A Lattice Coding Scheme for Secret Key Generation from Gaussian Markov Tree Sources

Shashank Vatedka and Navin Kashyap
Department of Electrical Communication Engineering
Indian Institute of Science, Bengaluru, India
email: {shashank,nkashyap}@ece.iisc.ernet.in

***Abstract*—To be considered for the 2016 IEEE Jack Keil Wolf ISIT Student Paper Award. In this article, we study the problem of secret key generation in the multiterminal source model, where the terminals have access to correlated Gaussian sources. We assume that the sources form a Markov chain on a tree. We give a nested lattice-based key generation scheme whose computational complexity is polynomial in the number, N, of independent and identically distributed samples observed by each source. We also compute the achievable secret key rate and give a class of examples where our scheme is optimal in the fine quantization limit. However, we also give examples that show that our scheme is not always optimal in the limit of fine quantization.**

I. Introduction

We study secret key (SK) generation in the multiterminal source model, where m terminals possess correlated Gaussian sources. Each terminal observes N independent and identically distributed (iid) samples of its source. The terminals have access to a noiseless public channel of infinite capacity, and their objective is to agree upon an SK by communicating across the public channel. The key must be such that an eavesdropper having access to the public communication must not be able to guess the key. In other words, the key must be independent (or almost independent) of the messages communicated across the channel. A measure of performance is the SK rate that can be achieved, which is the number of bits of SK generated per source sample. On the other hand, the probability that any terminal is unable to reconstruct the key correctly should be arbitrarily small.

The discrete setting — the case where the correlated sources take values in a finite alphabet — was studied by Csiszár and Narayan [1]. They gave a scheme for computing a secret key in this setting and found the SK capacity, i.e., the maximum achievable secret key rate. This was later generalized in [7] to the case where the terminals possess correlated Gaussian sources.

In a practical setting, we can assume that the random sources are obtained by observing some natural parameters, e.g., temperature in a field. In other words, the underlying source is continuous. However, for the purposes of storage and computation, these sources must be quantized, and only the quantized source can be used for SK generation. If each terminal uses a scalar quantizer, then we get the discrete source model studied in [1]. However, we could do better and instead use a vector quantizer to obtain a higher SK rate. Nitinawarat and Narayan [7] found the SK capacity for correlated Gaussian sources in such a setting. However, to approach capacity, the quantization rate and the rate of public communication at each terminal must approach infinity. In practice, it is reasonable to have a constraint on the quantization rate at each terminal. The terminals can only use the quantized source for SK generation. Nitinawarat and Narayan [7] also studied a two-terminal version of this problem, where a quantization rate constraint was imposed on only one of the terminals. They gave a nested lattice coding scheme and showed that it was optimal, i.e., no other scheme can give a higher SK rate. In related work, Watanabe and Oohama [10] characterized the maximum SK rate achievable under a constraint on the sum rate of public communication in the two-terminal setting. More recently, Ling et al. [5] gave a lattice coding scheme for the public communication-constrained problem and were able to achieve an SK rate within $1/2$ nats of the maximum in [10].

We consider a multiterminal generalization of the two-terminal version studied by [7] where individual quantization rate constraints are imposed on each of the terminals. Terminal i has access to N iid copies of a Gaussian source $X_i(1), X_i(2), \ldots, X_i(N)$. The sources are correlated across the terminals. We assume that the joint distribution of the sources has a *Markov tree* structure [1, Example 7], which is a generalization of a Markov chain. Let us define this formally. Suppose that $T = (V, E)$ is a tree and $\{X_i : i \in V\}$ is a collection of random variables indexed by the vertices. Consider any two disjoint subsets $\mathcal{I}$ and $\mathcal{J}$ of V. Let v be any vertex such that removal of v from T disconnects $\mathcal{I}$ from $\mathcal{J}$ (Equivalently, for every $i \in \mathcal{I}$ and $j \in \mathcal{J}$, the path connecting i and j passes through v). For every such $\mathcal{I}, \mathcal{J}, \mathtt{v}$, if $\{X_i : i \in \mathcal{I}\}$ and $\{X_j : j \in \mathcal{J}\}$ are conditionally independent given X_v, then we say that $\{X_i : i \in T\}$ form a Markov chain on T, or $\{X_i : i \in V\}$ is a Markov tree source.

The contributions of this paper are the following. We study the problem of SK generation in a Gaussian Markov tree source model with individual quantization rate constraints imposed at each terminal. We give a nested lattice-based scheme and find the achievable SK rate. For certain classes of Markov trees, particularly homogeneous Markov trees[1], we show that our scheme achieves the SK capacity in the limit as the quantization rates go to infinity. However, we also

[1]We say that a Markov tree is homogeneous if $I(X_{\mathtt{u}}; X_{\mathtt{v}})$ is the same for all edges $(\mathtt{u}, \mathtt{v})$

give examples where our scheme does not achieve the key capacity. A salient feature of our scheme is that the overall computational complexity required for quantization and key generation is polynomial in the number of samples. It is also interesting to note that unlike the general schemes in [1], [7], we give a scheme where at least one terminal remains silent (does not participate in public communication), and omniscience is not attained.

Notation: If $\mathcal{I}$ is an index set and $\{A_i : i \in \mathcal{I}\}$ is a class of sets indexed by $\mathcal{I}$, then their Cartesian product is denoted by $\bigtimes_{i\in\mathcal{I}} A_i$. Given two sequences indexed by $n \in \mathbb{N}$, $f(n)$ and $g(n)$, we say that $f(n) = O(g(n))$ if there exists a constant c such that $f(n) \leq cg(n)$ for all sufficiently large n. Furthermore, $f(n) = o_n(1)$ if $f(n) \to 0$ as $n \to \infty$.

