Secret key generation from Gaussian sources using lattice-based extractors

Laura Luzzi, Cong Ling and Matthieu R. Bloch

Abstract

We propose a lattice-based scheme for secret key generation from Gaussian sources in the presence of an eavesdropper, and show that it achieves the strong secret key capacity in the case of degraded source models, as well as the optimal secret key / public communication rate trade-off. The key ingredients of our scheme are a lattice extractor to extract the channel intrinsic randomness, based on the notion of flatness factor, together with a randomized lattice quantization technique to quantize the continuous source. Compared to previous works, we introduce two new notions of flatness factor based on L^1 distance and KL divergence, respectively, which might be of independent interest. We prove the existence of secrecy-good lattices under L^1 distance and KL divergence, whose L^1 and KL flatness factors vanish for volume-to-noise ratios up to $2\pi e$. This improves upon the volume-to-noise ratio threshold 2π of the L^∞ flatness factor.

Index Terms

Extractor, secret key generation, strong secrecy, lattice coding, flatness factor.

I. Introduction

Secret key generation (also known as key agreement) at the physical layer was first investigated by Maurer [3] and Ahlswede and Csiszár [4], who showed that correlated observations of noisy phenomena could be used to distill secret keys by exchanging information over a public channel. In recent years, this subject has received considerable attention in literature (see, e.g., [5–10]). The setup has been extended to the vector case [11, 12], the multi-terminal case [13–16], the quantum case [17] and the case with feedback [18]. Second-order asymptotics have been derived in [19, 20]. Code constructions for the discrete memoryless case have been proposed, e.g. [21, 22].

Most existing secret key generation schemes rely heavily on the assumption of discrete random sources over finite or countable alphabets. In order to apply these techniques to wireless communications, it is necessary to extend the key generation framework to the case of continuous sources, such as Gaussian sources [11, 23–25]. In [25], the authors study a multi-terminal scenario for secret key generation in the special case for which the eavesdropper only has access to the public channel. Beside providing a characterization of the optimal strongly secret key rate, the authors show that this optimal rate can be achieved using lattice codes (for information reconciliation only).

We consider here the problem of secret key generation between two terminals, Alice and Bob, who observe correlated Gaussian sequences X^n and Y^n, in the presence of an eavesdropper, Eve, who also obtains a correlated sequence Z^n. For simplicity, we suppose that a single round of unidirectional public communication takes place in order to establish the key. Our main contribution is to show that, in the case of a degraded source model, the strong secret key capacity can be achieved by a complete lattice-coding scheme considerably different from and perhaps simpler than [25]. This extends our previous work [1], in which it was shown that a secret key rate up to half a nat from the optimal was achievable.

The work of L. Luzzi was supported in part by the INEX CY Initiative AAP2017 Lattice Hashing and the INEX CY Initiative Ambition AAP2020 PHEBE. The work of C. Ling was supported in part by the Engineering and Physical Sciences Research Council (EPSRC) under Grant No. EP/S021043/1. The work of M. Bloch was supported in part by the National Science Foundation under award 1955401. This work was presented in part at the IEEE International Symposium on Information Theory (ISIT 2013), Istanbul, Turkey [1], and in part at the International Zurich Seminar on Communications (IZS 2018) [2].

L. Luzzi is with ETIS, UMR 8051 (CY Cergy Paris Université, ENSEA, CNRS), 95014 Cergy-Pontoise, France (e-mail: laura.luzzi@ensea.fr).

C. Ling is with the Department of Electrical and Electronic Engineering, Imperial College London, London SW7 2AZ, U.K. (e-mail: cling@ieee.org).

M. R. Bloch is with School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, Georgia (email: matthieu.bloch@ece.gatech.edu).

Typically, secret key generation consists of two distinct procedures: *information reconciliation*, in which public messages are exchanged to ensure that Alice and Bob can construct the same data sequence with vanishing error probability, and *privacy amplification* to extract from this shared sequence a secret key that is statistically independent from Eve's observation and from the public messages.

Privacy amplification and randomness extraction: Our privacy amplification strategy is based on the concept of *channel intrinsic randomness*, or the maximum bit rate that can be extracted from a channel output independently of its input [26–28]. We begin by considering a simplified scenario in which Bob and Alice share the same variable X^n. In this case, the amount of randomness that can be extracted from X^n independently of Z^n is precisely the maximum available secret key rate. We propose a *lattice-based extractor* to extract the randomness, by reducing the source modulo a suitable lattice. Although our main objective in this paper is to solve the problem of privacy amplification, our lattice extractor is also an intriguing result in its own right, which could have other applications.

The flatness factor and its variants: In our previous work [1], we provided a characterization of the class of lattices that are good for randomness extraction, which was based on a computable parameter, the *flatness factor*, measuring the L^∞ distance between the "folded" Gaussian distribution modulo the lattice and the uniform distribution on the corresponding fundamental region. The concept of flatness factor is related to the smoothing parameter used in lattice-based cryptography [29], and was first introduced in [30] in the context of physical-layer network coding. In [31], two of the authors also showed the relevance of the flatness factor for secrecy and introduced the notion of *secrecy-good lattices* for the wiretap channel. In this work, we consider two extended notions of flatness factor by which the L^∞ distance is replaced respectively by the L^1 distance and the Kullback-Leibler (KL) divergence. These new flatness conditions are satisfied by a wider range of variance parameters, resulting in improved volume conditions for the chain of lattices under consideration, which allows us to achieve the secret key capacity. The existence of lattices with vanishing L^1 and KL flatness factors follows by leveraging an existence result for resolvability codes for regular channels [32]. We note that the L^1 smoothing parameter was already considered in [33, 34], while L^1 and KL flatness factors were used implicitly earlier in [35, p. 1656]. An upper bound on the L^1 flatness factor based on the Cauchy-Schwarz inequality was given in [36]. The independent work [37] studied L^1 smoothing parameters both for lattices and for codes, also based on the Cauchy-Schwarz inequality. Our approach bypasses the Cauchy-Schwarz inequality, therefore leading to a tighter bound than [36]. We note however that [37] obtained a bound on the L^1 smoothing parameter as tight as that in this paper, by decomposing the discrete Gaussian distribution into a convex combination of uniform ball distributions.

Information reconciliation and Wyner-Ziv coding: Our strategy for information reconciliation follows the outline of [23, 25]: first, the source X^n is vector quantized; then, a public message is generated in the manner of Wyner-Ziv coding, so that Bob can decode the quantized variable using the sequence Y^n as side information. The existence of good nested lattices for Wyner-Ziv coding has been established in [38] (see also [39, 40]). We show that this construction is compatible with the secrecy-goodness property to conclude our existence proof.

Randomized quantization technique: Unlike our previous work [1], the quantization performed at Alice's side is not deterministic. We introduce a new *randomized quantization* step inspired by the randomized rounding technique in [41]. Essentially, this technique allows to round a continuous Gaussian into a *discrete Gaussian distribution* with slightly larger variance, provided that the L^∞ flatness factor of the lattice is small. We partially extend the result of [41] under an L^1 flatness factor criterion. We show that randomized quantization with uniform dithering (where the dither is known by all parties, including the eavesdropper) achieves the optimal trade-off between public communication rate and secret key rate established in [23]. The dithering technique is widely used to achieve capacity in literature [42, 43].

Relation to fuzzy extractors: The lattice extractor proposed in this paper is related to fuzzy extractors in the cryptographic literature, usually defined for discrete sources [44]. A fuzzy extractor allows one to extract a secret key from a noisy measurement, which means that it is resilient to small measurement errors. Fuzzy extractors for continuous signals were proposed in [45, 46]. Our proposed lattice code is also robust to measurement errors, thanks to its channel coding component of Wyner-Ziv coding. A difference is that min-entropy is used in fuzzy extractors, while Shannon entropy is used in our lattice extractor. In order to be consistent with the literature, we change the terminology *lattice hashing* used in the conference version of this paper [1] to *lattice extractor*.

Organization: This paper is organized as follows. In Section II we provide basic definitions about lattices and introduce the flatness factor and its variants, which allows us to define the notion of secrecy-good lattices. In Section III, we focus on the extraction of channel intrinsic randomness over Gaussian channels using lattices. In Section

IV, we introduce the Gaussian source model and describe our lattice-based secret key generation scheme. Finally, in Section V we offer some conclusions and perspectives. The existence of sequences of nested lattices satisfying the required conditions is proven in the Appendix.

II. Lattices and Flatness Factor

Notation: All logarithms in this paper are assumed to be natural logarithms, and information is measured in nats. Given a set A, the notation $\mathcal{U}_A$ stands for the uniform distribution over A. We denote the variational distance between two (discrete or continuous) distributions p, q by $\mathbb{V}(p, q)$, and their KL divergence by $\mathbb{D}(p\|q)$.

A. Lattice definitions

In this section, we introduce the mathematical tools we use to describe and analyze our proposed scheme.

An n-dimensional lattice Λ in the Euclidean space $\mathbb{R}^n$ is the discrete set defined by

$$\Lambda = \mathcal{L}(\mathbf{B}) = \{\mathbf{B}\mathbf{x} : \mathbf{x} \in \mathbb{Z}^n\}$$

where the columns of the basis matrix $\mathbf{B} = [\mathbf{b}_1 \cdots \mathbf{b}_n]$ are linearly independent.

Given a lattice Λ, its dual lattice Λ^* is defined as the set of vectors λ^* in $\mathbb{R}^n$ such that $\langle \lambda^*, \lambda \rangle \in \mathbb{Z}$ for all $\lambda \in \Lambda$.

A measurable set $\mathcal{R}(\Lambda) \subset \mathbb{R}^n$ is called a fundamental region of the lattice Λ if the disjoint union $\cup_{\lambda\in\Lambda}(\mathcal{R}(\Lambda) + \lambda) = \mathbb{R}^n$. Examples of fundamental regions include the fundamental parallelepiped $\mathcal{P}(\Lambda)$ and the Voronoi region $\mathcal{V}(\Lambda)$. All the fundamental regions have equal volume $V(\Lambda)$.

Given a lattice Λ and a fundamental region $\mathcal{R}(\Lambda)$, any point $\mathbf{x} \in \mathbb{R}^n$ can be written uniquely as a sum

$$\mathbf{x} = \lambda + \bar{\mathbf{x}},$$

where $\lambda \in \Lambda$ and $\bar{\mathbf{x}} \in \mathcal{R}(\Lambda)$. The vector λ is the quantization of $\mathbf{x}$ with respect to $\mathcal{R}(\Lambda)$ and is denoted as $Q_{\mathcal{R}(\Lambda)}(\mathbf{x})$, where boundary points are decided systematically. Thus we define

$$[\mathbf{x}] \bmod \mathcal{R}(\Lambda) = \mathbf{x} - Q_{\mathcal{R}(\Lambda)}(\mathbf{x}) = \bar{\mathbf{x}}. \tag{1}$$

In particular, for any $\mathbf{x} \in \mathbb{R}^n$, the nearest-neighbor quantizer associated with Λ is given by

$$Q_\Lambda(\mathbf{x}) = Q_{\mathcal{V}(\Lambda)}(\mathbf{x}) = \arg\min_{\lambda\in\Lambda} \|\lambda - \mathbf{x}\|$$

where ties are broken systematically. Note that $\mathbf{x} \bmod \mathcal{V}(\Lambda) = \mathbf{x} - Q_\Lambda(\mathbf{x})$. The modulo lattice operation satisfies the distributive law [47, Proposition 2.3.1], i.e., $\forall \lambda \in \Lambda$

$$[\mathbf{x} + \lambda] \bmod \mathcal{R}(\Lambda) = [\mathbf{x}] \bmod \mathcal{R}(\Lambda). \tag{2}$$

The following property [48, equation (35)] will also be used in the paper: given two lattices $\Lambda \subseteq \Lambda_1$, $\mathbf{x} \in \mathbb{R}^n$, and a fundamental region $\mathcal{R}(\Lambda)$,

$$[Q_{\Lambda_1}(\mathbf{x})] \bmod \mathcal{R}(\Lambda) = [Q_{\Lambda_1}([\mathbf{x}] \bmod \mathcal{R}(\Lambda))] \bmod \mathcal{R}(\Lambda). \tag{3}$$

Given a sublattice $\Lambda' \subset \Lambda$, the quotient group Λ/Λ' is defined as the group of distinct cosets $\lambda + \Lambda'$ for $\lambda \in \Lambda$. It can be identified by a set of coset representatives $\Lambda \cap \mathcal{R}(\Lambda')$, where $\mathcal{R}(\Lambda')$ is any fundamental region of Λ'. Furthermore, $\mathcal{R}(\Lambda')$ can be written as a disjoint union of translates of any fundamental region $\mathcal{R}(\Lambda)$ as follows [47, equation (8.33)]:

$$\mathcal{R}(\Lambda') = \bigcup_{\lambda\in\Lambda\cap\mathcal{R}(\Lambda')} \left([\lambda + \mathcal{R}(\Lambda)] \bmod \mathcal{R}(\Lambda')\right). \tag{4}$$

B. Gaussian distributions and the L^∞ flatness factor

Suppose that X^n is an n-dimensional i.i.d. Gaussian random variable of variance σ^2 with distribution

$$f_\sigma(\mathbf{x}) = \frac{1}{(\sqrt{2\pi}\sigma)^n} e^{-\frac{\|\mathbf{x}\|^2}{2\sigma^2}},$$

for $\mathbf{x} \in \mathbb{R}^n$. The following useful property of Gaussian distributions was proven in [41, Fact 2.1][1]:

Lemma 1: Given $\sigma_1, \sigma_2 > 0$, let σ and $\bar{\sigma}$ be such that $\sigma^2 = \sigma_1^2 + \sigma_2^2$, and $\frac{1}{\bar{\sigma}^2} = \frac{1}{\sigma_1^2} + \frac{1}{\sigma_2^2}$. Moreover, let $\mathbf{c}_1, \mathbf{c}_2 \in \mathbb{R}^n$, and $\bar{\mathbf{c}} = \frac{\bar{\sigma}^2}{\sigma_1^2}\mathbf{c}_1 + \frac{\bar{\sigma}^2}{\sigma_2^2}\mathbf{c}_2$. Then $\forall \mathbf{x} \in \mathbb{R}^n$,

$$f_{\sigma_1}(\mathbf{x} - \mathbf{c}_1) f_{\sigma_2}(\mathbf{x} - \mathbf{c}_2) = f_{\sigma}(\mathbf{c}_1 - \mathbf{c}_2) f_{\bar{\sigma}}(\mathbf{x} - \bar{\mathbf{c}}).$$

Given a lattice Λ, we define the Λ-periodic function

$$f_{\sigma,\Lambda}(\mathbf{x}) = \frac{1}{(\sqrt{2\pi}\sigma)^n} \sum_{\lambda \in \Lambda} e^{-\frac{\|\mathbf{x}+\lambda\|^2}{2\sigma^2}}, \tag{5}$$

for all $\mathbf{x} \in \mathbb{R}^n$. We denote by $f_{\sigma,\mathcal{R}(\Lambda)} = f_{\sigma,\Lambda|\mathcal{R}(\Lambda)}$ its restriction to the fundamental region $\mathcal{R}(\Lambda)$. Note that $f_{\sigma,\mathcal{R}(\Lambda)}$ is the probability density of $\bar{\mathsf{X}}^n = [\mathsf{X}^n] \bmod \mathcal{R}(\Lambda)$. Given $\mathbf{c} \in \mathbb{R}^n$, we will also use the notation

$$f_{\sigma,\Lambda,\mathbf{c}}(\mathbf{x}) = f_{\sigma,\Lambda}(\mathbf{x} - \mathbf{c})$$

to denote a shifted Λ-periodic function.

Definition 1 (L^∞ Flatness factor [31]): For a lattice Λ and for a parameter σ, the L^∞ flatness factor is defined by:

$$\epsilon_\Lambda(\sigma) \triangleq \max_{\mathbf{x} \in \mathcal{R}(\Lambda)} \left| V(\Lambda) f_{\sigma,\Lambda}(\mathbf{x}) - 1 \right|.$$

In other words, $\epsilon_\Lambda(\sigma)$ characterizes the L^∞ distance of $f_{\sigma,\Lambda}(\mathbf{x})$ to the uniform distribution $U_{\mathcal{R}(\Lambda)}$ over $\mathcal{R}(\Lambda)$.

The L^∞ flatness factor is independent of the choice of the fundamental region $\mathcal{R}(\Lambda)$ and can be computed from the theta series of the lattice

$$\Theta_\Lambda(\tau) = \sum_{\lambda \in \Lambda} e^{-\pi\tau\|\lambda\|^2} \tag{6}$$

using the identity [31, Proposition 2]

$$\epsilon_\Lambda(\sigma) = \left(\frac{\gamma_\Lambda(\sigma)}{2\pi}\right)^{\frac{n}{2}} \Theta_\Lambda\left(\frac{1}{2\pi\sigma^2}\right) - 1, \tag{7}$$

where $\gamma_\Lambda(\sigma) = \frac{V(\Lambda)^{\frac{2}{n}}}{\sigma^2}$ is the volume-to-noise ratio (VNR). Moreover, the following relation holds between the flatness factor of Λ and the theta series of its dual lattice Λ^* [31, Corollary 1]:

$$\Theta_{\Lambda^*}(2\pi\sigma^2) = \epsilon_\Lambda(\sigma) + 1. \tag{8}$$

Remark 1: We have shown in [31] that ϵ_Λ is a monotonically decreasing function, i.e., for $\sigma < \sigma'$, we have $\epsilon_\Lambda(\sigma') \leq \epsilon_\Lambda(\sigma)$.

The notion of secrecy-goodness characterizes lattice sequences whose L^∞ flatness factors vanish exponentially fast as $n \to \infty$.

Definition 2 (Secrecy-good lattices under L^∞ flatness factor [31]): A sequence of lattices $\Lambda^{(n)}$ is *secrecy-good* under L^∞ flatness factor if $\epsilon_{\Lambda^{(n)}}(\sigma) = e^{-\Omega(n)}$ for all fixed $\gamma_{\Lambda^{(n)}}(\sigma) < 2\pi$.

In [31] we have proven the existence of sequences of secrecy-good lattices under L^∞ flatness factor as long as

$$\gamma_\Lambda(\sigma) < 2\pi. \tag{9}$$

Remark 2: In fact, we can show a concentration result: $\forall \eta > 0$ there exists a mod-p lattice ensemble such that lattice sequences from this ensemble are secrecy-good with probability greater than $1 - \eta$ (see [31, Appendix III]).

C. The mod-Λ channel and the mod-Λ/Λ' channel

Following Forney et al. [49], given a fundamental region $\mathcal{R}(\Lambda)$ of Λ we can define the mod-Λ channel with input $\mathsf{X}^n \in \mathcal{R}(\Lambda)$ and output

$$\mathsf{Y}^n = [\mathsf{X}^n + \mathsf{W}^n] \bmod \mathcal{R}(\Lambda),$$

[1]Note that although the statement in [41] refers to (unnormalized) Gaussian functions, one can check that it also holds for Gaussian distributions.

where W^n is a noise vector. When W^n is i.i.d. Gaussian with variance σ^2, this channel has capacity

$$C(\Lambda, \sigma^2) = \log V(\Lambda) - h(f_{\sigma,\Lambda}).$$

In the above expression, with slight abuse of notation we denote by $h(f_{\sigma,\Lambda})$ the differential entropy of $f_{\sigma,\mathcal{R}(\Lambda)}$, which does not depend on the choice of the region $\mathcal{R}(\Lambda)$.

