ISIT'2013 1569719269

Lattice Coding for Strongly Secure Compute-and-Forward in a Bidirectional Relay

Shashank V. and Navin Kashyap
Dept. of Electrical Communication Engineering
Indian Institute of Science, Bangalore, India
Email: {shashank,nkashyap}@ece.iisc.ernet.in

***Abstract*—We study the problem of secure bidirectional relaying in the presence of an "honest but curious" relay. We consider the setting where all links between nodes are additive white Gaussian noise (AWGN) channels, and show that using nested lattice codes, it is possible to obtain strong secrecy. A randomized encoder based on probability mass functions obtained by sampling the Gaussian function is used, and we show that the mutual information between the secret messages and the vector received by the relay is arbitrarily small for large block lengths. We determine sufficient conditions for secure and reliable communication, and find achievable rates. We then extend the results to the case of secure relaying in a multi-hop network with $K+1$ hops.**

I. Introduction

Consider the bidirectional relay problem, where two nodes, A and B (called the user nodes) wish to exchange messages via an intermediate relay node, R. All nodes operate in the half-duplex mode, and all links between nodes are additive white Gaussian noise (AWGN) channels.

We will use the compute-and-forward protocol [13], [14] for this problem. In this protocol, communication takes place in two phases: the multiple-access phase and the broadcast phase. In the multiple-access phase, both user nodes encode their messages and simultaneously transmit to the relay. Let X (resp. Y) be the message possessed by user A (resp. B). The messages are independent, and uniformly distributed over the set of all messages, say $\mathbb{X}$. The encoder at node A (resp. B) stochastically maps the message X (resp. Y) into a d-dimensional real vector $\mathbf{u}$ (resp. $\mathbf{v}$), which is sent to the relay. The relay receives

$$\mathbf{w} = \mathbf{u} + \mathbf{v} + \mathbf{z}, \tag{1}$$

where $\mathbf{z}$ denotes independent zero-mean AWGN with variance σ^2. We assume that the channel gains from the user nodes to the relay are equal to 1, and the general case is left as future work. An average transmit power constraint of $\mathcal{P}$ is imposed on the user nodes, i.e.,

$$\frac{1}{d}\mathbb{E}\|\mathbf{u}\|^2 \le \mathcal{P}, \text{ and } \frac{1}{d}\mathbb{E}\|\mathbf{v}\|^2 \le \mathcal{P}, \tag{2}$$

the expectations being taken over $\mathbf{u}$ and $\mathbf{v}$, respectively. From $\mathbf{w}$, the relay R is required to compute $X \oplus Y$, for an appropriately chosen binary operator $\oplus$ on $\mathbb{X}$ which makes $\mathbb{X}$ a finite Abelian group. In the broadcast phase, R encodes $X \oplus Y$ into a d-dimensional real vector, and broadcasts it to the user nodes. Our focus for the rest of this paper lies exclusively on the multiple-access phase, and we will not consider the broadcast phase hereafter.

Our measure of secrecy at the relay is the mutual information between X (resp. Y) and $\mathbf{u}+\mathbf{v}$, i.e., $\mathcal{I}(X;\mathbf{u}+\mathbf{v})$ (resp. $\mathcal{I}(Y;\mathbf{u}+\mathbf{v})$), and we want to make this arbitrarily small as the number of channel uses increases. Note that since the noise $\mathbf{z}$ is independent of everything else, this also means that $\mathcal{I}(X;\mathbf{w})$ and $\mathcal{I}(Y;\mathbf{w})$ become arbitrarily small. This is referred to as *strong secrecy* in the literature [12].

The problem of secure bidirectional relaying was earlier studied in [7] under a *weak secrecy* constraint, where only the mutual information *rate*, $\frac{1}{d}\mathcal{I}(X;\mathbf{w})$, goes to zero. The results were extended to strong secrecy in [8], where it was shown that a rate of $\frac{1}{2}\log_2\left(\frac{1}{2}+\frac{\mathcal{P}}{\sigma^2}\right) - 1$ can be obtained with strong secrecy using nested lattice codes and universal hash functions.

We here propose a scheme that uses nested lattice codes and randomized encoding to achieve strong secrecy. For a given message, the user node transmits a lattice point at random, according to a probability mass function which is obtained by sampling and appropriately normalizing a Gaussian function, $e^{-\frac{\|\mathbf{u}\|^2}{2\mathcal{P}}}$. We will prove that such a scheme guarantees strong secrecy, and we will then study achievable rates. The novelty of our scheme is that given a pair of nested lattices, we specify exactly what probability mass function (pmf) is used to randomize at the encoder to achieve secure communication. We also show that the rate of convergence to zero of $\mathcal{I}(X;\mathbf{u}+\mathbf{v})$ and $\mathcal{I}(Y;\mathbf{u}+\mathbf{v})$ is exponential in d. A similar scheme was studied earlier in [9], [10], wherein a pmf obtained by sampling a density function having a compactly supported characteristic function was used. It was shown there that perfect secrecy, i.e., $\mathcal{I}(X;\mathbf{u}+\mathbf{v}) = \mathcal{I}(Y;\mathbf{u}+\mathbf{v}) = 0$, could be obtained. However, in that case, we were only able to achieve a transmission rate of $\frac{1}{2}\log_2\left(\frac{\mathcal{P}}{\sigma^2}\right) - \log_2(2e)$. Employing a signalling scheme that uses sampled Gaussians allows us to improve the achievable rate to $\frac{1}{2}\log_2\left(\frac{1}{2}+\frac{\mathcal{P}}{\sigma^2}\right) - \frac{1}{2}\log_2(2e)$. Sampled Gaussian functions have been previously used in the context of the wiretap channel [11], and we will make good use of the techniques developed there.

