Compute-and-Forward Can Buy Secrecy Cheap

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

***Abstract*—We consider a Gaussian multiple access channel with K transmitters, a (intended) receiver and an external eavesdropper. The transmitters wish to reliably communicate with the receiver while concealing their messages from the eavesdropper. This scenario has been investigated in prior works using two different coding techniques; the random i.i.d. Gaussian coding and the signal alignment coding. Although, the latter offers promising results in a very high SNR regime, extending these results to the finite SNR regime is a challenging task. In this paper, we propose a new lattice alignment scheme based on the compute-and-forward decoding strategy which works at any finite SNR. We show that our achievable secure sum rate scales with $\log(\mathrm{SNR})$ and hence, in most SNR regimes, our scheme outperforms the random coding scheme in which the secure sum rate does not grow with the input power. Furthermore, we show that our obtained result matches the previous results in the infinite SNR regime.**

I. Introduction

Gaussian Multiple Access Channel (MAC) has been considered under different security scenarios. One interesting scenario is the K-user Gaussian MAC with an external eavesdropper in which the users wish to reliably send their messages to the receiver while keeping them hidden from the eavesdropper. This scenario has been investigated in [1] using the Gaussian i.i.d. random codes and while these codes achieve the capacity region of MAC without security, it has been shown that they have a poor performance in most SNR regimes when the security constraint is added. To overcome this issue, researchers have used the signal alignment technique in the K-user Gaussian wiretap MAC [2]- [3]. Their results show a significant improvement over the random coding result in a very high SNR regime. In fact, the scheme proposed in [3] achieves the optimal secure Degrees of Freedom (DoF) of the K-user Gaussian wiretap MAC. However, as these existing alignment schemes use a maximum-likelihood decoder, bounding the error probability of the decoder in the finite SNR regime is challenging and this limits their results to the high SNR regime.

In light of the lattice alignment technique, the compute-and-forward decoding strategy was proposed in [4] which can operate at any finite SNR. Recently, the K-user Gaussian MAC without security constraint has been investigated in [5] based on lattice coding and the compute-and-forward decoding strategy. The proposed scheme in [5] achieves the MAC sum capacity within a constant gap and for any finite SNR.

Motivated by the above arguments, we propose a new achievable scheme for the K-user Gaussian wiretap MAC in which lattice alignment is used along with the asymmetric compute-and-forward framework. We evaluate the performance of our proposed scheme both analytically and computationally for any finite SNR. We prove that our proposed scheme achieves a secure sum rate that scales with $\log(\mathrm{SNR})$, in contrast to the Gaussian random coding result which does not grow with SNR and therefore, it somehow fails at moderate and high SNR regime. Finally, we show that the asymptotic behavior of our proposed scheme agrees with the prior work's result in the high SNR regime [2].

The paper is organized as follows. In Section II, our setup preliminaries are described. Our main result is given in Section III along with the comparison to the prior works. In Section IV, the proof of the main result is presented. We conclude the paper in Section V. The proof of Lemma 1 used in Section IV is presented in Appendix.

II. Problem Statement

A K-user asymmetric (real) Gaussian wiretap multiple-access channel (MAC) consists of K transmitters, a receiver and an external eavesdropper. The relations between the channel inputs and outputs are given as

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

where $\mathbf{x}_\ell$ is an N-length channel input vector of user ℓ which satisfies the following power constraint.

$$\|\mathbf{x}_\ell\|^2\leq NP,\quad \forall\ell\in\{1,\dots,K\} \tag{2}$$

The vectors $\mathbf{y}$ and $\mathbf{y}_E$ in (1) are the receiver and the eavesdropper channel outputs, respectively. Also, $\mathbf{z}$ and $\mathbf{z}_E$ are the independent channel noises, each distributed i.i.d. according to $\mathcal{N}(0,1)$. Finally, vectors $\mathbf{h}\triangleq[h_1,\dots,h_K]^T$ and $\mathbf{g}\triangleq[g_1,\dots,g_K]^T$ are real-valued vectors representing the channel gains to the receiver and the eavesdropper, respectively. The channel model is illustrated in Fig. 1.

User ℓ encodes its confidential message W_ℓ, which is uniformly distributed over the set $\{1,\dots,2^{nR_\ell}\}$ and is independent of other users' messages, through some stochastic mapping $\mathcal{E}_\ell$, i.e., $\mathbf{x}_\ell=\mathcal{E}_\ell(W_\ell)$, for $\ell\in\{1,\dots,K\}$. There is also a decoder D at the receiver side which estimates the messages, i.e., $D(\mathbf{y})=\{\hat{W}_\ell\}_{\ell=1}^{K}$.

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

$$\Pr\left(\bigcup_{\ell=1}^{K}\{\hat{W}_\ell\neq W_\ell\}\right)<\epsilon, \tag{3}$$

and

$$\sum_{\ell=1}^{K}R_\ell\leq\frac{1}{N}H(W_1,W_2,\dots,W_K|\mathbf{y}_E)+\epsilon, \tag{4}$$

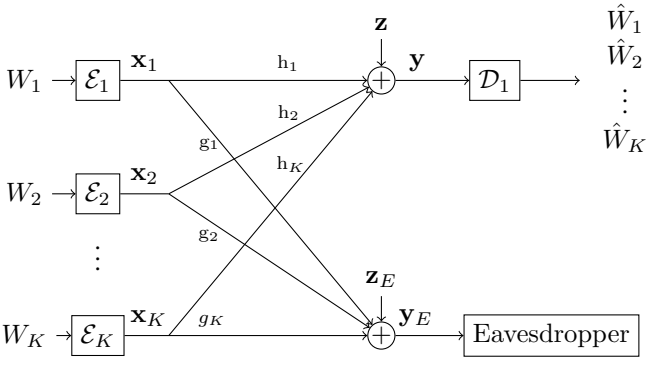

Fig. 1: The asymmetric Gaussian wiretap multiple-access channel model

where $\Pr$ denotes the probability of the event. The secret sum capacity is the supremum of all achievable secret sum rates.

