Secret Key Generation for Correlated Gaussian Sources

Sirin Nitinawarat, *Member, IEEE*, and Prakash Narayan, *Fellow, IEEE*

***Abstract*—Secret key generation by multiple terminals is considered based on their observations of jointly distributed Gaussian signals, followed by public communication among themselves. Exploiting an inherent connection between secrecy generation and lossy data compression, two main contributions are made. The first is a characterization of strong secret key capacity, and entails a converse proof technique that is valid for real-valued (and not necessarily Gaussian) as well as finite-valued signals. The capacity formula acquires a simple form when the terminals observe "symmetrically correlated" jointly Gaussian signals. For the latter setup with two terminals, considering schemes that involve quantization at one terminal, the best rate of an achievable secret key is characterized as a function of quantization rate; secret key capacity is attained as the quantization rate tends to infinity. Structured codes are shown to attain the optimum tradeoff between secret key rate and quantization rate, constituting our second main contribution.**

***Index Terms*—Linear code, multiterminal Gaussian source model, nested lattice code, public communication, quantization, secret key capacity, strong secrecy.**

I. Introduction

It is well known that separate terminals which observe the outputs of distinct albeit correlated sources can generate a secret key (SK) by means of public communication. Specifically, these terminals are able to generate "common randomness" (CR) regarding which an eavesdropper, with access to the public communication, can elicit only a negligible small amount of mutual information. This phenomenon, first observed for a model with two terminals by Bennett *et al.* [3] and Maurer [16], followed by Ahlswede and Csiszár [1], has been investigated further by many researchers. A model that includes a "helper" terminal observing the output of another source and assisting in generating SK was investigated by Ahlswede and Csiszár [1], and by Csiszár and Narayan [8]. These works were followed by those of Csiszár and Narayan [9], [10], in which SK generation was studied for models with an arbitrary number of terminals and an arbitrary subset of helpers. These models of SK generation, with all the underlying random variables (rvs) having finite alphabets, have been referred to broadly as "multiterminal source models."

In such a model [9], each terminal observes a distinct component of a *discrete* memoryless multiple source (DMMS). A set of terminals then wish to generate an SK with the cooperation of the remaining terminals. To this end, all the terminals are allowed to communicate publicly with each other, possibly interactively in several rounds, over a channel of unlimited capacity. No rate constraint is imposed on the public communication. We assume that an eavesdropper has full access to the public interterminal communication, but it is passive, i.e., it cannot tamper with the public communication. No restrictions are assumed on the eavesdropper's computational power. It is supposed further that the eavesdropper does not possess a wiretapping capability, i.e., it does not have direct access to a component of the multiple source; for a survey of wiretap models, see [15]. The SK capacity—the largest rate at which an SK can be generated—for a multiterminal source model involving a DMMS is determined in [9].

The capacity result in [9] reveals an innate connection between SK generation and lossless distributed data compression without any secrecy constraints. In particular, consider m terminals each observing independent and identically distributed (i.i.d.) repetitions of finite-valued rvs $X_1, \ldots, X_m$, respectively. A set of terminals $A \subseteq \{1, \ldots, m\}$ seek to generate an SK with the help of the remaining terminals. The SK capacity for this model equals the difference between the total joint entropy $H(X_1, \ldots, X_m)$ and the smallest rate of communication which enables each terminal in A to reconstruct near-losslessly all the m components of the DMMS, i.e., for the terminals in A to become "omniscient" [9]. The problem of determining the latter minimum rate is one of multiterminal data compression and does not involve any secrecy constraints.

The mentioned connection also suggests a means of generating an SK of optimum rate for this model by decomposing the problem of SK generation into two parts. First, the terminals publicly communicate at the most parsimonious rate to enable all the terminals in A to become omniscient. Second, each terminal in A generates an SK by extracting from this omniscience a part that is nearly independent of the public communication, and of which the eavesdropper has provably little knowledge. It is also shown in [9], [10] that the SK capacity can be achieved, based on the decomposition, by noninteractive communication and without randomization at the terminals.

In this paper, we consider SK generation for a "multiterminal Gaussian source model" by multiple terminals based on prior and privileged access to a set of (correlated) jointly Gaussian signals, followed by public discussion among themselves. A

Manuscript received March 25, 2011; revised October 20, 2011; accepted November 24, 2011. Date of publication January 12, 2012; date of current version May 15, 2012. This work was supported by the National Science Foundation under Grants ITR/SI(SPIII) 0112560, CCF0515124, CCF0635271, and CCF0830697. The material in this paper was presented in part at the 2008 IEEE International Symposium on Information Theory.

S. Nitinawarat was with the Department of Electrical and Computer Engineering and the Institute for Systems Research, University of Maryland, College Park, MD 20742 USA. He is now with the Department of Electrical and Computer Engineering and the Coordinated Science Laboratory, University of Illinois, Urbana, IL 61801 USA (e-mail: nitinawa@illinois.edu).

P. Narayan is with the Department of Electrical and Computer Engineering and the Institute for Systems Research, University of Maryland, College Park, MD 20742 USA (e-mail: prakash@umd.edu).

Communicated by Y. Oohama, Associate Editor for Shannon Theory.

Digital Object Identifier 10.1109/TIT.2012.2184075

characterization of SK capacity is not immediate, in general, since there is no meaningful analog of the concept of minimum communication for omniscience; in particular, the minimum rate of public communication for omniscience is unbounded. However, from the aforementioned discussion, we can expect an inherent connection between the problem of SK generation and lossy data compression, prompting the following natural questions. What is a characterization of SK capacity for a source model with memoryless jointly Gaussian multiple sources? Can an SK of optimum rate be generated using structured codes, e.g., lattice and linear codes?

This paper makes two main contributions. The first is a characterization of SK capacity for a multiterminal source model with $\mathbb{R}$-valued jointly Gaussian rvs X_i, $i = 1, \ldots, m$. This capacity result, obtained under suitable technical conditions, holds in a strong sense: the mutual information of the SK and the public communication vanishes exponentially in signal observation length. A concept of strong SK capacity was introduced in [17] in which the mentioned mutual information was required to decay to 0, while the stronger version we use here was considered first in [7]–[9]. Our achievability proof is based on a suitably refined quantization of the signals at the terminals. The converse proof develops a technique that is applicable to models with $\mathbb{R}$-valued (and not necessarily jointly Gaussian) rvs, as well as to the finite-alphabet model in [9]. Our general SK capacity formula acquires a simple form for a mutiterminal Gaussian source model in which the terminals observe "symmetrically correlated" jointly Gaussian signals. Our second main contribution involves a model of special interest that consists of two terminals which observe signals that are *a fortiori* symmetrically correlated. Considering schemes that involve quantization at one terminal, we characterize the best rate of an achievable SK as a function of quantization rate; SK capacity is attained as the quantization rate tends to infinity. Structured codes are shown to attain the optimum tradeoff between SK rate and quantization rate, constituting our second main contribution. This result shows how SK rate increases optimally with processing complexity (as measured by quantization rate) [18].

Our general model for SK generation with an arbitrary number of terminals resembles in structure the discrete mutiterminal models considered in [1], [9], and [16]. In particular, as in the latter models, we too do not impose any explicit constraints on the rates of public communication. For a discrete multiterminal source model, SK generation in the presence of rate constraints on public communication required a separate analysis, as in [8]. In this study, we have chosen to allow unfettered interactive public communication in order to understand the connections between SK generation and quantization rates for analog sources. Theorem 3.1 shows that every SK rate below SK capacity can be achieved by finite-rate quantization of the $\mathbb{R}$-valued multiple sources followed by finite-rate public communication; however, to approach SK capacity, the public communication rate grows (unboundedly) with the quantization rate. The question of characterizing the largest achievable SK rate for our model with public communication of bounded rate remains open in general. In recent related work [21], the authors have studied SK generation for two terminals observing correlated vector Gaussian sources, focusing on rate-constrained one-way communication from one terminal to a second terminal.

Our problem formulation is described in Section II, and the capacity results are proved in Section III. In Section IV, considering a model with two terminals, we propose a capacity-achieving algorithm for SK generation based on structured codes and quantization. We conclude in Section V with specific open questions that emerge from our study.

II. Preliminaries

We begin with a description of the multiterminal Gaussian source model for SK generation. Our model builds on the finite-alphabet model introduced in [9], [10]. Terminals $1, \ldots, m$ represent legitimate parties that cooperate in SK generation. We denote $\mathcal{M} = \{1, \ldots, m\}$.

Let $X_1, \ldots, X_m$ be $\mathbb{R}$-valued jointly Gaussian rvs with

$$\mathbb{E}\begin{bmatrix} X_1 \\ \vdots \\ X_m \end{bmatrix} = \mathbf{0}, \quad Q = \mathbb{E}\left[\begin{bmatrix} X_1 \\ \vdots \\ X_m \end{bmatrix}\begin{bmatrix} X_1, \ldots, X_m \end{bmatrix}\right] \tag{1}$$

where $Q_{ij} = \sigma_i \sigma_j \rho_{ij}$ with $\sigma_i^2 = \mathbb{E}\left[X_i^2\right]$, $1 \le i, j \le m$. We assume that Q is positive definite. It follows that

$$-\infty < h(X_B) \le h(X_{\mathcal{M}}) < \infty \tag{2}$$

for every (nonempty) $B \subseteq \mathcal{M}$, where h denotes differential entropy.

Terminal $i \in \mathcal{M}$ observes n i.i.d. repetitions of the rv X_i, namely $\mathbf{X}_i = \mathbf{X}_i^{(n)} = (X_{i1}, \ldots, X_{in})$. We use the notation $X_{\mathcal{M}} \triangleq (X_1, \ldots, X_m)$ and $\mathbf{X}_{\mathcal{M}} = \mathbf{X}_{\mathcal{M}}^{(n)} \triangleq (\mathbf{X}_1, \ldots, \mathbf{X}_m)$. Following these observations, the terminals are allowed to communicate over a public noiseless channel of unlimited capacity, possibly interactively in multiple rounds. We assume without loss of generality that the public communication, which can be interactive, takes place in consecutive time slots in r rounds. Specifically, following the formulation in [9], it is depicted by the mappings $f_1, \ldots, f_{mr}$ with f_ν corresponding to the transmission in slot ν by terminal $i \equiv \nu \bmod m$; we allow f_ν to yield any function of the source sequence $(\mathbf{X}_i = \mathbf{x}_i)$ observed at terminal i and of all previous communication $f_{[1,\nu-1]} = (f_1, \ldots, f_{\nu-1})$. The corresponding rvs representing the communication are denoted by $F_1, \ldots, F_{mr}$, with $F_\nu = f_\nu(\mathbf{X}_i, F_{[1,\nu-1]})$. We denote the communication collectively by $\mathbf{F} = F_{[1,mr]}$. The goal is for a set of terminals $A \subseteq \mathcal{M}$ to generate *secret* CR with the cooperation of the remaining terminals in $\mathcal{M} \backslash A$, which is concealed from an eavesdropper with access to the public communication $\mathbf{F}$. This is formalized next.

Following [9], given $\epsilon > 0$, a rv L is *ϵ-recoverable* from a rv Z if there exists a function $f(Z)$ that satisfies $\Pr\{L \ne f(Z)\} \le \epsilon$.

A function L of $\mathbf{X}_{\mathcal{M}}$ is *ϵ-common randomness* (ϵ-CR) for a set of terminals $A \subseteq \mathcal{M}$, achievable with communication $\mathbf{F}$, if L is ϵ-recoverable from $(\mathbf{X}_i, \mathbf{F})$, for each $i \in A$.

A function K of $\mathbf{X}_{\mathcal{M}}$ with values in a *finite* set $\mathcal{K}$ constitutes an *ϵ-secret key* (ϵ-SK) for a set of terminals $A \subseteq \mathcal{M}$, achievable with communication $\mathbf{F}$, if K is ϵ-CR for A and, in addition, K has a *security index*[1]

[1]All logarithms are natural.

$$s(K;\mathbf{F}) \stackrel{\triangle}{=} \log|\mathcal{K}| - H(K|\mathbf{F}) \leq \epsilon \tag{3}$$

where $|\mathcal{K}|$ denotes the cardinality of $\mathcal{K}$. Observe that if K is an ϵ-SK, then both

$$\log|\mathcal{K}| - H(K) \leq \epsilon \tag{4}$$

and

$$I(K \wedge \mathbf{F}) \leq \epsilon \tag{5}$$

hold so that, with ϵ typically being small, K is nearly uniformly distributed and is nearly independent of $\mathbf{F}$.

Definition 2.1: A nonnegative number R is an *achievable SK rate* for a set of terminals $A \subseteq \mathcal{M}$ if there exist[2] ϵ_n-SKs $K^{(n)}$ with values in finite sets $\mathcal{K}^{(n)}$ that are achievable with suitable public communication (with the number of rounds possibly depending on n), such that $\lim_{n\to\infty} \epsilon_n = 0$ and $\lim_{n\to\infty} \frac{1}{n}\log|\mathcal{K}^{(n)}| = R$. The supremum of achievable SK rates for A is called the *SK capacity* $C(A)$. An ϵ_n-SK is termed a *strong* SK if ϵ_n vanishes exponentially in n; the corresponding SK capacity is called the *strong SK capacity*.

Remark: In the early works on SK generation for source models, a weaker notion of SK was adopted [16], [1]. In particular, the corresponding notion of SK capacity therein, which we term *weak* SK capacity, is defined as the largest rate of a sequence of ϵ_n-SKs with ϵ_n being required to satisfy the weaker condition $\lim_{n\to\infty} n\epsilon_n = 0$; in effect, the secrecy requirement on the SK is relaxed from that in Definition 2.1 to $\lim_{n\to\infty} \frac{1}{n} s(K;\mathbf{F}) = 0$.

III. SK Capacity

We begin with the observation that the SK capacity $C(A)$ will depend on the joint distribution of $X_1,\ldots,X_m$ only through the correlation coefficients $\{\rho_{ij},\ 1 \leq i \neq j \leq n\}$. Clearly, replacing X_i by $\frac{X_i}{\sigma_i}$ where $\sigma_i > 0$ (by (1)), $i = 1,\ldots,m$, does not alter SK capacity.

As in [10], for $A \subseteq \mathcal{M}$, let

$$\mathcal{B}(A) = \{B \subset \mathcal{M} : B \neq \emptyset,\ B \not\supseteq A\} \tag{6}$$

and $\mathcal{B}_i(A)$ be its subset consisting of those $B \in \mathcal{B}(A)$ that contain i, $i \in \mathcal{M}$. Let $\Lambda(A)$ be the set of all collections $\lambda = \{\lambda_B : B \in \mathcal{B}(A)\}$ of weights $0 \leq \lambda_B \leq 1$, satisfying

$$\sum_{B\in\mathcal{B}_i(A)} \lambda_B = 1, \text{ for all } i = 1,\ldots,m. \tag{7}$$

Theorem 3.1: The (strong) SK capacity equals

$$C(A) = h(X_1,\ldots,X_m) - \max_{\lambda\in\Lambda(A)} \sum_{B\in\mathcal{B}(A)} \lambda_B h(X_B|X_{B^c}). \tag{8}$$

Corollary 3.2: The (strong) SK capacity for a "symmetric" Gaussian model with

$$Q = \begin{cases} Q_{ii} = \sigma_i^2, & 1 \leq i \leq m \\ Q_{ij} = \rho\sigma_i\sigma_j, & 1 \leq i \neq j \leq m \end{cases} \tag{9}$$

and with $A = \mathcal{M}$ equals

$$C(\mathcal{M}) = \frac{1}{2}\log\left[\frac{1}{(1-\rho)\,(1+(m-1)\rho)^{\frac{1}{m-1}}}\right]. \tag{10}$$

In particular, for $A = \mathcal{M} = \{1,2\}$

$$C(\{1,2\}) = \frac{1}{2}\log\frac{1}{1-\rho^2} = I\left(X_1 \wedge X_2\right). \tag{11}$$

Remarks:

1) The formula for SK capacity in Theorem 3.1 has the same form as that in ([9], Theorem 1) but with differential entropies in lieu of discrete entropies. As such, the terms appearing in the difference in (8) do not constitute meaningful analogs of the rate of omniscience and the minimum rate of communication for omniscience, respectively, unlike in ([9], Theorem 1).
2) As can be gleaned from its proof, Theorem 3.1 holds for $\mathbb{R}$-valued rvs X_i, $i = 1,\ldots,m$, that are not necessarily jointly Gaussian, provided that they satisfy (2) and the technical conditions (18), (19). Specifically, the achievability proof holds under (2), (18) and (19), whereas the converse proof requires only (2).

Proof of Theorem 3.1: The proof of Theorem 3.1 constitutes our first main contribution.

Achievability: The idea is to use scalar quantization of X_i at terminal i, $i = 1,\ldots,m$, followed by SK generation for the resulting finite-alphabet source model along the lines of [9]. By appropriately choosing the scalar quantizer, the claimed rate in (8) will be shown to be achievable in the limit of infinite quantization rates.

In particular, for each positive integer q, consider a quantizer $f_q : \mathbb{R} \to \{0,1,\ldots,2q^2\}$, where

$$f_q(x) = \begin{cases} 0, & \text{if } x > q \text{ or } x \leq -q \\ \lceil q(x+q)\rceil, & \text{if } -q < x \leq q. \end{cases} \tag{12}$$

At each terminal i, consider the $\{0,1,\ldots,2q^2\}$-valued rv $Y_i^{(q)} = f_q(X_i)$, $i = 1,\ldots,m$. Define the $\{0,1\}^m$-valued rv $Y_{m+1}^{(q)} = (\mathbf{1}(f_q(X_i) \neq 0))_{i=1}^m$.

Next, consider a fictitious (finite-alphabet) source model for "private key" generation with $m+1$ terminals consisting of legitimate terminals $1,\ldots,m$ that observe, respectively, $\mathbf{Y}_1^{(q)},\ldots,\mathbf{Y}_m^{(q)}$, and a (compromised helper) terminal $m+1$ that observes $\mathbf{Y}_{m+1}^{(q)}$. Now the terminals in the set $A \subseteq \mathcal{M} = \{1,\ldots,m\}$ seek to generate a *private key* (PK), say K, with the help of all the remaining terminals including terminal $m+1$, using public communication, say $\mathbf{F}$, so that the security condition (3) is satisfied with $\left(\mathbf{Y}_{m+1}^{(q)},\mathbf{F}\right)$ in the role of $\mathbf{F}$, i.e.

$$s\left(K;\mathbf{Y}_{m+1}^{(q)},\mathbf{F}\right) \leq \epsilon. \tag{13}$$

[2]The requirement is only for an infinite sequence of $K^{(n)}$ (i.e., for infinitely many n), and not necessarily for all n sufficiently large.