We also extend these results to the problem of relaying

messages in a multi-hop line network with $K+1$ hops, where the relays are independent, passive eavesdroppers. This problem was studied in [7], and achievable rates were found under a weak secrecy constraint. We use the same protocol as in [7], and show that strong secrecy can be achieved using our scheme. In comparison to [7], the transmission rates obtained using our scheme is lower by around 0.11 bits, but we obtain strong secrecy.

The paper is organized as follows. In Section II, we describe our coding scheme, and state the main result (Theorem 1) for the bidirectional relay. The theorem is proved in Section III, with some of the details given in an appendix. Finally, in Section IV, we extend the results to the multi-hop scenario.

II. Coding scheme

We first establish some notation. The set of real numbers and the set of integers are denoted by $\mathbb{R}$ and $\mathbb{Z}$, respectively. For a d-dimensional real vector $\mathbf{x}$, the ℓ^2 norm of $\mathbf{x}$ is denoted by $\|\mathbf{x}\|$. If X is a random variable, then $\mathbb{E}[X]$ denotes the expected value of X.

Let $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ be a set of k linearly independent vectors in $\mathbb{R}^d$. The set of all integer-linear combinations of the $\mathbf{v}_i$'s is called a lattice in $\mathbb{R}^d$ [2], and k is called the rank of the lattice. In this work, we will consider only full-rank lattices, i.e., $k=d$. For any $\mathbf{x}, \mathbf{z} \in \mathbb{R}^d$, and real $\kappa > 0$, we define

$$f_{\kappa,\mathbf{x}}(\mathbf{z}) := \frac{1}{\left(\sqrt{2\pi}\kappa\right)^d} e^{-\frac{\|\mathbf{z}-\mathbf{x}\|^2}{2\kappa^2}}, \tag{3}$$

and for any lattice Λ in $\mathbb{R}^d$,

$$f_{\kappa,\mathbf{x}}(\Lambda) := \sum_{\lambda\in\Lambda} f_{\kappa,\mathbf{x}}(\lambda). \tag{4}$$

For ease of notation, $f_\kappa(\mathbf{z})$ will mean $f_{\kappa,\mathbf{0}}(\mathbf{z})$, and $f_\kappa(\Lambda)$ will mean $f_{\kappa,\mathbf{0}}(\Lambda)$.

The coding scheme used in the sequel is described below:

Code: We use a $(\Lambda^{(d)}, \Lambda_0^{(d)})$ nested lattice code. It consists of a pair of full-rank nested lattices, $\Lambda^{(d)}$ and $\Lambda_0^{(d)}$, with $\Lambda_0^{(d)} \subseteq \Lambda^{(d)} \subseteq \mathbb{R}^d$. The lattice $\Lambda_0^{(d)}$ is called the coarse lattice, and $\Lambda^{(d)}$ is called the fine lattice. The messages are chosen from the quotient group, $\mathbb{G}^{(d)} := \Lambda^{(d)}/\Lambda_0^{(d)}$, and $\oplus$ will be the addition operation on $\mathbb{G}^{(d)}$.

Encoding: Let $\mathcal{V}(\Lambda_0^{(d)})$ denote the fundamental Voronoi region[1] of $\Lambda_0^{(d)}$. For any coset Λ_j in $\Lambda^{(d)}/\Lambda_0^{(d)}$, we can choose a unique representative lattice point for Λ_j from $\Lambda^{(d)} \cap \mathcal{V}(\Lambda_0^{(d)})$. Call this λ_j. Observe that $\Lambda_j = \Lambda_0^{(d)} + \lambda_j := \{\lambda + \lambda_j : \lambda \in \Lambda_0^{(d)}\}$. Fix a $\kappa > 0$. If node A possesses message (coset) Λ_j, then it transmits a random lattice point, $\mathbf{u}$, chosen from the coset Λ_j according to the pmf

$$p_j(\mathbf{u}) = \begin{cases} \frac{f_\kappa(\mathbf{u})}{f_{\kappa,-\lambda_j}(\Lambda_0^{(d)})}, & \text{if } \mathbf{u} \in \Lambda_0^{(d)} + \lambda_j \\ \mathbf{0}, & \text{otherwise.} \end{cases} \tag{5}$$

[1]For a lattice Λ in $\mathbb{R}^d$, and any $\mathbf{x} \in \mathbb{R}^d$, let $Q_\Lambda(\mathbf{x}) = \arg\min_{\lambda\in\Lambda}\|\mathbf{x}-\lambda\|$ be the map that sends $\mathbf{x}$ to the closest lattice point. Then, the fundamental Voronoi region of Λ is the set $\{\mathbf{x} \in \mathbb{R}^d : Q_\Lambda(\mathbf{x}) = \mathbf{0}\}$.

Similarly, if node B possesses message Λ_k, then it transmits a random lattice point according to $p_k(\mathbf{v})$.

Decoding: The relay uses a lattice decoder. Let $\mathbf{w}$, given by (1), be the vector received by R. Then, the relay estimates $\Lambda_j \oplus \Lambda_k$ to be coset represented by the closest point in $\Lambda^{(d)}$ to $\mathbf{w}$.