III. Main Results

The problem described in Section (II) has been treated in the prior works in the infinite SNR regime. The idea is to directly bound the minimum distance between the lattice-codewords of the receiver's effective codebook. It is shown that by using this idea, the decoding error probability tends to zero, provided that the power goes to infinity [2], [3]. In this paper, we present a new scheme which provides a lower bound on the secure sum capacity for the same model and for any finite value of SNR. To this end, we utilize the compute-and-forward strategy presented in [4]. More precisely, we develop a coding scheme using an asymmetric compute-and-forward framework to address the asymmetric transmitter-eavesdropper channel gains. It is worth to mention that the asymmetric compute-and-forward framework is also treated in [6], but here we include the security concerns in the framework.

In the compute-and-forward decoding strategy, the receiver first decodes K linearly independent integer combinations of the transmitted lattice codewords and then, it solves for its desired lattice codewords. It decodes the equations successively, meaning that at each step k it cancels the effect of the $k-1$ previously decoded codewords from the current equation and solves it for the next codeword. The approach is similar to the Gaussian elimination with a difference that row switching is not allowed here. This limitation is due to the fact that a codeword cannot be eliminated from the current equation using another equation which has not been decoded yet. As a result, the order of canceling out the codewords cannot be chosen arbitrary, however, it can be shown that there exists at least one successive cancellation order such that all K codewords can be decoded [5].

Proposition 1: Assume that a permutation matrix π over indices $\{1,\dots,K\}$ defines a successive cancellation order in the compute-and-forward strategy. Also, assume the set of linearly independent K-length vectors $\{\mathbf{a}_1,\dots,\mathbf{a}_K\}$ be the integer coefficients used for estimating the linear combination equations. Then, for the channel model in Section II, the receiver can decode the message $W_\ell \in \{1,\dots,2^{nR_\ell}\}$ with a vanishing error probability if

$$R_\ell \le R_{comb,\pi(\ell)} \triangleq \max\left(\frac{1}{2}\log\left(\frac{\mathrm{SNR}_\ell}{\|\mathbf{F}\ \mathbf{a}_{\pi(\ell)}\|^2}\right),0\right), \quad (5)$$

where the matrix $\mathbf{F}$ is given as

$$\mathbf{F} \triangleq \left(\frac{1}{P}\mathbf{I}_{K\times K}+\mathbf{h}\mathbf{h}^T\right)^{\frac{-1}{2}} \times \mathrm{diag}\left(\sqrt{\frac{\mathrm{SNR}_1}{P}},\dots,\sqrt{\frac{\mathrm{SNR}_K}{P}}\right).$$

The notation $\mathrm{diag}(\mathbf{v})$ stands for the diagonal matrix built from the vector $\mathbf{v}$ and $\mathrm{SNR}_\ell > 0$ is a power used at encoder ℓ to generate its codewords. Notice that as long as the generated codewords are scaled properly before transmission, they would satisfy the channel input power constraint.[1]

Proposition 1 is immediately deduced from applying the Theorem 2 in [5] with an exception that, here, users operate at different powers.

In the following, we present a lower bound on the secure sum capacity achieved by the proposed scheme.

Theorem 1: A sequence of rates $(R_1,\dots,R_K)$ offers an achievable secure sum-rate for the K-user asymmetric Gaussian wiretap MAC, if they satisfy in the following constraints.

$$R_\ell \ge 0,\ R_\ell \le R_{comb,\pi(\ell)} \quad \forall \ell \in \{1,\dots,K\}, \quad (6)$$

$$\sum_{\ell=1}^{K} R_\ell \le \max_{\pi} R_{\mathbf{sum}}\ , \quad (7)$$

where

$$R_{\mathbf{sum}} = \left(\sum_{k=2}^{K} R_{comb,k} - \frac{1}{2}\log\left(\frac{\sum_{\ell=1}^{K} g_\ell^2}{g^2_{\pi^{-1}(1)}}\right)\right). \quad (8)$$

The maximum in (7) is taken over all the possible successive cancellation orders π and the notation $\pi^{-1}(.)$ simply denotes the inverse permutation operator.

Proof of Theorem 1 is given in Section IV.

A. Comparison to the prior works

The K-user Gaussian wiretap MAC has been investigated in [1] by means of i.i.d. Gaussian random coding. According to [1], for the considered channel model, the following secure sum rate is achievable.

$$\sum_{\ell=1}^{K} R_\ell \le \max\left(\frac{1}{2}\log\left(\frac{1+\|\mathbf{h}\|^2 P}{1+\|\mathbf{g}\|^2 P}\right),0\right). \quad (9)$$

Note that the right hand side of the expression (9) does not scale with power P, in other words, the asymptotic behavior of (9) tends to a constant rate for a fixed number of users and a given set of channel gains. In contrast, our achievable secure sum rate in (8) scales logarithmic with P. To prove this, we only need to show that the first term in (8) grows with $\log(P)$ as the second term is constant with respect to the power. Without loss of generality, let us assume $\mathrm{SNR}_\ell = \alpha_\ell P,\ \forall\ \ell$ and some $\alpha_\ell > 0$. Then we have,