Such a PK K is concealed from terminal $m+1$ as well as from an eavesdropper that observes $\mathbf{F}$. The corresponding largest rate of such a PK, namely PK capacity, was characterized in ([9], Theorem 2); it was shown therein that PK capacity is achievable by allowing the compromised terminal $m+1$ to fully reveal its observations $\mathbf{Y}_{m+1}^{(q)}$ prior to public communication by the various terminals. From [9], the (strong) PK capacity for this finite-alphabet source model equals

$$\min_{\lambda\in\Lambda(A)} \begin{bmatrix} H\left(Y_{\mathcal{M}}^{(q)}|Y_{m+1}^{(q)}\right) \\ -\sum_{B\in\mathcal{B}(A)} \lambda_B H\left(Y_B^{(q)}|Y_{\mathcal{M}\setminus B}^{(q)}, Y_{m+1}^{(q)}\right) \end{bmatrix}. \quad (14)$$

Returning to the Gaussian model at hand, terminals $1,\ldots,m$ can simulate the mentioned model for PK generation by using the scalar quantizer f_q at each terminal and letting each terminal i reveal publicly the i.i.d. repetitions of the rv $\mathbf{1}(f_q(X_i)\neq 0)$, $i=1,\ldots,m$. Consequently, in the limit of infinite quantization

$$\lim_{q\to\infty}\min_{\lambda\in\Lambda(A)} \begin{bmatrix} H\left(Y_{\mathcal{M}}^{(q)}|Y_{m+1}^{(q)}\right) - \\ \sum_{B\in\mathcal{B}(A)} \lambda_B H\left(Y_B^{(q)}|Y_{\mathcal{M}\setminus B}^{(q)}, Y_{m+1}^{(q)}\right) \end{bmatrix} \quad (15)$$

is an achievable (strong) SK rate for the Gaussian model, by (14).

Next, for a fixed $\lambda\in\Lambda(A)$, using (7), we get

$$\begin{aligned} \sum_{B\in\mathcal{B}(A)} \lambda_B|\mathcal{B}\setminus B| &= \sum_{B\in\mathcal{B}(A)} \lambda_B\left(m-|B|\right) \\ &= m\sum_{B\in\mathcal{B}(A)}\lambda_B \\ &\quad - \sum_{B\in\mathcal{B}(A)}\lambda_B \sum_{i=1,\ldots,m}\mathbf{1}(i\in B) \\ &= m\left(\sum_{B\in\mathcal{B}(A)}\lambda_B - 1\right). \end{aligned} \quad (16)$$

Consequently, we have

$$\begin{aligned} &H\left(Y_{\mathcal{M}}^{(q)}|Y_{m+1}^{(q)}=\mathbf{1}\right) - \sum_{B\in\mathcal{B}(A)}\lambda_B H\left(Y_B^{(q)}|Y_{\mathcal{M}\setminus B}^{(q)}, Y_{m+1}^{(q)}=\mathbf{1}\right) \\ &= \sum_{B\in\mathcal{B}(A)}\lambda_B H\left(Y_{\mathcal{M}\setminus B}^{(q)}|Y_{m+1}^{(q)}=\mathbf{1}\right) \\ &\quad - \left(\sum_{B\in\mathcal{B}(A)}\lambda_B - 1\right) H\left(Y_{\mathcal{M}}^{(q)}|Y_{m+1}^{(q)}=\mathbf{1}\right) \\ &= \sum_{B\in\mathcal{B}(A)}\lambda_B\left[H\left(Y_{\mathcal{M}\setminus B}^{(q)}|Y_{m+1}^{(q)}=\mathbf{0}\right) - |\mathcal{M}\setminus B|\log q\right] \\ &\quad - \left(\sum_{B\in\mathcal{B}(A)}\lambda_B - 1\right)\left[H\left(Y_{\mathcal{M}}^{(q)}|Y_{m+1}^{(q)}=\mathbf{1}\right) - m\log q\right] \end{aligned} \quad (17)$$

by (16).

We proceed by using the following technical lemma whose proof is relegated to Appendix A.

Lemma 3.1: For the Gaussian rvs $X_1\ldots,X_m$ of Theorem 3.1, a quantizer f_q as described in (12), and every $B\subseteq\mathcal{M}=\{1,\ldots,m\}$, we get that

$$\lim_{q\to\infty}\left[H\left(Y_B^{(q)}|Y_{m+1}^{(q)}=\mathbf{1}\right) - |B|\log q\right] = h(X_B). \quad (18)$$

Furthermore

$$\lim_{q\to\infty} Pr\left\{Y_{m+1}^{(q)}=\mathbf{1}\right\} = 1. \quad (19)$$

Continuing with (17) upon using (18) of Lemma 3.1, we get that for every $\lambda\in\Lambda(A)$

$$\begin{aligned} &\lim_{q\to\infty}\begin{bmatrix} H\left(Y_{\mathcal{M}}^{(q)}|Y_{m+1}^{(q)}=\mathbf{1}\right) \\ -\sum_{B\in\mathcal{B}(A)}\lambda_B H\left(Y_B^{(q)}|Y_{\mathcal{M}\setminus B}^{(q)}, Y_{m+1}^{(q)}=\mathbf{1}\right)\end{bmatrix} \\ &= \sum_{B\in\mathcal{B}(A)}\lambda_B h\left(X_{\mathcal{M}\setminus B}\right) - \left(\sum_{B\in\mathcal{B}(A)}\lambda_B - 1\right) h\left(X_{\mathcal{M}}\right) \\ &= h\left(X_{\mathcal{M}}\right) - \sum_{B\in\mathcal{B}(A)}\lambda_B h\left(X_B|X_{B^c}\right). \end{aligned} \quad (20)$$

In [9], it was shown using the duality of linear programming that the minimization on the right side of the expression for the PK capacity (14) can be taken over a finite subset $\Lambda'(A)$ (of $\Lambda(A)$) that depends only on $\mathcal{M}$ and A. Consequently, the following achievable (strong) SK rate in (15) can be bounded below further as follows:

$$\begin{aligned} &\lim_{q\to\infty}\min_{\lambda\in\Lambda(A)}\begin{bmatrix} H\left(Y_{\mathcal{M}}^{(q)}|Y_{m+1}^{(q)}\right) \\ -\sum_{B:B\in\mathcal{B}(A)}\lambda_B H\left(Y_B^{(q)}|Y_{\mathcal{M}\setminus B}^{(q)}, Y_{m+1}^{(q)}\right)\end{bmatrix} \\ &= \lim_{q\to\infty}\min_{\lambda\in\Lambda'(A)\subset\Lambda(A)} \begin{bmatrix} H\left(Y_{\mathcal{M}}^{(q)}|Y_{m+1}^{(q)}\right) \\ -\sum_{B\in\mathcal{B}(A)}\lambda_B H\left(Y_B^{(q)}|Y_{\mathcal{M}\setminus B}^{(q)}, Y_{m+1}^{(q)}\right)\end{bmatrix} \\ &\geq \lim_{q\to\infty}\min_{\lambda\in\Lambda'(A)\subset\Lambda(A)} \Pr\left\{Y_{m+1}^{(q)}=\mathbf{1}\right\}\times \\ &\qquad \begin{bmatrix} H\left(Y_{\mathcal{M}}^{(q)}|Y_{m+1}^{(q)}=\mathbf{1}\right) \\ -\sum_{B\in\mathcal{B}(A)}\lambda_B H\left(Y_B^{(q)}|Y_{\mathcal{M}\setminus B}^{(q)}, Y_{m+1}^{(q)}=\mathbf{1}\right)\end{bmatrix} \\ &= \min_{\lambda\in\Lambda'(A)\subset\Lambda(A)}\left[h\left(X_{\mathcal{M}}\right) - \sum_{B\in\mathcal{B}(A)}\lambda_B h\left(X_B|X_{B^c}\right)\right] \\ &= \min_{\lambda\in\Lambda(A)}\left[h(X_{\mathcal{M}}) - \sum_{B\in\mathcal{B}(A)}\lambda_B h(X_B|X_{B^c})\right] \end{aligned}$$

which is (8), where the last-but-one equality above is by (19), (20) and by the fact that $\Lambda'(A)$, which does not depend on q, is finite.

Converse: The main technical tools are supplied by Lemma 3.2.

Lemma 3.2: Consider the i.i.d. repetitions of the jointly Gaussian rvs $X_{\mathcal{M}}=(X_1,\ldots,X_m)$ of Theorem 3.1, namely, $\mathbf{X}_{\mathcal{M}}=(\mathbf{X}_1,\ldots,\mathbf{X}_m)$, and let Z be a rv with a given joint distribution with $\mathbf{X}_{\mathcal{M}}$.

i) For any $\lambda\in\Lambda(A)$

$$h\left(\mathbf{X}_{\mathcal{M}}|Z\right)-\sum_{B\in\mathcal{B}(A)}\lambda_B h\left(\mathbf{X}_B|\mathbf{X}_{B^c},Z\right)\geq 0. \tag{21}$$

ii) For any $\lambda\in\Lambda(A)$, any $i=1,\ldots,m$, and any U_i that is a function of $(\mathbf{X}_i,Z)$, i.e., $U_i=u_i\left(\mathbf{X}_i,Z\right)$

$$\begin{aligned}&h\left(\mathbf{X}_{\mathcal{M}}|Z\right)-\sum_{B\in\mathcal{B}(A)}\lambda_B h\left(\mathbf{X}_B|\mathbf{X}_{B^c},Z\right)\\&=\sum_{B\in\mathcal{B}(A):B\ni i}\lambda_B I\left(U_i\wedge\mathbf{X}_{B^c}|Z\right)\\&\quad+\left[h\left(\mathbf{X}_{\mathcal{M}}|Z,U_i\right)-\sum_{B\in\mathcal{B}(A)}\lambda_B h\left(\mathbf{X}_B|\mathbf{X}_{B^c},Z,U_i\right)\right].\end{aligned} \tag{22}$$

Proof:

1) We have

$$\begin{aligned}&h\left(\mathbf{X}_{\mathcal{M}}|Z\right)\\&=\sum_{i\in\mathcal{M}}\left(\sum_{B\in\mathcal{B}(A):B\ni i}\lambda_B\right)h\left(\mathbf{X}_i|\mathbf{X}_1,\ldots,\mathbf{X}_{i-1},Z\right)\\&=\sum_{B\in\mathcal{B}(A)}\lambda_B\sum_{i\in B}h\left(\mathbf{X}_i|\mathbf{X}_1,\ldots,\mathbf{X}_{i-1},Z\right)\\&\geq\sum_{B\in\mathcal{B}(A)}\lambda_B\sum_{i\in B}h\left(\mathbf{X}_i|\mathbf{X}_{\{1,\ldots,i-1\}\cap B},\mathbf{X}_{B^c},Z\right)\\&=\sum_{B\in\mathcal{B}(A)}\lambda_B h\left(\mathbf{X}_B|\mathbf{X}_{B^c},Z\right).\end{aligned}$$

2) We see that

$$\begin{aligned}&h\left(\mathbf{X}_{\mathcal{M}}|Z\right)-\sum_{B\in\mathcal{B}(A)}\lambda_B h\left(\mathbf{X}_B|\mathbf{X}_{B^c},Z\right)\\&=h\left(\mathbf{X}_{\mathcal{M}}|Z,U_i\right)+I\left(U_i\wedge\mathbf{X}_{\mathcal{M}}|Z\right)\\&\quad-\sum_{B\in\mathcal{B}(A)}\lambda_B\begin{bmatrix}h\left(\mathbf{X}_B|\mathbf{X}_{B^c},Z,U_i\right)\\+I\left(U_i\wedge\mathbf{X}_B|\mathbf{X}_{B^c},Z\right)\end{bmatrix}\\&=\left[h\left(\mathbf{X}_{\mathcal{M}}|Z,U_i\right)-\sum_{B\in\mathcal{B}(A)}\lambda_B h\left(\mathbf{X}_B|\mathbf{X}_{B^c},Z,U_i\right)\right]\\&\quad+\left[I\left(U_i\wedge\mathbf{X}_{\mathcal{M}}|Z\right)-\sum_{B\in\mathcal{B}(A)}\lambda_B I\left(U_i\wedge\mathbf{X}_B|\mathbf{X}_{B^c},Z\right)\right]\\&=\left[h\left(\mathbf{X}_{\mathcal{M}}|Z,U_i\right)-\sum_{B\in\mathcal{B}(A)}\lambda_B h\left(\mathbf{X}_B|\mathbf{X}_{B^c},Z,U_i\right)\right]\\&\quad+\left(\sum_{B\in\mathcal{B}(A):B\ni i}\lambda_B\right)I\left(U_i\wedge\mathbf{X}_{\mathcal{M}}|Z\right)\\&\quad-\sum_{B\in\mathcal{B}(A):B\ni i}\lambda_B I\left(U_i\wedge\mathbf{X}_B|\mathbf{X}_{B^c},Z\right)\\&=\left[h\left(\mathbf{X}_{\mathcal{M}}|Z,U_i\right)-\sum_{B\in\mathcal{B}(A)}\lambda_B h\left(\mathbf{X}_B|\mathbf{X}_{B^c},Z,U_i\right)\right]\\&\quad+\sum_{B\in\mathcal{B}(A):B\ni i}\lambda_B I\left(U_i\wedge\mathbf{X}_{B^c}|Z\right).\end{aligned}$$

■

Suppose that $K^{(n)}$ represents an ϵ_n-SK for A achievable with (possibly interactive) communication $\mathbf{F}^{(n)}$ of, say, r rounds (as described in the second paragraph of Section II), where $\lim_{n\to 0}\epsilon_n=0$ (see Definition 2.1).

For $j=1,\ldots,mr$, by a repeated application of Lemma 3.2(ii) with $F_{[1,j]}$, F_j, and $j \bmod m$ in the roles of Z, U_i, and i, respectively, and the fact that $\sum_{B\in\mathcal{B}(A):B\ni i}\lambda_B I\left(U\wedge\mathbf{X}_{B^c}|Z\right)\geq 0$, we obtain

$$\begin{aligned}&h\left(\mathbf{X}_{\mathcal{M}}\right)-\sum_{B\in\mathcal{B}(A)}\lambda_B h\left(\mathbf{X}_B|\mathbf{X}_{B^c}\right)\\&\qquad\geq h\left(\mathbf{X}_{\mathcal{M}}|\mathbf{F}\right)-\sum_{B\in\mathcal{B}(A)}\lambda_B h\left(\mathbf{X}_B|\mathbf{X}_{B^c},\mathbf{F}\right).\end{aligned} \tag{23}$$

Next, for some $i\in A$, let $K_i=k_i^{(n)}\left(\mathbf{X}_i,\mathbf{F}\right)$ be such that $\Pr\left\{K_i^{(n)}=K^{(n)}\right\}\leq\epsilon_n$. Continuing from (23) by using Lemma 3.2(ii) again but now with $\mathbf{F}$ and K_i in the roles of Z and U_i, respectively, we obtain that

$$\begin{aligned}&h\left(\mathbf{X}_{\mathcal{M}}|\mathbf{F}\right)-\sum_{B\in\mathcal{B}(A)}\lambda_B h\left(\mathbf{X}_B|\mathbf{X}_{B^c},\mathbf{F}\right)\\&=\sum_{B\in\mathcal{B}(A):B\ni i}\lambda_B I\left(K_i\wedge\mathbf{X}_{B^c}|\mathbf{F}\right)\\&\quad+\left[h\left(\mathbf{X}_{\mathcal{M}}|\mathbf{F},K_i\right)-\sum_{B\in\mathcal{B}(A)}\lambda_B h\left(\mathbf{X}_B|\mathbf{X}_{B^c},\mathbf{F},K_i\right)\right]\\&\geq\sum_{B\in\mathcal{B}(A):B\ni i}\lambda_B I\left(K_i\wedge\mathbf{X}_{B^c}|\mathbf{F}\right),\ \text{by Lemma 3.2 (i)}\\&\geq\sum_{B\in\mathcal{B}(A):B\ni i}\lambda_B\left[H\left(K_i|\mathbf{F}\right)-H(K_i|\mathbf{X}_{B^c},\mathbf{F})\right]\\&\geq\sum_{B\in\mathcal{B}(A):B\ni i}\lambda_B\begin{bmatrix}H\left(K|\mathbf{F}\right)-H(K|K_i,\mathbf{F})\\-H\left(K_i|\mathbf{X}_{B^c},\mathbf{F}\right)\end{bmatrix}\\&\geq H\left(K|\mathbf{F}\right)-2\left[\log|\mathcal{K}|\epsilon_n+1\right],\\&\quad\text{by (7) and Fano's inequality}\\&\geq\left(\log|\mathcal{K}|-\epsilon_n\right)-2\left[\log|\mathcal{K}|\epsilon_n+1\right],\ \text{by (4)}\\&\geq(1-2\epsilon_n)\log|\mathcal{K}|-\epsilon_n-2.\end{aligned} \tag{24}$$

Consequently, by (24) and (23), we have for every $\lambda\in\Lambda(A)$ that

$$\lim_{n\to\infty}\frac{1}{n}\log|\mathcal{K}|\leq h(X_{\mathcal{M}})-\sum_{B\in\mathcal{B}(A)}\lambda_B h(X_B|X_{B^c})$$

The converse proof is completed by minimization over $\lambda\in\Lambda(A)$. ■

Proof of Corollary 3.2: For a set $B=\{i_1,\ldots,i_b\}\subset\mathcal{M}$, $i_1<i_2<\cdots<i_b$, and a permutation π of $\{1,\ldots,m\}$, let $\pi(B)$ denote $\{\pi(i_1),\ldots,\pi(i_b)\}$. For $\lambda^*\in\Lambda(\mathcal{M})$ attaining the maximum on the right side of (8) for the symmetric Gaussian model, consider $\lambda^{**}=\left\{\frac{1}{m!}\sum_\pi\lambda^*_{\pi(B)},\ B\in\mathcal{B}(\mathcal{M})\right\}$ where the summation is over all permutations of $\{1,\ldots,m\}$. It is readily seen that λ^{**} is in $\Lambda(\mathcal{M})$. By virtue of the fact that