Achievable power-rate pair: We say that a power-rate pair $(\mathcal{P}, \mathcal{R})$ is achievable with strong secrecy if for every $\delta > 0$, there exists a sequence of $(\Lambda^{(d)}, \Lambda_0^{(d)})$ nested lattice codes such that for all sufficiently large d,

- The average transmit power, defined to be $\frac{1}{d}\mathbb{E}\|\mathbf{u}\|^2 = \frac{1}{d}\mathbb{E}\|\mathbf{v}\|^2$, is less than $\mathcal{P}+\delta$;
- The transmission rate, which is defined as $\frac{1}{d}\log_2|\mathbb{G}^{(d)}|$, is greater than $\mathcal{R}-\delta$;
- The average probability of decoding $X \oplus Y$ incorrectly from $\mathbf{u}+\mathbf{v}+\mathbf{z}$ is less than δ; and
- The mutual information, $\mathcal{I}(X; \mathbf{u}+\mathbf{v}) = \mathcal{I}(Y; \mathbf{u}+\mathbf{v})$ is less than δ.

The main result of this paper can be stated as follows:

Theorem 1. *Over the bidirectional relay, for any $\mathcal{P} \geq 4e\sigma^2$, a power-rate pair of*

$$\left(\mathcal{P}, \frac{1}{2}\log_2\left(\frac{\mathcal{P}}{\sigma^2}\right) - \frac{1}{2}\log_2 2e\right)$$

is achievable with strong secrecy.

The achievable rate can be improved using random dithering and MMSE equalization at the relay [5], [13]. An argument as in [13] yields that a power-rate pair of

$$\left(\mathcal{P}, \frac{1}{2}\log_2\left(\frac{1}{2}+\frac{\mathcal{P}}{\sigma^2}\right) - \frac{1}{2}\log_2 2e\right)$$

is achievable with strong secrecy.

III. Proof of Theorem 1

Consider the coding scheme described in Section II, taking the parameter κ in (5) to be equal to $\sqrt{\mathcal{P}}$. To prove strong secrecy, we use a technique from [11]. Let $p_{U+V}(\cdot)$ denote the pmf of $\mathbf{u}+\mathbf{v}$. For any coset Λ_j of $\Lambda_0^{(d)}$ in $\Lambda^{(d)}$, having λ_j as its coset representative in $\Lambda^{(d)} \cap \mathcal{V}(\Lambda_0^{(d)})$, let $p_{U+V|X}(\cdot|\lambda_j)$ denote the pmf of $\mathbf{u}+\mathbf{v}$ conditioned on the event $\{X = \Lambda_j\}$. We will first show that for every $\mathbf{x}$ in $\Lambda^{(d)} \cap \mathcal{V}(\Lambda^{(d)})$, the variational distance,

$$\mathbb{V}(p_{U+V}, p_{U+V|X}(\cdot|\mathbf{x})) := \sum_{\mathbf{w}\in\Lambda^{(d)}} |p_{U+V}(\mathbf{w}) - p_{U+V|X}(\mathbf{w}|\mathbf{x})|$$

goes to zero exponentially (in d) as d goes to infinity. We will then use the following basic result, which bounds from above the mutual information $\mathcal{I}(X; \mathbf{u}+\mathbf{v})$ in terms of the average variational distance

$$d_V := \sum_{\mathbf{x}} \mathbb{V}(p_{U+V}, p_{U+V|X}(\cdot|\mathbf{x}))p_X(\mathbf{x})$$

between the distributions p_{U+V} and $p_{U+V|X}$.

Lemma 1 ([4], Lemma 1)**.** *For $|\mathbb{G}^{(d)}| \geq 4$, we have $\mathcal{I}(X; \mathbf{u}+\mathbf{v}) \leq d_V\left(\log_2|\mathbb{G}^{(d)}| - \log_2 d_V\right)$.*

Given a lattice Λ in $\mathbb{R}^d$, we define $\mathrm{vol}(\Lambda)$ to be the volume of $\mathcal{V}(\Lambda)$. For any $\kappa > 0$, the flatness factor, $\epsilon_\Lambda(\kappa)$, is defined [1], [11] as

$$\epsilon_\Lambda(\kappa) = \frac{\max_{\mathbf{x}\in\mathcal{V}(\Lambda)} \left| \left(\sum_{\lambda\in\Lambda} f_{\kappa,\lambda}(\mathbf{x})\right) - 1/\mathrm{vol}(\Lambda)\right|}{1/\mathrm{vol}(\Lambda)}. \quad (6)$$

The following theorem gives a bound on the variational distance in terms of the flatness factor. A proof is sketched in the appendix.