The following result [50, Lemma 1] relates the L^∞ flatness factor to the capacity of the mod Λ channel.

Lemma 2: The capacity $C(\Lambda, \sigma^2)$ of the mod-Λ channel is bounded by $C(\Lambda, \sigma^2) \le \log(1 + \epsilon_\Lambda(\sigma)) \le \epsilon_\Lambda(\sigma)$.

Given two nested lattices $\Lambda' \subset \Lambda$ and a fundamental region $\mathcal{R}(\Lambda')$, we can define the mod Λ/Λ' channel with discrete input $\mathsf{X}^n \in \Lambda \cap \mathcal{R}(\Lambda')$ and output

$$\mathsf{Y}^n = [\mathsf{X}^n + \mathsf{W}^n] \bmod \mathcal{R}(\Lambda').$$

It was shown in [49] that this channel has capacity

$$C(\Lambda/\Lambda', \sigma^2) = \log \left|\Lambda/\Lambda'\right| + h(f_{\sigma,\Lambda}) - h(f_{\sigma,\Lambda'}).$$

In particular, the following relation holds:

$$C(\Lambda/\Lambda', \sigma) = C(\Lambda', \sigma^2) - C(\Lambda, \sigma^2). \tag{10}$$

Lemma 3: For any $\sigma > 0$,

$$C(\Lambda/\Lambda', \sigma^2) = \mathbb{D}\left(f_{\sigma,\mathcal{R}(\Lambda')} \middle\| \frac{1}{|\Lambda/\Lambda'|} f_{\sigma,\Lambda|\mathcal{R}(\Lambda')}\right).$$

The proof of Lemma 3 can be found in Appendix A.

D. The L^1 flatness factor and the KL flatness factor

In this section, we introduce a weaker notion of flatness based on the L^1 distance.

Definition 3: Given a lattice Λ, a fundamental region $\mathcal{R}(\Lambda)$ and $\sigma > 0$, we define the L^1 *flatness factor* as follows:

$$\epsilon^1_\Lambda(\sigma) = \int_{\mathcal{R}(\Lambda)} \left| f_{\sigma,\Lambda}(\mathbf{x}) - \frac{1}{V(\Lambda)} \right| d\mathbf{x} = \mathbb{V}(f_{\sigma,\mathcal{R}(\Lambda)}, \mathcal{U}_{\mathcal{R}(\Lambda)}). \tag{11}$$

Similarly to the L^∞ flatness factor, the L^1 flatness factor does not depend on the choice of the fundamental region.

Remark 3: For any lattice Λ, $\forall \sigma > 0$, we have $\epsilon^1_\Lambda(\sigma) \le \epsilon_\Lambda(\sigma)$.

The L^1 flatness factor is related to the L^1 smoothing parameter, which was discussed in [33, 34].

We also introduce yet another notion of flatness factor which replaces L^1 distance with KL divergence.

Definition 4: Given a lattice Λ, a fundamental region $\mathcal{R}(\Lambda)$ and $\sigma > 0$, we define the *KL flatness factor* as follows:

$$\epsilon^{KL}_\Lambda(\sigma) = \mathbb{D}(f_{\sigma,\mathcal{R}(\Lambda)} || \mathcal{U}_{\mathcal{R}(\Lambda)}). \tag{12}$$

As before, the definition does not depend on the choice of the fundamental region.

Remark 4: By Pinsker's inequality, $\forall \sigma > 0$,

$$\epsilon^1_\Lambda(\sigma) \le \sqrt{2\epsilon^{KL}_\Lambda(\sigma)}.$$

Remark 5 (Relation to the capacity of the mod-Λ channel): Note that [35, p.1656]

$$\mathbb{D}(f_{\sigma,\mathcal{R}(\Lambda)} || \mathcal{U}_{\mathcal{R}(\Lambda)}) = \log V(\Lambda) - h(f_{\sigma,\Lambda}) = C(\Lambda, \sigma^2).$$

By shift-invariance of the differential entropy, the KL flatness factor is also shift-invariant, i.e.

$$\epsilon_\Lambda(\sigma) = \mathbb{D}(f_{\sigma,\Lambda,\mathbf{c}|\mathcal{R}(\Lambda)} || \mathcal{U}_{\mathcal{R}(\Lambda)})$$

for all $\mathbf{c} \in \mathbb{R}^n$.

Thanks to Remark 5, we are able to prove the following

Lemma 4: The L^1 and KL flatness factors are monotonic, i.e. for any lattice Λ, $\forall \sigma' > \sigma$,

$$\epsilon^1_\Lambda(\sigma') \le \epsilon^1_\Lambda(\sigma), \quad \text{and} \quad \epsilon^{KL}_\Lambda(\sigma') \le \epsilon^{KL}_\Lambda(\sigma).$$

Proof: Let $\mathsf{W}^n \sim \mathcal{N}(0, \sigma^2 I_n)$ and $\mathsf{X}^n = \mathsf{W}^n \bmod \mathcal{R}(\Lambda) \sim f_{\sigma,\mathcal{R}(\Lambda)}$.
Given $\sigma_0 > 0$, let $\mathsf{W}_0^n \sim \mathcal{N}(0, \sigma_0^2 I_n)$ and consider

$$\mathsf{Y}^n = [\mathsf{X}^n + \mathsf{W}_0^n] \bmod \mathcal{R}(\Lambda) = [[\mathsf{W}^n] \bmod \mathcal{R}(\Lambda)) + \mathsf{W}_0^n] \bmod \mathcal{R}(\Lambda) = [\mathsf{W}^n + \mathsf{W}_0^n] \bmod \mathcal{R}(\Lambda) \sim f_{\sqrt{\sigma^2+\sigma_0^2},\mathcal{R}(\Lambda)}.$$

using the distributive property (2). Now consider the random variable $\mathsf{U}^n \sim \mathcal{U}_{\mathcal{R}(\Lambda)}$. By the Crypto Lemma [47, Lemma 4.1.1],

$$[\mathsf{U}^n + \mathsf{W}_0^n] \bmod \mathcal{R}(\Lambda) \sim \mathcal{U}_{\mathcal{R}(\Lambda)}.$$

Then using the data processing inequality for the variational distance,

$$\epsilon_\Lambda^1\left(\sqrt{\sigma^2+\sigma_0^2}\right) = \mathbb{V}\left(f_{\sqrt{\sigma^2+\sigma_0^2},\mathcal{R}(\Lambda)}, \mathcal{U}_{\mathcal{R}(\Lambda)}\right) = \mathbb{V}(\mathsf{Y}^n, \mathsf{U}^n) \le \mathbb{V}(\mathsf{X}^n, \mathsf{U}^n) = \mathbb{V}(f_{\sigma,\mathcal{R}(\Lambda)}, \mathcal{U}_{\mathcal{R}(\Lambda)}) = \epsilon_\Lambda^1(\sigma).$$

Similarly, from the data processing inequality for the KL divergence [51, Lemma 3.11], we have

$$\epsilon_\Lambda^{KL}\left(\sqrt{\sigma^2+\sigma_0^2}\right) = \mathbb{D}\left(f_{\sqrt{\sigma^2+\sigma_0^2},\mathcal{R}(\Lambda)} || \mathcal{U}_{\mathcal{R}(\Lambda)}\right) = \mathbb{D}(\mathsf{Y}^n || \mathsf{U}^n) \le \mathbb{D}(\mathsf{X}^n || \mathsf{U}^n) = \mathbb{D}(f_{\sigma,\mathcal{R}(\Lambda)} || \mathcal{U}_{\mathcal{R}(\Lambda)}) = \epsilon_\Lambda^{KL}(\sigma).$$

Since this is true for any $\sigma_0 > 0$, the conclusion follows. □

We will next show that lattices that are good for secrecy in the KL sense exist and that the corresponding volume condition is less stringent than the condition (9) for secrecy-goodness based on the L^∞ metric.

Definition 5: A sequence of lattices $\{\Lambda^{(n)}\}$ is L^1 *secrecy-good* if for all fixed $\gamma_{\Lambda^{(n)}}(\sigma) < 2\pi e$, $\forall c > 0$, $\epsilon^1_{\Lambda^{(n)}}(\sigma) = o\left(\frac{1}{n^c}\right)$, i.e., the L^1 flatness factor vanishes super-polynomially. It is *KL secrecy-good* if $\epsilon^{KL}_{\Lambda^{(n)}}(\sigma) = o\left(\frac{1}{n^c}\right)$.

By Remark 4, a sequence of KL secrecy-good lattices is also L^1 secrecy-good. The following theorem, which was presented in [2], is the first main result of this paper:

Theorem 1: If $\gamma_\Lambda(\sigma) < 2\pi e$ is fixed, then there exists a sequence $\{\Lambda^{(n)}\}$ of lattices which are KL secrecy-good (and also L^1-secrecy good).

The proof of Theorem 1 is given in Appendix C. Our proof is information-theoretic and does not require the knowledge of the theta series, in contrast to the L^∞ flatness factor. We summarize the main idea here. We use the standard Construction A to find the sought-after lattice Λ from a fine lattice Λ_f where $\Lambda \subseteq \Lambda_f^n$. Using the chain rule (10), we have

$$\mathbb{D}(f_{\mathcal{R}(\Lambda),\sigma} || \mathcal{U}_{\mathcal{R}(\Lambda)}) = C(\Lambda, \sigma^2) = C(\Lambda_f^n, \sigma^2) + C(\Lambda_f^n/\Lambda, \sigma^2).$$

Now, using a sufficiently fine lattice Λ_f, we can easily make $C(\Lambda_f^n, \sigma^2) \to 0$ thanks to the flatness phenomenon (cf. Lemma 2). The non-trivial part of the proof is to exhibit a lattice Λ such that $C(\Lambda_f^n/\Lambda, \sigma^2) \to 0$ as well. Here, opposite to the usual goal of achieving channel capacity in information theory, we use a code ($\cong \Lambda_f^n/\Lambda$) whose "capacity" is vanishing. Such a code can be a linear *resolvability code*. More precisely, because the Λ_f^n/Λ channel is regular, its capacity is attained by the uniform input distribution. Thus

$$C(\Lambda_f^n/\Lambda, \sigma^2) = \mathbb{I}(\mathsf{M}; \mathsf{Y}^n),$$

the mutual information for uniform input $\mathsf{M} \in \Lambda_f^n/\Lambda$. This means that if M is encoded by a linear code achieving strong secrecy over the Λ_f^n/Λ channel, then $\mathbb{I}(\mathsf{M}; \mathsf{Y}^n) \to 0$ and accordingly $C(\Lambda_f^n/\Lambda, \sigma^2) \to 0$. However, making the above argument rigorous involve certain technicalities, which are sorted out in Appendix C.

Remark 6: It is worth mentioning that as soon as the VNR exceeds 2π, the L^∞ flatness factor increases exponentially. In fact, it is easy to see that the bound $\gamma_\Lambda(\sigma) < 2\pi$ is sharp: the L^∞ flatness factor of a lattice cannot vanish for any $\gamma_\Lambda(\sigma) > 2\pi$. This is simply because (7) implies that

$$\epsilon_\Lambda(\sigma) > \left(\frac{\gamma_\Lambda(\sigma)}{2\pi}\right)^{\frac{n}{2}} - 1$$

since $\Theta_\Lambda(\tau) > 1$ for any $\tau > 0$. Thus, as the VNR approaches $2\pi e$, the L^∞ flatness factor $\approx e^{n/2}$, but the L^1 flatness factor can still be brought under control. This demonstrates the advantage of the L^1 flatness factor.

Also note that the VNR of a secrecy-good lattice approaches $2\pi e$ from below, while that of an AWGN-good lattice approaches $2\pi e$ from above. Recall that the normalized second moment of a quantization-good lattice approaches $1/(2\pi e)$, so all three types of lattices finally share the same VNR threshold $2\pi e$.

Remark 7: In the following, we discuss the implication of Theorem 1 on the smoothing parameter[2] that is commonly used in lattice-based cryptography.

Definition 6 (Smoothing parameter): For a lattice Λ and for $\varepsilon > 0$, the L^∞ and L^1 smoothing parameters $\eta_\varepsilon(\Lambda)$ and $\eta^1_\varepsilon(\Lambda)$, respectively, are the smallest $\sigma > 0$ such that $\epsilon_\Lambda(\sigma), \epsilon^1_\Lambda(\sigma) \leq \varepsilon$.

Theorem 1 implies the existence of lattices whose smoothing parameters $\eta^1_\varepsilon(\Lambda) = \frac{V^{1/n}(\Lambda)}{\sqrt{2\pi e}}$. This improves upon the result $\eta_\varepsilon(\Lambda) = \frac{V^{1/n}(\Lambda)}{\sqrt{2\pi}}$.

From the Cauchy-Schwarz inequality, the following bound was proven in [36][3]

$$\epsilon^1_\Lambda(\sigma) \leq \sqrt{\epsilon_\Lambda\left(\sqrt{2}\sigma\right)} \tag{13}$$

which implies the bound $\eta^1_\varepsilon(\Lambda) \leq \frac{V^{1/n}(\Lambda)}{2\sqrt{\pi}}$. However, this bound is not optimal.

E. Discrete Gaussians and randomized rounding

Given an n-dimensional lattice Λ in $\mathbb{R}^n$ and a vector $\mathbf{c} \in \mathbb{R}^n$, we define the *discrete Gaussian distribution* over Λ centered at $\mathbf{c}$ as the following discrete distribution taking values in $\lambda \in \Lambda$:

$$D_{\Lambda,\sigma,\mathbf{c}}(\lambda) = \frac{f_{\sigma,\mathbf{c}}(\lambda)}{f_{\sigma,\mathbf{c}}(\Lambda)} \quad \forall \lambda \in \Lambda,$$

where $f_{\sigma,\mathbf{c}}(\Lambda) \triangleq \sum_{\lambda\in\Lambda} f_{\sigma,\mathbf{c}}(\lambda)$. We write $D_{\Lambda,\sigma} = D_{\Lambda,\sigma,\mathbf{0}}$.

Extending Peikert [41, Section 4.1], we introduce the notion of randomized rounding:

Definition 7 (Randomized rounding): Given an input vector X^n, we define

$$\lfloor \mathsf{X}^n \rceil_{\Lambda,\sigma} \sim D_{\Lambda,\sigma,\mathsf{X}^n}.$$

It was shown in [41] that when X^n is i.i.d. Gaussian with variance σ^2, the randomly rounded variable $\lfloor \mathsf{X}^n \rceil_{\Lambda,\sigma_Q}$ is close in L^1 distance to the discrete Gaussian $D_{\Lambda,\tilde{\sigma}}$, where $\tilde{\sigma}^2 = \sigma^2 + \sigma_Q^2$, provided that the L^∞ flatness factor $\epsilon_\Lambda(\sigma_Q)$ is small:

Proposition 1 (Adapted from Theorem 3.1 of [41]): Let $\mathsf{X}^n \sim \mathcal{N}(0, \sigma^2 I_n)$ and $\boldsymbol{\mu} \in \mathbb{R}^n$, and consider $\mathsf{X}_Q = \lfloor \mathsf{X}^n + \boldsymbol{\mu} \rceil_{\Lambda,\sigma_Q}$. If $\epsilon_\Lambda(\sigma_Q) < 1/2$, then

$$\mathbb{V}(p_{\mathsf{X}_Q}, D_{\Lambda,\tilde{\sigma},\boldsymbol{\mu}}) \leq 4\epsilon_\Lambda(\sigma_Q),$$

where $\tilde{\sigma}^2 = \sigma^2 + \sigma_Q^2$.

In the following, we prove a partial generalization of this result under an L^1 flatness factor condition, for randomized rounding with uniform dithering, which may be of independent interest.

Theorem 2: Let $\mathsf{X}^n \sim \mathcal{N}(0, \sigma^2 I_n)$, and $\mathsf{U} \sim \mathcal{U}_{\mathcal{R}(\Lambda)}$ uniform over a fundamental region $\mathcal{R}(\Lambda)$ and independent of X^n. Given $\boldsymbol{\mu} \in \mathbb{R}^n$, let $\mathsf{X}_Q = \lfloor \mathsf{X}^n + \mathsf{U} + \boldsymbol{\mu} \rceil_{\Lambda,\sigma_Q}$. Then

$$\mathbb{E}_{\mathsf{U}}\left[\mathbb{V}\left(p_{\mathsf{X}_Q|\mathsf{U}}, D_{\Lambda,\tilde{\sigma},\mathsf{U}+\boldsymbol{\mu}}\right)\right] \leq 2\epsilon^1_\Lambda(\sigma_Q).$$

In order to prove Theorem 2, we need the following Lemma, which will be used several times throughout the paper.

Lemma 5: Under the same hypotheses as in Theorem 2,

$$\sum_{\mathbf{x}_Q\in\Lambda} \int_{\mathcal{R}(\Lambda)} \left| \int_{\mathbb{R}^n} \frac{f_\sigma(\mathbf{x}-\boldsymbol{\mu}) f_{\sigma_Q}(\mathbf{x}_Q - \mathbf{x} - \mathbf{u})}{V(\Lambda) f_{\sigma_Q}(\Lambda - \mathbf{x} - \mathbf{u})} d\mathbf{x} - f_{\tilde{\sigma}}(\mathbf{x}_Q - \mathbf{u} - \boldsymbol{\mu}) \right| d\mathbf{u} \leq \epsilon^1_\Lambda(\sigma_Q).$$

Proof of Lemma 5: By Lemma 1,

$$f_{\sigma_Q}(\mathbf{x}_Q - \mathbf{x} - \mathbf{u}) f_\sigma(\mathbf{x} - \boldsymbol{\mu}) = f_{\tilde{\sigma}}(\mathbf{x}_Q - \mathbf{u} - \boldsymbol{\mu}) f_{\bar{\sigma}}(\mathbf{x} - \bar{\mathbf{c}}(\mathbf{x}_Q, \mathbf{u}, \boldsymbol{\mu})), \tag{14}$$

[2]We remark that this definition differs slightly from the one in [29], where σ is scaled by a constant factor $\sqrt{2\pi}$ (i.e., $s = \sqrt{2\pi}\sigma$).