$h(X_B|X_{B^c})$ depends on B only through $|B|$, it is clear that λ^{**} also attains the maximum in (8). Note that λ^{**} has the property that $\lambda^{**}_B = \lambda^{**}_{B'}$ for any B, B' such that $|B| = |B'|$. Consequently, the maximization on the right side of (8) reduces to

$$\max_{(\gamma_i)_{i=1}^{m-1}:\, \sum_{i=1}^{m-1}\gamma_i\binom{m-1}{i-1}=1} \sum_{i=1}^{m-1}\gamma_i\binom{m}{i}H_i = \max_{i=1,\ldots,m-1} \frac{\binom{m}{i}H_i}{\binom{m-1}{i-1}} \tag{25}$$

where $H_i = h\left(X_{\{1,\ldots,i\}}|X_{\{i+1,\ldots,m\}}\right) = h(X_B|X_{B^c})$ for any B with $|B| = i$. Let K_i denote the $i \times i$ matrix with diagonal entries being 1 and with all off-diagonal entries being ρ. It now follows from (8) that

$$\begin{aligned}
&C(\mathcal{M})\\
&= h(X_{\mathcal{M}}) - \max_{i=1,\ldots,m-1} \frac{\binom{m}{i}H_i}{\binom{m-1}{i-1}}\\
&= h(X_{\mathcal{M}}) - \max_{i=1,\ldots,m-1} \frac{m}{i}H_i\\
&= \min_{i=1,\ldots,m-1} \begin{bmatrix} h(X_1,\ldots,X_m) \\ -\frac{m}{i}h(X_1,\ldots,X_m) \\ +\frac{m}{i}h(X_{i+1},\ldots,X_m)\end{bmatrix}\\
&= \min_{i=1,\ldots,m-1} \begin{bmatrix} -\left(\frac{m-i}{i}\right)h(X_1,\ldots,X_m) \\ +\frac{m}{i}h(X_{i+1},\ldots,X_m)\end{bmatrix}\\
&= \min_{i=1,\ldots,m-1} \begin{bmatrix} -\left(\frac{m-i}{i}\right)\frac{1}{2}\log\left((2\pi e)^m \det(K_m)\right) \\ +\frac{m}{i}\frac{1}{2}\log\left((2\pi e)^{m-i}\det(K_{m-i})\right)\end{bmatrix}\\
&= \min_{i=1,\ldots,m-1} \frac{1}{2i}\log\left(\frac{(2\pi e)^{(m-i)m}\det(K_{m-i})^m}{(2\pi e)^{m(m-i)}\det(K_m)^{m-i}}\right)\\
&= \min_{i=1,\ldots,m-1} -\frac{1}{2i}\log\left(\frac{\det(K_{m-i})^m}{\det(K_m)^{m-i}}\right)\\
&= \min_{i=1,\ldots,m-1} \frac{1}{2i}\log\left(\frac{\left(\frac{1}{(1-\rho)^{m-i-1}(1+(m-i-1)\rho)}\right)^m}{\left(\frac{1}{(1-\rho)^{m-1}(1+(m-1)\rho)}\right)^{m-i}}\right)\\
&= \min_{i=1,\ldots,m-1} \frac{1}{2i}\log\left(\frac{(1-\rho)^i(1+(m-1)\rho)^{m-i}}{(1+(m-i-1)\rho)^m}\right)
\end{aligned} \tag{26}$$

where $-\frac{1}{m-1} < \rho < 1$ by the assumed positive definiteness of Q. By monotonicity, the minimum in (26) occurs at $i^* = m-1$, from which (10) follows. ∎

IV. Trading SK Rate Off Quantization Rate by Structured Codes

The achievability proof of Theorem 3.1 involves a scalar quantization of X_i at terminal i, $i = 1,\ldots,m$, followed by SK generation for the resulting finite-alphabet source model along the lines of [9], [10]; SK capacity is attained in the limit of infinite quantization rate. The SK, extracted from omniscience at all the terminals in $\mathcal{M}$, involves public communication by said terminals. As underlying the proof of achievability of SK capacity for the finite-alphabet source model with two terminals [16], [1], communication from a single terminal, say terminal 1, suffices to generate an optimum-rate SK from less-than-omniscience, namely from $\mathbf{X}_1$.

In the context of a Gaussian source model with two terminals, this motivates the following questions.

1) Supposing that quantization at rate R is permitted at terminal 1, what is the largest rate of an SK that can be generated from the quantized source at terminal 1 and the original Gaussian source at terminal 2 using public communication?
2) Does the rate of the SK thereby generated tend to SK capacity $C(\mathcal{M}=\{1,2\}) = \frac{1}{2}\log\frac{1}{1-\rho^2}$ (by (11) of Corollary 3.2) as $R \to \infty$?
3) Can an explicit code structure be identified for quantization, communication, as well as SK extraction?

The answers to these questions involve structured codes, namely nested lattice codes and linear codes, combined with randomization at the terminals.

Let M_1 and M_2 be independent $\mathcal{M}_1$- and $\mathcal{M}_2$-valued rvs with (M_1, M_2) being independent of $(\mathbf{X}_1, \mathbf{X}_2)$. For each $R > 0$, let $q_R : \mathcal{M}_1 \times \mathbb{R}^n \to \mathcal{Q}_R$ be a random (vector) quantizer of rate R, where $\mathcal{Q}_R \subset \mathbb{R}^n$ with $\frac{1}{n}\log|\mathcal{Q}_R| \le R$. Let $C(R)$ be the largest rate of an SK that can be generated from $q_R(M_1, \mathbf{X}_1)$ at terminal 1 and $(M_2, \mathbf{X}_2)$ at terminal 2 by public communication (cf., the second paragraph of Section II, with $(M_1, \mathbf{X}_1)$ and $(M_2, \mathbf{X}_2)$ in the roles of $\mathbf{X}_1$ and $\mathbf{X}_2$, respectively) among all choices of q_R, M_1, M_2 as above.

Theorem 4.1: For every $R > 0$, we have

$$C(R) = \frac{1}{2}\log\frac{1}{e^{-2I(X_1\wedge X_2)} + \left(1 - e^{-2I(X_1\wedge X_2)}\right)e^{-2R}}. \tag{27}$$

Furthermore, $C(R)$ is nondecreasing, concave, and continuous for $R \ge 0$, with $C(0) = 0$ and

$$\lim_{R\to\infty} C(R) = I(X_1 \wedge X_2) = C(\mathcal{M} = \{1,2\}). \tag{28}$$

Remark: The result of Theorem 4.1 cannot be compared directly with ([21, Theorem 1]). owing to differences in the specifics of the two respective models. Our model allows unrestricted interactive public communication but constrains signal quantization rate, whereas the latter considers rate-constrained one-way public communication but without any quantization restrictions. Also, while our achievability proof involves only one-way communication, the converse holds for any interactive communication based on the quantized source at terminal 1 and the Gaussian source at terminal 2.

It is clear from (27) that $C(R)$ is increasing and continuous for $R \ge 0$. Furthermore, $C(0) = 0$ and $\lim_{R\to\infty} C(R) = C(\mathcal{M} = \{1,2\})$ by (11). Concavity follows from the fact that

$$\frac{dC(R)}{dR} = \frac{(1-e^{-2I})e^{-2R}}{e^{-2R}(1-e^{-2I}) + e^{-2I}} = \frac{1}{1 + e^{2R}\frac{e^{-2I}}{1-e^{-2I}}}$$

which is positive and decreasing for $R \ge 0$, where

$$I = I(X_1 \wedge X_2) = \frac{1}{2}\log\frac{1}{1-\rho^2}. \tag{29}$$

We present first the converse proof. The proof of achievability using structured lattice codes and linear codes constitutes a second main contribution of this paper and is presented in Section IV-B.

A. Converse Proof

The proof uses the following technical lemma, the first part of which provides an alternative expression for $C(R)$ in Theorem 4.1.

Lemma 4.1:

(i) For every $R \geq 0$, it holds that

$$C(R) = \max_{\substack{U \multimap X_1 \multimap X_2 \\ I(U \wedge X_1) \leq R}} I(U \wedge X_2). \tag{30}$$

(ii) For each $n \geq 1$ and for every quantizer $q : \mathbb{R}^n \to \mathcal{Q}$ where $\mathcal{Q}$ is a finite set and $R' = \frac{1}{n} \log |\mathcal{Q}|$, it holds that

$$\frac{1}{n} I(q(\mathbf{X}_1) \wedge \mathbf{X}_2) \leq C(R'). \tag{31}$$

Proof: Without loss of generality, we assume that $X_2 = X_1 + N$, where $N \sim \mathcal{N}(0, \sigma_N^2)$ is independent of $X_1 \sim \mathcal{N}(0,1)$. Since

$$\rho = \frac{\mathbb{E}[X_1 X_2]}{\sqrt{\mathbb{E}[X_1^2]}\sqrt{\mathbb{E}[X_2{}^2]}} = \frac{\mathbb{E}[X_1(X_1+N)]}{\sqrt{1+\sigma_N^2}} = \frac{1}{\sqrt{1+\sigma_N^2}}$$

it follows that:

$$\sigma_N^2 = \frac{1}{\rho^2} - 1 \tag{32}$$

and $X_2 \sim \mathcal{N}\left(0, \frac{1}{\rho^2}\right)$.

Let (U, X_1, X_2) be such that $U \multimap X_1 \multimap X_2$ and $I(U \wedge X_1) \leq R$. We get

$$\begin{aligned}
&I(U \wedge X_2) \\
&\quad = h(X_2) - h(X_2|U) \\
&\quad = h(X_2) - h(X_1 + N|U) \\
&\quad \leq h(X_2) - \frac{1}{2} \log \left[e^{2h(X_1|U)} + e^{2h(N|U)} \right] && (33) \\
&\quad = h(X_2) - \frac{1}{2} \log \left[e^{2h(X_1|U)} + e^{2h(N)} \right] && (34)
\end{aligned}$$

where (33) follows from the conditional entropy power inequality, and (34) follows from:

$$\begin{aligned}
0 &= I(U \wedge X_2|X_1) = I(U \wedge X_1 + N|X_1) \\
&= I(U \wedge N|X_1) = I(U, X_1 \wedge N) \\
&\geq I(U \wedge N)
\end{aligned}$$

where the fourth equality is by the fact that X_1 and N are independent.

Following from (34), we have

$$\begin{aligned}
&I(U \wedge X_2) \\
&\quad \leq \frac{1}{2} \log ((2\pi e) \frac{1}{\rho^2}) \\
&\qquad - \frac{1}{2} \log \left[e^{2h(X_1|U)} + (2\pi e) \frac{1-\rho^2}{\rho^2} \right] && (35) \\
&\quad = \frac{1}{2} \log ((2\pi e) \frac{1}{\rho^2}) \\
&\qquad - \frac{1}{2} \log \left[e^{-2I(U \wedge X_1)} e^{2h(X_1)} + (2\pi e) \frac{1-\rho^2}{\rho^2} \right] \\
&\quad \leq \frac{1}{2} \log ((2\pi e) \frac{1}{\rho^2}) \\
&\qquad - \frac{1}{2} \log \left[e^{-2R} (2\pi e) + (2\pi e) \frac{1-\rho^2}{\rho^2} \right] \\
&\quad = \frac{1}{2} \log \frac{1}{e^{-2R}\rho^2 + (1-\rho^2)} \\
&\quad = \frac{1}{2} \log \frac{1}{e^{-2R}(1 - e^{-2I(X_1 \wedge X_2)}) + e^{-2I(X_1 \wedge X_2)}} \\
&\quad = C(R). && (36)
\end{aligned}$$

The first inequality follows from (32); the second inequality follows from $I(U \wedge X_1) \leq R$. Consequently

$$\max_{\substack{U \multimap X_1 \multimap X_2 \\ I(U \wedge X_1) \leq R}} I(U \wedge X_2) \leq C(R).$$

To show equality, i.e., to establish (30), we shall select a rv U that satisfies $U \multimap X_1 \multimap X_2$ and achieves equalities in both (33) (and, hence, (35)) and (36). To this end, we shall find a zero-mean Gaussian rv U satisfying $I(U \wedge X_2|X_1) = 0$, $I(X_1 \wedge N|U) = 0$ and $I(U \wedge X_1) = R$. By the conditional entropy power inequality, the condition $I(X_1 \wedge N|U) = 0$ will give equality in (33) and the condition $I(U \wedge X_1) = R$ will give equality in (36). Specifically, let $U = X_1 + \tilde{N}$, where $\tilde{N}$ is independent of (X_1, X_2) and $\tilde{N} \sim \mathcal{N}(0, \left(\frac{e^{-2R}}{1-e^{-2R}}\right))$. Clearly, $I(U \wedge X_2|X_1) = 0$. Also

$$\begin{aligned}
I(U \wedge X_1) &= h(U) - h(U|X_1) = \frac{1}{2} \log \frac{\sigma_U^2}{\sigma_{\tilde{N}}^2} \\
&= \frac{1}{2} \log \left(\frac{1}{\sigma_{\tilde{N}}^2} + 1 \right) = R.
\end{aligned}$$

Next

$$\begin{aligned}
\mathbb{E}[NU] &= \mathbb{E}[(X_2 - X_1)(X_1 + \tilde{N})] = \mathbb{E}[(X_2 - X_1)X_1] \\
&= \mathbb{E}[NX_1] = 0.
\end{aligned}$$

The second and last equalities hold since $\tilde{N}$ is independent of (X_1, X_2) and N is independent of X_1, respectively. Since (U, N) are jointly Gaussian with $\mathbb{E}[U] = 0$ $(= \mathbb{E}[N])$, U is independent of N. Consequently

$$\begin{aligned}
I(X_1 \wedge N|U) &= I(X_1, U \wedge N) = I(X_1, \tilde{N} \wedge N) \\
&= I(X_1 \wedge N) + I(\tilde{N} \wedge N|X_1) \\
&\leq I(X_1 \wedge N) + I(\tilde{N} \wedge N, X_1)
\end{aligned}$$

$$= I(X_1 \wedge N) + I(\tilde{N} \wedge X_1, X_2) = 0$$

again using the independence of N and X_1 and that of $\tilde{N}$ and (X_1, X_2). With this choice of U, (30) is established.

The proof of part (ii) is similar to the converse proof in [22] and is given in Appendix B. ∎

Let K be an ϵ_n-SK generated by a scheme in Theorem 4.1 using a randomized quantizer q of rate at most R together with public communication $\mathbf{F}$ and randomization M_1, M_2. Then

$$\begin{aligned}
H(K) &= I(K \wedge M_2, \mathbf{F}, \mathbf{X}_2) + H(K|M_2, \mathbf{F}, \mathbf{X}_2) \\
&= I(K \wedge \mathbf{F}) + I(K \wedge M_2, \mathbf{X}_2|\mathbf{F}) \\
&\quad + H(K|M_2, \mathbf{F}, \mathbf{X}_2) \\
&\le \epsilon_n + I(K, M_1, q(M_1, \mathbf{X}_1) \wedge M_2, \mathbf{X}_2|\mathbf{F}) \\
&\quad + H(K|M_2, \mathbf{F}, \mathbf{X}_2) \\
&= \epsilon_n + I(M_1, q(M_1, \mathbf{X}_1) \wedge M_2, \mathbf{X}_2|\mathbf{F}) \\
&\quad + I(K \wedge M_2, \mathbf{X}_2|M_1, q(M_1, \mathbf{X}_1), \mathbf{F}) \\
&\quad + H(K|M_2, \mathbf{F}, \mathbf{X}_2) \\
&\le \epsilon_n + I(M_1, q(M_1, \mathbf{X}_1) \wedge M_2, \mathbf{X}_2|\mathbf{F}) \\
&\quad + H(K|M_1, q(M_1, \mathbf{X}_1), \mathbf{F}) + H(K|M_2, \mathbf{F}, \mathbf{X}_2) \\
&\le \epsilon_n + I(M_1, q(M_1, \mathbf{X}_1) \wedge M_2, \mathbf{X}_2|\mathbf{F}) \\
&\quad + 2(\epsilon_n \log|\mathcal{K}| + 1) \\
&\le \epsilon_n + I(M_1, q(M_1, \mathbf{X}_1) \wedge M_2, \mathbf{X}_2) \\
&\quad + 2(\epsilon_n \log|\mathcal{K}| + 1) \qquad (37) \\
&\le \epsilon_n + I(q(M_1, \mathbf{X}_1) \wedge \mathbf{X}_2|M_1) \\
&\quad + 2(\epsilon_n \log|\mathcal{K}| + 1) \qquad (38)
\end{aligned}$$

where the first inequality follows from (5); the third inequality follows from the fact that K is recoverable from $(M_1, q(M_1, \mathbf{X}_1), \mathbf{F})$ as also from $(M_2, \mathbf{F}, \mathbf{X}_2)$; (37) follows from [1, Lemma 2.2] (equivalently, this is tantamount to the repeated use of Lemma 3.2 (ii) in a manner similar to the attainment of (23)); and the last inequality follows from the mutual independence of M_1, M_2 and $(\mathbf{X}_1, \mathbf{X}_2)$.

Using Lemma 4.1 and the fact that M_1 and $(\mathbf{X}_1, \mathbf{X}_2)$ are mutually independent, it follows that:

$$\frac{1}{n} I(q(M_1, \mathbf{X}_1) \wedge \mathbf{X}_2|M_1) \le C(\frac{1}{n} \log|\mathcal{Q}|).$$

Continuing from (38) using (4), we have

$$\frac{1}{n} \log|\mathcal{K}| \le C(\frac{1}{n} \log|\mathcal{Q}|) + o_n(1).$$

The converse proof is completed by noting that $C(R)$ is continuous for $R \ge 0$. ∎

B. SK Generation Scheme Using Nested Lattice and Linear Codes, and Achievability Proof

In order to describe our scheme for achieving $C(R)$ and, hence, SK capacity in Theorem 4.1, using nested lattice codes and linear codes, we first compile pertinent definitions and facts from [25]. Our scheme and its performance are presented in Section IV-BI.

Nested Lattice Codes: Definitions and Facts

Definition 4.1: Consider n basis (column) vectors $\mathbf{g}_1, \ldots, \mathbf{g}_n$ in $\mathbb{R}^n$. An *n-dimensional lattice code* Λ is the set of all integral combinations of these basis vectors, i.e.

$$\Lambda \stackrel{\triangle}{=} \{\lambda : \lambda = G\mathbf{i} \text{ for some } \mathbf{i} \in \mathbb{Z}^n\}$$

with $n \times n$ generating matrix $G = [\mathbf{g}_1, \ldots, \mathbf{g}_n]$. Clearly, Λ contains the zero vector $\mathbf{0}$ in $\mathbb{R}^n$.