Theorem 2. *If the sequence of nested lattice pairs, $(\Lambda^{(d)}, \Lambda_0^{(d)})$ is such that the flatness factor, $\epsilon^{(d)} := \epsilon_{\Lambda_0^{(d)}}\left(\sqrt{\mathcal{P}/2}\right)$ is less than $1/2$, then the variational distance is bounded from above as*

$$\mathbb{V}(p_{U+V}, p_{U+V|X}(\cdot|\mathbf{x})) \le 216\epsilon^{(d)}. \quad (7)$$

Therefore, if the hypothesis of the above theorem holds, then by Lemma 1, we have

$$\mathcal{I}(X; \mathbf{u}+\mathbf{v}) \le 216\epsilon^{(d)}(\log_2 |\mathbb{G}^{(d)}| - \log_2 216\epsilon^{(d)}).$$

As we will see below in Section III-B, we can choose nested lattices $(\Lambda^{(d)}, \Lambda_0^{(d)})$ such that $|\mathbb{G}^{(d)}|$ grows exponentially in d, while $\epsilon^{(d)}$ goes to zero exponentially in d. Thus, the mutual information $\mathcal{I}(X; \mathbf{u}+\mathbf{v})$ (and similarly $\mathcal{I}(Y; \mathbf{u}+\mathbf{v})$) goes to zero exponentially as d goes to infinity, thereby guaranteeing strong secrecy.

A. Average transmit power

The average transmit power is given by $\frac{1}{d}\mathbb{E}\|\mathbf{u}\|^2 = \frac{1}{d}\mathbb{E}\|\mathbf{v}\|^2 = \frac{1}{d}\sum_{\lambda\in\Lambda^{(d)}} \|\lambda\|^2 p_U(\lambda)$. Using inequalities (16) and (17) from the appendix, we can bound the average transmit power on either side as follows:

$$\left(\frac{1-\epsilon^{(d)}}{1+\epsilon^{(d)}}\right)\frac{1}{d}\sum_{\lambda\in\Lambda^{(d)}} \|\lambda\|^2 \frac{f_{\sqrt{\mathcal{P}}}(\lambda)}{f_{\sqrt{\mathcal{P}}}(\Lambda^{(d)})} \le \frac{1}{d}\mathbb{E}\|\mathbf{u}\|^2 \le \left(\frac{1+\epsilon^{(d)}}{1-\epsilon^{(d)}}\right)\frac{1}{d}\sum_{\lambda\in\Lambda^{(d)}} \|\lambda\|^2 \frac{f_{\sqrt{\mathcal{P}}}(\lambda)}{f_{\sqrt{\mathcal{P}}}(\Lambda^{(d)})}. \quad (8)$$

Now, Lemma 6 from [11] shows that as $d \to \infty$, the term $\frac{1}{d}\sum_{\lambda\in\Lambda^{(d)}} \|\lambda\|^2 \frac{f_{\sqrt{\mathcal{P}}}(\lambda)}{f_{\sqrt{\mathcal{P}}}(\Lambda^{(d)})}$ converges to $\mathcal{P}$, provided $\epsilon_{\Lambda^{(d)}}(\sqrt{\mathcal{P}}/2) \to 0$. We thus have the following lemma.

Lemma 2. *As $d \to \infty$, if the flatness factors $\epsilon_{\Lambda_0^{(d)}}(\sqrt{\mathcal{P}/2})$, and $\epsilon_{\Lambda^{(d)}}(\sqrt{\mathcal{P}}/2)$ both converge to zero, then the average transmit power, $\frac{1}{d}\mathbb{E}\|\mathbf{u}\|^2 = \frac{1}{d}\mathbb{E}\|\mathbf{v}\|^2$, converges to $\mathcal{P}$.*

B. Achievable rate

We choose our sequence of nested lattices, $(\Lambda^{(d)}, \Lambda_0^{(d)})$ so as to satisfy the following properties:

(L1) The sequence of coarse lattices, $\Lambda_0^{(d)}$, is good for covering, MSE quantization, and AWGN channel coding[2].

[2]For the definitions of lattices good for covering, MSE quantization, and AWGN channel coding, and discussions involving these, see e.g. [6].

(L2) The sequence of fine lattices, $\Lambda^{(d)}$, is good for AWGN channel coding.

(L3) The flatness factor $\epsilon_{\Lambda_0^{(d)}}(\sqrt{\mathcal{P}/2})$ goes to zero exponentially as d goes to infinity.

(L4) The flatness factor $\epsilon_{\Lambda^{(d)}}(\sqrt{\mathcal{P}}/2)$ goes to zero exponentially as d goes to infinity.

From [13], we know that for any $\mathcal{R} > 0$, a sequence of nested lattices $(\Lambda^{(d)}, \Lambda_0^{(d)})$ can be chosen to satisfy (L1) and (L2), with $\frac{1}{d}\log_2|\mathbb{G}^{(d)}| = \frac{1}{d}\log_2\frac{\mathrm{vol}(\Lambda_0^{(d)})}{\mathrm{vol}(\Lambda^{(d)})} \to \mathcal{R}$ as $d \to \infty$. Theorem 3 and Proposition 4 of [11] show that such a sequence of nested lattices can also be made to satisfy (L3) if

$$\frac{\left(\mathrm{vol}(\Lambda_0^{(d)})\right)^{2/d}}{2\pi(\mathcal{P}/2)} < 1, \quad (9)$$

and (L4) if

$$\frac{\left(\mathrm{vol}(\Lambda^{(d)})\right)^{2/d}}{2\pi(\mathcal{P}/4)} < 1. \quad (10)$$

In order to satisfy (9), let us choose $\left(\mathrm{vol}(\Lambda_0^{(d)})\right)^{2/d} = \pi\mathcal{P} - \delta$ for some arbitrary $\delta > 0$. Using $\mathrm{vol}(\Lambda^{(d)}) = \mathrm{vol}(\Lambda_0^{(d)})/|\mathbb{G}^{(d)}|$, we see that for (10) to hold, the transmission rate has to satisfy

$$\frac{1}{d}\log_2|\mathbb{G}^{(d)}| > 1/2 + \frac{1}{2}\log_2\left(1 - \frac{\delta}{\pi\mathcal{P}}\right). \quad (11)$$

Thus, if the above holds, then we can have properties (L3) and (L4), and hence, by Lemma 2, we can have the average transmit power converging to $\mathcal{P}$.