Given a rooted tree $T = (V, E)$ with root $\mathtt{r}(T)$ we say that a vertex $\mathtt{u}$ is the parent of $\mathtt{v} \neq \mathtt{r}(T)$, denoted $\mathtt{u} = \mathrm{par}(\mathtt{v})$, if $\mathtt{u}$ lies in the shortest path from $\mathtt{r}(T)$ to $\mathtt{v}$ and the distance between $\mathtt{u}$ and $\mathtt{v}$ is 1. Furthermore, for every $\mathtt{v} \in V$, we define $N_T(\mathtt{v})$ to be the set of all neighbours of $\mathtt{v}$ in T.

II. Secret Key Generation from Correlated Gaussian Sources

A. The Problem

We now formally define the problem. We consider a multiterminal Gaussian source model [7], which is described as follows. There are m terminals, each having access to N independent and identically distributed (iid) copies of a correlated Gaussian source, i.e., the lth terminal observes $X_l(1), X_l(2), \ldots, X_l(N)$ which are iid. Without loss of generality, we can assume that $X_l(i)$ has mean zero and variance 1. The joint distribution of $\{X_l(i) : 1 \leq l \leq m\}$ can be described by their covariance matrix Φ. Specifically, we assume that the sources form a Markov tree, defined in Sec. I. Let $T = (V, E)$ be a tree having $|V| = m$ vertices, which defines the conditional independence structure of the sources. For $\mathtt{u}, \mathtt{v} \in V$, let us define $\rho_{\mathtt{uv}} := \mathbb{E}[X_{\mathtt{u}} X_{\mathtt{v}}]$. We can therefore write

$$X_{\mathtt{u}} = \rho_{\mathtt{uv}} X_{\mathtt{v}} + \sqrt{1-\rho_{\mathtt{uv}}^2}\, Z_{\mathtt{uv}}$$

where $Z_{\mathtt{uv}}$ is a zero-mean, unit-variance Gaussian random variable which is independent of $X_{\mathtt{v}}$. Similarly,

$$X_{\mathtt{v}} = \rho_{\mathtt{uv}} X_{\mathtt{u}} + \sqrt{1-\rho_{\mathtt{uv}}^2}\, Z_{\mathtt{vu}}$$

where $Z_{\mathtt{vu}}$ is also a zero-mean, unit-variance Gaussian random variable (different from $Z_{\mathtt{uv}}$) which is independent of $X_{\mathtt{u}}$.

Our objective is to generate an SK using public communication. For $\mathtt{v} \in V$, let $\mathbf{X}_{\mathtt{v}}^N := (X_{\mathtt{v}}(1), \ldots, X_{\mathtt{v}}(N))$ denote the N iid copies of $X_{\mathtt{v}}$ available at terminal $\mathtt{v}$. Each terminal uses a vector quantizer $Q_{\mathtt{v}} : \mathbb{R}^N \to \mathcal{X}_{\mathtt{v}}$ of rate $R_{\mathrm{q}}^{(\mathtt{v})} := \frac{1}{N}\log_2 |\mathcal{X}_{\mathtt{v}}|$. Terminal $\mathtt{v}$ transmits $\mathbf{F}_{\mathtt{v}}^{(N)} \in \mathcal{F}_{\mathtt{v}}^{(N)}$ — which is a (possibly randomized) function of $Q_{\mathtt{v}}(\mathbf{X}_{\mathtt{v}}^N)$ — across a noiseless public channel that an eavesdropper may have access to[2]. Using the public communication and their respective observations of the quantized random variables, $Q_{\mathtt{v}}(\mathbf{X}_{\mathtt{v}}^N)$, the terminals must generate a secret key $\mathbf{K}^{(N)} \in \mathcal{K}^{(N)}$ which is concealed from the eavesdropper. Let $\mathcal{F}_G := \bigtimes_{\mathtt{v}\in V} \mathcal{F}_{\mathtt{v}}^{(N)}$.

Fix any $\epsilon > 0$. We say that $\mathbf{K}^{(N)}$ is an ϵ-secret key (ϵ-SK) if there exist functions $f_{\mathtt{v}} : (\mathcal{X}_{\mathtt{v}}, \mathcal{F}_G) \to \mathcal{K}^{(N)}$ such that:

- $\Pr\left[f_{\mathtt{v}}(Q_{\mathtt{v}}(\mathbf{X}_{\mathtt{v}}^N), \{\mathbf{F}_{\mathtt{u}}^{(N)} : \mathtt{u} \in V\}) \neq \mathbf{K}^{(N)}\right] < \epsilon$,
- $\log_2 |\mathcal{K}^{(N)}| - H(\mathbf{K}^{(N)}) < \epsilon$, and
- $I\left(\{\mathbf{F}_{\mathtt{v}}^{(N)} : \mathtt{v} \in V\}\,;\, \mathbf{K}^{(N)}\right) < \epsilon$.

We say that R_{key} is an achievable SK rate if for every $\epsilon > 0$, there exist quantizers $\{Q_{\mathtt{v}}\}$, a scheme for public communication, $\{\mathbf{F}_{\mathtt{v}}^{(N)}\}$, and a secret key $\mathbf{K}^{(N)}$, such that for all sufficiently large N, $\mathbf{K}^{(N)}$ is an ϵ-SK, and $\frac{1}{N}\log_2 |\mathcal{K}^{(N)}| \geq R_{\mathrm{key}} - \epsilon$.

Consider the following procedure to obtain a class of rooted subtrees of T:

- Identify a vertex $\mathtt{v}$ in V as the root. The tree T with $\mathtt{v}$ as the root is a rooted tree. Call this $T'_{\mathtt{v}}$.
- Delete all the leaves of $T'_{\mathtt{v}}$. Call the resulting rooted subtree $T^*_{\mathtt{v}}$.