1) The *Voronoi region* of a lattice code Λ, denoted by $\nu(\Lambda)$, is the nearest neighbor set of $\mathbf{0}$ in $\mathbb{R}^n$, i.e.
$$\nu(\Lambda) \stackrel{\triangle}{=} \{\mathbf{u} \in \mathbb{R}^n : \|\mathbf{u}\| < \min_{\lambda \in \Lambda, \lambda \ne \mathbf{0}} \|\mathbf{u} - \lambda\|\}$$
where $\|\cdot\|$ denotes Euclidean norm. Let $|\nu(\Lambda)|$ denote the volume in $\mathbb{R}^n$ of $\nu(\Lambda)$.
2) The *second moment per dimension* of a lattice code Λ, denoted by $\sigma^2(\Lambda)$, is
$$\sigma^2(\Lambda) \stackrel{\triangle}{=} \frac{1}{n} \text{Var}[\text{rv distributed uniformly in } \nu(\Lambda)].$$
3) The *covering radius of a lattice code* Λ, denoted by $r_\Lambda^{\text{cov}}(n)$, is the infimum of all positive numbers r such that $\mathbb{R}^n \subseteq \Lambda + r\mathcal{B}$, where $\mathcal{B}$ be the n-dimensional sphere with unit radius.
4) The operation of *quantization* by a lattice code Λ, denoted by Q_Λ, is
$$Q_\Lambda(\mathbf{x}) \stackrel{\triangle}{=} \arg\min_{\lambda \in \Lambda} \|\mathbf{x} - \lambda\|, \ \mathbf{x} \in \mathbb{R}^n$$
where ties are broken arbitrarily.
5) The *mod* operation of a lattice code Λ is
$$\mathbf{x} \bmod \Lambda \stackrel{\triangle}{=} \mathbf{x} - Q_\Lambda(\mathbf{x}), \ \mathbf{x} \in \mathbb{R}^n$$
and corresponds to the quantization error.

The following property of the mod operation (cf., [25]) will be useful:

$$((\mathbf{x} \bmod \Lambda) + \mathbf{y}) \bmod \Lambda = (\mathbf{x} + \mathbf{y}) \bmod \Lambda, \ \mathbf{x}, \mathbf{y} \in \mathbb{R}^n. \quad (39)$$

A pair of lattice codes Λ_1, Λ_2 are *nested*, i.e., $\Lambda_1 \supset \Lambda_2$, if there exists an $n \times n$ matrix H with $\mathbb{Z}$-valued entries and with $\det(H) > 1$, such that $G_2 = G_1 H$, where G_1 and G_2 are the generating matrices of Λ_1 and Λ_2, respectively. It follows that $|\nu(\Lambda_2)|/|\nu(\Lambda_1)| = \det(H)$.

For $\lambda \in \Lambda_1$, the set $\lambda + \Lambda_2 \subset \Lambda_1$ is called a coset of Λ_2 relative to Λ_1; there are exactly $|\nu(\Lambda_2)|/|\nu(\Lambda_1)|$ distinct such cosets. For $\lambda' \ne \lambda''$ belonging to both Λ_1 and $\nu(\Lambda_2)$, the cosets $\lambda' + \Lambda_2$ and $\lambda'' + \Lambda_2$ are disjoint. It transpires that we can always find a set $\mathcal{S}$ of $|\nu(\Lambda_2)|/|\nu(\Lambda_1)|$ lattice points of Λ_1, comprising all the lattice points of Λ_1 in $\nu(\Lambda_2)$ and some of the lattice points of Λ_1 on the boundary of $\nu(\Lambda_2)$ such that for distinct $\mathbf{v} \in \mathcal{S}$, the sets $\mathbf{v} + \Lambda_2$ are disjoint and furthermore

$$\Lambda_1 = \bigsqcup_{\mathbf{v} \in \mathcal{S}} \{\mathbf{v} + \Lambda_2\}.$$

The set $\mathcal{S} \subset \Lambda_1$ is called a set of coset leaders of Λ_2 relative to Λ_1; note that there can be several such sets $\mathcal{S}$ since the lattice points of Λ_1 on the boundary of $\nu(\Lambda_2)$ can be selected in many ways. Upon fixing one such set $\mathcal{S}$, the ties of the quantization operation $Q_{\Lambda_2}(\mathbf{x})$, $\mathbf{x} \in \Lambda_1$, can be broken systematically in a

unique manner by requiring that $\mathbf{x} \bmod \Lambda_2 = \mathbf{x} - Q_{\Lambda_2}(\mathbf{x})$ coincides with the unique coset leader in $\mathcal{S}$ of the coset containing $\mathbf{x}$.

In the *dithered* quantization of a source using a lattice code (cf., [23], [24]), a rv distributed uniformly in its Voronoi region and independent of the source is added to the source sequence prior to quantization. This procedure, in effect, decorrelates the "quantization error" from the source, as formalized in the following result from [23], [24].

Lemma 4.2 [23], [24]: For an $\mathbb{R}^n$-valued rv $\mathbf{X}$ and any given lattice code Λ, let $\mathbf{U}$ be the "dither" rv distributed uniformly in $\nu(\Lambda)$ and independent of $\mathbf{X}$. Then, the quantization error $(\mathbf{X}+\mathbf{U}) - Q_\Lambda(\mathbf{X}+\mathbf{U})$ is independent of $\mathbf{X}$ and is distributed as $\mathbf{U}$.

1) Scheme: Our scheme for SK generation consists of two steps—analog, followed by digital. It is motivated by, and partly follows, the approach in [25].

Analog Part: In the first (analog) step, terminals 1 and 2 agree upon three n-dimensional nested lattice codes $\Lambda_1 \supset \Lambda_2 \supset \Lambda_3$ to be specified later. The following operations are performed on N i.i.d. repetitions $(\mathbf{X}_{1,i}, \mathbf{X}_{2,i})$, $i = 1, \ldots, N$, of $(\mathbf{X}_1, \mathbf{X}_2)$, where $\mathbf{X}_1$, $\mathbf{X}_2 \in \mathbb{R}^n$. *We remark that the reason for the use of N i.i.d. repetitions is to obtain strong secrecy in step (D.2) below.*

- (A.1) *Dithered quantization at terminal 1*: Terminal 1 generates i.i.d. rvs $\mathbf{U}_i$, $i = 1, \ldots, N$, where $\mathbf{U}_i$ is uniformly distributed in $\nu(\Lambda_1)$, and $\{\mathbf{U}_i, \mathbf{X}_{1,i}, \mathbf{X}_{2,i}\}_{i=1}^N$ are mutually independent. This is followed by dithered quantization of $\alpha\mathbf{X}_{1,i}$, $i = 1, \ldots, N$, and a mod operation of the lattice code Λ_3 to yield
$$\mathbf{L}_i = Q_{\Lambda_1}(\alpha\mathbf{X}_{1,i} + \mathbf{U}_i) \bmod \Lambda_3 \tag{40}$$
for $\alpha > 0$ to be specified later. Each $\mathbf{L}_i$ takes values in the set of coset leaders of Λ_3 relative to Λ_1, denoted by $\mathcal{L}$, where $|\mathcal{L}| = \frac{|\nu(\Lambda_3)|}{|\nu(\Lambda_1)|}$. The associated quantization rate is $\cong \frac{1}{n}\log\frac{|\nu(\Lambda_3)|}{|\nu(\Lambda_1)|}$.
- (A.2) *Public communication from terminal 1 to terminal 2*: Terminal 1 computes
$$\mathbf{P}_i = \mathbf{L}_i \bmod \Lambda_2 = Q_{\Lambda_1}(\alpha\mathbf{X}_{1,i} + \mathbf{U}_i) \bmod \Lambda_2,\ i = 1, \ldots, N \tag{41}$$
since $\Lambda_2 \supset \Lambda_3$, and publicly communicates $(\mathbf{P}^N, \mathbf{U}^N) = (\mathbf{P}_1, \ldots, \mathbf{P}_N, \mathbf{U}_1, \ldots, \mathbf{U}_N)$ to terminal 2. Observe that each $\mathbf{P}_i$ takes values in the set of coset leaders of Λ_2 relative to Λ_1, denoted by $\mathcal{P}$, with $|\mathcal{P}| = \frac{|\nu(\Lambda_2)|}{|\nu(\Lambda_1)|}$.
- (A.3) *Reconstruction of quantized rvs at terminal 2*: Terminal 2 reconstructs $\mathbf{L}_i$ as $\hat{\mathbf{L}}_i$, $i = 1, \ldots, N$, where
$$\hat{\mathbf{L}}_i = [(\mathbf{P}_i - \alpha\mathbf{X}_{2,i} - \mathbf{U}_i) \bmod \Lambda_2 + \alpha\mathbf{X}_{2,i} + \mathbf{U}_i] \bmod \Lambda_3. \tag{42}$$

For $R > 0$ and an arbitrary but fixed $D > 0$, we select α as
$$\alpha(R, D) = \frac{\sqrt{D}\sqrt{e^{2R} - 1}}{\sigma_{X_1}} \tag{43}$$
whereby
$$R = \frac{1}{2}\log\frac{\alpha^2\sigma_{X_1}^2 + D}{D}. \tag{44}$$

Our following main technical lemma summarizes the outcome of the first step of the algorithm.

Lemma 4.3: For $R > 0$, let
$$R_p = R_p(R) \stackrel{\triangle}{=} \frac{1}{2}\log\left(\left(e^{2R} - 1\right)e^{-2I} + 1\right) \tag{45}$$
with I as in (29). For every $\epsilon > 0$ and all n sufficiently large, there exist n-dimensional nested lattice codes $\Lambda_1 \supset \Lambda_2 \supset \Lambda_3$ such that, for $i = 1, \ldots, N$
$$\frac{1}{n}\log|\mathcal{L}| \le R + \epsilon,\ \frac{1}{n}\log|\mathcal{P}| \le R_p + \epsilon \tag{46}$$
$$Pr\{\hat{\mathbf{L}}_i \ne \mathbf{L}_i\} = o_n(1) \tag{47}$$
and
$$R - \frac{1}{n}H(\mathbf{L}_i|\mathbf{U}_i) = o_n(1). \tag{48}$$

Digital Part: Before describing the second (digital) part, we note that the (finite) set $\mathcal{L}$ in step A.1 can be shown to be in 1–1 correspondence with a (finite) field $\mathbb{F}_{|\mathcal{L}|}$ through a mapping f (see Lemma 4.4 and Appendix C); the rvs $f(\mathbf{L}_i)$ then will take values in $\mathbb{F}_{|\mathcal{L}|}$, $i = 1, \ldots, N$. The Digital Part of the scheme entails the following.

- (D.1) *CR generation at terminals 1 and 2 by Slepian-Wolf data compression*: The i.i.d. sequence $f(\mathbf{L}_i)$, $i = 1, \ldots, N$, at terminal 1 is reconstructed near-losslessly at terminal 2 with $f(\hat{\mathbf{L}}_i)$, $i = 1, \ldots, N$, as side information using Slepian–Wolf data compression. This reconstruction is performed with decoding error probability vanishing exponentially in N. Specifically, a linearly encoded Slepian–Wolf codeword $A_1 f(\mathbf{L})^N$ is transmitted publicly, where $f(\mathbf{L})^N = (f(\mathbf{L}_1), \ldots, f(\mathbf{L}_N))$ and A_1 is a matrix with entries taking values in $\mathbb{F}_{|\mathcal{L}|}$. Terminal 2 produces an estimate
$$\widehat{f(\mathbf{L})^N} = (f(\mathbf{L}_1), \widehat{\ldots}, f(\mathbf{L}_N))$$
based on the codeword $A_1 f(\mathbf{L})^N$ and the side information
$$f(\hat{\mathbf{L}})^N = (f(\hat{\mathbf{L}}_1), \ldots, f(\hat{\mathbf{L}}_N)).$$
The rate of the codeword $A_1 f(\mathbf{L})^N$ is
$$\frac{1}{n}H(f(\mathbf{L}_1)|f(\hat{\mathbf{L}}_1)) = o_n(1)$$
by Fano's inequality since, from (47), $\Pr\{\mathbf{L}_1 \ne \hat{\mathbf{L}}_1\} = o_n(1)$.
- (D.2) *SK generation by a linear operation on CR*: Finally, terminals 1 and 2 generate an SK K, by means of a linear operation on the CR $f(\mathbf{L})^N$, viz., $K = A_2 f(\mathbf{L})^N$, with A_2 having entries in $\mathbb{F}_{|\mathcal{L}|}$, of rate arbitrarily close to
$$C(R) = R - R_p = \frac{1}{2}\log\frac{1}{e^{-2I} + (1 - e^{-2I})e^{-2R}}$$
the optimum tradeoff between SK rate and the quantization rate in Theorem 4.1.

2) Proof of Achievability of $C(R)$: Using the two-step scheme of the previous section, we show that for any $R > 0$ and any $R_s < C(R)$ (cf., Theorem 4.1), there exist n-dimensional nested lattice codes $\Lambda_1 \supset \Lambda_2 \supset \Lambda_3$, mapping f and matrices A_1, A_2, such that the scheme produces a rv

$f(\mathbf{L})^N$ of rate arbitrarily close to R from which a strong SK $K^{(n)} = A_2 f(\mathbf{L})^N$ can be extracted of rate arbitrarily close to R_s.

Without loss of generality, we can write

$$\mathbf{X}_1 = \mathbf{X}_2 + \mathbf{Z} \tag{49}$$

where $\mathbf{Z}$ is independent of $\mathbf{X}_2$ and consists of n i.i.d. repetitions of the rv $Z \sim \mathcal{N}(0, \sigma_Z^2)$ with $\sigma_Z^2 = \sigma_{X_1}^2 - \sigma_{X_2}^2$ so that, from (44), $R_p = R_p(R)$ can also be written as

$$\begin{aligned} R_p &= \frac{1}{2}\log\left((e^{2R}-1)e^{-2I}+1\right) \\ &= \frac{1}{2}\log\left(\frac{(e^{2R}-1)\sigma_Z^2}{\sigma_{X_1}^2}+1\right) \\ &= \frac{1}{2}\log\frac{\alpha^2\sigma_Z^2+D}{D}. \end{aligned} \tag{50}$$

Further, $\mathbf{U}$ is taken to be independent of $(\mathbf{X}_2, \mathbf{Z})$ and, hence, of $(\mathbf{X}_1, \mathbf{X}_2, \mathbf{Z})$. A main step in the proof of achievability of $C(R)$ is the proof of Lemma 4.3.

Proof of Lemma 4.3: We suppress the symbol i. The proof relies on the existence of three "good" n-dimensional nested lattice codes $\Lambda_1 \supset \Lambda_2 \supset \Lambda_3$ with the properties stated in Lemma 4.4; the proof of existence is obtained by suitably generalizing ideas from [13], and is given in Appendix C.

Lemma 4.4: ("Good" Lattice Codes): For each $R > 0$ and $D > 0$, let $R_p = R_p(R)$ and $\alpha = \alpha(R, D)$ as in (45), (43). For every $\epsilon > 0$ and all n sufficiently large, there exist n-dimensional nested lattice codes $\Lambda_1 \supset \Lambda_2 \supset \Lambda_3$ with

$$\frac{1}{n}\log\frac{|\nu(\Lambda_3)|}{|\nu(\Lambda_1)|} \le R+\epsilon, \quad \frac{1}{n}\log\frac{|\nu(\Lambda_2)|}{|\nu(\Lambda_1)|} \le R_p+\epsilon \tag{51}$$

$$Pr\{\alpha\mathbf{Z} - \mathbf{U} \notin \nu(\Lambda_2)\} = o_n(1) \tag{52}$$

$$Pr\{\alpha\mathbf{X}_1 - \mathbf{U} \notin \nu(\Lambda_3)\} = o_n(1) \tag{53}$$

$$\sigma^2(\Lambda_1) = D \tag{54}$$

and

$$r_{\Lambda_1}^{\mathrm{cov}}(n) = O(\sqrt{n}). \tag{55}$$

Upon using such "good" lattice codes, the claimed rates in (46) follow from (51). We next consider (47). By (41), upon using (39), we get

$$\begin{aligned} &(\mathbf{P} - \alpha\mathbf{X}_2 - \mathbf{U}) \bmod \Lambda_2 \\ &\quad = (Q_{\Lambda_1}(\alpha\mathbf{X}_1 + \mathbf{U}) \bmod \Lambda_2 - \alpha\mathbf{X}_2 - \mathbf{U}) \bmod \Lambda_2 \\ &\quad = (Q_{\Lambda_1}(\alpha\mathbf{X}_1 + \mathbf{U}) - \alpha\mathbf{X}_2 - \mathbf{U}) \bmod \Lambda_2 \\ &\quad = (\alpha\mathbf{Z} - \mathbf{E}) \bmod \Lambda_2 \end{aligned}$$

where $\mathbf{E} = (\alpha\mathbf{X}_1 + \mathbf{U}) \bmod \Lambda_1$ is a quantization error with respect to Λ_1. Therefore, from (42)

$$\begin{aligned} \hat{\mathbf{L}} &= [\,[(\mathbf{P} - \alpha\mathbf{X}_2 - \mathbf{U}) \bmod \Lambda_2] + \alpha\mathbf{X}_2 + \mathbf{U}] \bmod \Lambda_3 \\ &= [(\alpha\mathbf{Z} - \mathbf{E}) \bmod \Lambda_2 + \alpha\mathbf{X}_2 + \mathbf{U}] \bmod \Lambda_3. \end{aligned}$$

Defining the event $\mathcal{E} = \{\alpha\mathbf{Z} - \mathbf{E} \notin \nu(\Lambda_2)\}$, we see that in $\mathcal{E}^c$

$$\begin{aligned} \hat{\mathbf{L}} &= (\alpha\mathbf{Z} - \mathbf{E} + \alpha\mathbf{X}_2 + \mathbf{U}) \bmod \Lambda_3 \\ &= (\alpha\mathbf{X}_1 + \mathbf{U} - (\alpha\mathbf{X}_1 + \mathbf{U}) \bmod \Lambda_1) \bmod \Lambda_3 \\ &= Q_{\Lambda_1}(\alpha\mathbf{X}_1 + \mathbf{U}) \bmod \Lambda_3 \\ &= \mathbf{L} \end{aligned}$$

so that $\{\mathbf{L} \neq \hat{\mathbf{L}}\} \subseteq \mathcal{E}$. Now, observe that $\mathbf{E}$ is conditionally independent of $\mathbf{Z}$ conditioned on $\mathbf{X}_2 = \mathbf{x}_2$, $\mathbf{x}_2 \in \mathbb{R}^n$, which, combined with the independence of $\mathbf{X}_2$ and $\mathbf{Z}$, gives that $\mathbf{E}$ is independent of $\mathbf{Z}$. Further, $\mathbf{E}$ is distributed as $\mathbf{U}$ by Lemma 4.2 and $\mathbf{U}$ is independent of $\mathbf{Z}$, so that

$$\begin{aligned} \Pr\{\mathbf{L} \neq \hat{\mathbf{L}}\} &\le \Pr\{\mathcal{E}\} = \Pr\{\alpha\mathbf{Z} - \mathbf{E} \notin \nu(\Lambda_2)\} \\ &= \Pr\{\alpha\mathbf{Z} - \mathbf{U} \notin \nu(\Lambda_2)\} = o_n(1) \end{aligned}$$

by Lemma 4.4, thereby establishing (47).

