The Rényi Smoothing Parameter and Its Applications in Lattice-Based Cryptography

Cong Ling[1], Laura Luzzi[2,3], and Hao Yan[1]

[1] Imperial College London
{h.yan22, c.ling}@imperial.ac.uk
[2] ETIS (UMR 8051, CY Cergy Paris Université, ENSEA, CNRS),
laura.luzzi@ensea.fr
[3] Équipe COSMIQ, Inria de Paris, laura.luzzi@inria.fr

Abstract. The smoothing parameter is a cornerstone concept in lattice-based cryptography. Traditionally defined using the L^∞ distance, this standard formulation can be overly stringent compared to the L^1 (or statistical) distance more commonly employed in cryptographic contexts. Recent work has proposed relaxed definitions based on Kullback-Leibler (KL) divergence and L^1 distance, thereby loosening the constraints required for the distance to vanish. However, the additive nature of the L^1 distance can be limiting for cryptographic applications where probability preservation is essential. In this paper, we introduce the Rényi smoothing parameter of a lattice, based on Rényi divergence, to address this limitation. The advantages of Rényi divergence in cryptographic settings are well known thanks to its multiplicative nature. The Rényi smoothing parameter provides a tunable framework that interpolates between the L^1 and L^∞ distances, offering enhanced flexibility. We present two complementary methods to study the average behavior of the Rényi flatness factor: one uses classical tools such as the Minkowski-Hlawka ensemble and Rogers' formula for computing lattice function moments; the other employs Construction A lattices derived from random codes. Finally, we illustrate how this new perspective yields improvements in lattice-based cryptographic constructions.

Keywords: Lattice-based cryptography · Minkowski-Hlawka theorem · Rényi divergence · Rogers' formula · smoothing parameter

1 Introduction

The *smoothing parameter* of a lattice Λ is defined as the smallest Gaussian width such that the distribution of Gaussian noise modulo the lattice is close to uniform over the fundamental domain $\mathbb{R}^n/\Lambda$ [31]. This concept plays a central role in both the theory and practice of lattice-based cryptography. Theoretically, it underpins the security proofs of a wide range of cryptographic constructions based on lattices [31, 39]; lattice Gaussian sampling with width close to the smoothing parameter enables solutions to the approximate closest vector problem (CVP)

and shortest vector problem (SVP) [1, 2, 36]. Practically, the smoothing parameter guides concrete parameter selection in several lattice-based schemes [19], such as the FALCON signature algorithm [38].

It is important to note that closeness to uniformity can be evaluated using different distance metrics. In cryptography, the L^1 (statistical) distance is the standard metric to measure proximity of distributions. However, its additive nature can be limiting in security proofs where preservation of probabilities is crucial. To address this, Rényi divergence has been proposed as a more suitable alternative [4]. Owing to its multiplicative property, Rényi divergence offers several benefits in cryptographic settings, including tighter security reductions and more efficient parameter selection. As a result, it has seen growing adoption in lattice-based cryptography (see, e.g., [4, 6, 8, 29, 34, 37, 42]).

Interestingly, the situation is reversed in the context of the smoothing parameter. Micciancio and Regev originally defined the smoothing parameter using the L^∞ distance [31], which corresponds to Rényi divergence of order ∞. This is a stricter notion than the L^1 distance, requiring a larger Gaussian parameter for the folded distribution to approximate uniformity. To mitigate this, an L^1-based version of the smoothing parameter was proposed in [12, 28], potentially enabling more efficient implementations through smaller parameter choices. Indeed, many lattice-based protocols require sampling at or above the smoothing parameter. Tighter sampling enhances security by resisting attacks that exploit large approximation factors. However, the L^1-based smoothing parameter lacks the multiplicative property, and thus inherits the same limitations as the L^1 distance.

This highlights a gap between the L^1 and L^∞ definitions of the smoothing parameter. To bridge this gap, we introduce the *Rényi smoothing parameter*[4], defined using the Rényi divergence of order $1 \leq \alpha \leq \infty$. This new definition interpolates between the two extremes and forms the central focus of this paper. In particular, choosing an order α close to 1—such as $\alpha = 2$—allows the smoothing parameter to retain both the multiplicative property and improved parameter efficiency, offering the best of both worlds.

1.1 Our Contributions

Given a lattice Λ and a noise probability density function (pdf) $\rho(\boldsymbol{x})$, define the Λ-periodic function

$$\rho_\Lambda(\boldsymbol{x}) = \sum_{\boldsymbol{\lambda} \in \Lambda} \rho(\boldsymbol{x} + \boldsymbol{\lambda}).$$

In this paper, we use the Rényi divergence to measure the closeness between the folded distribution $\rho_\Lambda(\boldsymbol{x})$ and the uniform distribution $U(\boldsymbol{x}) = U_{\mathcal{R}(\Lambda)}(\boldsymbol{x}) = 1/V(\Lambda)$, where $V(\Lambda)$ is the covolume of Λ, over a fundamental domain $\mathcal{R}(\Lambda)$ of

[4] Rényi divergence-based smoothing was previously considered in [4], but their analysis was limited to the case of Rényi divergence of order ∞, which coincides with the standard smoothing parameter [31].

Λ:

$$R_\alpha(\rho_\Lambda \| U) = \left(\int_{\mathcal{R}(\Lambda)} \frac{\rho_\Lambda(\boldsymbol{x})^\alpha}{1/V(\Lambda)^{\alpha-1}} \, d\boldsymbol{x} \right)^{\frac{1}{\alpha-1}}, \quad \alpha > 1.$$

We define $R_1(\rho_\Lambda \| U)$ and $R_\infty(\rho_\Lambda \| U)$ as the limits of $R_\alpha(\rho_\Lambda \| U)$ as $\alpha \to 1$ and $\alpha \to \infty$, respectively.

Typically, we consider the n-dimensional Gaussian distribution with parameter $s > 0$:

$$\rho_s(\boldsymbol{x}) = \frac{1}{s^n} \exp\left(-\frac{\pi \|\boldsymbol{x}\|^2}{s^2} \right).$$

In this case, we write $R_\alpha(\rho_\Lambda \| U)$ more explicitly as $R_\alpha(\rho_{s,\Lambda} \| U)$.

Definition 1. *Let $\rho_s(\boldsymbol{x})$ be a Gaussian noise pdf and $\varepsilon \geq 0$. The Rényi smoothing parameter $\eta_\varepsilon^{(\alpha)}(\Lambda)$ of a lattice Λ with order $\alpha \in [1, \infty]$ is defined as the smallest $s > 0$ such that $R_\alpha(\rho_{s,\Lambda} \| U) \leq 1 + \varepsilon$.*

In Section 2, we derive a closed-form expression for $R_\alpha(\rho_{s,\Lambda} \| U)$ when $\alpha \in \mathbb{N}_{\geq 2}$, which allows the Rényi smoothing parameter $\eta_\varepsilon^{(\alpha)}(\Lambda)$ to be explicitly defined as the smallest $s > 0$ satisfying:

$$\sum_{\boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_{\alpha-1} \in \Lambda^*} \exp\left(-\pi s^2 (\boldsymbol{\lambda}_1^T, \ldots, \boldsymbol{\lambda}_{\alpha-1}^T)(\boldsymbol{A} \otimes \boldsymbol{I}_n)(\boldsymbol{\lambda}_1^T, \ldots, \boldsymbol{\lambda}_{\alpha-1}^T)^T \right) \leq (1+\varepsilon)^{\alpha-1}, \tag{1}$$

where Λ^* is the dual lattice and $\boldsymbol{A} = \boldsymbol{I}_{\alpha-1} + \boldsymbol{J}_{\alpha-1}$, with $\boldsymbol{I}_k$ the $k \times k$ identity matrix and $\boldsymbol{J}_k$ the $k \times k$ all-one matrix. Here, $\otimes$ denotes the Kronecker product.

For $\alpha = 2$, this simplifies to the particularly elegant expression:

$$\sum_{\boldsymbol{\lambda} \in \Lambda^*} \exp\left(-2\pi s^2 \|\boldsymbol{\lambda}\|^2 \right) \leq 1 + \varepsilon.$$

Interestingly, this resembles the expression for the standard L^∞ smoothing parameter, defined as in [31] as the smallest $s > 0$ such that

$$\sum_{\boldsymbol{\lambda} \in \Lambda^*} \exp\left(-\pi s^2 \|\boldsymbol{\lambda}\|^2 \right) \leq 1 + \varepsilon.$$

The only difference is a factor of 2 in the exponent. Hence, we obtain the exact relation:

$$\eta_\varepsilon^{(2)}(\Lambda) = \frac{\sqrt{2}}{2} \eta_\varepsilon^{(\infty)}(\Lambda). \tag{2}$$

This highlights the advantage of using the Rényi smoothing parameter: for order $\alpha = 2$, it yields a $\frac{\sqrt{2}}{2}$ reduction in s. Although seemingly modest, this gain can have a significant impact in lattice-based cryptography. For example, the security of the GPV signature scheme is highly sensitive to the value of s [37].

While this is encouraging, we should also be aware of the inherent limit of Rényi smoothing. As shown in Section 3, on average the smoothing parameter

of a random lattice with unit volume (as the lattice dimension $n \to \infty$) is given by:

$$\eta_\varepsilon^{(\alpha)}(\Lambda) \to \alpha^{-1/2(\alpha-1)} = \begin{cases} \frac{1}{\sqrt{e}}, & \text{as } \alpha \to 1; \\ \frac{1}{\sqrt{2}}, & \text{for } \alpha = 2; \\ \frac{1}{\sqrt[4]{3}}, & \text{for } \alpha = 3; \\ \vdots & \\ 1, & \text{as } \alpha \to \infty. \end{cases}$$

Therefore, the maximum possible reduction is a factor of $\sqrt{e}$, achieved in the limit as $\alpha \to 1$ [12, 28].

Remark 1. By defining the Rényi flatness factor $\epsilon_\Lambda^{(\alpha)}(s) \triangleq R_\alpha(\rho_{s,\Lambda} \| U) - 1$, the connection between $\epsilon_\Lambda^{(\alpha)}(s)$ and $\eta_\varepsilon^{(\alpha)}(\Lambda)$ is as follows. For $\alpha \in \mathbb{N}_{\geq 2} \cup \{\infty\}$,

$$\epsilon_\Lambda^{(\alpha)}(s) = \varepsilon \Leftrightarrow s = \eta_\varepsilon^{(\alpha)}(\Lambda).$$

Specifically $\eta_\varepsilon^{(\infty)}(\Lambda) = \eta_\varepsilon(\Lambda)$ where $\eta_\varepsilon(\Lambda)$ is the commonly defined smoothing parameter in [31].

Theorem 1 (Informal)**.** *For $\alpha \in \mathbb{N}_{\geq 2}$ and a suitable ensemble of random lattices of unit volume,*

$$\mathbb{E}_{\Lambda^{(n)}}[\epsilon_{\Lambda^{(n)}}^{(\alpha)}(s)] \to 0$$

exponentially fast as the dimension $n \to \infty$, provided:

$$s > \alpha^{-1/(2\alpha-2)},$$

which is optimal.

Here 'optimal' means that there cannot exist any sequence of lattices of unit volume with vanishing flatness factor unless the above bound is satisfied, which is stated in the following.

Theorem 2 (Informal)**.** *For $\alpha \in \mathbb{N}_{\geq 2}$ and any sequence of lattices $\{\Lambda^{(n)}\}$ of unit volume,*

$$\epsilon_{\Lambda^{(n)}}^{(\alpha)}(s) \to \infty,$$

exponentially fast as the dimension $n \to \infty$, provided that:

$$s < \alpha^{-1/(2\alpha-2)}.$$

Thus the bound $s > \alpha^{-1/(2\alpha-2)}$ is sharp: the Rényi flatness factor of order α of a lattice cannot vanish for any $s < \alpha^{-1/(2\alpha-2)}$. In particular, the L^∞ flatness factor explodes exponentially for any $s < 1$. In fact, one can show that

$$\epsilon_\Lambda^{(\infty)}(s) > \frac{1}{s^n} - 1.$$

In contrast, when $1/\sqrt{e} < s < 1$, the Rényi flatness factor can still be brought under control for a suitable choice of α. This demonstrates the advantage of the Rényi flatness factor.

We also obtain vanishing rates of the Rényi flatness factor with explicit exponents.

Theorem 3 (Informal)**.** *For $\alpha \in \mathbb{N}_{\geq 2}$, $s > \alpha^{-1/(2\alpha-2)}$ and a suitable ensemble of random lattices of unit volume,*

$$\mathbb{E}_{\Lambda^{(n)}}\left[\epsilon^{(\alpha)}_{\Lambda^{(n)}}(s)\right] = O(e^{-nE_s^{(\alpha)}})$$

where

$$E_s^{(\alpha)} = \min\left\{\frac{1}{2}\log\alpha + (\alpha-1)\log s, \frac{1}{2}\log 2s^2\right\}.$$

The formal versions of these results appear in Theorem 5, Theorem 6 and Theorem 7.

1.2 Technical Overview

Random Lattice Ensembles In our subsequent proofs establishing the existence of smoothing-good lattices, we analyze the average behavior of lattices drawn from certain random ensembles. In particular, we consider two ensembles: the Minkowski–Hlawka ensemble and Loeliger's ensemble via Construction A [26]. These two ensembles form the basis for our analysis of smoothing-good lattices. Their averaging properties allow us to deduce that there exist lattices whose average behavior meets the requirements for smoothing.

Rogers' Formula. To study the asymptotic behavior of lattices drawn from the Minkowski–Hlawka ensemble, one must evaluate expectations of the form

$$\mathbb{E}_{\Lambda}\big[f(\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2, \ldots, \boldsymbol{\lambda}_k)\big].$$

This requires the Rogers averaging formula [40], which generalizes Siegel's mean-value theorem [41] to the multivariate setting. In the resulting expansion, the leading terms are straightforward to compute, but the remaining terms are notoriously difficult to handle. In this work, we treat each term in the Gaussian case in turn and derive explicit asymptotic convergence bounds.

Loeliger's Formula for Higher-Order Moments. To derive bounds for the Rényi flatness factor of order $\alpha \geq 2$ for the Construction A lattice ensemble, we extend Loeliger's averaging lemma to α-fold correlations, mirroring the multivariate Rogers formula. Recall that a Construction A lattice $\Lambda(\mathcal{C}) \subseteq \mathbb{R}^n$ is obtained by lifting a linear code $\mathcal{C} \subseteq \mathbb{F}_p^n$ modulo p. By grouping ordered α-tuples of codewords according to the dimension k of their span, one shows that the probability a random α-tuple spans a k-dimensional subspace of $\mathbb{F}_q^n$ is related to the Gaussian binomial coefficient. Substituting this decomposition into the ensemble average produces a finite sum of Gaussian integrals indexed by $k = 1, \ldots, \min(\alpha, n)$. Each term can then be bounded asymptotically, yielding explicit convergence rates for the α-th moment.

Cryptographic Applications. In Section 4 we show that Rényi smoothing can be used in place of the classical smoothing parameter in standard lattice based cryptographic analyses: it yields discrete-Gaussian tail bounds sufficient for correctness and norm control, and it captures the behavior of a discrete Gaussian modulo a sublattice under Rényi smoothing, thereby providing the same kind of near-uniformity guarantees on the quotient that are typically derived from standard smoothing. We then apply these tools to FALCON [38], Leftover Hash Lemma [9], Regev encryption [19], and LIP-based signatures [13], obtaining concrete parameter savings and/or security improvements.

1.3 Related Work and Open Problems

Our research builds upon and complements several recent advances in information theory and lattice-based cryptography. Luzzi, Ling and Bloch [28] analyzed the Kullback–Leibler (KL) and L^1 smoothing behavior of Construction A ensembles under Gaussian noise. Debris-Alazard, Ducas, Resch and Tillich [12] performed an analysis of L^1 smoothing using both Minkowski–Hlawka and Construction A ensembles, considering both Gaussian and ball-shaped noise distributions. They both [12,28] showed the existence of lattices whose L^1 smoothing parameter $\eta_\varepsilon^{(1)}(\Lambda) \to V(\Lambda)^{1/n}/\sqrt{e}$ for a suitable sequence $\varepsilon_n \to 0$. This improves upon the result on L^∞ smoothing parameter $\eta_{\varepsilon_n}(\Lambda) \to V(\Lambda)^{1/n}$.

Beyond asymptotic smoothing bounds, another line of work studies how $\eta_\varepsilon(\Lambda)$ can be used inside concrete lattice-signature proofs. Fouque et al. [15] used Rényi divergence in a security proof for a conservatively modified version of FALCON. Zhang et al. [45] studied GPV preimage sampling under weak smoothness assumptions and applied it to lattice signatures. Jia et al. [24] further revisited the concrete security of FALCON-type signatures. These works are scheme-specific, while our paper studies Rényi smoothing as a general lattice notion and later uses GPV/FALCON as one representative application.

Pouly and Shen [36] employed Rogers' formula to study the L^∞ smoothing properties of the Minkowski–Hlawka ensemble under Gaussian noise. Rogers' formula has also been used in [17,18] to prove probabilistic bounds for the shortest vectors in module lattices.

Interestingly, the left-hand side of (1) can be identified with the degree-$(\alpha-1)$ Siegel theta series [16] associated to the dual lattice Λ^*:

$$\Theta_{\Lambda^*}^{(\alpha-1)}\big(\boldsymbol{A}s^2\big) \;=\; \sum_{(\boldsymbol{\lambda}_1,\cdots,\boldsymbol{\lambda}_{\alpha-1})\in\Lambda^*\times\cdots\times\Lambda^*} e^{-\pi s^2\,\mathrm{tr}(\boldsymbol{S}_{\alpha-1}\boldsymbol{A})},$$

where $\mathrm{tr}(\cdot)$ denotes the trace of a matrix, and the Gram matrix $\boldsymbol{S}_{\alpha-1} = (S_{ij})$ where $S_{ij} = \langle \boldsymbol{\lambda}_i, \boldsymbol{\lambda}_j \rangle, i, j = 1, \ldots, \alpha-1$. Moreover, the infinite sum appearing in Proposition 1—which involves matrix determinants—bears a resemblance to a variant of the Selberg zeta function, as studied by Koecher [43]:

$$\zeta_{\boldsymbol{A}}(k) = \sum_{\boldsymbol{0}\neq\boldsymbol{D}\in\mathbb{Z}^{m\times n}} \det(\boldsymbol{D}\boldsymbol{A}\boldsymbol{D}^T)^{-k}$$

where $\boldsymbol{A}$ is positive definite symmetric and the sum is over a complete set of representatives for equivalence relation $\boldsymbol{D} \sim \boldsymbol{D}'$ if $\boldsymbol{D}' = \boldsymbol{D}\boldsymbol{U}$ with $\boldsymbol{U} \in \mathrm{GL}_n(\mathbb{Z})$. This function extends the classical Epstein zeta function from quadratic forms over vectors to quadratic forms over matrices. Exploring these connections may offer a fruitful direction for future research.

While we have illustrated some applications of the Rényi smoothing parameter, we believe that many more problems in lattice-based cryptography could benefit from this framework, particularly given the central role played by Rényi divergence in recent cryptographic analyses.

1.4 Roadmap

The remainder of this paper is organized as follows: Section 2 introduces the basic definitions of lattices, discrete Gaussian distributions, information theoretic measures, and the Rényi smoothing parameter. Section 3 is concerned with the averaging behavior of Rényi smoothing for the Minkowski–Hlawka ensemble and the Construction A ensemble. Finally, we present selected applications in lattice-based cryptography in Section 4.

Throughout the paper, we use standard asymptotic notation: $f(x) = O(g(x))$ if $\limsup_{x\to\infty} |f(x)/g(x)| < \infty$, $f(x) = o(g(x))$ if $\limsup_{x\to\infty} |f(x)/g(x)| = 0$, and $f(x) = \omega(g(x))$ if $\limsup_{x\to\infty} |g(x)/f(x)| = 0$. All logarithms are natural unless stated otherwise.

2 Definitions

2.1 Information-Theoretic Measures and Inequalities

We define the Rényi divergence and other distances in the same way as in [4].

Let $p(\boldsymbol{x})$ and $q(\boldsymbol{x})$ be probability density functions on $\mathbb{R}^n$. Define

$$\Delta(p,q) = \frac{1}{2}\,\|p-q\|_1 = \frac{1}{2}\int \big|\, p(\boldsymbol{x}) - q(\boldsymbol{x})\big|\, d\boldsymbol{x},$$
$$\|p-q\|_\infty = \sup_{\boldsymbol{x}} \big|\, p(\boldsymbol{x}) - q(\boldsymbol{x})\big|.$$

For $\alpha \neq 1$, the Rényi divergence is defined by [5]

$$R_\alpha\big(p\|q\big) = \left(\int \frac{p(\boldsymbol{x})^\alpha}{q(\boldsymbol{x})^{\alpha-1}}\, d\boldsymbol{x}\right)^{1/(\alpha-1)}.$$

The limit $\alpha \to 1$ corresponds to the KL divergence. In the limit $\alpha \to \infty$ [14],

$$R_\infty\big(p\|q\big) = \operatorname{ess\,sup}_p \frac{p(\boldsymbol{x})}{q(\boldsymbol{x})}.$$

[5] In cryptography, the convention for Rényi divergence typically refers to the exponential of the classical Rényi divergence, which is originally defined using the logarithm.

Here, ess sup denotes the essential supremum, i.e., the supremum taken after ignoring sets of measure zero. The Rényi divergence satisfies the following monotonicity property for $\alpha_1 \leq \alpha_2$:

$$R_{\alpha_1}(p\|q) \;\leq\; R_{\alpha_2}(p\|q).$$

We will also use the following key inequality:

Lemma 1 (Pinsker's Inequality)**.** *For $\alpha \in [1, \infty]$,*

$$R_\alpha(p\|q) \geq e^{2\,\Delta(p,q)^2}.$$

We now present the properties including probability preservation and data processing inequality.

Lemma 2 ([4, Lem. 2.9])**.** *Let p, q be two probability density functions over a measurable space $\mathcal{X}$, and let $(p_i)_i, (q_i)_i$ be two families of density functions. The Rényi divergence satisfies the following properties:*

- ***Data processing inequality:*** *For any measurable function f, and letting p_f, q_f denote the pushforward densities of p, q through f,*

$$R_\alpha(p_f\|q_f) \leq R_\alpha(p\|q).$$

- ***Multiplicativity:*** *For product densities,*

$$R_\alpha\left(\prod_i p_i \middle\| \prod_i q_i\right) = \prod_i R_\alpha(p_i\|q_i).$$

- ***Probability preservation:*** *For any measurable event $E \subseteq \mathrm{Supp}(q)$ and $\alpha \in (1, +\infty)$,*

$$\int_E q(\boldsymbol{x})\,d\boldsymbol{x} \geq \frac{\left(\int_E p(\boldsymbol{x})\,d\boldsymbol{x}\right)^{\alpha/(\alpha-1)}}{R_\alpha(p\|q)}.$$

Rényi divergence is most directly useful for search problems. For decision problems, the advantage is a difference of two probabilities, which is not directly preserved by this multiplicative bound. Thus, Rényi-based decision reductions usually require extra structure, such as the public-sampleability framework of [4]. This limitation will be relevant in our Dual-Regev application.

2.2 Lattice Gaussian Distribution

An n-dimensional lattice Λ in the Euclidean space $\mathbb{R}^n$ is a set defined by $\Lambda = \mathcal{L}(\boldsymbol{B}) = \{\boldsymbol{B}\boldsymbol{x} : \boldsymbol{x} \in \mathbb{Z}^n\}$ where the columns of the basis matrix $\boldsymbol{B} = [\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n]$ are assumed to be linearly independent. The dual lattice Λ^* of a lattice Λ is defined as the set of vectors $\boldsymbol{v} \in \mathbb{R}^n$ such that $\langle \boldsymbol{v}, \boldsymbol{\lambda} \rangle \in \mathbb{Z}$, for all $\boldsymbol{\lambda} \in \Lambda$ (see, e.g., [11]).

A measurable set $\mathcal{R}(\Lambda) \subseteq \mathbb{R}^n$ is a fundamental region of the lattice Λ if $\cup_{\boldsymbol{\lambda}\in\Lambda}(\mathcal{R}(\Lambda)+\boldsymbol{\lambda}) = \mathbb{R}^n$ and if $(\mathcal{R}(\Lambda)+\boldsymbol{\lambda}) \cap (\mathcal{R}(\Lambda)+\boldsymbol{\lambda}')$ has measure 0 for any $\boldsymbol{\lambda} \neq \boldsymbol{\lambda}'$ in Λ. The volume of a fundamental region is equal to that of the Voronoi cell $V(\Lambda) = \sqrt{|\det(\boldsymbol{B}^T\boldsymbol{B})|}$.

For $s > 0$ and $\boldsymbol{v} \in \mathbb{R}^n$, the Gaussian pdf of parameter s centered at $\boldsymbol{v} \in \mathbb{R}^n$ is given by

$$\rho_{s,\boldsymbol{v}}(\boldsymbol{x}) = \frac{1}{s^n} e^{-\frac{\pi\|\boldsymbol{x}-\boldsymbol{v}\|^2}{s^2}},$$

for all $\boldsymbol{x} \in \mathbb{R}^n$. For convenience, we write $\rho_s(\boldsymbol{x}) = \rho_{s,\boldsymbol{0}}(\boldsymbol{x})$.

Consider the Λ-periodic function

$$\rho_{s,\Lambda}(\boldsymbol{x}) = \sum_{\boldsymbol{\lambda}\in\Lambda} \rho_{s,\boldsymbol{\lambda}}(\boldsymbol{x}) = \frac{1}{s^n} \sum_{\boldsymbol{\lambda}\in\Lambda} e^{-\frac{\pi\|\boldsymbol{x}-\boldsymbol{\lambda}\|^2}{s^2}}, \tag{3}$$

for all $\boldsymbol{x} \in \mathbb{R}^n$. Observe that $\rho_{s,\Lambda}$ restricted to the fundamental region $\mathcal{R}(\Lambda)$ is a probability density.

We define the *discrete Gaussian distribution* over Λ centered at $\boldsymbol{v} \in \mathbb{R}^n$ as the following discrete distribution taking values in $\boldsymbol{\lambda} \in \Lambda$:

$$D_{\Lambda,s,\boldsymbol{v}}(\boldsymbol{\lambda}) = \frac{\rho_{s,\boldsymbol{v}}(\boldsymbol{\lambda})}{\rho_{s,\boldsymbol{v}}(\Lambda)}, \quad \forall \boldsymbol{\lambda} \in \Lambda,$$

where $\rho_{s,\boldsymbol{v}}(\Lambda) \triangleq \sum_{\boldsymbol{\lambda}\in\Lambda} \rho_{s,\boldsymbol{v}}(\boldsymbol{\lambda}) = \rho_{s,\Lambda}(\boldsymbol{v})$. Again for convenience, we write $D_{\Lambda,s} = D_{\Lambda,s,\boldsymbol{0}}$.

In some sense, the continuous distribution $\rho_{s,\Lambda}$ and the discrete distribution $D_{\Lambda,s}$ are the Fourier dual of each other. To see this, note that since $\rho_{s,\Lambda}(\boldsymbol{x})$ is Λ-periodic, it admits a Fourier expansion on the dual lattice Λ^*:

$$\rho_{s,\Lambda}(\boldsymbol{x}) = \frac{1}{V(\Lambda)} \sum_{\boldsymbol{\lambda}^*\in\Lambda^*} \hat{\rho}_s(\boldsymbol{\lambda}^*) e^{\mathrm{i}2\pi\langle\boldsymbol{\lambda}^*,\boldsymbol{x}\rangle}, \tag{4}$$

where

$$\hat{\rho}_s(\boldsymbol{y}) = \int \rho_s(\boldsymbol{x}) e^{-\mathrm{i}2\pi\langle\boldsymbol{x},\boldsymbol{y}\rangle} = e^{-\pi s^2\|\boldsymbol{y}\|^2} \tag{5}$$

is the Fourier transform. Thus, the Fourier coefficients $\hat{\rho}_s(\boldsymbol{\lambda}^*)$ have a discrete Gaussian distribution over the dual lattice Λ^* (upon normalization).

Definition 2 (L^∞ Flatness Factor [25]). *For a lattice Λ and for a parameter s, the L^∞ flatness factor is defined by:*

$$\epsilon_\Lambda(s) \triangleq \max_{\boldsymbol{x}\in\mathcal{R}(\Lambda)} |V(\Lambda)\rho_{s,\Lambda}(\boldsymbol{x}) - 1|.$$

The expression of $\epsilon_\Lambda(s)$ can be related to the theta series [11] defined as

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

Lemma 3 (Expression of $\epsilon_{\Lambda}(s)$ [25])**.**

$$\epsilon_{\Lambda}(s) = \frac{V(\Lambda)}{s^n}\Theta_{\Lambda}\left(\frac{1}{s^2}\right) - 1 = \Theta_{\Lambda^*}(s^2) - 1. \tag{6}$$

The flatness factor is shown to be equivalent to the notion of smoothing parameter.

Definition 3 (L^∞ Smoothing Parameter [31, 39]). *For a lattice Λ and for $\varepsilon > 0$, the L^∞ smoothing parameter $\eta_\varepsilon(\Lambda)$ is the smallest $s > 0$ such that $\sum_{\boldsymbol{\lambda}\in\Lambda^*} e^{-\pi s^2\|\boldsymbol{\lambda}\|^2} \leq 1+\varepsilon$.*

Lemma 4 ([25, Prop. 3])**.** *If $s = \eta_\varepsilon(\Lambda)$, then $\epsilon_{\Lambda}(s) = \varepsilon$.*

2.3 Rényi Smoothing Parameter

In this section, we generalize both the smoothing parameter and flatness factor to their Rényi versions.