Let $\mathcal{T}^* := \{T^*_{\mathtt{v}} : \mathtt{v} \in V\}$ denote the set of all rooted subtrees of T obtained in the above manner. Fig. 1 illustrates this for a tree having four vertices. Note that there are $|V|$ trees in $\mathcal{T}^*$, one corresponding to each vertex. For any such rooted subtree $T^* = (V^*, E^*)$ in $\mathcal{T}^*$, let $\mathtt{r}(T^*)$ denote the root of T^*. We will see later that it is only the terminals that correspond to T^* that participate in the public communication while the other terminals remain silent. For any $\mathtt{v} \in V^*$, let $N_T(\mathtt{v})$ denote the set of all neighbours of $\mathtt{v}$ in T (*not* T^*). Recall that each terminal $\mathtt{v}$ operates under a quantization rate constraint of $R_{\mathrm{q}}^{(\mathtt{v})}$. For every $T^* = (V^*, E^*)$, us define

$$\mathcal{R}_{\mathrm{ent}} = R_q^{(\mathtt{r}(T^*))} + \sum_{\mathtt{u}\in V^*\setminus\mathtt{r}(T^*)} \frac{1}{2}\log_2\left((e^{2R_{\mathrm{q}}^{(\mathtt{u})}} - 1)(1-\rho^2_{\mathtt{u},\mathrm{par}(\mathtt{u})}) + 1\right) \quad (1)$$

$$\mathcal{R}_{\mathrm{com}} = \sum_{\mathtt{v}\in V^*} \max_{\mathtt{u}\in N_T(\mathtt{v})} \frac{1}{2}\log_2\left((e^{2R_{\mathrm{q}}^{(\mathtt{v})}} - 1)(1-\rho^2_{\mathtt{uv}}) + 1 + \frac{\rho^2_{\mathtt{uv}} e^{2R_{\mathrm{q}}^{(\mathtt{v})}}}{e^{2R_{\mathrm{q}}^{(\mathtt{u})}} - 1}\right). \quad (2)$$

We will show that the (normalized) joint entropy of the quantized sources is at least $\mathcal{R}_{\mathrm{ent}}$ and the sum rate of public communication is at most $\mathcal{R}_{\mathrm{com}}$ in our scheme. Also, the public communication that achieves $\mathcal{R}_{\mathrm{com}}$ requires only the terminals in T^* to participate in the communication; the terminals in $V\setminus V^*$ are silent. Let us also define

$$\alpha := \left(\max_{\mathtt{u}\in V^*} R_{\mathrm{q}}^{(\mathtt{u})}\right) \Big/ \left(\min_{\mathtt{v}\in V^*} R_{\mathrm{q}}^{(\mathtt{v})}\right). \quad (3)$$

Our aim is to prove the following result

Theorem 1. *For a fixed quantization rate constraint $\{R_{\mathrm{q}}^{(\mathtt{v})} : \mathtt{v} \in V\}$, a secret key rate of*

$$R_{\mathrm{key}} = \max_{T^*\in\mathcal{T}^*} (\mathcal{R}_{\mathrm{ent}} - \mathcal{R}_{\mathrm{com}}) \quad (4)$$

[2]In this work, we only consider noninteractive communication, i.e., the public communication is only a function of the source and not of the prior communication.

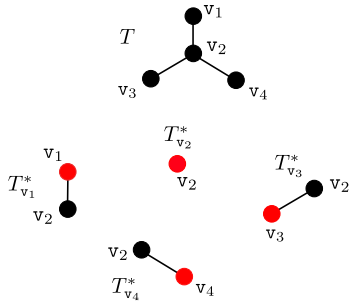

Fig. 1. Illustration of $\mathcal{T}^*$ for a tree having four vertices.

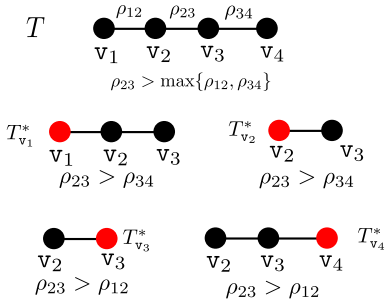

Fig. 2. An example where our scheme is suboptimal.

is achievable using a nested lattice coding scheme whose computational complexity grows as $O(N^{\alpha+1})$.

Note that if all terminals have identical quantization rate constraints, then the complexity is $O(N^2)$. Letting the quantization rates $R_{\mathrm{q}}^{(\mathtt{u})}$ in (4) go to infinity, we get that

Corollary 2. *In the fine quantization limit, i.e., as $R_{\mathrm{q}}^{(\mathtt{v})} \to \infty$ for all $\mathtt{v}$, a secret key rate of*

$$R_{\mathrm{key}} = \max_{T^* \in \mathcal{T}^*} \left\{ \min_{\mathtt{v} \in N_T(\mathtt{r}(T^*))} \frac{1}{2} \log_2 \left(\frac{1}{1-\rho^2_{\mathtt{r}(T^*)\mathtt{v}}} \right) + \sum_{\mathtt{u} \in V^* \setminus \mathtt{r}(T^*)} \min_{\mathtt{v} \in N_T(\mathtt{u})} \frac{1}{2} \log_2 \left(\frac{1-\rho^2_{\mathtt{u},\mathrm{par}(\mathtt{u})}}{1-\rho^2_{\mathtt{u},\mathtt{v}}} \right) \right\} \quad (5)$$

is achievable.

