)} \gamma_{\ell,i} \mathbf{x}_{\ell,i}$ from vector $\mathbf{y}$. Therefore, substituting the optimal β in equation (17) yields

$$\sigma^2_{\text{eff},k}(\mathbf{h}, \vec{\gamma}, \mathbf{a}^{(k)}) = \| \mathbf{F} . \mathbf{a}^{(k)} \|^2 \tag{21}$$

Where the dot operation is the matrix-vector product and matrix $\mathbf{F}$ is given as

$$\mathbf{F} \triangleq \left(\frac{1}{P} \Gamma^{-2} + \tilde{\mathbf{h}} \tilde{\mathbf{h}}^T \right)^{\frac{-1}{2}} . \Gamma \tag{22}$$

Note that among the lattice codewords participating in equation $\mathbf{v}_k$, the one constructed on the densest lattice can be recovered by decoding the equation $\mathbf{v}_k$. The receiver decodes upon receiving each n-length block and concatenates the block estimates at the end to get an estimate of the transmitted outer codeword. Consider a $k > 2$ and assume that lattice $\Lambda_{f,(\ell,i)}$ is the densest lattice participating in $\mathbf{v}_k$. In fact, mapping ϕ is deduced from this step, i.e., $k = \phi(\ell,i)$. Subsequently, the receiver estimates the corresponding codeword $\bar{\mathbf{t}}_{\ell,i}$ by decoding the equation $\mathbf{v}_k$ as

$$\hat{\mathbf{v}}_k = \left[Q_{f,(\ell,i)}(\mathbf{s}_k) \right] \bmod \Lambda \tag{23}$$

Where $Q_\Lambda(.)$ is the nearest neighbor qunatizer associated with lattice Λ. From (23), it can be seen that the probability of decoding equation $\mathbf{v}_k$ with error is upper-bounded as

$$\text{Prob}(\hat{\mathbf{v}}_k \neq \mathbf{v}_k) = \text{Prob}(\mathbf{z}_{\text{eff},k} \notin \mathcal{V}_{(\ell,i)})$$

Consequently, based on arguments similar to those in Theorem 2 in [6], it can be shown that for sufficiently high dimensional lattices, the decoding error probability can be chosen smaller than ϵ, for any arbitrary $\epsilon > 0$, provided that

$$R_{comb,k} < \frac{1}{2} \log \left(\frac{\gamma^2_{(\ell,i)} P_{\ell,i}}{\sigma^2_{\text{eff},k}} \right) \quad s.t.\ \phi(\ell,i) = k,\ k \neq 1 \tag{24}$$

and

$$R_{comb,1} < \max_{\ell} \left(\frac{1}{2} \log \left(\frac{\gamma^2_{(\ell,\ell)} P_{\ell,\ell}}{\sigma^2_{\text{eff},1}} \right) \right) \tag{25}$$

Finally, recall that by Theorem 1, the achievable sum secure rate must satisfy in $\sum_{\ell=1}^{K} R_\ell < \sum_{k=2}^{K(K-1)+1} R_{comb,k}$; therefore we have

$$\text{Prob}\left(\bigcup_{\ell=1}^{K} \{ \hat{W}_\ell \neq W_\ell \} \right) < \epsilon$$

Proof of weak secrecy

Base on our scheme, the eavesdropper observes the sequence $\mathbf{y}_E$ as

$$\mathbf{y}_E = \sum_{\ell=1}^{K} \sum_{\substack{i=1 \\ i\neq\ell}}^{K} \frac{g_i}{h_i} \left(\left[\bar{\mathbf{t}}_{\ell,i} + \bar{\mathbf{d}}_{\ell,i} \right] \bmod \Lambda_{(\ell,i)} \right) + \sum_{\ell=1}^{K} \left(\frac{g_\ell}{h_\ell} \left[\bar{\mathbf{t}}_{\ell,\ell} + \bar{\mathbf{d}}_{\ell,\ell} \right] \bmod \Lambda_{(\ell,\ell)} \right) + \mathbf{z}_E \quad (26)$$

Define a sequence of vectors $\mathbf{y}_E^{(1)}, \ldots, \mathbf{y}_E^{(K)}$ where

$$\mathbf{y}_E^{(\ell)} \triangleq \sum_{\substack{j=1 \\ j\neq\ell}}^{K} \left(\left[\bar{\mathbf{t}}_{j\ell} + \bar{\mathbf{d}}_{j,\ell} \right] \bmod \Lambda_{(j,\ell)} \right) + \left(\left[\bar{\mathbf{t}}_{\ell,\ell} + \bar{\mathbf{d}}_{\ell,\ell} \right] \bmod \Lambda_{(\ell,\ell)} \right) \quad (27)$$

Note that

$$\frac{1}{N} H(W_1,...,W_K|\mathbf{y}_E) \geq \frac{1}{N} H(W_1,...,W_K|\mathbf{y}_E^{(1)},...,\mathbf{y}_E^{(K)}).$$