Since the sequence of fine lattices is good for AWGN channel coding, the probability of error in decoding $X \oplus Y$ from $\mathbf{u}+\mathbf{v}+\mathbf{z}$ can be made to decay to zero as $d \to \infty$ if

$$\frac{\left(\mathrm{vol}(\Lambda^{(d)})\right)^{2/d}}{2\pi e\sigma^2} > 1. \quad (12)$$

We have $\mathrm{vol}(\Lambda^{(d)}) = \mathrm{vol}(\Lambda_0^{(d)})/|\mathbb{G}^{(d)}|$, and we have chosen $(\mathrm{vol}(\Lambda_0^{(d)}))^{2/d} = \pi\mathcal{P} - \delta$. Putting these into (12), and observing that δ is arbitrary, we see that if

$$\frac{1}{d}\log_2|\mathbb{G}^{(d)}| < \frac{1}{2}\log_2\left(\frac{\mathcal{P}}{\sigma^2}\right) - \frac{1}{2}\log_2 2e, \quad (13)$$

then the probability of error can be made to go down to zero as d goes to infinity.

If $\mathcal{P} \ge 4e\sigma^2$, then the right-hand side of (13) exceeds that of (11). Hence, we can find a sequence of nested lattice codes that achieves a power-rate pair of $\left(\mathcal{P}, \frac{1}{2}\log_2\left(\frac{\mathcal{P}}{\sigma^2}\right) - \frac{1}{2}\log_2 2e\right)$ with strong secrecy, thus proving Theorem 1.

Remark. The strongly secure scheme proposed by He and Yener in [8] also used nested lattice codes as we have done here. They obtain strong secrecy using universal hash functions, and show the existence of a suitable linear hash function that ensures that the mutual information decays exponentially in d. On the other hand, we have

used a sampled Gaussian pmf for randomization at the encoder, and hence, for a given pair of nested lattices, we explicitly specify the distribution used for randomization. Even using our scheme, the mutual information goes down to zero exponentially in d. But unlike [8], which was valid under a maximum power constraint at each node, the codebook we use is unbounded, so our scheme can only satisfy an average power constraint. Also, the achievable rate in the scheme of He and Yener is slightly higher (by $\frac{1}{2}\log_2\frac{e}{2}$ bits per channel use). Our scheme has these two drawbacks but is still attractive because unlike [8], which is only an existence result, we give an explicit randomization technique for security. The scheme in [8] was coupled with an Algebraic Manipulation Detection (AMD) code [3] for Byzantine detection, and it was shown that the probability of a Byzantine attack being undetected could be made to decay to zero exponentially in d. We remark that our coding scheme can also be extended to this scenario, and be used as a replacement for the nested lattice code in [8].

IV. Multi-hop relaying

In this section, we apply our coding scheme to the scenario of multi-hop relaying. A multi-hop line network with $K+1$ hops consists of $K+2$ nodes: a source (node 0), a destination (node $K+1$), and K relay nodes, labelled by $1, 2, \ldots, K$. The nodes are laid out in a straight line, in increasing order of their labels. All nodes are half-duplex. Each node can communicate only with its immediate neighbours, and communication is by broadcast of messages to the neighbours. All links between nodes are identical, zero mean, variance σ^2 AWGN channels. The source has to send M independent messages, $X_1, X_2, \ldots, X_M$, to the destination across the network. The relays act as passive eavesdroppers, but do not cooperate with each other, i.e., the information available at a relay is not shared with the other relays. We use the scheme proposed by He and Yener [7] for relaying, except that each node in the network employs the coding scheme described in Section II. The communication takes place in $2M+K+1$ phases. Each phase requires d channel uses. An average power constraint is imposed at the nodes[3]. If $\mathbf{v}_i[t]$ denotes the vector transmitted by the ith node in phase t, then $\frac{1}{d}\mathbb{E}\|\mathbf{v}_i[t]\| \leq P^{(d)}$, for $0 \leq i \leq K+1$ and $1 \leq i \leq K+2M+1$. The *rate* of the scheme, $R_M^{(d)}$, is the number of bits of information transmitted per channel use by the source in order to send M messages to the destination, i.e., $R_M^{(d)} := \frac{M}{d(K+2M+1)}\log_2|\mathbb{G}^{(d)}|$.