If there are no constraints on the quantization rates, then from [7, Theorem 3.1] and [1, Example 7], we know that the maximum achievable secret key rate is

$$C_{\mathrm{key}}^{(\infty)} = \min_{(\mathtt{u},\mathtt{v}) \in E} \frac{1}{2} \log_2 \left(\frac{1}{1-\rho^2_{\mathtt{uv}}} \right). \quad (6)$$

III. Remarks on the Achievable Secret Key Rate

A. The Two-User Case

Consider the two-user case with terminals $\mathtt{u}$ and $\mathtt{v}$. Let

$$\mathcal{R}(\mathtt{u},\mathtt{v}) := \frac{1}{2} \log_2 \left(\frac{e^{2R_{\mathrm{q}}^{(\mathtt{u})}}}{(e^{2R_{\mathrm{q}}^{(\mathtt{u})}}-1)(1-\rho^2_{\mathtt{uv}}) + 1 + \frac{\rho^2_{\mathtt{uv}} e^{2R_{\mathrm{q}}^{(\mathtt{u})}}}{e^{2R_{\mathrm{q}}^{(\mathtt{v})}}-1}} \right)$$

As we will see later, the above SK rate is achieved with $\mathtt{u}$ participating in the public communication and $\mathtt{v}$ remaining silent. The achievable SK rate, (4), is equal to $\max\{\mathcal{R}(\mathtt{u},\mathtt{v}), \mathcal{R}(\mathtt{v},\mathtt{u})\}$. A simple calculation reveals that if $R_{\mathrm{q}}^{(\mathtt{v})} > R_{\mathrm{q}}^{(\mathtt{u})}$, then $\mathcal{R}(\mathtt{u},\mathtt{v}) > \mathcal{R}(\mathtt{v},\mathtt{u})$. This means that in order to obtain a higher secret key rate using our scheme, the terminal with the lower quantization rate must communicate, while the other must remain silent.

If we let $R_{\mathrm{q}}^{(\mathtt{v})}$ in $\mathcal{R}(\mathtt{u},\mathtt{v})$ go to infinity, then we get the rate $R_{\mathrm{NN}} = \frac{1}{2} \log_2 \left(\frac{e^{2R_{\mathrm{q}}^{(\mathtt{u})}}}{(e^{2R_{\mathrm{q}}^{(\mathtt{u})}}-1)(1-\rho^2_{\mathtt{uv}})+1} \right)$ achieved in [7], which was shown to be optimal when we only restrict the quantization rate of one terminal.

B. Optimality of R_{key} in the Fine Quantization Limit

We present a class of examples where R_{key} is equal to the secret key capacity $C_{\mathrm{key}}^{(\infty)}$ in the fine quantization limit. One such example is the class of *homogeneous* Markov trees, where $\rho_{\mathtt{uv}} = \rho$ for all edges $(\mathtt{u},\mathtt{v})$. In this case, $\min_{\mathtt{v} \in N_T(\mathtt{u})} \frac{1}{2} \log_2 \left(\frac{1-\rho^2_{\mathtt{u},\mathrm{par}(\mathtt{u})}}{1-\rho^2_{\mathtt{u},\mathtt{v}}} \right) = 0$, and hence, by Corollary 2, $R_{\mathrm{key}} = \frac{1}{2} \log_2 \left(\frac{1}{1-\rho^2} \right) = C_{\mathrm{key}}^{(\infty)}$.

This property holds for a wider class of examples. Consider the case where T has a rooted subtree T^* such that for every $\mathtt{u} \in V^*$, $\arg\min_{\mathtt{v} \in N_T(\mathtt{u})} \rho_{\mathtt{uv}} = \mathrm{par}(\mathtt{u})$. Once again, we have $\min_{\mathtt{v} \in N_T(\mathtt{u})} \frac{1}{2} \log_2 \left(\frac{1-\rho^2_{\mathtt{u},\mathrm{par}(\mathtt{u})}}{1-\rho^2_{\mathtt{u},\mathtt{v}}} \right) = 0$. Moreover, the edge $(\mathtt{u},\mathtt{v}) \in E$ with the minimizing $\rho_{\mathtt{uv}}$ is incident on $\mathtt{r}(T^*)$. Hence, $R_{\mathrm{key}} = C_{\mathrm{key}}^{(\infty)}$.

C. Suboptimality of R_{key} in the Fine Quantization Limit

We can give several examples for which R_{key} in the fine quantization limit is strictly less than $C_{\mathrm{key}}^{(\infty)}$. Note that $\min_{\mathtt{v} \in N_T(\mathtt{u})} \frac{1}{2} \log_2 \left(\frac{1-\rho^2_{\mathtt{u},\mathrm{par}(\mathtt{u})}}{1-\rho^2_{\mathtt{u},\mathtt{v}}} \right) \le 0$, and if these terms are nonzero for every $T^* \in \mathcal{T}^*$, then the scheme is suboptimal. As a specific example, consider the Markov chain of Fig. 2, where $\rho_{23} > \max\{\rho_{12}, \rho_{34}\}$. Let us further assume that $\rho_{12} = \rho_{34}$. The secret key capacity is $C_{\mathrm{key}}^{(\infty)} = \frac{1}{2} \log_2 \frac{1}{1-\rho^2_{12}}$. Irrespective of which $T^* \in \mathcal{T}^*$ we choose (see Fig. 2), we have $\min_{\mathtt{v} \in N_T(\mathtt{r}(T^*))} \frac{1}{2} \log_2 \left(\frac{1}{1-\rho^2_{\mathtt{r}(T^*)\mathtt{v}}} \right) = C_{\mathrm{key}}^{(\infty)}$. Furthermore, the second term in (5) is negative for every T^*. This is because every T^* has some $\mathtt{u} \neq \mathtt{r}(T^*)$ for which $\arg\min_{\mathtt{v} \in V^*} \rho_{\mathtt{uv}} \neq \mathrm{par}(\mathtt{v})$.