In order to establish (48), the idea is to show that $\mathbf{L}$ serves as a codeword of an optimum Gaussian rate distortion code for the source $\mathbf{X}_1$, with CR $\mathbf{U}$ at the encoder and decoder. Since $\mathbf{L}$ can be selected to have rate arbitrarily close to R, it will possess the mentioned attribute if there exists a decoder for reconstructing $\mathbf{X}_1$ from $(\mathbf{L}, \mathbf{U})$ with mean-squared error distortion $\cong e^{-2R}\sigma_{X_1}^2$. Then, with $\mathbf{U}$ (independent of $\mathbf{X}_1$) being known to the encoder and decoder, the codeword $\mathbf{L}$—at optimality—must be nearly independent of $\mathbf{U}$ and nearly uniformly distributed, thereby establishing (48). First, we show that upon using the nested lattice codes above with a suitable decoder, we can reconstruct $\mathbf{X}_1$ from $(\mathbf{L}, \mathbf{U})$ with the aforementioned distortion. To this end, consider the decoder, that reconstructs $\mathbf{X}_1$ as

$$\hat{\mathbf{X}}_1 = c((\mathbf{L} - \mathbf{U}) \bmod \Lambda_3)$$

where $c > 0$ is to be chosen later so as to minimize the mean-squared error distortion.

Using (39), we have

$$\begin{aligned} (\mathbf{L} - \mathbf{U}) \bmod \Lambda_3 &= (\,Q_{\Lambda_1}(\alpha\mathbf{X}_1 + \mathbf{U}) \bmod \Lambda_3 - \mathbf{U}) \\ &\qquad \bmod \Lambda_3 \\ &= (\,Q_{\Lambda_1}(\alpha\mathbf{X}_1 + \mathbf{U}) - \mathbf{U}) \bmod \Lambda_3 \\ &= (\alpha\mathbf{X}_1 - \mathbf{E}) \bmod \Lambda_3 \end{aligned}$$

so that $\hat{\mathbf{X}}_1 = c((\alpha\mathbf{X}_1 - \mathbf{E}) \bmod \Lambda_3)$. Observe next that by Lemma 4.2, $\mathbf{E}$ is independent of $\mathbf{X}_1$ and is distributed as $\mathbf{U}$, and hence by (53)

$$\Pr\{(\alpha\mathbf{X}_1 - \mathbf{E}) \bmod \Lambda_3 \neq \alpha\mathbf{X}_1 - \mathbf{E}\} = o_n(1). \tag{56}$$

It readily follows, as shown in Appendix E, that

$$\lim_{n\to\infty}\frac{1}{n}\mathbb{E}[\|\mathbf{X}_1 - \hat{\mathbf{X}}_1\|^2] \le (1-c\alpha)^2\sigma_{X_1}^2 + c^2 D + o_n(1). \tag{57}$$

The significant sum on the right side above is minimized by the choice $c = \frac{\alpha\sigma_{X_1}^2}{\alpha^2\sigma_{X_1}^2 + D} = \frac{\alpha\sigma_{X_1}^2}{De^{2R}}$ by (44), and so

$$\lim_{n\to\infty}\frac{1}{n}\mathbb{E}[\|\mathbf{X}_1 - \hat{\mathbf{X}}_1\|^2] \le \sigma_{X_1}^2 e^{-2R} + o_n(1). \tag{58}$$

Now we are ready to prove (48). With

$$R_{X_1}(D) \stackrel{\triangle}{=} \min_{\mathbb{E}[(\hat{X}_1 - X_1)^2] \le D} I(\hat{X}_1 \wedge X_1) = \frac{1}{2}\log\frac{\sigma_{X_1}^2}{D}, D \ge 0$$

$$\begin{aligned}
\frac{1}{n}H(\mathbf{L}|\mathbf{U}) &= \frac{1}{n}I(\mathbf{L} \wedge \mathbf{X}_1|\mathbf{U}) \\
&= \frac{1}{n}I(\mathbf{L}, \mathbf{U} \wedge \mathbf{X}_1) \\
&\ge \frac{1}{n}I(\hat{\mathbf{X}}_1 \wedge \mathbf{X}_1) \\
&\ge \frac{1}{n}\sum_{t=1}^{n} I(\hat{X}_{1,t} \wedge X_{1,t}) \\
&\ge \frac{1}{n}\sum_{t=1}^{n} R_{X_1}(\mathbb{E}[(\hat{X}_{1,t} - X_{1,t})^2]) \\
&\ge R_{X_1}(\frac{1}{n}\sum_{t=1}^{n}\mathbb{E}[(\hat{X}_{1,t} - X_{1,t})^2]) \qquad (59)
\end{aligned}$$

where the second equality is by the independence of $\mathbf{U}$ and $\mathbf{X}_1$; the first inequality follows from $\hat{\mathbf{X}}_1$ being a function of $\mathbf{L}$ and $\mathbf{U}$; the second inequality is from $\mathbf{X}_1$ having independent components; and the last inequality is by the convexity of $R_{X_1}(\cdot)$. Finally, combining (58) and (59), and noting that $R_{X_1}(\cdot)$ is non-increasing and uniformly continuous, we get

$$\frac{1}{n}H(\mathbf{L}|\mathbf{U}) \ge R - o_n(1)$$

which is (48). ■

Continuing with the proof of achievability of $C(R)$, fix $R > 0$ and $\epsilon > 0$, the latter to be specified later. For every $\eta > 0$ and all n sufficiently large, Lemma 4.3 provides for the existence of n-dimensional lattice codes $\Lambda_1 \supset \Lambda_2 \supset \Lambda_3$ such that

$$\log|\mathcal{L}| < n(R + \eta/2), \ \log|\mathcal{P}| < n(R_p + \eta/2) \qquad (60)$$

$$\Pr\{\hat{\mathbf{L}}_1 \ne \mathbf{L}_1\} < \epsilon \qquad (61)$$

and

$$H(\mathbf{L}_1|\mathbf{U}_1) > n(R - \epsilon) \qquad (62)$$

By Fano's inequality and (60), (61)

$$H(\mathbf{L}_1|\hat{\mathbf{L}}_1) \le \epsilon n(R + \eta/2) + h(\epsilon) \qquad (63)$$

where $h(\cdot)$ is the binary entropy function. With f being a $\mathbb{F}_{|\mathcal{L}|}$-valued mapping in the Digital Part in Section IV-BI, the existence of the matrix A_1 follows from [6, Theorem 1] on the adequacy of linear encoding for the Slepian–Wolf data compression of the i.i.d. rvs $f(\mathbf{L}_i)$, $i = 1, \ldots, N$, with decoder side information $f(\hat{\mathbf{L}}_i)$, $i = 1, \ldots, N$, and decoding error probability vanishing to zero exponentially in N. Specifically, from [6, Theorem 1] and using (63), there exists a $\lceil \frac{N[\epsilon n(R+\eta/2)+h(\epsilon)]}{\log|\mathcal{L}|} \rceil \times N$-matrix A_1 with $\mathbb{F}_{|\mathcal{L}|}$-valued entries such that $f(\mathbf{L})^N$ can be reconstructed from $A_1 f(\mathbf{L})^N$ and $f(\hat{\mathbf{L}})^N$ with the probability of decoding error vanishing exponentially in N.

It remains to show the existence of a matrix A_2 with the asserted property. To this end, we shall use Lemma 4.5 whose proof is provided in Appendix D

Lemma 4.5: Let A be a rv with values in a Galois field $\mathbb{F}_q$ and let U be an $\mathbb{R}^n$-valued rv (with or without a density with respect to the Lebesgue measure). Consider N i.i.d. repetitions of (A, U), namely $(A^N, U^N) = ((A_1, U_1), \ldots, (A_N, U_N))$, and let $B = B^{(N)} \in \mathcal{B} = \mathcal{B}^{(N)}$ be a finite-valued rv with a given joint distribution with (A^N, U^N). Then, for every $\delta > 0$ and every $R < H(A|U) - \frac{1}{N}\log|\mathcal{B}| - 2\delta$, there exists a $\lfloor \frac{NR}{\log q} \rfloor \times N$ matrix L with $\mathbb{F}_q$-valued entries such that $s(LA^N; U^N, B)$ vanishes exponentially in N.

Apply Lemma 4.5 with $A = f(\mathbf{L}_1)$, $U = \mathbf{U}_1$, and $B = (\mathbf{P}^N, A_1 f(\mathbf{L})^N)$ with

$$\frac{1}{n}\log|\mathcal{B}| \le n(R_p + \eta/2) + \epsilon n(R + \eta/2) + h(\epsilon)$$

and consequentially, using (62)

$$\begin{aligned}
H(A|U) - \frac{1}{n}\log|\mathcal{B}| &= H(\mathbf{L}_1|\mathbf{U}_1) \\
&\quad - \begin{bmatrix} n(R_p + \eta/2) \\ +\epsilon n(R + \eta/2) + h(\epsilon) \end{bmatrix} \\
&\ge n(R - R_p - \eta) \\
&= n(C(R) - \eta) \qquad (64)
\end{aligned}$$

if (the yet unspecified) $\epsilon > 0$ is chosen to be sufficiently small. Hence, Lemma 4.5 gives that there exists a matrix A_2 such that for $K^{(nN)} = A_2 f(\mathbf{L})^N$ of range $\mathcal{K}^{(nN)}$

$$\begin{aligned}
\log|\mathcal{K}^{(nN)}| &= \log|\mathcal{L}|^{\frac{\lceil NR_s \rceil}{\lceil \log|\mathcal{L}| \rceil}} \\
&\ge NR_s(1 - o_n(1)) \\
&\ge nN(C(R) - \eta)(1 - o_n(1)) \qquad (65)
\end{aligned}$$

and $s(K^{(nN)}; \mathbf{U}^N, \mathbf{P}^N, A_1 f(\mathbf{L})^N)$ vanishes exponentially in N. Since η was arbitrary, the rate of $f(\mathbf{L})$, and hence $f(\mathbf{L})^N$, can be chosen arbitrary close to R, and the rate of $K^{(nN)}$ can be chosen arbitrarily close to $C(R)$ for all n sufficiently large. This completes the proof of achievability of $C(R)$. ■

V. Discussion

One main contribution of this paper is the converse proof of the SK capacity in Theorem 3.1; in fact, this proof applies even when the signals observed by the m terminals are i.i.d. repetitions of the $\mathbb{R}$-valued (and not necessarily jointly Gaussian) rvs X_i, $i = 1, \ldots, m$, provided that condition (2) is met. Our proof technique, which differs from the entropy decomposition approach in [9] for counterpart finite-valued rvs, can be used for the latter as well upon replacing differential entropy by its discrete counterpart. A characterization of SK capacity in a general setting in which the collection of rvs $\{X_i, \ i = 1, \ldots, m\}$ can have mixed alphabets remains open.

Turning to the two-terminal Gaussian model in Section IV, the choice of quantization at just a single terminal was motivated by the study of SK generation for a discrete model in [10] where it was shown that an optimum-rate SK could be generated as a function of the signal $\mathbf{X}_i$ observed at any particular $i \in A$. Thereupon, we show in Theorem 4.1 that such quantization of rate R at terminal 1 alone enables the attainable of a maximum SK rate $C(R)$ which tends to SK capacity as $R \to \infty$. Other models with quantization can be studied. For instance, quantization can be considered at both the terminals with constraints on the individual rates or the sum rate. In the latter case, under

a sum rate constraint R, clearly the best attainable SK rate is no smaller than $C(R)$. Can it be larger?

Another direction entails an extension of the formulation of Theorem 4.1 to Gaussian models with an arbitrary number $m > 2$ of terminals; the resulting model will involve quantization at one terminal in the secrecy-seeking set A, say terminal k, with randomization allowed at all the terminals. In particular, following the paragraph preceding the statement of Theorem 4.1, the model under consideration can be described as follows. Let M_i be a $\mathcal{M}_i$-valued rv, $i = 1, \ldots, m$, with $M_1, M_2, \ldots, M_m, \mathbf{X}_{\mathcal{M}}$ being mutually independent. For each $R > 0$, let $q_R : \mathcal{M}_k \times \mathbb{R}^n \to \mathcal{Q}_R$ be a random (vector) quantizer at terminal k of rate R, where $\mathcal{Q}_R \subset \mathbb{R}^n$ with $\frac{1}{n}\log|\mathcal{Q}_R| \le R$. Let $C(R)$ be the largest rate of an SK that can be generated from $q_R(M_k, \mathbf{X}_k)$ at terminal k and $(M_i, \mathbf{X}_i)$ at each of the other terminals $i \in \mathcal{M}\backslash\{k\}$. A characterization of the optimum tradeoff $C(R)$, and devising algorithms for SK generation that attain $C(R)$, constitute open problems. Similarly as in Theorem 4.1, these questions are connected to problems in multiterminal Gaussian lossy data compression (cf., e.g., [20]).

Appendix A

1) Proof of Lemma 3.1: We have

$$\begin{aligned}
\Pr\left\{Y_{m+1}^{(q)} \neq \mathbf{1}\right\} &= \Pr\left\{(X_1, \ldots, X_m) \in ([-q,q]^m)^c\right\} \\
&= \int_{([-q,q]^m)^c} \frac{\exp\left(-\frac{1}{2}\mathbf{x}^T Q^{-1}\mathbf{x}\right)}{(2\pi)^{n/2}|Q|^{1/2}} d\mathbf{x} \\
&\le \int_{\{\mathbf{x}:\|\mathbf{x}\|\ge q\}} \frac{\exp\left(-\frac{1}{2}\mathbf{x}^T Q^{-1}\mathbf{x}\right)}{(2\pi)^{n/2}|Q|^{1/2}} d\mathbf{x} \\
&\le \int_{\{\mathbf{x}:\|\mathbf{x}\|\ge q\}} \frac{\exp\left(-\frac{1}{2}\frac{\|\mathbf{x}\|^2}{\lambda_{\max}}\right)}{(2\pi)^{n/2}|Q|^{1/2}} d\mathbf{x} \qquad (66) \\
&= \frac{mC_m}{(2\pi)^{n/2}|Q|^{1/2}} \int_q^\infty r^{m-1} \exp\left(-\frac{r^2}{2}\right) dr \\
&= O\left(q^{(m-2)} \exp\left(-\frac{q^2}{2\lambda_{\max}}\right)\right) \qquad (67)
\end{aligned}$$

which $\to 0$ as $q \to \infty$, where $\lambda_{\max} > 0$ in (66) is the largest eigenvalue of Q and C_m in (67) is a constant that depends only on m. This establishes (19).

Next, for each $B \subseteq \mathcal{M}$, observe that

$$\epsilon_q \stackrel{\triangle}{=} \Pr\left\{(\mathbf{1}(Y_i \neq 0))_{i\in B} \neq \mathbf{1}\right\} \le \Pr\left\{Y_{m+1}^{(q)} \neq \mathbf{1}\right\} = o_q(1). \qquad (68)$$

Further, for any collection of $|B|$ integers k_B, $k_i \in \{1, 2, \ldots, 2q^2\}$, $i \in B$, let $P_{k_B} = \Pr\{Y_B = k_B\}$. It now follows by the uniform continuity of the density function f_{X_B} of X_B and the mean-value theorem that for any k_B, there exists $x_B(k_B)$ satisfying $Y_i = f_q(x_i(k_B)) = k_i$, $i \in B$, so that $P_{k_B} = f_{X_B}(x_B(k_B))q^{-|B|}$. Consequently

$$\begin{aligned}
&H\left(Y_B \middle| (\mathbf{1}(Y_i \neq 0))_{i\in B} = \mathbf{1}\right) \\
&= -\sum_{k_B \in \{1\ldots,2q^2\}^{|B|}} \left(\frac{P_{k_B}}{1-\epsilon_q}\right) \log\left(\frac{P_{k_B}}{1-\epsilon_q}\right) \\
&= -\sum_{k_B \in \{1\ldots,2q^2\}^{|B|}} \left[\begin{matrix}\left(\frac{f_{X_B}(x_B(k_B))q^{-|B|}}{1-\epsilon_q}\right)\times \\ \log\left(f_{X_B}(x_B(k_B))q^{-|B|}\right)\end{matrix}\right] \\
&\quad - \log(1-\epsilon_q) \\
&= -\frac{1}{1-\epsilon_q}\left[\sum_{k_B \in \{1\ldots,2q^2\}^{|B|}} \left[\begin{matrix}\left(f_{X_B}(x_B(k_B))q^{-|B|}\right)\times \\ \log\left(f_{X_B}(x_B(k_B))\right)\end{matrix}\right]\right] \\
&\quad + \log(1-\epsilon_q) + |B|\log q.
\end{aligned}$$

Hence

$$\begin{aligned}
&H\left(Y_B \middle| (\mathbf{1}(Y_i \neq 0))_{i\in B} = \mathbf{1}\right) - |B|\log q \\
&= -\frac{1}{1-\epsilon_q}\left[\sum_{k_B \in \{1\ldots,2q^2\}^{|B|}} \left[\begin{matrix}\left(f_{X_B}(x_B(k_B))q^{-|B|}\right)\times \\ \log\left(f_{X_B}(x_B(k_B))\right)\end{matrix}\right]\right].
\end{aligned}$$

Taking limits as $q \to \infty$, we obtain (18); this concludes the proof of Lemma 3.1.