[1]The scaling factors can be absorbed into the the channel gains.

$$\sum_{k=1}^{K} R_{comb,k}$$
$$\stackrel{a}{\geq} \frac{K}{2}\log(P) + \frac{1}{2}\sum_{k=1}^{K}\log(\alpha_k) - \frac{1}{2}\log(K^K|\det(\mathbf{F})|^2)$$
$$= \frac{K}{2}\log(P) + \frac{1}{2}\sum_{k=1}^{K}\log(\alpha_k) - \frac{K}{2}\left(\log(K)+\log(P)\right)$$
$$+\frac{1}{2}\log(1+\|\mathbf{h}\|^2P) - \frac{1}{2}\sum_{k=1}^{K}\log(\alpha_k)$$
$$= \frac{1}{2}\log(1+\|\mathbf{h}\|^2P) - \frac{K}{2}\log(K) \qquad (10)$$

where inequality (a) is deduced from Theorem 4 in [5]. Now, we exploit Theorem 12 in [5] in which it is shown that $R_{comb,k} < \frac{1+\delta(K-1)}{K+\delta(K-1)}\cdot\frac{1}{2}\log(P)+c,\ \forall\ k$, where the inequality holds for any $\delta > 0$ and some c constant with respect to P. Therefore, if we take $\delta \to 0$ and ignore the constant terms in (10), we have $\sum_{k=2}^{K} R_{comb,k} \propto \frac{1}{2}.\frac{K-1}{K}\log(P)$. As a result, the secure sum-rate in (8) grows with $\log(P)$.

The numerical results are given in Fig. 2 which is evaluated for the three-user channel and random i.i.d. (real) Gaussian channel gains. It can be seen that for the moderate and high SNR regimes, our proposed scheme outperforms the random coding result presented in [1]. Notice that the achievable non-secure results are shown in the figure as well which can be considered as an upper bound on the secure sum rate.

Another interesting observation occurs when the channel to the legitimate receiver is degraded with respect to the channel to the eavesdropper. For the Gaussian setting and the same noise power, this corresponds to the case $\|\mathbf{h}\| \leq \|\mathbf{g}\|$. In this case, according to the expression in (9), random-coding fails to achieve a positive secure sum rate, while, our scheme achieves a strictly positive secure sum rate, as long as the ratios $\frac{\mathbf{h}_\ell}{\mathbf{g}_\ell}$ are not rational.[2] To illustrate this observation, we ran an experiment on a two-user Gaussian wiretap-MAC with a fixed power (at SNR= 25dB) in which the channel gains are given as

$$\mathbf{h} = \left[1, \sqrt{2}\right]^T, \quad \mathbf{g} = \left[\sqrt{3}\cos(\theta), \sqrt{3}\sin(\theta)\right]^T, \qquad (11)$$

for some random θ uniformly distributed over $[0, 2\pi]$. This is an example of the case where $\|\mathbf{h}\| = \|\mathbf{g}\|$. Fig. 3 shows that as long as the ratios of $\frac{h_\ell}{g_\ell}$ are not rational, a positive secure sum-rate can be attained following our scheme.

At last, we investigate the asymptotic behavior of the expression (8). We show that our scheme achieves a total secure DoF of $\frac{K-1}{K}$. Earlier, to prove the scalability of (8) with $\log(P)$, we showed that the R_{sum} is proportional to $\frac{1}{2}.\frac{K-1}{K}\log(P)$, provided that the constant terms are ignored. Therefore,

$$\lim_{P\to\infty} \frac{R_{\text{sum}}}{\frac{1}{2}\log(1+P)} = \frac{K-1}{K}. \qquad (12)$$

Thus, the asymptotic behavior of the proposed scheme agrees with the result in [2]. In fact, we can further improve the presented scheme so that its asymptotic behavior reaches the optimal secure degrees of freedom given in [3]. The latter is aimed to be presented in the extended version.

[2]It can be shown that the Lebesgue measure of such rational ratios is small

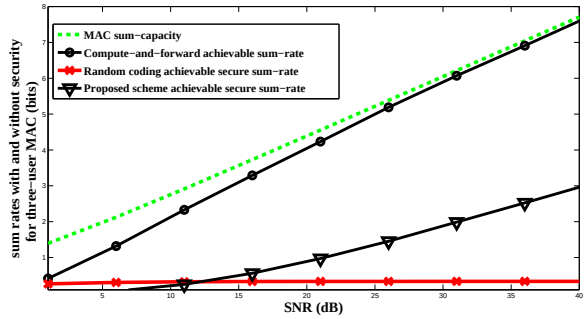

Fig. 2: Achievable sum-rate, with and without security evaluated for the three-user asymmetric Gaussian MAC at different SNR.

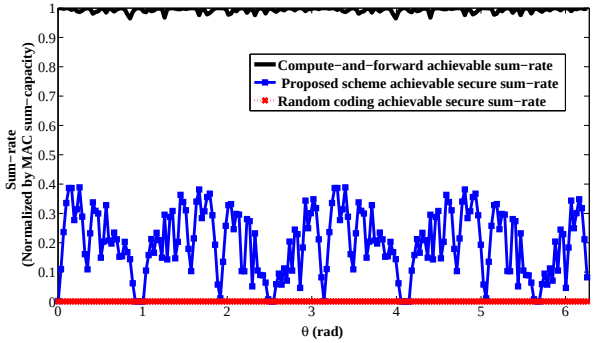

Fig. 3: Achievable sum-rate evaluated for the two-user asymmetric Gaussian wiretap MAC with channel gains given as in (11) at SNR=25 dB.