[3]A similar bound was given in [37] using the statistical distance, which differs from the L^1 distance by a factor $\frac{1}{2}$.

where $\frac{1}{\bar{\sigma}^2} = \frac{1}{\sigma^2} + \frac{1}{\sigma_Q^2}$ and $\bar{\mathbf{c}}(\mathbf{x}_Q, \mathbf{u}, \boldsymbol{\mu}) = \frac{\bar{\sigma}^2}{\sigma_Q^2}(\mathbf{x}_Q - \mathbf{u}) + \frac{\bar{\sigma}^2}{\sigma^2}\boldsymbol{\mu}$. Then we can write

$$\begin{aligned}
&\sum_{\mathbf{x}_Q \in \Lambda} \int_{\mathcal{R}(\Lambda)} \left| \int_{\mathbb{R}^n} \frac{f_\sigma(\mathbf{x}-\boldsymbol{\mu}) f_{\sigma_Q}(\mathbf{x}_Q - \mathbf{x} - \mathbf{u})}{V(\Lambda) f_{\sigma_Q}(\Lambda - \mathbf{x} - \mathbf{u})} d\mathbf{x} - f_{\tilde{\sigma}}(\mathbf{x}_Q - \mathbf{u} - \boldsymbol{\mu}) \right| d\mathbf{u} \\
&\overset{(a)}{=} \sum_{\mathbf{x}_Q \in \Lambda} \int_{\mathcal{R}(\Lambda)} \left| \int_{\mathbb{R}^n} \frac{f_\sigma(\mathbf{x}-\boldsymbol{\mu}) f_{\sigma_Q}(\mathbf{x}_Q - \mathbf{x} - \mathbf{u})}{V(\Lambda) f_{\sigma_Q}(\Lambda - \mathbf{x} - \mathbf{u})} d\mathbf{x} - f_{\tilde{\sigma}}(\mathbf{x}_Q - \mathbf{u} - \boldsymbol{\mu}) \int_{\mathbb{R}^n} f_{\bar{\sigma}}(\mathbf{x} - \bar{\mathbf{c}}(\mathbf{x}_Q, \mathbf{u}, \boldsymbol{\mu})) d\mathbf{x} \right| d\mathbf{u} \\
&\overset{(b)}{=} \sum_{\mathbf{x}_Q \in \Lambda} \int_{\mathcal{R}(\Lambda)} \left| \int_{\mathbb{R}^n} \frac{f_\sigma(\mathbf{x}-\boldsymbol{\mu}) f_{\sigma_Q}(\mathbf{x}_Q - \mathbf{x} - \mathbf{u})}{V(\Lambda) f_{\sigma_Q}(\Lambda - \mathbf{x} - \mathbf{u})} d\mathbf{x} - \int_{\mathbb{R}^n} f_{\sigma_Q}(\mathbf{x}_Q - \mathbf{x} - \mathbf{u}) f_\sigma(\mathbf{x} - \boldsymbol{\mu}) d\mathbf{x} \right| d\mathbf{u} \\
&\leq \int_{\mathcal{R}(\Lambda)} \int_{\mathbb{R}^n} \sum_{\mathbf{x}_Q \in \Lambda} \frac{f_\sigma(\mathbf{x}-\boldsymbol{\mu}) f_{\sigma_Q}(\mathbf{x}_Q - \mathbf{x} - \mathbf{u})}{f_{\sigma_Q}(\Lambda - \mathbf{x} - \mathbf{u})} \left| \frac{1}{V(\Lambda)} - f_{\sigma_Q}(\Lambda - \mathbf{x} - \mathbf{u}) \right| d\mathbf{x} d\mathbf{u} \\
&= \int_{\mathbb{R}^n} f_\sigma(\mathbf{x}-\boldsymbol{\mu}) \int_{\mathcal{R}(\Lambda)} \left| \frac{1}{V(\Lambda)} - f_{\Lambda,\sigma_Q}(\mathbf{x}+\mathbf{u}) \right| d\mathbf{u} d\mathbf{x} \\
&= \int_{\mathbb{R}^n} f_\sigma(\mathbf{x}-\boldsymbol{\mu}) \int_{\mathcal{R}(\Lambda)} \left| \frac{1}{V(\Lambda)} - f_{\Lambda,\sigma_Q}(\mathbf{u}) \right| d\mathbf{u} d\mathbf{x} = \epsilon_\Lambda^1(\sigma_Q),
\end{aligned}$$

where (a) follows from the fact that $\int_{\mathbb{R}^n} f_{\bar{\sigma}}(\mathbf{x} - \bar{\mathbf{c}}(\mathbf{x}_Q, \mathbf{u}, \boldsymbol{\mu}))d\mathbf{x} = 1$, and (b) follows from (14). □

Proof of Theorem 2: We have

$$\begin{aligned}
&\mathbb{E}_{\mathsf{U}} \left[\mathbb{V} \left(p_{\mathsf{X}_Q|\mathsf{U}}, D_{\Lambda,\tilde{\sigma},\mathsf{U}+\boldsymbol{\mu}} \right) \right] = \\
&= \int_{\mathcal{R}(\Lambda)} \frac{1}{V(\Lambda)} \sum_{\mathbf{x}_Q \in \Lambda} \left| p_{\mathsf{X}_Q|\mathsf{U}}(\mathbf{x}_Q|\mathbf{u}) - D_{\Lambda,\tilde{\sigma},\mathbf{u}}(\mathbf{x}_Q) \right| d\mathbf{u} \\
&= \sum_{\mathbf{x}_Q \in \Lambda} \int_{\mathcal{R}(\Lambda)} \frac{1}{V(\Lambda)} \left| \int_{\mathbb{R}^n} \frac{f_\sigma(\mathbf{x}-\boldsymbol{\mu}) f_{\sigma_Q}(\mathbf{x}_Q - \mathbf{x} - \mathbf{u})}{f_{\sigma_Q}(\Lambda - \mathbf{x} - \mathbf{u})} d\mathbf{x} - \frac{f_{\tilde{\sigma}}(\mathbf{x}_Q - \mathbf{u} - \boldsymbol{\mu})}{f_{\tilde{\sigma}}(\Lambda - \mathbf{u} - \boldsymbol{\mu})} \right| d\mathbf{u} \\
&\overset{(a)}{\leq} \sum_{\mathbf{x}_Q \in \Lambda} \int_{\mathcal{R}(\Lambda)} \frac{1}{V(\Lambda)} \left| \int_{\mathbb{R}^n} \frac{f_\sigma(\mathbf{x}-\boldsymbol{\mu}) f_{\sigma_Q}(\mathbf{x}_Q - \mathbf{x} - \mathbf{u})}{f_{\sigma_Q}(\Lambda - \mathbf{x} - \mathbf{u})} d\mathbf{x} - f_{\tilde{\sigma}}(\mathbf{x}_Q - \mathbf{u} - \boldsymbol{\mu}) V(\Lambda) \right| d\mathbf{u} \qquad (15) \\
&+ \sum_{\mathbf{x}_Q \in \Lambda} \int_{\mathcal{R}(\Lambda)} \frac{1}{V(\Lambda)} \left| f_{\tilde{\sigma}}(\mathbf{x}_Q - \mathbf{u} - \boldsymbol{\mu}) V(\Lambda) - \frac{f_{\tilde{\sigma}}(\mathbf{x}_Q - \mathbf{u} - \boldsymbol{\mu})}{f_{\tilde{\sigma}}(\Lambda - \mathbf{u} - \boldsymbol{\mu})} \right| d\mathbf{u}, \qquad (16)
\end{aligned}$$

where (a) follows from the triangle inequality. The term (15) is bounded by $\epsilon_\Lambda^1(\sigma_Q)$ because of Lemma 5. The term (16) is equal to

$$\begin{aligned}
&\sum_{\mathbf{x}_Q \in \Lambda} \int_{\mathcal{R}(\Lambda)} \frac{f_{\tilde{\sigma}}(\mathbf{x}_Q - \mathbf{u} - \boldsymbol{\mu})}{f_{\tilde{\sigma}}(\Lambda - \mathbf{u} - \boldsymbol{\mu})} \left| f_{\tilde{\sigma}}(\Lambda - \mathbf{u} - \boldsymbol{\mu}) - \frac{1}{V(\Lambda)} \right| d\mathbf{u} \\
&= \int_{\mathcal{R}(\Lambda)} \left| f_{\tilde{\sigma}}(\Lambda - \mathbf{u} - \boldsymbol{\mu}) - \frac{1}{V(\Lambda)} \right| d\mathbf{u} = \epsilon_\Lambda^1(\tilde{\sigma}) \overset{(b)}{\leq} \epsilon_\Lambda^1(\sigma_Q),
\end{aligned}$$

where (b) follows from Lemma 4. □

III. Lattice extractor for Gaussian sources

In this section, we present a primitive called lattice extractor to extract the randomness of a source, without dithering.

Consider a source model for secret key generation with public discussion, in the presence of an eavesdropper. For simplicity, we first assume that Alice and Bob observe the same i.i.d. Gaussian random variable $\mathsf{X}^n = \mathsf{Y}^n$ of variance σ_x^2 per dimension. Eve observes a correlated i.i.d. random variable Z^n. We assume that X^n and Z^n are jointly Gaussian, according to the following model

$$\mathsf{X}^n = \mathsf{Z}^n + \mathsf{W}^n, \qquad (17)$$

where W^n is an i.i.d. zero-mean Gaussian random vector of variance σ^2 per dimension, and is independent of Z^n.

Our aim is to extract from X^n a random number that is almost uniform on $\mathcal{R}(\Lambda)$ and almost independent of Z^n. To do this, we apply the mod $\mathcal{R}(\Lambda)$ operation in Eq. (1). Recall that

$$p_{\bar{\mathsf{X}}^n}(\bar{\mathbf{x}}) = f_{\sigma_x,\Lambda}(\bar{\mathbf{x}})\mathbb{1}_{\mathcal{R}(\Lambda)}(\bar{\mathbf{x}}).$$

The conditional density of $\bar{\mathsf{X}}^n = \mathsf{X}^n \bmod \mathcal{R}(\Lambda)$ given Z^n is

$$\begin{aligned} p_{\bar{\mathsf{X}}^n|\mathsf{Z}^n}(\bar{\mathbf{x}}|\mathbf{z}) &= \sum_{\mathbf{x}:\ \bar{\mathbf{x}}=\mathbf{x} \bmod \mathcal{R}(\Lambda)} p_{\mathsf{X}^n|\mathsf{Z}^n}(\mathbf{x}|\mathbf{z}) \\ &= \sum_{\mathbf{x}\in\bar{\mathbf{x}}+\Lambda} p_{\mathsf{X}^n|\mathsf{Z}^n}(\mathbf{x}|\mathbf{z}) = \sum_{\lambda\in\Lambda} \frac{1}{(\sqrt{2\pi}\sigma)^n} e^{-\frac{\|\bar{\mathbf{x}}+\lambda-\mathbf{z}\|^2}{2\sigma^2}} \\ &= f_{\sigma,\Lambda}(\bar{\mathbf{x}}-\mathbf{z})\mathbb{1}_{\mathcal{R}(\Lambda)}(\bar{\mathbf{x}}) = f_{\sigma,\Lambda,\mathbf{z}}(\bar{\mathbf{x}})\mathbb{1}_{\mathcal{R}(\Lambda)}(\bar{\mathbf{x}}). \end{aligned}$$

So, if the flatness factor $\epsilon_\Lambda^{KL}(\sigma) = \mathbb{D}(f_{\sigma,\mathcal{R}(\Lambda)}||\mathcal{U}_{\mathcal{R}(\Lambda)}) = \mathbb{D}(f_{\sigma,\Lambda,\mathbf{z}|\mathcal{R}(\Lambda)}||\mathcal{U}_{\mathcal{R}(\Lambda)})$ is small, $p_{\mathsf{X}^n|\mathsf{Z}^n=\mathbf{z}}$ is almost uniform over $\mathcal{R}(\Lambda)$ for any $\mathbf{z}\in\mathbb{R}^n$. Note that

$$\begin{aligned} &h(\bar{\mathsf{X}}^n) = h(f_{\sigma_x,\Lambda}), \\ &h(\bar{\mathsf{X}}^n|\mathsf{Z}^n=\mathbf{z}) = -\int_{\mathcal{R}(\Lambda)} p_{\bar{\mathsf{X}}^n|\mathsf{Z}^n}(\bar{\mathbf{x}}|\mathbf{z})\log p_{\bar{\mathsf{X}}^n|\mathsf{Z}^n}(\bar{\mathbf{x}}|\mathbf{z})d\bar{\mathbf{x}} = -\int_{\mathcal{R}(\Lambda)} f_{\sigma,\Lambda}(\bar{\mathbf{x}}-\mathbf{z})\log f_{\sigma,\Lambda}(\bar{\mathbf{x}}-\mathbf{z})d\bar{\mathbf{x}} \\ &= -\int_{\mathcal{R}(\Lambda)-\mathbf{z}} f_{\sigma,\Lambda}(\bar{\mathbf{x}})\log f_{\sigma,\Lambda}(\bar{\mathbf{x}})d\bar{\mathbf{x}} = h(f_{\sigma,\Lambda}) \end{aligned}$$

since $f_{\sigma,\Lambda}$ is Λ-periodic and $\mathcal{R}(\Lambda)-\mathbf{z}$ is a fundamental region.

One can now bound the mutual information

$$\begin{aligned} &\mathbb{I}(\bar{\mathsf{X}}^n;\mathsf{Z}^n) = h(\bar{\mathsf{X}}^n) - h(\bar{\mathsf{X}}^n|\mathsf{Z}^n) \\ &= h(f_{\sigma_x,\Lambda}) - \int_{\mathbb{R}^n} p_{\mathsf{Z}^n}(\mathbf{z})h(\bar{\mathsf{X}}^n|\mathsf{Z}^n=\mathbf{z})d\mathbf{z} = h(f_{\sigma_x,\Lambda}) - h(f_{\sigma,\Lambda}) \\ &= \log V(\Lambda) - h(f_{\sigma,\Lambda}) - (\log V(\Lambda) - h(f_{\sigma_x,\Lambda})) = \epsilon_\Lambda^{KL}(\sigma) - \epsilon_\Lambda^{KL}(\sigma_x) \le \epsilon_\Lambda^{KL}(\sigma). \end{aligned}$$

By Theorem 1, if $\gamma_\Lambda(\sigma) < 2\pi e$, there exists a sequence of lattices $\{\Lambda^{(n)}\}$ such that $\lim_{n\to\infty}\mathbb{I}(\bar{\mathsf{X}}^n;\mathsf{Z}^n) = 0$.

Observe that depending on the choice of Λ, the rate of extracted randomness can be arbitrarily large (as expected for the case of continuous random variables).

Remark 8: The asymptotic differential entropy rate of $\bar{\mathsf{X}}^n$ is

$$r = \liminf_{n\to\infty}\frac{1}{n}h(\bar{\mathsf{X}}^n) = \liminf_{n\to\infty}\frac{1}{n}(\log V(\Lambda) - \epsilon_\Lambda^{KL}(\sigma_x)) = \liminf_{n\to\infty}\frac{1}{n}\log V(\Lambda) < \frac{1}{2}\log 2\pi e\sigma^2.$$

since, by monotonicity of the KL flatness factor (Lemma 4), $\epsilon_\Lambda^{KL}(\sigma_x) \le \epsilon_\Lambda^{KL}(\sigma) \to 0$. Taking a sequence of KL secrecy-good lattices, we can obtain the asymptotic rate $r = \log(\sqrt{2\pi e}\sigma)$, which is equal to the asymptotic differential entropy rate of the Gaussian noise W^n. Hence, we have used the mod operation to extract the intrinsic randomness [26]. This improves upon our previous result for continuous lattice extractors [1, Section III] using the L^∞ flatness factor, which was $\frac{1}{2}$ nat from the optimal differential entropy rate.

Remark 9: It is worth mentioning that unlike other works that use dithering or the high-resolution assumption [38], in this section we have obtained uniformity and independence from the flatness factor. Moreover, nearest-neighbor quantization is not needed in our continuous lattice extractor scheme, and we only need to implement the mod $\mathcal{R}(\Lambda)$ operation, which can be performed in polynomial time for many fundamental regions $\mathcal{R}(\Lambda)$. In particular, we can choose the fundamental parallelepiped.

However, in the next section, both dithering and nearest-neighbor quantization will be required for our secret key generation scheme.

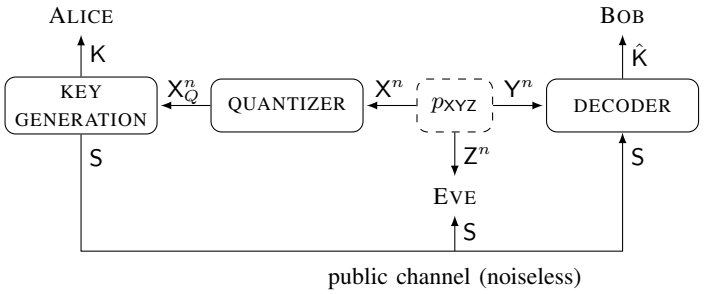

Fig. 1. Secret key generation in the presence of an eavesdropper with communication over a public channel.

IV. SECRET KEY GENERATION

A. System model

We consider the same model as in [1], illustrated in Figure 1, in which Alice, Bob and Eve observe the random variables X^n, Y^n, Z^n respectively, generated by an i.i.d. memoryless Gaussian source p_{XYZ} whose components are jointly Gaussian with zero mean. The distribution is fully described by the variances σ_x^2, σ_y^2, σ_z^2 and the correlation coefficients ρ_{xy}, ρ_{xz}, ρ_{yz}. We can write [23, Eq. (6)]:

$$\begin{cases} \mathsf{X}^n = \rho_{xy}\dfrac{\sigma_x}{\sigma_y}\mathsf{Y}^n + \mathsf{W}_1^n, \\ \mathsf{X}^n = \rho_{xz}\dfrac{\sigma_x}{\sigma_z}\mathsf{Z}^n + \mathsf{W}_2^n, \end{cases} \tag{18}$$

where W_1^n and W_2^n are i.i.d. zero-mean Gaussian noise vectors of variances

$$\sigma_1^2 = \sigma_x^2(1-\rho_{xy}^2), \quad \sigma_2^2 = \sigma_x^2(1-\rho_{xz}^2), \tag{19}$$

respectively. Further, W_1^n is independent of Y^n, and W_2^n is independent of Z^n.

To simplify notation, we define $\hat{\mathsf{Y}}^n = \rho_{xy}\frac{\sigma_x}{\sigma_y}\mathsf{Y}^n$ and $\hat{\mathsf{Z}}^n = \rho_{xz}\frac{\sigma_x}{\sigma_z}\mathsf{Z}^n$, so that

$$\begin{cases} \mathsf{X}^n = \hat{\mathsf{Y}}^n + \mathsf{W}_1^n, \\ \mathsf{X}^n = \hat{\mathsf{Z}}^n + \mathsf{W}_2^n, \end{cases} \tag{20}$$

where $\hat{\mathsf{Y}}^n$ and W_1^n are independent, and $\hat{\mathsf{Z}}^n$ and W_2^n are independent. We denote the variances of $\hat{\mathsf{Y}}^n$ and $\hat{\mathsf{Z}}^n$ by $\hat{\sigma}_y = \rho_{xy}\sigma_x = \sqrt{\sigma_x^2 - \sigma_1^2}$ and $\hat{\sigma}_z = \rho_{xz}\sigma_x = \sqrt{\sigma_x^2 - \sigma_2^2}$ respectively.