We say that a power-rate pair of $(\mathcal{P}, \mathcal{R})$ is achievable for M-message transmission with strong secrecy in a multi-hop line network with $K+1$ hops, if for every $\delta > 0$, there exists a sequence of $(\Lambda_0^{(d)}, \Lambda^{(d)})$ nested lattice codes such that for all sufficiently large d, we have $P^{(d)} < \mathcal{P}+\delta$, $R_M^{(d)} > \mathcal{R}-\delta$, the probability of the destination decoding $X_1, X_2, \ldots, X_M$ incorrectly, $\eta^{(d)} < \delta$, and the mutual information between the messages and all variables available at the kth relay is at most δ for each k. It can be shown that a power-rate pair of $\left(\mathcal{P}, \frac{M}{2(K+2M+1)}\left[\log_2\left(\frac{\mathcal{P}}{\sigma^2}\right) - \log_2 2e\right]\right)$ is achievable for M-message transmission with strong secrecy using this scheme. We omit the details due to lack of space. Letting the number of messages, M, go to infinity, we have

Theorem 3. *For $\mathcal{P} \geq 4e\sigma^2$, a power-rate pair of*

$$\left(\mathcal{P}, \frac{1}{4}\log_2\left(\frac{\mathcal{P}}{\sigma^2}\right) - \frac{1}{4}\log_2 2e\right)$$

is achievable with strong secrecy in a multi-hop network.

Appendix: Proof of Theorem 2

The following lemma from [11] will be used in the proof.

Lemma 3 ([11], Lemma 4)**.** *Let Λ be a lattice in $\mathbb{R}^d$. Then, for all $\mathbf{z} \in \mathbb{R}^d$, and $\kappa > 0$,*

$$\frac{1-\epsilon_\Lambda(\kappa)}{1+\epsilon_\Lambda(\kappa)} \leq \frac{f_{\kappa,\mathbf{z}}(\Lambda)}{f_\kappa(\Lambda)} \leq 1.$$

For ease of notation, we will suppress the index d in $\epsilon^{(d)}$, $\Lambda_0^{(d)}$ and $\Lambda^{(d)}$. For a message X chosen at node $\mathtt{A}$, let $\mathbf{x}$ be the coset representative of X from $\Lambda \cap \mathcal{V}(\Lambda_0)$. For any subset $S \subseteq \mathbb{R}^d$, let $\mathbf{1}_S(\cdot)$ denote the indicator function of S, i.e., $\mathbf{1}_S(\mathbf{u})$ is 1 if $\mathbf{u} \in S$, and 0 otherwise. From (5), with $\kappa = \sqrt{\mathcal{P}}$, we have

$$p_{U|X}(\mathbf{u}|\mathbf{x}) = \frac{f_{\sqrt{\mathcal{P}}}(\mathbf{u})}{f_{\sqrt{\mathcal{P}},-\mathbf{x}}(\Lambda_0)}\mathbf{1}_{\Lambda_0+\mathbf{x}}(\mathbf{u}). \tag{14}$$

Let $\mathbb{G}_X := \Lambda \cap \mathcal{V}(\Lambda_0)$, and $N := |\mathbb{G}^{(d)}| = |\mathbb{G}_X|$. Since the messages are uniformly distributed,

$$p_U(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{G}_X} \frac{f_{\sqrt{\mathcal{P}}}(\mathbf{u})}{f_{\sqrt{\mathcal{P}},-\mathbf{x}}(\Lambda_0)}\frac{\mathbf{1}_{(\Lambda_0+\mathbf{x})}(\mathbf{u})}{N}. \tag{15}$$

Now, we can bound p_U in terms of $\epsilon_{\Lambda_0}(\kappa)$ as follows. Since the flatness factor, $\epsilon_{\Lambda_0}(\kappa)$, is a decreasing function of κ [11], we have $\epsilon_{\Lambda_0}(\sqrt{\mathcal{P}}) < \epsilon_{\Lambda_0}(\sqrt{\mathcal{P}/2}) = \epsilon$. Hence, writing $\frac{f_{\sqrt{\mathcal{P}}}(\mathbf{u})}{f_{\sqrt{\mathcal{P}},-\mathbf{x}}(\Lambda_0)}$ in (15) as $\frac{f_{\sqrt{\mathcal{P}}}(\mathbf{u})}{f_{\sqrt{\mathcal{P}}}(\Lambda_0)}\frac{f_{\sqrt{\mathcal{P}}}(\Lambda_0)}{f_{\sqrt{\mathcal{P}},-\mathbf{x}}(\Lambda_0)}$, we get via Lemma 3,

$$\frac{f_{\sqrt{\mathcal{P}}}(\mathbf{u})}{Nf_{\sqrt{\mathcal{P}}}(\Lambda_0)} \leq p_U(\mathbf{u}) \leq \frac{f_{\sqrt{\mathcal{P}}}(\mathbf{u})}{Nf_{\sqrt{\mathcal{P}}}(\Lambda_0)}\left(\frac{1+\epsilon}{1-\epsilon}\right). \tag{16}$$

Re-arranging, we obtain

$$\left(\frac{1-\epsilon}{1+\epsilon}\right)p_U(\mathbf{u})Nf_{\sqrt{\mathcal{P}}}(\Lambda_0) \leq f_{\sqrt{\mathcal{P}}}(\mathbf{u}) \leq p_U(\mathbf{u})Nf_{\sqrt{\mathcal{P}}}(\Lambda_0).$$

Since $\sum_{\mathbf{u}\in\Lambda} p_U(\mathbf{u}) = 1$, we see that

$$\left(\frac{1-\epsilon}{1+\epsilon}\right)Nf_{\sqrt{\mathcal{P}}}(\Lambda_0) \leq f_{\sqrt{\mathcal{P}}}(\Lambda) \leq Nf_{\sqrt{\mathcal{P}}}(\Lambda_0). \tag{17}$$

[3]He and Yener [7] use a slightly different power constraint than the one defined here, and hence their expression for achievable rate is different.