Definition 4 (Rényi Flatness Factor). *Given a lattice Λ, and Gaussian noise pdf $\rho_s(\boldsymbol{x})$, the Rényi flatness factor of order $\alpha > 1$ is defined as:*

$$\epsilon_{\Lambda}^{(\alpha)}(s) \triangleq R_\alpha(\rho_{s,\Lambda}\|U) - 1 = \left(\int_{\mathcal{R}(\Lambda)} \frac{\rho_{s,\Lambda}(\boldsymbol{x})^\alpha}{1/V(\Lambda)^{\alpha-1}} d\boldsymbol{x}\right)^{\frac{1}{\alpha-1}} - 1.$$

For $\alpha \in \mathbb{N}_{\geq 2}$ we obtain the following expression of $\epsilon_{\Lambda}^{(\alpha)}(s)$.

Theorem 4. *Let Λ be an n-dimensional lattice, with Λ^* its dual lattice, and $\alpha \in \mathbb{N}_{\geq 2}$. Then*

$$\epsilon_{\Lambda}^{(\alpha)}(s) = \left(\sum_{\boldsymbol{\lambda}_1,\ldots,\boldsymbol{\lambda}_{\alpha-1}\in\Lambda^*} e^{-\pi s^2(\boldsymbol{\lambda}_1^T,\ldots,\boldsymbol{\lambda}_{\alpha-1}^T)(\boldsymbol{A}\otimes\boldsymbol{I}_n)(\boldsymbol{\lambda}_1^T,\ldots,\boldsymbol{\lambda}_{\alpha-1}^T)^T}\right)^{\frac{1}{\alpha-1}} - 1$$

*where $\boldsymbol{A} = \boldsymbol{I}_{\alpha-1} + \boldsymbol{J}_{\alpha-1}$ with $\boldsymbol{J}_{\alpha-1}$ the all-one matrix (*i.e.*, all entries are 1) of size $(\alpha-1)\times(\alpha-1)$ and $\otimes$ the Kronecker product.*

The infinite sum on the right-hand side is a theta function. Note that the matrix $\boldsymbol{A}$ has one eigenvalue equal to α and the other eigenvalues equal to 1, with determinant $|\boldsymbol{A}| = \alpha$. It is worth pointing out that $\boldsymbol{A}$ is the Gram matrix of the $A_{\alpha-1}$ lattice whose squared minimum distance is 2.

Proof. We need a basic property of the Fourier transform:

$$\int_{\mathcal{R}(\Lambda)} e^{\mathrm{i}2\pi\langle\boldsymbol{\lambda},\boldsymbol{x}\rangle} d\boldsymbol{x} = \begin{cases} V(\Lambda), & \boldsymbol{\lambda} = \boldsymbol{0}; \\ 0, & \boldsymbol{\lambda} \in \Lambda^* \setminus \{\boldsymbol{0}\}. \end{cases}$$

Using the Fourier expansion (4), we have

$$\begin{aligned}
V(\Lambda)^\alpha \int_{\mathcal{R}(\Lambda)} \rho_{s,\Lambda}(\boldsymbol{x})^\alpha d\boldsymbol{x} &= \int_{\mathcal{R}(\Lambda)} \left(\sum_{\boldsymbol{\lambda}\in\Lambda^*} \hat{\rho}_s(\boldsymbol{\lambda}) e^{\mathrm{i}2\pi\langle \boldsymbol{\lambda}, \boldsymbol{x}\rangle} \right)^\alpha d\boldsymbol{x} \\
&= \int_{\mathcal{R}(\Lambda)} \sum_{\boldsymbol{\lambda}_1,\ldots,\boldsymbol{\lambda}_\alpha\in\Lambda^*} \hat{\rho}_s(\boldsymbol{\lambda}_1)\cdots\hat{\rho}_s(\boldsymbol{\lambda}_\alpha) e^{\mathrm{i}2\pi\langle \boldsymbol{\lambda}_1+\cdots\boldsymbol{\lambda}_\alpha, \boldsymbol{x}\rangle} d\boldsymbol{x} \\
&= \sum_{\boldsymbol{\lambda}_1,\ldots,\boldsymbol{\lambda}_\alpha\in\Lambda^*} \hat{\rho}_s(\boldsymbol{\lambda}_1)\cdots\hat{\rho}_s(\boldsymbol{\lambda}_\alpha) \int_{\mathcal{R}(\Lambda)} e^{\mathrm{i}2\pi\langle \boldsymbol{\lambda}_1+\cdots\boldsymbol{\lambda}_\alpha, \boldsymbol{x}\rangle} d\boldsymbol{x} \\
&= V(\Lambda) \sum_{\boldsymbol{\lambda}_1,\ldots,\boldsymbol{\lambda}_\alpha\in\Lambda^*,\ \sum \boldsymbol{\lambda}_i=\boldsymbol{0}} \hat{\rho}_s(\boldsymbol{\lambda}_1)\cdots\hat{\rho}_s(\boldsymbol{\lambda}_\alpha).
\end{aligned}$$

Recalling that $\hat{\rho}_s(\boldsymbol{y}) = e^{-\pi s^2\|\boldsymbol{y}\|^2}$, we deduce

$$\begin{aligned}
R_\alpha(\rho_{s,\Lambda}\|U)^{\alpha-1} &= V(\Lambda)^{\alpha-1} \int_{\mathcal{R}(\Lambda)} \rho_{s,\Lambda}(\boldsymbol{x})^\alpha d\boldsymbol{x} \\
&= \sum_{\boldsymbol{\lambda}_1,\ldots,\boldsymbol{\lambda}_\alpha\in\Lambda^*,\ \sum \boldsymbol{\lambda}_i=\boldsymbol{0}} e^{-\pi s^2(\|\boldsymbol{\lambda}_1\|^2+\cdots\|\boldsymbol{\lambda}_\alpha\|^2)} \\
&= \sum_{\boldsymbol{\lambda}_1,\ldots,\boldsymbol{\lambda}_{\alpha-1}\in\Lambda^*} e^{-\pi s^2(\|\boldsymbol{\lambda}_1\|^2+\cdots\|\boldsymbol{\lambda}_{\alpha-1}\|^2+\|\boldsymbol{\lambda}_1+\cdots\boldsymbol{\lambda}_{\alpha-1}\|^2)} \\
&= \sum_{\boldsymbol{\lambda}_1,\ldots,\boldsymbol{\lambda}_{\alpha-1}\in\Lambda^*} e^{-\pi s^2(\boldsymbol{\lambda}_1^T,\ldots,\boldsymbol{\lambda}_{\alpha-1}^T)(\boldsymbol{A}\otimes\boldsymbol{I}_n)(\boldsymbol{\lambda}_1^T,\ldots,\boldsymbol{\lambda}_{\alpha-1}^T)^T}. \qquad (7)
\end{aligned}$$

The proof is completed by substituting the above expression into the definition of $\epsilon_\Lambda^{(\alpha)}(s)$. □

From this theorem we are able to give an equivalent and more explicit definition of the Rényi smoothing parameter $\eta_\varepsilon^{(\alpha)}(\Lambda)$ (see Definition 1) when $\alpha \in \mathbb{N}_{\geq 2}$:

Definition 5 (Rényi Smoothing Parameter for $\alpha \in \mathbb{N}_{\geq 2}$). *Given a lattice Λ, and $\boldsymbol{A}$ as defined previously, the Rényi smoothing parameter $\eta_\varepsilon^{(\alpha)}(\Lambda)$ with order $\alpha \in \mathbb{N}_{\geq 2}$ is defined as the smallest $s > 0$ such that*

$$\sum_{\boldsymbol{\lambda}_1,\ldots,\boldsymbol{\lambda}_{\alpha-1}\in\Lambda^*} e^{-\pi s^2(\boldsymbol{\lambda}_1^T,\ldots,\boldsymbol{\lambda}_{\alpha-1}^T)(\boldsymbol{A}\otimes\boldsymbol{I}_n)(\boldsymbol{\lambda}_1^T,\ldots,\boldsymbol{\lambda}_{\alpha-1}^T)^T} \leq (1+\varepsilon)^{\alpha-1}. \qquad (8)$$

Setting $\alpha = 2$, we recognize the left-hand side

$$\sum_{\boldsymbol{\lambda}\in\Lambda^*} e^{-2\pi s^2\|\boldsymbol{\lambda}\|^2} = \Theta_{\Lambda^*}(2s^2) \qquad (9)$$

which coincides with the theta series of the dual lattice Λ^*, thus showing (2).

When we set $\alpha = 3$, the original series reduces to

$$\sum_{\boldsymbol{\lambda}_1,\boldsymbol{\lambda}_2\in\Lambda^*} \exp\Big(-2\pi s^2\big(\|\boldsymbol{\lambda}_1\|^2 + \|\boldsymbol{\lambda}_2\|^2 + \langle\boldsymbol{\lambda}_1,\boldsymbol{\lambda}_2\rangle\big)\Big).$$

Moreover, this double sum can be identified with the degree-2 Siegel theta series [16] associated to the dual lattice Λ^*:

$$\Theta^{(2)}_{\Lambda^*}\big(\boldsymbol{A}s^2\big) \;=\; \sum_{(\boldsymbol{\lambda}_1,\boldsymbol{\lambda}_2)\in\Lambda^*\times\Lambda^*} e^{-\pi s^2\,\mathrm{tr}(\boldsymbol{S}_2\boldsymbol{A})},$$

where the Gram matrix $\boldsymbol{S}_2 = (S_{ij})_{2\times 2}$, $S_{ij} = \big\langle \boldsymbol{\lambda}_i, \boldsymbol{\lambda}_j \big\rangle$, $i,j = 1,2$.

In general, the left-hand side of (8) can be identified with the degree-$(\alpha-1)$ Siegel theta series $\Theta^{(\alpha-1)}_{\Lambda^*}\big(\boldsymbol{A}s^2\big)$.

For any integer $\alpha \geq 2$, the Rényi smoothing parameter and the Rényi flatness factor satisfy

$$\epsilon^{(\alpha)}_{\Lambda}(s) = \varepsilon \quad\Longleftrightarrow\quad s = \eta^{(\alpha)}_{\varepsilon}(\Lambda)\,.$$

Moreover, by Lemma 3 and the definition of the Rényi divergence of order ∞,

$$\epsilon^{(\infty)}_{\Lambda}(s) = \max_{\boldsymbol{x}\in\mathcal{R}(\Lambda)} \{V(\Lambda)\,\rho_{s,\Lambda}(\boldsymbol{x})\} - 1 = \epsilon_{\Lambda}(s)\,.$$

Combining this with Lemma 4 yields

$$\epsilon^{(\infty)}_{\Lambda}(s) = \varepsilon \quad\Longleftrightarrow\quad s = \eta_{\varepsilon}(\Lambda) = \eta^{(\infty)}_{\varepsilon}(\Lambda)\,,$$

which shows that the usual smoothing parameter is the same as the Rényi smoothing parameter of order ∞.

The following Theorem provides a lower bound for $\epsilon^{(\alpha)}_{\Lambda}(s)$.

Theorem 5. *For $\alpha > 1$, for any sequence $\{\Lambda^{(n)}\}$ of lattices of unit volume, where $\Lambda^{(n)} \subset \mathbb{R}^n$ is n-dimensional, given*

$$s < \alpha^{-1/(2\alpha-2)}.$$

we have

$$\epsilon^{(\alpha)}_{\Lambda^{(n)}}(s) \geq \frac{1}{\big(s^2\;\alpha^{\frac{1}{\alpha-1}}\big)^{\frac{n}{2}}} - 1,$$

and $\lim_{n\to\infty} \epsilon^{(\alpha)}_{\Lambda^{(n)}}(s) = \infty$.

Proof. Since $\alpha > 1$, for an n-dimensional lattice Λ,

$$\begin{aligned}
\epsilon^{(\alpha)}_{\Lambda}(s) &= R_\alpha(\rho_{s,\Lambda}\|U) - 1 \\
&= \bigg(\int_{\mathcal{R}(\Lambda)} \bigg(\sum_{\boldsymbol{\lambda}\in\Lambda} \rho_s(\boldsymbol{x}+\boldsymbol{\lambda}) \bigg)^{\alpha} d\boldsymbol{x} \bigg)^{\frac{1}{\alpha-1}} - 1 \\
&\geq \bigg(\int_{\mathcal{R}(\Lambda)} \sum_{\boldsymbol{\lambda}\in\Lambda} \rho_s(\boldsymbol{x}+\boldsymbol{\lambda})^{\alpha} d\boldsymbol{x} \bigg)^{\frac{1}{\alpha-1}} - 1 \\
&= \bigg(\sum_{\boldsymbol{\lambda}\in\Lambda} \int_{\mathcal{R}(\Lambda)+\boldsymbol{\lambda}} \rho_s(\boldsymbol{x})^{\alpha} d\boldsymbol{x} \bigg)^{\frac{1}{\alpha-1}} - 1 \\
&= \bigg(\int_{\mathbb{R}^n} \rho_s(\boldsymbol{x})^{\alpha} d\boldsymbol{x} \bigg)^{\frac{1}{\alpha-1}} - 1 \\
&= \big(s^2\;\alpha^{\frac{1}{\alpha-1}}\big)^{-\frac{n}{2}} - 1.
\end{aligned}$$

In particular, if $s^2\,\alpha^{\frac{1}{\alpha-1}} < 1$, then the factor $\left(s^2\,\alpha^{1/(\alpha-1)}\right)^{-n/2}$ grows exponentially as $n \to \infty$. Hence the entire expression diverges in that regime. □

In the next section we will explore the regimes of s such that a lattice can have a vanishing Rényi flatness factor.

3 Proofs for Random Lattice Ensembles

In this section, we employ the Minkowski-Hlawka ensemble and Loeliger's ensemble via Construction A to examine the conditions under which $\epsilon_{\Lambda}^{(\alpha)}(s)$ approaches zero as n tends to infinity.

We emphasize that these two random ensembles are also cryptographically relevant. Construction-A lattices are the natural model behind q-ary kernel lattices of the form $\Lambda_{\boldsymbol{A}}^{\perp} = \{\boldsymbol{x} \in \mathbb{Z}^m : \boldsymbol{A}\boldsymbol{x} = \boldsymbol{0} \bmod q\}$, which appear in GPV signatures [19] and Regev/Dual-Regev encryption [4, 19, 39]. The Minkowski–Hlawka analysis serves a complementary purpose: it gives a construction-independent geometric result and shows that the same threshold is intrinsic, rather than related to a particular coding construction. The recent work [36] also considers the Minkowski-Hlawka ensemble in order to establish a tighter probabilistic upper bound on the L^{∞} smoothing parameter.

3.1 Minkowski–Hlawka Ensemble

The Minkowski–Hlawka ensemble is constructed by considering the space of unimodular lattices. Specifically, define $\mathfrak{L}_n \cong \mathrm{SL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{Z})$, where each lattice $\Lambda_n \in \mathfrak{L}_n$ is represented by a generator matrix $\boldsymbol{B}$ and the coset $\boldsymbol{B}\mathrm{SL}_n(\mathbb{Z})$ uniquely corresponds to the lattice $\boldsymbol{B}\mathbb{Z}^n$. In this ensemble, each lattice is identified up to scaling and basis transformation, which enables a uniform treatment of lattice properties. The space $\mathfrak{L}_n$ is endowed with the unique, normalized invariant Haar measure μ_n. A central result underlying this ensemble is Siegel's averaging formula [41]:

Lemma 5 ([22,41])**.** *For $n \geq 2$, let $f : \mathbb{R}^n \to \mathbb{R}$ be a Riemann integrable function such that $\|\boldsymbol{x}\|^{n+c} f(\boldsymbol{x})$ is bounded on $\mathbb{R}^n$ for some fixed $c > 0$. Then, for lattices $\Lambda_n \in \mathfrak{L}_n$ drawn according to the Haar measure μ_n,*

$$\mathbb{E}_{\Lambda_n \sim \mu_n}\left[\sum_{\boldsymbol{x} \in \Lambda_n \setminus \{0\}} f(\boldsymbol{x})\right] = \int_{\mathbb{R}^n} f(\boldsymbol{x})\, d\boldsymbol{x}.$$

Note that the lemma has been generalized to apply to essentially bounded Lebesgue measurable functions $f(\boldsymbol{x})$ that vanish outside a bounded region [30]. For convenience in subsequent proofs, we omit the notation $\Lambda_n \sim \mu_n$ and simply write Λ_n when the distribution is understood. With this ensemble, we are able to study the average behavior of the Rényi smoothing parameter.

3.2 Average Behavior for $\boldsymbol{\alpha \in \mathbb{N}_{\geq 2}}$

Fix an integer $\alpha \geq 2$. We first consider the average over the ensemble,

$$\mathbb{E}_{\Lambda}\left[\sum_{\boldsymbol{\lambda}_1,\ldots,\boldsymbol{\lambda}_{\alpha-1}\in\Lambda^*} e^{-\pi s^2(\boldsymbol{\lambda}_1^T,\ldots,\boldsymbol{\lambda}_{\alpha-1}^T)(\boldsymbol{A}\otimes\boldsymbol{I}_n)(\boldsymbol{\lambda}_1^T,\ldots,\boldsymbol{\lambda}_{\alpha-1}^T)^T}\right].$$

If $\Lambda = \boldsymbol{B}\mathbb{Z}^n$, with $\boldsymbol{B} \in \mathrm{SL}_n(\mathbb{R})$, then $\Lambda^* = \boldsymbol{B}^{-T}\mathbb{Z}^n$. Hence on cosets we have the one-to-one correspondence

$$\boldsymbol{B}\,\mathrm{SL}_n(\mathbb{Z}) \;\longmapsto\; \boldsymbol{B}^{-T}\,\mathrm{SL}_n(\mathbb{Z}).$$

It follows that averaging any summation over nonzero lattice points yields the same result whether one averages over Λ or over its dual Λ^* and it can be obtained that $\mathbb{E}_{\Lambda} = \mathbb{E}_{\Lambda^*}$. Therefore, in what follows we will no longer distinguish between $\mathbb{E}_{\Lambda}$ and $\mathbb{E}_{\Lambda^*}$, and denote them both simply by $\mathbb{E}_{\Lambda}$.

Rogers' mean-value formula then provides an explicit expression for this expectation.

Lemma 6 ([40, Theorem 4]). *Consider the Minkowski-Hlawka ensemble of random lattices Λ of dimension n and a Riemann-integrable function f. For $\alpha \in \mathbb{N}_{\geq 2}$, the average*

$$\begin{aligned}
&\mathbb{E}_{\Lambda}\left[\sum_{\boldsymbol{\lambda}_1,\ldots,\boldsymbol{\lambda}_{\alpha-1}\in\Lambda} f(\boldsymbol{\lambda}_1,\boldsymbol{\lambda}_2,\ldots,\boldsymbol{\lambda}_{\alpha-1})\right] \\
&= f(\mathbf{0},\mathbf{0},\ldots,\mathbf{0}) + \int_{\mathbb{R}^n}\cdots\int_{\mathbb{R}^n} f(\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_{\alpha-1})d\boldsymbol{x}_1 d\boldsymbol{x}_2\ldots d\boldsymbol{x}_{\alpha-1} \qquad (10)\\
&+ \sum_{m=1}^{\alpha-2}\sum_{\boldsymbol{\nu},\boldsymbol{\mu}}\sum_{q=1}^{\infty}\sum_{\tilde{\boldsymbol{D}}}\left(\frac{e_1}{q}\cdots\frac{e_m}{q}\right)^n\int_{\mathbb{R}^n}\cdots\int_{\mathbb{R}^n} f\left(\sum_{i=1}^{m}\frac{\tilde{d}_{i1}}{q}\boldsymbol{x}_i,\ldots,\sum_{i=1}^{m}\frac{\tilde{d}_{i(\alpha-1)}}{q}\boldsymbol{x}_i\right)d\boldsymbol{x}_1\ldots d\boldsymbol{x}_m, \qquad (11)
\end{aligned}$$

where the second sum is over all divisions $(\boldsymbol{\nu};\boldsymbol{\mu}) = (\nu_1,\ldots,\nu_m;\mu_1,\ldots,\mu_{\alpha-1-m})$ of the numbers $1,2,\ldots,\alpha-1$ into two sequences,

$$\begin{aligned}
&1 \leq \nu_1 \leq \ldots \leq \nu_m \leq \alpha-1\\
&1 \leq \mu_1 \leq \ldots \leq \mu_{\alpha-1-m} \leq \alpha-1\\
&\nu_i \neq \mu_j, 1 \leq i \leq m, 1 \leq j \leq \alpha-1-m.
\end{aligned}$$

The inner sum is over all $m\times(\alpha-1)$ matrices $\tilde{\boldsymbol{D}}$, with integer elements having greatest common divisor (gcd) relatively prime to q, and with

$$\begin{aligned}
&\tilde{d}_{i\nu_j} = q\delta_{ij}, \quad i=1,\ldots,m, \quad j=1,\ldots,m,\\
&\tilde{d}_{i\mu_j} = 0, \quad \text{if} \quad \mu_j < \nu_i, i=1,\ldots,m, \quad j=1,\ldots,\alpha-1-m,
\end{aligned}$$

where $\delta_{ij} = 1$ only for $i=j$, $e_i = \gcd(\epsilon_i, q), i=1,\ldots,m$, and ϵ_i are the elementary divisors of the matrix $\tilde{\boldsymbol{D}}$.

Proposition 1. *For order $\alpha \in \mathbb{N}_{\geq 2}$, following the notation of Lemma 6, the flatness factor of the Minkowski-Hlawka ensemble of random lattices satisfies*

$$\mathbb{E}_{\Lambda}\left[\epsilon_{\Lambda}^{(\alpha)}(s)\right] \leq \left(1 + \frac{1}{s^{(\alpha-1)n} \cdot \alpha^{n/2}} + \sum_{m=1}^{\alpha-2} \sum_{\boldsymbol{\nu},\boldsymbol{\mu}} \sum_{q=1}^{\infty} \sum_{\tilde{\boldsymbol{D}}} \left(\frac{e_1}{q}\frac{e_2}{q}\cdots\frac{e_m}{q}\right)^n \left(\frac{q}{s}\right)^{mn} \det(\tilde{\boldsymbol{D}}\boldsymbol{A}\tilde{\boldsymbol{D}}^T)^{-n/2}\right)^{1/(\alpha-1)} - 1. \tag{12}$$

Proof. By Theorem 4, we obtain

$$\begin{aligned}\mathbb{E}_{\Lambda}\left[\epsilon_{\Lambda}^{(\alpha)}(s)\right] &= \mathbb{E}_{\Lambda}\left[\left(\sum_{\boldsymbol{\lambda}_1,\ldots,\boldsymbol{\lambda}_{\alpha-1}\in\Lambda^*} e^{-\pi s^2(\boldsymbol{\lambda}_1^T,\ldots,\boldsymbol{\lambda}_{\alpha-1}^T)(\boldsymbol{A}\otimes\boldsymbol{I}_n)(\boldsymbol{\lambda}_1^T,\ldots,\boldsymbol{\lambda}_{\alpha-1}^T)^T}\right)^{\frac{1}{\alpha-1}}\right] - 1 \\ &\leq \left(\mathbb{E}_{\Lambda}\sum_{\boldsymbol{\lambda}_1,\ldots,\boldsymbol{\lambda}_{\alpha-1}\in\Lambda^*} e^{-\pi s^2(\boldsymbol{\lambda}_1^T,\ldots,\boldsymbol{\lambda}_{\alpha-1}^T)(\boldsymbol{A}\otimes\boldsymbol{I}_n)(\boldsymbol{\lambda}_1^T,\ldots,\boldsymbol{\lambda}_{\alpha-1}^T)^T}\right)^{\frac{1}{\alpha-1}} - 1\end{aligned}$$

where Jensen's inequality is applied. To evaluate the expectation of the lattice-sum inside, define the function

$$f(\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2, \ldots, \boldsymbol{\lambda}_{\alpha-1}) = e^{-\pi s^2(\boldsymbol{\lambda}_1^T,\ldots,\boldsymbol{\lambda}_{\alpha-1}^T)(\boldsymbol{A}\otimes\boldsymbol{I}_n)(\boldsymbol{\lambda}_1^T,\ldots,\boldsymbol{\lambda}_{\alpha-1}^T)^T}$$

and apply Lemma 6 where the terms (10) and (11) are analyzed below.

The first term of (10) is

$$f(\mathbf{0}, \mathbf{0}, \ldots, \mathbf{0}) = 1,$$

while the second term of (10) can be derived as

$$\begin{aligned}\int_{\mathbb{R}^n}\cdots\int_{\mathbb{R}^n} f(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{\alpha-1}) d\boldsymbol{x}_1 d\boldsymbol{x}_2 \ldots d\boldsymbol{x}_{\alpha-1} &= \frac{1}{s^{(\alpha-1)n}}\det(\boldsymbol{A}\otimes\boldsymbol{I}_n)^{-1/2} \\ &= \frac{1}{s^{(\alpha-1)n}\cdot\alpha^{n/2}}\end{aligned}$$

For the infinite sum in (11), we derive

$$\begin{aligned}&\sum_{m=1}^{\alpha-2}\sum_{\boldsymbol{\nu},\boldsymbol{\mu}}\sum_{q=1}^{\infty}\sum_{\tilde{\boldsymbol{D}}}\left(\frac{e_1}{q}\cdots\frac{e_m}{q}\right)^n \int_{\mathbb{R}^n}\cdots\int_{\mathbb{R}^n} f\left(\sum_{i=1}^{m}\frac{\tilde{d}_{i1}}{q}\boldsymbol{x}_i, \ldots, \sum_{i=1}^{m}\frac{\tilde{d}_{i(\alpha-1)}}{q}\boldsymbol{x}_i\right) d\boldsymbol{x}_1\ldots d\boldsymbol{x}_m \\ &= \sum_{m=1}^{\alpha-2}\sum_{\boldsymbol{\nu},\boldsymbol{\mu}}\sum_{q=1}^{\infty}\sum_{\tilde{\boldsymbol{D}}}\left(\frac{e_1}{q}\cdots\frac{e_m}{q}\right)^n \int_{\mathbb{R}^n}\cdots\int_{\mathbb{R}^n} e^{-\frac{\pi s^2}{q^2}(\boldsymbol{x}_1^T,\cdots,\boldsymbol{x}_m^T)(\tilde{\boldsymbol{D}}\boldsymbol{A}\tilde{\boldsymbol{D}}^T\otimes\boldsymbol{I}_n)(\boldsymbol{x}_1^T,\cdots,\boldsymbol{x}_m^T)^T} d\boldsymbol{x}_1\ldots d\boldsymbol{x}_m \\ &= \sum_{m=1}^{\alpha-2}\sum_{\boldsymbol{\nu},\boldsymbol{\mu}}\sum_{q=1}^{\infty}\sum_{\tilde{\boldsymbol{D}}}\left(\frac{e_1}{q}\cdots\frac{e_m}{q}\right)^n \left(\frac{q}{s}\right)^{mn}\det(\tilde{\boldsymbol{D}}\boldsymbol{A}\tilde{\boldsymbol{D}}^T)^{-n/2}. \qquad \square\end{aligned}$$

To bound the contribution of the infinite sum in (12) for large n, we use the following Lemma.

Lemma 7. *For $1 \le m \le \alpha - 2$, let $t = m(\alpha - 1 - m) + 1$ and $K_{m,\alpha} = 3^{t+1}(m+1)^{(t+2)/2}$. Then, for $n \ge t + 3$,*

$$\sum_{m=1}^{\alpha-2} \sum_{\boldsymbol{\nu},\boldsymbol{\mu}} \sum_{q=1}^{\infty} \sum_{\tilde{\boldsymbol{D}}} \left(\frac{e_1}{q} \frac{e_2}{q} \cdots \frac{e_m}{q} \right)^n \frac{(q/s)^{mn}}{\det(\tilde{\boldsymbol{D}} \boldsymbol{A} \tilde{\boldsymbol{D}}^T)^{n/2}}$$
$$\le \sum_{m=1}^{\alpha-2} \binom{\alpha-1}{m} (1 + K_{m,\alpha}) \frac{1}{s^{mn}(m+1)^{\frac{n}{2}}} = O\left(\max_{1 \le m \le \alpha-2} \frac{1}{s^{mn}(m+1)^{\frac{n}{2}}} \right).$$

Proof. See Appendix B. □

Combining results above, we are able to specify the average behavior of $\epsilon_{\Lambda}^{(\alpha)}(s)$.