The secret key capacity of the Gaussian source model (18) is given by [52, 23]

$$C_s = \frac{1}{2}\log\frac{\sigma_2^2}{\sigma_1^2}.$$

We assume that only one round of one-way public communication (from Alice to Bob) takes place. More precisely, Alice computes a public message S and a secret key K from her observation X^n; she then transmits S over the public channel (see Fig. 1). From this message and his own observation Y^n, Bob reconstructs a key $\hat{\mathsf{K}}$. Let $\mathcal{K}_n$ and $\mathcal{S}_n$ be the sets of secret keys and public messages respectively. A *secret key rate - public rate pair* (R_K, R_P) is achievable if there exists a sequence of protocols with

$$\liminf_{n\to\infty}\frac{1}{n}\log|\mathcal{K}_n| \geq R_K, \quad \limsup_{n\to\infty}\frac{1}{n}\log|\mathcal{S}_n| \leq R_P,$$

such that the following properties hold:

$$\lim_{n\to\infty} \log|\mathcal{K}_n| - \mathbb{H}(\mathsf{K}) = 0 \qquad \text{(uniformity)}$$
$$\lim_{n\to\infty} \mathbb{P}\left\{\mathsf{K} \neq \hat{\mathsf{K}}\right\} = 0 \qquad \text{(reliability)}$$
$$\lim_{n\to\infty} \mathbb{I}(\mathsf{K}; \mathsf{S}, \mathsf{Z}^n) = 0 \qquad \text{(strong secrecy).}$$

To define our key generation scheme, we use the lattice partition chain $\Lambda_1/\Lambda_2/\Lambda_3$, where

- Λ_1 is L^1 secrecy-good with respect to σ_Q, and serves as the "source-code" component of Wyner-Ziv coding;
- Λ_2 is AWGN-good with respect to $\tilde{\sigma}_1 = \sqrt{\sigma_1^2 + \sigma_Q^2}$, and serves as the "channel-code" component in Wyner-Ziv coding;
- Λ_3 is L^1 secrecy-good with respect to $\tilde{\sigma}_2 = \sqrt{\sigma_2^2 + \sigma_Q^2}$, and serves as the extractor of randomness.

The existence of such a chain of lattices will be established in Appendix D.

In addition, we assume that U is a uniform dither over a fundamental region $\mathcal{R}(\Lambda_1)$, which is known by Alice, Bob and Eve[4].

B. Secret key generation protocol

The secret key generation proceeds as follows:

- Alice quantizes X^n to
$$\mathsf{X}_Q = \lfloor \mathsf{X}^n + \mathsf{U} \rceil_{\Lambda_1, \sigma_Q}.$$
That is, $\mathsf{X}_Q \sim D_{\Lambda_1, \sigma_Q, \mathbf{x}+\mathbf{u}}$ if $\mathsf{X}^n = \mathbf{x}$, $\mathsf{U} = \mathbf{u}$, or equivalently
$$p_{\mathsf{X}_Q|\mathsf{X}^n,\mathsf{U}}(\mathbf{x}_Q|\mathbf{x},\mathbf{u}) = \frac{f_{\sigma_Q}(\mathbf{x}_Q - \mathbf{x} - \mathbf{u})}{f_{\sigma_Q}(\Lambda_1 - \mathbf{x} - \mathbf{u})}. \tag{21}$$
Alice then computes the public message S and the key K as follows:
$$\mathsf{S} = \mathsf{X}_Q \bmod \mathcal{V}(\Lambda_2),$$
$$\mathsf{K} = Q_{\Lambda_2}(\mathsf{X}_Q) \bmod \mathcal{R}(\Lambda_3),$$
and transmits S to Bob over the public channel.
- Upon receiving S, Bob reconstructs
$$\hat{\mathsf{X}}_Q = \mathsf{S} + Q_{\Lambda_2}\left(\rho_{xy}\frac{\sigma_x}{\sigma_y}\mathsf{Y}^n + \mathsf{U} - \mathsf{S}\right).$$
He then computes his version of the key:
$$\hat{\mathsf{K}} = Q_{\Lambda_2}(\hat{\mathsf{X}}_Q) \bmod \mathcal{R}(\Lambda_3).$$

Let $\bar{\mathsf{X}}_Q = \mathsf{X}_Q \bmod \mathcal{R}(\Lambda_3) \in \Lambda_1/\Lambda_3$, where the quotient Λ_1/Λ_3 is identified with the set of coset representatives $\Lambda_1 \cap \mathcal{R}(\Lambda_3)$. By definition, $\bar{\mathsf{X}}_Q = \mathsf{S} + \mathsf{K}$. Note that K and S are both functions of $\bar{\mathsf{X}}_Q$:

$$\mathsf{K} = Q_{\Lambda_2}(\mathsf{X}_Q) \bmod \mathcal{R}(\Lambda_3) \overset{(a)}{=} Q_{\Lambda_2}(\mathsf{X}_Q \bmod \mathcal{R}(\Lambda_3)) \bmod \mathcal{R}(\Lambda_3) = Q_{\Lambda_2}(\bar{\mathsf{X}}_Q) \bmod \mathcal{R}(\Lambda_3) = f(\bar{\mathsf{X}}_Q). \tag{22}$$

where (a) follows from equation (3). Similarly,

$$\begin{aligned}\bar{\mathsf{X}}_Q \bmod \Lambda_2 &= \bar{\mathsf{X}}_Q - Q_{\Lambda_2}(\bar{\mathsf{X}}_Q) = \mathsf{X}_Q - Q_{\mathcal{R}(\Lambda_3)}(\mathsf{X}_Q) - Q_{\Lambda_2}(\mathsf{X}_Q - Q_{\mathcal{R}(\Lambda_3)}(\mathsf{X}_Q)) = \mathsf{X}_Q - Q_{\Lambda_2}(\mathsf{X}_Q) \\ &= \mathsf{X}_Q \bmod \Lambda_2 = \mathsf{S} = g(\bar{\mathsf{X}}_Q).\end{aligned} \tag{23}$$

Remark 10: Because of the previous relations, we can conclude that there exists a bijection $(f, g) : \Lambda_1/\Lambda_3 \to \Lambda_1/\Lambda_2 \times \Lambda_2/\Lambda_3$ that sends $\bar{\mathsf{X}}_Q$ into the corresponding pair (S, K).

We now state the main result of the paper, which will be proven in the following sections:

[4]If Alice and Bob already share a secret source of randomness, there is no need for secret key generation. Hence, Eve should know U to avoid trivializing the problem.

Theorem 3: For the Gaussian source model (18), for any secret key rate $R_K < C_s = \frac{1}{2}\log\frac{\sigma_2^2}{\sigma_1^2}$, there exists a sequence of nested lattices $\Lambda_3^{(n)} \subset \Lambda_2^{(n)} \subset \Lambda_1^{(n)}$ such that the previous secret key generation protocol achieves the rate R_K.

C. Reliability

We want to show that the error probability $P_e = \mathbb{P}\{\mathsf{K} \neq \hat{\mathsf{K}}\} \to 0$ as $n \to \infty$.
Note that $\mathsf{K} = \hat{\mathsf{K}}$ if $\hat{\mathsf{X}}_Q = \mathsf{X}_Q$. Since $\mathsf{X}_Q = \mathsf{S} + Q_{\Lambda_2}(\mathsf{X}_Q)$, we have

$$\hat{\mathsf{X}}_Q = \mathsf{X}_Q \;\Leftrightarrow\; Q_{\Lambda_2}(\hat{\mathsf{Y}}^n + \mathsf{U} - \mathsf{S}) = Q_{\Lambda_2}(\mathsf{X}_Q).$$

Observe that

$$Q_{\Lambda_2}(\hat{\mathsf{Y}}^n + \mathsf{U} - \mathsf{S}) = Q_{\Lambda_2}\left(\hat{\mathsf{Y}}^n + \mathsf{U} - \mathsf{X}_Q + Q_{\Lambda_2}(\mathsf{X}_Q)\right) = Q_{\Lambda_2}(\hat{\mathsf{Y}}^n + \mathsf{U} - \mathsf{X}_Q) + Q_{\Lambda_2}(\mathsf{X}_Q).$$

Therefore

$$\hat{\mathsf{X}}_Q = \mathsf{X}_Q \;\Leftrightarrow\; Q_{\Lambda_2}(\hat{\mathsf{Y}}^n + \mathsf{U} - \mathsf{X}_Q) = 0 \;\Leftrightarrow\; \hat{\mathsf{Y}}^n \in \mathsf{X}_Q - \mathsf{U} + \mathcal{V}(\Lambda_2). \tag{24}$$

The error probability is bounded by

$$\begin{aligned}
P_e \leq \mathbb{P}\{\hat{\mathsf{X}}_Q \neq \mathsf{X}_Q\} &= \int_{\mathbb{R}^n}\int_{\mathcal{R}(\Lambda_1)} \mathbb{P}\{\hat{\mathsf{X}}_Q \neq \mathsf{X}_Q \mid \hat{\mathsf{Y}}^n = \mathbf{y}, \mathsf{U} = \mathbf{u}\}\frac{p_{\hat{\mathsf{Y}}^n}(\mathbf{y})}{V(\Lambda_1)}d\mathbf{u}d\mathbf{y} \\
&= \int_{\mathbb{R}^n}\int_{\mathbb{R}^n}\int_{\mathcal{R}(\Lambda_1)} \mathbb{P}\{\hat{\mathsf{X}}_Q \neq \mathsf{X}_Q \mid \hat{\mathsf{Y}}^n = \mathbf{y}, \mathsf{X}^n = \mathbf{x}, \mathsf{U} = \mathbf{u}\}\frac{p_{\mathsf{X}^n|\hat{\mathsf{Y}}^n}(\mathbf{x}|\mathbf{y})p_{\hat{\mathsf{Y}}^n}(\mathbf{y})}{V(\Lambda_1)}d\mathbf{u}d\mathbf{y}d\mathbf{x} \\
&= \sum_{\mathbf{x}_Q\in\Lambda_1}\int_{\mathbb{R}^n}\int_{\mathbb{R}^n}\int_{\mathcal{R}(\Lambda_1)} p_{\mathsf{X}_Q|\mathsf{X}^n\mathsf{U}}(\mathbf{x}_Q|\mathbf{x},\mathbf{u})\mathbb{P}\{\hat{\mathsf{X}}_Q \neq \mathbf{x}_Q \mid \hat{\mathsf{Y}}^n = \mathbf{y}, \mathsf{U} = \mathbf{u}, \mathsf{X}_Q = \mathbf{x}_Q\}\frac{p_{\mathsf{X}^n|\hat{\mathsf{Y}}^n}(\mathbf{x}|\mathbf{y})p_{\hat{\mathsf{Y}}^n}(\mathbf{y})}{V(\Lambda_1)}d\mathbf{u}d\mathbf{y}d\mathbf{x}.
\end{aligned}$$

In the last step we have used the Markov chain $\mathsf{X}^n - (\hat{\mathsf{Y}}^n, \mathsf{X}_Q, \mathsf{U}) - \hat{\mathsf{X}}_Q$. Replacing the expression for the conditional distribution in equation (21), we obtain

$$\begin{aligned}
P_e &= \sum_{\mathbf{x}_Q\in\Lambda_1}\int_{\mathbb{R}^n}\int_{\mathcal{R}(\Lambda_1)}\left(\int_{\mathbb{R}^n}\frac{f_{\sigma_Q}(\mathbf{x}_Q-\mathbf{x}-\mathbf{u})}{f_{\sigma_Q}(\Lambda_1-\mathbf{x}-\mathbf{u})}\frac{f_{\sigma_1}(\mathbf{x}-\mathbf{y})}{V(\Lambda_1)}d\mathbf{x}\right)\mathbb{1}_{\{\mathbf{y}\notin\mathbf{x}_Q-\mathbf{u}+\mathcal{V}(\Lambda_2)\}}f_{\hat{\sigma}_y}(\mathbf{y})d\mathbf{u}\,d\mathbf{y} \\
&\overset{(a)}{\leq} \sum_{\mathbf{x}_Q\in\Lambda_1}\int_{\mathbb{R}^n}\int_{\mathcal{R}(\Lambda_1)}\left|\int_{\mathbb{R}^n}\frac{f_{\sigma_Q}(\mathbf{x}_Q-\mathbf{x}-\mathbf{u})f_{\sigma_1}(\mathbf{x}-\mathbf{y})}{f_{\sigma_Q}(\Lambda_1-\mathbf{x}-\mathbf{u})V(\Lambda_1)}d\mathbf{x} - f_{\tilde{\sigma}_1}(\mathbf{x}_Q-\mathbf{u}-\mathbf{y})\right|\mathbb{1}_{\{\mathbf{y}\notin\mathbf{x}_Q-\mathbf{u}+\mathcal{V}(\Lambda_2)\}}f_{\hat{\sigma}_y}(\mathbf{y})d\mathbf{u}\,d\mathbf{y} \qquad (25) \\
&+ \sum_{\mathbf{x}_Q\in\Lambda_1}\int_{\mathbb{R}^n}\int_{\mathcal{R}(\Lambda_1)} f_{\tilde{\sigma}_1}(\mathbf{x}_Q-\mathbf{u}-\mathbf{y})\mathbb{1}_{\{\mathbf{y}\notin\mathbf{x}_Q-\mathbf{u}+\mathcal{V}(\Lambda_2)\}}f_{\hat{\sigma}_y}(\mathbf{y})d\mathbf{u}\,d\mathbf{y} \qquad (26)
\end{aligned}$$

where (a) follows from the triangle inequality.
The term (25) is upper bounded by

$$\begin{aligned}
&\int_{\mathbb{R}^n}\sum_{\mathbf{x}_Q\in\Lambda_1}\int_{\mathcal{R}(\Lambda_1)}\left|\int_{\mathbb{R}^n}\frac{f_{\sigma_Q}(\mathbf{x}_Q-\mathbf{x}-\mathbf{u})f_{\sigma_1}(\mathbf{x}-\mathbf{y})}{f_{\sigma_Q}(\Lambda_1-\mathbf{x}-\mathbf{u})V(\Lambda_1)}d\mathbf{x} - f_{\tilde{\sigma}_1}(\mathbf{x}_Q-\mathbf{u}-\mathbf{y})\right|d\mathbf{u}f_{\hat{\sigma}_y}(\mathbf{y})d\mathbf{y} \\
&\leq \int_{\mathbb{R}^n}\epsilon^1_{\Lambda_1}(\sigma_Q)f_{\hat{\sigma}_y}(\mathbf{y})d\mathbf{y} = \epsilon^1_{\Lambda_1}(\sigma_Q)
\end{aligned}$$

using Lemma 5. This tends to 0 provided that Λ_1 is L^1 secrecy-good and

$$\frac{V(\Lambda_1)^{2/n}}{\sigma_Q^2} < 2\pi e. \tag{27}$$

With the change of variables $\mathbf{y}' = \mathbf{y} - \mathbf{x}_Q + \mathbf{u}$, the term (26) can be rewritten as

$$\begin{aligned}
&\sum_{\mathbf{x}_Q \in \Lambda_1} \int_{\mathcal{R}(\Lambda_1)} \int_{\mathbb{R}^n} f_{\tilde{\sigma}_1}(\mathbf{y}') \mathbb{1}_{\{\mathbf{y}' \notin \mathcal{V}(\Lambda_2)\}} f_{\hat{\sigma}_y}(\mathbf{y}' + \mathbf{x}_Q - \mathbf{u}) d\mathbf{y}' d\mathbf{u} \\
&= \sum_{\mathbf{x}_Q \in \Lambda_1} \int_{\mathcal{R}(\Lambda_1)} \int_{\mathbb{R}^n \setminus \mathcal{V}(\Lambda_2)} f_{\tilde{\sigma}_1}(\mathbf{y}') f_{\hat{\sigma}_y}(\mathbf{y}' + \mathbf{x}_Q - \mathbf{u}) d\mathbf{y}' d\mathbf{u} \\
&= \int_{\mathbb{R}^n \setminus \mathcal{V}(\Lambda_2)} f_{\tilde{\sigma}_1}(\mathbf{y}') \int_{\mathcal{R}(\Lambda_1)} f_{\hat{\sigma}_y, \Lambda_1}(\mathbf{y}' - \mathbf{u}) d\mathbf{u} d\mathbf{y}' \\
&\overset{(b)}{=} \int_{\mathbb{R}^n \setminus \mathcal{V}(\Lambda_2)} f_{\tilde{\sigma}_1}(\mathbf{y}') d\mathbf{y}'
\end{aligned}$$

where (b) follows from the fact that $\int_{\mathcal{R}(\Lambda_1)} f_{\hat{\sigma}_y, \Lambda_1}(\mathbf{y}' - \mathbf{u}) d\mathbf{u} = 1$. This tends to 0 provided that Λ_2 is AWGN-good and

$$\frac{V(\Lambda_2)^{2/n}}{\tilde{\sigma}_1^2} > 2\pi e. \tag{28}$$

D. Uniformity

We want to show that the key is asymptotically uniform when $n \to \infty$. First, we want to bound the L^1 distance between $p_{\bar{\mathsf{X}}_Q}$ and the uniform distribution over Λ_1/Λ_3. Given $\mathbf{x} \in \mathbb{R}^n, \bar{\mathbf{x}}_Q \in \Lambda_1/\Lambda_3$, we have

$$p_{\bar{\mathsf{X}}_Q|\mathsf{X}^n\mathsf{U}}(\bar{\mathbf{x}}_Q|\mathbf{x}, \mathbf{u}) = \sum_{\lambda_3 \in \Lambda_3} p_{\mathsf{X}_Q|\mathsf{X}^n,\mathsf{U}}(\bar{\mathbf{x}}_Q + \lambda_3|\mathbf{x}, \mathbf{u}) = \sum_{\lambda_3 \in \Lambda_3} \frac{f_{\sigma_Q}(\bar{\mathbf{x}}_Q + \lambda_3 - \mathbf{x} - \mathbf{u})}{f_{\sigma_Q}(\Lambda_1 - \mathbf{x} - \mathbf{u})}. \tag{29}$$

Then

$$p_{\bar{\mathsf{X}}_Q}(\bar{\mathbf{x}}_Q) = \int_{\mathcal{R}(\Lambda_1)} \int_{\mathbb{R}^n} p_{\bar{\mathsf{X}}_Q|\mathsf{X}^n,\mathsf{U}}(\bar{\mathbf{x}}_Q|\mathbf{x}, \mathbf{u}) \frac{p_{\mathsf{X}^n}(\mathbf{x})}{V(\Lambda_1)} d\mathbf{x}\, d\mathbf{u} = \sum_{\lambda_3 \in \Lambda_3} \int_{\mathcal{R}(\Lambda_1)} \int_{\mathbb{R}^n} \frac{f_{\sigma_Q}(\bar{\mathbf{x}}_Q + \lambda_3 - \mathbf{x} - \mathbf{u}) f_{\sigma_x}(\mathbf{x})}{f_{\sigma_Q}(\Lambda_1 - \mathbf{x} - \mathbf{u}) V(\Lambda_1)} d\mathbf{x}\, d\mathbf{u}.$$