IV. Proof of Theorem 1

In this section, we use notions and properties related to the lattice coding and nested lattice structure which are originated and fully discussed in the seminal work by Erez and Zamir in [7]. Due to the space limitation, we avoid discussing the previously known results in this paper and we focus on the new results. The proposed scheme provides security by confusing the eavesdropper through aligning the codewords at the eavesdropper side so that it can only decode the subsets of the codewords which have the same sum values in $\mathbb{R}^N$. To this end, each encoded codeword $\tilde{\mathbf{x}}$ at transmitter ℓ is scaled by a factor of $\frac{1}{g_\ell}$, i.e., $\mathbf{x}_\ell = \frac{\tilde{\mathbf{x}}}{g_\ell}$ so that the eavesdropper receives the sum of the codewords $\tilde{\mathbf{x}}$ as its channel output, i.e., $\mathbf{y}_E = \sum_{\ell=1}^{K}\tilde{\mathbf{x}} + \mathbf{z}_E$. Consequently, user ℓ generates its codewords $\tilde{\mathbf{x}}$ using power of $\text{SNR}_\ell \triangleq g_\ell^2 P$ so that the transmitted codewords $\mathbf{x}_\ell$ satisfy the power constraint in (2).

As it was mentioned earlier, to address the problem of users with different powers, we utilize the asymmetric compute-and-forward framework along with a nested lattice structure. In our asymmetric compute-and-forward framework, user ℓ generates a sequence of n-length vectors $\mathbf{t}_\ell$ using a pair of fine and coarse lattice sets as $(\Lambda_{f,\ell}, \Lambda_\ell)$. The coarse lattice Λ_ℓ is scaled so that its second moment equals to the available power at user ℓ, i.e., $\text{SNR}_\ell = g_\ell^2 P$. Also, we impose a nested structure on the users' lattice pairs as

$$\Lambda \subseteq \Lambda_K \subseteq \Lambda_{K-1} \subseteq \cdots \subseteq \Lambda_1 \subseteq \Lambda_{f,K} \subseteq \cdots \subseteq \Lambda_{f,1} \qquad (13)$$

In the rest of the proof, we shall assume $\pi(\ell) = \ell$ in (8). If that is not the case, we can simply re-index the users' indices and define a nested structure as in (13) for the re-indexed users.

Each user ℓ constructs its codebook in three steps. The first step for user ℓ is to construct its inner codebook $\mathcal{L}_\ell \triangleq \Lambda_{f,\ell} \cap \mathcal{V}_\ell$, where $\mathcal{V}_\ell$ is the fundamental Voronoi region of the coarse lattice Λ_ℓ. The ratio between the coarse and the fine lattices is set such that $\mathcal{L}_\ell$ consists of $2^{nR_{comb,\ell}}$ inner codewords $\mathbf{t}_\ell$, i.e., $R_{comb,\ell} = \frac{1}{n}\log\left|\Lambda_{f,\ell} \cap \mathcal{V}_\ell\right|,\ \forall\ \ell$. The inner codewords $\mathbf{t}_\ell$ have a uniform distribution over $\mathcal{L}_\ell$.

In the second step, it builds the outer codebook by generating B i.i.d. copies of the inner codewords. Let us denote the outer codewords as $\bar{\mathbf{t}}_\ell$, then we have $\bar{\mathbf{t}}_\ell \triangleq [\mathbf{t}_\ell^{[1]}, \ldots, \mathbf{t}_\ell^{[B]}]$. Note that each $\mathbf{t}_\ell^{[i]}$ is independently distributed uniform over $\mathcal{L}_\ell$.

Finally, in the third step, the wiretap codebook is built. To this end, user ℓ partitions the outer codewords $\bar{\mathbf{t}}_\ell$ into 2^{NR_ℓ} equal-size bins and randomly assigns each index $w_\ell \in \{1, \ldots, 2^{NR_\ell}\}$ to exactly one bin. The rates R_ℓ are chosen such that they satisfy in (6) and $\sum_{\ell=1}^K R_\ell = \sum_{\ell=2}^K R_{comb,\ell} - \frac{1}{2}\log\left(\frac{\sum_\ell g_\ell^2}{g_1^2}\right) + \epsilon_1$, for some small $\epsilon_1 > 0$. Also, user ℓ has a random dither $\mathbf{d}_\ell^{[i]}$ for each block i, which is independently generated according to a uniform distribution over $\mathcal{V}_\ell$. Dithers are public and do not increase to secrecy.[3]

To send a message $W_\ell = w_\ell$, user ℓ picks randomly a codeword $\bar{\mathbf{t}}_\ell$ from the corresponding bin and dithers it. Then, it scales the resulting codeword by the factor of $\frac{1}{g_\ell}$. The signal transmitted by user ℓ is

$$\mathbf{x}_\ell \triangleq \frac{1}{g_\ell}\left(\left[\bar{\mathbf{t}}_\ell + \bar{\mathbf{d}}_\ell\right] \bmod \Lambda_\ell\right) \tag{14}$$

Note that in (14) the modular operation is done componentwise per each block i, i.e., for $i \in \{1, \ldots, B\}$, the signal transmitted at block i is $\frac{1}{g_\ell}\left(\left[\mathbf{t}_\ell^{[i]} + \mathbf{d}_\ell^{[i]}\right] \bmod \Lambda_\ell\right)$.