Theorem 6. *Consider a sequence $\{\Lambda^{(n)}\}$, where $\Lambda^{(n)}$ is an n-dimensional random lattice in the Minkowski-Hlawka ensemble $\mathfrak{L}_n$ drawn according to the Haar measure μ_n (see Section 3.1). Then, for any $\alpha \in \mathbb{N}_{\ge 2}$, if*

$$s > \alpha^{-1/2(\alpha-1)},$$

then

$$\mathbb{E}_{\mathfrak{L}_n}\left[\epsilon_{\Lambda^{(n)}}^{(\alpha)}(s) \right] = O\left(\max\left\{ \frac{1}{(\sqrt{2}s)^n}, \frac{1}{s^{(\alpha-1)n}\alpha^{\frac{n}{2}}} \right\} \right) \to 0.$$

Proof. Combining Proposition 1 and Lemma 7, we obtain

$$\begin{aligned} \mathbb{E}_{\mathfrak{L}_n}\left[\epsilon_{\Lambda^{(n)}}^{(\alpha)}(s) \right] &\le \left(1 + \frac{1}{s^{(\alpha-1)n}\alpha^{\frac{n}{2}}} + \max_{1 \le m \le \alpha-2} O\left(\frac{1}{s^{mn}(m+1)^{\frac{n}{2}}} \right) \right)^{\frac{1}{\alpha-1}} - 1 \\ &\le \frac{1}{\alpha-1} \frac{1}{s^{(\alpha-1)n}\alpha^{\frac{n}{2}}} + \frac{1}{\alpha-1} \max_{1 \le m \le \alpha-2} O\left(\frac{1}{s^{mn}(m+1)^{\frac{n}{2}}} \right) \\ &= O\left(\max_{1 \le m \le \alpha-1} \frac{1}{s^{mn}(m+1)^{\frac{n}{2}}} \right). \end{aligned} \tag{13}$$

where Bernoulli's inequality $(1+a)^{\frac{1}{\alpha-1}} - 1 \le \frac{a}{\alpha-1}$ for $\alpha \ge 2$ is applied. For (13) to vanish as $n \to \infty$, it is required for each $1 \le m \le \alpha - 1$, $\frac{1}{s^m(m+1)^{\frac{1}{2}}} < 1 \Rightarrow \frac{1}{s^2} < (m+1)^{1/m}$. Since $g_1(m) = (m+1)^{1/m}$ is monotonically decreasing for $m \ge 1$, it suffices that $s > \alpha^{-1/2(\alpha-1)}$.

To better estimate the convergence rate in (13), consider the function $g_2(m) = \frac{1}{s^m(m+1)^{1/2}}$. Setting $\frac{d}{dm} g_2(m) = 0$, we get the critical point $m^* = -\frac{1}{\log(s^2)} - 1$. If $m^* > 1$, $g_2(m)$ is decreasing for $[1, m^*)$, and then increasing for (m^*, ∞) . If

$m^* \leq 1$, $g_2(m)$ is increasing over $[1, \infty)$. Combining these results, (13) can be expressed as

$$\mathbb{E}_{\mathfrak{L}_n}\left[\epsilon^{(\alpha)}_{\Lambda^{(n)}}(s)\right] = O\left(\max\left\{\frac{1}{(\sqrt{2}s)^n}, \frac{1}{s^{(\alpha-1)n}\alpha^{\frac{n}{2}}}\right\}\right). \tag{14}$$

□

Thus we have obtained a full spectrum of smoothing parameters. The Rényi smoothing parameter decreases with the order α, from 1 for $\alpha \to \infty$ (the usual smoothing parameter) to $1/\sqrt{e}$ for $\alpha \to 1$ (KL divergence) [28].

We now present some examples for small orders α.

Example 1 ($\alpha = 2$)**.** *In this case, only the terms of* (10) *exist so that*

$$\mathbb{E}_{\mathfrak{L}_n}\left[\epsilon^{(2)}_{\Lambda^{(n)}}(s)\right] \leq \frac{1}{(\sqrt{2}s)^n} \to 0$$

if $s > \frac{1}{\sqrt{2}}$*. This agrees with the analysis using* (2)*, since*

$$\Theta_{\Lambda^*}(2s^2) = \frac{1}{(\sqrt{2}s)^n}\Theta_{\Lambda}\left(\frac{1}{2s^2}\right).$$

Example 2 ($\alpha = 3$)**.** *In this case,* $m = 1$ *and the only possible partitions are* $(\boldsymbol{\nu}, \boldsymbol{\mu}) = (1; 2)$ *and* $(2; 1)$*. Thus the* 1×2 *matrix* $\tilde{\boldsymbol{D}} = (q, p)$ *for* $q \geq 1, \gcd(p, q) = 1$ *or* $\tilde{\boldsymbol{D}} = (0, 1)$ [6]*; in either case it holds that* $\epsilon_1 = 1$*.*

The two terms of (10) *are given by*

$$1 + \int_{\mathbb{R}^n}\int_{\mathbb{R}^n} e^{-\pi s^2(\boldsymbol{x}_1^T, \boldsymbol{x}_2^T)(\boldsymbol{I}_{2n} + \boldsymbol{J}_2 \otimes \boldsymbol{I}_n)(\boldsymbol{x}_1^T, \boldsymbol{x}_2^T)^T} d\boldsymbol{x}_1 d\boldsymbol{x}_2 = 1 + \frac{1}{(\sqrt{3}s^2)^n}. \tag{15}$$

The infinite sum in (11) *is given by*

$$\begin{aligned}
&\sum_{\boldsymbol{\nu},\boldsymbol{\mu}}\sum_{q=1}^{\infty}\sum_{\tilde{\boldsymbol{D}}}\left(\frac{e_1}{q}\frac{e_2}{q}\cdots\frac{e_m}{q}\right)^n\left(\frac{q}{s}\right)^{mn}\det(\tilde{\boldsymbol{D}}\boldsymbol{A}\tilde{\boldsymbol{D}}^T)^{-n/2} \\
&= \sum_{q=1}^{\infty}\sum_{p:\gcd(p,q)=1}\frac{1}{s^n}\left(\frac{1}{2(p^2+pq+q^2)}\right)^{n/2} + \left(\frac{1}{\sqrt{2}s}\right)^n \\
&\leq \left(\frac{1}{\sqrt{2}s}\right)^n \sum_{(p,q)\neq(0,0)}\left(\frac{1}{p^2+pq+q^2}\right)^{n/2} \\
&= \left(\frac{1}{\sqrt{2}s}\right)^n \zeta_Q(n/2),
\end{aligned} \tag{16}$$

[6] In general, the second case is $(0, q)$ for $q \geq 1$, but it is required that $\gcd(q, q) = 1$ which leaves $q = 1$ as the only possibility.

where $\zeta_Q(n/2)$ is the Epstein zeta function associated with the positive-definite quadratic form $Q(p,q) = p^2+pq+q^2$. The Epstein zeta function corresponding to a binary quadratic form Q is defined by $\zeta_Q(z) = \sum_{(p,q)\neq(0,0)} \frac{1}{Q(p,q)^z}$ for $\Re(z) > 1$. The Epstein zeta function converges if $n > 2$ in this case. If we consider (15) *and* (16) *both vanish, then it suffices that* (15) *vanishes, i.e.*

$$s > \frac{1}{\sqrt[4]{3}}.$$

But for the dominant term, we need to compare (15) *and* (16) *depending on s. In fact for $n \geq 4$, $\zeta_Q(n/2) \leq \zeta_Q(2) \approx 2.873 < 3$. Thus*

$$\mathbb{E}_{\mathfrak{L}_n}\left[\epsilon^{(3)}_{\Lambda^{(n)}}(s)\right] \;\leq\; \begin{cases} \dfrac{1}{2\cdot\left(\sqrt{3}\,s^2\right)^n}\,(1+o(1)), & s \in \left(\dfrac{1}{\sqrt[4]{3}}, \sqrt{\dfrac{2}{3}}\right], \\ \dfrac{3}{2\cdot\left(\sqrt{2}\,s\right)^n}\,(1+o(1)), & s \in \left(\sqrt{\dfrac{2}{3}}, +\infty\right). \end{cases}$$

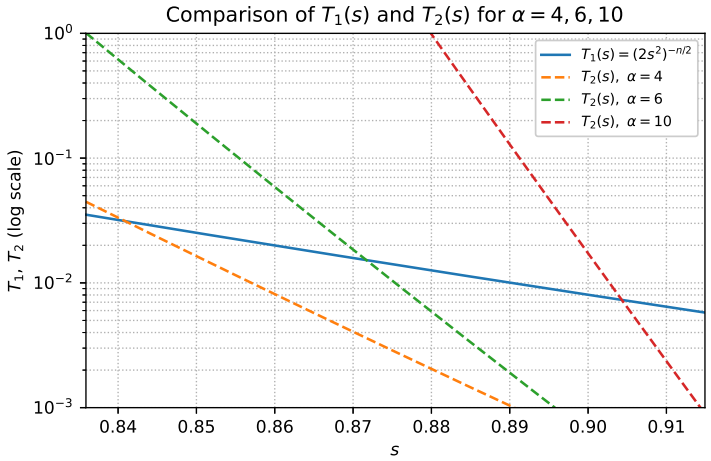

Fig. 1. Comparison of $T_1(s) = (2s^2)^{-n/2}$ and $T_2(s) = s^{-(\alpha-1)n}\,\alpha^{-n/2}$, with $n = 20$. The solid black line is $T_1(s)$; dashed lines are $T_2(s)$ for $\alpha = 4$, 6, and 10. The horizontal axis spans $s \approx [0.83, 0.92]$, and the vertical axis is logarithmic over $[10^{-3}, 1]$ to emphasize where each T_2 curve crosses T_1 (the critical s_c).

For large n and general α, one sees by comparing

$$\frac{1}{(\sqrt{2}s)^n} \quad \text{and} \quad \frac{1}{s^{(\alpha-1)n}\,\alpha^{n/2}}$$

that the sign of

$$\log(2s^2) \;-\; \left[(\alpha-1)\log(s^2) + \log\alpha\right]$$

determines which term is exponentially larger: if s exceeds the unique critical value $s_c(\alpha)$ solving

$$\log(2s^2) \;=\; (\alpha-1)\log(s^2)+\log\alpha,$$

then the Gaussian kernel term $(\sqrt{2}s)^{-n}$ dominates, whereas for $s < s_c(\alpha)$ the mixture term $\left(s^{(\alpha-1)}\,\alpha^{1/2}\right)^{-n}$ prevails. Figure 1 illustrates this crossover for $\alpha = 4, 6, 10$, showing how the threshold $s_c(\alpha)$ shifts to larger values as α increases.

3.3 Loeliger's Ensemble via Construction A

While the Minkowski-Hlawka ensemble encompasses a rich variety of lattices, it presents significant computational challenges for practical implementation. A more tractable alternative is Loeliger's ensemble, which can be efficiently generated by lifting linear codes over $\mathbb{F}_p$ through Construction A, as described in [27]. Let p be a prime number and let $C \subseteq \mathbb{F}_p^n$ be an $[n,k]_p$-linear code over the finite field $\mathbb{F}_p$. The lattice associated with C is defined via Construction A as

$$\Lambda_C = \gamma \cdot \{\boldsymbol{x} \in \mathbb{Z}^n : \boldsymbol{x} \bmod p \in C\} = \gamma \cdot (C + p\mathbb{Z}^n)\,, \tag{17}$$

where γ is a scaling factor (typically chosen in $(0,1)$) to ensure that the lattice has the desired volume properties.

To analyze the average behavior of lattices constructed from linear codes, let $\mathcal{C}_p(n,k)$ denote the ensemble of all $[n,k]_p$-linear codes over $\mathbb{F}_p^n$. The following averaging lemma, analogous to Siegel's formula, holds for the Construction A ensemble:

Lemma 8 (Averaging Lemma [10,27])**.** *Let $f : \mathbb{R}^n \to \mathbb{R}$ be a Riemann integrable function that is semi-admissible, i.e., $(1+\|\boldsymbol{x}\|)^{n+c}|f(\boldsymbol{x})|$ is bounded for some fixed $\boldsymbol{c} > 0$. Then, for any integer k satisfying $0 < k < n$ and any fixed volume V, the following holds:*

$$\frac{1}{|\mathcal{C}_p(n,k)|}\sum_{C\in\mathcal{C}_p(n,k)}\sum_{\boldsymbol{v}\in\Lambda_C} f(\boldsymbol{v}) = \sum_{\boldsymbol{v}\in p\mathbb{Z}^n} f(\gamma\boldsymbol{v}) + \frac{p^k-1}{p^n-1}\Bigg(\sum_{\boldsymbol{v}\in\mathbb{Z}^n} f(\gamma\boldsymbol{v}) - \sum_{\boldsymbol{v}'\in p\mathbb{Z}^n} f(\gamma\boldsymbol{v}')\Bigg),$$

and

$$\lim_{p\to\infty}\frac{1}{|\mathcal{C}_p(n,k)|}\sum_{C\in\mathcal{C}_p(n,k)}\sum_{\boldsymbol{v}\in\Lambda_C\setminus\{\boldsymbol{0}\}} f(\boldsymbol{v}) = \frac{1}{V}\int_{\mathbb{R}^n} f(\boldsymbol{v})\,d\boldsymbol{v},$$

with the constraint $\gamma^n p^{n-k} = V$.

Using this lemma, we establish the following theorem. The proof is conceptually similar to that of Theorem 6. See Appendix C for details.

Theorem 7. *Given $n \in \mathbb{N}_{\geq 1}$, consider the ensemble of Construction A lattices $\Lambda_C^{(n)}$ of unit volume of the form (17), where C is drawn uniformly from the set $\mathcal{C}_p(n,k)$ of $[n,k]_p$ linear codes, with fixed rate $R = k/n \in (0,1)$ and parameter $\gamma = p^{R-1}$.*

Let $\alpha \in \mathbb{N}_{\geq 2}$. Then the following bounds hold:

1. ***Asymptotic Bound:*** *As $n \to \infty$, assuming the prime p satisfies:*

$$p = p(n) = \Theta(n^{\beta}) \quad \textit{with} \quad \beta > \frac{1}{2\min(R,\, 1-R)},$$

and $s > \alpha^{-\frac{1}{2(\alpha-1)}}$, then:

$$\mathbb{E}_{\mathcal{C}_p(n,k)}\big[\epsilon^{(\alpha)}_{\Lambda_C^{(n)}}(s)\big] \leq \max\left\{ \frac{1}{(\sqrt{2}s)^{n(1-o(1))}},\ \frac{1}{(s^{\alpha-1}\sqrt{\alpha})^{n(1-o(1))}} \right\}$$

2. ***Non-Asymptotic Bound:*** *For any $n \geq 2$ and approximation error parameter $\delta \in (0,1]$ (one may choose $\delta = e^{-\omega(n)}$), if s satisfies the following interval condition:*

$$\frac{(\alpha-1)\gamma^2}{\pi}\log\left(\frac{8n}{\delta}\right) \leq s^2 \leq \frac{(p\gamma)^2}{(\alpha-1)\log\left(\frac{8n}{\delta}\right)},$$

then

$$\mathbb{E}_{\mathcal{C}_p(n,k)}[\epsilon^{(\alpha)}_{\Lambda_C}(s)] \leq \frac{(1+\delta)(1+p^{\alpha-2})}{s^n \alpha^{\frac{n}{2(\alpha-1)}}} + \delta.$$

Remark 2. Assume $p = \Theta(n^{\beta})$ with $\beta > \frac{1}{2\min(R,1-R)}$ and choose, e.g., $\delta = n^{-n}$. Then $\frac{(\alpha-1)\gamma^2}{\pi}\log\left(\frac{8n}{\delta}\right) \to 0$, $\frac{(p\gamma)^2}{(\alpha-1)\log\left(\frac{8n}{\delta}\right)} \to \infty$, so the interval condition in Lemma 13 eventually holds for fixed $s > \alpha^{-\frac{1}{2(\alpha-1)}}$, the closed-form non-asymptotic bound in Theorem 7 yields $\mathbb{E}[\epsilon^{(\alpha)}_{\Lambda_C}(s)] = \frac{1}{(s\sqrt{\alpha})^{\frac{n}{\alpha-1}(1-o(1))}}$ the exponent of which is generally weaker than that in the asymptotic bound, reflecting the looseness of the closed-form estimate.

4 Cryptographic Applications

For cryptographic applications using integer lattices, we need to consider Rényi divergences between discrete distributions.

Definition 6 (Discrete Rényi divergence). *Consider a pair of nested lattices $\Lambda' \subseteq \Lambda$. Given two discrete distributions P, Q over Λ/Λ' and $\alpha \in [1,\infty]$, their Rényi divergence of order α is*

$$\mathbb{D}_{\alpha}(P||Q) = \left(\sum_{\boldsymbol{x} \in \Lambda/\Lambda'} \frac{P(\boldsymbol{x})^{\alpha}}{Q(\boldsymbol{x})^{\alpha-1}} \right)^{\frac{1}{\alpha-1}}.$$

With slight abuse of notation, we denote by $D_{\Lambda,s,\mathbf{c}} \bmod \Lambda'$ the density of the random variable $Y \bmod \Lambda'$, where $Y \sim D_{\Lambda,s,\mathbf{c}}$. In different cryptographic applications, we will need to bound the Rényi divergence $\mathbb{D}_{\alpha}(D_{\Lambda,s,\mathbf{c}} \bmod \Lambda' || U_{\Lambda/\Lambda'})$, where $U_{\Lambda/\Lambda'}$ denotes the uniform distribution over the set Λ/Λ'.

When $\alpha = \infty$, $\mathbb{D}_\alpha(D_{\Lambda,s,\boldsymbol{c}} \bmod \Lambda' \| U_{\Lambda/\Lambda'})$ can be bounded using its continuous counterpart $R_\alpha(\rho_{s,\Lambda'} \| U_{\mathcal{R}(\Lambda')})$ in a straightforward manner [19, Cor. 2.8], [4, Lem. 2.10]. In the following, we show that, if $\alpha \in \mathbb{N}_{\geq 2}$, $\mathbb{D}_\alpha(D_{\Lambda,s,\boldsymbol{c}} \bmod \Lambda' \| U_{\Lambda/\Lambda'})$ is still bounded in terms of its continuous counterpart $R_\alpha(\rho_{s,\Lambda'} \| U_{\mathcal{R}(\Lambda')})$. We also show in Appendix F.2 that its limit converges to its continuous counterpart, upon proper scaling.

Lemma 9. *For any pair of lattices $\Lambda' \subseteq \Lambda$, any shift vector $\boldsymbol{c} \in \mathbb{R}^n$, let $D_{\Lambda,s,\boldsymbol{c}} \bmod \Lambda'$ denote the distribution on Λ/Λ' induced by sampling from $D_{\Lambda,s,\boldsymbol{c}}$ and reducing modulo Λ'. Then for $\forall \alpha \in \mathbb{N}_{\geq 2}$,*

$$\mathbb{D}_\alpha(D_{\Lambda,s,\boldsymbol{c}} \bmod \Lambda' \| \mathcal{U}_{\Lambda/\Lambda'}) \leq \frac{\left(\sum_{\boldsymbol{\lambda} \in \Lambda^*} e^{-\pi s^2 \frac{\|\boldsymbol{\lambda}\|^2}{\alpha}}\right)^{\frac{1}{\alpha-1}}}{\left|\sum_{\boldsymbol{\lambda} \in \Lambda^*} e^{-\pi s^2 \|\boldsymbol{\lambda}\|^2} e^{-2\pi \mathrm{i} \langle \boldsymbol{c}, \boldsymbol{\lambda} \rangle}\right|^{\frac{\alpha}{\alpha-1}}} R_\alpha(\rho_{s,\Lambda'} \| \mathcal{U}_{\mathcal{R}(\Lambda')}). \tag{18}$$

Consequently, if $s \geq \eta_\epsilon^{(\alpha)}(\Lambda')$ and $s \geq \sqrt{\alpha} \eta_\epsilon^{(\infty)}(\Lambda)$, then

$$\mathbb{D}_\alpha(D_{\Lambda,s,\boldsymbol{c}} \bmod \Lambda' \| \mathcal{U}_{\Lambda/\Lambda'}) \leq \begin{cases} (1+\epsilon)^{\frac{\alpha}{\alpha-1}} & \text{if } \boldsymbol{c} = \boldsymbol{0}, \\ \left((1+\epsilon)/(1-\epsilon)\right)^{\frac{\alpha}{\alpha-1}} & \text{if } \boldsymbol{c} \neq \boldsymbol{0}. \end{cases} \tag{19}$$

Proof. See Appendix F.1. □

Lemma 10. *Let $\Lambda = \{\boldsymbol{x} : \mathsf{A}\boldsymbol{x} = 0 \mod p\} \subseteq \mathbb{Z}^n$, where $\mathsf{A} \in \mathbb{Z}_p^{m \times n}$ is full rank, and $n > m$. Let $\varepsilon_\alpha = (1+\varepsilon)^{\alpha-1} - 1$. If the modulus p satisfies $p^{2m/n} \geq 2\alpha n \cdot \frac{\log\left(2n(1+1/\varepsilon)\right)}{\log\left(2(\alpha-1)^2/\varepsilon_\alpha\right)}$, then*

$$\frac{1}{\sqrt{\alpha}} \eta_\varepsilon^{(\alpha)}(\Lambda) \;\geq\; \eta_\varepsilon(\mathbb{Z}^n). \tag{20}$$

Assume additionally $\varepsilon \leq \min\{1/2, 1/(\alpha-1)\}$ and any constant $c > 1$. If $\varepsilon \leq \left(\frac{2(\alpha-1)}{e}\right)^{\frac{c}{c-1}} (4n)^{-\frac{1}{c-1}}$, then the simpler condition $p^{2m/n} \geq 2c\alpha n$ suffices.

Proof. See Appendix F.4. □

Remark 3. In particular, setting $c = 2, 3/2, 5/4$ in Lemma 10 yields the following sufficient parameter pairs respectively: $(\varepsilon \leq \frac{(\alpha-1)^2}{ne^2}, p \geq (2\sqrt{\alpha n})^{n/m})$, $(\varepsilon \leq \frac{(\alpha-1)^3}{2e^3 n^2}, p \geq (\sqrt{3\alpha n})^{n/m})$, and $(\varepsilon \leq \frac{(\alpha-1)^5}{8e^5 n^4}, p \geq (\sqrt{\frac{5}{2}\alpha n})^{n/m})$.

We will also need the following lemma, which is proven in Appendix F.3.

Lemma 11 (Tail bound for discrete Gaussian)**.** *Let $\Lambda \subseteq \mathbb{R}^n$ be an n-dimensional lattice and $\boldsymbol{c} \in \mathbb{R}^n$. Assume $s \geq \eta_\varepsilon^{(\alpha)}(\Lambda)$ with $\alpha \geq 2$ and $\varepsilon \in (0, 1/2)$. Then*

$$\Pr_{\boldsymbol{x} \sim D_{\Lambda,s,\boldsymbol{c}}}\left(\|\boldsymbol{x} - \boldsymbol{c}\| > s\sqrt{n}\right) \leq (1+\varepsilon) e^{-nC},$$

where $C = \frac{1}{2}(\pi - 1 - \log(2\pi)) \approx 0.1519$.

Since the tightness of security reductions is not the main focus of this paper, we concentrate on the savings in the smoothing parameter. If needed, tight security reductions can still be achieved by selecting an appropriate order α [42]. For convenience, we focus on the case $\alpha = 2$ in the following.

4.1 GPV Signature Scheme/FALCON

The sampling parameter of the GPV Signature Scheme [19] has been reduced in [4] by using Rényi smoothing of order ∞. Here we show it can be further reduced by Rényi smoothing of order $\alpha < \infty$.

The core technique underlying GPV's signature scheme is discrete Gaussian sampling over a trapdoor lattice [19]. Its security crucially relies on the property that the output distribution of discrete Gaussian sampling is oblivious to any particular basis used in the sampling process, therefore preventing leakage of the private key. We provide a high-level introduction to the GPV signature (see [19] for details). In key generation, one generates a hard public basis for a random lattice Λ, together with a short private basis of Λ. The public basis serves as the public key, while the private basis serves as the private key. Given a message $\boldsymbol{m}$, one uses the private basis to sample a point $\boldsymbol{x}$ from $D_{\Lambda+H(\boldsymbol{m},\boldsymbol{s}),r}$ with parameter r, where $H(\cdot)$ is a hash function and $\boldsymbol{s}$ is a random salt. The signature of $\boldsymbol{m}$ is $\boldsymbol{x}, \boldsymbol{s}$. The verifier checks that $\boldsymbol{x}$ is short and that $\boldsymbol{x} - H(\boldsymbol{m}, \boldsymbol{s}) \in \Lambda$ using the public basis.

The security of GPV signing can be reduced to the hardness of the inhomogeneous short integer solution (ISIS) problem with approximation factor $\sqrt{n}r$ [19]. Therefore, the width r is the most important property of a discrete Gaussian sampler in this context. A key component in the security proof of the GPV signature scheme is the closeness of the distribution of $\mathsf{A}\boldsymbol{x} \mod q$, where $\boldsymbol{x} \leftarrow D_{\mathbb{Z}^m,r}$, to the uniform distribution $U_{\mathbb{Z}_q^n}$. For statistical distance, this requires $r = \Omega(\sqrt{\lambda + \log q_s})$, where λ is the security parameter and q_s denotes the number of signing queries made by the attacker [4]. Using Rényi divergence of order ∞, [4] obtained a smaller bound, namely $r = \Omega(\sqrt{\log \lambda + \log q_s})$.

Notice that here the random lattice Λ is of the form $\Lambda_{\mathsf{A}}^{\perp} = \{\boldsymbol{x} \in \mathbb{Z}^m : \mathsf{A}\boldsymbol{x} = \boldsymbol{0} \mod q\}$, where $\mathsf{A} \in \mathbb{Z}_q^{n\times m}$ is uniformly random. This is actually Construction A defined with parity-check matrix A, thus for prime q we can claim concentration and domain syndrome closeness properties of the Loeliger ensemble thanks to Lemma 9 and Lemma 11. The Rényi divergence under consideration is given by $\mathbb{D}_\alpha(F_{r,\Lambda_{\mathsf{A}}^{\perp}} \| U_{\mathbb{Z}^m/\Lambda_{\mathsf{A}}^{\perp}}) = \mathbb{D}_\alpha(F_{r,\Lambda_{\mathsf{A}}^{\perp}} \| U_{\mathbb{Z}_q^n})$. If we use Rényi smoothing of order $\alpha = 2$, by the relation (2) the required parameter r can be further reduced by a constant $\frac{\sqrt{2}}{2}$. Although the constant may appear small, the security level is quite sensitive to the choice of r [37].

FALCON is a post-quantum digital signature scheme based on the GPV framework and NTRU lattices. In 2022, FALCON was one of four algorithms selected as part of NIST's PQC standardization effort. It uses the fast Fourier transform (FFT) technique on NTRU lattices to achieve great efficiency. Here $r = \sqrt{2\pi}\sigma$ where σ is the standard deviation of FALCON's signing algorithm.

Table 1. Bit-security comparison.

Attack	N	Previous work (σ)		This work ($\sigma/\sqrt{2}$)		Security improvement	
		Classical	Quantum	Classical	Quantum	Classical	Quantum
Forgery	512	120	108	136	122	+16	+14
	1024	277	252	310	278	+33	+26

Note that if $\sigma \geq \eta_\varepsilon^{(\infty)}(\Lambda)$, then $\sigma/\sqrt{2} \geq \eta_\varepsilon^{(2)}(\Lambda)$. To quantify the practical implications of our theoretical improvement, we analyze the effect of scaling the discrete Gaussian parameter from σ to $\sigma/\sqrt{2}$ on FALCON's security against signature forgery, fixing $q = 12289$ as in the specification [38].

Concrete security. We now check Lemma 10 for FALCON. Let $N \in \{512, 1024\}$ be the FALCON ring degree shown in Table 1. The corresponding NTRU lattice is associated with an $N \times 2N$ parity-check matrix, so in Lemma 10 we use $n_{\mathrm{Lem}} = 2N$, $m_{\mathrm{Lem}} = N$, $p = q = 12289$. Hence $p^{2m_{\mathrm{Lem}}/n_{\mathrm{Lem}}} = p$. For $\alpha = 2$ and $c = \frac{3}{2}$, the condition $p^{2m_{\mathrm{Lem}}/n_{\mathrm{Lem}}} \geq 2c\alpha n_{\mathrm{Lem}}$ becomes $p \geq 12N$, which holds for both FALCON parameters: $12289 \geq 12 \cdot 512 = 6144$, $12289 \geq 12 \cdot 1024 = 12288$.

FALCON accepts signatures of squared norm at most $\lfloor \beta^2 \rfloor$ with $\beta = 1.1\sqrt{2n}\sigma$, so scaling $\sigma \to \sigma/\sqrt{2}$ gives $\beta' = \beta/\sqrt{2}$ [38, (2.14)]. To estimate the BKZ blocksize B needed for a successful forgery, we use FALCON's bound

$$\left(\frac{B}{2\pi e}\right)^{n/B} \sqrt{q} \leq \beta,$$

and then convert B to bit-security via the core-SVP rules $\lfloor 0.292\, B \rfloor$ (classical) and $\lfloor 0.262\, B \rfloor$ (quantum) [38, (2.4)–(2.6)]. Plugging in FALCON's recommended β^2 values [38, Table 3.3] yields

$$\beta' = \beta/\sqrt{2} = \begin{cases} \sqrt{34034726/2} \approx 4125.21, & n = 512, \\ \sqrt{70265242/2} \approx 5927.28, & n = 1024\ , \end{cases}$$

which in turn gives $B' \approx \begin{cases} 469, & n = 512, \\ 1064, & n = 1024\ , \end{cases}$ to be compared with FALCON's forgery settings $B \approx 411$ and 952 [38, Table 3.3]. Applying [38, (2.5)–(2.6)], we obtain the following bit-security estimates: $\lfloor 0.292\, B' \rfloor = 136$ (resp. 310) against classical attacks and $\lfloor 0.262\, B' \rfloor = 122$ (resp. 278) against quantum attacks for $n = 512$ (resp. $n = 1024$). These results are included in Table 1.