Using the previous expression, we find

$$\begin{aligned}
&\left\| p_{\bar{\mathsf{X}}_Q} - \mathcal{U}_{\Lambda_1/\Lambda_2} \right\|_{L^1} = \sum_{\bar{\mathbf{x}}_Q \in \Lambda_1/\Lambda_3} \left| p_{\bar{\mathsf{X}}_Q}(\bar{\mathbf{x}}_Q) - \frac{V(\Lambda_1)}{V(\Lambda_3)} \right| \\
&= \sum_{\bar{\mathbf{x}}_Q \in \Lambda_1/\Lambda_3} \left| \int_{\mathcal{R}(\Lambda_1)} \sum_{\lambda_3 \in \Lambda_3} \int_{\mathbb{R}^n} \frac{f_{\sigma_Q}(\bar{\mathbf{x}}_Q + \lambda_3 - \mathbf{x} - \mathbf{u}) f_{\sigma_x}(\mathbf{x})}{f_{\sigma_Q}(\Lambda_1 - \mathbf{x} - \mathbf{u}) V(\Lambda_1)} d\mathbf{x} d\mathbf{u} - \frac{V(\Lambda_1)}{V(\Lambda_3)} \right| \\
&\overset{(a)}{\leq} \sum_{\bar{\mathbf{x}}_Q \in \Lambda_1/\Lambda_3} \left| \int_{\mathcal{R}(\Lambda_1)} \sum_{\lambda_3 \in \Lambda_3} \int_{\mathbb{R}^n} \frac{f_{\sigma_Q}(\bar{\mathbf{x}}_Q + \lambda_3 - \mathbf{x} - \mathbf{u}) f_{\sigma_x}(\mathbf{x})}{f_{\sigma_Q}(\Lambda_1 - \mathbf{x} - \mathbf{u}) V(\Lambda_1)} d\mathbf{x} d\mathbf{u} - \sum_{\lambda_3 \in \Lambda_3} \int_{\mathcal{R}(\Lambda_1)} f_{\tilde{\sigma}_x}(\bar{\mathbf{x}}_Q + \lambda_3 - \mathbf{u}) d\mathbf{u} \right| \qquad (30) \\
&+ \sum_{\bar{\mathbf{x}}_Q \in \Lambda_1/\Lambda_3} \left| \int_{\mathcal{R}(\Lambda_1)} \sum_{\lambda_3 \in \Lambda_3} f_{\tilde{\sigma}_x}(\bar{\mathbf{x}}_Q + \lambda_3 - \mathbf{u}) d\mathbf{u} - \frac{V(\Lambda_1)}{V(\Lambda_3)} \right| \qquad (31)
\end{aligned}$$

where (a) follows from the triangle inequality, and $\tilde{\sigma}_x^2 = \sigma_x^2 + \sigma_Q^2$. The term (30) is upper bounded by

$$\begin{aligned}
&\sum_{\bar{\mathbf{x}}_Q \in \Lambda_1/\Lambda_3} \sum_{\lambda_3 \in \Lambda_3} \int_{\mathcal{R}(\Lambda_1)} \left| \int_{\mathbb{R}^n} \frac{f_{\sigma_Q}(\bar{\mathbf{x}}_Q + \lambda_3 - \mathbf{x} - \mathbf{u}) f_{\sigma_x}(\mathbf{x})}{f_{\sigma_Q}(\Lambda_1 - \mathbf{x} - \mathbf{u}) V(\Lambda_1)} d\mathbf{x} - f_{\tilde{\sigma}_x}(\bar{\mathbf{x}}_Q + \lambda_3 - \mathbf{u}) \right| d\mathbf{u} \\
&\leq \sum_{\mathbf{x}_Q \in \Lambda_1} \int_{\mathcal{R}(\Lambda_1)} \left| \int_{\mathbb{R}^n} \frac{f_{\sigma_Q}(\mathbf{x}_Q - \mathbf{x} - \mathbf{u}) f_{\sigma_x}(\mathbf{x})}{f_{\sigma_Q}(\Lambda_1 - \mathbf{x} - \mathbf{u}) V(\Lambda_1)} d\mathbf{x} - f_{\tilde{\sigma}_x}(\mathbf{x}_Q - \mathbf{u}) \right| d\mathbf{u} \leq \epsilon_{\Lambda_1}^1(\sigma_Q)
\end{aligned}$$

by Lemma 5. This vanishes as $o\left(\frac{1}{n}\right)$ if Λ_1 is L^1 secrecy-good and the condition (27) is satisfied.
The term (31) is equal to

$$\sum_{\bar{\mathbf{x}}_Q \in \Lambda_1/\Lambda_3} \left| \int_{\mathcal{R}(\Lambda_1)} f_{\tilde{\sigma}_x,\Lambda_3}(\bar{\mathbf{x}}_Q - \mathbf{u}) d\mathbf{u} - \int_{\mathcal{R}(\Lambda_1)} \frac{1}{V(\Lambda_1)} d\mathbf{u} \frac{V(\Lambda_1)}{V(\Lambda_3)} \right|$$
$$\leq \sum_{\bar{\mathbf{x}}_Q \in \Lambda_1/\Lambda_3} \int_{\mathcal{R}(\Lambda_1)} \left| f_{\tilde{\sigma}_x,\Lambda_3}(\bar{\mathbf{x}}_Q - \mathbf{u}) - \frac{1}{V(\Lambda_3)} \right| d\mathbf{u}.$$

Setting $\mathbf{v} = \bar{\mathbf{x}}_Q - \mathbf{u} \bmod \mathcal{R}(\Lambda_3)$, and recalling that $\mathcal{R}(\Lambda_3) = \bigcup_{\bar{\mathbf{x}}_Q \in \Lambda_1 \cap \mathcal{R}(\Lambda_3)} ([\bar{\mathbf{x}}_Q + \mathcal{R}(\Lambda_1)] \bmod \mathcal{R}(\Lambda_3))$ by (4), where the union is disjoint, the last expression is equal to

$$\int_{\mathcal{R}(\Lambda_3)} \left| f_{\tilde{\sigma}_x,\Lambda_3}(\mathbf{v}) - \frac{1}{V(\Lambda_3)} \right| d\mathbf{v} = \epsilon^1_{\Lambda_3}(\tilde{\sigma}_x) \leq \epsilon^1_{\Lambda_3}(\tilde{\sigma}_2)$$

where $\tilde{\sigma}_2^2 = \sigma_2^2 + \sigma_Q^2 \leq \sigma_x^2 + \sigma_Q^2 = \tilde{\sigma}_x^2$. Thus, the term (31) vanishes as $o\left(\frac{1}{n}\right)$ if Λ_3 is L^1-secrecy good and satisfies the volume condition

$$\frac{V(\Lambda_3)^{2/n}}{\tilde{\sigma}_2^2} < 2\pi e. \tag{32}$$

We now show that the distribution of the key is close to the uniform distribution $\mathcal{U}_\mathcal{K}$ over $\mathcal{K} = \Lambda_2/\Lambda_3$:

$$\mathbb{V}(p_\mathsf{K}, \mathcal{U}_\mathcal{K}) = \sum_{k \in \mathcal{K}} \left| p_\mathsf{K}(k) - \frac{V(\Lambda_2)}{V(\Lambda_3)} \right| = \sum_{k \in \mathcal{K}} \left| \sum_{s \in \Lambda_1/\Lambda_2} p_{\bar{\mathsf{X}}_Q}(s \oplus k) - \sum_{s \in \Lambda_1/\Lambda_2} \frac{V(\Lambda_1)}{V(\Lambda_3)} \right|$$
$$\leq \sum_{k \in \mathcal{K}} \sum_{s \in \Lambda_1/\Lambda_2} \left| p_{\bar{\mathsf{X}}_Q}(s \oplus k) - \frac{V(\Lambda_1)}{V(\Lambda_3)} \right|$$
$$= \sum_{\bar{\mathbf{x}}_Q \in \Lambda_1/\Lambda_3} \left| p_{\bar{\mathsf{X}}_Q}(\bar{\mathbf{x}}_Q) - \frac{V(\Lambda_1)}{V(\Lambda_3)} \right| = \mathbb{V}(p_{\bar{\mathsf{X}}_Q}, \mathcal{U}_{\Lambda_1/\Lambda_3})$$

which tends to 0 as shown previously. Using [51, Lemma 2.7], we have that if $\mathbb{V}(p_\mathsf{K}, \mathcal{U}_\mathcal{K}) \leq \frac{1}{2}$,

$$|\mathbb{H}(p_\mathsf{K}) - \mathbb{H}(\mathcal{U}_\mathcal{K})| \leq -\mathbb{V}(p_\mathsf{K}, \mathcal{U}_\mathcal{K}) \log \frac{\mathbb{V}(p_\mathsf{K}, \mathcal{U}_\mathcal{K})}{|\mathcal{K}|} = \mathbb{V}(p_\mathsf{K}, \mathcal{U}_\mathcal{K}) \log \frac{2^{nR_K}}{\mathbb{V}(p_\mathsf{K}, \mathcal{U}_\mathcal{K})}$$
$$= nR_K \mathbb{V}(p_\mathsf{K}, \mathcal{U}_\mathcal{K}) - \mathbb{V}(p_\mathsf{K}, \mathcal{U}_\mathcal{K}) \log \mathbb{V}(p_\mathsf{K}, \mathcal{U}_\mathcal{K}).$$

This vanishes as long as $\mathbb{V}(p_\mathsf{K}, \mathcal{U}_\mathcal{K}) \sim o\left(\frac{1}{n}\right)$, which is indeed the case.

E. Strong secrecy

Using [53, Lemma 1], we can bound the leakage as follows:

$$\mathbb{I}(\mathsf{K}; \mathsf{S}, \mathsf{Z}^n, \mathsf{U}) = \mathbb{I}(\mathsf{K}; \mathsf{S}, \hat{\mathsf{Z}}^n, \mathsf{U}) \leq d_{\text{av}} \log \frac{|\mathcal{K}|}{d_{\text{av}}}, \tag{33}$$

where

$$d_{\text{av}} = \sum_{k \in \mathcal{K}} p_\mathsf{K}(k) \mathbb{V}(p_{\mathsf{S}\hat{\mathsf{Z}}^n\mathsf{U}|\mathsf{K}=k}, p_{\mathsf{S}\hat{\mathsf{Z}}^n\mathsf{U}})$$
$$\leq \sum_{k \in \mathcal{K}} p_\mathsf{K}(k) \sum_{s \in \Lambda_1/\Lambda_2} \int_{\mathcal{R}(\Lambda_1)} \int_{\mathbb{R}^n} \left| p_{\mathsf{S}\hat{\mathsf{Z}}^n\mathsf{U}|\mathsf{K}=k}(s, \mathbf{z}, \mathbf{u}|k) - \frac{p_{\hat{\mathsf{Z}}^n}(\mathbf{z})}{V(\Lambda_2)} \right| d\mathbf{z}\, d\mathbf{u} \tag{34}$$
$$+ \sum_{k \in \mathcal{K}} p_\mathsf{K}(k) \sum_{s \in \Lambda_1/\Lambda_2} \int_{\mathcal{R}(\Lambda_1)} \int_{\mathbb{R}^n} \left| \frac{p_{\hat{\mathsf{Z}}^n}(\mathbf{z})}{V(\Lambda_2)} - p_{\mathsf{S}\hat{\mathsf{Z}}^n\mathsf{U}}(s, \mathbf{z}, \mathbf{u}) \right| d\mathbf{z}\, d\mathbf{u} \tag{35}$$

by the triangle inequality.
Due to Remark 10, we can write

$$p_{\mathsf{S}\hat{\mathsf{Z}}^n\mathsf{U}|\mathsf{K}=k}(s,\mathbf{z},\mathbf{u}|k) = \frac{p_{\mathsf{S}\hat{\mathsf{Z}}^n\mathsf{U}\mathsf{K}}(s,\mathbf{z},\mathbf{u},k)}{p_{\mathsf{K}}(k)} = \frac{p_{\hat{\mathsf{Z}}^n}(\mathbf{z})}{V(\Lambda_1)}\frac{p_{\bar{\mathsf{X}}_Q|\hat{\mathsf{Z}}^n,\mathsf{U}}(k+s|\mathbf{z},\mathbf{u})}{p_{\mathsf{K}}(k)}$$
$$= \frac{p_{\hat{\mathsf{Z}}^n}(\mathbf{z})}{V(\Lambda_1)p_{\mathsf{K}}(k)}\sum_{\lambda_3\in\Lambda_3} p_{\mathsf{X}_Q|\hat{\mathsf{Z}}^n,\mathsf{U}}(k+s+\lambda_3|\mathbf{z},\mathbf{u}),$$

and so the term (34) is equal to

$$\sum_{k\in\mathcal{K}}\sum_{s\in\Lambda_1/\Lambda_2}\int_{\mathcal{R}(\Lambda_1)}\int_{\mathbb{R}^n} p_{\hat{\mathsf{Z}}^n}(\mathbf{z})\left|\sum_{\lambda_3\in\Lambda_3}\frac{p_{\mathsf{X}_Q|\hat{\mathsf{Z}}^n,\mathsf{U}}(k+s+\lambda_3|\mathbf{z},\mathbf{u})}{V(\Lambda_1)} - \frac{p_{\mathsf{K}}(k)}{V(\Lambda_2)}\right| d\mathbf{z}d\mathbf{u}$$
$$\le \sum_{k\in\mathcal{K}}\sum_{s\in\Lambda_1/\Lambda_2}\int_{\mathcal{R}(\Lambda_1)}\int_{\mathbb{R}^n} p_{\hat{\mathsf{Z}}^n}(\mathbf{z})\left|\sum_{\lambda_3\in\Lambda_3}\frac{p_{\mathsf{X}_Q|\hat{\mathsf{Z}}^n,\mathsf{U}}(k+s+\lambda_3|\mathbf{z},\mathbf{u})}{V(\Lambda_1)} - \sum_{\lambda_3\in\Lambda_3} f_{\tilde{\sigma}_2}(k+s+\lambda_3-\mathbf{u}-\mathbf{z})\right| d\mathbf{z}d\mathbf{u} \quad (36)$$
$$+\sum_{k\in\mathcal{K}}\sum_{s\in\Lambda_1/\Lambda_2}\int_{\mathcal{R}(\Lambda_1)}\int_{\mathbb{R}^n} p_{\hat{\mathsf{Z}}^n}(\mathbf{z})\left|\sum_{\lambda_3\in\Lambda_3} f_{\tilde{\sigma}_2}(k+s+\lambda_3-\mathbf{u}-\mathbf{z}) - \frac{p_{\mathsf{K}}(k)}{V(\Lambda_2)}\right| d\mathbf{z}d\mathbf{u}, \quad (37)$$

where $\tilde{\sigma}_2^2 = \sigma_2^2 + \sigma_Q^2$. Recalling that

$$p_{\mathsf{X}_Q|\hat{\mathsf{Z}}^n,\mathsf{U}}(\mathbf{x}_Q|\mathbf{z},\mathbf{u}) = \int_{\mathbb{R}^n} p_{\mathsf{X}_Q|\mathsf{X}^n,\mathsf{U}}(\mathbf{x}_Q|\mathbf{x},\mathbf{u})p_{\mathsf{X}^n|\hat{\mathsf{Z}}^n}(\mathbf{x}|\mathbf{z})d\mathbf{x} = \int_{\mathbb{R}^n}\frac{f_{\sigma_Q}(\mathbf{x}_Q-\mathbf{x}-\mathbf{u})}{f_{\sigma_Q}(\Lambda_1-\mathbf{x}-\mathbf{u})}f_{\sigma_2}(\mathbf{x}-\mathbf{z})d\mathbf{x},$$

the term (36) can be upper bounded by

$$\int_{\mathbb{R}^n} p_{\hat{\mathsf{Z}}^n}(\mathbf{z})\int_{\mathcal{R}(\Lambda_1)}\sum_{k\in\mathcal{K}}\sum_{s\in\Lambda_1/\Lambda_2}\sum_{\lambda_3\in\Lambda_3}\left|\int_{\mathbb{R}^n}\frac{f_{\sigma_Q}(k+s+\lambda_3-\mathbf{x}-\mathbf{u})}{V(\Lambda_1)f_{\sigma_Q}(\Lambda_1-\mathbf{x}-\mathbf{u})}f_{\sigma_2}(\mathbf{x}-\mathbf{z})d\mathbf{x} - f_{\tilde{\sigma}_2}(k+s+\lambda_3-\mathbf{u}-\mathbf{z})\right| d\mathbf{u}\,d\mathbf{z}$$
$$= \int_{\mathbb{R}^n} p_{\hat{\mathsf{Z}}^n}(\mathbf{z})\int_{\mathcal{R}(\Lambda_1)}\sum_{\mathbf{x}_Q\in\Lambda_1}\left|\int_{\mathbb{R}^n}\frac{f_{\sigma_Q}(\mathbf{x}_Q-\mathbf{x}-\mathbf{u})}{V(\Lambda_1)f_{\sigma_Q}(\Lambda_1-\mathbf{x}-\mathbf{u})}f_{\sigma_2}(\mathbf{x}-\mathbf{z})d\mathbf{x} - f_{\tilde{\sigma}_2}(\mathbf{x}_Q-\mathbf{u}-\mathbf{z})\right| d\mathbf{u}\,d\mathbf{z} \le \epsilon^1_{\Lambda_1}(\sigma_Q)$$

by Lemma 5. This vanishes as $o\left(\frac{1}{n}\right)$ assuming the condition (27).
On the other hand, by the triangle inequality the term (37) can be bounded by

$$\sum_{k\in\mathcal{K}}\sum_{s\in\Lambda_1/\Lambda_2}\int_{\mathcal{R}(\Lambda_1)}\int_{\mathbb{R}^n} p_{\hat{\mathsf{Z}}^n}(\mathbf{z})\left|\sum_{\lambda_3\in\Lambda_3} f_{\tilde{\sigma}_2}(k+s+\lambda_3-\mathbf{u}-\mathbf{z}) - \frac{1}{V(\Lambda_3)}\right| d\mathbf{z}d\mathbf{u} \quad (38)$$
$$+\sum_{k\in\mathcal{K}}\sum_{s\in\Lambda_1/\Lambda_2}\int_{\mathcal{R}(\Lambda_1)}\int_{\mathbb{R}^n} p_{\hat{\mathsf{Z}}^n}(\mathbf{z})\left|\frac{1}{V(\Lambda_3)} - \frac{p_{\mathsf{K}}(k)}{V(\Lambda_2)}\right| d\mathbf{z}d\mathbf{u}. \quad (39)$$