First, we show that the following sum secure rate provides weak secrecy.

$$\sum_{\ell=1}^{K} R_\ell = \frac{1}{N} H\left(\bar{\mathbf{t}}_{1,1},\bar{\mathbf{t}}_{1,2},...,\bar{\mathbf{t}}_{K-1,K},\bar{\mathbf{t}}_{K,K}|\mathbf{y}_E^{(1)},...,\mathbf{y}_E^{(K)},D\right) + \epsilon_1 \quad (28)$$

In which $\epsilon_1 > 0$ goes to zero as $N \to \infty$ and D is defined as $D \triangleq \{\bar{\mathbf{d}}_{\ell,i}\}_{(\ell,i)}$. We have

$$\begin{aligned}
&\frac{1}{N} I(W_1,\ldots,W_K;\mathbf{y}_E|D) \leq \\
&\frac{1}{N} H(W_1,...,W_K|D) - \frac{1}{N} H(W_1,...,W_K|\mathbf{y}_E^{(1)},...,\mathbf{y}_E^{(K)},D) \\
&= \frac{1}{N} H(W_1,...,W_K) - \frac{1}{N} H(W_1,...,W_K|\mathbf{y}_E^{(1)},...,\mathbf{y}_E^{(K)},D) \\
&= \sum_{\ell=1}^{K} R_\ell - \frac{1}{N} H(W_1,...,W_K|\mathbf{y}_E^{(1)},...,\mathbf{y}_E^{(K)},D) \quad (29)
\end{aligned}$$

Next, we bound the second term in (29).

$$\begin{aligned}
&\frac{1}{N} H(W_1,\ldots,W_K|\mathbf{y}_E^{(1)},\ldots,\mathbf{y}_E^{(K)},D) \\
&= \frac{1}{N} H(W_1,...,W_K,\mathbf{y}_E^{(1)},...,\mathbf{y}_E^{(K)}|D) - \frac{1}{N} H(\mathbf{y}_E^{(1)},...,\mathbf{y}_E^{(K)}|D) \\
&\overset{(a)}{\geq} \frac{1}{N} H(\bar{\mathbf{t}}_{1,2},\ldots,\bar{\mathbf{t}}_{\ell-1,\ell},\bar{\mathbf{t}}_{\ell+1,\ell},\ldots,\bar{\mathbf{t}}_{K,K-1},\mathbf{y}_E^{(1)},\ldots,\mathbf{y}_E^{(K)}|D) \\
&- \frac{1}{N} H(\mathbf{y}_E^{(1)},\ldots,\mathbf{y}_E^{(K)}|D) \\
&- \frac{1}{N} H(\bar{\mathbf{t}}_{1,2},...,\bar{\mathbf{t}}_{\ell-1,\ell},\bar{\mathbf{t}}_{\ell+1,\ell},...,\bar{\mathbf{t}}_{K,K-1}|\mathbf{y}_E^{(1)},...,\mathbf{y}_E^{(K)},W_1,...,W_K,D) \\
&\overset{(b)}{\geq} \frac{1}{N} H(\bar{\mathbf{t}}_{1,2},...,\bar{\mathbf{t}}_{\ell-1,\ell},\bar{\mathbf{t}}_{\ell+1,\ell},...,\bar{\mathbf{t}}_{K,K-1},\mathbf{y}_E^{(1)},...,\mathbf{y}_E^{(K)}|D) \\
&- \frac{1}{N} H(\mathbf{y}_E^{(1)},\ldots,\mathbf{y}_E^{(K)}|D) - 2\epsilon_2 \\
&\overset{(c)}{=} \frac{1}{N} H(\bar{\mathbf{t}}_{1,2},...,\bar{\mathbf{t}}_{K,K-1}) - \frac{1}{N} H(\mathbf{y}_E^{(1)},...,\mathbf{y}_E^{(K)}|D) - 2\epsilon_2 \\
&+ \frac{1}{N} H(\mathbf{y}_E^{(1)},\ldots,\mathbf{y}_E^{(K)}|D,\bar{\mathbf{t}}_{1,2},\ldots,\bar{\mathbf{t}}_{K,K-1}) \quad (30)
\end{aligned}$$

Where inequality (a) comes from the chain rule. Note that in the sequence of $\bar{\mathbf{t}}_{1,2},\ldots,\bar{\mathbf{t}}_{K,K-1}$, the indices $i = \ell$ are excluded. Soundness of inequality (b) is shown in Lemma 1 in Appendix. In short, it comes from applying Packing Lemma to the outer codewords which have a random i.i.d. structure. Equality (c) is due to chain rule.