Table 1 shows that, assuming access to an oracle capable of sampling exactly at or slightly above the smoothing parameter [7, 35, 44] [7] the improvement in the security level can be substantial. Note that reducing the sampling width to

[7] In FALCON-like systems, the signer has a good basis, so this assumption is quite reasonable: [44, Fig.4] shows that running time of the MCMC sampler is nearly unchanged.

$\sigma/\sqrt{2}$ has essentially no impact on key generation and verification running time[8]. We remark that it is worth leaving some security margin, since as lattice attack algorithms improve [46], FALCON with current parameters may fall short of the security levels set by NIST.

Signature size. A smaller parameter does not only give higher security, but also more compact signatures. Recalling that FALCON's signature vector s_2 is sampled according to an n-dimensional discrete Gaussian of parameter σ and then compressed [38, Section 3.11.2], and that the entropy (in bits) of the discrete Gaussian scales like $\log_2(\sigma)$, reducing the sampling parameter by $\sqrt{2}$ amounts to saving approximately $1/2$ bits per dimension. For FALCON-512, we can save 256 bits (32 bytes) so the total signature size will be reduced from 666 to 634 bytes, i.e. by 4.8%.

Note that our approach and Rényi-based optimization in [37] are complementary. We focus on security estimates below the L^∞ smoothing parameter via Rényi smoothing (tightening the required Gaussian width and indistinguishability between $(\mathsf{A}\boldsymbol{x} \bmod q)$ and uniform distribution), while [37] optimizes the sampler itself above the L^∞ smoothing parameter. Our discussion should also be distinguished from the recent FALCON analysis [15] which gives a security proof for a conservative modified version of FALCON using Rényi divergence and L^∞-smoothing. Their goal is to validate the concrete FALCON proof. Our analysis is complementary: we replace L^∞-smoothing by order-2 Rényi smoothing which changes the Gaussian width and the corresponding forgery estimate, assuming an appropriate sampler is available. These techniques may be combined if necessary: for example the Lee weight and MCMC samplers in [7, 35, 44] can be optimized à la [37], while our results can be applied in the security proof. However, the analysis and implementation of such a sampling algorithm is beyond the scope of this paper, and we encourage further research in this direction.

4.2 Cyclotomic Leftover Hash Lemmas

We compare with the smoothing-based cyclotomic LHL in [9, Thm. 6]. The comparison below is therefore made in the same order-2 Rényi measure. Generally speaking, the advantage comes from replacing the usual smoothing by an order-2 Rényi smoothing. Since $\eta_\varepsilon^{(2)}(\Lambda) = \eta_\varepsilon^{(\infty)}(\Lambda)/\sqrt{2}$, the kernel-lattice smoothing requirement is reduced by a factor $\sqrt{2}$ in the Gaussian width.

Let K be a cyclotomic number field of degree N, $\mathcal{O}_K$ its ring of integers, and $\mathcal{O}_q = \mathcal{O}_K/q\mathcal{O}_K$. For $\mathsf{A} \in \mathcal{O}_q^{n\times m}$, with $m \geq n$, write $\Lambda_{\mathsf{A}} = \varphi(\Lambda_q^\perp(\mathsf{A}))$, $\Lambda_q^\perp(\mathsf{A}) = \{\boldsymbol{x} \in \mathcal{O}_K^m : \mathsf{A}\boldsymbol{x} \in (q\mathcal{O}_K)^n\}$, where $\varphi : \mathcal{O}_K^m \hookrightarrow \mathbb{R}^{Nm}$ is either the coefficient embedding τ or the canonical embedding θ, so that $\varphi(\mathcal{O}_K^m)$ is an Nm-dimensional lattice.

[8] Key generation depends on solving the NTRU equation and building the LDL tree, hence on (n, q) rather than on the Gaussian width. Verification still performs the same $O(n \log n)$ NTT-based arithmetic and checks whether $\|(s_1, s_2)\| \leq \beta$.

Given a symmetric positive definite matrix $\Sigma \in \mathbb{R}^{t\times t}$ and a t-dimensional lattice Λ, we define the non-spherical discrete Gaussian $D_{\Lambda,\sqrt{\Sigma},\boldsymbol{c}}(\boldsymbol{x}) = \frac{\rho_{\sqrt{\Sigma},\boldsymbol{c}}(\boldsymbol{x})}{\rho_{\sqrt{\Sigma},\boldsymbol{c}}(\Lambda)}$, where $\rho_{\sqrt{\Sigma},\boldsymbol{c}}(\boldsymbol{x}) = e^{-\pi(\boldsymbol{x}-\boldsymbol{c})^T\Sigma^{-1}(\boldsymbol{x}-\boldsymbol{c})}$. Recall that $\sqrt{\Sigma} \succeq \eta_\varepsilon^{(\infty)}(\Lambda)\boldsymbol{I}$ if and only if $\eta_\varepsilon^{(\infty)}(\sqrt{\Sigma}^{-1}\Lambda) \le 1$ [33]. As in [9], we use the shorthand $\boldsymbol{x} \leftarrow D^{\varphi}_{\mathcal{O}_K^m,\sqrt{\Sigma},\boldsymbol{c}}$ to mean that $\varphi(\boldsymbol{x}) \leftarrow D_{\varphi(\mathcal{O}_K^m),\sqrt{\Sigma},\boldsymbol{c}}$. We now adapt Lemma 9 to this setting.

Theorem 8 (Order-2 Rényi smoothing LHL)**.** *Let P_{A} be a distribution over $\mathcal{O}_q^{n\times m}$. Suppose that, for some $\beta, \delta_1, \delta_2 > 0$,*

$$\Pr_{\mathsf{A}\leftarrow P_{\mathsf{A}}}[\eta_\varepsilon^{(\infty)}(\Lambda_{\mathsf{A}}) > \beta] < \delta_1, \qquad \Pr_{\mathsf{A}\leftarrow P_{\mathsf{A}}}[\mathrm{im}(\mathsf{A}) \neq \mathcal{O}_q^n] < \delta_2.$$

Let $\boldsymbol{x} \leftarrow D^{\varphi}_{\mathcal{O}_K^m,\sqrt{\Sigma},\boldsymbol{c}}$ with $\boldsymbol{c} \in \varphi(\mathcal{O}_K^m)$, and assume

$$\Sigma \succeq \max\left\{\beta/\sqrt{2}, \sqrt{2}\,\eta_\varepsilon^{(\infty)}(\varphi(\mathcal{O}_K^m))\right\}^2 \boldsymbol{I}_{Nm}.$$

Let P' denote the distribution of $(\mathsf{A}, \boldsymbol{y}) = (\mathsf{A}, \mathsf{A}\boldsymbol{x} \bmod q)$ and U' the distribution of $(\mathsf{A}, \boldsymbol{u})$, where $\boldsymbol{u} \leftarrow U(\mathcal{O}_q^n)$. Then

$$\mathbb{D}_2(P'\|U') \le (1+\varepsilon)^2 + (\delta_1+\delta_2)q^{Nn}.$$

Proof. Since the marginal distribution of A is the same in P' and U', $\mathbb{D}_2(P'\|U') = \mathbb{E}_{\mathsf{A}\leftarrow P_{\mathsf{A}}}\left[\mathbb{D}_2(P_{\boldsymbol{y}}\|U(\mathcal{O}_q^n))\right]$, where $P_{\boldsymbol{y}}$ is the distribution of $\boldsymbol{y}$.

Let G be the event that $\eta_\varepsilon^{(\infty)}(\Lambda_{\mathsf{A}}) \le \beta$ and $\mathrm{im}(\mathsf{A}) = \mathcal{O}_q^n$. On G, the map $\boldsymbol{x} \longmapsto \boldsymbol{y} = \mathsf{A}\boldsymbol{x} \bmod q$ induces an isomorphism $\varphi(\mathcal{O}_K^m)/\Lambda_{\mathsf{A}} \simeq \mathcal{O}_q^n$. Thus it suffices to study the distribution $P_{\boldsymbol{z}}$ of $\boldsymbol{z} \leftarrow D_{\varphi(\mathcal{O}_K^m),\sqrt{\Sigma},\boldsymbol{c}}$ modulo Λ_{A}. Similarly to Lemma 9, by Poisson summation and using the character orthogonality,

$$\sum_{\boldsymbol{z}\in\varphi(\mathcal{O}_K^m)/\Lambda_{\mathsf{A}}} e^{2\pi i\langle\boldsymbol{\eta},\boldsymbol{z}\rangle} = |\varphi(\mathcal{O}_K^m)/\Lambda_{\mathsf{A}}| \cdot \mathbf{1}_{\boldsymbol{\eta}\in\varphi(\mathcal{O}_K^m)^*},$$

we obtain, with $Z(\boldsymbol{c}) = \sum_{\boldsymbol{\mu}\in\varphi(\mathcal{O}_K^m)^*} e^{-\pi\boldsymbol{\mu}^T\Sigma\boldsymbol{\mu}}e^{-2\pi i\langle\boldsymbol{c},\boldsymbol{\mu}\rangle}$,

$$\begin{aligned}\mathbb{D}_2(P_{\boldsymbol{z}} \bmod \Lambda_{\mathsf{A}}\|U_{\varphi(\mathcal{O}_K^m)/\Lambda_{\mathsf{A}}}) &\le \frac{1}{|Z(\boldsymbol{c})|^2} \sum_{\substack{\boldsymbol{\nu}_1,\boldsymbol{\nu}_2\in\Lambda_{\mathsf{A}}^*\\ \boldsymbol{\nu}_1+\boldsymbol{\nu}_2\in\varphi(\mathcal{O}_K^m)^*}} e^{-\pi(\boldsymbol{\nu}_1^T\Sigma\boldsymbol{\nu}_1+\boldsymbol{\nu}_2^T\Sigma\boldsymbol{\nu}_2)}\\ &\le \frac{1}{|Z(\boldsymbol{c})|^2}\sum_{\boldsymbol{\mu}\in\varphi(\mathcal{O}_K^m)^*} e^{-\frac{\pi}{2}\boldsymbol{\mu}^T\Sigma\boldsymbol{\mu}}\sum_{\boldsymbol{\nu}\in\Lambda_{\mathsf{A}}^*} e^{-2\pi(\boldsymbol{\nu}-\boldsymbol{\mu}/2)^T\Sigma(\boldsymbol{\nu}-\boldsymbol{\mu}/2)}.\end{aligned}$$

In the second step above we have used the identity $\boldsymbol{\nu}^T\Sigma\boldsymbol{\nu} + (\boldsymbol{\mu}-\boldsymbol{\nu})^T\Sigma(\boldsymbol{\mu}-\boldsymbol{\nu}) = 2(\boldsymbol{\nu}-\boldsymbol{\mu}/2)^T\Sigma(\boldsymbol{\nu}-\boldsymbol{\mu}/2) + \frac{1}{2}\boldsymbol{\mu}^T\Sigma\boldsymbol{\mu}$. The shifted theta sum is maximized at zero shift, hence $\sum_{\boldsymbol{\nu}\in\Lambda_{\mathsf{A}}^*} e^{-2\pi(\boldsymbol{\nu}-\boldsymbol{\mu}/2)^T\Sigma(\boldsymbol{\nu}-\boldsymbol{\mu}/2)} \le \sum_{\boldsymbol{\nu}\in\Lambda_{\mathsf{A}}^*} e^{-2\pi\boldsymbol{\nu}^T\Sigma\boldsymbol{\nu}} \le 1+\varepsilon$, because

$\Sigma \succeq \beta^2 \boldsymbol{I}/2$ and $\eta_\varepsilon^{(\infty)}(\Lambda_{\mathsf{A}}) \le \beta$. Also, $\sum_{\boldsymbol{\mu} \in \varphi(\mathcal{O}_K^m)^*} e^{-\frac{\pi}{2}\boldsymbol{\mu}^T \Sigma \boldsymbol{\mu}} \le 1+\varepsilon$, $|Z(\boldsymbol{c})| \ge 1$, since $\Sigma \succeq 2\eta_\varepsilon^{(\infty)}(\varphi(\mathcal{O}_K^m))^2 \boldsymbol{I}$ and $\boldsymbol{c} \in \varphi(\mathcal{O}_K^m)$. Therefore,

$$\mathbb{D}_2(P_{\boldsymbol{y}} \| U(\mathcal{O}_q^n)) = \mathbb{D}_2(P_{\boldsymbol{z}} \bmod \Lambda_{\mathsf{A}} \| U_{\varphi(\mathcal{O}_K^m)/\Lambda_{\mathsf{A}}}) \le (1+\varepsilon)^2.$$

On the complement of G, we use the trivial bound $\mathbb{D}_2(\cdot \| U(\mathcal{O}_q^n)) \le |\mathcal{O}_q^n| = q^{Nn}$. Since $\Pr[\overline{\mathsf{G}}] \le \delta_1 + \delta_2$, the result follows. □

For $\Sigma = s^2 \boldsymbol{I}_{Nm}$, the condition becomes

$$s \ge \max\left\{\beta/\sqrt{2},\ \sqrt{2}\,\eta_\varepsilon^{(\infty)}(\varphi(\mathcal{O}_K^m))\right\},$$

which saves a factor $\sqrt{2}$ in the Gaussian width in the kernel-dominated regime, order-2 Rényi smoothing. This applies, for example, to dual-Regev encryption scheme for proving $\mathsf{A}\boldsymbol{y} \bmod q$ close to uniform, and can translate into smaller noise width, smaller modulus, or shorter keys/ciphertexts. See Appendix G for details.

4.3 LIP-Based Cryptography

Given two lattices Λ and Λ' with bases $\boldsymbol{B}$ and $\boldsymbol{B'}$ respectively, the Lattice Isomorphism Problem (LIP) is to find an orthogonal matrix $\boldsymbol{O} \in O_n(\mathbb{R})$ and a unimodular matrix $\boldsymbol{U} \in \mathrm{GL}_n(\mathbb{Z})$ such that $\boldsymbol{B'} = \boldsymbol{OBU}$. Lattices can also be represented using quadratic forms. Given a lattice basis $\boldsymbol{B}$, its Gram matrix is defined as $\boldsymbol{Q} = \boldsymbol{B}^T\boldsymbol{B}$. Two quadratic forms $\boldsymbol{Q}$ and $\boldsymbol{Q'}$ are equivalent if there exists a unimodular matrix $\boldsymbol{U}$ such that $\boldsymbol{Q'} = \boldsymbol{U}^T\boldsymbol{QU}$. Thus, the LIP in terms of quadratic forms can be formulated as follows: given two lattices Λ and Λ' with Gram matrices $\boldsymbol{Q}$ and $\boldsymbol{Q'}$ respectively, the LIP asks to find a unimodular matrix $\boldsymbol{U} \in \mathrm{GL}_n(\mathbb{Z})$ such that $\boldsymbol{Q'} = \boldsymbol{U}^T\boldsymbol{QU}$ if it exists. Let $\|\boldsymbol{x}\|_{\boldsymbol{Q}}^2 = \boldsymbol{x}^T\boldsymbol{Q}\boldsymbol{x}$. We write $[\boldsymbol{Q}] := \{\boldsymbol{U}^T\boldsymbol{QU} : \boldsymbol{U} \in \mathrm{GL}_n(\mathbb{Z})\}$ for the integral equivalence class of $\boldsymbol{Q}$, and use the notations $D_{\boldsymbol{Q},s,\boldsymbol{c}}(\boldsymbol{x}) := D_{\Lambda,s,\sqrt{\boldsymbol{Q}}\boldsymbol{c}}(\sqrt{\boldsymbol{Q}}\boldsymbol{x})\ \forall \boldsymbol{x} \in \mathbb{Z}^n$ and $\eta_\varepsilon^{(\alpha)}([\boldsymbol{Q}]) := \eta_\varepsilon^{(\alpha)}(\Lambda)$ where Λ has Gram matrix $\boldsymbol{Q}$.

Recently, the LIP has found numerous applications in cryptography. In [13], an identification scheme, a KEM, and a signature scheme were given with security dependent on problems related to LIP. All these schemes require Gaussian sampling to generate a random form from the equivalent class of $\boldsymbol{S}$, which, for the KEM and signature schemes, serves as the public key. Given a quadratic form $\boldsymbol{S}$ and a parameter $s > \max\{\lambda_n(\boldsymbol{S}), \|\boldsymbol{B}_{\boldsymbol{S}}^*\| \cdot \sqrt{\log(2n+4/\pi)}\}$ where $\boldsymbol{B}_{\boldsymbol{S}}^*$ represents the Gram-Schmidt orthogonalization of a matrix $\boldsymbol{B}_{\boldsymbol{S}}$, [13, Algorithm 1] returns a form $\boldsymbol{P} = \boldsymbol{U}^T\boldsymbol{SU}$ together with $\boldsymbol{U} \in \mathrm{GL}_n(\mathbb{Z})$. This is achieved by running Gaussian sampling over the lattice represented by $\boldsymbol{S}$ with parameter s. Accordingly, we write $\boldsymbol{P} \leftarrow D_s([\boldsymbol{S}])$ for the form output.

The average-case distinguishing version of LIP [13] can be stated as follows:

Definition 7 (ac-$\Delta\mathrm{LIP}_s^{\boldsymbol{Q}_0,\boldsymbol{Q}_1}$). *Given $\boldsymbol{Q'} \leftarrow D_s([\boldsymbol{Q}_b])$ for uniform $b \in \{0,1\}$, output b.*

The hash-then-sign signature scheme given in [13] requires another Gaussian sampler with parameter r, above the smoothing parameter. The signature scheme is EUF-CMA secure if the ac-$\Delta\mathrm{LIP}_s^{\boldsymbol{S},\boldsymbol{Q}^{-1}}$ problem involving a (different) quadratic form $\boldsymbol{Q}$ is hard, where $\boldsymbol{Q}$ has a dense sublattice $\boldsymbol{D}\mathbb{Z}^k \subseteq \mathbb{Z}^n$ of rank $k = \Theta(n)$ such that

$$2r/\sqrt{k} \leq (\sqrt{8\pi e} \cdot \det(\boldsymbol{D}^T\boldsymbol{Q}\boldsymbol{D})^{1/2k})^{-1}. \tag{21}$$

The security proof contains a component that is similar to that of GPV, requiring $r/\sqrt{n} \geq \eta_\varepsilon([\boldsymbol{P}])$ [13]. Reducing the parameter r will relax the above constraint (21) on $\boldsymbol{Q}$ so that the security proof would hold more generally.

Now we give a variant of the LIP-based hash-then-sign scheme [13] using Rényi smoothing of order 2 and prove its correctness and EUF-CMA security.

- **Public parameters.** A positive definite quadratic form $\boldsymbol{S} \in \mathbb{S}^n_{>0}(\mathbb{Z})$, $\varepsilon \in (0, 1/2)$, and a width $r > 0$ with

  $$r/\sqrt{n} \geq \eta_\varepsilon^{(2)}([\boldsymbol{S}]),$$

  and a sampling parameter $s \geq \max\{\lambda_n(\boldsymbol{S}), \|\boldsymbol{B}_{\boldsymbol{S}}^*\|\sqrt{\log(2n+4)/\pi}\}$. We also fix a full-domain hash function modeled as random oracle $H : \mathcal{M} \to \mathbb{T}_q^n$ on the discrete torus $\mathbb{T}_q = \{0, \frac{1}{q}, \ldots, \frac{q-1}{q}\}$ with $q = \lceil \frac{sn}{r}\sqrt{\frac{\log(2n+4)}{\pi}} \rceil$.
- **Key generation.** Sample $\boldsymbol{P} \leftarrow D_s([\boldsymbol{S}])$ as $\boldsymbol{P} = \boldsymbol{U}^T\boldsymbol{S}\boldsymbol{U}$ with $\boldsymbol{U} \in \mathrm{GL}_n(\mathbb{Z})$ using Alg. 1 of [13], and set $(pk, sk) = (\boldsymbol{P}, \boldsymbol{U})$.
- **Signing** $(\boldsymbol{U}, \boldsymbol{m}) \mapsto \boldsymbol{\sigma}$. Let $\boldsymbol{t} \leftarrow H(\boldsymbol{m}) \in \mathbb{T}_q^n$. Sample $\boldsymbol{\sigma}_1 \leftarrow D_{\boldsymbol{S}, r/\sqrt{n}, \boldsymbol{U}\boldsymbol{t}}$ and set $\boldsymbol{\sigma} = \boldsymbol{U}^{-1}\boldsymbol{\sigma}_1 \in \mathbb{Z}^n$.
- **Verification** $(\boldsymbol{P}, \boldsymbol{m}, \boldsymbol{\sigma}) \mapsto \{0, 1\}$. Compute $\boldsymbol{t} \leftarrow H(\boldsymbol{m})$; accept iff $\|\boldsymbol{t} - \boldsymbol{\sigma}\|_{\boldsymbol{P}} \leq r$.

Here we assume access to an efficient sampler to draw $\boldsymbol{\sigma}_1 \leftarrow D_{\boldsymbol{S}, r/\sqrt{n}, \boldsymbol{U}\boldsymbol{t}}$ at the stated width; the hypothesis $s \geq \|\boldsymbol{B}_{\boldsymbol{S}}^*\|\sqrt{\log(2n+4)/\pi}$ guarantees that $\boldsymbol{P}$ can be sampled in polynomial time [13, Lemma 3.4].

Correctness. Since $\boldsymbol{P} = \boldsymbol{U}^T\boldsymbol{S}\boldsymbol{U}$, Lemma 11 yields

$$\|\boldsymbol{t} - \boldsymbol{\sigma}\|_{\boldsymbol{P}} = \|\boldsymbol{U}\boldsymbol{t} - \boldsymbol{U}\boldsymbol{\sigma}\|_{\boldsymbol{S}} = \|\boldsymbol{U}\boldsymbol{t} - \boldsymbol{\sigma}_1\|_{\boldsymbol{S}} \leq r$$

with overwhelming probability by the discrete Gaussian tail bound at width $r/\sqrt{n}$.

Security. We prove the following variant of [13, Thm. 6.2].

Corollary 1 (EUF-CMA under Rényi smoothing of order 2). *Let $\boldsymbol{S}, \boldsymbol{Q} \in \mathbb{S}_n^{>0}(\mathbb{Z})$. Assume $\frac{r}{\sqrt{n}} \geq \eta_\varepsilon^{(2)}(\boldsymbol{S})$ for some $\varepsilon \in (0, 1/2)$, and that there exists $\boldsymbol{D} \in \mathbb{Z}^{n\times k}$ of rank $k = \Theta(n)$ such that (21) holds. Assume access to an efficient sampler used only to draw $\boldsymbol{\sigma}_1 \leftarrow D_{\boldsymbol{S}, r/\sqrt{n}, \boldsymbol{U}\boldsymbol{t}}$. Then the above scheme is EUF-CMA secure if ac-$\Delta\mathrm{LIP}_s^{\boldsymbol{S},\boldsymbol{Q}^{-1}}$ is hard.*

Proof. We follow the three-game sequence of [13, Thm. 6.2] and only change the steps using the properties of the smoothing parameter of $\boldsymbol{S}$.

Game 1 (real). The real EUF-CMA game for the scheme above.

Game 2 (reprogrammed Random Oracle + simulated signing). For each signing query on $\boldsymbol{m}_i$ do: (i) sample $\boldsymbol{e}_i \leftarrow \frac{1}{q} D_{\boldsymbol{P}, qr/\sqrt{n}}$, (ii) set $\boldsymbol{t}_i = H(\boldsymbol{m}_i) = \boldsymbol{e}_i \bmod \mathbb{Z}^n \in \mathbb{T}_q^n$, (iii) return $\boldsymbol{\sigma}_i = \boldsymbol{t}_i - \boldsymbol{e}_i \in \mathbb{Z}^n$. By Lemma 11 , $\|\boldsymbol{t}_i - \boldsymbol{\sigma}_i\|_{\boldsymbol{P}} = \|\boldsymbol{e}_i\|_{\boldsymbol{P}} \le r$ except with negligible probability, hence verification holds. The only distributional change is $\boldsymbol{t}_i = \boldsymbol{e}_i \bmod \mathbb{Z}^n$; conditioned on $\boldsymbol{t}_i$, we have $\boldsymbol{\sigma}_i = \boldsymbol{t}_i - \boldsymbol{e}_i \sim D_{\boldsymbol{P}, r/\sqrt{n}, \boldsymbol{t}_i}$ exactly as in Game 1. Note that for $q \ge 2$ and any n dimensional lattice Λ,

$$\eta_\varepsilon^{(2)}(q\Lambda) = q\,\eta_\varepsilon^{(2)}(\Lambda) = q/\sqrt{2}\,\eta_\varepsilon(\Lambda) \ge \sqrt{2}\,\eta_\varepsilon(\Lambda).$$

Thus by setting $\alpha = 2$ in Lemma 9 and Lemma 1, $q\boldsymbol{t}_i \sim \left(D_{\boldsymbol{P}, qr/\sqrt{n}} \right) \bmod q\mathbb{Z}^n$ is close to uniform distribution over $\mathbb{Z}_q^n$ and thus $\boldsymbol{t}_i$ is close to uniform over $\mathbb{T}_q^n$. Thus the random oracle is still simulated correctly. So Game 1 and Game 2 are statistically indistinguishable.

Game 3. Replace $\boldsymbol{P} \leftarrow D_s([\boldsymbol{S}])$ by $\boldsymbol{P} \leftarrow D_s([\boldsymbol{Q}^{-1}])$. Following the same argument in [13, Thm. 6.2], Game 2 is computationally indistinguishable from Game 3 if ac-$\Delta\mathrm{LIP}_s^{\boldsymbol{S},\boldsymbol{Q}^{-1}}$ is hard, and in Game 3, forging is statistically impossible. This completes the proof. □

In fact, the reduction of r by $\frac{\sqrt{2}}{2}$ can be turned into an argument for stronger concrete security as follows. In the instantiation of the signature scheme in [13, Section 8.2] the lattices associated with $\boldsymbol{S}$ and $\boldsymbol{Q}^{-1}$ are given by $\Lambda_{\boldsymbol{S}} = g\Lambda \oplus (g+1)\Lambda$ and $\Lambda_{\boldsymbol{Q}^{-1}} = \Lambda \oplus g(g+1)\Lambda$, respectively, for some integer $g \ge 1$, where Λ is a lattice with $\mathrm{gap}(\Lambda) \le f$. Then (21) can be rewritten as [13]

$$\Theta(g \cdot f \cdot \det(\Lambda)^{1/n}) \le \Theta(g^2 \cdot \det(\Lambda)^{1/n}),$$

leading to $g = \Theta(f)$ and the primal-dual gap $O(gf) = O(f^2)$. A smaller parameter r in (21) will reduce g, hence the primal-dual gap, by a constant, which implies a gain in concrete security estimates.

Example 3. *Let $\Lambda = \Lambda^* = E_8^{\oplus 32}$ with $n = 256$. Then $\det(\Lambda)^{1/n} = 1, \lambda_1(\Lambda) = \sqrt{2}$, and the Gaussian heuristic gives $\mathrm{gh}(\Lambda) = \sqrt{n/(2\pi e)} \approx 3.8$. Hence gap$(\Lambda)$ is $f = \frac{\mathrm{gh}(\Lambda)}{\lambda_1(\Lambda)} \approx 2.73$. We take the concrete level $\eta_{2^{-n}}(\Lambda) \approx \sqrt{n}/\lambda_1(\Lambda^*) = \sqrt{2\pi e} f$ and $\frac{r}{\sqrt{2n}} \approx g \cdot \eta_{2^{-n}}(\Lambda)$. By (21) this yields $g + 1 \ge 8\sqrt{2}\pi e f$ which gives $g_{\min} \approx 264$ (standard smoothing). If we apply Rényi smoothing of order 2 (which divides the width by $\sqrt{2}$), it becomes $g + 1 \ge 8\pi e f$, and the corresponding $g_{\min}^{(2)} \approx 187$. The primal and dual gaps are*

$$\mathrm{gap}(\Lambda_{\boldsymbol{S}}; g) = \sqrt{2} f \sqrt{1 + 1/g}, \qquad \mathrm{gap}(\Lambda_{\boldsymbol{Q}^{-1}}; g) = \sqrt{2} f \sqrt{g(g+1)}.$$

An α-approx-SVP oracle solves $\Delta\mathrm{LIP}^{\boldsymbol{S},\boldsymbol{Q}^{-1}}$ if $\alpha \le \max\{\mathrm{gap}(\Lambda_{\boldsymbol{S}}; g), \mathrm{gap}(\Lambda_{\boldsymbol{Q}^{-1}}; g)\}$ [13]. For standard smoothing ($g = 264$), $\mathrm{gap}(\Lambda_S; 264) \approx 3.88$, $\mathrm{gap}(\Lambda_{Q^{-1}}; 264) \approx 1024$, hence the primal-dual gap ≈ 1024. For Rényi smoothing of order 2 ($g = 187$), $\mathrm{gap}(\Lambda_S; 187) \approx 3.88$, $\mathrm{gap}(\Lambda_{Q^{-1}}; 187) \approx 726$, hence the primal-dual gap ≈ 726. Thus switching to Rényi smoothing reduces the primal-dual gap by 29%.

Acknowledgments. The authors are grateful to Ling Liu for helpful discussions. This work was supported in part by the Engineering and Physical Sciences Research Council (EPSRC) [grant numbers EP/X037010/1 and EP/Y004477/1].
The work of L. Luzzi was supported in part by CY Initiative of Excellence (Investissements d'Avenir) INEX PHEBE under Grant ANR-16-IDEX-0008 and by the French National Research Agency under Grant ANR JCJC DECODE (ANR-22-CE39-0004-01).