IV. The Secret Key Generation Scheme

We now describe the lattice coding scheme that achieves the promised SK rate. Our scheme is very similar to the scheme given by Nitinawarat and Narayan [7] for the two-terminal case. We use a block encoding scheme just like the one in [7]. The total blocklength N is partitioned into N_{out} blocks of n samples each, i.e., $N = nN_{\mathrm{out}}$, where $N_{\mathrm{out}} = \min_{\mathtt{v}} 2^{nR_{\mathrm{q}}^{(\mathtt{v})}} - 1$.

A. Nested Lattices

We first describe the nested lattice codes which form the main component of our scheme. Some basic definitions and

relevant results on lattices have been outlined in [9, Appendix A]. Given a lattice Λ, let Q_Λ denote the lattice quantizer that maps every point in $\mathbb{R}^n$ to the closest point in Λ. The fundamental Voronoi region is defined as $\mathcal{V}(\Lambda) := \{\mathbf{x} \in \mathbb{R}^n : Q_\Lambda(\mathbf{x}) = \mathbf{0}\}$. For $\mathbf{x} \in \mathbb{R}^n$, let $[\mathbf{x}] \bmod \Lambda := \mathbf{x} - Q_\Lambda(\mathbf{x})$. Also, $\mathrm{vol}(\Lambda) := \mathrm{vol}(\mathcal{V}(\Lambda))$. The second moment per dimension of Λ is $\sigma^2(\Lambda) := \frac{1}{n\mathrm{vol}(\Lambda)} \int_{\mathcal{V}(\Lambda)} \|\mathbf{x}\|^2 d\mathbf{x}$.

Each terminal $\mathtt{v}$ uses a chain of n-dimensional nested lattices $(\Lambda_\mathtt{v}, \Lambda_\mathtt{v}^{(1)}, \Lambda_\mathtt{v}^{(2)})$, with $\Lambda_\mathtt{v}^{(2)} \subset \Lambda_\mathtt{v}^{(1)} \subset \Lambda_\mathtt{v}$. These are all Construction-A lattices [2], [3] obtained from linear codes of blocklength n over $\mathbb{F}_p$, with the prime p chosen large enough to ensure that these lattices satisfy the required goodness properties. Furthermore, $\Lambda_\mathtt{v}^{(1)}$ and $\Lambda_\mathtt{v}^{(2)}$ are obtained from subcodes of linear codes that generate $\Lambda_\mathtt{v}$. It is a fact [2] that $|\Lambda_\mathtt{v} \cap \mathcal{V}(\Lambda_\mathtt{v}^{(2)})|$ is an integer power of p. Let $p^{k_\mathtt{v}} := |\Lambda_\mathtt{v} \cap \mathcal{V}(\Lambda_\mathtt{v}^{(2)})|$. Fix any $\delta > 0$. The lattices are chosen so as to satisfy

$$\frac{1}{n}\log_2 |\Lambda_\mathtt{v} \cap \mathcal{V}(\Lambda_\mathtt{v}^{(2)})| = \frac{1}{n}\log_2 \frac{\mathrm{vol}(\Lambda_\mathtt{v}^{(2)})}{\mathrm{vol}(\Lambda_\mathtt{v})} = \frac{k_\mathtt{v}}{n}\log_2 p = R_\mathrm{q}^{(\mathtt{v})}, \tag{7}$$

$$\Big(\big(\mathrm{vol}(\Lambda_\mathtt{v}^{(2)})\big)^{2/n}/(2\pi e)\Big) = \big(1 + \sigma^2(\Lambda_\mathtt{v})\big)(1+\delta), \tag{8}$$

$$\frac{\big(\mathrm{vol}(\Lambda_\mathtt{v}^{(1)})\big)^{2/n}}{2\pi e} = \max_{\mathtt{u} \in N_T(\mathtt{v})} \Big(1 - \rho_{\mathtt{uv}}^2 + \sigma^2(\Lambda_\mathtt{v}) + \rho_{\mathtt{uv}}^2 \sigma^2(\Lambda_\mathtt{u})\Big) \times (1+\delta). \tag{9}$$

Furthermore, these lattices satisfy the following "goodness" properties [3]:

- $\Lambda_\mathtt{v}$ is good for covering.
- $\Lambda_\mathtt{v}^{(1)}$ and $\Lambda_\mathtt{v}^{(2)}$ are good for AWGN channel coding.

B. The SK Generation Protocol

Let us now describe the protocol. Suppose $\mathbf{x}_\mathtt{v} = (\mathbf{x}_\mathtt{v}^{(1)}, \ldots, \mathbf{x}_\mathtt{v}^{(N_\mathrm{out})})$ where $\mathbf{x}_\mathtt{v}^{(i)}$ denotes the ith block of length n. Each terminal $\mathtt{v}$ also generates random dithers $\{\mathbf{d}_\mathtt{v}^{(i)} : 1 \le i \le N_\mathrm{out}\}$, which are all uniformly distributed over $\mathcal{V}(\Lambda_\mathtt{v})$ and independent of each other. These are assumed to be known to all terminals.[3] The protocol consists of four parts.