By substituting (30) into (29), we get

$$\begin{aligned}
&\frac{1}{N} I(W_1,\ldots,W_K;\mathbf{y}_E|D) \leq \\
&\frac{1}{N} H\left(\bar{\mathbf{t}}_{1,1},...,\bar{\mathbf{t}}_{K,K}|\mathbf{y}_E^{(1)},...,\mathbf{y}_E^{(K)},D\right) - \frac{1}{N} H(\bar{\mathbf{t}}_{1,2},...,\bar{\mathbf{t}}_{K,K-1}) \\
&+ \frac{1}{N} H(\mathbf{y}_E^{(1)},...,\mathbf{y}_E^{(K)}|D) - \frac{1}{N} H(\mathbf{y}_E^{(1)},...,\mathbf{y}_E^{(K)}|D,\bar{\mathbf{t}}_{1,2},...,\bar{\mathbf{t}}_{K,K-1}) \\
&+ 2\epsilon_2 + \epsilon_1 \\
&= \frac{1}{N} H(\bar{\mathbf{t}}_{1,2},...,\bar{\mathbf{t}}_{K,K-1},\mathbf{y}_E^{(1)},...,\mathbf{y}_E^{(K)}|D) \\
&- \frac{1}{N} H(\bar{\mathbf{t}}_{1,2},\ldots,\bar{\mathbf{t}}_{K,K-1},\mathbf{y}_E^{(1)},\ldots,\mathbf{y}_E^{(K)}|D) + 2\epsilon_2 + \epsilon_1 \\
&= 2\epsilon_2 + \epsilon_1 \quad (31)
\end{aligned}$$

In which ϵ_2 and ϵ_1 tend to zero for sufficiently large N. Therefore, the sum secure rate in (28) provides weak secrecy; thus any sum secure rate satisfying

$$\sum_{\ell=1}^{K} R_\ell \leq \frac{1}{N} H\left(\bar{\mathbf{t}}_{1,1},\ldots,\bar{\mathbf{t}}_{K,K}|\mathbf{y}_E^{(1)},\ldots,\mathbf{y}_E^{(K)},D\right) + \epsilon_1 \quad (32)$$

is also achievable with weak secrecy. Hence, we only need to show that the sum secure rate in (4) is a lower bound on (28). We have

$$\begin{aligned}
&\frac{1}{N} H\left(\bar{\mathbf{t}}_{1,1},\ldots,\bar{\mathbf{t}}_{K,K}|\mathbf{y}_E^{(1)},\ldots,\mathbf{y}_E^{(K)},D\right) + \epsilon_1 \\
&\geq \frac{1}{N} H(\bar{\mathbf{t}}_{1,1},...,\bar{\mathbf{t}}_{K,K}) - \frac{1}{N} H\left(\mathbf{y}_E^{(1)},...,\mathbf{y}_E^{(K)}|D\right) + \epsilon_1 \\
&= \frac{1}{N} H\left(\bar{\mathbf{t}}_{1,2},\ldots,\bar{\mathbf{t}}_{K,K-1}\right) + \frac{1}{N} \sum_{\ell=1}^{K} H\left(\bar{\mathbf{t}}_{\ell,\ell}\right) \\
&- \frac{1}{N} H\left(\mathbf{y}_E^{(1)},\ldots,\mathbf{y}_E^{(K)}|D\right) + \epsilon_1 \\
&= \sum_{k=2}^{K(K-1)+1} R_{comb,k} + \frac{1}{N} \sum_{\ell=1}^{K} H(\bar{\mathbf{t}}_{\ell,\ell}) \quad (33) \\
&- \frac{1}{N} H\left(\mathbf{y}_E^{(1)},\ldots,\mathbf{y}_E^{(K)}|D\right) + \epsilon_1 \quad (34)
\end{aligned}$$

Next, we bound the first term in (34). We have

$$\begin{aligned}
&\frac{1}{N} H(\mathbf{y}_E^{(1)},\ldots,\mathbf{y}_E^{(K)}|D) \leq \sum_{\ell=1}^{K} \frac{1}{N} H(\mathbf{y}_E^{(\ell)}|D) \\
&= \frac{1}{N} \sum_{\ell=1}^{K} H\left(\left[\mathbf{y}_E^{(\ell)}\right] \bmod \Lambda_{(\ell,\ell)}, Q_{\Lambda_{(\ell,\ell)}}(\mathbf{y}_E^{(\ell)})|D\right) \\
&\leq \frac{1}{N} \sum_{\ell=1}^{K} H\left(\left[\mathbf{y}_E^{(\ell)}\right] \bmod \Lambda_{(\ell,\ell)}|\bar{\mathbf{d}}_{\ell,\ell}, D\backslash\{\bar{\mathbf{d}}_{\ell,\ell}\}\right) \\
&+ \frac{1}{N} \sum_{\ell=1}^{K} H\left(Q_{\Lambda_{(\ell,\ell)}}(\mathbf{y}_E^{(\ell)})\right)
\end{aligned}$$