A. Proof of secrecy

In this subsection, we bound the eavesdropper's equivocation rate. Without loss of generality, let us assume $R_{comb,\ell} > 0,\ \forall\ \ell$. We have

$$\begin{aligned}
&\frac{1}{N}H(W_1, \ldots, W_K | \mathbf{y}_E, \bar{\mathbf{d}}_1, \ldots, \bar{\mathbf{d}}_K)\\
&\geq \frac{1}{N}H(\bar{\mathbf{t}}_1, \ldots, \bar{\mathbf{t}}_K | \mathbf{y}_E, \bar{\mathbf{d}}_1, \ldots, \bar{\mathbf{d}}_K)\\
&- \frac{1}{N}H(\bar{\mathbf{t}}_1, \ldots, \bar{\mathbf{t}}_K | W_1, \ldots, W_K, \mathbf{y}_E, \bar{\mathbf{d}}_1, \ldots, \bar{\mathbf{d}}_K)\\
&\overset{(a)}{\geq} \frac{1}{N}H(\bar{\mathbf{t}}_1, \ldots, \bar{\mathbf{t}}_K | \mathbf{y}_E, \bar{\mathbf{d}}_1, \ldots, \bar{\mathbf{d}}_K) - 2\epsilon_2\\
&\geq \frac{1}{N}H(\bar{\mathbf{t}}_1, \ldots, \bar{\mathbf{t}}_K | \mathbf{y}_E, \bar{\mathbf{d}}_1, \ldots, \bar{\mathbf{d}}_K, \mathbf{z}_E) - 2\epsilon_2\\
&\overset{(b)}{=} \frac{1}{N}H\left(\bar{\mathbf{t}}_1, \ldots, \bar{\mathbf{t}}_K \middle| \sum_{\ell=1}^K g_\ell \mathbf{x}_\ell, \bar{\mathbf{d}}_1, \ldots, \bar{\mathbf{d}}_K\right) - 2\epsilon_2\\
&\overset{(c)}{=} \frac{1}{N}H\left(\bar{\mathbf{t}}_1, \ldots, \bar{\mathbf{t}}_K \middle| \left[\sum_{\ell=1}^K \bar{\mathbf{t}}_\ell\right] \bmod \Lambda_1, \bar{\mathbf{u}}_1, \bar{\mathbf{d}}_1, \ldots, \bar{\mathbf{d}}_K\right) - 2\epsilon_2\\
&\overset{(d)}{=} \frac{1}{N}H\left(\bar{\mathbf{t}}_2, \ldots, \bar{\mathbf{t}}_K \middle| \left[\sum_{\ell=1}^K \bar{\mathbf{t}}_\ell\right] \bmod \Lambda_1, \bar{\mathbf{u}}_1, \bar{\mathbf{d}}_1, \ldots, \bar{\mathbf{d}}_K\right) - 2\epsilon_2\\
&\overset{(e)}{\geq} \frac{1}{N}H\left(\bar{\mathbf{t}}_2, \ldots, \bar{\mathbf{t}}_K \middle| \left[\sum_{\ell=1}^K \bar{\mathbf{t}}_\ell\right] \bmod \Lambda_1\right) - \frac{1}{N}H(\bar{\mathbf{u}}_1) - 2\epsilon_2\\
&\overset{(f)}{=} \frac{1}{N}H(\bar{\mathbf{t}}_2, \ldots, \bar{\mathbf{t}}_K) - \frac{1}{N}H(\bar{\mathbf{u}}_1) - 2\epsilon_2\\
&\overset{(g)}{=} \frac{B}{N}\sum_{\ell=2}^K nR_{comb,\ell} - \frac{B}{N}H(\mathbf{u}_1^{[1]}) - 2\epsilon_2\\
&\overset{(h)}{\geq} \sum_{\ell=2}^K R_{comb,\ell} - (1-\epsilon)\frac{1}{2}\log\left(\frac{\sum_{\ell=1}^K g_\ell^2 + \epsilon}{g_1^2}\right) - \delta(\epsilon) - 2\epsilon_2\\
&\geq \sum_{\ell=2}^K R_{comb,\ell} - \frac{1}{2}\log\left(\frac{\sum_{\ell=1}^K g_\ell^2}{g_1^2}\right) - \log(\frac{\epsilon}{g_1^2}) - \delta(\epsilon) - 2\epsilon_2\\
&\overset{(i)}{=} \sum_{\ell=2}^K R_{comb,\ell} - \frac{1}{2}\log\left(\frac{\sum_{\ell=1}^K g_\ell^2}{g_1^2}\right) - \epsilon_3.
\end{aligned} \tag{15}$$

In the above inequalities, (a) is deduced from applying the packing lemma to the outer codewords (detailed proof of this step is provided in Appendix). (b) is true since after subtracting the noise from $\mathbf{y}_E$, the remaining random vectors become independent of the noise. (c) is true as Λ_1 is the densest lattice among the lattices $(\Lambda_1, \Lambda_2, \ldots, \Lambda_K)$, according to the nested structure in (13). Therefore,

$$\left[\sum_{\ell=1}^K g_\ell \mathbf{x}_\ell - \sum_{\ell=1}^K \bar{\mathbf{d}}_\ell\right] \bmod \Lambda_1 = \left[\sum_{\ell=1}^K \bar{\mathbf{t}}_\ell\right] \bmod \Lambda_1.$$