Appendix B

1) Proof of Lemma 4.1: Part (II): Note that $\mathbf{X}_1 = (X_{1,1}, \ldots, X_{1,n}) = X_1^n$ and $\mathbf{X}_2 = (X_{2,1}, \ldots, X_{2,n}) = X_2^n$, where $(X_{1,i}, X_{2,i})$, $i = 1, \ldots, n$, are i.i.d. repetitions of the jointly Gaussian rvs (X_1, X_2) with both means being zero and with correlation coefficient ρ

$$\begin{aligned}
\frac{1}{n}I(q(\mathbf{X}_1) \wedge \mathbf{X}_2) &= \frac{1}{n}I(q(X_1^n) \wedge X_2^n) \\
&= \frac{1}{n}h(X_2^n) - \frac{1}{n}h(X_2^n|q(X_1^n)) \\
&= \frac{1}{n}\sum_{i=1}^n h(X_{2,i}) \\
&\quad - \frac{1}{n}\sum_{i=1}^n h(X_{2,i}|q(X_1^n), X_{2,1}^{i-1}) \\
&\le \frac{1}{n}\sum_{i=1}^n h(X_{2,i}) \\
&\quad - \frac{1}{n}\sum_{i=1}^n h(X_{2,i}|q(X_1^n), X_{1,1}^{i-1}, X_{2,1}^{i-1}) \\
&= \frac{1}{n}\sum_{i=1}^n I(q(X_1^n), X_{1,1}^{i-1}, X_{2,1}^{i-1} \wedge X_{2,i})
\end{aligned} \qquad (69)$$

where $X_{1,l}^k \stackrel{\triangle}{=} (X_{1,l}, \ldots, X_{1,k})$, $1 \le l < k \le n$.

Next

$$\begin{aligned}\frac{1}{n}\log|\mathcal{Q}| &\geq \frac{1}{n}I(q(X_1^n)\wedge X_1^n)\\ &= \frac{1}{n}h(X_1^n)-\frac{1}{n}h(X_1^n|q(X_1^n))\\ &= \frac{1}{n}\sum_{i=1}^{n}h(X_{1,i})-\frac{1}{n}\sum_{i=1}^{n}h(X_{1,i}|q(X_1^n),X_{1,1}^{i-1})\\ &= \frac{1}{n}\sum_{i=1}^{n}h(X_{1,i})\\ &\quad-\frac{1}{n}\sum_{i=1}^{n}h(X_{1,i}|q(X_1^n),X_{1,1}^{i-1},X_{2,1}^{i-1})\\ &= \frac{1}{n}\sum_{i=1}^{n}I(q(X_1^n),X_{1,1}^{i-1},X_{2,1}^{i-1}\wedge X_{1,i}) \qquad (70)\end{aligned}$$

where the last equality is from

$$\begin{aligned}&I(X_{1,i}\wedge X_{2,1}^{i-1}|q(X_1^n),X_{1,1}^{i-1})\\ &\quad\leq I(X_{1,i},q(X_1^n)\wedge X_{2,1}^{i-1}|X_{1,1}^{i-1})\\ &\quad\leq I(X_{1,i},X_{1,i+1}^{n}\wedge X_{2,1}^{i-1}|X_{1,1}^{i-1})\\ &\quad\leq I(X_{1,i},X_{1,i+1}^{n}\wedge X_{1,1}^{i-1},X_{2,1}^{i-1})=0\end{aligned}$$

by the assumption that $(X_{1,i},X_{2,i})$, $i=1,\ldots,n$, are i.i.d.

Let $U_i=(q(X_1^n),X_{1,1}^{i-1},X_{2,1}^{i-1})$. Then

$$\begin{aligned}I(U_i\wedge X_{2,i}|X_{1,i}) &= I(q(X_1^n),X_{1,1}^{i-1},X_{2,1}^{i-1}\wedge X_{2,i}|X_{1,i})\\ &\leq I(X_{1,1}^{i-1},X_{1,i}^{n},X_{2,1}^{i-1}\wedge X_{2,i}|X_{1,i})\\ &\leq I(X_{1,1}^{i-1},X_{1,i}^{n},X_{2,1}^{i-1}\wedge X_{1,i},X_{2,1}^{i-1})\\ &= 0 \qquad (71)\end{aligned}$$

by the assumption that $(X_{1,i},X_{2,i})$, $i=1,\ldots,n$, are i.i.d., so that U_i —o— $X_{1,i}$ —o— $X_{2,i}$. Consequently, from (69) and (30), we get

$$\frac{1}{n}I(q(\mathbf{X}_1)\wedge\mathbf{X}_2)\leq\frac{1}{n}\sum_{i=1}^{n}C(I(U_i\wedge X_{1,i})) \qquad (72)$$

and, from (70), we get

$$\frac{1}{n}\sum_{i=1}^{n}I(U_i\wedge X_{1,i})\leq\frac{1}{n}\log|\mathcal{Q}|. \qquad (73)$$

Continuing from (72), we have

$$\begin{aligned}\frac{1}{n}I(q(\mathbf{X}_1)\wedge\mathbf{X}_2) &\leq \frac{1}{n}\sum_{i=1}^{n}C(I(U_i\wedge X_{1,i}))\\ &\leq C\left(\frac{1}{n}\sum_{i=1}^{n}I(U_i\wedge X_{1,i})\right)\\ &\leq C\left(\frac{1}{n}\log|\mathcal{Q}|\right)\end{aligned}$$

where the second inequality is by the concavity of $C(\cdot)$ and the last inequality is from (73) and the fact that $C(\cdot)$ is increasing.

APPENDIX C

1) PROOF OF LEMMA *4.4:* We shall need the following concepts from [25].

Definition C.1: The *effective radius* of an n-dimensional lattice code Λ, denoted by $r_\Lambda^{\text{eff}}(n)$, is the radius of an n-dimensional sphere with the same volume as the Voronoi region of the lattice code.

Definition C.2: A sequence of lattice codes is *good for covering* if the ratio of its covering radius to effective radius approaches 1 as the dimension of the lattice codes tends to ∞.

Definition C.3: Let $Z\sim\mathcal{N}\left(0,\sigma_Z^2\right)$ and let $\mathbf{Z}$ be n i.i.d. repetitions of Z. For each $\delta>h(Z)=\frac{1}{2}\log(2\pi e\sigma_Z^2)$, a sequence of lattice codes Λ is said to be *exponentially good for AWGN channel coding* (without power constraint) for noise Z and with parameter δ if there exists a mapping $E(\cdot)$ such that $E(u)>0$ for every $u>0$

$$\lim_{n\to\infty}\frac{1}{n}\log|\nu(\Lambda)|=\delta$$

and

$$\Pr\{\mathbf{Z}\notin\nu(\Lambda)\}<e^{-n(E(\delta-h(Z))-o_n(1))}$$

The exponent of the error probability $\Pr\{\mathbf{Z}\notin\nu(\Lambda)\}$ can be expressed in terms of the ratio, $\rho>1$, of the effective radius of the lattice code to the (approximated) radius of the Gaussian noise vector $\sqrt{n}\sigma_Z$. In [19], the existence is shown of a sequence of lattice codes $\Lambda=\Lambda^{(n)}$ with the property that

$$\lim_{n\to\infty}\frac{r_\Lambda^{\text{eff}}(n)}{\sqrt{n}\sigma_Z^2}=\rho$$

and

$$\Pr\{\mathbf{Z}\notin\nu(\Lambda)\}\leq e^{-n(E_P(\rho)-o_n(1))}$$

where $E_P(\rho)$ is the *Poltyrev* exponent given by

$$E_P(\rho)=\begin{cases}\frac{1}{2}[(\rho^2-1)-\ln\rho], & 1\leq\rho^2\leq 2\\ \frac{1}{2}\ln\frac{e\rho^2}{4}, & 2\leq\rho^2\leq 4\\ \frac{\rho^2}{8}, & \rho^2\geq 4.\end{cases}$$

Observe that the properties of being good for covering, and being exponentially good for AWGN channel coding and achieving the Poltyrev exponent, are invariant under scaling. To prove the existence of nested lattice codes with the required properties, we shall use the results of [13] where a random lattice ensemble is constructed from a random linear code $\mathcal{C}$ by the following procedure described in Definition C.4. (The construction is known as Construction A in the theory of lattices, see, e.g., [5].) The random lattice ensemble is denoted by $\mathbb{Z}^n+\frac{1}{p(n)}\mathcal{C}$, where $p(n)$ is a sequence of primes and $\mathcal{C}$ is the ensemble of uniform random linear code over $\mathbb{Z}_{p(n)}$.

Definition C.4:

1) Let $\mathcal{C}$ denote the uniform random $(n,k(n))$ linear code ensemble over $\mathbb{Z}_{p(n)}$. Specifically, the random generating matrix G of the code in the ensemble is obtained by drawing each element of G independently and uniformly from $\mathbb{Z}_{p(n)}$ and letting $\mathcal{C}\stackrel{\triangle}{=}\{\mathbf{x}=\mathbf{i}G,\,\mathbf{i}\in\mathbb{Z}_{p(n)}^{k(n)}\}$, where all the operations are over $\mathbb{Z}_{p(n)}$ (i.e., modulo-p).

2) Transform each codeword of $\mathcal{C}$ into a point in $[0,1]^n \subset \mathbb{R}^n$ by dividing all the coordinates by $p(n)$. Denote such a random constellation by $\frac{1}{p(n)}\mathcal{C} \subset [0,1]^n$.
3) Replicate $\frac{1}{p(n)}\mathcal{C}$ over all of $\mathbb{R}^n$ by performing $\mathbb{Z}^n + \frac{1}{p(n)}\mathcal{C}$. It is easy to check that $\mathbb{Z}^n + \frac{1}{p(n)}\mathcal{C}$ is indeed a lattice.

Note that if G is nonsingular, then the volume of the Voronoi region is $p(n)^{-k(n)}$. The probability of G being singular can be easily shown to be at most $p(n)^{-n}(p^k(n)-1)$ (see [13, eq. (24)]). Following [13], we shall consider only lattice ensembles such that $k(n) \leq \beta n$ for some $0 < \beta < 1$, so that this mentioned probability goes to zero in n at least exponentially (p may also grow with n). Consequently, there is a relation among the parameters $p(n)$, $k(n)$, and $r_\Lambda^{\text{eff}}(n)$ for typical lattice codes in the ensemble which can be stated as

$$p(n)^{k(n)} = \frac{1}{V_{\mathcal{B}}(r_\Lambda^{\text{eff}}(n))} = \frac{\Gamma(\frac{n}{2}+1)}{\pi^{n/2}(r_\Lambda^{\text{eff}}(n))^n} \approx \sqrt{n\pi}\left(\frac{n}{2\pi(r_\Lambda^{\text{eff}}(n))^2}\right)^{\frac{n}{2}} \tag{74}$$

where $V_{\mathcal{B}}(r_\Lambda^{\text{eff}}(n))$ denotes the volume of the ball of radius $r_\Lambda^{\text{eff}}(n)$ in $\mathbb{R}^n$.

As in [13], we shall hold $r_\Lambda^{\text{eff}}(n)$ approximately constant as $n \to \infty$. (Since $p(n)$ is prime and $k(n)$ is an integer, $r_\Lambda^{\text{eff}}(n)$ cannot be a constant.) For a suitably chosen $k(n)$, it suffices to pick $p(n)$ such that $r_\Lambda^{\text{eff}}(n)$ as defined in (74) satisfies, for all sufficiently large n

$$r_{\min} < r_\Lambda^{\text{eff}}(n) < 2r_{\min} \tag{75}$$

for a constant $r_{\min}$. By the fact that $k(n) \leq \beta n$ for some $\beta < 1$, it transpires that for a fixed $r_{\min}$ and for all n sufficiently large there exist a prime $p(n)$ and $r_\Lambda^{\text{eff}}(n)$ satisfying both (74) and (75). The results in [13], restated later as Lemmas C.1 and C.2, give constraints on the ranges of $r_{\min}$ and $k(n)$ of the random lattice ensemble $\mathbb{Z}^n + \frac{1}{p(n)}\mathcal{C}$, with $p(n)$ appropriately picked as earlier, such that with probability approaching 1, a lattice code in the ensemble has full dimension and is good for covering or is exponentially good for AWGN channel coding, respectively. These constraints are summarized next.

Lemma C.1: (Goodness for covering) [13, Theorem 2]: For any fixed $r_{\min}$ such that $0 < r_{\min} < \frac{1}{4}$ and any $k(n)$ such that $\log^2 n < k(n) \leq \beta n$, for some $\beta < 1$, let $p(n)$ and $r_\Lambda^{\text{eff}}(n)$ be such that both (74) and (75) are satisfied (for all n sufficiently large). Then, for such parameters $(n, p(n), k(n))$, with probability approaching 1, the random lattice code in the lattice ensemble $\mathbb{Z}^n + \frac{1}{p(n)}\mathcal{C}$ is good for covering and $\mathcal{C}$ has dimension exactly $k(n)$.

Lemma C.2 (Exponential goodness for AWGN channel coding achieving the Poltyrev exponent evaluated at ρ) [13, Th. 4]: For any fixed $r_{\min}$ such that $0 < r_{\min} < \min(\frac{\rho^2}{32E_P(\rho)}, \frac{1}{4})$ and any $k(n)$ such that $k(n) \leq \beta n$ for some $\beta < \frac{1}{2}$, let $p(n)$ and $r_\Lambda^{\text{eff}}(n)$ be such that both (74) and (75) are satisfied for all n sufficiently large. Then, for such parameters $(n, p(n), k(n))$, with probability approaching 1, the random lattice code in the lattice ensemble $\mathbb{Z}^n + \frac{1}{p(n)}\mathcal{C}$ is exponentially good for AWGN channel coding and for achieving the Poltyrev exponent evaluated at ρ, and $\mathcal{C}$ has dimension exactly $k(n)$.

Our next lemma is a consequence of Lemmas C.1 and C.2.

Lemma C.3: For any D, R_2, R_3, $\rho_2 > 1$, and $\rho_3 > 1$, there exists a sequence of three-level nested lattice codes $\Lambda_1 \supset \Lambda_2 \supset \Lambda_3$ such that $\left(\frac{|\nu(\Lambda_3)|}{|\nu(\Lambda_2)|}\right)^{\frac{1}{n}} = e^{R_3 + o_n(1)}$ and $\left(\frac{|\nu(\Lambda_2)|}{|\nu(\Lambda_1)|}\right)^{\frac{1}{n}} = e^{R_2 + o_n(1)}$. Furthermore, Λ_1 is good for covering with second moment per dimension D and Λ_2 (resp. Λ_3) is exponentially good for AWGN channel coding and achieving the Poltyrev exponents evaluated at ρ_2 (resp. ρ_3), respectively.

Proof of Lemma C.3: We shall consider the nested ensembles of lattice codes $\Lambda_1 = \mathbb{Z}^n + \frac{1}{p(n)}\mathcal{C}_1 \supset \Lambda_2 = \mathbb{Z}^n + \frac{1}{p(n)}\mathcal{C}_2 \supset \Lambda_3 = \mathbb{Z}^n + \frac{1}{p(n)}\mathcal{C}_3$, where $\mathcal{C}_1 \supset \mathcal{C}_2 \supset \mathcal{C}_3$ denote the nested uniform random $(n, k_1(n))$, $(n, k_2(n))$, and $(n, k_3(n))$ linear codes over $\mathbb{Z}_{p(n)}$, respectively. In particular, we first draw a uniform random $k_1(n) \times n$ matrix (with entries taking values uniformly and independently in $\mathbb{Z}_{p(n)}$) to be the random generating matrix of $\mathcal{C}_1$. Then, the first $k_2(n)$, $k_3(n)$ rows of the random matrix constitute the random generating matrices of $\mathcal{C}_2$, $\mathcal{C}_3$, respectively. It is then left to pick $(p(n), k_1(n), k_2(n), k_3(n))$ appropriately to obtain the required nested lattice codes.

To this end, we first select $r_{\min} = \min(\frac{\rho_2{}^2}{32E_P(\rho_2)}, \frac{\rho_3{}^2}{32E_P(\rho_3)}, \frac{1}{4})$. Next, we select $r_{\min 3}$ small enough and $r_{\min 1} < r_{\min 2} < r_{\min 3} < r_{\min}$ so that $\frac{r_{\min 2}}{r_{\min 1}} = e^{R_2}$ and $\frac{r_{\min 3}}{r_{\min 2}} = e^{R_3}$. We then select $k_1(n)$ as growing linearly in n, say $\frac{1}{4}n$. Then, $k_2(n)$ and $k_3(n)$ are constrained by the ratios of the volumes of the Voronoi regions of the three lattice codes, namely $k_2(n) = k_1(n) - \lfloor \frac{nR_2}{\log p(n)} \rfloor$ and $k_3(n) = k_2(n) - \lfloor \frac{nR_3}{\log p(n)} \rfloor$. Finally, we shall select a prime number $p(n)$ so that $r_{\min 1} < r_{\Lambda_1}^{\text{eff}}(n) < 2r_{\min 1}$. Observe that this selection is possible for every large enough n. To see this, let $p^* \in \mathbb{R}$ satisfy (74) for a radius $2r_{\min 1}$, i.e., $p^{*k_1(n)} = \frac{1}{V_{\mathcal{B}}(2r_{\min 1})}$. From (74) and by $r_{\min 1} < r_{\Lambda_1}^{\text{eff}}(n) < 2r_{\min 1}$, our claim is true if we can find a prime $p(n) \in [p^*, 2^{\frac{n}{k_1(n)}}p^*]$. Since $k_1(n) = \frac{1}{4}n$, it follows that there exists such a prime for every large enough n, because there is a prime number between i and $2i$ for every integer i (Bertrand's postulate, see, for instance, [14]). By (74), the choice of $k_1(n)$ above and the fact that $r_{\min 1} < r_{\Lambda_1}^{\text{eff}}(n) < 2r_{\min 1}$, it is clear that $p(n)$ grows subexponentially in n. It then follows, for all n sufficiently large, by the manner of selection of $k_2(n)$, $k_3(n)$, $r_{\min 2}$, and $r_{\min 3}$ that $r_{\min 2} < r_{\Lambda_2}^{\text{eff}}(n) < 2r_{\min 2}$ and $r_{\min 3} < r_{\Lambda_3}^{\text{eff}}(n) < 2r_{\min 3}$. It is clear that $(r_{\min 1}, k_1(n))$ satisfies the constraints in Lemma C.1 for Λ_1 to be good for covering, and $(r_{\min 2}, k_2(n))$, $(r_{\min 3}, k_3(n))$ satisfy the constraints in Lemma C.2 for Λ_2, Λ_3 to be exponentially good for AWGN channel coding and achieving the Poltyrev exponent evaluated at ρ_2, ρ_3, respectively. Specifically, by Lemmas C.1 and C.2, we have that the events

$$A = \{\Lambda_1 \text{ is good for covering and } dim(\mathcal{C}_1) = k_1(n)\}$$
$$B = \left\{ \begin{array}{l} \Lambda_2 \text{ is good for AWGN channel coding and} \\ \text{achieving } E_P(\rho_2) \text{ and } dim(\mathcal{C}_2) = k_2(n) \end{array} \right\}$$

and

$$C = \left\{ \begin{array}{l} \Lambda_3 \text{ is good for AWGN channel coding and} \\ \text{achieving } E_P(\rho_3) \text{ and } dim(\mathcal{C}_3) = k_3(n) \end{array} \right\}$$

satisfy $\Pr\{A\} = 1-o_n(1), \Pr\{B\} = 1-o_n(1)$, and $\Pr\{C\} = 1 - o_n(1)$, respectively. Consequently

$$\Pr\{A \cap B \cap C\} = 1 - \Pr\{A^c \cup B^c \cup C^c\} > 1 - o_n(1).$$

Therefore, there exists a sequence of three-level nested lattice codes $\Lambda_1 \supset \Lambda_2 \supset \Lambda_3$ such that Λ_1 is good for covering, and Λ_2, Λ_3 are exponentially good for AWGN channel coding and achieving the Poltyrev exponents evaluated at ρ_2, ρ_3, respectively. The claims regarding the ratio of volume of the Voronoi region of Λ_3 to that of Λ_2 and the ratio of volume of the Voronoi region of Λ_2 to that of Λ_1 follow from $k_2(n) - k_3(n) = \lfloor \frac{nR_3}{\log p(n)} \rfloor$, $k_1(n) - k_2(n) = \lfloor \frac{nR_2}{\log p(n)} \rfloor$ and the fact that $p(n)$ grows subexponentially, respectively. Finally, we shall scale all lattice codes so that the second moment per dimension of Λ_1 is D. ■

Now, returning to Lemma 4.4, we have the following next step.