$$
\begin{aligned}
&=\frac{1}{N}\sum_{\ell=1}^{K} H\left(\left[\bar{\mathbf{t}}_{\ell,\ell}+\sum_{j\neq\ell}[\bar{\mathbf{t}}_{j,\ell}+\bar{\mathbf{d}}_{j,\ell}] \bmod \Lambda_{(j,\ell)}\right] \bmod \Lambda_{(\ell,\ell)}\middle| D\right)\\
&+\frac{1}{N}\sum_{\ell=1}^{K} H\left(Q_{\Lambda_{(\ell,\ell)}}(\mathbf{y}_E^{(\ell)})\right)\\
&=\frac{1}{N}\sum_{\ell=1}^{K} H\left(\left[\bar{\mathbf{t}}_{\ell,\ell}+\sum_{j\neq\ell}\bar{\mathbf{t}}_{j,\ell}-\sum_{j\neq\ell}Q_{\Lambda_{(j,\ell)}}(\bar{\mathbf{t}}_{j,\ell}+\bar{\mathbf{d}}_{j,\ell})\right] \bmod \Lambda_{(\ell,\ell)}\middle| D\right)\\
&+\frac{1}{N}\sum_{\ell=1}^{K} H\left(Q_{\Lambda_{(\ell,\ell)}}(\mathbf{y}_E^{(\ell)})\right)\\
&\overset{(d)}{=}\frac{1}{N}\sum_{\ell=1}^{K} H\left([\bar{\mathbf{t}}_{\ell,\ell}+\bar{\mathbf{q}}_\ell] \bmod \Lambda_{(\ell,\ell)}\right)+\frac{1}{N}\sum_{\ell=1}^{K} H\left(Q_{\Lambda_{(\ell,\ell)}}(\mathbf{y}_E^{(\ell)})\right)\\
&\overset{(e)}{=}\frac{1}{N}\sum_{\ell=1}^{K} H\left([\bar{\mathbf{t}}_{\ell,\ell}] \bmod \Lambda_{(\ell,\ell)}\right)+\frac{1}{N}\sum_{\ell=1}^{K} H\left(Q_{\Lambda_{(\ell,\ell)}}(\mathbf{y}_E^{(\ell)})\right)\\
&=\frac{1}{N}\sum_{\ell=1}^{K} H(\bar{\mathbf{t}}_{\ell,\ell})+\frac{1}{N}\sum_{\ell=1}^{K} H\left(Q_{\Lambda_{(\ell,\ell)}}(\mathbf{y}_E^{(\ell)})\right)\\
&\overset{(f)}{\leq}\frac{1}{N}\sum_{\ell=1}^{K} H(\bar{\mathbf{t}}_{\ell,\ell})\\
&+\frac{1}{2}\sum_{\ell=1}^{K}\log\left(\frac{\sum_{j=1,j\neq\ell}^{K}\gamma_{j,\ell}^2 P_{j,\ell}+\gamma_{\ell,\ell}^2 P_{\ell,\ell}}{\gamma_{\ell,\ell}^2 P_{\ell,\ell}}\right)+\delta(\epsilon) \qquad (35)
\end{aligned}
$$

Where in equality (d), the random vector $\bar{\mathbf{q}}_\ell$ has been defined as

$$
\bar{\mathbf{q}}_\ell \triangleq \left[\sum_{j\neq\ell}\bar{\mathbf{t}}_{j,\ell}-\sum_{j\neq\ell}Q_{\Lambda_{(j,\ell)}}(\bar{\mathbf{t}}_{j,\ell}+\bar{\mathbf{d}}_{j,\ell})\right] \bmod \Lambda_{(\ell,\ell)} \qquad (36)
$$

Furthermore, equality (e) comes from conditions in (10) along with the Crypto Lemma [Lemma 2, [10]] in which the compact group satisfying in the lemma's conditions is the set $\mathcal{L}_{\ell,\ell}=\Lambda_{f(,\ell,\ell)}\cap\mathcal{V}_{(\ell,\ell)}$. Lastly, inequality (f) is deduced from Lemma 1 in [8]. Here $\gamma_{j,i}$ is defined as in (5) and (6).

Consequently, expressions (33), (34), and (35) yield

$$
\begin{aligned}
&\frac{1}{N}H\left(\bar{\mathbf{t}}_{1,1},\ldots,\bar{\mathbf{t}}_{K,K}\middle|\mathbf{y}_E^{(1)},\ldots,\mathbf{y}_E^{(K)},D\right)+\epsilon_1\\
&\geq \sum_{k=2}^{K(K-1)+1} R_{comb,k}\\
&-\frac{1}{2}\sum_{\ell=1}^{K}\log\left(\frac{\sum_{j=1,j\neq\ell}^{K}\gamma_{j,\ell}^2 P_{j,\ell}+\gamma_{\ell,\ell}^2 P_{\ell,\ell}}{\gamma_{\ell,\ell}^2 P_{\ell,\ell}}\right)-\delta(\epsilon)+\epsilon_1
\end{aligned}
$$

In which ϵ_1 and $\delta(\epsilon)$ tend to zero for sufficiently large N. This completes the proof of weak secrecy of Theorem 1. ■

V. Simulation Results

In this section, we evaluate the performance of our proposed scheme numerically. To this end, we compute our achievable results with and without security for a three-user Gaussian wiretap MAC and then compare the achievable sum secure rate with the result implied by i.i.d. Gaussian random codes in [5] as well as the result in [8]. Furthermore, we show experimentally that our achievable sum rate, i.e., $\sum_{k=1}^{K(K-1)+1} R_{comb,k}$ reaches Gaussian MAC capacity in high-SNR regimes.