It can similarly be verified that for any $\mathbf{a} \in \mathbb{R}^n$,

$$\left(\frac{1-\epsilon}{1+\epsilon}\right) N f_{\sqrt{\frac{\mathcal{P}}{2}},\mathbf{a}}(\Lambda_0) \leq f_{\sqrt{\frac{\mathcal{P}}{2}},\mathbf{a}}(\Lambda) \leq N f_{\sqrt{\frac{\mathcal{P}}{2}},\mathbf{a}}(\Lambda_0). \tag{18}$$

We establish some more notation for convenience. Let

$$\alpha(\mathbf{w}) := \frac{f_{\sqrt{2\mathcal{P}}}(\mathbf{w})}{N f_{\sqrt{\mathcal{P}}}(\Lambda_0)} \frac{f_{\sqrt{\frac{\mathcal{P}}{2}}}(\Lambda_0)}{f_{\sqrt{\mathcal{P}}}(\Lambda_0)}, \tag{19}$$

$$\beta(\mathbf{x},\mathbf{w}) := \left(\frac{f_{\sqrt{\frac{\mathcal{P}}{2}},\frac{\mathbf{w}}{2}-\mathbf{x}}(\Lambda_0)}{f_{\sqrt{\frac{\mathcal{P}}{2}}}(\Lambda_0)}\right)\left(\frac{f_{\sqrt{\mathcal{P}},-\mathbf{x}}(\Lambda_0)}{f_{\sqrt{\mathcal{P}}}(\Lambda_0)}\right)^{-1}. \tag{20}$$

We can bound $p_{U+V|X}$ and p_{U+V} as follows.

Lemma 4. *For any lattice point $\mathbf{w} \in \Lambda$, and any $\mathbf{x} \in \mathbb{G}_X$, we have*

$$\left(\frac{1-\epsilon}{1+\epsilon}\right)\alpha(\mathbf{w}) \leq p_{U+V}(\mathbf{w}) \leq \left(\frac{1+\epsilon}{1-\epsilon}\right)^2 \alpha(\mathbf{w}) \tag{21}$$

$$\beta(\mathbf{x},\mathbf{w})\alpha(\mathbf{w}) \leq p_{U+V|X}(\mathbf{w}|\mathbf{x}) \leq \left(\frac{1+\epsilon}{1-\epsilon}\right)\beta(\mathbf{x},\mathbf{w})\alpha(\mathbf{w}). \tag{22}$$

Proof: Let $\mathbf{x}$ be any fine lattice point from $\mathbb{G}_X$. Then,

$$p_{U+V|X}(\mathbf{w}|\mathbf{x}) = \sum_{\mathbf{t}\in\Lambda_0+\mathbf{x}} p_{U|X}(\mathbf{t}|\mathbf{x}) p_V(\mathbf{w}-\mathbf{t})$$

Using (14) and (16) in the above equation, we obtain

$$\sum_{\mathbf{t}\in\Lambda_0+\mathbf{x}} \frac{f_{\sqrt{\mathcal{P}}}(\mathbf{t})}{f_{\sqrt{\mathcal{P}},-\mathbf{x}}(\Lambda_0)} \frac{f_{\sqrt{\mathcal{P}}}(\mathbf{w}-\mathbf{t})}{N f_{\sqrt{\mathcal{P}}}(\Lambda_0)} \leq p_{U+V|X}(\mathbf{w}|\mathbf{x}) \leq \sum_{\mathbf{t}\in\Lambda_0+\mathbf{x}} \frac{f_{\sqrt{\mathcal{P}}}(\mathbf{t})}{f_{\sqrt{\mathcal{P}},-\mathbf{x}}(\Lambda_0)} \frac{f_{\sqrt{\mathcal{P}}}(\mathbf{w}-\mathbf{t})}{N f_{\sqrt{\mathcal{P}}}(\Lambda_0)} \left(\frac{1+\epsilon}{1-\epsilon}\right). \tag{23}$$

Expanding $f_{\sqrt{\mathcal{P}}}(\mathbf{t}) f_{\sqrt{\mathcal{P}}}(\mathbf{w}-\mathbf{t})$ in terms of exponentials, and some algebraic manipulation reveals that

$$\sum_{\mathbf{t}\in\Lambda_0+\mathbf{x}} \frac{f_{\sqrt{\mathcal{P}}}(\mathbf{t})}{f_{\sqrt{\mathcal{P}},-\mathbf{x}}(\Lambda_0)} \frac{f_{\sqrt{\mathcal{P}}}(\mathbf{w}-\mathbf{t})}{N f_{\sqrt{\mathcal{P}}}(\Lambda_0)} = \frac{f_{\sqrt{2\mathcal{P}}}(\mathbf{w})}{N f_{\sqrt{\mathcal{P}}}(\Lambda_0)} \frac{f_{\sqrt{\frac{\mathcal{P}}{2}},\frac{\mathbf{w}}{2}-\mathbf{x}}(\Lambda_0)}{f_{\sqrt{\mathcal{P}},-\mathbf{x}}(\Lambda_0)}. \tag{24}$$

Substituting this in (23), and writing this in terms of α and β, we obtain (22). Similarly, bounding p_U and p_V from above and below using (16), proceeding as above, and finally using (18) to bound $f_{\sqrt{\frac{\mathcal{P}}{2}},\frac{\mathbf{w}}{2}}(\Lambda)$, we get (21). ∎