Setting $\mathbf{v} = k+s-\mathbf{u} \bmod \mathcal{R}(\Lambda_3)$ and using the property (4), the term (38) can be written as

$$\int_{\mathbb{R}^n} p_{\hat{\mathsf{Z}}^n}(\mathbf{z})\int_{\mathcal{R}(\Lambda_3)}\left|f_{\tilde{\sigma}_2,\Lambda_3}(\mathbf{v}-\mathbf{z}) - \frac{1}{V(\Lambda_3)}\right| d\mathbf{v}d\mathbf{z} = \epsilon^1_{\Lambda_3}(\tilde{\sigma}_2),$$

which vanishes as $o\left(\frac{1}{n}\right)$ assuming the condition (32). Finally, (39) is equal to

$$V(\Lambda_2)\sum_{k\in\mathcal{K}}\left|\frac{1}{V(\Lambda_3)} - \frac{p_{\mathsf{K}}(k)}{V(\Lambda_2)}\right| = \sum_{k\in\mathcal{K}}|\mathcal{U}_{\mathcal{K}} - p_{\mathsf{K}}(k)| = \mathbb{V}(\mathcal{U}_{\mathcal{K}}, p_{\mathsf{K}}) = o\left(\frac{1}{n}\right) \to 0$$

as already shown in Section IV-D.
We now come back to the expression (35), which is equal to

$$\sum_{s\in\Lambda_1/\Lambda_2}\int_{\mathcal{R}(\Lambda_1)}\int_{\mathbb{R}^n}\left|\frac{p_{\hat{\mathsf{Z}}^n}(\mathbf{z})}{V(\Lambda_2)}-p_{\mathsf{S}\hat{\mathsf{Z}}^n\mathsf{U}}(s,\mathbf{z},\mathbf{u})\right|d\mathbf{z}d\mathbf{u}$$

$$\leq\sum_{s\in\Lambda_1/\Lambda_2}\int_{\mathcal{R}(\Lambda_1)}\int_{\mathbb{R}^n}\left|\frac{p_{\hat{\mathsf{Z}}^n}(\mathbf{z})}{V(\Lambda_2)}-\sum_{k'\in\mathcal{K}}\sum_{\lambda_3\in\Lambda_3}p_{\hat{\mathsf{Z}}^n}(\mathbf{z})f_{\tilde{\sigma}_2}(k'+s+\lambda_3-\mathbf{u}-\mathbf{z})\right|d\mathbf{z}d\mathbf{u} \tag{40}$$

$$+\sum_{s\in\Lambda_1/\Lambda_2}\int_{\mathcal{R}(\Lambda_1)}\int_{\mathbb{R}^n}\left|\sum_{k'\in\mathcal{K}}\sum_{\lambda_3\in\Lambda_3}p_{\hat{\mathsf{Z}}^n}(\mathbf{z})f_{\tilde{\sigma}_2}(k'+s+\lambda_3-\mathbf{u}-\mathbf{z})-p_{\mathsf{S}\hat{\mathsf{Z}}^n\mathsf{U}}(s,\mathbf{z},\mathbf{u})\right|d\mathbf{z}d\mathbf{u} \tag{41}$$

by the triangle inequality.
The term (40) is upper bounded by

$$\int_{\mathbb{R}^n}p_{\hat{\mathsf{Z}}^n}(\mathbf{z})\sum_{s\in\Lambda_1/\Lambda_2}\sum_{k'\in\mathcal{K}}\int_{\mathcal{R}(\Lambda_1)}\left|\frac{1}{V(\Lambda_3)}-f_{\tilde{\sigma}_2,\Lambda_3}(k'+s-\mathbf{u}-\mathbf{z})\right|d\mathbf{u}d\mathbf{z}$$

$$=\int p_{\hat{\mathsf{Z}}^n}(\mathbf{z})\int_{\mathcal{R}(\Lambda_3)}\left|\frac{1}{V(\Lambda_3)}-f_{\tilde{\sigma}_2,\Lambda_3}(\mathbf{v}-\mathbf{z})\right|d\mathbf{v}\,d\mathbf{z}=\epsilon^1_{\Lambda_3}(\tilde{\sigma}_2)$$

and vanishes as $o\left(\frac{1}{n}\right)$ if condition (32) is satisfied.
Observe that

$$p_{\mathsf{S}\hat{\mathsf{Z}}^n\mathsf{U}}(s,\mathbf{z},\mathbf{u})=\sum_{k'\in\mathcal{K}}p_{\mathsf{S}\mathsf{K}\hat{\mathsf{Z}}^n\mathsf{U}}(s,k',\mathbf{z},\mathbf{u})=\sum_{k'\in\mathcal{K}}\frac{p_{\hat{\mathsf{Z}}^n}(\mathbf{z})}{V(\Lambda_1)}p_{\bar{\mathsf{X}}_Q|\hat{\mathsf{Z}}^n\mathsf{U}}(s+k'|\mathbf{z},\mathbf{u})$$

$$=\sum_{k'\in\mathcal{K}}\frac{p_{\hat{\mathsf{Z}}^n}(\mathbf{z})}{V(\Lambda_1)}\sum_{\lambda_3\in\Lambda_3}p_{\mathsf{X}_Q|\hat{\mathsf{Z}}^n\mathsf{U}}(s+k'+\lambda_3|\mathbf{z},\mathbf{u})=\sum_{k'\in\mathcal{K}}\frac{p_{\hat{\mathsf{Z}}^n}(\mathbf{z})}{V(\Lambda_1)}\sum_{\lambda_3\in\Lambda_3}\int_{\mathbb{R}^n}\frac{f_{\sigma_Q}(s+k'+\lambda_3-\mathbf{x}-\mathbf{u})f_{\sigma_2}(\mathbf{x}-\mathbf{z})}{f_{\sigma_Q}(\Lambda_1-\mathbf{x}-\mathbf{u})}d\mathbf{x}.$$

Thus the term (41) can be bounded by

$$\int_{\mathbb{R}^n}p_{\hat{\mathsf{Z}}^n}(\mathbf{z})\int_{\mathcal{R}(\Lambda_1)}\sum_{k'\in\mathcal{K}}\sum_{s\in\Lambda_1/\Lambda_2}\sum_{\lambda_3\in\Lambda_3}\left|f_{\tilde{\sigma}_2}(k'+s+\lambda_3-\mathbf{u}-\mathbf{z})-\int_{\mathbb{R}^n}\frac{f_{\sigma_Q}(s+k'+\lambda_3-\mathbf{x}-\mathbf{u})f_{\sigma_2}(\mathbf{x}-\mathbf{z})}{V(\Lambda_1)f_{\sigma_Q}(\Lambda_1-\mathbf{x}-\mathbf{u})}d\mathbf{x}\right|d\mathbf{u}\,d\mathbf{z}$$

$$=\int_{\mathbb{R}^n}p_{\hat{\mathsf{Z}}^n}(\mathbf{z})\int_{\mathcal{R}(\Lambda_1)}\sum_{\mathbf{x}_Q\in\Lambda_1}\left|f_{\tilde{\sigma}_2}(\mathbf{x}_Q-\mathbf{u}-\mathbf{z})-\int_{\mathbb{R}^n}\frac{f_{\sigma_Q}(\mathbf{x}_Q-\mathbf{x}-\mathbf{u})f_{\sigma_2}(\mathbf{x}-\mathbf{z})}{V(\Lambda_1)f_{\sigma_Q}(\Lambda_1-\mathbf{x}-\mathbf{u})}d\mathbf{x}\right|d\mathbf{u}d\mathbf{z}\leq\epsilon^1_{\Lambda_1}(\sigma_Q)$$

by Lemma 5, which again vanishes as $o\left(\frac{1}{n}\right)$ under condition (27).
In conclusion, $d_{\text{av}}\sim o\left(\frac{1}{n}\right)$ and thus from (33), we find that the leakage vanishes asymptotically as $n\to\infty$.

Remark 11: Although in Section IV-D we only showed that the key is close to uniform on average over the dither U, using the results in this section we see that

$$\mathbb{H}(\mathcal{U}_{\mathcal{K}})-\mathbb{H}(\mathsf{K}|\mathsf{U})=\mathbb{H}(\mathcal{U}_{\mathcal{K}})-\mathbb{H}(\mathsf{K})+\mathbb{I}(\mathsf{K};\mathsf{U})\leq\mathbb{H}(\mathcal{U}_{\mathcal{K}})-\mathbb{H}(\mathsf{K})+\mathbb{I}(\mathsf{K};\mathsf{S},\mathsf{Z}^n,\mathsf{U})\to 0.$$

F. Achievable strong secrecy rate and optimal trade-off

Recall that in the previous sections we have imposed the conditions (27), (28) and (32) on the volumes of Λ_1, Λ_2 and Λ_3 respectively, i.e.

$$\frac{V(\Lambda_1)^{2/n}}{\sigma_Q^2}<2\pi e,\quad\frac{V(\Lambda_2)^{2/n}}{\tilde{\sigma}_1^2}>2\pi e,\quad\frac{V(\Lambda_3)^{2/n}}{\tilde{\sigma}_2^2}<2\pi e.$$

Therefore, the achievable secret key rate is upper bounded by

$$R_K=\frac{1}{n}\log\frac{V(\Lambda_3)}{V(\Lambda_2)}<\frac{1}{2}\log\frac{\tilde{\sigma}_2^2}{\tilde{\sigma}_1^2}=\frac{1}{2}\log\frac{\sigma_2^2+\sigma_Q^2}{\sigma_1^2+\sigma_Q^2} \tag{42}$$

As $\sigma_Q \to 0$,

$$R_K \to \frac{1}{2}\log\frac{\sigma_2^2}{\sigma_1^2},$$

which is the optimal secret key rate. This improves upon our previous work [1] in which the achievable secrecy rate had a $1/2$ nat gap compared to the optimal.

Remark 12: The optimal scaling of the lattice Λ_3 requires the noise variance σ_2 to be known by Alice; if only a lower bound for σ_2 is available, positive secret key rates can still be attained.

The public communication rate is lower bounded by

$$R_P = \frac{1}{n}\log\frac{V(\Lambda_2)}{V(\Lambda_1)} > \frac{1}{2}\log\frac{\sigma_1^2+\sigma_Q^2}{\sigma_Q^2}.$$

Equivalently, we have $\sigma_Q^2 > \frac{\sigma_1^2}{e^{2R_P}-1}$. Replacing this expression in the bound (42) for R_K, and observing that (42) is a decreasing function of σ_Q^2, we find

$$R_K < \frac{1}{2}\log\left(e^{-2R_P} + \frac{\sigma_2^2}{\sigma_1^2}(1-e^{-2R_P})\right).$$

which corresponds to the optimal public rate / secret key rate tradeoff [23] (see Appendix E for details.)

V. Conclusions and perspectives

To conclude, we have proposed a lattice extractor to extract a secret key from correlated Gaussian sources against an eavesdropper. Using L^1 distance and KL divergence, we have proved the existence of lattices with a vanishing flatness factor for all VNRs up to $2\pi e$. This improves upon the previous result for VNRs up to 2π, based on L^∞ distance. Together with dithering and randomized rounding, it has enabled us to achieve the optimal trade-off with one-way public communication. In the same way, it may be possible to remove the $\frac{1}{2}$-nat gap, associated to the L^∞ flatness factor, to the secrecy capacity of wiretap channels [31].

An immediate step for future work is to turn the existence result of this paper into a practical scheme. For example, one may instantiate the lattices using polar codes. Another problem is to see if it is possible to modify the design of this paper to yield a fuzzy extractor, which would require redesigning a lattice with respect to other entropy measures. Other open problems include identifying whether is is possible to remove dithering and/or randomized quantization, characterizing the second-order asymptotics and the extension of the proposed key-agreement protocol to multi-terminal systems. Furthermore, the reconciliation technique based on Wyner-Ziv coding may be extended to key-encapsulation mechanisms (KEM) in lattice-based cryptography, due to the similarity between KEM and secret key agreement. Finally, it is interesting to explore the applications of L^1 and KL smoothing parameters in other cryptographic and mathematical problems [33, 34].

Acknowledgment

The second author would like to thank Antonio Campello, Daniel Dadush and Ling Liu for helpful discussions.

Appendix A
Proof of Lemma 3

By definition,

$$\begin{aligned}
&\mathbb{D}\left(f_{\sigma,\mathcal{R}(\Lambda')}\middle\|\frac{1}{|\Lambda/\Lambda'|}f_{\sigma,\Lambda|\mathcal{R}(\Lambda')}\right) = \int_{\mathcal{R}(\Lambda')} f_{\sigma,\Lambda'}(\mathbf{y})\log\frac{f_{\sigma,\Lambda'}(\mathbf{y})\,|\Lambda/\Lambda'|}{f_{\sigma,\Lambda}(\mathbf{y})}d\mathbf{y}\\
&= -h(f_{\sigma,\Lambda'}) + \int_{\mathcal{R}(\Lambda')} f_{\sigma,\Lambda'}(\mathbf{y})\log\frac{|\Lambda/\Lambda'|}{f_{\sigma,\Lambda}(\mathbf{y})}d\mathbf{y}\\
&= -h(f_{\sigma,\Lambda'}) + \log\left|\Lambda/\Lambda'\right| - \int_{\mathcal{R}(\Lambda')} f_{\sigma,\Lambda'}(\mathbf{y})\log f_{\sigma,\Lambda}(\mathbf{y})d\mathbf{y}.
\end{aligned}$$

The conclusion follows by observing that

$$-\int_{\mathcal{R}(\Lambda')} f_{\sigma,\Lambda'}(\mathbf{y})\log f_{\sigma,\Lambda}(\mathbf{y})d\mathbf{y} = -\sum_{\lambda\in\Lambda/\Lambda'}\int_{\mathcal{R}(\Lambda)+\lambda} f_{\sigma,\Lambda'}(\mathbf{y})\log f_{\sigma,\Lambda}(\mathbf{y})d\mathbf{y}$$

$$= -\sum_{\lambda\in\Lambda/\Lambda'}\int_{\mathcal{R}(\Lambda)} f_{\sigma,\Lambda'}(\mathbf{y}-\lambda)\log f_{\sigma,\Lambda}(\mathbf{y})d\mathbf{y} = -\int_{\mathcal{R}(\Lambda)} f_{\sigma,\Lambda}(\mathbf{y})\log f_{\sigma,\Lambda}(\mathbf{y})d\mathbf{y} = h(f_{\sigma,\Lambda}). \qquad \square$$

APPENDIX B
RESOLVABILITY CODES

In this section we review some results from [32] about resolvability codes for regular channels, which are needed for the proof of Theorem 1.

First, we need some preliminary definitions. In the following, we assume $\mathcal{X}$ is a finite abelian group and $\mathcal{Y}$ is a measurable space. Given a channel $W:\mathcal{X}\to\mathcal{Y}$, we use the notation $W_x(y)=W(y|x)$ for $x\in\mathcal{X}, y\in\mathcal{Y}$.

Definition 8 (Rényi Entropy): Given a discrete distribution p_{A} on $\mathcal{A}$ and $\rho\geq 0$, we define

$$H_{1+\rho}(\mathsf{A}) = -\frac{1}{\rho}\log\sum_{a\in\mathcal{A}} p_{\mathsf{A}}(a)^{1+\rho}.$$

Definition 9: Given a channel $W:\mathcal{X}\to\mathcal{Y}$ and a probability distribution p_{X} on $\mathcal{X}$, we define $\forall\rho\geq 0$

$$\psi(\rho|W,p_{\mathsf{X}}) = \log\sum_{x\in\mathcal{X}} p_{\mathsf{X}}(x)\int_{\mathcal{Y}} W_x(y)^{1+\rho}(W\circ p_X)(y)^{-\rho}dy.$$

This function has the following properties:

$$\psi(0|W,p_{\mathsf{X}}) = 0, \tag{43}$$

$$\psi(\rho|W^n,p_{\mathsf{X}}^{\otimes n}) = n\psi(\rho|W,p_{\mathsf{X}}), \tag{44}$$

$$\lim_{\rho\to 0}\frac{\psi(\rho|W,p_{\mathsf{X}})}{\rho} = \mathbb{I}(\mathsf{X};\mathsf{Y}). \tag{45}$$

We also compute the second derivative in 0 which will be needed in the next section.

Lemma 6:

$$\psi''(0) = \sum_{x\in\mathcal{X}} p_{\mathsf{X}}(x)\int_{\mathcal{Y}} W_x(y)\left(\log\frac{W_x(y)}{(W\circ p_{\mathsf{X}}(y))}\right)^2 dy - \left(\sum_{x\in\mathcal{X}} p_{\mathsf{X}}(x)\int_{\mathcal{Y}} W_x(y)\log\frac{W_x(y)}{(W\circ p_{\mathsf{X}})(y)}dy\right)^2.$$

The proof of Lemma 6 can be found in Appendix F.

Definition 10 (Regular channel): The channel $W:\mathcal{X}\to\mathcal{Y}$ is called *regular* if $\mathcal{X}$ acts on $\mathcal{Y}$ by permutations $\{\pi_x\}_{x\in\mathcal{X}}$ such that $\pi_x(\pi'_x(y)) = \pi_{x+x'}(y)\ \forall x,x'\in\mathcal{X}$, and there exists a probability density p_{Y} on $\mathcal{Y}$ such that $W_x(y) = p_{\mathsf{Y}}(\pi_x(y))\ \forall x\in\mathcal{X}, \forall y\in\mathcal{Y}$.

In particular, a regular channel is symmetric [49, 54] in the sense of Gallager [55], and its capacity is achieved by the uniform distribution.

The following theorem was stated for discrete memoryless channels [32, Corollary 18] but can be extended to continuous outputs [32, Appendix D] as follows:

Theorem 4: Let $\mathcal{M}$ and $\mathcal{X}$ be a finite-dimensional vector spaces over $\mathbb{F}_p$ and $\mathcal{Y}$ a measurable space. Consider a uniform random variable F taking values over the set of linear mappings $f:\mathcal{M}\to\mathcal{X}$ and a distribution p_{M} on $\mathcal{M}$. If $W:\mathcal{X}\to\mathcal{Y}$ is regular, then $\forall\rho>0$,

$$\mathbb{E}_{\mathsf{F}}\left[e^{\rho\mathbb{D}(W\circ\mathsf{F}\circ p_{\mathsf{M}}||W\circ\mathcal{U}_{\mathcal{X}})}\right] \leq 1 + e^{-\rho H_{1+\rho}(\mathsf{M})}e^{\psi(\rho|W,\mathcal{U}_{\mathcal{X}})}.$$

Theorem 4 is a one-shot result, but we can apply it to n uses of an i.i.d. channel to get the following.

Corollary 1: Let $\mathcal{X}$ be a finite-dimensional vector space over $\mathbb{F}_p$ and $\mathcal{Y}$ a measurable space, and $W:\mathcal{X}\to\mathcal{Y}$ a regular channel. Let $R>\mathbb{I}(\mathsf{X};\mathsf{Y})$, where $\mathsf{X}\sim\mathcal{U}_{\mathcal{X}}$ and $\mathsf{Y}\sim W\circ\mathcal{U}_{\mathcal{X}}$. Consider $\mathsf{C}_n\subset\mathcal{X}^n$ chosen uniformly at random in the set of (n,k) linear codes in $\mathcal{X}^n$, where $k=\frac{\lceil nR\rceil}{\log p}$. Denote by $\mathcal{U}_{\mathsf{C}_n}$ the uniform distribution over the codewords in C_n. Then

$$\mathbb{E}_{\mathsf{C}_n}[\mathbb{D}(W^n\circ\mathcal{U}_{\mathsf{C}_n}||W^n\circ\mathcal{U}_{\mathcal{X}}^{\otimes n})]\to 0$$

exponentially fast as $n \to \infty$.