References

1. Aggarwal, D., Dadush, D., Regev, O., Stephens-Davidowitz, N.: Solving the Shortest Vector Problem in 2^n Time Using Discrete Gaussian Sampling: Extended Abstract. In: Proceedings of the Forty-Seventh Annual ACM Symposium on Theory of Computing (STOC '15). pp. 733–742. Association for Computing Machinery, New York, NY, USA (2015). https://doi.org/10.1145/2746539.2746606
2. Aggarwal, D., Dadush, D., Stephens-Davidowitz, N.: Solving the closest vector problem in 2^n time – the discrete Gaussian strikes again! In: 2015 IEEE 56th Annual Symposium on Foundations of Computer Science. pp. 563–582 (2015). https://doi.org/10.1109/FOCS.2015.41
3. Alamati, N., Peikert, C., Stephens-Davidowitz, N.: New (and old) proof systems for lattice problems. In: Public-Key Cryptography – PKC 2018. pp. 619–643. Springer (2018). https://doi.org/10.1007/978-3-319-76581-5_21
4. Bai, S., Lepoint, T., Roux-Langlois, A., Sakzad, A., Stehlé, D., Steinfeld, R.: Improved security proofs in lattice-based cryptography: Using the Rényi divergence rather than the statistical distance. Journal of Cryptology **31**(2), 610–640 (2018). https://doi.org/10.1007/s00145-017-9265-9
5. Banaszczyk, W.: New bounds in some transference theorems in the geometry of numbers. Math. Ann. **296**, 625–635 (1993)
6. Bogdanov, A., Guo, S., Masny, D., Richelson, S., Rosen, A.: On the hardness of learning with rounding over small modulus. In: Fischlin, M., Coron, J.S. (eds.) Theory of Cryptography. LNCS, vol. 9562, pp. 209–224. Springer Berlin Heidelberg (2016). https://doi.org/10.1007/978-3-662-49096-9_9
7. Bollauf, M.F., Lie, M., Ling, C.: On Gaussian sampling for q-ary lattices and linear codes with Lee weight. In: Tauman Kalai, Y., Kamara, S.F. (eds.) Advances in Cryptology – CRYPTO 2025. pp. 321–352. Springer Nature Switzerland, Cham (2025)
8. Boudgoust, K., Costache, A.: Improved rényi arguments for lattice-based threshold encryption. Cryptology ePrint Archive, Paper 2025/735 (2025), https://eprint.iacr.org/2025/735
9. Boudgoust, K., Lapiha, O.: Leftover hash lemma(s) over cyclotomic rings. In: Daemen, J., Thomé, E. (eds.) Advances in Cryptology – EUROCRYPT 2026. Lecture Notes in Computer Science, vol. 16544, pp. 62–91. Springer, Cham (2026). https://doi.org/10.1007/978-3-032-25327-9_3
10. Campello, A.: Random Ensembles of Lattices From Generalized Reductions. IEEE Transactions on Information Theory **64**(7), 5231–5239 (2018). https://doi.org/10.1109/TIT.2018.2803839
11. Conway, J.H., Sloane, N.J.A.: Sphere Packings, Lattices, and Groups. Springer-Verlag, New York, 3rd edn. (1998)

12. Debris-Alazard, T., Ducas, L., Resch, N., Tillich, J.P.: Smoothing codes and lattices: Systematic study and new bounds. IEEE Transactions on Information Theory **69**(9), 6006–6027 (2023). https://doi.org/10.1109/TIT.2023.3276921
13. Ducas, L., van Woerden, W.: On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. In: Dunkelman, O., Dziembowski, S. (eds.) Advances in Cryptology – EUROCRYPT 2022. LNCS, vol. 13277, pp. 643–673. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-07082-2_23
14. van Erven, T., Harremos, P.: Rényi Divergence and Kullback-Leibler Divergence. IEEE Trans. Inf. Theory **60**(7), 3797–3820 (2014). https://doi.org/10.1109/TIT.2014.2320500
15. Fouque, P.A., Gajland, P., de Groote, H., Janneck, J., Kiltz, E.: A closer look at falcon. In: Daemen, J., Thomé, E. (eds.) Advances in Cryptology – EUROCRYPT 2026. LNCS, vol. 16544, pp. 3–31. Springer, Cham (2026). https://doi.org/10.1007/978-3-032-25327-9_1
16. Freitag, E.: Siegelsche Modulfunktionen. Grundlehren der mathematischen Wissenschaften, Springer, Berlin, Heidelberg (1983). https://doi.org/10.1007/978-3-642-68649-8
17. Gargava, N., Serban, V., Viazovska, M.: Moments of the number of points in a bounded set for number field lattices (2023), https://arxiv.org/abs/2308.15275
18. Gargava, N., Serban, V., Viazovska, M., Viglino, I.: Effective module lattices and their shortest vectors (2024), https://arxiv.org/abs/2402.10305
19. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing. p. 197–206. STOC '08, Association for Computing Machinery, New York, NY, USA (2008). https://doi.org/10.1145/1374376.1374407
20. Hardy, G.H., Littlewood, J.E., Pólya, G.: Inequalities. Cambridge University Press (1952)
21. Harville, D.A.: Matrix algebra from a statistician's perspective. Taylor & Francis (1998)
22. Hlawka, E.: Zur geometrie der zahlen. Mathematische Zeitschrift **49**(1), 285–312 (1943)
23. Horn, R.A., Johnson, C.R.: Matrix analysis. Cambridge University Press (2012)
24. Jia, H., Zhang, S., Yu, Y., Tang, C.: Revisiting the concrete security of Falcon-type signatures. In: Public-Key Cryptography – PKC 2026. Lecture Notes in Computer Science, Springer (2026)
25. Ling, C., Luzzi, L., Belfiore, J.C., Stehlé, D.: Semantically secure lattice codes for the gaussian wiretap channel. IEEE Transactions on Information Theory **60**(10), 6399–6416 (2014). https://doi.org/10.1109/TIT.2014.2343226
26. Loeliger, H.A.: Averaging bounds for lattices and linear codes. IEEE Trans. Inf. Theory **43**, 1767–1773 (Nov 1997)
27. Loeliger, H.A.: Averaging bounds for lattices and linear codes. IEEE Transactions on Information Theory **43**(6), 1767–1773 (1997). https://doi.org/10.1109/18.641543
28. Luzzi, L., Ling, C., Bloch, M.R.: Optimal rate-limited secret key generation from gaussian sources using lattices. IEEE Transactions on Information Theory **69**(8), 4944–4960 (2023). https://doi.org/10.1109/TIT.2023.3266033
29. Lyubashevsky, V., Peikert, C., Regev, O.: On Ideal Lattices and Learning with Errors over Rings. In: Gilbert, H. (ed.) Advances in Cryptology – EUROCRYPT 2010. LNCS, vol. 6110, pp. 1–23. Springer, Berlin, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_1

30. Macbeath, A., Rogers, C.: A modified form of Siegel's mean value theorem. II. In: Mathematical Proceedings of the Cambridge Philosophical Society. vol. 54, pp. 322–326. Cambridge University Press (1958)
31. Micciancio, D., Regev, O.: Worst-case to average-case reductions based on Gaussian measures. In: 45th Annual IEEE Symposium on Foundations of Computer Science (FOCS). pp. 372–381. IEEE Computer Society (2004). https://doi.org/10.1109/FOCS.2004.72
32. Pathegama, M., Barg, A.: Rényi divergence guarantees for hashing with linear codes. IEEE Trans. Inf. Theory **71**(8), 5809–5819 (2025). https://doi.org/10.1109/TIT.2025.3577765
33. Peikert, C.: An efficient and parallel Gaussian sampler for lattices. In: Proc. of CRYPTO. LNCS, vol. 6223, pp. 80–97. Springer-Verlag (2010)
34. del Pino, R., Katsumata, S., Prest, T., Rossi, M.: Raccoon: A Masking-Friendly Signature Proven in the Probing Model. In: Reyzin, L., Stebila, D. (eds.) Advances in Cryptology – CRYPTO 2024. LNCS, vol. 14920, pp. 395–426. Springer, Cham (2024). https://doi.org/10.1007/978-3-031-68376-3_13
35. Pouly, A., Shen, Y.: Discrete Gaussian Sampling for BKZ-Reduced Basis. In: Niederhagen, R., Saarinen, M.J.O. (eds.) Post-Quantum Cryptography. LNCS, vol. 15578. Springer, Cham (2025). https://doi.org/10.1007/978-3-031-86602-9_3
36. Pouly, A., Shen, Y.: Solving the Shortest Vector Problem in $2^{0.63269n+o(n)}$ time on random lattices. In: Advances in Cryptology – EUROCRYPT 2026, Part IV. LNCS, vol. 16544, pp. 92–123. Springer, Cham (2026). https://doi.org/10.1007/978-3-032-25327-9_4
37. Prest, T.: Sharper bounds in lattice-based cryptography using the rényi divergence. In: Takagi, T., Peyrin, T. (eds.) Advances in Cryptology – ASIACRYPT 2017. LNCS, vol. 10624, pp. 371–401. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70694-8_13
38. Prest, T., Kirchner, P., Killijian, M.O., Fouque, P.A., Lyubashevsky, V., Pornin, T.: FALCON: Fast-fourier lattice-based compact signatures over NTRU. https://falcon-sign.info/falcon.pdf (2020), NIST Post-Quantum Cryptography Standardization, Round 3 Submission
39. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. J. ACM **56**(6) (Sep 2009). https://doi.org/10.1145/1568318.1568324
40. Rogers, C.A.: Mean values over the space of lattices. Acta Math. **94**, 249–287 (1955), https://doi.org/10.1007/BF02392493
41. Siegel, C.L.: A mean value theorem in geometry of numbers. Annals of Mathematics **46**(2), 340–347 (1945)
42. Takashima, K., Takayasu, A.: Tighter Security for Efficient Lattice Cryptography via the Rényi Divergence of Optimized Orders. In: Au, M.H., Miyaji, A. (eds.) Provable Security. ProvSec 2015. LNCS, vol. 9451, pp. 388–407. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-26059-4_23
43. Terras, A.: Fourier Coefficients of Eisenstein Series of One Complex Variable for the Special Linear Group. Transactions of the American Mathematical Society **205**, 97–114 (Apr 1975). https://doi.org/10.2307/1997193
44. Wang, Z., Ling, C.: Lattice Gaussian sampling by Markov Chain Monte Carlo: Bounded distance decoding and trapdoor sampling. IEEE Transactions on Information Theory **65**(6), 3630–3645 (2019). https://doi.org/10.1109/TIT.2019.2901497
45. Zhang, S., Jia, H., Ran, D., Yu, Y., Yu, Y., Wang, X.: GPV preimage sampling with weak smoothness and its applications to lattice signatures. In: Advances in

Cryptology – ASIACRYPT 2025. Lecture Notes in Computer Science, vol. 16247, pp. 233–264. Springer (2025). https://doi.org/10.1007/978-981-95-5099-9_8
46. Zhao, Z., Ding, J.: Towards large-scale lattice attack: New lattice records by disk-based sieving. In: Daemen, J., Thomé, E. (eds.) Advances in Cryptology – EUROCRYPT 2026. pp. 154–182. Springer Nature Switzerland, Cham (2026)

Appendix

A Asymptotic behavior of Rogers's sums

Lemma 12. *Let $m, \alpha \in \mathbb{N}$ such that $1 \le m < \alpha - 1$. For $q \in \mathbb{Z}^+$, define the set of matrices*

$$\mathcal{D}_q \triangleq \{\boldsymbol{D} \in \mathbb{Z}^{m\times(\alpha-1)} : \boldsymbol{D} = (q\boldsymbol{I}_m, \boldsymbol{C}),\ \text{where } \boldsymbol{C} \in \mathbb{Z}^{m\times(\alpha-1-m)}, \boldsymbol{C} \neq \boldsymbol{0}\}$$

Let $\boldsymbol{A} = \boldsymbol{I}_{\alpha-1} + \boldsymbol{J}_{\alpha-1}$, where $\boldsymbol{J}_{\alpha-1} = \boldsymbol{1}_{\alpha-1}\boldsymbol{1}_{\alpha-1}^T$ is the all-one matrix, and set $t = m(\alpha - 1 - m) + 1$. Then, for all $n \ge t + 3$,

$$\sum_{q=1}^{\infty} \sum_{\boldsymbol{D}\in\mathcal{D}_q} \frac{1}{s^{mn}} \left(\frac{q^{m-1}}{\sqrt{\det(\boldsymbol{D}\boldsymbol{A}\boldsymbol{D}^T)}} \right)^n \le 3^{t+1}(m+1)^{(t+2)/2} \frac{1}{s^{mn}(m+1)^{\frac{n}{2}}}.$$

In particular, as $n \to \infty$,

$$\sum_{q=1}^{\infty} \sum_{\boldsymbol{D}\in\mathcal{D}_q} \frac{1}{s^{mn}} \left(\frac{q^{m-1}}{\sqrt{\det(\boldsymbol{D}\boldsymbol{A}\boldsymbol{D}^T)}} \right)^n = O\left(\frac{1}{s^{mn}(m+1)^{\frac{n}{2}}} \right).$$

More generally, for any permutation matrix $\boldsymbol{P}$, the same result holds when summing over $\mathcal{D}_q(\boldsymbol{P}) \triangleq \{\boldsymbol{D} : \boldsymbol{D}\boldsymbol{P} = (q\boldsymbol{I}_m, \boldsymbol{C}), \boldsymbol{C} \neq \boldsymbol{0}\}$ instead. Note that the case above corresponds to $\mathcal{D}_q = \mathcal{D}_q(\boldsymbol{I}_{\alpha-1})$.

Proof. Note that the general case can be reduced to the special case where $\boldsymbol{D} \in \mathcal{D}_q$, because

$$(\boldsymbol{D}\boldsymbol{P})\boldsymbol{A}(\boldsymbol{D}\boldsymbol{P})^T = \boldsymbol{D}\boldsymbol{P}(\boldsymbol{I}_{\alpha-1} + \boldsymbol{J}_{\alpha-1})\boldsymbol{P}^T\boldsymbol{D}^T = \boldsymbol{D}(\boldsymbol{I}_{\alpha-1} + \boldsymbol{J}_{\alpha-1})\boldsymbol{D}^T = \boldsymbol{D}\boldsymbol{A}\boldsymbol{D}^T.$$

Hence, we assume without loss of generality that $\boldsymbol{D} = (q\boldsymbol{I}_m, \boldsymbol{C})$.

Let $\boldsymbol{C} = (c_{ij}) \in \mathbb{Z}^{m\times(\alpha-1-m)} \setminus \boldsymbol{0}_{m\times(\alpha-1-m)}$ and

$$R(q, \boldsymbol{C}) \triangleq \sqrt{q^2 + \|\boldsymbol{C}\|_F^2} = \sqrt{q^2 + \sum_{i=1}^{m}\sum_{j=1}^{\alpha-1-m} c_{ij}^2}.$$

Denote $\boldsymbol{d}_m = \boldsymbol{D}\boldsymbol{1}_{\alpha-1} = \left(q + \sum_j c_{1j}, \ldots, q + \sum_j c_{mj}\right)^T$. Since

$$\boldsymbol{D}\boldsymbol{A}\boldsymbol{D}^T = q^2\boldsymbol{I}_m + \boldsymbol{C}\boldsymbol{C}^T + \boldsymbol{d}_m\boldsymbol{d}_m^T,$$

and $\boldsymbol{d}_m\boldsymbol{d}_m^T \succeq 0$, we first have by the inequality $\det(\boldsymbol{A} + \boldsymbol{B}) \ge \det(\boldsymbol{A}) + \det(\boldsymbol{B})$ for positive definite symmetric matrices,

$$\begin{aligned} \det(\boldsymbol{D}\boldsymbol{A}\boldsymbol{D}^T) &\ge \det(q^2\boldsymbol{I}_m + \boldsymbol{C}\boldsymbol{C}^T) \\ &\ge q^{2m} + q^{2m-2}\|\boldsymbol{C}\|_F^2 = q^{2m-2}R(q, \boldsymbol{C})^2. \end{aligned} \tag{22}$$

Moreover, we have

$$\begin{aligned}
\det(\boldsymbol{D}\boldsymbol{A}\boldsymbol{D}^T) &= \det(q^2\boldsymbol{I}_m + \boldsymbol{C}\boldsymbol{C}^T + \boldsymbol{d}_m\boldsymbol{d}_m^T) \\
&= \det(q^2\boldsymbol{I}_m + \boldsymbol{C}\boldsymbol{C}^T) \cdot \det(\boldsymbol{I}_m + \left(q^2\boldsymbol{I}_m + \boldsymbol{C}\boldsymbol{C}^T\right)^{-1}\boldsymbol{d}_m\boldsymbol{d}_m^T) \quad (23) \\
&= \prod_{i=1}^{m}\left(q^2 + s_i^2\right) \cdot \left(1 + \boldsymbol{d}_m^T\left(q^2\boldsymbol{I}_m + \boldsymbol{C}\boldsymbol{C}^T\right)^{-1}\boldsymbol{d}_m\right) \quad (24) \\
&\geq \prod_{i=1}^{m}\left(q^2 + s_i^2\right) \cdot \left(1 + \frac{\boldsymbol{d}_m^T\boldsymbol{d}_m}{q^2 + s_1^2}\right) \quad (25) \\
&= \prod_{i=1}^{m}\left(q^2 + s_i^2\right) + \prod_{i=2}^{m}\left(q^2 + s_i^2\right)\boldsymbol{d}_m^T\boldsymbol{d}_m \\
&\geq q^{2m} + q^{2m-2}\sum_{i=1}^{m}s_i^2 + q^{2m-2}\boldsymbol{d}_m^T\boldsymbol{d}_m \quad (26) \\
&= q^{2m-2}\left(q^2 + \sum_{i=1}^{m}\left((q + \sum_j c_{ij})^2 + \sum_j c_{ij}^2\right)\right) \\
&\geq q^{2m-2}(q^2 + m) \quad (27) \\
&\geq q^{2m-2}(1 + m). \quad (28)
\end{aligned}$$

Here (23) is derived by identity $\det(\boldsymbol{A} + \boldsymbol{B}) = \det(\boldsymbol{A}) \cdot \det(\boldsymbol{I} + \boldsymbol{A}^{-1}\boldsymbol{B})$. (24) is derived by noting that $\left(q^2\boldsymbol{I}_m + \boldsymbol{C}\boldsymbol{C}^T\right)^{-1}\boldsymbol{d}_m\boldsymbol{d}_m^T$ is a dyadic product matrix of a column vector $\left(q^2\boldsymbol{I}_m + \boldsymbol{C}\boldsymbol{C}^T\right)^{-1}\boldsymbol{d}_m$ and a row vector $\boldsymbol{d}_m^T$, and applying the matrix-determinant lemma [21, p. 446], i.e. $\det(\boldsymbol{I} + \boldsymbol{u}\boldsymbol{v}^T) = 1 + \boldsymbol{v}^T\boldsymbol{u}$. (25) is derived by Rayleigh-Ritz theorem [23, p. 176]. To establish (26), we begin by applying the inequality $\prod_{i=1}^{m}\left(q^2 + s_i^2\right) \geq q^{2m} + q^{2m-2}\sum_{i=1}^{m}s_i^2$ which provides a lower bound for the first term, and subsequently employ the inequality $\prod_{i=2}^{m}\left(q^2 + s_i^2\right) \geq q^{2m-2}$ on the last term. (27) is obtained from the fact that $q \geq 1$, and for each i we have $(q + \sum_j c_{ij})^2 + \sum_j c_{ij}^2 \geq 1$ holds. This is because the result is always a non-zero integer for any $c_{ij} \in \mathbb{Z}$ and $q \in \mathbb{Z}^+$.

Combining (22) and (28), we obtain the unified lower bound

$$\det(\boldsymbol{D}\boldsymbol{A}\boldsymbol{D}^T) \geq q^{2m-2}\max\{m + 1, R(q, \boldsymbol{C})^2\}. \quad (29)$$

Therefore

$$\begin{aligned}
&\sum_{q=1}^{\infty}\sum_{\boldsymbol{D}\in\mathcal{D}_q}\frac{1}{s^{mn}}\left(\frac{q^{m-1}}{\sqrt{\det(\boldsymbol{D}\boldsymbol{A}\boldsymbol{D}^T)}}\right)^n \\
&\leq \frac{1}{s^{mn}}\sum_{q=1}^{\infty}\sum_{\substack{\boldsymbol{C}\in\mathbb{Z}^{m\times(\alpha-1-m)} \\ \boldsymbol{C}\neq\boldsymbol{0}}}\max\{m + 1, R(q, \boldsymbol{C})^2\}^{-n/2}. \quad (30)
\end{aligned}$$

We split the last sum according to whether $R(q, \boldsymbol{C})^2 \leq m+1$ or $R(q, \boldsymbol{C})^2 > m+1$.

– If $R(q,\boldsymbol{C})^2 \le m+1$, then the number of possible integer tuples $(q,\boldsymbol{C})$ is at most $(2\sqrt{m+1}+1)^t$. Hence this part is bounded by

$$\frac{(2\sqrt{m+1}+1)^t}{s^{mn}(m+1)^{n/2}} \le 3^t \frac{(m+1)^{t/2}}{s^{mn}(m+1)^{n/2}}. \tag{31}$$

– If $R(q,\boldsymbol{C})^2 > m+1$, then, since $R(q,\boldsymbol{C})^2$ is an integer, $R(q,\boldsymbol{C}) \ge \sqrt{m+2}$. To bound the remaining series, note that the number of pairs $(q,\boldsymbol{C})$ with $R(q,\boldsymbol{C})^2 = r$ is at most $(2\sqrt{r}+1)^t$, and so

$$\begin{aligned}
&\sum_{q,\boldsymbol{C}\,:\,R(q,\boldsymbol{C})^2>m+1} \frac{1}{R(q,\boldsymbol{C})^n} \le \sum_{r=m+2}^{\infty} \frac{(2\sqrt{r}+1)^t}{r^{n/2}} \le \sum_{r=m+2}^{\infty} \frac{(3\sqrt{r})^t}{r^{n/2}} \\
&= 3^t \sum_{r=m+2}^{\infty} r^{-(n-t)/2} \le 3^t \int_{m+1}^{\infty} x^{-(n-t)/2} dx \\
&= 3^t \left(\frac{2}{n-t-2} (m+1)^{-(n-t-2)/2} \right) \le 3^t 2 \frac{(m+1)^{(t+2)/2}}{(m+1)^{n/2}}
\end{aligned} \tag{32}$$

assuming $n \ge t+3$.

Combining (31) and (32), we find that (30) is upper bounded by

$$3^{t+1} 2 \frac{(m+1)^{(t+2)/2}}{s^{mn}(m+1)^{n/2}}.$$

□

B Proof of Lemma 7

Proof. After permuting the columns, one may write $\widetilde{\boldsymbol{D}} = \big(q\boldsymbol{I}_m \mid \boldsymbol{C}\big)$, where $\boldsymbol{I}_m$ is the $m \times m$ identity matrix and $\boldsymbol{C}$ is an $m \times (\alpha - 1 - m)$ integer matrix all of whose entries are coprime to q. Let $N(\boldsymbol{C}, q)$ denote the number of vectors $\boldsymbol{x} \in (\mathbb{Z}/q\mathbb{Z})^m$ satisfying $\boldsymbol{C}^T\boldsymbol{x} \equiv \boldsymbol{0} \pmod q$. Then by [40, Lem. 1] we have

$$e_1 e_2 \cdots e_m \;=\; N(\boldsymbol{C}, q) \;=\; \begin{cases} q^m, & \text{if } \boldsymbol{C} = \boldsymbol{0}, \\ \le q^{m-1}, & \text{if } \boldsymbol{C} \ne \boldsymbol{0}. \end{cases} \tag{33}$$

Therefore

$$\sum_{m=1}^{\alpha-2}\sum_{\boldsymbol{\nu},\boldsymbol{\mu}}\sum_{q=1}^{\infty}\sum_{\tilde{\boldsymbol{D}}}\left(\frac{e_1}{q}\frac{e_2}{q}\cdots\frac{e_m}{q}\right)^n\left(\frac{q}{s}\right)^{mn}\det(\tilde{\boldsymbol{D}}\boldsymbol{A}\tilde{\boldsymbol{D}}^T)^{-n/2}$$

$$\leq\sum_{m=1}^{\alpha-2}\sum_{\boldsymbol{\nu},\boldsymbol{\mu}}\frac{1}{s^{mn}}\left(\frac{q^{nm}}{\det((q\boldsymbol{I},\boldsymbol{C})\boldsymbol{A}\,(q\boldsymbol{I},\boldsymbol{C})^T)^{\frac{n}{2}}}\bigg|_{\substack{q=1\\ \boldsymbol{C}=\boldsymbol{0}}}+\sum_{q=1}^{\infty}\sum_{\tilde{\boldsymbol{D}}}\frac{q^{n(m-1)}}{\det(\tilde{\boldsymbol{D}}\boldsymbol{A}\tilde{\boldsymbol{D}}^T)^{\frac{n}{2}}}\bigg|_{\boldsymbol{C}\neq\boldsymbol{0}}\right) \tag{34}$$

$$\leq\sum_{m=1}^{\alpha-2}\sum_{\boldsymbol{\nu},\boldsymbol{\mu}}\frac{1}{s^{mn}}\left(\left(\frac{q^m}{\sqrt{\det((q\boldsymbol{I},\boldsymbol{C})\boldsymbol{A}\,(q\boldsymbol{I},\boldsymbol{C})^T)}}\right)^n\bigg|_{\substack{q=1\\ \boldsymbol{C}=\boldsymbol{0}}}+\sum_{q=1}^{\infty}\sum_{\boldsymbol{D}\in\mathcal{D}_q(\boldsymbol{P}_{\boldsymbol{\nu},\boldsymbol{\mu}})}\left(\frac{q^{m-1}}{\sqrt{\det(\boldsymbol{D}\boldsymbol{A}\boldsymbol{D}^T)}}\right)^n\right). \tag{35}$$

Here (34) is derived from (33). The case $\boldsymbol{C}=\boldsymbol{0}$ only appears when $q=1$, since 1 is the only positive integer coprime with 0. (35) is derived by relaxing matrices $\tilde{\boldsymbol{D}}$ that require elements of $\boldsymbol{C}$ coprime with q to matrices $\boldsymbol{D}$ with nonzero $\boldsymbol{C}$. The notation $\mathcal{D}_q(\boldsymbol{P}_{\boldsymbol{\nu},\boldsymbol{\mu}})$ in (35) represents a set of matrices for permutation matrix $\boldsymbol{P}_{\boldsymbol{\nu},\boldsymbol{\mu}}$, which is defined as a $m\times m$ permutation matrix with $(\boldsymbol{P}_{\boldsymbol{\nu},\boldsymbol{\mu}})_{\nu_i,i}=1$ for $i=1,2,\ldots,m$. For any permutation matrix $\boldsymbol{P}$, $\mathcal{D}_q(\boldsymbol{P})$ is defined as

$$\mathcal{D}_q(\boldsymbol{P})\triangleq\{\boldsymbol{D}\in\mathbb{Z}^{m\times(\alpha-1)}:\boldsymbol{D}\boldsymbol{P}=(q\boldsymbol{I}_m,\boldsymbol{C}),\ \text{where }\boldsymbol{C}\in\mathbb{Z}^{m\times(\alpha-1-m)},\boldsymbol{C}\neq\boldsymbol{0}\}.$$

We show in Lemma 12 (Appendix A) that for $t=m(\alpha-1-m)+1$ and $K_{m,\alpha}$ as above, for $n\geq t+3$,

$$\sum_{q=1}^{\infty}\sum_{\boldsymbol{D}\in\mathcal{D}_q(\boldsymbol{P})}\left(\frac{q^{m-1}}{s^m\sqrt{\det(\boldsymbol{D}\boldsymbol{A}\boldsymbol{D}^T)}}\right)^n\leq\frac{K_{m,\alpha}}{s^{mn}(m+1)^{\frac{n}{2}}}=O\left(\frac{1}{s^{mn}(m+1)^{\frac{n}{2}}}\right) \tag{36}$$

Note that the relaxation in (35) only enlarges the summation domain, so it preserves the upper bound. Moreover, the leading order already appears in the contribution with $q=1$ and $\boldsymbol{C}=\boldsymbol{0}$, while the enlarged nonzero-$\boldsymbol{C}$ part is bounded by Lemma 12; hence the relaxation only changes the multiplicative constant. Continuing from (35), we have

$$\sum_{m=1}^{\alpha-2}\sum_{\boldsymbol{\nu},\boldsymbol{\mu}}\sum_{q=1}^{\infty}\sum_{\tilde{\boldsymbol{D}}}\left(\frac{e_1}{q}\frac{e_2}{q}\cdots\frac{e_m}{q}\right)^n\left(\frac{q}{s}\right)^{mn}\det(\tilde{\boldsymbol{D}}\boldsymbol{A}\tilde{\boldsymbol{D}}^T)^{-n/2}$$

$$\leq\sum_{m=1}^{\alpha-2}\sum_{\boldsymbol{\nu},\boldsymbol{\mu}}(1+K_{m,\alpha})\frac{1}{s^{mn}(m+1)^{\frac{n}{2}}} \tag{37}$$

$$\leq\sum_{m=1}^{\alpha-2}\binom{\alpha-1}{m}\frac{1+K_{m,\alpha}}{s^{mn}(m+1)^{\frac{n}{2}}}=O\left(\max_{1\leq m\leq\alpha-2}\frac{1}{s^{mn}(m+1)^{\frac{n}{2}}}\right). \tag{38}$$

Here (37) is derived by computing the first term and applying (36) to the second term. Moreover, $K_{m,\alpha}$ is bounded above by a constant depending only on m and α, and the number of divisions $(\boldsymbol{\nu}, \boldsymbol{\mu})$ for fixed m is $\binom{\alpha-1}{m}$. Since m ranges from 1 to $\alpha - 2$, this gives (38). □

C Bounds for the Rényi flatness factor of Construction A lattices

C.1 Notations

For a pdf $f : \mathbb{R}^n \to \mathbb{R}^{\geq 0}$ and $j > 0$, we define the capped L^j-norm integral as

$$\|f\|_j^j \triangleq \int_{\mathbb{R}^n} f(\boldsymbol{x})^j \, d\boldsymbol{x},$$

For notational convenience, we define $\|f\|_0^0 = 1$. Another notation is

$$\sum_{k_1+\cdots+k_i=i}$$

where the summation is over i nonnegative integers $k_1, \ldots, k_i$ satisfying $k_1 + \cdots + k_i = i$.