- *Quantization:* Terminal $\mathtt{v} \in V$ computes
$$\mathbf{y}_\mathtt{v}^{(i)} = \big[Q_{\Lambda_\mathtt{v}}(\mathbf{x}_\mathtt{v}^{(i)} + \mathbf{d}_\mathtt{v}^{(i)}) - \mathbf{d}_\mathtt{v}^{(i)}\big] \bmod \Lambda_\mathtt{v}^{(2)}.$$
The terminals can only use $\mathbf{y}_\mathtt{v}^{(i)}$ for SK generation.
- *Information reconciliation: Analog phase:* Let $T^* = (V^*, E^*)$ denote the rooted tree in $\mathcal{T}^*$ which achieves the maximum in (4). The terminals in V^* are the only ones that communicate across the public channel. Terminal $\mathtt{v} \in V^*$ broadcasts
$$\mathbf{w}_\mathtt{v}^{(i)} = [\mathbf{y}_\mathtt{v}^{(i)}] \bmod \Lambda_\mathtt{v}^{(1)}.$$
across the public channel. Terminal $\mathtt{u}$ has access to $\mathbf{y}_\mathtt{u}^{(i)}$, and for every $\mathtt{v} \in N_{T^*}(\mathtt{u})$, it estimates
$$\widehat{\mathbf{y}}_\mathtt{v}^{(i)} = \mathbf{w}_\mathtt{v}^{(i)} + Q_{\Lambda_\mathtt{v}^{(1)}}\left(\rho_{\mathtt{uv}}\mathbf{y}_\mathtt{u}^{(i)} - \mathbf{w}_\mathtt{v}^{(i)}\right).$$
Having estimated $\mathbf{y}_\mathtt{v}^{(i)}$ for all neighbours $\mathtt{v}$, it estimates $\mathbf{y}_\mathtt{v}^{(i)}$ for all $\mathtt{v} \in V^*$ which are at a distance 2 from $\mathtt{u}$ (in the same manner), and so on, till it has estimated $\{\mathbf{y}_\mathtt{v}^{(i)} : \mathtt{v} \in V^*, 1 \le i \le N_\mathrm{out}\}$.
- *Information reconciliation: Digital phase:* To ensure that all N_out blocks can be recovered at all terminals with an arbitrarily low probability of error, we use a Slepian-Wolf scheme using Reed-Solomon codes. Terminal $\mathtt{v}$ uses an $(N_\mathrm{out}, K_\mathrm{out})$ Reed-Solomon code $\mathcal{C}_\mathtt{v}$ over $\mathbb{F}_{p^{k_\mathtt{v}}}$, where $K_\mathrm{out} = N_\mathrm{out}(1-2\delta)$. There exists a bijection $\phi_\mathtt{v}$ from $\Lambda_\mathtt{v} \cap \mathcal{V}(\Lambda_\mathtt{v}^{(2)})$ to $\mathbb{F}_{p^{k_\mathtt{v}}}$. Let $y_\mathtt{v}^{(i)} = \phi_\mathtt{v}(\mathbf{y}_\mathtt{v}^{(i)})$ and $\widehat{y}_\mathtt{v}^{(i)} = \phi_\mathtt{v}(\widehat{\mathbf{y}}_\mathtt{v}^{(i)})$. Let $\mathsf{y}_\mathtt{v}^{N_\mathrm{out}} = (y_\mathtt{v}^{(1)}, \ldots, y_\mathtt{v}^{(N_\mathrm{out})})$ and $\widehat{\mathsf{y}}_\mathtt{v}^{N_\mathrm{out}} = (\widehat{y}_\mathtt{v}^{(1)}, \ldots, \widehat{y}_\mathtt{v}^{(N_\mathrm{out})})$. We can write $\widehat{\mathsf{y}}_\mathtt{v}^{N_\mathrm{out}} = \mathsf{y}_\mathtt{v}^{N_\mathrm{out}} + \mathsf{e}_\mathtt{v}^{N_\mathrm{out}}$, where $\mathsf{e}_\mathtt{v}^{N_\mathrm{out}} = (e_\mathtt{v}^{(1)}, \ldots, e_\mathtt{v}^{(N_\mathrm{out})})$ is the error vector. Every $\mathsf{y}_\mathtt{v}^{N_\mathrm{out}}$ can be written uniquely as $\mathsf{y}_\mathtt{v}^{N_\mathrm{out}} = \mathsf{c}_\mathtt{v}^{N_\mathrm{out}} + \mathsf{s}_\mathtt{v}^{N_\mathrm{out}}$, where $\mathsf{c}_\mathtt{v}^{N_\mathrm{out}} \in \mathcal{C}_\mathtt{v}$, and $\mathsf{s}_\mathtt{v}^{N_\mathrm{out}}$ is a minimum Hamming weight representative of the coset to which $\mathsf{y}_\mathtt{v}^{N_\mathrm{out}}$ belongs in $\mathbb{F}_{p^{k_\mathtt{v}}}^{N_\mathrm{out}}/\mathcal{C}_\mathtt{v}$. Terminal $\mathtt{v}$ broadcasts $\mathsf{s}_\mathtt{v}^{N_\mathrm{out}}$ across the public channel.
From $\mathsf{s}_\mathtt{v}^{N_\mathrm{out}}$ and $\widehat{\mathsf{y}}_\mathtt{v}^{N_\mathrm{out}}$, terminal $\mathtt{u} \in V$ can compute $\widehat{\mathsf{c}}_\mathtt{v}^{N_\mathrm{out}} = \widehat{\mathsf{y}}_\mathtt{v}^{N_\mathrm{out}} - \mathsf{s}_\mathtt{v}^{N_\mathrm{out}} = \mathsf{c}_\mathtt{v}^{N_\mathrm{out}} + \mathsf{e}_\mathtt{v}^{N_\mathrm{out}}$. Using the decoder for the Reed-Solomon code, terminal $\mathtt{u}$ can compute $\mathsf{c}_\mathtt{v}^{N_\mathrm{out}}$ and hence $(\mathbf{y}_\mathtt{v}^{(i)} : 1 \le i \le N_\mathrm{out})$ provided that the Hamming weight of $\mathsf{e}_\mathtt{v}^{N_\mathrm{out}}$ is not too large.
- *Key generation:* Let $k := \sum_{\mathtt{v} \in V^*} k_\mathtt{v}$. There exists a (set) bijection ϕ from $(\bigtimes_{\mathtt{v} \in V^*} \mathbb{F}_{p^{k_\mathtt{v}}})$ to $\mathbb{F}_{p^k}$. Let $y^{(i)} = \phi(\mathbf{y}_\mathtt{v}^{(i)} : \mathtt{v} \in V^*)$. Let $q = p^k$ and $B = (\mathbf{w}_\mathtt{v}, \mathsf{s}_\mathtt{v}^{N_\mathrm{out}} : \mathtt{v} \in V^*)$. Then, [7, Lemma 4.5] guarantees the existence of an $\mathbb{F}_{p^k}$-valued $\lfloor \frac{N_\mathrm{out} R_\mathrm{key}}{\log_2 q} \rfloor \times N_\mathrm{out}$ matrix L, so that $L(y^{(1)}, \ldots, y^{(N_\mathrm{out})})^T$ is a secret key with a rate of
$$R_\mathrm{key} = \frac{1}{N} H(Y|D) - \sum_{\mathtt{v} \in V^*} R_\mathrm{com}^{(\mathtt{v})}, \tag{10}$$
where $Y = (\mathbf{y}_\mathtt{v}^{(i)} : \mathtt{v} \in V^*, 1 \le i \le N_\mathrm{out})$, $D := (\mathbf{d}_\mathtt{v}^{(i)} : \mathtt{v} \in V^*, 1 \le i \le N_\mathrm{out})$, and $R_\mathrm{com}^{(\mathtt{v})}$ denotes the total rate of communication of terminal $\mathtt{v}$.