Observe that (20) is a ratio of two terms, both of which can be bounded using Lemma 3 to get

$$\left(\frac{1-\epsilon}{1+\epsilon}\right) \leq \beta(\mathbf{x},\mathbf{w}) \leq \left(\frac{1+\epsilon}{1-\epsilon}\right). \tag{25}$$

Let $\overline{p}_{U+V}$ and $\underline{p}_{U+V}$ respectively denote the upper and lower bounds for p_{U+V} in (21), and let $\overline{p}_{U+V|X}$ and $\underline{p}_{U+V|X}$ respectively denote the upper and lower bounds for $p_{U+V|X}$ in (22). Then, we can say that $|p_{U+V|X}(\mathbf{w}|\mathbf{x}) - p_{U+V}(\mathbf{w})|$ is less than or equal to the maximum of $|\overline{p}_{U+V|X}(\mathbf{w}|\mathbf{x}) - \underline{p}_{U+V}(\mathbf{w})|$ and $|\underline{p}_{U+V|X}(\mathbf{w}|\mathbf{x}) - \overline{p}_{U+V}(\mathbf{w})|$.

Substituting for $|\overline{p}_{U+V|X}(\mathbf{w}|\mathbf{x}) - \underline{p}_{U+V}(\mathbf{w})|$, and noting that $((1+\epsilon)/(1-\epsilon))^3 \leq 1 + 64\epsilon$ for $\epsilon < 1/2$, we obtain

$$|\overline{p}_{U+V|X}(\mathbf{w}|\mathbf{x}) - \underline{p}_{U+V}(\mathbf{w})| \leq \alpha(\mathbf{w}) \left(\frac{1-\epsilon}{1+\epsilon}\right) 64\epsilon. \tag{26}$$

Similarly, expressing $|\underline{p}_{U+V|X}(\mathbf{w}|\mathbf{x}) - \overline{p}_{U+V}(\mathbf{w})|$ in terms of α and β, and using the fact that $((1-\epsilon)/(1+\epsilon))^3 \geq 1 - 8\epsilon$ for $\epsilon < 1/2$, we get

$$|\underline{p}_{U+V|X}(\mathbf{w}|\mathbf{x}) - \overline{p}_{U+V}(\mathbf{w})| \leq \alpha(\mathbf{w}) \left(\frac{1+\epsilon}{1-\epsilon}\right)^2 8\epsilon. \tag{27}$$

Using (21) and the fact that $\sum_{\mathbf{w}\in\Lambda} p_{U+V}(\mathbf{w}) = 1$, we have

$$\left(\frac{1-\epsilon}{1+\epsilon}\right)^2 \leq \sum_{\mathbf{w}\in\Lambda} \alpha(\mathbf{w}) \leq \left(\frac{1+\epsilon}{1-\epsilon}\right). \tag{28}$$

The inequality (7) can now be obtained by combining (26) and (27), summing over $\mathbf{w}$, and using (28) to bound $\sum_{\mathbf{w}\in\Lambda} \alpha(\mathbf{w})$ from above. Theorem 2 is thus proved.

References

[1] J.-C. Belfiore, "Lattice codes for the compute-and-forward protocol: The flatness factor," in *Proc. 2011 Information Theory Workshop (ITW 2011)*, Paraty, Brazil.

[2] J.H. Conway, N.J.A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, 1988.

[3] R. Cramer, Y. Dodis, S. Fehr, C. Padro, D. Wichs, "Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors," *Adv. Cryptology*, vol. 4965, pp. 471–488, 2008.

[4] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.

[5] U. Erez and R. Zamir, "Achieving 1/2log(1+SNR) on the AWGN channel with lattice encoding and decoding," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2293–2314, Oct. 2004.

[6] U. Erez, S. Litsyn and R. Zamir, "Lattices which are good for (almost) everything," *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3401–3416, Oct. 2005.

[7] X. He and A. Yener, "Providing secrecy with lattice codes," *Proc. 46th Annual Allerton Conference on Communication, Control, and Computing*, pp. 1199–1206, Sept. 2008.

[8] X. He and A. Yener, "Strong secrecy and reliable Byzantine detection in the presence of an untrusted relay," *IEEE Trans. Inf. Theory*, vol. 59, no. 1, July 2013.

[9] N. Kashyap, V. Shashank, A. Thangaraj, "Secure computation in a bidirectional relay," in *Proc. 2012 IEEE Int. Symp. Inf. Theory (ISIT 2012)*, Cambridge, Mass., USA.

[10] N. Kashyap, V. Shashank, A. Thangaraj, "Secure compute-and-forward in a bidirectional relay," `arXiv:1206.3392`.

[11] C. Ling, L. Luzzi, J.-C. Belfiore, D. Stehlé, "Semantically secure lattice codes for the Gaussian wiretap channel," `arXiv:1210.6673`.

[12] U. Maurer and S. Wolf. "Information-theoretic key agreement: From weak to strong secrecy for free," *Proc. EUROCRYPT–2000 on Advances in Cryptology*, vol. 1807, pp. 351–368, Springer, 2000.

[13] B. Nazer and M. Gastpar, "Compute-and-forward: harnessing interference through structured codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6463–6486, Oct. 2011.

[14] M. Wilson, K. Narayanan, H. Pfister, and A. Sprintson, "Joint physical layer coding and network coding for bidirectional relaying," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5641–5654, Nov. 2010.