Proof: Note that $W^n : \mathcal{X}^n \to \mathcal{Y}^n$ is still a regular channel with respect to the set of permutations $\{\pi_{\mathbf{x}}\}_{\mathbf{x}\in\mathcal{X}^n}$, where we define $\pi_{\mathbf{x}}(y_1,\dots,y_n) = (\pi_{x_1}(y_1),\dots,\pi_{x_n}(y_n))$ for $\mathbf{x} = (x_1,\dots,x_n)$.
Applying Theorem 4 to this channel, and taking $\mathcal{M} = \mathbb{F}_p^k$ with $k = \frac{\lceil nR\rceil}{\log p}$ and $p_{\mathsf{M}} = \mathcal{U}_{\mathcal{M}}$, for F_n representing a random linear encoder $f_n : \mathcal{M} \to \mathcal{X}^n$ we have

$$\mathbb{E}_{\mathsf{F}_n}\left[e^{\rho\mathbb{D}(W^n\circ\mathsf{F}_n\circ\mathcal{U}_{\mathcal{M}}||W^n\circ\mathcal{U}_{\mathcal{X}}^{\otimes n})}\right] \le 1 + e^{-\rho H_{1+\rho}(\mathsf{M})}e^{\psi(\rho|W^n,\mathcal{U}_{\mathcal{X}}^{\otimes n})}.$$

By Jensen's inequality,

$$\mathbb{E}_{\mathsf{F}_n}[\mathbb{D}(W^n\circ\mathsf{F}_n\circ\mathcal{U}_{\mathcal{M}}||W^n\circ\mathcal{U}_{\mathcal{X}}^{\otimes n})] \le \frac{1}{\rho}\log\left(1 + e^{-\rho H_{1+\rho}(\mathsf{M})}e^{\psi(\rho|W^n,\mathcal{U}_{\mathcal{X}}^{\otimes n})}\right) \le \frac{1}{\rho}e^{-\rho H_{1+\rho}(\mathsf{M})+\psi(\rho|W^n,\mathcal{U}_{\mathcal{X}}^{\otimes n})}.$$

Note that $H_{1+\rho}(\mathsf{M}) = nR$ since M is uniform. Using (44), we find that $\forall\rho > 0$,

$$\mathbb{E}_{\mathsf{F}_n}[\mathbb{D}(W^n\circ\mathsf{F}_n\circ\mathcal{U}_{\mathcal{M}}||W^n\circ\mathcal{U}_{\mathcal{X}}^{\otimes n})] \le \frac{1}{\rho}e^{-n(\rho R-\psi(\rho|W,\mathcal{U}_{\mathcal{X}}))}. \tag{46}$$

From (43) and (45), we have $\psi(\rho|W,p_{\mathsf{X}}) = \rho\mathbb{I}(\mathsf{X};\mathsf{Y}) + \eta(\rho)$, where $\lim_{\rho\to 0}\frac{\eta(\rho)}{\rho} = 0$. Given $R > \mathbb{I}(\mathsf{X};\mathsf{Y})$, $\exists\bar{\rho}$ sufficiently small such that $\delta = R - \mathbb{I}(\mathsf{X};\mathsf{Y}) - \frac{\eta(\bar{\rho})}{\bar{\rho}} > 0$. Therefore

$$\mathbb{E}_{\mathsf{F}_n}[\mathbb{D}(W^n\circ\mathsf{F}_n\circ\mathcal{U}_{\mathcal{M}}||W^n\circ\mathcal{U}_{\mathcal{X}}^{\otimes n})] \le \frac{1}{\bar{\rho}}e^{-n\bar{\rho}\delta} \to 0 \tag{47}$$

as $n \to \infty$.

Appendix C
Proof of Theorem 1

For a given dimension n, we will construct Λ as a scaled mod-p lattice [56] of the form $\Lambda = \alpha(p\mathbb{Z}^n + \mathcal{C}_n)$, where $\mathcal{C}_n$ is an (n,k)-linear code over $\mathbb{F}_p$.

We will consider the asymptotic behavior as $n \to \infty$, $\alpha \to 0, p \to \infty$ while satisfying the volume condition $\alpha^n p^{n-k} = V(\Lambda) = (\gamma\sigma^2)^{n/2}$. Here, γ is the volume-to-noise ratio, which is assumed to be fixed.

By construction, $\Lambda_c^n \subset \Lambda \subset \Lambda_f^n$, where $\Lambda_c = \alpha p\mathbb{Z}$ and $\Lambda_f = \alpha\mathbb{Z}$ are one-dimensional lattices.

From Remark 5 and the relation (10), we have

$$\mathbb{D}(f_{\sigma,\mathcal{R}(\Lambda)}||\mathcal{U}_{\mathcal{R}(\Lambda)}) = C(\Lambda,\sigma^2) = C(\Lambda_f^n,\sigma^2) + C(\Lambda_f^n/\Lambda,\sigma^2).$$

We want to show that both terms in the sum tend to zero when $n \to \infty$.

1) First, we will show that $C(\Lambda_f^n,\sigma^2) = C((\alpha\mathbb{Z})^n,\sigma^2) \to 0$ if $\alpha = o\left(\frac{1}{n^c}\right)$ for some $c > 0$. We follow the same approach as in [50, Appendix A]. From Lemma 2 we have that $C(\Lambda_f^n,\sigma^2) \le \epsilon_{\Lambda_f^n}(\sigma)$. Furthermore, it was shown in [57, Lemma 3] that
$$\epsilon_{\Lambda_f^n}(\sigma) = (1 + \epsilon_{\Lambda_f}(\sigma))^n - 1. \tag{48}$$
Finally, one can show that [50, Appendix A]
$$\epsilon_{\Lambda_f}(\sigma) = \epsilon_{\alpha\mathbb{Z}}(\sigma) \le 4e^{-\frac{2\pi^2\sigma^2}{\alpha^2}}. \tag{49}$$
Then
$$\epsilon_{\Lambda_f^n}(\sigma) \le \left(1 + 4e^{-\frac{2\pi^2\sigma^2}{\alpha^2}}\right)^n - 1 \le 4ne^{-\frac{2\pi^2\sigma^2}{\alpha^2}} + o(e^{-\frac{2\pi^2\sigma^2}{\alpha^2}}) \to 0.$$
since $(1+x)^n = 1 + nx + o(x)$ when $x \to 0$.
2) Next, we want to show that there exists a sequence of lattices Λ of the form $\alpha(p\mathbb{Z}^n + \mathcal{C}_n)$ such that $C(\Lambda_f^n/\Lambda,\sigma^2) \to 0$ as $n \to \infty$.
Consider the mod-(Λ_f/Λ_c) channel $W : \Lambda_f \cap \mathcal{R}(\Lambda_c) \to \mathcal{R}(\Lambda_c)$. This channel is regular (see Definition 10 in Appendix B) with respect to the set of permutations $\pi_x(y) = [y-x] \mod \Lambda_c$ for $x \in \mathcal{X} = \Lambda_f \cap \mathcal{R}(\Lambda_c)$, $y \in \mathcal{R}(\Lambda_c)$. In fact,
$$W_x(y) = W(y|x) = f_{\sigma,\Lambda_c}(y-x) = f_{\sigma,\Lambda_c}([y-x] \bmod \Lambda_c) = f_{\sigma,\Lambda_c}(\pi_x(y)).$$

Being regular, the mod Λ_f/Λ_c channel is symmetric and the uniform distribution over $\mathcal{X}$ achieves capacity (see Appendix B). Moreover, $\Lambda_f/\Lambda_c \cong \mathbb{F}_p$. We consider the required rate condition in Corollary 1:

$$R = \frac{1}{n}\log|\mathcal{C}_n| = \frac{1}{n}\log|\Lambda/\Lambda_c^n| = \frac{1}{n}\log\frac{\alpha^n p^n}{V(\Lambda)} > \mathbb{I}(\mathsf{X};\mathsf{Y}) = C(\Lambda_f/\Lambda_c,\sigma^2). \tag{50}$$

We have

$$\begin{aligned} &C(\Lambda_f/\Lambda_c,\sigma^2) = \log|\Lambda_f/\Lambda_c| + h(f_{\sigma,\Lambda_f}) - h(f_{\sigma,\Lambda_c}) = \log p + h(f_{\sigma,\Lambda_f}) - h(f_{\sigma,\Lambda_c}) \\ &= \log p + \log\alpha - C(\Lambda_f,\sigma^2) - h(f_{\sigma,\Lambda_c}). \end{aligned}$$

Therefore, the condition (50) is equivalent to

$$\frac{1}{n}\log V(\Lambda) < h(f_{\sigma,\Lambda_c}) + C(\Lambda_f,\sigma^2).$$

In the asymptotic limit for $\alpha \to 0$, $p \to \infty$ while keeping $\alpha^n p^{n-k} = V(\Lambda) = (\gamma\sigma^2)^{n/2}$, we have $C(\Lambda_f,\sigma^2) \to 0$. Moreover, $\alpha p \to \infty$, and so $h(\Lambda_c,\sigma^2) \to \frac{1}{2}\log 2\pi e\sigma^2$. So asymptotically, the rate condition is satisfied when

$$\frac{V(\Lambda)^{2/n}}{2\pi e\sigma^2} < 1. \tag{51}$$

In this case we have

$$R - \mathbb{I}(\mathsf{X};\mathsf{Y}) = -\frac{1}{n}\log V(\Lambda) + C(\Lambda_f,\sigma^2) - h(f_{\sigma,\Lambda_c}) \to \delta_0 = \frac{1}{2}\log\frac{2\pi e\sigma^2}{V(\Lambda)^{2/n}} = \frac{1}{2}\log\frac{2\pi e}{\gamma_\Lambda(\sigma)} > 0 \tag{52}$$

as $n \to \infty$.

Remark 13: Note that we cannot directly apply Corollary 1 in Appendix B to this setting, since the definition of the channel W depends on α and p which are not fixed but are a function of n. However, we will show that the proof of the Corollary can be extended to this channel since the convergence in (47) is uniform.

Proof of Remark 13: Let X be a uniformly distributed variable on $\Lambda_f \cap \mathcal{R}(\Lambda_c)$ and Y the corresponding output distribution. Consider the function $\psi(\rho) = \psi(\rho|W,\mathcal{U}_\mathcal{X})$ in Definition 9. From (43) and (45), it follows that its Taylor expansion in 0 is given by

$$\psi(\rho) = \rho\mathbb{I}(\mathsf{X};\mathsf{Y}) + \rho^2\psi''(0) + o(\rho^2), \tag{53}$$

where $\psi''(0)$ is given in Lemma 6. Noting that

$$(W\circ\mathcal{U}_\mathcal{X})(y) = \sum_{x\in\mathcal{X}}\frac{1}{|\mathcal{X}|}W_x(y) = \sum_{x\in\Lambda_f\cap\mathcal{R}(\Lambda_c)}\frac{1}{|\Lambda_f/\Lambda_c|}f_{\sigma,\Lambda_c}(y-x) = \frac{1}{|\Lambda_f/\Lambda_c|}f_{\sigma,\Lambda_f(y)},$$

we find

$$\begin{aligned} \psi''(0) &= \sum_{x\in\Lambda_f\cap\mathcal{R}(\Lambda_c)}\frac{1}{|\Lambda_f/\Lambda_c|}\int_{\mathcal{R}(\Lambda_c)} f_{\sigma,\Lambda_c}(y-x)\left(\log\frac{f_{\sigma,\Lambda_c}(y-x)}{\frac{1}{|\Lambda_f/\Lambda_c|}f_{\sigma,\Lambda_f}(y)}\right)^2 dy \\ &- \left(\sum_{x\in\Lambda_f\cap\mathcal{R}(\Lambda_c)}\frac{1}{|\Lambda_f/\Lambda_c|}\int_{\mathcal{R}(\Lambda_c)} f_{\sigma,\Lambda_c}(y-x)\log\frac{f_{\sigma,\Lambda_c}(y-x)}{\frac{1}{|\Lambda_f/\Lambda_c|}f_{\sigma,\Lambda_f}(y)}dy\right)^2 \\ &\le \sum_{x\in\Lambda_f\cap\mathcal{R}(\Lambda_c)}\frac{1}{|\Lambda_f/\Lambda_c|}\int_{\mathcal{R}(\Lambda_c)} f_{\sigma,\Lambda_c}(y-x)\left(\log\frac{f_{\sigma,\Lambda_c}(y-x)}{\frac{1}{|\Lambda_f/\Lambda_c|}f_{\sigma,\Lambda_f}(y)}\right)^2 dy \\ &= \int_{\mathcal{R}(\Lambda_c)} f_{\sigma,\Lambda_c}(y')\left(\log\frac{f_{\sigma,\Lambda_c}(y')}{\frac{1}{|\Lambda_f/\Lambda_c|}f_{\sigma,\Lambda_f}(y')}\right)^2 dy' \end{aligned}$$

with the change of variables $y' = y - x \bmod \mathcal{R}(\Lambda_c)$. From the definition of flatness factor and the bound (49),

we find that $\forall y' \in \mathcal{R}(\Lambda_c)$,

$$f_{\sigma,\Lambda_f}(y') \geq \frac{1-\epsilon_{\Lambda_f}(\sigma)}{V(\Lambda_f)} \geq \frac{1-4e^{-\frac{2\pi^2\sigma^2}{\alpha^2}}}{\alpha}.$$

Recalling the definition of the theta series of a lattice in (6) and the relation (8), we have $\epsilon_\Lambda(\sigma) = \Theta_{\Lambda^*}(2\pi\sigma^2) - 1$, where Λ^* is the dual lattice of Λ. Then by [31, Remark 1], $\forall y' \in \mathcal{V}(\Lambda_c)$

$$f_{\sigma,\Lambda_c}(y') \leq f_{\sigma,\Lambda_c}(0) = \frac{1}{\sqrt{2\pi}\sigma}\Theta_{\Lambda_c}\left(\frac{1}{2\pi\sigma^2}\right) = \frac{1}{\sqrt{2\pi}\sigma}\left(1+\epsilon_{\Lambda_c^*}\left(\frac{1}{2\pi\sigma}\right)\right).$$

Again using the bound (49), we have

$$\epsilon_{\Lambda_c^*}\left(\frac{1}{2\pi\sigma}\right) = \epsilon_{\frac{1}{\alpha p}\mathbb{Z}}\left(\frac{1}{2\pi\sigma}\right) \leq 4e^{-\frac{\alpha^2p^2}{2\sigma^2}}.$$

Then, since $\alpha \to 0$ and $\alpha p \to \infty$ when $n \to \infty$, for sufficiently large n we have

$$\frac{f_{\sigma,\Lambda_c}(y')}{\frac{1}{|\Lambda_f/\Lambda_c|}f_{\sigma,\Lambda_f}(y')} \leq \frac{1}{\sqrt{2\pi}\sigma}\frac{\alpha p(1+4e^{-\frac{\alpha^2p^2}{2\sigma^2}})}{1-4e^{-\frac{2\pi^2\sigma^2}{\alpha^2}}} \leq C\alpha p$$

for some constant $C > 0$. Consequently, for large enough n, $\exists C' > 0$ such that

$$\psi''(0) \leq C'(\log \alpha p)^2.$$

Then, from the Taylor expansion (53) we obtain the bound

$$\psi(\rho) \leq \rho\mathbb{I}(\mathsf{X};\mathsf{Y}) + \rho^2 C''(\log \alpha p)^2$$

for another suitable constant $C'' > 0$. In particular, we can bound the exponent in equation (46) as follows:

$$\rho R - \psi(\rho|W,\mathcal{U}_\mathcal{X}) \geq \rho(R - \mathbb{I}(\mathsf{X};\mathsf{Y}) - \rho C''(\log \alpha p)^2) > \rho\frac{\delta_0}{2}$$

for sufficiently large n, where δ_0 is defined in (52), as long as $\rho = o\left(\frac{1}{(\log \alpha p)^2}\right)$ and the VNR condition (51) is satisfied. In particular if we choose the scaling[5]

$$p = \xi n^{3/2}, \quad \alpha p = 2\sqrt{n}, \tag{54}$$

where ξ is the smallest number in the interval $[1,2)$ such that p is prime [58, Section IV], we have convergence in (47) with $\bar{\rho} = \frac{1}{(\log 2\sqrt{n})^{2+\eta}}$ for some $\eta > 0$ since

$$\frac{1}{\bar{\rho}}e^{-n\bar{\rho}\frac{\delta_0}{2}} = (\log 2\sqrt{n})^{2+\eta}e^{-\frac{n\delta_0}{2(\log 2\sqrt{n})^{2+\eta}}} \to 0.$$

This concludes the proof of Remark 13.

Then according to Corollary 1, for C_n chosen uniformly in the set of (n,k) linear codes over $\mathbb{F}_p$ of rate $R = \frac{k}{n}\log p$,

$$\mathbb{E}_{\mathsf{C}_n}\left[\mathbb{D}(W^n \circ \mathcal{U}_{\mathsf{C}_n} \| W^n \circ \mathcal{U}_\mathcal{X}^{\otimes n})\right] \leq \frac{1}{\bar{\rho}}e^{-n\bar{\rho}\frac{\delta_0}{2}} \to 0$$

as $n \to \infty$. In particular, there exists at least one code $\mathcal{C}_n$ such that $\mathbb{D}(W^n \circ \mathcal{U}_{\mathcal{C}_n} \| W^n \circ \mathcal{U}_\mathcal{X}^{\otimes n}) \to 0$. Note that

$$(W^n \circ \mathcal{U}_{\mathcal{C}_n})(\mathbf{y}) = \sum_{\mathbf{c}\in\mathcal{C}_n}\frac{1}{|\mathcal{C}_n|}f_{\sigma,\Lambda_c^n}(\mathbf{y}-\alpha\mathbf{c}) = \sum_{\mathbf{c}\in\mathcal{C}_n}\sum_{\boldsymbol{\lambda}_c\in\Lambda_c^n}\frac{1}{p^k}f_\sigma(\mathbf{y}-\alpha\mathbf{c}-\boldsymbol{\lambda}_c) = \frac{1}{p^k}\sum_{\boldsymbol{\lambda}\in\Lambda}f_\sigma(\mathbf{y}-\boldsymbol{\lambda})$$

$$= \frac{1}{p^k}f_{\sigma,\Lambda}(\mathbf{y}), \tag{55}$$

$$(W^n \circ \mathcal{U}_\mathcal{X}^{\otimes n})(\mathbf{y}) = \sum_{\mathbf{x}\in\Lambda_f^n\cap\mathcal{R}(\Lambda_c^n)}\frac{1}{p^n}f_{\sigma,\Lambda_c^n}(\mathbf{y}-\mathbf{x}) = \frac{1}{p^n}f_{\sigma,\Lambda_f^n}(\mathbf{y}). \tag{56}$$

[5]This choice of scaling is compatible with the existence of a suitable sequence of nested lattices, see Appendix D.

Since both $(W^n \circ \mathcal{U}_{\mathcal{C}_n})$ and $(W^n \circ \mathcal{U}_{\mathcal{X}}^{\otimes n})$ are Λ-periodic, we can write

$$\mathbb{D}(W^n \circ \mathcal{U}_{\mathcal{C}_n} \| W^n \circ \mathcal{U}_{\mathcal{X}}^{\otimes n}) = \int_{\mathcal{R}(\Lambda_c^n)} p^{-k} f_{\sigma,\Lambda}(\mathbf{y}) \log \frac{p^{-k} f_{\sigma,\Lambda}(\mathbf{y})}{p^{-n} f_{\sigma,\Lambda_f^n}(\mathbf{y})} d\mathbf{y}$$
$$= \int_{\mathcal{R}(\Lambda)} f_{\sigma,\Lambda}(\mathbf{y}) \log \frac{f_{\sigma,\Lambda}(\mathbf{y})}{p^{-(n-k)} f_{\sigma,\Lambda_f^n}(\mathbf{y})} d\mathbf{y} = \mathbb{D}(f_{\sigma,\mathcal{R}(\Lambda)} \| p^{-(n-k)} f_{\sigma,\Lambda_f^n | \mathcal{R}(\Lambda)}) = C(\Lambda_f^n/\Lambda, \sigma^2) \to 0$$

using Lemma 3. This concludes the proof.