Lemma C.4: For $R > 0$ and an arbitrary but fixed $D > 0$, let α be as in (43). Then, for any $P > \alpha^2\sigma_Z^2 + D$ and any $Q > \alpha^2\sigma_{X_1}^2 + D$, there exists a sequence of nested lattice codes $\Lambda_1 \supset \Lambda_2 \supset \Lambda_3$ such that $\sigma^2(\Lambda_1) = D$, Λ_1 is good for covering

$$\lim_{n\to\infty} \frac{1}{n} \log \frac{|\nu(\Lambda_3)|}{|\nu(\Lambda_1)|} = \frac{1}{2} \log Q/D \tag{76}$$

$$\lim_{n\to\infty} \frac{1}{n} \log \frac{|\nu(\Lambda_2)|}{|\nu(\Lambda_1)|} = \frac{1}{2} \log P/D \tag{77}$$

$$Pr\{\alpha\mathbf{Z} - \mathbf{U} \notin \nu(\Lambda_2)\} \to 0 \textit{ exponentially in } n \tag{78}$$

and

$$Pr\{\alpha\mathbf{X}_1 - \mathbf{U} \notin \nu(\Lambda_3)\} \to 0 \textit{ exponentially in } n. \tag{79}$$

Proof of Lemma C.4: Let $r > 1$ be sufficiently close to 1 such that $\frac{P}{r^2} > \alpha^2\sigma_Z^2 + D$ and $\frac{Q}{r^2} > \alpha^2\sigma_{X_1}^2 + D$. By Lemma C.3, there exists a sequence of nested lattice codes $\Lambda_1 \supset \Lambda_2 \supset \Lambda_3$ such that

$$\frac{|\nu(\Lambda_2)|}{|\nu(\Lambda_1)|} = e^{\frac{n}{2}(\log \frac{P}{D} + o_n(1))};\ \frac{|\nu(\Lambda_3)|}{|\nu(\Lambda_2)|} = e^{\frac{n}{2}(\log \frac{Q}{P} + o_n(1))} \tag{80}$$

Λ_1 is good for covering with second moment per dimension D, and Λ_2, Λ_3 are exponentially good for AWGN channel coding and achieving the Poltyrev exponent evaluated at ρ_2, ρ_3, respectively, where

$$\rho_2 = \sqrt{\frac{P}{r^2(\alpha^2\sigma_Z^2 + D)}}, \quad \rho_3 = \sqrt{\frac{Q}{r^2(\alpha^2\sigma_{X_1}^2 + D)}}. \tag{81}$$

It is then left to prove (78) and (79) for the sequence of nested lattice codes $\Lambda_1 \supset \Lambda_2 \supset \Lambda_3$.

First, we claim that

$$\frac{2}{n} \log |\nu(\Lambda_1)| = \log (2\pi e)D + o_n(1). \tag{82}$$

The normalized second moment of $\nu(\Lambda_1)$, denoted by $G(\nu(\Lambda_1))$, is defined as (see, e.g., [5])

$$G(\nu(\Lambda_1)) \triangleq \frac{\sigma^2(\Lambda_1)}{|\nu(\Lambda_1)|^{2/n}} \tag{83}$$

It is known that the normalized second moment is invariant under scaling and that the normalized second moment of a sphere, denoted by G_n^*, converges to $\frac{1}{2\pi e}$ as $n \to \infty$ (see, e.g., [5]). By the fact that Λ_1 is good for covering, we have that (see [13, Proposition 1])

$$G(\nu(\Lambda_1)) \to \frac{1}{2\pi e}. \tag{84}$$

Then, (82) follows from $\sigma^2(\Lambda_1) = D$, (83), and (84).

The following lemma, from [12, Lemmas 6 and 11], gives upper bounds for the two probabilities in (78) and (79) in terms of those for i.i.d. Gaussian rvs with asymptotically equal variances per source symbol.

Lemma C.5 [12]: If Λ_1 is good for covering and $\sigma^2(\Lambda_1) = D$, then there exist $\epsilon_1^{(n)}$ and $\epsilon_2^{(n)}$ depending only on Λ_1 and tending to 0 and 1 in n, respectively, such that

$$Pr\{\alpha\mathbf{Z} - \mathbf{U} \notin \nu(\Lambda_2)\} \le \Pr\{\hat{\mathbf{Z}} \notin \nu(\Lambda_2)\} e^{n\epsilon_1^{(n)}}$$

and

$$Pr\{\alpha\mathbf{X}_1 - \mathbf{U} \notin \nu(\Lambda_3)\} \le \Pr\{\hat{\mathbf{X}}_1 \notin \nu(\Lambda_3)\} e^{n\epsilon_1^{(n)}}$$

where $\hat{\mathbf{Z}}$ and $\hat{\mathbf{X}}_1$ are n i.i.d. repetitions of $\mathcal{N}\left(0, \epsilon_2^{(n)}(\alpha^2\sigma_Z^2 + D)\right)$ and $\mathcal{N}\left(0, \epsilon_2^{(n)}(\alpha^2\sigma_{X_1}^2 + D)\right)$ rvs, respectively. Specifically

$$\frac{n}{n+2} \le \epsilon_1^{(n)} < \left(\frac{r_{\Lambda_1}^{\mathrm{cov}}(n)}{r_{\Lambda_1}^{\mathrm{eff}}(n)}\right)^2$$

and

$$\epsilon_2^{(n)} = \log \left(\frac{r_{\Lambda_1}^{\mathrm{cov}}(n)}{r_{\Lambda_1}^{\mathrm{eff}}(n)}\right) + \frac{1}{2} \log 2\pi e G_n^* + \frac{1}{n}.$$

Resuming the proof of Lemma C.4, let $\tilde{\rho}_2$ denote the the ratio of the effective radius of Λ_2 to the approximated radius of the Gaussian rv $\left(\sqrt{n\epsilon_2^{(n)}(\alpha^2\sigma_Z^2 + D)}\right)\hat{\mathbf{Z}}$, i.e.

$$\begin{aligned}\tilde{\rho}_2 &= \frac{|\nu(\Lambda_2)|^{\frac{1}{n}}}{V_{\mathcal{B}}(1)^{\frac{1}{n}}\sqrt{n\epsilon_2^{(n)}(\alpha^2\sigma_Z^2 + D)}} \\ &= \frac{|\nu(\Lambda_2)|^{\frac{1}{n}} t_n}{\sqrt{(2\pi e)\epsilon_2^{(n)}(\alpha^2\sigma_Z^2 + D)}}\end{aligned} \tag{85}$$

and let $\tilde{\rho}_3$ denote the ratio of the radius of Λ_3 to the approximated radius of the Gaussian rv $\left(\sqrt{n\epsilon_2^{(n)}(\alpha^2\sigma_{X_1}^2 + D)}\right)\hat{\mathbf{X}}_1$, i.e.

$$\tilde{\rho}_3 = \frac{|\nu(\Lambda_3)|^{\frac{1}{n}} t_n}{\sqrt{(2\pi e)\epsilon_2^{(n)}(\alpha^2\sigma_{X_1}^2 + D)}} \tag{86}$$

where $V_{\mathcal{B}}(1)$ is the volume of the ball in $\mathbb{R}^n$ of radius 1, and hence, from (74), $t_n = \sqrt{\frac{2\pi e}{n}}\left(\frac{\Gamma(n/2+1)}{\pi^{n/2}}\right)^{1/n} \to 1$ (see, e.g., [5]).

Using (82), it follows from (80) that $|\nu(\Lambda_2)| = e^{\frac{n}{2}(\log(2\pi e)P + o_n(1))}$ and $|\nu(\Lambda_3)| = e^{\frac{n}{2}(\log(2\pi e)Q + o_n(1))}$.

Consequently, for all n sufficiently large, we get from (81) and (85) that

$$\tilde{\rho}_2 > \rho_2 = \sqrt{\frac{P}{r^2(\alpha^2\sigma_Z^2 + D)}} > 1 \tag{87}$$

and, from (81) and (86) that

$$\tilde{\rho}_3 > \rho_3 = \sqrt{\frac{Q}{r^2(\alpha^2\sigma_{X_1}^2 + D)}} > 1. \tag{88}$$

Let $\hat{\hat{\mathbf{Z}}}$ and $\hat{\hat{\mathbf{X}}}_1$ be n i.i.d. repetitions of $\mathcal{N}\left(0, r^2(\alpha^2\sigma_Z^2 + D)\right)$ and $\mathcal{N}\left(0, r^2(\alpha^2\sigma_{X_1}^2 + D)\right)$ rvs, respectively. From Lemma C.5, (87), (88), and the fact that Λ_2, Λ_3 are exponentially good for AWGN channel coding and achieving the Poltyrev exponent evaluated at ρ_2, ρ_3, respectively, for all n sufficiently large

$$\begin{aligned}\Pr\{\alpha\mathbf{Z} - \mathbf{U} \notin \nu(\Lambda_2)\} &\le \Pr\{\hat{\hat{\mathbf{Z}}} \notin \nu(\Lambda_2)\} \\ &\le e^{-n(E_P(\rho_2) - o_n(1))} \\ \Pr\{\alpha\mathbf{X}_1 - \mathbf{U} \notin \nu(\Lambda_3)\} &\le \Pr\{\hat{\hat{\mathbf{X}}}_1 \notin \nu(\Lambda_3)\} \\ &\le e^{-n(E_P(\rho_3) - o_n(1))}\end{aligned}$$

thereby establishing (78) and (79). ■

All assertions in Lemma 4.4 except for (55) follow from Lemma C.4 by noting from (44) and (50) that

$$R = \frac{1}{2}\log\frac{\alpha^2\sigma_{X_1}^2 + D}{D}, \quad R_p = \frac{1}{2}\log\frac{\alpha^2\sigma_Z^2 + D}{D}.$$

To see (55), note that we have shown that $\log\frac{|\nu(\Lambda_1)|^{\frac{2}{n}}}{(2\pi e)D} \to 0$. Consequently

$$r_{\Lambda_1}^{\text{eff}}(n) = O(\frac{\sqrt{(2\pi e)D}}{V_{\mathcal{B}}(1)^{\frac{1}{n}}}) = O(\sqrt{nD}).$$

By the fact that Λ_1 is good for covering, i.e.

$$\frac{r_{\Lambda_1}^{\text{cov}}(n)}{r_{\Lambda_1}^{\text{eff}}(n)} \to 1$$

we get

$$r_{\Lambda_1}^{\text{cov}}(n) = O(\sqrt{nD}).$$

Appendix D

1) Proof of Lemma 4.5: Consider a random $\lfloor\frac{NR}{\log q}\rfloor \times N$ matrix $\mathbf{L}$ with entries taking values mutually independently and uniformly in $\mathbb{F}_q$, i.e., $\mathbf{L}$ is uniformly distributed on the set of all $M \times N = \lfloor\frac{NR}{\log q}\rfloor \times N$ matrices with $\mathbb{F}_q$-valued entries. Further, assume that $\mathbf{L}$ is independent of (A^N, U^N, B), and hence, the average of $H(LA^N|U^N, B)$ over the set of all $M \times N$ matrices L can be written as $H(\mathbf{L}A^N|\mathbf{L}, U^N, B)$.

The proof of Lemma 4.5 involves a series of steps that result in successive lower bounds for $H(\mathbf{L}A^N \,|\, \mathbf{L}, U^N, B)$, yielding eventually that under the assumptions of the lemma

$$H(\mathbf{L}A^N \,|\, \mathbf{L}, U^N, B) \ge M\log q - \epsilon_N \tag{89}$$

for an exponentially vanishing ϵ_N, whereupon the assertion of the lemma follows. These steps in the proof will follow, in a similar manner, the recipe in the proof of [18, Lemma 7] which established an analogous version of Lemma 4.5 but with an extra assumption that U is also a finite-valued rv.

Note that the set of all $M \times N$ matrices with $\mathbb{F}_q$-valued entries correspond, in a one-to-one manner, to the set of all linear functions $\mathcal{G} = \{g : \mathbb{F}_q^N \to \mathbb{F}_q^M\}$. Let G denote a rv distributed uniformly on $\mathcal{G}$. Then, it holds for any $a_1^N \ne a_2^N$, $a_1^N, a_2^N \in \mathbb{F}_q^N$ that

$$\Pr\{G(a_1^N) = G(a_2^N)\} = \Pr\{\mathbf{L}a_1^N = \mathbf{L}a_2^N\} = q^{-M} = \frac{1}{|\mathbb{F}_q^M|}. \tag{90}$$

For a set of functions, not necessarily linear, with a common domain and a common range, this very property (90) of the set that for a random function distributed uniformly on the set, the reciprocal of the cardinality of the size of the common range equals the probability that the two values of the random function applied to *any* two distinct inputs coincide is referred to as the "universal" property in [2], and is used therein to prove the following result.

Lemma D.1 [2, Th. 3]: For a finite-valued rv $X \in \mathcal{X}$, let G be the rv uniformly distributed on a universal set of functions $\mathcal{G}$ from $\mathcal{X}$ to a finite set $\mathcal{B}$. Then, it holds that

$$H(G(X)|G) \ge \log|\mathcal{B}| - e^{\log|\mathcal{B}| - H_c(X)}$$

where

$$H_c(X) \stackrel{\triangle}{=} -\log\sum_{x\in\mathcal{X}} P_X(x)^2. \tag{91}$$

The proof of Lemma 4.5 relies, additionally, on the following three lemmas; the first two of these lemmas are new with their proofs being relegated to the end of this appendix, while the third lemma was shown in [4].

Lemma D.2: For $\delta > 0$, let

$$\mathcal{G}_N(\delta) = \left\{ \begin{array}{l} (a^N, u^N) \in \mathbb{F}_q^N \times \mathbb{R}^{nN} : \\ P_{A^N|U^N}(a^N|u^N) \le e^{-N(H(A|U)-\delta)} \end{array} \right\}$$

where $H(A|U) \stackrel{\triangle}{=} \mathbb{E}[-\log P_{A|U}(A|U)]$ and $P_{A|U}(\cdot|u)$, $u \in \mathbb{R}^n$, is the conditional pmf of A conditioned on $U = u$. Then, $\Pr\Big((A^N, U^N) \notin \mathcal{G}_N(\delta)\Big) = o_N(e^{-\alpha N})$, for some $\alpha > 0$.

Lemma D.3: For $\delta > 0$, let

$$\mathcal{F}_N(\delta) = \mathcal{G}_N(\delta) \bigcap \left[\mathbb{F}_q^N \times \left\{u^N : \sum_{a^N:(a^N,u^N)\in\mathcal{G}_N(\delta)} P_{A^N|U^N}(a^N|u^N) > e^{-\delta N}\right\}\right].$$

Then, $\Pr\Big((A^N,U^N) \notin \mathcal{F}_N(\delta)\Big) = o_N(e^{-\beta N})$ for some $\beta > 0$. Furthermore, for every u^N in a subset of $\mathbb{R}^{nN}$ of $P_{U^N|\mathcal{F}_N(\delta)}$-measure 1, it holds that[3]

$$H_c\left(A^N|U^N=u^N,(A^N,U^N)\in\mathcal{F}_N(\delta)\right)\geq N(H(A|U)-2\delta)$$

for all N sufficiently large.

Lemma D.4 [4]: Let A and B be finite-valued rvs, and let $\epsilon > 0$ be given. Then

$$P_B\Big(\{b\in\mathcal{B}: H_c(A)-H_c(A|B=b)\leq \log|\mathcal{B}|+\epsilon\}\Big) \geq 1-2e^{-\epsilon/2}.$$

Fix $\epsilon > 0$. By Lemma D.4, for every $u^N \in \mathbb{R}^{nN}$, we get (92), shown at the bottom of the page.

Then, with $\mathcal{S} = \mathcal{S}^{(N)} \subset \mathbb{R}^{nN}$ denoting the special subset from Lemma D.3 of $P_{U^N|\mathcal{F}_N(\delta)}$-measure 1, we have that (93), shown also at the bottom of the page, holds for all $N = N(\delta)$ sufficiently large, where

$$Q \triangleq N\left(H(A|U)-2\delta\right)-\log|\mathcal{B}|-\epsilon.$$

By Lemma D.1, for (u^N, b) satisfying condition (93), we have

$$H\Big(\mathbf{L}A^N|\mathbf{L},U^N=u^N,B=b,\mathbf{1}\Big(\left(A^N,U^N\right)\in\mathcal{F}_N(\delta)\Big)=1\Big) \geq M\log q - e^{M\log q-Q}. \quad (94)$$

Since

$$\begin{aligned} &H(\mathbf{L}A^N|\mathbf{L},U^N,B)\\ &\geq P_{A^N,U^N}(\mathcal{F}(\delta))\\ &\quad\times H\left(\mathbf{L}A^N|\mathbf{L},U^N,B,\mathbf{1}\Big(\left(A^N,U^N\right)\in\mathcal{F}_N(\delta)\Big)=1\right)\end{aligned}$$

and furthermore by (93), (94)

$$H\left(\mathbf{L}A^N|\mathbf{L},U^N,B,\mathbf{1}\Big(\left(A^N,U^N\right)\in\mathcal{F}_N(\delta)\Big)=1\right) \geq (1-2e^{-\epsilon/2})(M\log q-e^{M\log q-Q}) \quad (95)$$

for all $N = N(\delta)$ sufficiently large, we obtain that

$$H(\mathbf{L}A^N|\mathbf{L},U^N,B)\geq Pr(\mathcal{F}(\delta))\times(1-2e^{-\epsilon/2}) \times(M\log q-e^{M\log q-Q}) \quad (96)$$

[3]Here, $H_c\left(A^N|U^N=u^N,(A^N,U^N)\in\mathcal{F}_N(\delta)\right)$ is computed according to (91) but with the conditional pmf of A^N conditioned on $\{U^n=u^N,(A^N,U^N)\in\mathcal{F}_N(\delta)\}$ instead of according to its marginal probability.

for all $N = N(\delta)$ sufficiently large.