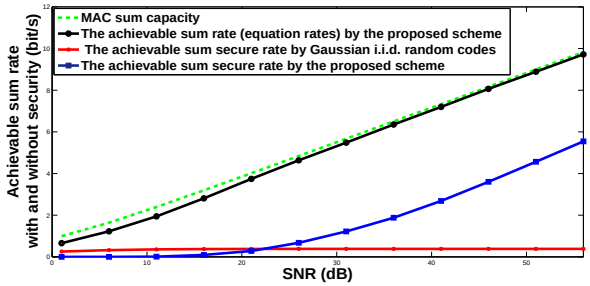

Fig. 3: Achievable sum rate, with and without security evaluated for a three-user Gaussian wiretap MAC at different SNR.

In the first experiment, we compare our sum secure rate with the one achieved by i.i.d. Gaussian random codes. To this end, we have considered a Three-user GW-MAC in which the channel gain vectors, $\mathbf{h}$, $\mathbf{g}$, were chosen as realizations of i.i.d. normal distributions. The simulation was run for 1000 instances and the average sum rates are shown as a function of SNR in Figure 3.

For simplicity, in implementing the achievable result of our scheme, we allocated powers among sub-message codewords equally, i.e., for $\ell\in\{1,\ldots,K\}$ we set $P_{\ell,i}=\frac{P}{K},\forall\ i$. Due to this simplification, the sum secure rate displayed as our achievable result in Figure 3 and Figure 4 are lower bounds on the highest sum secure rate that can be achieved by (4). Also, similar to [6], we have approximated the best integer coefficient vectors $\mathbf{a}^{(k)}$ for all equations using the LLL reduction algorithm which forms a set of $K(K-1)+1$ linearly independent lattice vectors [11].

A comparison between the curve displayed as our achievable sum secure rate and the one related to the achievable sum secure rate offered by i.i.d. Gaussian random codes reveals the advantage of our scheme versus pure random coding in moderate and high SNR regimes. Moreover, to shed light on the performance of our decoding strategy, we plotted the sum of the integer combinations rates, i.e., $\sum_k R_{comb,k}$ as well. As it can be seen, our achievable sum rate (without security) reaches Gaussian MAC capacity in the high SNR regimes. Recall that the compute-and-forward decoding strategy in [6] offers a lower bound on sum rate that achieves MAC sum capacity within a constant gap. Figure 3 shows numerically that our extension to their decoding strategy yields the same performance in terms of the achievable sum rate without security.

Also, Figure 4 illustrates the advantage of our new scheme over the one in [8]. The improvement can be clearly seen in high SNR regimes. This result is expected as the sum secure degrees of freedom achieved by our new scheme is higher than the one achieved by [8]. Note that due to the sub-optimal power allocation considered in the numerical implementation, the red curve displayed in Figure 4 is a lower bound on the maximum sum secure rate that can be achieved by our proposed scheme. Therefore, given the fact

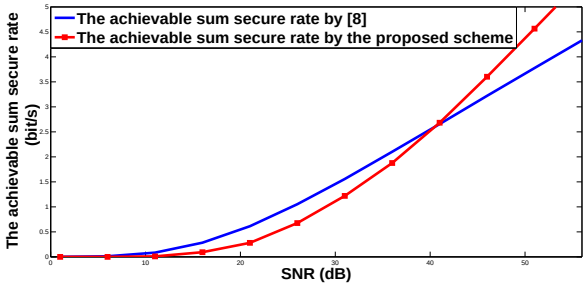

Fig. 4: Achievable sum secure rate for a three-user Gaussian wiretap MAC at different SNR.

that the average slope of the red curve is much bigger than for the blue curve, our achievable sum secure rate under the optimal power allocation crosses the blue curve at lower SNR values. Furthermore, the location of the crossing point is also dependent on the number of users.

VI. Conclusion

In this work, we considered the K-user Gaussian wiretap multiple-access channel. We developed a new scheme based on an extension of the compute-and-forward decoding strategy, nested lattice structure, and cooperative jamming. Our scheme consists of two layers: the inner layer which is the nested lattice coding structure and the outer layer which is the random coding. In short, our scheme achieves weak secrecy by means of three factors including proper lattice alignment, cooperative jamming signals, and i.i.d. repetitions of lattice codebook. Note that the latter has been added only to prove weak secrecy for the finite-SNR regime. Furthermore, we derived a new lower bound on sum secure rate for the finite-SNR regime based on our scheme and showed that it achieves the optimal sum secure degrees of freedom.

Acknowledgment

The authors would like to thank Bobak Nazer and Prakash Ishwar for their valuable comments and helpful discussions.