C. Technical Lemmas

The following lemmas will be required to prove Theorem 1. Proofs of the same can be found in [9].

Lemma 3. *Fix a $\delta > 0$. For every $1 \le i \le N_\mathrm{out}$, we have*
$$\mathbb{E}_{\mathbf{y}_\mathtt{u}^{(i)}} \Pr[\widehat{\mathbf{y}}_\mathtt{v}^{(i)} \neq \mathbf{y}_\mathtt{v}^{(i)}] \le e^{-nE_{\mathtt{uv}}(\delta)} \tag{11}$$
where $E_{\mathtt{uv}}$ is a quantity which is positive for all $\delta > 0$ and all sufficiently large n.

Lemma 4 (Theorem 2, [8])**.** *The probability that the Reed-Solomon decoder incorrectly decodes $\mathbf{c}_\mathtt{v}^{N_\mathrm{out}}$ from $\widehat{\mathbf{c}}_\mathtt{v}^{N_\mathrm{out}}$ decays exponentially in N.*

[3] In principle, the random dither is not required. Similar to [6], we can show that there exist fixed dithers for which all our results hold. One could avoid the use of dithers by employing the techniques in [5], but we do not take that approach here.

Lemma 5. *Fix a $\delta > 0$, and let $D_i := (\mathbf{d}_{\mathtt{v}}^{(i)} : \mathtt{v} \in V^*)$. For all sufficiently large n, we have*

$$\frac{1}{n} H(\mathbf{y}_{\mathtt{v}}^{(i)} : \mathtt{v} \in V^* | D_i) \geq \mathcal{R}_{\text{ent}} - \delta, \tag{12}$$

where $\mathcal{R}_{\text{ent}}$ is given by (1).

V. Proof of Theorem 1

From (7) and (8), we can see that the quantization rates satisfy

$$R_{\text{q}}^{(\mathtt{v})} = \frac{1}{2} \log_2 \left(1 + \frac{1}{\sigma^2(\Lambda_{\mathtt{v}})} \right) + \log_2(1+\delta) + o_n(1). \tag{13}$$

One can see using Lemma 3 that at the end of the analog phase, the probability that an arbitrary terminal $\mathtt{u}$ erroneously estimates $\mathbf{y}_{\mathtt{v}}^{(i)}$ is at most $P_e^{\text{analog}} := \sum_{\mathtt{v}' \in V^*} \max_{\mathtt{u}' \in N_T(\mathtt{v}')} e^{-nE_{\mathtt{u}'\mathtt{v}'}(\delta)}$ for every $\mathtt{v}$ and every i. Lemma 4 then ensures that the probability of $\mathtt{u}$ making an error in estimating the entire block $(\mathbf{y}_{\mathtt{v}}^{(i)} : \mathtt{v} \in V^*, 1 \leq i \leq N_{\text{out}})$ goes to zero exponentially in N. This ensures that all terminals are able to recover the secret key reliably.

The achievable SK rate is given by (4). Let $D := (D_i : 1 \leq i \leq N_{\text{out}})$. Since the $\{\mathbf{y}_{\mathtt{v}}^{(i)} : 1 \leq i \leq N_{\text{out}}\}$ are i.i.d. for all $\mathtt{v}$, we have $\frac{1}{N} H(\mathbf{y}_{\mathtt{v}}^{(i)} : \mathtt{v} \in V^*, 1 \leq i \leq N_{\text{out}} | D) \geq \mathcal{R}_{\text{ent}} - \delta$ from Lemma 5. During the analog phase, each terminal $\mathtt{v}$ in V^* publicly communicates

$$\begin{aligned} R_{\text{analog}}^{(\mathtt{v})} &= \frac{1}{n} \log_2 \big(\text{vol}(\Lambda_{\mathtt{v}}^{(1)}) \big) / \big(\text{vol}(\Lambda_{\mathtt{v}}) \big) \\ &\leq \max_{\mathtt{u} \in N_T(\mathtt{v})} \frac{1}{2} \log_2 \frac{\big(1 - \rho_{\mathtt{uv}}^2 + \sigma^2(\Lambda_{\mathtt{v}}) + \rho_{\mathtt{uv}}^2 \sigma^2(\Lambda_{\mathtt{u}})\big)}{\sigma^2(\Lambda_{\mathtt{v}})} \\ &\qquad + o_n(1) + \delta. \end{aligned} \tag{14}$$