The key tool in our analysis is understanding the behavior of lattice point distributions. Let $\mathcal{C}_p(n,k)$ denote the set of all $[n,k]_p$-linear codes over $\mathbb{F}_p^n$. For any $\boldsymbol{m} \in \mathbb{F}_p^k$, let

$$\varphi_{\boldsymbol{x}}(\boldsymbol{G}, \boldsymbol{m}) \triangleq \rho_s(\boldsymbol{x} + \gamma \cdot \boldsymbol{G}\boldsymbol{m} + \gamma \cdot p\mathbb{Z}^n) = \sum_{\boldsymbol{v} \bmod p = \boldsymbol{G}\boldsymbol{m}} \rho_s(\boldsymbol{x} + \gamma \boldsymbol{v}),$$

where $\boldsymbol{G} \in \mathbb{F}_p^{n \times k}$ is the generator matrix for the code $C \in \mathcal{C}_p(n,k)$. For any non-zero codeword $\bar{\boldsymbol{v}} = \boldsymbol{G}\boldsymbol{m} \in \mathbb{F}_p^n \setminus \{\boldsymbol{0}\}$, we abbreviate $\varphi_{\boldsymbol{x}}(\boldsymbol{G}, \boldsymbol{m})$ as $\varphi_{\boldsymbol{x}}(\bar{\boldsymbol{v}})$. Leveraging the uniform distribution of codewords $\boldsymbol{G}\boldsymbol{m}$ over $\mathbb{F}_p^n$ for random $\boldsymbol{G}$, Lemma 8 simplifies to:

$$\begin{aligned} \mathbb{E}_{\boldsymbol{G} \sim \mathcal{C}_p(n,k)} \left[\sum_{\boldsymbol{m} \in \mathbb{F}_p^k \setminus \{\boldsymbol{0}\}} \varphi_{\boldsymbol{x}}(\boldsymbol{G}, \boldsymbol{m}) \right] &= \frac{p^k - 1}{p^n - 1} \sum_{\bar{\boldsymbol{v}} \in \mathbb{F}_p^n \setminus \{\boldsymbol{0}\}} \varphi_{\boldsymbol{x}}(\bar{\boldsymbol{v}}) \\ &\sim \frac{1}{V} \int_{\mathbb{R}^n} \rho_s(\boldsymbol{x} + \boldsymbol{v}) \, d\boldsymbol{v} \end{aligned} \tag{39}$$

as $p \to \infty$, $\gamma \to 0$, $\gamma^n p^{n-k} = V$. In the analysis that follows, we normalize the fundamental volume $V = 1$ for simplicity. For convenience, we shall write $\mathbb{E}_{\boldsymbol{G}}$ instead of $\mathbb{E}_{C \sim \mathcal{C}_p(n,k)}$ in what follows.

C.2 Average Behavior

To estimate $\epsilon_{\Lambda_C}^{(\alpha)}(s)$ and $\rho_s^{(\alpha)}(\Lambda_C^*)$ for lattices Λ_C in Loeliger's ensemble (see Section 3.3), we need to extend (39) to higher moments. The main challenge is to control the recursive structure of higher-order moment functions while maintaining tight approximation bounds as $n \to \infty$.

To address this challenge, we extend the averaging framework by defining the following moment functions on $\boldsymbol{x} \in \mathbb{R}^n$,

$$S_{i,j}(\boldsymbol{x}) \triangleq \begin{cases} \mathbb{E}_{\boldsymbol{G}}\left[\left(\sum_{\boldsymbol{m}\in\mathbb{F}_p^k} \varphi_{\boldsymbol{x}}(\boldsymbol{G},\boldsymbol{m})\right)^i\right], & \text{if } i \in \mathbb{N}^+ \text{ and } j = 0. \\ \mathbb{E}_{\boldsymbol{G}}\left[\left(\sum_{\boldsymbol{m}\in\mathbb{F}_p^k} \varphi_{\boldsymbol{x}}(\boldsymbol{G},\boldsymbol{m})\right)^i \sum_{\boldsymbol{m}'\in\mathbb{F}_p^k} \varphi_{\boldsymbol{x}}(\boldsymbol{G},\boldsymbol{m}')^j\right], & \text{if } i \in \mathbb{N} \text{ and } j \geq 1. \end{cases}$$

The $S_{i,j}(\boldsymbol{x})$ exhibit recursive structure. For instance, $S_{0,0}(\boldsymbol{x}) = 1$ and $S_{i,0}(\boldsymbol{x}) = S_{i-1,1}(\boldsymbol{x})$ for $i \in \mathbb{N}^+$ establishes a recursive link between orders. In this way, in order to obtain all the terms $S_{i,j}(\boldsymbol{x})$ it is sufficient to compute

$$S_{0,j}(\boldsymbol{x}) = \varphi_{\boldsymbol{x}}(\boldsymbol{0})^j + \frac{p^k - 1}{p^n - 1} \sum_{\bar{\boldsymbol{v}}\in\mathbb{F}_p^n\setminus\{\boldsymbol{0}\}} \varphi_{\boldsymbol{x}}(\bar{\boldsymbol{v}})^j, \quad j \geq 1.$$

Having introduced the functions, we proceed as follows. We first relate $\epsilon_{\Lambda_C}^{(\alpha)}(s)$ to the $(\alpha-1)$-st moment $S_{\alpha-1,0}(\boldsymbol{x})$. A recursive decomposition then expresses higher moments entirely in terms of the base layer $S_{0,j}(\boldsymbol{x})$. Next, we employ careful approximation analysis to control the continuous limit behavior under appropriate parameter scaling. Combining these ingredients yields exponential decay in n for the remaining contributions, establishing the desired bounds.

This strategy requires precise threshold conditions on the parameter s and polynomial scaling of the Loeliger ensemble parameters.

Technical Foundation. Our analysis relies on two key technical results that control both the recursive behavior and approximation accuracy.

Proposition 2 (Recursive Bounds)**.** *Based on the notation above, $\forall \boldsymbol{x} \in \mathbb{R}^n$, the following recurrence relation holds for $i, j \in \mathbb{N}^+$:*

$$S_{i,j}(\boldsymbol{x}) \leq p^i S_{i-1,j+1}(\boldsymbol{x}) + S_{0,j}(\boldsymbol{x}) S_{i-1,1}(\boldsymbol{x}), \tag{40}$$

Furthermore, for any subset $T \subseteq \{1,\ldots,i\}$, there exists a sequence of positive integers $\boldsymbol{a}_T = (a_{T,1},\ldots,a_{T,r})$ such that:

$$S_{i,1} \leq \sum_{T\subseteq\{1,\ldots,i\}} \left(\prod_{t\in T} p^t\right) \prod_{l=1}^{r} S_{0,a_{T,l}}, \tag{41}$$

where $r = i - |T| + 1$ and $\sum_{l=1}^{r} a_{T,l} = i + 1$. More precisely, $a_{T,l} = \tau_{l-1} - \tau_l$ for $l = 1,\ldots,r$, where $T^c = \{1,\ldots,i\} \setminus T = \{\tau_1,\ldots,\tau_{r-1}\}$ with $i \geq \tau_1 > \cdots > \tau_{r-1} \geq 1$.

Proof. The second claim follows by repeatedly calling for the first claim. For details, see Appendix D. □

Lemma 13 (Approximation Control)**.** *Let $\gamma^n p^{n-k} = 1$ and $j \in \mathbb{N}_{\geq 1}$. Fix any $\delta \in (0, 1]$. If $n \geq 2$ and $\frac{j\gamma^2}{\pi} \log(\frac{8n}{\delta}) \leq s^2 \leq \frac{(p\gamma)^2}{j \log(\frac{8n}{\delta})}$, the following bounds hold:*

$$S_{0,j}(\boldsymbol{x}) \leq \varphi_{\boldsymbol{x}}(\mathbf{0})^j + \|\rho_s\|_j^j (1+\delta)^j,$$
$$\int_{\mathbb{R}^n} \rho_s(\boldsymbol{x}) \varphi_{\boldsymbol{x}}(\mathbf{0})^j \, d\boldsymbol{x} \leq \|\rho_s\|_{j+1}^{j+1} (1+\delta)^j.$$

Proof. See Appendix E. □

Remark 4. Fix $R = \frac{k}{n} \in (0, 1)$ and $j \in \mathbb{N}_{\geq 1}$. For applications, one can choose $\delta = \delta_n = e^{-\omega(n)}$, for example $\delta_n = e^{-n \log n} = n^{-n}$. We can set prime p as

$$p = p(n) = \Theta(n^\beta) \quad \text{with} \quad \beta > \frac{1}{2 \min(R, 1-R)},$$

and set $\gamma = \gamma(n) = p^{R-1}$. We have $\frac{j\gamma^2}{\pi} \log(\frac{8n}{\delta}) \to 0$ and $\frac{(p\gamma)^2}{j \log(\frac{8n}{\delta})} \to \infty$, so the interval condition in Lemma 13 eventually holds for any fixed $s > 0$ when n is sufficiently large.

These technical tools provide the foundation for our analysis. Proposition 2 expresses arbitrary higher-order moments entirely in terms of the base functions $S_{0,j}(\boldsymbol{x})$, which are easier to analyze via Lemma 8. Lemma 13 establishes tight control over the Riemann approximation errors, crucial for managing the transition from discrete lattice sums to integrals while maintaining the exponential accuracy required for our final bounds.

Armed with these technical tools, we are now ready to establish our main result for the average behavior in the $\alpha \geq 2$ regime.

C.3 Detailed Proof of Theorem 7

Proof. We proceed through the three-step strategy outlined above.

Step 1: Establishing the connection between $\epsilon_{\Lambda_C}^{(\alpha)}(s)$ and $S_{\alpha-1,0}(\boldsymbol{x})$.
From the averaging identity established in our previous analysis, and applying Jensen's inequality (for $z \mapsto z^{\frac{1}{\alpha-1}}$), we have:

$$\begin{aligned}
\mathbb{E}_{\mathcal{C}_p(n,k)}\left[\epsilon_{\Lambda_C}^{(\alpha)}(s)\right] &= \mathbb{E}_{\mathcal{C}_p(n,k)}\left[\left(\int_{\mathcal{R}(\Lambda_C)} \rho_{s,\Lambda_C}(\boldsymbol{x})^\alpha d\boldsymbol{x}\right)^{\frac{1}{\alpha-1}} - 1\right] \\
&\leq \left(\mathbb{E}_{\mathcal{C}_p(n,k)}\left[\int_{\mathcal{R}(\Lambda_C)} \rho_{s,\Lambda_C}(\boldsymbol{x})^\alpha d\boldsymbol{x}\right]\right)^{\frac{1}{\alpha-1}} - 1
\end{aligned}$$

And it can be derived that

$$\begin{aligned}
\mathbb{E}_{\mathcal{C}_p(n,k)}\left[\int_{\mathcal{R}(\Lambda_C)} \rho_{s,\Lambda_C}(\boldsymbol{x})^{\alpha} d\boldsymbol{x}\right] &= \mathbb{E}_{\mathcal{C}_p(n,k)}\left[\int_{\mathcal{R}(\Lambda_C)} \sum_{\boldsymbol{v}\in\Lambda_C} \rho_s(\boldsymbol{x}+\boldsymbol{v})\rho_{s,\Lambda_C}(\boldsymbol{x})^{\alpha-1} d\boldsymbol{x}\right] \\
&= \mathbb{E}_{\mathcal{C}_p(n,k)}\left[\sum_{\boldsymbol{v}\in\Lambda_C} \int_{\mathcal{R}(\Lambda_C)} \rho_s(\boldsymbol{x}+\boldsymbol{v})\rho_{s,\Lambda_C}(\boldsymbol{x})^{\alpha-1} d\boldsymbol{x}\right] \\
&= \mathbb{E}_{\mathcal{C}_p(n,k)}\left[\sum_{\boldsymbol{v}\in\Lambda_C} \int_{\mathcal{R}(\Lambda_C)+\boldsymbol{v}} \rho_s(\boldsymbol{y})\rho_{s,\Lambda_C}(\boldsymbol{y})^{\alpha-1} d\boldsymbol{y}\right] \\
&= \int_{\mathbb{R}^n} \rho_s(\boldsymbol{y})\mathbb{E}_{\mathcal{C}_p(n,k)}\left[\rho_{s,\Lambda_C}(\boldsymbol{y})^{\alpha-1}\right] d\boldsymbol{y} \\
&= \int_{\mathbb{R}^n} \rho_s(\boldsymbol{y}) S_{\alpha-1,0}(\boldsymbol{y})\, d\boldsymbol{y} \qquad (42)
\end{aligned}$$

Note that $S_{\alpha-1,0}(\boldsymbol{y}) = S_{\alpha-2,1}(\boldsymbol{y})$. Denote the target integral as $\mathcal{I}_{\alpha-2}$:

$$\mathcal{I}_{\alpha-2} = \int_{\mathbb{R}^n} \rho_s(\boldsymbol{x}) S_{\alpha-2,1}(\boldsymbol{x}) d\boldsymbol{x}$$

In summary, we obtain:

$$\mathbb{E}_{\mathcal{C}_p(n,k)}[\epsilon^{(\alpha)}_{\Lambda_C}(s)] \le \mathcal{I}_{\alpha-2}^{\frac{1}{\alpha-1}} - 1 \qquad (43)$$

Step 2: Recursive decomposition to base functions.

Continuing from (42), we apply Proposition 2 and then use the first statement of Lemma 13 for $j \le \alpha-1$, we expand $\int \rho_s(\boldsymbol{x}) \prod_l S_{0,a_{T,l}}(\boldsymbol{x}) d\boldsymbol{x}$ by substituting the upper bounds and partitioning the index set $\{1,\dots,r(T)\}$ into disjoint subsets I (main terms) and J (error terms):

$$\begin{aligned}
\mathcal{I}_{\alpha-2} &= \int_{\mathbb{R}^n} \rho_s(\boldsymbol{x}) S_{\alpha-2,1}(\boldsymbol{x}) d\boldsymbol{x} \\
&\le \sum_{T\subseteq\{1,\dots,\alpha-2\}} \left(\prod_{t\in T} p^t\right) \int_{\mathbb{R}^n} \rho_s(\boldsymbol{x}) \prod_{l=1}^{r(T)} S_{0,a_{T,l}}(\boldsymbol{x}) d\boldsymbol{x} \\
&\le \sum_{T\subseteq\{1,\dots,\alpha-2\}} \left(\prod_{t\in T} p^t\right) \int_{\mathbb{R}^n} \rho_s(\boldsymbol{x}) \prod_{l=1}^{r(T)} \left(\varphi_{\boldsymbol{x}}(0)^{a_{T,l}} + (1+\delta)^{a_{T,l}} \|\rho_s\|_{a_{T,l}}^{a_{T,l}}\right) d\boldsymbol{x} \\
&\le (1+\delta)^{\alpha-1} \sum_{T\subseteq\{1,\dots,\alpha-2\}} \left(\prod_{t\in T} p^t\right) \underbrace{\sum_{\substack{I\cup J=\{1,\dots,r(T)\} \\ I\cap J=\emptyset}} \|\rho_s\|_{1+\sum_{l\in I} a_{T,l}}^{1+\sum_{l\in I} a_{T,l}} \prod_{l\in J} \|\rho_s\|_{a_{T,l}}^{a_{T,l}}}_{(i)},
\end{aligned} \qquad (44)$$

where in the last step we use the second statement of Lemma 13.

We now prove the asymptotic bound. Note that the sums in the expression for $\mathcal{I}_{\alpha-2}$ (specifically within (i)) are finite, and their structure depends solely on α. The terms involved are products of norms $\|\rho_s\|_\beta^\beta$ with factors in $p(n)$, where p is polynomial in n. Assuming that $s > \alpha^{-\frac{1}{2(\alpha-1)}}$, since $g(\beta) = \beta^{-\frac{1}{2(\beta-1)}}$ is non-decreasing when $\beta > 1$,

$$\|\rho_s\|_\beta^\beta = \frac{1}{s^{n(\beta-1)}\beta^{\frac{n}{2}}} \to 0$$

exponentially fast as $n \to \infty$. As in Remark 4, one can choose $\delta = n^{-n} = e^{-\omega(n)}$ when $p = \Theta(n^\beta)$ with $\beta > \frac{1}{2\min(R,\,1-R)}$. Thus, we can retain only the exponential term with the dominant convergence rate as

$$\begin{aligned}\mathbb{E}_{\mathcal{C}_p(n,k)}\left[\epsilon_{\Lambda_C}^{(\alpha)}(s)\right] &\le \left(1 + \max_{2\le\beta\le\alpha} \frac{1}{\left(s^{(\beta-1)}\sqrt{\beta}\right)^{n(1-o(1))}}\right)^{\frac{1}{\alpha-1}} - 1 \\ &= \max_{2\le\beta\le\alpha} \frac{1}{\left(s^{(\beta-1)}\sqrt{\beta}\right)^{n(1-o(1))}}.\end{aligned}$$

Here the term "1+" is from $T = I = \emptyset, J = \{1, \cdots, \alpha-1\}$ and $a_{T,l} = 1$ for $l \in J$. The proof of the asymptotic statement is completed as follows. Consider $h(\beta) := \frac{1}{s^{\beta-1}\sqrt{\beta}}, \beta \in [2, \alpha]$. Note that $\log h(\beta) = -(\beta-1)\log s - \frac{1}{2}\log\beta$ is convex in β, since $\frac{d^2}{d\beta^2}\log h(\beta) = \frac{1}{2\beta^2} > 0$. Hence $h(\beta)$ is log-convex on $[2, \alpha]$, and therefore its maximum over the interval is attained at an endpoint, i.e. $\beta = \alpha$ or $\beta = 2$.

Step 3: Summation analysis

Here we follow similar ideas from [32, Sec. 3]. To obtain a precise non-asymptotic closed-form upper bound, we proceed with analyzing (i). Note that we keep $\delta \in (0, 1]$ as a free approximation parameter and the following summation bounds hold uniformly for any such δ. We first observe that the total degree of norms in any term of (i) is conserved: $\left(1 + \sum_{l\in I} a_{T,l}\right) + \sum_{l\in J} a_{T,l} = 1 + \sum_{l=1}^{r(T)} a_{T,l} = \alpha$. Using Lyapunov's inequality [20, Thm. 17]

$$\|f\|_q^q \le \|f\|_{q_0}^{q_0(1-\theta)} \cdot \|f\|_{q_1}^{q_1\theta} \quad \text{for } q = (1-\theta)q_0 + \theta q_1,\ \theta \in (0,1)$$

with $q_0 = 1, q_1 = \alpha$, we have $\|\rho_s\|_q^q \le (\|\rho_s\|_\alpha^\alpha)^{\frac{q-1}{\alpha-1}}$ for $q \in [1, \alpha]$. Applying this to the product terms in (i) we find:

$$\begin{aligned}\|\rho_s\|_{1+\sum_{l\in I} a_{T,l}}^{1+\sum_{l\in I} a_{T,l}} \prod_{l\in J} \|\rho_s\|_{a_{T,l}}^{a_{T,}} &\le (\|\rho_s\|_\alpha^\alpha)^{\frac{(1+\sum_{l\in I} a_{T,l})-1}{\alpha-1}} \prod_{l\in J} (\|\rho_s\|_\alpha^\alpha)^{\frac{a_{T,l}-1}{\alpha-1}} \\ &= (\|\rho_s\|_\alpha^\alpha)^{\frac{\alpha-1-|J|}{\alpha-1}} = \|\rho_s\|_\alpha^\alpha \cdot \left((\|\rho_s\|_\alpha^\alpha)^{-\frac{1}{\alpha-1}}\right)^{|J|}.\end{aligned}$$

The general term depends only on the size of the set J. Summing over all possible subsets J using the binomial theorem, we bound (i):

$$(i) \le \sum_{|J|=0}^{r(T)} \binom{r(T)}{|J|} \|\rho_s\|_\alpha^\alpha \left((\|\rho_s\|_\alpha^\alpha)^{-\frac{1}{\alpha-1}}\right)^{|J|} = \|\rho_s\|_\alpha^\alpha \left(1 + (\|\rho_s\|_\alpha^\alpha)^{-\frac{1}{\alpha-1}}\right)^{r(T)}.$$

Substituting this back into the expression for $\mathcal{I}_{\alpha-2}$, summing over paths T, and applying algebraic simplification we obtain:

$$\begin{aligned}
\mathcal{I}_{\alpha-2} &\leq (1+\delta)^{\alpha-1} \sum_{T\subseteq\{1,\ldots,\alpha-2\}} \left(\prod_{t\in T} p^t\right) \|\rho_s\|_\alpha^\alpha \left(1+(\|\rho_s\|_\alpha^\alpha)^{-\frac{1}{\alpha-1}}\right)^{r(T)} \\
&= (1+\delta)^{\alpha-1} \|\rho_s\|_\alpha^\alpha \left(1+(\|\rho_s\|_\alpha^\alpha)^{-\frac{1}{\alpha-1}}\right) \sum_{T\subseteq\{1,\ldots,\alpha-2\}} \left(\prod_{t\in T} p^t\right) \\
&\qquad \cdot \left(1+(\|\rho_s\|_\alpha^\alpha)^{-\frac{1}{\alpha-1}}\right)^{\alpha-2-|T|} \\
&= (1+\delta)^{\alpha-1} \|\rho_s\|_\alpha^\alpha \left(1+(\|\rho_s\|_\alpha^\alpha)^{-\frac{1}{\alpha-1}}\right) \prod_{t=1}^{\alpha-2} \left(1+(\|\rho_s\|_\alpha^\alpha)^{-\frac{1}{\alpha-1}}+p^t\right) \\
&\leq (1+\delta)^{\alpha-1} \left[(\|\rho_s\|_\alpha^\alpha)^{\frac{1}{\alpha-1}} \left(1+(\|\rho_s\|_\alpha^\alpha)^{-\frac{1}{\alpha-1}}+p^{\alpha-2}\right)\right]^{\alpha-1} \\
&= (1+\delta)^{\alpha-1} \left[1+(1+p^{\alpha-2}) \|\rho_s\|_\alpha^{\frac{\alpha}{\alpha-1}}\right]^{\alpha-1}.
\end{aligned}$$

This yields the final closed-form upper bound. Substituting back into (43), we obtain:

$$\mathbb{E}_{\mathcal{C}_p(n,k)}[\epsilon_{\Lambda_C}^{(\alpha)}(s)] \leq (1+\delta)(1+p^{\alpha-2}) s^{-n} \alpha^{-\frac{n}{2(\alpha-1)}} + \delta.$$

□

D Proof of Proposition 2

Proof. For simplicity, we write $S_{i,j}(\boldsymbol{x})$ as $S_{i,j}$ throughout this proof, because $\boldsymbol{x}$ remains fixed.

1. We begin with proof of the recurrence relation claim of $S_{i,j} \leq p^i S_{i-1,j+1} + S_{0,j} S_{i-1,1}$ for $i \in \mathbb{N}^+$ and $j \geq 1$.

$$\begin{aligned}
S_{i,j} &= \mathbb{E}_{\boldsymbol{G}}\left[\left(\sum_{\boldsymbol{m}\in\mathbb{F}_p^k} \varphi_{\boldsymbol{x}}(\boldsymbol{G},\boldsymbol{m})\right)^i \sum_{\boldsymbol{m}'\in\mathbb{F}_p^k} \varphi_{\boldsymbol{x}}(\boldsymbol{G},\boldsymbol{m}')^j\right] \\
&= \mathbb{E}_{\boldsymbol{G}}\left[\sum_{\boldsymbol{m}_1,\ldots,\boldsymbol{m}_i\in\mathbb{F}_p^k} \prod_{l=1}^i \varphi_{\boldsymbol{x}}(\boldsymbol{G},\boldsymbol{m}_l) \sum_{\boldsymbol{m}'\in\mathbb{F}_p^k} \varphi_{\boldsymbol{x}}(\boldsymbol{G},\boldsymbol{m}')^j\right] \\
&= \underbrace{\mathbb{E}_{\boldsymbol{G}}\left[\sum_{\boldsymbol{m}_1,\ldots,\boldsymbol{m}_i\in\mathbb{F}_p^k} \prod_{l=1}^i \varphi_{\boldsymbol{x}}(\boldsymbol{G},\boldsymbol{m}_l) \sum_{\boldsymbol{m}'\in U_i\setminus\{\boldsymbol{0}\}} \varphi_{\boldsymbol{x}}(\boldsymbol{G},\boldsymbol{m}')^j\right]}_{(i)} + \\
&\underbrace{\sum_{\boldsymbol{m}_1,\ldots,\boldsymbol{m}_i\in\mathbb{F}_p^k} \mathbb{E}_{\boldsymbol{G}\boldsymbol{m}_{1:i}}\left[\prod_{l=1}^i \varphi_{\boldsymbol{x}}(\boldsymbol{G},\boldsymbol{m}_l)\left(\varphi_{\boldsymbol{x}}(\boldsymbol{0})^j + \mathbb{E}_{\boldsymbol{G}|\boldsymbol{G}\boldsymbol{m}_{1:i}}\left[\sum_{\boldsymbol{m}'\notin U_i} \varphi_{\boldsymbol{x}}(\boldsymbol{G},\boldsymbol{m}')^j\right]\right)\right]}_{(ii)}.
\end{aligned} \tag{45}$$

Here we denote $\boldsymbol{G}\boldsymbol{m}_{1:i} = \{\boldsymbol{G}\boldsymbol{m}_1, \ldots, \boldsymbol{G}\boldsymbol{m}_i\}$, $U_i = \mathrm{span}\{\boldsymbol{m}_1, \ldots, \boldsymbol{m}_i\}$, and divide the vectors of $\boldsymbol{m}'$'s into two parts depending on whether they belong to $U_i \backslash \{\boldsymbol{0}\}$ or not. For vectors not in U_i, we split the expectation into conditional fixed codewords $\{\boldsymbol{G}\boldsymbol{m}_1, \ldots, \boldsymbol{G}\boldsymbol{m}_i\}$ in the last step. Now we estimate (i) and (ii) separately.
To estimate (i), we need the following inequality.

Lemma 14 (Rearrangement Inequality, [20])**.** *Let $a_1 \le a_2 \le \cdots \le a_n$ and $b_1 \le b_2 \le \cdots \le b_n$ be sequences of real numbers. Then,*

$$a_1 b_1 + a_2 b_2 + \cdots + a_n b_n \ge a_{s(1)} b_1 + a_{s(2)} b_2 + \cdots + a_{s(n)} b_n,$$

for any permutation s of $\{1, 2, \ldots, n\}$.