References

[1] J. Korner and K. Marton, "How to encode the modulo-two sum of binary sources (corresp.)," *IEEE Transactions on Information Theory*, vol. 25, no. 2, pp. 219–221, 1979.

[2] 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.

[3] 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.

[4] 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.

[5] E. Tekin and A. Yener, "The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[6] 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.

[7] 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.

[8] P. Babaheidarian and S. Salimi, "Compute-and-forward can buy secrecy cheap," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT 2015)*, Hong Kong, June 2015.

[9] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J*, vol. 54, no. 8, pp. 1355–1387, 1975.

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

[12] D. A. Harville, *Matrix algebra from a statistician's perspective*, vol. 1. Springer, 1997.

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

VII. Appendix

A. Proof of Corollary 1

We begin the proof by showing that $\sum_{k=1}^{K(K-1)+1} R_{comb,k}$ scales with $\log(P)$. We have

$$\begin{aligned}
&\sum_{k=1}^{K(K-1)+1} R_{comb,k} = \sum_{k=1}^{K(K-1)+1} \frac{1}{2}\log\left(\frac{\Gamma(k,k)^2 P}{\|\mathbf{F}.\mathbf{a}^{(k)}\|^2}\right)\\
&= \frac{K(K-1)+1}{2}\log(P) + \frac{1}{2}\log\left(\prod_k \Gamma(k,k)^2\right)\\
&-\frac{1}{2}\log\left(\prod_k \|\mathbf{F}.\mathbf{a}^{(k)}\|^2\right)\\
&\overset{(a)}{\geq} \frac{K(K-1)+1}{2}\log(P) + \frac{1}{2}\log\left(\prod_k \Gamma(k,k)^2\right)\\
&-\frac{1}{2}\log\left((K(K-1)+1)^{(K(K-1)+1)}.|\det(\mathbf{F})|^2\right)\\
&= \frac{K(K-1)+1}{2}\log(P) + \frac{1}{2}\log\left(\prod_k \Gamma(k,k)^2\right)\\
&-(K(K-1)+1)\frac{1}{2}\log\left(K(K-1)+1\right)\\
&-\frac{1}{2}\log\left(\prod_k \Gamma(k,k)^2\right) - \frac{1}{2}\log\left(\det\left(\frac{1}{P}\Gamma^{-2} + \tilde{\mathbf{h}}\tilde{\mathbf{h}}^T\right)\right)\\
&=\frac{K(K-1)+1}{2}\log(P)-(K(K-1)+1)\frac{1}{2}\log(K(K-1)+1)\\
&-\frac{1}{2}\log\left(\det\left(\Gamma^{-1}(\frac{1}{P}\mathbf{I} + \Gamma\tilde{\mathbf{h}}\tilde{\mathbf{h}}^T\Gamma)\Gamma^{-1}\right)\right)\\
&=\frac{K(K-1)+1}{2}\log(P)-(K(K-1)+1)\frac{1}{2}\log(K(K-1)+1)\\
&-\frac{1}{2}\log\left(\det\left(\Gamma^{-2}\right)\right) - \frac{1}{2}\log\left(\det\left(\frac{1}{P}\mathbf{I} + \Gamma\tilde{\mathbf{h}}\tilde{\mathbf{h}}^T\Gamma\right)\right)\\
&\overset{(b)}{=} \frac{K(K-1)+1}{2}\log(P) - \frac{1}{2}\log\left(\frac{P^{K(K-1)+1}}{1+\|\Gamma.\tilde{\mathbf{h}}\|^2 P}\right)\\
&-(K(K-1)+1)\frac{1}{2}\log\left(K(K-1)+1\right) - \frac{1}{2}\log\left(\det\left(\Gamma^{-2}\right)\right)\\
&=\frac{1}{2}\log\left(1+\|\Gamma.\tilde{\mathbf{h}}\|^2 P\right)-\frac{1}{2}\log\left(\det\left(\Gamma^{-2}\right)\right)\\
&-(K(K-1)+1)\frac{1}{2}\log\left(K(K-1)+1\right) \qquad (37)
\end{aligned}$$

In the above arguments, inequality (a) is concluded from Minkowski Theorem in [6] and equality (b) is the result of applying Sylvester's determinant identity (refer e.g. to [12]).

Note that from (37) two points can be deduced: First, our achievable sum rate (without security) is within a constant gap (with respect to P) from K-user MAC sum capacity[7] and second, $\sum_{k=1}^{K(K-1)+1} R_{comb,k} \propto \log(P)$. Now, using Corollary 5 in [6], for large enough P, we have

$$R_{comb,k} \leq \frac{1}{K(K-1)+1} \log(P) \quad \forall k \tag{38}$$

As a result, (37) and (38) together yield $\sum_{k=2}^{K(K-1)+1} R_{comb,k} \propto \log(P)$. This completes the proof of Corollary 1. ■