bits per sample. Here, we have used the fact that a covering-good lattice $\Lambda_{\mathtt{v}}$ satisfies $\text{vol}(\Lambda_{\mathtt{v}}) \to 2\pi e \sigma^2(\Lambda)$ as $n \to \infty$. On the other hand, during the digital phase, terminal $\mathtt{v}$ communicates $\frac{1}{N} \log |\mathbb{F}_{p^{k_{\mathtt{v}}}}^{N_{\text{out}}} / \mathcal{C}_{\mathtt{v}}| = 2\delta R_{\text{q}}^{(\mathtt{v})}$ bits per sample across the public channel. The total rate of communication by terminal $\mathtt{v}$, $R_{\text{com}}^{(\mathtt{v})}$, is at most $R_{\text{analog}}^{(\mathtt{v})} + 2\delta R_{\text{q}}^{(\mathtt{v})}$ bits per sample. Using this and (12) in (10), and finally substituting (13), we obtain (4).

A. Computational Complexity

We now show that the computational complexity is polynomial in N. The computational complexity is measured in terms of the number of binary operations required, and we assume that each floating-point operation (i.e., operations in $\mathbb{R}$) requires $O(1)$ binary operations. In other words, the complexity of a floating-point operation is independent of N. Recall that $N = nN_{\text{out}}$, where $N_{\text{out}} = \min_{\mathtt{v} \in V^*}(2^{nR_{\text{q}}^{(\mathtt{v})}} - 1)$. Also, $\alpha = (\max_{\mathtt{v} \in V^*} R_{\text{q}}^{(\mathtt{v})}) / (\min_{\mathtt{v} \in V^*} R_{\text{q}}^{(\mathtt{v})})$.

- *Quantization*: Each lattice quantization operation has complexity at most $O(2^{nR_{\text{q}}^{(\mathtt{v})}}) = O(N_{\text{out}}^{\alpha})$. There are N_{out} such quantization operations performed at each terminal, and hence the total complexity is $O(N_{\text{out}}^{\alpha+1})$.
- *Analog Phase*: Terminal $\mathtt{v}$ performs N_{out} quantization and $\text{mod}\Lambda_{\mathtt{v}}^{(1)}$ operations to compute $\{\mathbf{w}_{\mathtt{v}}^{(i)} : 1 \leq i \leq N_{\text{out}}\}$, and this requires a total complexity of $O(N_{\text{out}}^{\alpha+1})$. Computation of $\{\widehat{\mathbf{y}}_{\mathtt{v}}^{(i)} : 1 \leq i \leq N_{\text{out}}, \mathtt{v} \in V^*\}$ requires at most $N_{\text{out}}(|V^*| - 1)$ quantization operations, which also has a total complexity of $O(N_{\text{out}}^{\alpha+1})$.
- *Digital Phase*: Each terminal has to compute the coset representative. This is followed by the decoding of the Reed-Solomon code. Both can be done using the Reed-Solomon decoder, and this requires $O(N_{\text{out}} \log_2 N_{\text{out}})$ operations in $\mathbb{F}_{p^{k_{\mathtt{v}}}}$. Each finite field operation on the other hand requires $O(\log_2^2 p^{k_{\mathtt{v}}}) = O(n^2)$ binary operations [4, Chapter 2]. The total complexity is therefore $O(N^2)$.
- *Secret Key Generation*: This involves multiplication of a $\lfloor \frac{N_{\text{out}} R}{\log_2 q} \rfloor \times N_{\text{out}}$ matrix with an N_{out}-length vector, which requires $O(N_{\text{out}}^2 / \log q)$ operations over $\mathbb{F}_q$. Hence, the complexity required is $O(N_{\text{out}}^2 \log q) = O(N^2)$.

From all of the above, we can conclude that the complexity required is at most $O(N^{\alpha+1})$. This completes the proof of Theorem 1. □

VI. Acknowledgments

The first author would like to thank Manuj Mukherjee for useful discussions. The work of the first author was supported by the TCS Research scholarship programme, and that of the second author by a Swarnajayanti fellowship awarded by the Department of Science and Technology (DST), India.

References

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

[2] 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.

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

[4] D. Hankerson, A.J. Menezes, S. Vanstone, *Guide to Elliptic Curve Cryptography,* Springer Science & Business Media, 2006.

[5] C. Ling, L. Luzzi, M.R. Bloch, "Secret key generation from Gaussian sources using lattice hashing," *Proc. 2013 IEEE Int. Symp. Information Theory (ISIT)*, Istanbul, Turkey, pp.2621-2625.

[6] 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.

[7] S. Nitinawarat and P. Narayan, "Secret Key Generation for Correlated Gaussian Sources," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3373–3391, Jun. 2012.

[8] S. Vatedka and N. Kashyap, "A capacity-achieving coding scheme for the AWGN channel with polynomial encoding and decoding complexity," *accepted, 2016 Nat. Conf. Communications (NCC),* Guwahati, India [Online] Available: http://ece.iisc.ernet.in/~shashank/publications.html.

[9] S. Vatedka and N. Kashyap, "A Lattice Coding Scheme for Secret Key Generation from Gaussian Markov Tree Sources," [Online] Available: http://ece.iisc.ernet.in/~shashank/publications.html.

[10] S. Watanabe and Y. Oohama, "Secret key agreement from vector Gaussian sources by rate limited communication," *IEEE Trans. Inf. Forensics Security,* vol. 6, no. 3, pp. 541–550, Sep. 2011.