Also, notice that

$$H\left(\sum_{\ell=1}^K g_\ell \mathbf{x}_\ell\right) = H\left(\left[\sum_{\ell=1}^K g_\ell \mathbf{x}_\ell\right] \bmod \Lambda_1, \bar{\mathbf{u}}_1\right),$$

where $\bar{\mathbf{u}}_1 \triangleq \sum_{\ell=1}^K g_\ell \mathbf{x}_\ell - \left[\sum_{\ell=1}^K g_\ell \mathbf{x}_\ell\right] \bmod \Lambda_1$. Inequality (d) is due to the reason that the codeword $\bar{\mathbf{t}}_1$ can be obtained from the modulo-sum $\left[\sum_{\ell=1}^K \bar{\mathbf{t}}_\ell\right] \bmod \Lambda_1$ and the sequence of codewords $\bar{\mathbf{t}}_2, \ldots, \bar{\mathbf{t}}_K$. (e) holds since dithers are independent of the codewords and condition reduces entropy. (f) comes from Lemma 2 in [8] (Crypto lemma), which implies that $\left[\mathbf{t}_1 + \sum_{\ell=2}^K \mathbf{t}_\ell\right] \bmod \Lambda_1$ has uniform distribution over the codebook $\mathcal{L}_1$ and is independent of $\sum_{\ell=2}^K \mathbf{t}_\ell$. (g) is true since $\left|\mathcal{L}_\ell\right| = 2^{nR_{comb,\ell}}$ and for $i \in \{1, \ldots, B\}$, inner codewords $\mathbf{t}_\ell^{[i]}$ has i.i.d. uniform distribution over $\mathcal{L}_\ell,\ \forall\ \ell$. Also, $\bar{\mathbf{u}}_1$ consists of B i.i.d. copies of $\mathbf{u}_1^{[i]}$. (h) follows from applying Lemma 1 in Appendix to $\mathbf{u}_1^{[1]}$, and finally, (i) is deduced by defining $\epsilon_3 \triangleq \delta(\epsilon) + \log(\frac{\epsilon}{g_1^2}) + 2\epsilon_2$. Thus, the condition in (4) is satisfied and the proof of secrecy is completed.

V. Conclusion

In this paper, we proposed a security scheme built on the asymmetric compute-and-forward framework, which works at

[3] As the average leakage rate (w.r.t. dithers) goes to zero, there must exists a sequence of deterministic dithers for which the leakage rate goes to zero.

any finite SNR. The achievable secure sum-rate presented by our scheme scales with $\log(\mathrm{SNR})$ and subsequently it significantly outperforms the existing random coding result for the most SNR regimes. The presented scheme also achieves a total secure DoF of $\frac{K-1}{K}$. This result can be furthered improved to achieve the optimal secure DoF which is aimed to be presented in our future work.

ACKNOWLEDGMENT

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

REFERENCES

[1] 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.

[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," Submitted September 2012, available online http://arxiv.org/abs/1209.5370.

[4] 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.

[5] O. Ordentlich, U. Erez, and B. Nazer, "The approximate sum capacity of the symmetric gaussian k-user interference channel," *IEEE Transactions on Information Theory*, To appear 2014, available online http://arxiv.org/abs/1206.0197.

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

[7] U. Erez and R. Zamir, "Achieving $\frac{1}{2}\log(1+\mathrm{SNR})$ on the AWGN channel with lattice encoding and decoding," *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2293–2314, 2004.

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

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

APPENDIX

Lemma 1: Consider a set of n-dimensional lattices $\Lambda_1,\ldots,\Lambda_K$ with their fundamental Voronoi regions as $\mathcal{V}_1,\ldots,\mathcal{V}_K$, respectively. Assume all the lattices are scaled such that their second moments equal to $\mathrm{SNR}_\ell = g_\ell^2 P,\ \forall\ \ell \in \{1,\ldots,K\}$, where $P>0$. Now construct random vectors $\mathbf{u}_j$, for $j\in\{1,\ldots,K\}$, as $\mathbf{u}_j \triangleq Q_{\Lambda_j}\left(\sum_{\ell=1}^K \mathbf{s}_\ell\right)$, where $\mathbf{s}_1,\ldots,\mathbf{s}_K$ are independent n-dimensional random vectors uniformly distributed over $\mathcal{V}_1,\ldots,\mathcal{V}_K$, respectively, and the operation $Q_{\Lambda_j}(.)$ is the nearest neighbor quantizer with respect to the lattice Λ_j. Then, for all $\epsilon>0$ and sufficiently large n, the entropy of $\mathbf{u}_j$ is bounded as

$$\frac{1}{n}H(\mathbf{u}_j) \le (1-\epsilon)\frac{1}{2}\log\left(\frac{\sum_{\ell=1}^K g_\ell^2+\epsilon}{g_j^2}\right)+\delta(\epsilon) \quad \forall j, \ (16)$$

where $\delta(\epsilon)$ tends to zero as $\epsilon\to 0$.

Proof: According to the definition of $\mathbf{u}_j$, it is the output of a quantizer Q_{Λ_j}, so it can only take discrete values. To bound the entropy of $\mathbf{u}_j$, first we bound the range of $\|\sum_{\ell=1}^K \mathbf{s}_\ell\|$ as follows. Let $r_{\mathrm{cov},\ell}$ denote the covering radius of Λ_ℓ, i.e., the radius of the smallest ball containing the Voronoi region $\mathcal{V}_\ell$. Also, let $r_{\mathrm{eff},\ell}$ denote the radius of the sphere which has the same volume as the volume of $\mathcal{V}_\ell$, i.e., $\mathrm{Vol}(B(r_{\mathrm{eff},\ell})) = \mathrm{Vol}(\mathcal{V}_\ell)$. Now, consider K (n-dimensional) balls whose second moments per dimension equal to $\sigma_1^2,\sigma_2^2,\ldots,\sigma_K^2$ and their radii are given as $r_{\mathrm{cov},1}, r_{\mathrm{cov},2},\ldots,r_{\mathrm{cov},K}$, respectively. Next, for each $\ell\in\{1,\ldots,K\}$, consider a random vector $\mathbf{b}_\ell$ with uniform distribution over an n-dimensional ball $B(r_{\mathrm{cov},\ell})$. Recall that a ball has the smallest normalized second moment for a given volume [7]. Therefore, we have