B. Proof of Corollary 2

We derive the sum secure degrees of freedom in two steps. In step one, we show that the limit of the first term in (4) when $P \to \infty$ is $\frac{K(K-1)}{K(K-1)+1}$. As it was mentioned earlier, the jamming codewords get aligned at the receiver's side and as a result, the receiver decodes $K(K-1)+1$ equations. This situation is equivalent to the multiple-access channel with $K(K-1)+1$ users in which user one has the highest rate of $R_{comb,1}$ and other users operate at rates equal to $R_{comb,k}$ for $\{2, \ldots, K(K-1)+1\}$. Thus, similar to the arguments in the proof of Corollary 1 and by using Corollary 5 in [6], we have

$$\limsup_{P\to\infty} \frac{R_{comb,k}}{\frac{1}{2}\log(1+P)} = \frac{1}{K(K-1)+1}, \quad \forall\ k \tag{39}$$

Therefore,

$$\limsup_{P\to\infty} \left(\sum_{k=2}^{K(K-1)+1} R_{comb,k} \right) = \frac{K(K-1)}{K(K-1)+1} \tag{40}$$

Next, we show that the second term in (4) is a constant with respect to the power P and hence it does not contribute to the sum secure degrees of freedom. To this end, let us consider a sub-optimal power allocation strategy in which user ℓ allocates its total power equally among its sub-codewords, i.e., $P_{\ell,i} = \frac{P}{K},\ \forall\ i \in \{1, \ldots, K\}$. Therefore, we have

$$\frac{\sum_{j=1, j\neq\ell}^{K} \gamma_{(j,\ell)}^2 P_{(j,\ell)} + \gamma_{(\ell,\ell)}^2 P_{\ell,\ell}}{\gamma_{(\ell,\ell)}^2 P_{\ell,\ell}} = \sum_{\substack{j=1 \\ j\neq\ell}}^{K} \frac{\gamma_{(j,\ell)}^2 + \gamma_{(\ell,\ell)}^2}{\gamma_{(\ell,\ell)}^2} \tag{41}$$

As a result, the second term in (4) is reduced to $\frac{1}{2}\sum_{\ell=1}^{K} \log\left(\sum_{\substack{j=1 \\ j\neq\ell}}^{K} \frac{\gamma_{(j,\ell)}^2 + \gamma_{(\ell,\ell)}^2}{\gamma_{(\ell,\ell)}^2} \right)$, which is a constant with respect to P, hence, the proof of Corollary 2 is completed. ■

C. Supplementary lemma

Lemma 1: For the achievable scheme presented in Section VII, we have

$$\frac{1}{nB} H(\bar{\mathbf{t}}_{1,2}, \ldots, \bar{\mathbf{t}}_{K,K-1} | W_1, \ldots, W_K, \mathbf{y}_E, D) \leq 2\epsilon_2, \tag{42}$$

where ϵ_2 goes to zero if B is taken large enough.

[7] To see this clearly, choose $\gamma_{\ell,i} = 1$ and $P_{\ell,i} = \frac{P}{K}$, for all i, ℓ.

Proof: We prove Lemma 1 by showing that

$$\frac{1}{nB} H(\bar{\mathbf{t}}_{1,1}, \bar{\mathbf{t}}_{1,2}, \ldots, \bar{\mathbf{t}}_{K,K} | W_1, \ldots, W_K, \mathbf{y}_E, D) \leq 2\epsilon_2 \tag{43}$$

Then, the correctness of Lemma 1 is automatically deduced.

Let us assume that for all $(\ell, i) \in \{1, \ldots, K\} \times \{1, \ldots, K\}$ each codeword $\bar{\mathbf{t}}_{\ell,i}$ is uniquely identified with two indices $(w_{\ell,i}, w'_{\ell,i})$. The corresponding index variable for $w_{\ell,i}$ is $W_{\ell,i},\ \forall i$. Also, assume that $H(w_{\ell,\ell}) = 0,\ \forall \ell$ and $H(\{w_{\ell,i}\}_{i=1, i\neq\ell}^{K}) = H(W_\ell)$. Assume that $1 \leq w_{\ell,i} \leq 2^{NR_{\ell,i}}$ and $1 \leq w'_{\ell,i} \leq 2^{NR'_{\ell,i}}$, where $N\sum_{(\ell,i)} R_{\ell,i} = N\sum_{\ell} R_\ell = H\left(\bar{\mathbf{t}}_{1,1}, \ldots, \bar{\mathbf{t}}_{K,K} \middle| \mathbf{y}_E^{(1)}, \ldots, \mathbf{y}_E^{(K)}, D\right) + N\epsilon_1$ and $N\sum_{(\ell,i)} R'_{\ell,i} = I\left(\bar{\mathbf{t}}_{1,1}, \ldots, \bar{\mathbf{t}}_{K,K}; \mathbf{y}_E^{(1)}, \ldots, \mathbf{y}_E^{(K)} \middle| D\right) - N\epsilon_1$, where $\epsilon_1 > 0$. Note that $N\sum_{(\ell,i)}(R'_{\ell,i} + R_{\ell,i}) = H(\bar{\mathbf{t}}_{1,1}, \ldots, \bar{\mathbf{t}}_{K,K}) = N\sum_{k=1}^{K(K-1)+1} R_{comb,k}$.