Remark 14: With a standard argument based on Markov's inequality, we can also show that the set of KL-secrecy good lattices has large measure, since $\forall \xi > 0$,

$$\mathbb{P}\left\{\mathbb{D}(W^n \circ \mathcal{U}_{\mathsf{C}_n} \| W^n \circ \mathcal{U}_{\mathcal{X}}^{\otimes n}) > \xi\right\} \leq \frac{1}{\xi} \mathbb{E}_{\mathsf{C}_n}\left[\mathbb{D}(W^n \circ \mathcal{U}_{\mathsf{C}_n} \| W^n \circ \mathcal{U}_{\mathcal{X}}^{\otimes n})\right].$$

Given $0 < c < 1/2$, we can take $\xi = \frac{1}{c} \frac{e^{-n\bar{\rho}\delta_0}}{\bar{\rho}}$ and we obtain

$$\mathbb{P}\left\{\mathbb{D}(W^n \circ \mathcal{U}_{\mathsf{C}_n} \| W^n \circ \mathcal{U}_{\mathcal{X}}^{\otimes n}) > \xi\right\} \leq c.$$

APPENDIX D
EXISTENCE OF A SEQUENCE OF NESTED LATTICES FOR SECRET KEY GENERATION

In this section, we show the existence of a sequence of nested lattices $\Lambda_3^{(n)} \subset \Lambda_2^{(n)} \subset \Lambda_1^{(n)}$ such that Λ_3 is KL secrecy-good, Λ_2 is AWGN-good and Λ_1 is KL secrecy-good. Note that we don't need covering-goodness, which requires more stringent conditions on the parameters [59].

We will follow the construction in [58]. We denote by $V_{\mathcal{B},n}$ the volume of the n-dimensional ball of radius 1. Given $P_3 > P_2 > P_1 > 0$, let $a_i = \log \frac{1}{P_i}$ for $i = 1, 2, 3$. We consider the dimensions $k_3 < k_2 < k_1 \leq n$ defined as follows:

$$k_i = \left\lfloor \frac{n}{2 \log p} \left(\log \left(\frac{4}{V_{\mathcal{B},n}^{2/n}} \right) + a_i \right) \right\rfloor, \quad i = 1, 2, 3,$$

where $p = \xi n^{3/2}$, and ξ is taken to be the smallest number in the interval $[1, 2)$ such that p is prime [58, Section IV][6]. Let $\mathcal{C}_1$ be uniformly sampled from the set of all linear (n, k_1) codes over $\mathbb{F}_p$, with generator matrix G_1 (in column notation). We denote by G_2 and G_3 the submatrices of G_1 corresponding to the first k_2 and k_3 columns respectively, and by $\mathcal{C}_2$, $\mathcal{C}_3$ the corresponding linear codes. Finally, we define the lattices $\tilde{\Lambda}_i = \frac{1}{p}\mathcal{C}_i + \mathbb{Z}^n$ and $\Lambda_i = \alpha p \tilde{\Lambda}_i$ for $i = 1, 2, 3$, where $\alpha = \frac{2\sqrt{n}}{p}$. Then by [58, Theorem 1 and Theorem 6], the matrices G_1, G_2, G_3 are full rank and the nested lattices $\Lambda_3^{(n)} \subset \Lambda_2^{(n)} \subset \Lambda_1^{(n)}$ obtained in this way are good for quantization and coding with probability that tends to 1 when $n \to \infty$ and

$$\lim_{n \to \infty} V^{2/n}(\Lambda_i^{(n)}) = 2\pi e P_i, \quad i = 1, 2, 3.$$

Note that we have taken the same scaling as in (54). In particular, when $n \to \infty$ we have $p \to \infty$, $\alpha \to 0$ and $\alpha p \to \infty$.

Moreover, $\alpha = \frac{2}{\xi n}$ satisfies the condition $\alpha = o\left(\frac{1}{n^c}\right)$ in Appendix C. Therefore, due to Remark 14 the lattices Λ_3 and Λ_1 are also KL secrecy-good with probability close to 1, which concludes the proof.

APPENDIX E
OPTIMAL PUBLIC RATE / SECRET KEY RATE TRADE-OFF

In this section, we derive the optimal trade-off between public rate and secret key rate from [23] for the setting in our paper. Note that Theorem 4 in [23] doesn't directly apply to our model because our source doesn't necessarily satisfy $\mathsf{X} \to \mathsf{Y} \to \mathsf{Z}$. However, the proof of Lemma 6 in [23] shows how to obtain a new source $(\bar{\mathsf{X}}, \bar{\mathsf{Y}}, \bar{\mathsf{Z}})$ which is

[6]Note that the conclusions of [58] still hold for any $p = \Theta(n^{\frac{1}{2}+\delta})$ with $\delta > 0$, see Remark 7 in that paper.

degraded ($\bar{\mathsf{X}} \to \bar{\mathsf{Y}} \to \bar{\mathsf{Z}}$) and has the same achievable region ($\mathcal{R}(\mathsf{X},\mathsf{Y},\mathsf{Z}) = \mathcal{R}(\bar{\mathsf{X}},\bar{\mathsf{Y}},\bar{\mathsf{Z}})$). In particular, translating the proof into our notation, we can take $\bar{\mathsf{X}} = \mathsf{X}$, $\bar{\mathsf{Y}} = \mathsf{Y}$ and

$$\bar{\mathsf{Z}} = \frac{\sigma_z \rho_{xz}}{\sigma_y \rho_{xy}} \mathsf{Y} + \hat{\mathsf{N}},$$

where $\hat{\mathsf{N}}$ is independent of all other random variables and has variance $\sigma_z^2 \left(1 - \frac{\rho_{xz}^2}{\rho_{xy}^2}\right)$.
From elementary computations we see that $\sigma_{\bar{z}} = \sigma_z$, $\rho_{x\bar{z}} = \rho_{xz}$ and $\rho_{y\bar{z}} = \frac{\rho_{xz}}{\rho_{xy}}$.
In our notation, the optimal trade-off given by Theorem 4 of [23] is given by

$$R_K \leq \frac{1}{2} \log \frac{(1-\rho_{\bar{y}\bar{z}}^2)(1-\rho_{\bar{x}\bar{z}}^2) - (\rho_{\bar{x}\bar{y}} - \rho_{\bar{y}\bar{z}}\rho_{\bar{x}\bar{z}})^2 e^{-2R_P}}{(1-\rho_{\bar{y}\bar{z}}^2)(1-\rho_{\bar{x}\bar{z}}^2) - (\rho_{\bar{x}\bar{y}} - \rho_{\bar{y}\bar{z}}\rho_{\bar{x}\bar{z}})^2}.$$

In terms of the original variables $\mathsf{X},\mathsf{Y},\mathsf{Z}$, after simplifying the expression we obtain the optimal trade-off

$$R_K \leq \frac{1}{2} \log \frac{(1-\rho_{xz}^2) - (\rho_{xy}^2 - \rho_{xz}^2) e^{-2R_P}}{1-\rho_{xy}^2}.$$

(Recall that $\rho_{xy} > \rho_{xz}$ in our setting). Using the notation $\sigma_1^2 = \sigma_x^2(1-\rho_{xy}^2)$, $\sigma_2^2 = \sigma_x^2(1-\rho_{xz}^2)$ from our paper, this is equal to

$$R_K \leq \frac{1}{2} \log \left(e^{-2R_P} + \frac{\sigma_2^2}{\sigma_1^2}(1 - e^{-2R_P}) \right). \tag{57}$$

Appendix F
Proof of Lemma 6

The first derivative of the function $\psi(\rho) = \psi(\rho | W, p_{\mathsf{X}})$ is

$$\psi'(\rho) = \frac{\sum_{x\in\mathcal{X}} p_{\mathsf{X}}(x) \int_{\mathcal{Y}} \frac{W_x(y)^{1+\rho}}{((W\circ p_{\mathsf{X}})(y))^{\rho}} \log \frac{W_x(y)}{(W\circ p_{\mathsf{X}})(y)} dy}{\sum_{x\in\mathcal{X}} p_{\mathsf{X}}(x) \int_{\mathcal{Y}} \frac{W_x(y)^{1+\rho}}{((W\circ p_{\mathsf{X}})(y))^{\rho}} dy} = \frac{f(\rho)}{g(\rho)}.$$

Then we have

$$\begin{aligned}
&g(0) = 1,\\
&f(0) = \sum_{x\in\mathcal{X}} p_{\mathsf{X}}(x) \int_{\mathcal{Y}} W_x(y) \log \frac{W_x(y)}{(W\circ p_{\mathsf{X}})(y)} dy = g'(0),\\
&f'(0) = \sum_{x\in\mathcal{X}} p_{\mathsf{X}}(x) \int_{\mathcal{Y}} W_x(y) \left(\log \frac{W_x(y)}{(W\circ p_{\mathsf{X}})(y)} \right)^2 dy.
\end{aligned}$$

The conclusion follows since

$$\psi''(0) = \frac{f'(0)g(0) - f(0)g'(0)}{g^2(0)}.$$

References

[1] C. Ling, L. Luzzi, and M. Bloch, "Secret key generation from Gaussian sources using lattice hashing," in *Proc. IEEE Int. Symp. Inf. Theory*, July 2013.

[2] C. Ling, A. Campello, and L. Liu, "On the L^1 flatness factor of lattices," in *International Zurich Seminar on Communications*, 2018, poster.

[3] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

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

[5] T.-H. Chou, V. Y. F. Tan, and S. C. Draper, "The sender-excited secret key agreement model: Capacity, reliability, and secrecy exponents," *IEEE Trans. Inf. Theory*, vol. 61, no. 1, pp. 609–627, 2015.

[6] C. Chan, M. Mukherjee, N. Kashyap, and Q. Zhou, "On the optimality of secret key agreement via omniscience," *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 2371–2389, 2018.

[7] H. Tyagi and S. Watanabe, "Converses for secret key agreement and secure computing," *IEEE Trans. Inf. Theory*, vol. 61, no. 9, pp. 4809–4827, 2015.

[8] M. Iwamoto, K. Ohta, and J. Shikata, "Security formalizations and their relationships for encryption and key agreement in information-theoretic cryptography," *IEEE Trans. Inf. Theory*, vol. 64, no. 1, pp. 654–685, 2018.

[9] A. Gohari, O. Günlü, and G. Kramer, "Coding for positive rate in the source model key agreement problem," *IEEE Trans. Inf. Theory*, vol. 66, no. 10, pp. 6303–6323, 2020.

[10] C. T. Li and V. Anantharam, "One-shot variable-length secret key agreement approaching mutual information," *IEEE Trans. Inf. Theory*, vol. 67, no. 8, pp. 5509–5525, 2021.

[11] J. Liu, P. Cuff, and S. Verdú, "Key capacity for product sources with application to stationary Gaussian processes," *IEEE Trans. Inf. Theory*, vol. 62, no. 2, pp. 984–1005, 2016.

[12] A. Khisti, "Secret-key agreement over non-coherent block-fading channels with public discussion," *IEEE Trans. Inf. Theory*, vol. 62, no. 12, pp. 7164–7178, 2016.

[13] C. Chan, M. Mukherjee, N. Kashyap, and Q. Zhou, "Upper bounds via lamination on the constrained secrecy capacity of hypergraphical sources," *IEEE Trans. Inf. Theory*, vol. 65, no. 8, pp. 5080–5093, 2019.

[14] H. Tyagi and S. Watanabe, "Universal multiparty data exchange and secret key agreement," *IEEE Trans. Inf. Theory*, vol. 63, no. 7, pp. 4057–4074, 2017.

[15] C. Chan and L. Zheng, "Multiterminal secret key agreement," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3379–3412, 2014.

[16] A. A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals—Part I," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3973–3996, 2010.

[17] K. P. Seshadreesan, M. Takeoka, and M. M. Wilde, "Bounds on entanglement distillation and secret key agreement for quantum broadcast channels," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2849–2866, 2016.

[18] G. Bassi, P. Piantanida, and S. Shamai Shitz, "The wiretap channel with generalized feedback: Secure communication and key generation," *IEEE Trans. Inf. Theory*, vol. 65, no. 4, pp. 2213–2233, 2019.

[19] M. Hayashi, H. Tyagi, and S. Watanabe, "Secret key agreement: General capacity and second-order asymptotics," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3796–3810, 2016.

[20] A. Poostindouz and R. Safavi-Naini, "Second-order asymptotics for one-way secret key agreement," in *2021 IEEE International Symposium on Information Theory (ISIT)*, 2021, pp. 1254–1259.

[21] J. Muramatsu and S. Miyake, "Construction of codes for the wiretap channel and the secret key agreement from correlated source outputs based on the hash property," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 671–692, 2012.

[22] R. A. Chou, M. R. Bloch, and E. Abbe, "Polar coding for secret-key generation," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 6213–6237, 2015.

[23] S. Watanabe and Y. Oohama, "Secret key agreement from correlated Gaussian sources by rate limited public communication," *IEICE Trans. Fundamentals*, vol. E93-A, pp. 1976–1983, Nov. 2010.

[24] A. Khisti, S. N. Diggavi, and G. W. Wornell, "Secret-key generation using correlated sources and channels," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 652–670, 2012.

[25] S. Nitinawarat and P. Narayan, "Secret key generation for correlated Gaussian sources," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3373 –3391, June 2012.

[26] M. Bloch, "Channel intrinsic randomness," in *Proc. Int. Symp. Inf. Theory (ISIT 2010)*, June 2010, pp. 2607 –2611.

[27] J. Muramatsu, H. Koga, and T. Mukouchi, "On the problem of generating mutually independent random sequences," *IEICE Trans. Fundamentals*, vol. E86-A, no. 5, pp. 1275–1284, May 2003.

[28] M. Hayashi, "Exponential decreasing rate of leaked information in universal random privacy amplification," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3989–4001, Jun. 2011.

[29] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on Gaussian measures," in *Proc. Ann. Symp. Found. Computer Science*, Rome, Italy, Oct. 2004, pp. 372–381.

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

[31] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé, "Semantically secure lattice codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 60, no. 10, pp. 6399–6416, Oct. 2014.

[32] M. Hayashi and R. Matsumoto, "Secure multiplex coding with dependent and non-uniform multiple messages," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2355–2409, 2016.

[33] K.-M. Chung, D. Dadush, F.-H. Liu, and C. Peikert, "On the lattice smoothing parameter problem," in *IEEE Conference on Computational Complexity*, 2013.

[34] D. Dadush and O. Regev, "Towards strong reverse Minkowski-type inequalities for lattices," in *2016 IEEE 57th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE, 2016, pp. 447–456.

[35] L. Liu, Y. Yan, and C. Ling, "Achieving secrecy capacity of the Gaussian wiretap channel with polar lattices," *IEEE Trans. Inf. Theory*, vol. 64, no. 3, pp. 1647–1665, 2018.

[36] H. Mirghasemi and J. Belfiore, "The semantic secrecy rate of the lattice Gaussian coding for the Gaussian wiretap channel," in *2014 IEEE Information Theory Workshop (ITW 2014)*, Nov 2014, pp. 112–116.

[37] T. Debris-Alazard, L. Ducas, N. Resch, and J.-P. Tillich, "Smoothing codes and lattices: Systematic study and new bounds," 2022. [Online]. Available: https://arxiv.org/abs/2205.10552

[38] R. Zamir, S. Shamai, and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Trans. Inf. Theory*, vol. 48, pp. 1250–1276, Jun. 2002.

[39] Z. Liu, S. Cheng, A. Liveris, and Z. Xiong, "Slepian-Wolf coded nested lattice quantization for Wyner-Ziv coding: High-rate performance analysis and code design," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4358 –4379, Oct. 2006.

[40] C. Ling, S. Gao, and J.-C. Belfiore, "Wyner-Ziv coding based on multidimensional nested lattices," *IEEE Trans. Commun.*, vol. 60, no. 5, pp. 1328–1335, May 2012.

[41] C. Peikert, "An efficient and parallel Gaussian sampler for lattices," in *Proc. CRYPTO*, vol. 6223. Springer-Verlag, 2010, pp. 80–97.

[42] U. Erez and R. Zamir, "Achieving 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.

[43] A. Campello, D. Dadush, and C. Ling, "AWGN-Goodness is enough: Capacity-achieving lattice codes based on dithered probabilistic shaping," *IEEE Trans. Inf. Theory*, vol. 65, no. 3, pp. 1961–1971, 2019.

[44] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM Journal on Computing*, vol. 38, no. 1, pp. 97–139, 2008.

[45] E. A. Verbitskiy, P. Tuyls, C. Obi, B. Schoenmakers, and B. Skoric, "Key extraction from general nondiscrete signals," *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 2, pp. 269–279, 2010.

[46] J.-P. Linnartz and P. Tuyls, "New shielding functions to enhance privacy and prevent misuse of biometric templates," in *Audio- and Video-Based Biometric Person Authentication*, J. Kittler and M. S. Nixon, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 393–402.

[47] R. Zamir, *Lattice Coding for Signals and Networks: A Structured Coding Approach to Quantization, Modulation, and Multiuser Information Theory*. Cambridge University Press, 2014.

[48] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Trans. Inf. Theory*, vol. 57, pp. 6463–6486, Oct. 2011.

[49] G. Forney, M. Trott, and S.-Y. Chung, "Sphere-bound-achieving coset codes and multilevel coset codes," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 820–850, May 2000.

[50] L. Liu, Y. Yan, C. Ling, and X. Wu, "Construction of capacity-achieving lattice codes: Polar lattices," *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 915–928, 2019.

[51] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge University Press, 2011.

[52] 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, 2000.

[53] I. Csiszár, "Almost independence and secrecy capacity," *Problems of Information Transmission*, vol. 32, pp. 40–47, 1996.

[54] P. Delsarte and P. Piret, "Algebraic constructions of shannon codes for regular channels," *IEEE Trans. Inf. Theory*, vol. 28, no. 4, pp. 593–599, 1982.

[55] R. G. Gallager, *Information Theory and Reliable Communication*. Wiley, 1968.

[56] H. A. Loeliger, "Averaging bounds for lattices and linear codes," *IEEE Trans. Inf. Theory*, vol. 43, pp. 1767–1773, Nov. 1997.

[57] C. Ling and J.-C. Belfiore, "Achieving AWGN channel capacity with lattice Gaussian coding," *IEEE Trans. Inf. Theory*, vol. 60, no. 10, pp. 5918–5929, Oct 2014.

[58] O. Ordentlich and U. Erez, "A simple proof for the existence of "good" pairs of nested lattices," *IEEE Trans. Inf. Theory*, vol. 62, no. 8, pp. 4439–4453, Aug 2016.

[59] 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.