Now we begin with

$$\sum_{\boldsymbol{m}_1, \ldots, \boldsymbol{m}_i \in \mathbb{F}_p^*} \prod_{\ell=1}^{i} \varphi_{\boldsymbol{x}}(\boldsymbol{G}, \boldsymbol{m}_\ell) \sum_{\boldsymbol{m}' \in U_i} \varphi_{\boldsymbol{x}}(\boldsymbol{G}, \boldsymbol{m})^j.$$

Since any $\boldsymbol{m}'$ can be written as $\boldsymbol{m} = \sum_{\ell=1}^{i} d_\ell \, \boldsymbol{m}_\ell$ with $d = (d_1, \ldots, d_i) \in \mathbb{F}_p^i \setminus \{0\}$, this becomes

$$\sum_{\boldsymbol{m}_1, \ldots, \boldsymbol{m}_i \in \mathbb{F}_p^*} \prod_{\ell=1}^{i} \varphi_{\boldsymbol{x}}(\boldsymbol{G}, \boldsymbol{m}_\ell) \sum_{\substack{\boldsymbol{d}=(d_1, \ldots, d_i) \in \mathbb{F}_p^i \\ \boldsymbol{d} \neq 0}} \varphi_{\boldsymbol{x}}\Big(\boldsymbol{G}, \sum_{\ell=1}^{i} d_\ell \, \boldsymbol{m}_\ell\Big)^j,$$

where some linear combinations may coincide. Re-ordering the sums, we obtain

$$\sum_{\boldsymbol{d} \in \mathbb{F}_p^i \backslash \{0\}} \sum_{\boldsymbol{m}_1, \ldots, \boldsymbol{m}_i \in \mathbb{F}_p^*} \Big(\prod_{\ell=1}^{i} \varphi_{\boldsymbol{x}}(\boldsymbol{G}, \boldsymbol{m}_\ell) \Big) \, \varphi_{\boldsymbol{x}}\Big(\boldsymbol{G}, \sum_{\ell=1}^{i} d_\ell \, \boldsymbol{m}_\ell\Big)^j.$$

Now set

$$i_0(\boldsymbol{d}) \;=\; \min\{\ell : d_\ell \neq 0\},$$

and group according to which coordinate is first nonzero:

$$(*) = \sum_{\boldsymbol{d} \neq 0} \sum_{\substack{\boldsymbol{m}_1, \ldots, \boldsymbol{m}_{i_0 - 1}, \\ \boldsymbol{m}_{i_0+1}, \ldots, \boldsymbol{m}_i \in \mathbb{F}_p^*}} \Big(\prod_{\substack{\ell=1 \\ \ell \neq i_0}}^{i} \varphi_{\boldsymbol{x}}(\boldsymbol{G}, \boldsymbol{m}_\ell) \Big) \sum_{\boldsymbol{m}_{i_0} \in \mathbb{F}_p^*} \varphi_{\boldsymbol{x}}(\boldsymbol{G}, \boldsymbol{m}_{i_0}) \, \varphi_{\boldsymbol{x}}\Big(\boldsymbol{G}, \sum_{\ell=1}^{i} d_\ell \, \boldsymbol{m}_\ell\Big)^j.$$

Note that as $\boldsymbol{m}_{i_0}$ runs through $\mathbb{F}_p^*$, since $d_{i_0} \neq 0$, the linear combination $\sum_\ell d_\ell \, \boldsymbol{m}_\ell$ also runs through $\mathbb{F}_p^*$. Hence by the "crypto-lemma" $\varphi_{\boldsymbol{x}}\big(\boldsymbol{G}, \sum_\ell d_\ell \boldsymbol{m}_\ell\big)$ is just a permutation of $\varphi_{\boldsymbol{x}}(\boldsymbol{G}, \boldsymbol{m}_{i_0})$.
Applying Lemma 14 to the term $(*)$ gives

$$(*) \;\le \sum_{\boldsymbol{d} \neq 0} \sum_{\boldsymbol{m}_1, \ldots, \boldsymbol{m}_i \in \mathbb{F}_p^*} \Big(\prod_{\ell \neq i_0} \varphi_{\boldsymbol{x}}(\boldsymbol{G}, \boldsymbol{m}_\ell) \Big) \sum_{\boldsymbol{m}_{i_0} \in \mathbb{F}_p^*} \varphi_{\boldsymbol{x}}(\boldsymbol{G}, \boldsymbol{m}_{i_0})^{\,j+1}.$$

Since $\sum_{\boldsymbol{d}\neq 0} 1 = p^i - 1$ and the remaining products factor,

$$(i) \leq (p^i-1)\mathbb{E}_{\boldsymbol{G}}\Big(\sum_{\boldsymbol{m}\in\mathbb{F}_p^*}\varphi_{\boldsymbol{x}}(\boldsymbol{G},\boldsymbol{m})\Big)^{i-1}\sum_{\boldsymbol{m}\in\mathbb{F}_p^*}\varphi_{\boldsymbol{x}}(\boldsymbol{G},\boldsymbol{m})^{j+1} \;<\; p^i\, S_{i-1,j+1}, \tag{46}$$

Now we estimate (ii). The Gaussian binomial coefficient, denoted

$$\begin{bmatrix} n \\ k \end{bmatrix}_p = \frac{(1-p^n)(1-p^{n-1})\cdots(1-p^{n-k+1})}{(1-p^k)(1-p^{k-1})\cdots(1-p)},$$

counts the number of k-dimensional subspaces of an n-dimensional vector space over $\mathbb{F}_p$. Denote $V = \mathrm{span}\{\boldsymbol{G}\boldsymbol{m}_1,\ldots,\boldsymbol{G}\boldsymbol{m}_i\}$ and then $V^\perp$ as the complement linear space of V with $\dim(V^\perp) = n - \dim(V)$. Thus

$$\mathbb{F}_p^n = V \oplus V^\perp.$$

If V is fixed, the number of linear codes in $\mathcal{C}_p(n,k)$ containing V is $\begin{bmatrix} n-\dim(V) \\ k-\dim(V) \end{bmatrix}_p$ and the number of linear codes in $\mathcal{C}_p(n,k)$ both containing V and a given $\bar{\boldsymbol{v}} \notin V$ is $\begin{bmatrix} n-\dim(V)-1 \\ k-\dim(V)-1 \end{bmatrix}_p$. Note that $\bar{\boldsymbol{v}}$ is a combination of vectors from V and $V^\perp$. Thus we have

$$\begin{aligned}
\mathbb{E}_{\boldsymbol{G}|\boldsymbol{G}\boldsymbol{m}_{1:i}}\left[\sum_{\boldsymbol{m}\notin U_i}\varphi_{\boldsymbol{x}}(\boldsymbol{G},\boldsymbol{m})^j\right] &= \frac{\begin{bmatrix} n-\dim(V)-1 \\ k-\dim(V)-1 \end{bmatrix}_p}{\begin{bmatrix} n-\dim(V) \\ k-\dim(V) \end{bmatrix}_p}\sum_{\bar{\boldsymbol{v}}\notin V}\varphi_{\boldsymbol{x}}(\bar{\boldsymbol{v}})^j \\
= \frac{p^{k-\dim(V)}-1}{p^{n-\dim(V)}-1}\sum_{\bar{\boldsymbol{v}}\notin V}\varphi_{\boldsymbol{x}}(\bar{\boldsymbol{v}})^j &\leq \frac{p^k-1}{p^n-1}\sum_{\bar{\boldsymbol{v}}\in\mathbb{F}_p^n\setminus\{\boldsymbol{0}\}}\varphi_{\boldsymbol{x}}(\bar{\boldsymbol{v}})^j
\end{aligned}$$

Thus

$$\begin{aligned}
(ii) &\leq \sum_{\boldsymbol{m}_1,\ldots,\boldsymbol{m}_i\in\mathbb{F}_p^k}\mathbb{E}_{\boldsymbol{G}\boldsymbol{m}_{1:i}}\left[\prod_{l=1}^i\varphi_{\boldsymbol{x}}(\boldsymbol{G},\boldsymbol{m}_l)\right]\left(\varphi_{\boldsymbol{x}}(\boldsymbol{0})^j + \frac{p^k-1}{p^n-1}\sum_{\bar{\boldsymbol{v}}\in\mathbb{F}_p^n\setminus\{\boldsymbol{0}\}}\varphi_{\boldsymbol{x}}(\bar{\boldsymbol{v}})^j\right) \\
&= S_{0,j}\mathbb{E}_{\boldsymbol{G}}\left[\sum_{\boldsymbol{m}_1,\ldots,\boldsymbol{m}_i\in\mathbb{F}_p^k}\prod_{l=1}^i\varphi_{\boldsymbol{x}}(\boldsymbol{G},\boldsymbol{m}_l)\right] \\
&= S_{0,j}S_{i-1,1}.
\end{aligned} \tag{47}$$

Substituting inequalities (46) and (47) into (45) yields the proof of the first claim of (40).

2. Now we prove the claim of (41) by iteratively applying the recurrence relation starting from $S_{i,1}$. The process can be modeled as a path on a recursion tree

from level $t = i$ down to $t = 0$. At each step t, we apply the recurrence ((40)) to $S_{t,k}$:

$$S_{t,k} \leq p^t S_{t-1,k+1} + S_{0,k} S_{t-1,1}$$

Each application of the recurrence produces two "branches":

- P-branch (Power branch), corresponding to the first term. This contributes a weight p^t, increments the second index $k \to k+1$, and proceeds to $S_{t-1,k+1}$.
- S-branch (Standard branch), corresponding to the second term. This factors out a base term $S_{0,k}$, resets the second index to 1, and proceeds to $S_{t-1,1}$.

Any expansion path is uniquely identified by the set of indices $T \subseteq \{1, \ldots, i\}$, where the P-branch is chosen. The complement set $T^c = \{1, \ldots, i\} \setminus T$ corresponds to the steps where the S-branch is chosen.

To explicitly determine $a_{T,l}$, we sort the elements of T^c in descending order:

$$T^c = \{\tau_1, \tau_2, \ldots, \tau_{r-1}\} \quad \text{satisfying } i \geq \tau_1 > \tau_2 > \cdots > \tau_{r-1} \geq 1$$

For convenience, we define boundary points $\tau_0 = i + 1$ and $\tau_r = 0$. The total number of generated base terms is $r = |T^c| + 1 = i - |T| + 1$ (the $+1$ comes from the termination at $t = 0$).

The terms $S_{0,a_{T,l}}$ are generated at levels $t \in T^c \cup \{0\}$. The index $a_{T,l}$ corresponds to the value of the second parameter k accumulated between two consecutive S-branches (or boundaries). Specifically, for each interval (τ_l, τ_{l-1}), all steps t with $\tau_l < t < \tau_{l-1}$ belong to T (i.e., are P-branches).

(a) At step τ_{l-1} (or the start), the index k is reset to 1 (if $\tau_{l-1} \leq i$) or starts at 1 (if $\tau_{l-1} = i + 1$).

(b) For each step $t \in T$ in the range $\tau_l < t < \tau_{l-1}$, the index k increments by 1. The number of such steps is $(\tau_{l-1} - 1) - \tau_l$.

Therefore, at the moment of generating the term at τ_l, the index value is:

$$a_{T,l} = 1 + \sum_{t=\tau_l+1}^{\tau_{l-1}-1} 1 = 1 + (\tau_{l-1} - \tau_l - 1) = \tau_{l-1} - \tau_l.$$

This defines the sequence $\boldsymbol{a}_T = (a_{T,1}, \ldots, a_{T,r})$ strictly based on the gaps between S-branches. The total weight for the path T is the product of weights from all P-branches: $W_T = \prod_{t \in T} p^t$. Noting that $\sum_{l=1}^{r} a_{T,l} = \sum_{l=1}^{r} (\tau_{l-1} - \tau_l) = \tau_0 - \tau_r = i + 1$ completes the proof.

□

E Proof of Lemma 13

Proof. Fix $j \in \mathbb{N}_{\geq 1}$ and $\boldsymbol{x} \in \mathbb{R}^n$. We first establish a bound on the Fourier transform of the product of Gaussians. Assuming $\boldsymbol{u}_0 = \boldsymbol{0}$ and $\rho_s(\boldsymbol{y}) = \frac{1}{s^n} e^{-\pi \|\boldsymbol{y}\|^2 / s^2}$,

we compute the Fourier transform in $\boldsymbol{v}$ of $\prod_{r=0}^{j-1}\rho_s(\boldsymbol{x}+\boldsymbol{v}+\boldsymbol{u}_r)$ as follows:

$$
\begin{aligned}
&\mathcal{F}\left\{\prod_{r=0}^{j-1}\rho_s(\boldsymbol{x}+\boldsymbol{v}+\boldsymbol{u}_r)\right\}(\boldsymbol{\xi})\\
&=e^{2\pi\mathrm{i}\langle\boldsymbol{x},\boldsymbol{\xi}\rangle}\int_{\mathbb{R}^n}\frac{1}{s^{jn}}\exp\Big(-\tfrac{\pi}{s^2}\sum_{r=0}^{j-1}\|\boldsymbol{v}+\boldsymbol{u}_r\|^2\Big)e^{-2\pi\mathrm{i}\langle\boldsymbol{\xi},\boldsymbol{v}\rangle}\,d\boldsymbol{v}\\
&=e^{2\pi\mathrm{i}\langle\boldsymbol{x},\boldsymbol{\xi}\rangle}\exp\left(\frac{\frac{1}{j}\left\|\sum_{r=1}^{j-1}\boldsymbol{u}_r\right\|^2-\sum_{r=1}^{j-1}\|\boldsymbol{u}_r\|^2}{s^2}\right)\\
&\qquad\cdot\int_{\mathbb{R}^n}\frac{1}{s^{jn}}e^{-\frac{\pi j}{s^2}\|\boldsymbol{v}+\frac{1}{j}\sum_{r=0}^{j-1}\boldsymbol{u}_r\|^2-2\pi\mathrm{i}\langle\boldsymbol{\xi},\boldsymbol{v}\rangle}\,d\boldsymbol{v} \qquad (48)\\
&=\exp\left(\frac{\frac{1}{j}\left\|\sum_{r=1}^{j-1}\boldsymbol{u}_r\right\|^2-\sum_{r=1}^{j-1}\|\boldsymbol{u}_r\|^2}{s^2}+2\pi\mathrm{i}\,\langle\boldsymbol{x}+\boldsymbol{u}',\boldsymbol{\xi}\rangle\right)\mathcal{F}\left\{\frac{1}{s^{jn}}e^{-\frac{\pi j\|\boldsymbol{v}\|^2}{s^2}}\right\}(\boldsymbol{\xi}) \qquad (49)\\
\Rightarrow\ &\left|\mathcal{F}\left\{\prod_{r=0}^{j-1}\rho_s(\boldsymbol{x}+\boldsymbol{v}+\boldsymbol{u}_r)\right\}(\boldsymbol{\xi})\right|\le\exp\left(-\frac{1}{s^2j}\sum_{r=1}^{j-1}\|\boldsymbol{u}_r\|^2\right)\cdot\frac{1}{s^{n(j-1)}j^{n/2}}e^{-\frac{\pi s^2}{j}\|\boldsymbol{\xi}\|^2}. \qquad (50)
\end{aligned}
$$

Here (48) uses the identity $\sum_{r=0}^{j-1}\|\boldsymbol{v}+\boldsymbol{u}_r\|^2=j\big\|\boldsymbol{v}+\frac{1}{j}\sum_{r=0}^{j-1}\boldsymbol{u}_r\big\|^2+\sum_{r=0}^{j-1}\|\boldsymbol{u}_r\|^2-j\big\|\frac{1}{j}\sum_{r=0}^{j-1}\boldsymbol{u}_r\big\|^2$. In (49) we used the phase shift property with $\boldsymbol{u}'=-\frac{1}{j}\sum_{r=1}^{j-1}\boldsymbol{u}_r$. Finally, (50) follows from Cauchy–Schwarz $\left\|\sum_{r=1}^{j-1}\boldsymbol{u}_r\right\|^2\le(j-1)\sum_{r=1}^{j-1}\|\boldsymbol{u}_r\|^2$ and $\left|e^{2\pi\mathrm{i}\langle\boldsymbol{x}+\boldsymbol{u}',\boldsymbol{\xi}\rangle}\right|=1$.

With this Fourier bound, we can now present the proof of the lemma. For $j\in\mathbb{N}^+$, it can be derived that

$$
\begin{aligned}
S_{0,j}(\boldsymbol{x})&=\varphi_{\boldsymbol{x}}(\boldsymbol{0})^j+\frac{p^k-1}{p^n-1}\sum_{\bar{\boldsymbol{v}}\in\mathbb{F}_p^n\setminus\{\boldsymbol{0}\}}\varphi_{\boldsymbol{x}}(\bar{\boldsymbol{v}})^j\\
&\le\varphi_{\boldsymbol{x}}(\boldsymbol{0})^j+p^{k-n}\sum_{\bar{\boldsymbol{v}}\in\mathbb{F}_p^n\setminus\{\boldsymbol{0}\}}\left(\sum_{\boldsymbol{u}\in p\gamma\mathbb{Z}^n}\rho_s(\boldsymbol{x}+\gamma\bar{\boldsymbol{v}}+\boldsymbol{u})\right)^j\\
&=\varphi_{\boldsymbol{x}}(\boldsymbol{0})^j+p^{k-n}\sum_{\bar{\boldsymbol{v}}\in\gamma\mathbb{F}_p^n\setminus\{\boldsymbol{0}\}}\sum_{\boldsymbol{u}\in p\gamma\mathbb{Z}^n}\sum_{\boldsymbol{u}_1,\ldots,\boldsymbol{u}_{j-1}\in p\gamma\mathbb{Z}^n}\prod_{r=0}^{j-1}\rho_s(\boldsymbol{x}+\bar{\boldsymbol{v}}+\boldsymbol{u}+\boldsymbol{u}_r)\\
&=\varphi_{\boldsymbol{x}}(\boldsymbol{0})^j+\sum_{\boldsymbol{u}_1,\ldots,\boldsymbol{u}_{j-1}\in p\gamma\mathbb{Z}^n}p^{k-n}\sum_{\bar{\boldsymbol{v}}\in\gamma\mathbb{F}_p^n\setminus\{\boldsymbol{0}\}}\sum_{\boldsymbol{u}\in p\gamma\mathbb{Z}^n}\prod_{r=0}^{j-1}\rho_s(\boldsymbol{x}+\bar{\boldsymbol{v}}+\boldsymbol{u}+\boldsymbol{u}_r)
\end{aligned}
$$

$$
\begin{aligned}
&\le \varphi_{\boldsymbol{x}}(\mathbf{0})^j + \sum_{\boldsymbol{u}_1,\dots,\boldsymbol{u}_{j-1}\in p\gamma\mathbb{Z}^n} p^{k-n} \sum_{\boldsymbol{v}\in\gamma\mathbb{Z}^n} \prod_{r=0}^{j-1} \rho_s(\boldsymbol{x}+\boldsymbol{v}+\boldsymbol{u}_r) \\
&\overset{(a)}{=} \varphi_{\boldsymbol{x}}(\mathbf{0})^j + \sum_{\boldsymbol{u}_1,\dots,\boldsymbol{u}_{j-1}\in p\gamma\mathbb{Z}^n} \frac{1}{p^{n-k}\gamma^n} \sum_{\boldsymbol{\xi}\in\frac{1}{\gamma}\mathbb{Z}^n} \mathcal{F}\left\{\prod_{r=0}^{j-1} \rho_s(\boldsymbol{x}+\boldsymbol{v}+\boldsymbol{u}_r)\right\}(\boldsymbol{\xi}) \\
&\overset{(b)}{\le} \varphi_{\boldsymbol{x}}(\mathbf{0})^j + \sum_{\boldsymbol{u}_1,\dots,\boldsymbol{u}_{j-1}\in p\gamma\mathbb{Z}^n} \sum_{\boldsymbol{\xi}\in\frac{1}{\gamma}\mathbb{Z}^n} e^{-\frac{1}{s^2 j}\sum_{r=1}^{j-1}\|\boldsymbol{u}_r\|^2} \cdot \frac{1}{s^{n(j-1)} j^{n/2}} e^{-\frac{\pi s^2}{j}\|\boldsymbol{\xi}\|^2} \\
&= \varphi_{\boldsymbol{x}}(\mathbf{0})^j + \frac{1}{s^{n(j-1)} j^{n/2}} \Bigg(\sum_{\boldsymbol{\xi}\in\frac{1}{\gamma}\mathbb{Z}^n} e^{-\frac{\pi s^2}{j}\|\boldsymbol{\xi}\|^2} \Bigg) \Bigg(\sum_{\boldsymbol{u}\in p\gamma\mathbb{Z}^n} e^{-\frac{1}{s^2 j}\|\boldsymbol{u}\|^2} \Bigg)^{j-1}
\end{aligned}
$$

where (a) follows by the Poisson summation formula, (b) follows by (50), and we used $\frac{p^k-1}{p^n-1} \le p^{k-n}$ and the unit-volume condition $\gamma^n p^{n-k} = 1$.

Noting that $\|\rho_s\|_j^j = \frac{1}{s^{n(j-1)} j^{n/2}}$, it remains to bound the two lattice Gaussian sums. Write

$$
\sum_{\boldsymbol{\xi}\in\frac{1}{\gamma}\mathbb{Z}^n} e^{-\frac{\pi s^2}{j}\|\boldsymbol{\xi}\|^2} = \Big(\sum_{t\in\mathbb{Z}} e^{-\frac{\pi s^2}{j\gamma^2} t^2} \Big)^n, \qquad \sum_{\boldsymbol{u}\in p\gamma\mathbb{Z}^n} e^{-\frac{1}{s^2 j}\|\boldsymbol{u}\|^2} = \Big(\sum_{t\in\mathbb{Z}} e^{-\frac{(p\gamma)^2}{j s^2} t^2} \Big)^n.
$$

Under the assumption $\frac{j\gamma^2}{\pi}\log(8n/\delta) \le s^2 \le \frac{(p\gamma)^2}{j\log(8n/\delta)}$, we have $\frac{\pi s^2}{j\gamma^2} \ge \log(8n/\delta)$ and $\frac{(p\gamma)^2}{j s^2} \ge \log(8n/\delta)$. Note that for $Q \ge \log(8n/\delta)$,

$$
\sum_{t\in\mathbb{Z}} e^{-Qt^2} = 1 + 2\sum_{t\ge 1} e^{-Qt^2} \le 1 + 2\sum_{t\ge 1} e^{-Qt} = 1 + \frac{2e^{-Q}}{1-e^{-Q}} \le 1 + 4e^{-Q} \le 1 + \frac{\delta}{2n},
$$

where we used $1 - e^{-Q} \ge 1 - \frac{\delta}{8n} \ge \frac{1}{2}$ (since $n \ge 2, \delta \le 1$). Therefore for $n \ge 2$,

$$
\Big(\sum_{t\in\mathbb{Z}} e^{-Qt^2} \Big)^n \le \Big(1 + \frac{\delta}{2n} \Big)^n \le \exp(\delta/2) \le 1 + \delta,
$$

where we used $e^x \le 1 + 2x$ for $x \in [0, 1/2]$ (here $x = \delta/2$). Applying this with $Q = \frac{\pi s^2}{j\gamma^2}$ and $Q = \frac{(p\gamma)^2}{j s^2}$ gives

$$
\sum_{\boldsymbol{\xi}\in\frac{1}{\gamma}\mathbb{Z}^n} e^{-\frac{\pi s^2}{j}\|\boldsymbol{\xi}\|^2} \le 1 + \delta, \qquad \sum_{\boldsymbol{u}\in p\gamma\mathbb{Z}^n} e^{-\frac{1}{s^2 j}\|\boldsymbol{u}\|^2} \le 1 + \delta.
$$

Plugging these bounds into the expanded form of $S_{0,j}(\boldsymbol{x})$ yields

$$
S_{0,j}(\boldsymbol{x}) \le \varphi_{\boldsymbol{x}}(\mathbf{0})^j + \|\rho_s\|_j^j (1+\delta)^j,
$$

which proves the first inequality.

For the second inequality, we write

$$\int_{\mathbb{R}^n} \rho_s(\boldsymbol{x})\, \varphi_{\boldsymbol{x}}(\mathbf{0})^j \, d\boldsymbol{x} = \int_{\mathbb{R}^n} \rho_s(\boldsymbol{x}) \Big(\sum_{\boldsymbol{u} \in p\gamma\mathbb{Z}^n} \rho_s(\boldsymbol{x}+\boldsymbol{u}) \Big)^j \, d\boldsymbol{x}$$
$$= \sum_{\boldsymbol{u}_1,\dots,\boldsymbol{u}_j \in p\gamma\mathbb{Z}^n} \int_{\mathbb{R}^n} \rho_s(\boldsymbol{x}) \prod_{r=1}^{j} \rho_s(\boldsymbol{x}+\boldsymbol{u}_r)\, d\boldsymbol{x}. \tag{51}$$

Similarly to (50), we have

$$\begin{aligned}
&\int_{\mathbb{R}^n} \rho_s(\boldsymbol{x}) \prod_{r=1}^{j} \rho_s(\boldsymbol{x}+\boldsymbol{u}_r)\, d\boldsymbol{x} \\
&= \frac{1}{s^{n(j+1)}} \int_{\mathbb{R}^n} \exp\left(-\frac{\pi}{s^2} ((j+1)\|\boldsymbol{x}\|^2 + 2 < \boldsymbol{x}, \sum_{r=1}^{j} \boldsymbol{u}_r > + \sum_{r=1}^{j} \|\boldsymbol{u}_r\|^2) \right) d\boldsymbol{x} \\
&= \exp\left(\frac{\pi}{s^2} \left(\frac{1}{j+1} \left\| \sum_{r=1}^{j} \boldsymbol{u}_r \right\|^2 - \sum_{r=1}^{j} \|\boldsymbol{u}_r\|^2 \right) \right) \int_{\mathbb{R}^n} \frac{1}{s^{n(j+1)}} \exp\left(-\frac{\pi(j+1)}{s^2} \left\| \boldsymbol{x} + \frac{1}{j+1} \sum_{r=1}^{j} \boldsymbol{u}_r \right\|^2 \right) d\boldsymbol{x} \\
&\le \exp\Big(-\frac{\pi}{(j+1)s^2} \sum_{r=1}^{j} \|\boldsymbol{u}_r\|^2 \Big) \int_{\mathbb{R}^n} \rho_s(\boldsymbol{x})^{j+1}\, d\boldsymbol{x}.
\end{aligned}$$

Since $\frac{\pi}{j+1} \ge \frac{1}{j}$ for all $j \ge 1$, we further have

$$\exp\Big(-\frac{\pi}{(j+1)s^2} \sum_{r=1}^{j} \|\boldsymbol{u}_r\|^2 \Big) \le \exp\Big(-\frac{1}{js^2} \sum_{r=1}^{j} \|\boldsymbol{u}_r\|^2 \Big).$$

Substituting this into (51) and factorizing the sum yields

$$\int_{\mathbb{R}^n} \rho_s(\boldsymbol{x})\, \varphi_{\boldsymbol{x}}(\mathbf{0})^j \, d\boldsymbol{x} \le \|\rho_s\|_{j+1}^{j+1} \Big(\sum_{\boldsymbol{u} \in p\gamma\mathbb{Z}^n} e^{-\frac{1}{s^2 j}\|\boldsymbol{u}\|^2} \Big)^j \le \|\rho_s\|_{j+1}^{j+1} (1+\delta)^j.$$

This completes the proof. □

F Lemmas in Application Section

F.1 Proof of Lemma 9

Proof. By definition,

$$\begin{aligned}
\mathbb{D}_\alpha(D_{\Lambda,s,\boldsymbol{c}} \bmod \Lambda' || \mathcal{U}_{\Lambda/\Lambda'})^{\alpha-1} &= \sum_{\boldsymbol{x} \in \Lambda/\Lambda'} |\Lambda/\Lambda'|^{\alpha-1} \left((D_{\Lambda,s,\boldsymbol{c}} \bmod \Lambda')(\boldsymbol{x}) \right)^\alpha \\
&= |\Lambda/\Lambda'|^{\alpha-1} \sum_{\boldsymbol{x} \in \Lambda/\Lambda'} \frac{\left(\sum_{\boldsymbol{\lambda}' \in \Lambda'} \rho_s(\boldsymbol{\lambda}' + \boldsymbol{x} - \boldsymbol{c}) \right)^\alpha}{\left(\sum_{\boldsymbol{\lambda} \in \Lambda} \rho_s(\boldsymbol{\lambda} - \boldsymbol{c}) \right)^\alpha}
\end{aligned}$$

Applying the Poisson summation formula to the numerator and denominator, we obtain

$$|\Lambda/\Lambda'|^{\alpha-1}\left(\frac{V(\Lambda)}{V(\Lambda')}\right)^{\alpha}\sum_{\boldsymbol{x}\in\Lambda/\Lambda'}\frac{\left(\sum_{\boldsymbol{\lambda}\in(\Lambda')^*}e^{-\pi s^2\|\boldsymbol{\lambda}\|^2}e^{2\pi\mathrm{i}\langle\boldsymbol{x}-\boldsymbol{c},\boldsymbol{\lambda}\rangle}\right)^{\alpha}}{\left(\sum_{\boldsymbol{\lambda}\in\Lambda^*}e^{-\pi s^2\|\boldsymbol{\lambda}\|^2}e^{-2\pi\mathrm{i}\langle\boldsymbol{c},\boldsymbol{\lambda}\rangle}\right)^{\alpha}}$$

$$=\frac{1}{|\Lambda/\Lambda'|}\sum_{\boldsymbol{x}\in\Lambda/\Lambda'}\frac{\sum_{\boldsymbol{\lambda}_1,\ldots,\boldsymbol{\lambda}_\alpha\in(\Lambda')^*}\exp\left(-\pi s^2\sum_{j=1}^{\alpha}\|\boldsymbol{\lambda}_j\|^2\right)\exp(2\pi\mathrm{i}\langle\sum_{j=1}^{\alpha}\boldsymbol{\lambda}_j,\boldsymbol{x}-\boldsymbol{c}\rangle)}{\left(\sum_{\boldsymbol{\lambda}\in\Lambda^*}e^{-\pi s^2\|\boldsymbol{\lambda}\|^2}e^{-2\pi\mathrm{i}\langle\boldsymbol{c},\boldsymbol{\lambda}\rangle}\right)^{\alpha}} \tag{52}$$

By the orthogonality of characters on the finite abelian group Λ/Λ', $\forall\boldsymbol{\eta}\in(\Lambda')^*$,

$$\sum_{\boldsymbol{x}\in\Lambda/\Lambda'}e^{2\pi\mathrm{i}\langle\boldsymbol{\eta},\boldsymbol{x}\rangle}=\begin{cases}|\Lambda/\Lambda'|, & \boldsymbol{\eta}\in\Lambda^*;\\ 0, & \boldsymbol{\eta}\notin\Lambda^*.\end{cases}$$