Having the bin indices $(w_1, \ldots, w_K)$, the eavesdropper needs to look for the transmitted codewords in the corresponding sub-codebooks $(\mathcal{C}_1(w_1), \ldots, \mathcal{C}_K(w_K))$. From the above setting, the number of codewords $\bar{\mathbf{t}}_{\ell,i}$ for the eavesdropper to check would be $2^{B\left(I\left(\mathbf{t}_{1,1},\ldots,\mathbf{t}_{K,K}; \mathbf{y}_{E,<n>}^{(1)},\ldots,\mathbf{y}_{E,<n>}^{(K)} \middle| \mathbf{d}_{1,1},\ldots,\mathbf{d}_{K,K}\right) - n\epsilon_1\right)}$, where the subscript $<n>$ denotes an n-length block of the corresponding random vector. Among these remaining codewords, the eavesdropper looks for those ones that satisfy in the following condition.

$$\left(\bar{\mathbf{t}}_{1,1},\ldots,\bar{\mathbf{t}}_{K,K},\mathbf{y}_E^{(1)},\ldots,\mathbf{y}_E^{(K)},D\right) \in \mathcal{T}_{\epsilon_2}^B\left(P_{\bar{\mathbf{t}}_{1,1},\ldots,\bar{\mathbf{t}}_{K,K},\mathbf{y}_E^{(1)},\ldots,\mathbf{y}_E^{(K)}|D}\right)$$

where $\mathcal{T}_{\epsilon_2}^B(P_{\bar{\mathbf{t}}_{1,1},\ldots,\bar{\mathbf{t}}_{K,K},\mathbf{y}_E^{(1)},\ldots,\mathbf{y}_E^{(K)}|D})$ is the set of ϵ_2-jointly typical sequences. Without loss of generality, let us assume that $\bar{\mathbf{t}}_{1,1} = \bar{\mathbf{t}}_{1,1}^*, \ldots, \bar{\mathbf{t}}_{K,K} = \bar{\mathbf{t}}_{K,K}^*$ are sent. For ease of notation, define $\bar{\mathbf{t}}_1^{*K} \triangleq (\bar{\mathbf{t}}_{1,1}^*, \ldots, \bar{\mathbf{t}}_{K,K}^*)$. Then, a decoding error would occur in either of the following two possible events.

$$\mathcal{E}_1 = \left\{ \left(\bar{\mathbf{t}}_1^{*K}, \mathbf{y}_E, \mathbf{d}_1^K\right) \notin \mathcal{T}_{\epsilon_2}^B(P_{\bar{\mathbf{t}}_1^K, \mathbf{y}_E|\mathbf{d}_1^K}) \right\}$$

$$\mathcal{E}_2 = \left\{ \exists \left(\bar{\mathbf{t}}_1^K, \mathbf{y}_E, D\right) \in \mathcal{T}_{\epsilon_2}^B(P_{\bar{\mathbf{t}}_1^K, \mathbf{y}_E|D}) : \right.$$
$$\left. \bar{\mathbf{t}}_1^K \neq \bar{\mathbf{t}}_1^{*K}, \mathbf{t}_\ell \in \mathcal{C}_\ell(w_\ell), \ell \in \{1, \ldots, K\} \right\}$$

By the AEP theorem, the first error event is bounded above by ϵ_2, and the second term can also be bounded by applying the Packing Lemma, [lemma 3.1, [13]] to codewords $\bar{\mathbf{t}}_{1,1}, \ldots, \bar{\mathbf{t}}_{K,K}$, i.e.,

$$\mathbb{P}\{\mathcal{E}_2\} \leq 2^{B\left(I\left(\mathbf{t}_{1,1},\ldots,\mathbf{t}_{K,K}; \mathbf{y}_{E,<n>}^{(1)},\ldots,\mathbf{y}_{E,<n>}^{(K)} \middle| \mathbf{d}_{1,1},\ldots,\mathbf{d}_{K,K}\right) - n\epsilon_1\right)}$$
$$\times 2^{-B\left(I\left(\mathbf{t}_{1,1},\ldots,\mathbf{t}_{K,K}; \mathbf{y}_{E,<n>}^{(1)},\ldots,\mathbf{y}_{E,<n>}^{(K)} \middle| \mathbf{d}_{1,1},\ldots,\mathbf{d}_{K,K}\right) - \delta(\epsilon_2)\right)}$$
$$\leq 2^{-B\left(n\epsilon_1 - \delta(\epsilon_2)\right)},$$

where $\delta(\epsilon_2)$ tends to zero as ϵ_2 goes to zero. Now, choose $n\epsilon_1 \geq \delta(\epsilon_2)$. Hence, for sufficiently large B, the total probability of the error events will be upper-bounded as $\mathrm{P}_e \leq 2\epsilon_2$. As a result, using Fano's inequality in [13], the correctness of (43) is concluded. ■