$$\begin{aligned} g_\ell^2 P &= \frac{1}{n}\mathbb{E}\|\mathbf{s}_\ell\|^2 \\ &\ge \frac{1}{n}\mathbb{E}\left\|\left(\frac{r_{\mathrm{eff},\ell}}{r_{\mathrm{cov},\ell}}\right)\mathbf{b}_\ell\right\|^2 = \left(\frac{r_{\mathrm{eff},\ell}}{r_{\mathrm{cov},\ell}}\right)^2\sigma_\ell^2,\ \forall\ \ell. \end{aligned} \quad (17)$$

Now, consider a random vector $\mathbf{z}_{eq} \triangleq \sum_{\ell=1}^K \mathbf{z}_\ell$, in which random vectors $\mathbf{z}_\ell$ are i.i.d. according to the distribution $\mathcal{N}(\mathbf{0},\sigma_\ell^2\mathbf{I})$, therefore, $\mathbf{z}_{eq}\sim\mathcal{N}(\mathbf{0},\sigma_{eq}^2\mathbf{I})$. Then, from (17) we have $\sigma^2_{\mathbf{z}_{eq}} = \sum_{\ell=1}^K\sigma_\ell^2 \le \sum_{\ell=1}^K\left(\frac{r_{\mathrm{cov},\ell}}{r_{\mathrm{eff},\ell}}\right)^2 g_\ell^2 P$. Now, using Lemma 11 in [7], we can conclude that

$$\begin{aligned} &e^{K.n.c(n)} f_{\mathbf{z}_{eq}}(\mathbf{z}_{eq}) = e^{K.n.c(n)}\left(f_{\mathbf{z}_1}(\mathbf{z}_{eq}) * \ldots * f_{\mathbf{z}_K}(\mathbf{z}_{eq})\right) \\ &\ge f_{\sum_{\ell=1}^K \mathbf{s}_\ell}(\mathbf{z}_{eq}). \end{aligned} \quad (18)$$

where $n.c(n)$ goes to zero as n goes to infinity. Notice that in deriving (18) we also used the fact that vectors $\mathbf{s}_\ell$ are independent vectors, and hence, pdf of their sum is the convolution of their individual pdfs. Now we are ready to bound the range of $\|\sum_{\ell=1}^K \mathbf{s}_\ell\|$ as follows. For any $\epsilon>0$,

$$\begin{aligned} &\Pr\left(\Big\|\sum_{\ell=1}^K \mathbf{s}_\ell\Big\| \notin B\left(\sqrt{n\sigma^2_{\mathbf{z}_{eq}}+n\epsilon}\right)\right) \\ &\overset{(a)}{\le} e^{K.n.c(n)}\Pr\left(\|\mathbf{z}_{eq}\| \notin B\left(\sqrt{n\sigma^2_{\mathbf{z}_{eq}}+n\epsilon}\right)\right) \le \epsilon \end{aligned}$$

Inequality (a) follows from (18) and non-negativity of the ℓ_2-norm. Also, the last inequality is deduced from the Weak Law of Large numbers (WLL) and for sufficiently large n. Since we showed $\|\sum_{\ell=1}^K \mathbf{s}_\ell\|$ belongs to the ball $B(\sqrt{n\sigma^2_{zeq}+n\epsilon})$ with probability $1-\epsilon$, it only remains to find an upper bound on the number of Voronoi regions $\mathcal{V}_j$ that can fit in this ball, i.e.,

$$\begin{aligned} &\frac{Vol\left(\mathcal{B}\left(\sqrt{n\sigma^2_{\mathbf{z}_{eq}}+n\epsilon}\right)\right)}{Vol\left(\mathcal{V}_j\right)} = \frac{Vol\left(\mathcal{B}\left(\sqrt{n\sigma^2_{\mathbf{z}_{eq}}+n\epsilon}\right)\right)}{Vol\left(B(r_{\mathrm{eff},j})\right)} \\ &\overset{(a)}{\le}\left(\frac{n\sigma^2_{\mathbf{z}_{eq}}+n\epsilon}{\left(\frac{r_{\mathrm{eff},j}}{r_{\mathrm{cov},j}}\right)^2 n g_j^2 P}\right)^{\frac{n}{2}} \overset{(b)}{\le}\left(\frac{\sum_{\ell=1}^K\left(\frac{r_{\mathrm{cov},\ell}}{r_{\mathrm{eff},\ell}}\right)^2 g_\ell^2+\epsilon}{\left(\frac{r_{\mathrm{eff},j}}{r_{\mathrm{cov},j}}\right)^2 g_j^2}\right)^{\frac{n}{2}} \end{aligned}$$

where inequality (a) is concluded from Lemma 6 in [7] and inequality (b) follows from (17). Finally, recall that for a high dimensional good lattices, we have $\log\left(\frac{r_{\mathrm{cov},\ell}}{r_{\mathrm{eff},\ell}}\right)\to 0$ [7]. Therefore,

$$\frac{1}{n}H(\mathbf{u}_j) \le (1-\epsilon)\frac{1}{2}\log\left(\frac{\sum_{\ell=1}^K g_\ell^2+\epsilon}{g_j^2}\right)+\delta(\epsilon).$$