Therefore (52) is equal to

$$\frac{1}{\left(\sum_{\boldsymbol{\lambda}\in\Lambda^*}e^{-\pi s^2\|\boldsymbol{\lambda}\|^2}e^{-2\pi\mathrm{i}\langle\boldsymbol{c},\boldsymbol{\lambda}\rangle}\right)^{\alpha}}\sum_{\substack{\boldsymbol{\lambda}_1,\ldots,\boldsymbol{\lambda}_\alpha\in(\Lambda')^*\\ \boldsymbol{\lambda}_1+\ldots+\boldsymbol{\lambda}_\alpha\in\Lambda^*}}e^{-\pi s^2(\|\boldsymbol{\lambda}_1\|^2+\ldots+\|\boldsymbol{\lambda}_\alpha\|^2)}e^{-2\pi\mathrm{i}\langle\sum\boldsymbol{\lambda}_j,\boldsymbol{c}\rangle}$$

$$\le\frac{1}{\left|\sum_{\boldsymbol{\lambda}\in\Lambda^*}e^{-\pi s^2\|\boldsymbol{\lambda}\|^2}e^{-2\pi\mathrm{i}\langle\boldsymbol{c},\boldsymbol{\lambda}\rangle}\right|^{\alpha}}\sum_{\substack{\boldsymbol{\lambda}_1,\ldots,\boldsymbol{\lambda}_\alpha\in(\Lambda')^*\\ \boldsymbol{\lambda}_1+\ldots+\boldsymbol{\lambda}_\alpha\in\Lambda^*}}e^{-\pi s^2(\|\boldsymbol{\lambda}_1\|^2+\ldots+\|\boldsymbol{\lambda}_\alpha\|^2)}$$

$$=\frac{\sum_{\boldsymbol{\lambda}_1,\ldots,\boldsymbol{\lambda}_{\alpha-1}\in(\Lambda')^*,\,\boldsymbol{\lambda}\in\Lambda^*}e^{-\pi s^2(\|\boldsymbol{\lambda}_1\|^2+\ldots+\|\boldsymbol{\lambda}_{\alpha-1}\|^2+\left\|\boldsymbol{\lambda}+\sum_{j=1}^{\alpha-1}\boldsymbol{\lambda}_j\right\|^2)}}{\left|\sum_{\boldsymbol{\lambda}\in\Lambda^*}e^{-\pi s^2\|\boldsymbol{\lambda}\|^2}e^{-2\pi\mathrm{i}\langle\boldsymbol{c},\boldsymbol{\lambda}\rangle}\right|^{\alpha}}. \tag{53}$$

To bound this expression, let $\mathbf{L}=(\boldsymbol{\lambda}_1^T,\ldots,\boldsymbol{\lambda}_{\alpha-1}^T)^T\in((\Lambda')^*)^{\alpha-1}$ and consider the all-ones vector $\mathbf{1}\in\mathbb{R}^{\alpha-1}$. A direct algebraic calculation verifies the identity:

$$\sum_{j=1}^{\alpha-1}\|\boldsymbol{\lambda}_j\|^2+\left\|\boldsymbol{\lambda}+\sum_{j=1}^{\alpha-1}\boldsymbol{\lambda}_j\right\|^2=\left(\mathbf{L}+\frac{1}{\alpha}(\mathbf{1}\otimes\boldsymbol{\lambda})\right)^T(\boldsymbol{A}\otimes\boldsymbol{I}_n)\left(\mathbf{L}+\frac{1}{\alpha}(\mathbf{1}\otimes\boldsymbol{\lambda})\right)+\frac{1}{\alpha}\|\boldsymbol{\lambda}\|^2.$$

Then the numerator of the expression (53) can be rewritten as

$$\sum_{\boldsymbol{\lambda}\in\Lambda^*}e^{-\pi s^2\frac{\|\boldsymbol{\lambda}\|^2}{\alpha}}\underbrace{\sum_{\boldsymbol{L}\in((\Lambda')^*)^{\alpha-1}}e^{-\pi s^2\left\|(\boldsymbol{A}^{1/2}\otimes\boldsymbol{I}_n)\left(\mathbf{L}+\frac{1}{\alpha}(\mathbf{1}\otimes\boldsymbol{\lambda})\right)\right\|^2}}_{S(\boldsymbol{\lambda})}. \tag{54}$$

The term $S(\boldsymbol{\lambda})$ is a shifted theta sum over the lattice $\mathcal{L}=(\boldsymbol{A}^{1/2}\otimes\boldsymbol{I}_n)((\Lambda')^*)^{\alpha-1}$. By the standard property of Gaussian theta sums, the mass is maximized at the zero shift, so $S(\boldsymbol{\lambda})\le S(\mathbf{0})$ for all $\boldsymbol{\lambda}$. Therefore, we have shown that

$$\mathbb{D}_\alpha(D_{\Lambda,s,\boldsymbol{c}}\bmod\Lambda'||\mathcal{U}_{\Lambda/\Lambda'})^{\alpha-1}\le\frac{1}{\left|\sum_{\boldsymbol{\lambda}\in\Lambda^*}e^{-\pi s^2\|\boldsymbol{\lambda}\|^2}e^{-2\pi\mathrm{i}\langle\boldsymbol{c},\boldsymbol{\lambda}\rangle}\right|^{\alpha}}\sum_{\boldsymbol{\lambda}\in\Lambda^*}e^{-\pi s^2\frac{\|\boldsymbol{\lambda}\|^2}{\alpha}}S(\mathbf{0}).$$

We use the direct relation $S(\mathbf{0}) = R_\alpha(\rho_{s,\Lambda'}||U_{\mathcal{R}(\Lambda')})^{\alpha-1}$ (by equation 7). Substituting this back, we obtain the inequality (18).

Assume now that $s \geq \eta_\epsilon^{(\alpha)}(\Lambda')$ and $s \geq \sqrt{\alpha}\eta_\epsilon^{(\infty)}(\Lambda)$. By the definition of the standard smoothing parameter (Definition 3) and of the Rényi smoothing parameter (Definition 1), we have $\sum_{\boldsymbol{\lambda}\in\Lambda^*} e^{-\pi s^2 \frac{\|\boldsymbol{\lambda}\|^2}{\alpha}} \leq (1+\varepsilon)$ and $S(\mathbf{0}) = R_\alpha(\rho_{s,\Lambda'}||U_{\mathcal{R}(\Lambda')})^{\alpha-1} \leq (1+\varepsilon)^{\alpha-1}$. For the denominator, we have:

$$\left|\sum_{\boldsymbol{\lambda}\in\Lambda^*} e^{-\pi s^2\|\boldsymbol{\lambda}\|^2} e^{-2\pi \mathrm{i}\langle \boldsymbol{c},\boldsymbol{\lambda}\rangle} - 1\right| \leq \sum_{\boldsymbol{\lambda}\in\Lambda^*\setminus\{\mathbf{0}\}} e^{-\pi s^2\|\boldsymbol{\lambda}\|^2} \leq \epsilon.$$

This implies that $\left|\sum_{\boldsymbol{\lambda}\in\Lambda^*} e^{-\pi s^2\|\boldsymbol{\lambda}\|^2} e^{-2\pi \mathrm{i}\langle \boldsymbol{c},\boldsymbol{\lambda}\rangle}\right| \geq 1-\epsilon$. Thus, for $\boldsymbol{c} \neq \mathbf{0}$, the denominator term is lower bounded by $(1-\epsilon)^\alpha$. For $\boldsymbol{c} = \mathbf{0}$, the denominator is $\sum e^{-\pi s^2\|\boldsymbol{\lambda}\|^2} \geq 1$, so we can simply bound the fraction by 1. Substituting these bounds yields the result (19). □

F.2 Convergence of the Smoothing Parameter for Discrete Distributions

Using the discrete Rényi divergence (Definition 6) we can define the Rényi smoothing parameter for discrete distributions as follows.

Definition 8 (Rényi Smoothing Parameter for Discrete Gaussian Distributions). *For a p-ary lattice $p\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Z}^n$, for $\boldsymbol{x} \in \mathbb{Z}^n/\Lambda$, consider the discrete distribution*

$$F_{s,\Lambda}(\boldsymbol{x}) = \frac{\rho_{s,\Lambda}(\boldsymbol{x})}{\rho_s(\mathbb{Z}^n)} = D_{\mathbb{Z}^n,s} \bmod \Lambda(\boldsymbol{x}).$$

The smoothing parameter $\tilde{\eta}_\varepsilon^{(\alpha)}(\Lambda)$ for $\varepsilon > 0$ is defined as the smallest $s > 0$ such that $\mathbb{D}_\alpha(F_{s,\Lambda}\|U_{\mathbb{Z}^n/\Lambda}) \leq 1+\varepsilon$.

Then we have the following Lemma.

Lemma 15. *For fixed n and $k < n$, consider a sequence $\{\mathcal{C}^{(p)}\}$ of $[n,k]_p$ linear codes, the corresponding Construction A lattices $\Lambda^{(p)} = \mathcal{C}^{(p)} + p\mathbb{Z}^n$ with $p\mathbb{Z}^n \subseteq \Lambda^{(p)} \subseteq \mathbb{Z}^n$, and their scaled versions $\bar{\Lambda}^{(p)} = \gamma\Lambda^{(p)}$, where $\gamma = p^{-(1-k/n)}\bar{V}^{1/n}$ is such that $V(\bar{\Lambda}^{(p)}) = \bar{V}$ is fixed. Then*

$$\lim_{p\to\infty} \mathbb{D}_\alpha(F_{s,\Lambda^{(p)}}||\mathcal{U}_{\mathbb{Z}^n/\Lambda^{(p)}}) \leq \lim_{p\to\infty} R_\alpha(\rho_{\gamma s,\bar{\Lambda}^{(p)}}||U_{\mathcal{R}(\bar{\Lambda}^{(p)})})$$

and consequently $\lim_{p\to\infty} \gamma\tilde{\eta}_\varepsilon^{(\alpha)}(\Lambda^{(p)}) \leq \lim_{p\to\infty} \eta_\varepsilon^{(\alpha)}(\bar{\Lambda}^{(p)})$.

Proof. Firstly, we note that $\rho_s(\mathbb{Z}^n) \geq 1$, thus $F_{s,\Lambda^{(p)}}(\boldsymbol{x}) \leq \rho_{s,\Lambda^{(p)}}(\boldsymbol{x})$. Secondly, it is easy to verify that $\rho_{s,\Lambda^{(p)}}(\boldsymbol{x})^\alpha = \rho_{\gamma s,\bar{\Lambda}^{(p)}}(\gamma\boldsymbol{x})^\alpha \gamma^{\alpha n}$. Then,

$$\begin{aligned}\sum_{\boldsymbol{x}\in\mathbb{Z}^n\cap\mathcal{R}(\Lambda^{(p)})} \frac{F_{s,\Lambda^{(p)}}(\boldsymbol{x})^\alpha}{1/|\mathbb{Z}^n/\Lambda|^{\alpha-1}} &\leq \sum_{\boldsymbol{x}\in\mathbb{Z}^n\cap\mathcal{R}(\Lambda^{(p)})} \frac{\rho_{s,\Lambda^{(p)}}(\boldsymbol{x})^\alpha}{1/p^{(\alpha-1)(n-k)}} \\ &= \sum_{\boldsymbol{x}\in\gamma\mathbb{Z}^n\cap\mathcal{R}(\bar{\Lambda}^{(p)})} \frac{\rho_{\gamma s,\bar{\Lambda}^{(p)}}(\boldsymbol{x})^\alpha \gamma^{\alpha n}}{1/p^{(\alpha-1)(n-k)}} \\ &= \sum_{\boldsymbol{x}\in\gamma\mathbb{Z}^n\cap\mathcal{R}(\bar{\Lambda}^{(p)})} \frac{\rho_{\gamma s,\bar{\Lambda}^{(p)}}(\boldsymbol{x})^\alpha \gamma^{n}}{1/(p^{(n-k)}\gamma^n)^{\alpha-1}}.\end{aligned}$$

Since $\gamma \to 0$ as $p \to \infty$, from the definition of Riemann integration we have

$$\lim_{p\to\infty} \sum_{\boldsymbol{x}\in\mathbb{Z}^n\cap\mathcal{R}(\Lambda^{(p)})} \frac{F_{s,\Lambda^{(p)}}(\boldsymbol{x})^\alpha}{1/|\mathbb{Z}^n/\Lambda^{(p)}|^{\alpha-1}} \leq \lim_{p\to\infty} \int_{\mathcal{R}(\bar{\Lambda}^{(p)})} \frac{\rho_{\gamma s,\bar{\Lambda}^{(p)}}(\boldsymbol{x})^\alpha}{1/(\bar{V})^{\alpha-1}} d\boldsymbol{x}.$$

Therefore, we have proven $\lim_{p\to\infty} \mathbb{D}_\alpha(F_{s,\Lambda^{(p)}} \| U_{\mathbb{Z}^n/\Lambda^{(p)}}) \leq \lim_{p\to\infty} R_\alpha(\rho_{\gamma s,\bar{\Lambda}^{(p)}} \| U_{\mathcal{R}(\bar{\Lambda}^{(p)})})$; by definition we have $\lim_{p\to\infty} \gamma\tilde{\eta}_\varepsilon^{(\alpha)}(\Lambda^{(p)}) \leq \lim_{p\to\infty} \eta_\varepsilon^{(\alpha)}(\bar{\Lambda}^{(p)})$. □

F.3 Proof of Lemma 11

Proof. It suffices to prove case $\alpha = 2$ as $s \geq \eta_\varepsilon^{(\alpha)}(\Lambda) \geq \eta_\varepsilon^{(2)}(\Lambda) = \frac{\eta_\varepsilon(\Lambda)}{\sqrt{2}}$.

Let $\boldsymbol{x_c} \in \Lambda$ be a closest lattice point to $\boldsymbol{c}$. Then

$$\begin{aligned}\sum_{\boldsymbol{x}\in\Lambda} e^{-\frac{\pi}{s^2}\|\boldsymbol{x}-\boldsymbol{c}\|^2} &= \sum_{\boldsymbol{x}\in\Lambda} e^{-\frac{\pi}{s^2}\|\boldsymbol{x}+\boldsymbol{x}_c-\boldsymbol{c}\|^2} \\ &= \frac{1}{2} e^{-\frac{\pi}{s^2}\|\boldsymbol{x}_c-\boldsymbol{c}\|^2} \sum_{\boldsymbol{x}\in\Lambda} e^{-\frac{\pi}{s^2}\|\boldsymbol{x}\|^2} \left(e^{-\frac{2\pi}{s^2}\langle\boldsymbol{x},\boldsymbol{x_c}-\boldsymbol{c}\rangle} + e^{\frac{2\pi}{s^2}\langle\boldsymbol{x},\boldsymbol{x_c}-\boldsymbol{c}\rangle}\right) \\ &\geq e^{-\frac{\pi}{s^2}\mu(\Lambda)^2} \sum_{\boldsymbol{x}\in\Lambda} e^{-\frac{\pi}{s^2}\|\boldsymbol{x}\|^2},\end{aligned}$$

where $\mu(\Lambda)$ is the covering radius of Λ.

Based on the inequality above, applying the Poisson summation formula with phase yields

$$\begin{aligned}\mathbb{E}_{\boldsymbol{x}\sim D_{\Lambda,s,\boldsymbol{c}}}\left[e^{\frac{\pi-1/2}{s^2}\|\boldsymbol{x}-\boldsymbol{c}\|^2}\right] &= \frac{\sum_{\boldsymbol{x}\in\Lambda} e^{-\frac{1}{2s^2}\|\boldsymbol{x}-\boldsymbol{c}\|^2}}{\sum_{\boldsymbol{x}\in\Lambda} e^{-\frac{\pi}{s^2}\|\boldsymbol{x}-\boldsymbol{c}\|^2}} \leq e^{\pi\mu(\Lambda)^2/s^2} \frac{\sum_{\boldsymbol{x}\in\Lambda} e^{-\frac{1}{2s^2}\|\boldsymbol{x}-\boldsymbol{c}\|^2}}{\sum_{\boldsymbol{x}\in\Lambda} e^{-\frac{\pi}{s^2}\|\boldsymbol{x}\|^2}} \\ &= e^{\pi\mu(\Lambda)^2/s^2} \frac{(2\pi)^{n/2} \sum_{\boldsymbol{x}\in\Lambda^*} e^{-2\pi^2 s^2\|\boldsymbol{x}\|^2} e^{2\pi\mathrm{i}\langle\boldsymbol{x},\boldsymbol{c}\rangle}}{\sum_{\boldsymbol{x}\in\Lambda^*} e^{-\pi s^2\|\boldsymbol{x}\|^2}} \\ &\leq e^{\pi\mu(\Lambda)^2/s^2}(2\pi)^{n/2}(1+\varepsilon). \qquad (55)\end{aligned}$$

In the last step we used the condition $s \geq \eta_\varepsilon(\Lambda)/\sqrt{2}$ to bound $\sum_{\boldsymbol{x}\in\Lambda^*} e^{-2\pi s^2\|\boldsymbol{x}\|^2} = \varrho_{\sqrt{2}s}(\Lambda^*) \leq 1+\varepsilon$.

Using [3, Lem. 8] which is implicit in [5], for $s \geq \eta_\varepsilon(\Lambda)/\sqrt{2}$, we have the bound

$$\frac{\mu(\Lambda)}{s} \leq \frac{\sqrt{2}\mu(\Lambda)}{\eta_\varepsilon(\Lambda)} \leq \sqrt{\frac{n}{2}}.$$

Combining (55) with this bound and applying Markov's inequality gives

$$\begin{aligned}
\Pr_{\boldsymbol{x}\sim D_{\Lambda,s,\boldsymbol{c}}}[\|\boldsymbol{x}-\boldsymbol{c}\| > s\sqrt{n}] &= \Pr_{\boldsymbol{x}\sim D_{\Lambda,s,\boldsymbol{c}}}\left[\exp\big(\frac{\pi-1/2}{s^2}\|\boldsymbol{x}-\boldsymbol{c}\|^2\big) > \exp\big((\pi-1/2)n\big)\right] \\
&\leq \mathbb{E}_{\boldsymbol{x}\sim D_{\Lambda,s,\boldsymbol{c}}}\left[\exp\left(\frac{\pi-1/2}{s^2}\|\boldsymbol{x}-\boldsymbol{c}\|^2\right)\right]/e^{(\pi-1/2)n} \\
&\leq e^{\pi\mu(\Lambda)^2/s^2}(2\pi)^{n/2}(1+\varepsilon)\cdot e^{-(\pi-1/2)n} \qquad \text{by (55)} \\
&\leq (1+\varepsilon)\exp\left(\frac{\pi n}{2}+\frac{n}{2}\log(2\pi)-n\pi+\frac{n}{2}\right) \\
&= (1+\varepsilon)\exp\left(-n\left[\frac{\pi-1-\log(2\pi)}{2}\right]\right).
\end{aligned}$$

This confirms the exponential decay of the tail probability. □

F.4 Proof of Lemma 10

Proof. By the definition of the Rényi smoothing parameter, any $s \geq \eta_\varepsilon^{(\alpha)}(\Lambda)$ must satisfy $\sum_{\boldsymbol{\lambda}\in(\Lambda^*)^{\alpha-1}\setminus\{\mathbf{0}\}} e^{-\pi s^2\boldsymbol{\lambda}^T(\boldsymbol{A}\otimes\boldsymbol{I}_n)\boldsymbol{\lambda}} \leq \varepsilon_\alpha$. We restrict the sum to a subset of vectors that minimize the quadratic form: (i) tuples with exactly one entry equal to a shortest vector $\boldsymbol{v}\in\Lambda^*$, and (ii) tuples with two entries equal to $\boldsymbol{v}$ and $-\boldsymbol{v}$. Both types yield a quadratic form value of $2\|\boldsymbol{v}\|^2 = 2\lambda_1(\Lambda^*)^2$. Counting the combinatorial possibilities for these tuples (at least $2(\alpha-1)^2$ terms given $\pm\boldsymbol{v}$), we obtain the lower bound:

$$2(\alpha-1)^2\exp\big(-2\pi s^2\lambda_1(\Lambda^*)^2\big) \leq \sum_{\boldsymbol{\lambda}\in(\Lambda^*)^{\alpha-1}\setminus\{\mathbf{0}\}} e^{-\pi s^2\boldsymbol{\lambda}^T(\boldsymbol{A}\otimes\boldsymbol{I}_n)\boldsymbol{\lambda}} \leq \varepsilon_\alpha.$$

Solving for s implies $s \geq \frac{1}{\lambda_1(\Lambda^*)}\sqrt{\frac{\log(2(\alpha-1)^2/\varepsilon_\alpha)}{2\pi}}$. Since A is full rank, there is a bijection $\mathbb{Z}^n/\Lambda \cong \mathbb{Z}_p^m$ and $\det(\Lambda) = p^m$. Using Minkowski's first theorem, $\lambda_1(\Lambda^*) \leq \sqrt{n}\,\det(\Lambda^*)^{1/n} = \sqrt{n}\,p^{-m/n}$. Substituting this into the inequality gives the explicit lower bound:

$$\eta_\varepsilon^{(\alpha)}(\Lambda) \;\geq\; \frac{p^{m/n}}{\sqrt{2\pi n}}\sqrt{\log\left(\frac{2(\alpha-1)^2}{\varepsilon_\alpha}\right)}.$$

Next, we establish the inequality $\frac{1}{\sqrt{\alpha}}\eta_\varepsilon^{(\alpha)}(\Lambda) \geq \eta_\varepsilon(\mathbb{Z}^n)$. Recall that $\eta_\varepsilon(\mathbb{Z}^n) \leq \sqrt{\frac{\log(2n(1+1/\varepsilon))}{\pi}}$ [19, Lem. 2.6]. Then, (20) is guaranteed provided that

$$\frac{p^{2m/n}}{2\alpha n}\log\left(\frac{2(\alpha-1)^2}{\varepsilon_\alpha}\right) \geq \log\big(2n(1+1/\varepsilon)\big) \iff p^{2m/n} \geq 2\alpha n \cdot \frac{\log\big(2n(1+1/\varepsilon)\big)}{\log\big(2(\alpha-1)^2/\varepsilon_\alpha\big)}, \tag{56}$$

as stated.

To derive the sufficient conditions involving $c > 1$, we bound the logarithmic ratio. As $\varepsilon \leq 1/2$ and $\varepsilon \leq 1/(\alpha-1)$, we have $\log(2n(1+1/\varepsilon)) \leq \log(4n/\varepsilon)$ and $\varepsilon_\alpha \leq e(\alpha-1)\varepsilon$. We seek a condition on ε such that the ratio is bounded by c:

$$\frac{\log(4n/\varepsilon)}{\log\big(\frac{2(\alpha-1)}{e\varepsilon}\big)} \leq c \iff \frac{4n}{\varepsilon} \leq \left(\frac{2(\alpha-1)}{e\varepsilon}\right)^c \iff \varepsilon \leq \left(\frac{2(\alpha-1)}{e}\right)^{\frac{c}{c-1}} (4n)^{-\frac{1}{c-1}}.$$

Substituting this into (56) shows that $p^{2m/n} \geq 2c\alpha n$ suffices. □

G Dual Regev Encryption

Dual Regev encryption is a public-key encryption scheme based on the Learning With Errors (LWE) problem, formulated in the dual style [19]. In this version, $\mathsf{A} \in \mathbb{Z}_q^{n\times m}$ is a public matrix chosen uniformly at random, the secret key is $\boldsymbol{y} \leftarrow D_{\mathbb{Z}^m,r}$, and the public key is a vector $\boldsymbol{u} = \mathsf{A}\boldsymbol{y} \in \mathbb{Z}_q^n$.

To encrypt a bit $b \in \{0,1\}$, the sender samples $\boldsymbol{s} \leftarrow U_{\mathbb{Z}_q^n}$, $\boldsymbol{e}_1 \leftarrow \chi^m$ and $e_2 \leftarrow \chi$, where χ is an error distribution (typically a discrete Gaussian). The ciphertext is given by

$$(\boldsymbol{c}_1, c_2) = (\mathsf{A}^T\boldsymbol{s} + \boldsymbol{e}_1,\ \boldsymbol{u}^T\boldsymbol{s} + e_2 + \lfloor q/2\rfloor \cdot b) \in \mathbb{Z}_q^m \times \mathbb{Z}_q.$$

The scheme is IND-CPA secure under the LWE assumption. A key step in the security proof is to show the public key $\boldsymbol{u} = \mathsf{A}\boldsymbol{y}$ is statistically close to uniform. Again, the relevant lattice here is $\Lambda_\mathsf{A}^\perp = \{\boldsymbol{x} \in \mathbb{Z}^m : \mathsf{A}\boldsymbol{x} = \boldsymbol{0} \mod q\}$. The Rényi divergence between the distribution of $\boldsymbol{u}$ and the uniform distribution is given by $\mathbb{D}_\alpha(F_{r,\Lambda_\mathsf{A}^\perp} \| U_{\mathbb{Z}^m/\Lambda_\mathsf{A}^\perp}) = \mathbb{D}_\alpha(F_{r,\Lambda_\mathsf{A}^\perp} \| U_{\mathbb{Z}_q^n})$. Using Rényi smoothing of order ∞, [4] showed that for $\varepsilon = O(2^{-\lambda})$, a sampling parameter $r = \Omega(\sqrt{\log\lambda})$ is sufficient, improving upon the bound $r = \Omega(\sqrt{\lambda})$ based on L^1 smoothing. If we use the Rényi smoothing parameter of order $\alpha = 2 < \infty$, the parameter r can be reduced further, resulting in more efficient implementation. We formalize this as follows.

Corollary 2. *Suppose q is prime, $m \geq 2n\log q$, and $r \geq 2\sqrt{2\log(12m)/\pi}$. If there exists an adversary against the IND-CPA security of the dual-Regev encryption scheme with run-time T and advantage ε, then there exists a distinguishing algorithm for $\mathrm{LWE}_{n,q,\chi,m+1}$ with run-time $O\big((\varepsilon')^{-2}\log(\varepsilon'^{-1})\cdot\big(T + \mathrm{poly}(m)\big)\big)$ and advantage $\Omega\big((\varepsilon')^3\big)$, where $\varepsilon' = \varepsilon - 2q^{-n}$.*

Proof. The proof is similar to [4, Cor. 4.4]. Define the correlated-key LWE variant as follows. Let Φ be the distribution of

$$\bar{\mathsf{A}} = \big(\mathsf{A}, \boldsymbol{u}\big) \in \mathbb{Z}_q^{n\times(m+1)}, \mathsf{A} \leftarrow \mathbb{Z}_q^{n\times m} \text{ uniform}, \boldsymbol{y} \leftarrow D_{\mathbb{Z}^m,r}, \boldsymbol{u} = \mathsf{A}\boldsymbol{y} \bmod q.$$

Write $\mathrm{LWE}_{n,q,\chi,m+1}(\Phi)$ for distinguishing $\big(\bar{\mathsf{A}},\ \bar{\mathsf{A}}^T\boldsymbol{s} + \boldsymbol{e} \bmod q\big)$ from $\big(\bar{\mathsf{A}},\ \boldsymbol{u}'\big)$, where $\boldsymbol{s} \leftarrow \mathbb{Z}_q^n$ is uniform, $\boldsymbol{e} \leftarrow \chi^{m+1}$, and $\boldsymbol{u}' \leftarrow \mathbb{Z}_q^{m+1}$ is uniform.

By [19, Lem. 5.3], we have $\eta^{(2)}_{1/3}(\Lambda^\perp_{\mathsf{A}}) = \frac{\sqrt{2}}{2}\eta_{1/3}(\Lambda^\perp_{\mathsf{A}}) \le 2\sqrt{2\log(12m)/\pi} \le r$, except for a fraction $\le q^{-n}$ of the choices of A's. Let **Bad** denote the union of such bad A's and the A's that are not full rank. It can be derived that $\Pr[\mathbf{Bad}] \le 2q^{-n}$.

By multiplicativity (Lemma 2),

$$\begin{aligned}\mathbb{D}_2(\Phi\|U_{\mathbb{Z}_q^{n\times(m+1)}}) &\le \mathbb{D}_\infty(\mathsf{A}\|U_{\mathbb{Z}_q^{n\times m}}) \cdot \max_{\mathsf{A}\notin\mathbf{Bad}} \mathbb{D}_2(\mathsf{A}\boldsymbol{y} \bmod q\|U_{\mathbb{Z}_q^n}) \\ &\le \max_{\mathsf{A}\notin\mathbf{Bad}} R_2(\rho_{r,\Lambda^\perp_{\mathsf{A}}}\|U_{\mathcal{R}(\Lambda^\perp_{\mathsf{A}})}) \le (1+1/3)^2 < 2\end{aligned}$$

except for probability $2q^{-n}$. Here we use $\sqrt{2}\eta_{1/3}(\mathbb{Z}^m) \le \sqrt{\frac{2\log(8m)}{\pi}} \le r$ and Lemma 9 with $\alpha = 2$ in the last step. Applying [4, Cor. 4.3] with $\alpha = 2$, we get a distinguisher against $\mathrm{LWE}_{n,q,\chi,m+1}$ with run-time $T' = O((\varepsilon')^{-2}\log(\varepsilon'^{-1})\cdot\big(T + \mathrm{poly}(m)\big)\big)$ and advantage $\Omega((\varepsilon - 2q^{-n})^3)$. □

Consequently, our Rényi smoothing of order 2 lowers the required Gaussian width by $\sqrt{2}$ compared with order ∞ in [4], while distinguishing advantage decreases from $\Omega((\varepsilon')^2)$ to $\Omega((\varepsilon')^3)$. This can save either a smaller modulus q or a larger noise rate, or any balanced trade-off between them. In practice this yields shorter keys and ciphertexts.