Upon selecting δ sufficiently small and $\gamma = \epsilon/N$ such that

$$R < [H(A|U)-2\delta-\frac{1}{N}\log|\mathcal{B}|-\gamma$$

we obtain from (96) that

$$H(\mathbf{A}U^N|\mathbf{L},U^N,B)\geq(1-o_N(e^{-\beta N}))\times(1-2e^{-\gamma N/2}) \times(M\log q-e^{-\eta N}) \quad (97)$$

for some $\eta > 0$. This proves (89) and, hence, the assertion of the lemma. ■

Proof of Lemma D.2: Let $X_i = -\log P_{A|U}(A_i|U_i)$, $i = 1,\ldots,N$, where $\left(A^N,U^N\right)$ are N i.i.d. repetitions of (A,U). Observe that $X_i \geq 0$ and $\mathbb{E}[X_i] = H(A|U)$, $i = 1,\ldots,N$, where $0 < H(A|U) \leq \log|\mathbb{F}_q| < \infty$.

Then, from [11, Th. 2.2.3], we have that for $0 < \delta < H(A|U)$

$$\limsup\frac{1}{N}\log P(\frac{1}{N}\sum_{i=1}^N X_i\in[0,H(A|U)-\delta]) \leq -\inf_{x\in[0,H(A|U)-\delta]}\Lambda^*(x)$$

where

$$\Lambda^*(x)\triangleq\sup_{\lambda\in\mathbb{R}}\lambda x-\Lambda(\lambda)$$

and

$$\Lambda(\lambda)\triangleq\log\mathbb{E}[e^{\lambda(-\log P_{A|U}(A|U))}].$$

As in [11], we define $\mathcal{D}_\Lambda\triangleq\{\lambda:\Lambda(\lambda)<\infty\}$. Next, we have

$$\begin{aligned}\Lambda(1)&=\log\mathbb{E}[\frac{1}{P_{A|U}(A|U)}]\\ &=\log\Big(\int\sum_{a:P_{A|U}(a|u)>0}P_{A|U}(a|u)\frac{1}{P_{A|U}(a|u)}dF_U(u)\Big)\\ &\leq\log|\mathbb{F}_q|<\infty.\end{aligned}$$

In addition, because $-\log P_{A|U}(A|U) \geq 0$, $\Lambda(\cdot)$ is nondecreasing. We then have that $(-\infty, 0]$ is in the interior of $\mathcal{D}_\Lambda$. It follows from [11, Lemma 2.2.5(b)] that $\Lambda^*(H(A|U)) = 0$ and that $\Lambda^*(x)$ is nonincreasing for $x < H(A|U)$. Consequently

$$\begin{aligned}\limsup\frac{1}{N}\log P(\frac{1}{N}\sum_{i=1}^N X_i\in[0,H(A|U)-\delta]) &\leq -\inf_{x\in[0,H(A|U)-\delta]}\Lambda^*(x)\\ &=\Lambda^*(H(A|U)-\delta).\end{aligned}$$

$$P_{B|U^N,\mathcal{F}_N(\delta)}\left(\left\{b\in\mathcal{B}:\begin{array}{c}H_c\Big(A^N|U^n=u^N,B=b,\mathcal{F}_N(\delta)\Big)\\ \geq H_c\Big(A^N|U^n=u^N,\mathcal{F}_N(\delta)\Big)\\ -\log|\mathcal{B}|-\epsilon\end{array}\right\}\Bigg|u^N,\mathcal{F}_N(\delta)\right)\geq 1-2e^{-\epsilon/2} \quad (92)$$

$$P_{U^N,B|\mathcal{F}_N(\delta)}\left(\left\{\begin{array}{l}(u^N,b)\in\mathcal{S}\times\mathcal{B}:\\ H_c\Big(A^N|U^n=u^N,B=b,\mathcal{F}_N(\delta)\Big)\geq Q\end{array}\right\}\Bigg|\mathcal{F}_N(\delta)\right)\geq 1-2e^{-\epsilon/2} \quad (93)$$

Also, from [11, Lemma 2.2.5(c)]. and the fact that 0 is in the the interior of $\mathcal{D}_\Lambda$, $\Lambda(\lambda)$ is differentiable at $\lambda = 0$ and $\Lambda'(0) = H(A|U)$. It suffices to prove that for $0 < \delta < H(A|U)$, $\Lambda^*(H(A|U) - \delta) > 0$. Suppose this is not the case, i.e., there exists $0 < \delta < H(A|U)$ such that $\Lambda^*(H(A|U) - \delta) = 0$. Then, from the definition of $\Lambda^*(x)$, it is necessarily true that for every $\lambda < 0$, $\lambda(H(A|U) - \delta) \leq \Lambda(\lambda)$. Consequently

$$\lim_{\lambda \to 0-} \frac{\Lambda(0) - \Lambda(\lambda)}{0 - \lambda} = \lim_{\lambda \to 0-} \frac{\Lambda(\lambda)}{\lambda} \leq H(A|U) - \delta$$

thereby contradicting the fact that $\Lambda'(0) = H(A|U)$. This completes the proof of Lemma D.2. ∎

Proof of Lemma D.3: We have

$$\begin{aligned}
&\Pr\Big((A^N, U^N) \notin \mathcal{F}_N(\delta)\Big) \\
&\leq \Pr\Big((A^N, U^N) \notin \mathcal{G}_N(\delta)\Big) \\
&+ P_{U^N}\left(\left\{u^N : \begin{matrix}\Pr\Big((A^N, U^N) \notin \mathcal{G}_N(\delta) | U^N = u^N\Big) \\ > 1 - e^{-\delta N}\end{matrix}\right\}\right).
\end{aligned}$$

On the right side above, the first term $= o_N(e^{-\alpha N})$ by Lemma D.2, while the second term $= \frac{o_N(e^{-\alpha N})}{1 - e^{-\delta N}} = o_N(e^{-\beta N})$ for some $\beta < \alpha$. Thus, $\Pr\Big((A^N, U^N) \notin \mathcal{F}_N(\delta)\Big) = o_N(e^{-\beta N})$, which is the first assertion of the lemma.

Next, for every $\big(a^N, u^N\big) \in \mathcal{F}_N(\delta)$

$$\begin{aligned}
&\Pr\Big(A^N = a^N | U^N = u^N, \big(A^N, U^N\big) \in \mathcal{F}_N(\delta)\Big) \\
&\qquad = \frac{P_{A^N|U^N}(a^N|u^N)}{\Pr\Big((A^N, U^N) \in \mathcal{F}_N(\delta) | U^N = u^N\Big)} \\
&\qquad = \frac{P_{A^N|U^N}(a^N|u^N)}{\sum_{a^N:(a^N,u^N)\in\mathcal{G}_N(\delta)} P_{A^N|U^N}(a^N|u^N)} \\
&\qquad < \frac{e^{-N(H(A|U)-\delta)}}{e^{-N\delta}}, \text{ since } \mathcal{F}_N(\delta) \subseteq \mathcal{G}_N(\delta) \\
&\qquad = e^{-N(H(A|U)-2\delta)}.
\end{aligned}$$

Hence, for every $u^N \in \mathcal{S}$, it holds that

$$\begin{aligned}
&H_c\Big(A^N | U^N = u^N, \big(A^N, U^N\big) \in \mathcal{F}_N(\delta)\Big) \\
&= -\log \sum_{a^N} \Big[\Pr\Big(A^N = a^N | U^N = u^N, \big(A^N, U^N\big) \in \mathcal{F}_N(\delta)\Big)\Big]^2 \\
&\geq -\log \left[\begin{matrix}\sum_{a^N} \Pr\Big(A^N = a^N | U^N = u^N, \big(A^N, U^N\big) \in \mathcal{F}_N(\delta)\Big) \\ \times e^{-N(H(A|U)-2\delta)}\end{matrix}\right] \\
&= N(H(A|U) - 2\delta)
\end{aligned}$$

thereby establishing the second assertion of the lemma. ∎

Appendix E

1) Proof of *(57):* Denoting $\mathcal{A} = \{(\alpha\mathbf{X}_1 - \mathbf{E}) \bmod \Lambda_3 = \alpha\mathbf{X}_1 - \mathbf{E}\}$, we have that $\Pr\{\mathcal{A}\} = 1 - o_n(1)$ by (56). Then

$$\begin{aligned}
&\mathbb{E}\left[||\mathbf{X}_1 - \hat{\mathbf{X}}_1||^2\right] \\
&\quad = \mathbb{E}\left[||\mathbf{X}_1 - c((\alpha\mathbf{X}_1 - \mathbf{E}) - Q_{\Lambda_3}(\alpha\mathbf{X}_1 - \mathbf{E}))||^2\right] \\
&\quad \leq \mathbb{E}\left[||(1 - c\alpha)\mathbf{X}_1 + c\mathbf{E}||^2\right] + \\
&\qquad \mathbb{E}\left[||cQ_{\Lambda_3}(\alpha\mathbf{X}_1 - \mathbf{E}))||^2\right] \\
&\quad = \mathbb{E}\left[||(1 - c\alpha)\mathbf{X}_1 + c\mathbf{E}||^2\right] + \\
&\qquad \mathbb{E}\left[||cQ_{\Lambda_3}(\alpha\mathbf{X}_1 - \mathbf{E}))||^2 \mathbf{1}(\mathcal{A}^c)\right] \\
&\quad \leq \mathbb{E}\left[||(1 - c\alpha)\mathbf{X}_1 + c\mathbf{E}||^2\right] + \\
&\qquad \sqrt{\mathbb{E}\left[||cQ_{\Lambda_3}(\alpha\mathbf{X}_1 - \mathbf{E}))||^4\right] \Pr(\mathbf{1}(\mathcal{A}^c))} \\
&\quad = n\left[(1 - c\alpha)^2\sigma_{X_1}^2 + c^2 D\right] + \\
&\qquad \sqrt{\mathbb{E}\left[||cQ_{\Lambda_3}(\alpha\mathbf{X}_1 - \mathbf{E}))||^4\right]} \sqrt{\Pr(\mathbf{1}(\mathcal{A}^c))}
\end{aligned}$$

where the second equality is by that fact that in $\mathcal{A}$, $Q_{\Lambda_3}(\alpha\mathbf{X}_1 - \mathbf{E}) = \mathbf{0}$; the two inequalities above are by the triangle inequality and the Cauchy–Schwarz inequality, respectively. Next

$$\begin{aligned}
&\sqrt{\mathbb{E}\left[||cQ_{\Lambda_3}(\alpha\mathbf{X}_1 - \mathbf{E}))||^4\right]} \\
&\quad = c^2 \sqrt{\mathbb{E}\left[||(\alpha\mathbf{X}_1 - \mathbf{E}) - (\alpha\mathbf{X}_1 - \mathbf{E}) \bmod \Lambda_3||^4\right]} \\
&\quad \leq c^2 \left[\begin{matrix}\mathbb{E}\left[||(\alpha\mathbf{X}_1 - \mathbf{E})||^4\right]^{\frac{1}{4}} \\ +\mathbb{E}\left[||(\alpha\mathbf{X}_1 - \mathbf{E}) \bmod \Lambda_3||^4\right]^{\frac{1}{4}}\end{matrix}\right]^2 \\
&\quad \leq c^2 \left[\mathbb{E}\left[||(\alpha\mathbf{X}_1 - \mathbf{E})||^4\right]^{\frac{1}{4}} + \mathbb{E}\left[||(\alpha\mathbf{X}_1 - \mathbf{E})||^4\right]^{\frac{1}{4}}\right]^2 \\
&\quad \leq 4c^2 \left[\mathbb{E}\left[||(\alpha\mathbf{X}_1 - \mathbf{E})||^4\right]^{\frac{1}{4}}\right]^2 \\
&\quad \leq 4c^2 \left[\mathbb{E}\left[||\alpha\mathbf{X}_1||^4\right]^{\frac{1}{4}} + \mathbb{E}\left[||\mathbf{E}||^4\right]^{\frac{1}{4}}\right]^2 \\
&\quad = \left[O(n^2)^{\frac{1}{4}} + O(n^2)^{\frac{1}{4}}\right]^2 = O(n)
\end{aligned}$$

where the first and the last inequalities are by Minkowski's inequality; the second inequality is from

$$||(\alpha\mathbf{X}_1 - \mathbf{E}) \bmod \Lambda_3|| \leq ||(\alpha\mathbf{X}_1 - \mathbf{E})||.$$

The last equality is a consequence of the components of $\mathbf{X}_1$ being i.i.d. Gaussian rvs and $\mathbf{E}$ taking values in $\nu(\Lambda_1)$ that is covered by a ball of radius $O(\sqrt{n})$ in (55). Consequently, we have

$$\mathbb{E}\left[||\mathbf{X}_1 - \hat{\mathbf{X}}_1||^2\right] \leq n(\left[(1 - c\alpha)^2\sigma_{X_1}^2 + c^2 D\right] + o_n(1)).$$

References

[1] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[2] C. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[3] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," *SIAM J. Comput.*, vol. 17, pp. 210–229, Apr. 1988.

[4] C. Cachin, "Entropy measures and unconditional security in cryptography," Ph.D. dissertation, ETH Zürich, Zürich, Switzerland, 1997.

[5] J. H. Conway and N. J. A. Sloane, *Sphere Packing, Lattices and Groups*. New York: Springer-Verlag, 1988.

[6] I. Csiszár, "Linear codes for sources and source networks: Error exponents, universal coding," *IEEE Trans. Inf. Theory*, vol. 28, no. 4, pp. 585–592, Jul. 1982.

[7] I. Csiszár, "Almost independence and secrecy capacity," *Probl. Pered. Inf.*, vol. 32, pp. 48–57, 1996.

[8] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 344–366, Mar. 2000.
[9] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.
[10] I. Csiszár and P. Narayan, "Secrecy capacities for multiterminal channel models," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2437–2452, Jun. 2008.
[11] A. Dembo and O. Zeitouni, *Large Deviations Techniques and Applications*. New York: Springer-Verlag, 1998.
[12] U. Erez and R. Zamir, "Achieving $\frac{1}{2}\log(1 + SNR)$ on the AWGN channel with lattice encoding and decoding," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2293–2314, Oct. 2004.
[13] 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.
[14] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed. Oxford, U.K.: Oxford Univ. Press, 1979.
[15] Y. Liang, H. V. Poor, and S. S. Shitz, "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, pp. 355–580, 2008.
[16] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
[17] U. M. Maurer, "The strong secret key rate of discrete random triples," in *Communications and Cryptography: Two Sides of One Tapestry*, R. E. Blahut, Ed. *et al.* Norwell, MA: Kluwer, 1994, ch. 26, pp. 271–285.
[18] U. M. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Advances in Cryptology—EUROCRYPT 2000*. New York: Springer-Verlag, 2000, vol. LNCS-1807, pp. 352–368.
[19] G. Poltyrev, "On coding without restrictions for the AWGN channel," *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 409–417, Mar. 1994.
[20] A. B. Wagner, S. Tavildar, and P. Viswanath, "Rate region of the quadratic Gaussian two-encoder source-coding problem," *IEEE Trans. Inf. Theory*, vol. 54, no. 5, pp. 1938–1961, May 2008.
[21] 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. 1556–6013, Sep. 2011.
[22] A. D. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. 22, no. 1, pp. 1–10, Jan. 1976.
[23] R. Zamir and M. Feder, "On universal quantization by randomized uniform/ lattice quantizer," *IEEE Trans. Inf. Theory*, vol. 38, no. 2, pp. 428–436, Mar. 1992.
[24] R. Zamir and M. Feder, "On lattice quantization noise," *IEEE Trans. Inf. Theory*, vol. 42, no. 4, pp. 1152–1159, Jul. 1996.
[25] R. Zamir, S. Shamai, and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1250–1276, Jun. 2002.

Sirin Nitinawarat (S'09–M'11) obtained the B.S.E.E. degree from Chulalongkorn University, Bangkok, Thailand, with first class honors, and the M.S.E.E. degree from the University of Wisconsin, Madison. He received his Ph.D. degree from the Department of Electrical and Computer Engineering and the Institute for Systems Research at the University of Maryland, College Park, in December 2010.

He is now a Postdoctoral Fellow at the University of Illinois at Urbana-Champaign and the Coordinated Science Laboratory. He was a finalist for the best student paper award for the IEEE International Symposium on Information Theory, which was held at Austin, TX, in 2010. His research interests are in information theory, estimation and detection theory, Markov decision processes, and coding theory.

Prakash Narayan (S'80–M'81–SM'94–F'01) received the Bachelor of Technology degree in electrical engineering from the Indian Institute of Technology, Madras, in 1976. He received the M.S. degree in systems science and mathematics in 1978, and the D.Sc. degree in electrical engineering in 1981, both from Washington University, St. Louis, MO.

He is Professor of Electrical and Computer Engineering at the University of Maryland, College Park, with a joint appointment at the Institute for Systems Research. He has held visiting appointments at ETH, Zurich; the Technion, Haifa; the Renyi Institute of the Hungarian Academy of Sciences, Budapest; the University of Bielefeld; the Institute of Biomedical Engineering (formerly LADSEB), Padova; and the Indian Institute of Science, Bangalore. His research interests are in multiuser information theory, communication theory, communication networks, cryptography, and information theory and statistics.

Dr. Narayan has served as an Associate Editor for Shannon Theory for the IEEE TRANSACTIONS ON INFORMATION THEORY; was Co-Organizer of the IEEE Workshop on Multiuser Information Theory and Systems, VA (1983); Technical Program Chair of the IEEE/IMS Workshop on Information Theory and Statistics, VA (1994); General Co-Chair of the IEEE International Symposium on Information Theory, Washington, D.C. (2001); and Technical Program Co-Chair of the IEEE Information Theory Workshop, Bangalore (2002). He currently serves as a Member of the Board of Governors of the IEEE Information Theory Society.