Also, using WLL, the term $\delta(\epsilon)$ tends zero as n goes to infinity. This completes the proof. ■

Lemma 2: For the achievable scheme presented in Section VII, we have

$$\frac{1}{nB}H(\mathbf{t}_1,\ldots,\mathbf{t}_K|W_1,\ldots,W_K,\mathbf{y}_E,\mathbf{d}_1,\ldots,\mathbf{d}_K)\leq 2\epsilon_2, \tag{19}$$

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

Proof: Let us assume that each codeword $\bar{\mathbf{t}}_\ell$ is uniquely identified with two indices (w_ℓ, w'_ℓ). Assume that $1\leq w_\ell\leq 2^{NR_\ell}$ and $1\leq w'_\ell\leq 2^{NR'_\ell}$, where $n\sum_{\ell=1}^{K}R_\ell = H\left(\mathbf{t}_1^{[1]},\ldots,\mathbf{t}_K^{[1]}\middle|\mathbf{y}_E,\mathbf{d}_1^{[1]},\ldots,\mathbf{d}_K^{[1]}\right)+n\epsilon_1$ and $nR'_\ell = I\left(\mathbf{t}_1^{[1]},\ldots,\mathbf{t}_K^{[1]};\mathbf{y}_E\middle|\mathbf{d}_1^{[1]},\ldots,\mathbf{d}_K^{[1]}\right)-n\epsilon_1$, where $\epsilon_1>0$. Therefore, $n\sum_{\ell=1}^{K}(R_\ell+R'_\ell) = H(\mathbf{t}_1^{[1]},\ldots,\mathbf{t}_K^{[1]})$. Now, having the bin indices $(w_1,\ldots,w_K)$, the eavesdropper needs to look for the transmitted codewords in the corresponding sub-codebooks $(\mathcal{C}_1(w_1),\ldots,\mathcal{C}_K(w_K))$. In other words, the number of codewords for the eavesdropper to check would be

$$2^{B(I(\mathbf{t}_1^{[1]},\ldots,\mathbf{t}_K^{[1]};\mathbf{y}_E|\mathbf{d}_1^{[1]},\ldots,\mathbf{d}_K^{[1]})-n\epsilon_1)}. \tag{20}$$

Among these remaining codewords, the eavesdropper looks for those ones that satisfy in the following condition.

$$\left(\bar{\mathbf{t}}_1,...,\bar{\mathbf{t}}_K;\mathbf{y}_E,\bar{\mathbf{d}}_1,...,\bar{\mathbf{d}}_K\right)\in\mathcal{T}_{\epsilon_2}^{B}(P_{\bar{\mathbf{t}}_1,\ldots,\bar{\mathbf{t}}_K,\mathbf{y}_E|\bar{\mathbf{d}}_1,\ldots,\bar{\mathbf{d}}_K}), \tag{21}$$

where $\mathcal{T}_{\epsilon_2}^{B}(P_{\bar{\mathbf{t}}_1,\ldots,\bar{\mathbf{t}}_K,\mathbf{y}_E|\bar{\mathbf{d}}_1,\ldots,\bar{\mathbf{d}}_K})$ is the set of ϵ_2-jointly typical sequences.

Without loss of generality, let us assume that $(\bar{\mathbf{t}}_1,\ldots,\bar{\mathbf{t}}_K) = (\bar{\mathbf{t}}_1^*,\ldots,\bar{\mathbf{t}}_K^*)$ are sent. Then, a decoding error would occur in either of the following two possible events.

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

and

$$\mathcal{E}_2 = \Big\{\exists\left(\bar{\mathbf{t}}_1,\ldots,\bar{\mathbf{t}}_K;\mathbf{y}_E,\bar{\mathbf{d}}_1,\ldots,\bar{\mathbf{d}}_K\right)\in \mathcal{T}_{\epsilon_2}^{B}(P_{\bar{\mathbf{t}}_1,\ldots,\bar{\mathbf{t}}_K,\mathbf{y}_E|\bar{\mathbf{d}}_1,\ldots,\bar{\mathbf{d}}_K})\Big\},$$

such that

$$(\bar{\mathbf{t}}_1,\ldots,\bar{\mathbf{t}}_K)\neq(\bar{\mathbf{t}}_1^*,\ldots,\bar{\mathbf{t}}_K^*)$$

where the notation $\mathbf{t}_1^K$ is defined as before. 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 of [9]] to the codewords $\mathbf{t}_1,\ldots,\mathbf{t}_K$, i.e.,

$$\begin{aligned}&\mathbb{P}\{\mathcal{E}_2\}\\&\leq 2^{B(I(\mathbf{t}_1^{[1]},\ldots,\mathbf{t}_K^{[1]};\mathbf{y}_E|\mathbf{d}_1^{[1]},\ldots,\mathbf{d}_K^{[1]})-n\epsilon_1)}\\&\times 2^{-B\left(I(\mathbf{t}_1^{[1]},\ldots,\mathbf{t}_K^{[1]};\mathbf{y}_E|\mathbf{d}_1^{[1]},\ldots,\mathbf{d}_K^{[1]})-\delta(\epsilon_3)\right)}\\&\leq 2^{-B\left(n\epsilon_1-\delta(\epsilon_2)\right)},\end{aligned}$$

where $\delta(\epsilon_2)$ tends to zero as ϵ_2 goes to zero. Now, choose

$$n\epsilon_1\geq\delta(\epsilon_2), \tag{22}$$

Hence, we have

$$\mathbb{P}\{error\}\leq 2\epsilon_2 \tag{23}$$

■