J. Math. Cryptol. ? (????), 1–37
DOI 10.1515/jmc-????-???

Towards a Ring Analogue of the Leftover Hash Lemma

Dana Dachman-Soled, Huijing Gong, Mukul Kulkarni and Aria Shahverdi

Communicated by ???

Abstract. The leftover hash lemma (LHL) is used in the analysis of various lattice-based cryptosystems, such as the Regev and Dual-Regev encryption schemes as well as their leakage-resilient counterparts. The LHL does not hold in the ring setting, when the ring is far from a field, which is typical for efficient cryptosystems. Lyubashevsky et al. (Eurocrypt '13) proved a "regularity lemma," which can be used instead of the LHL, but applies only for Gaussian inputs. This is in contrast to the LHL, which applies when the input is drawn from any high min-entropy distribution. Our work presents an approach for generalizing the "regularity lemma" of Lyubashevsky et al. to certain conditional distributions. We assume the input was sampled from a discrete Gaussian distribution and consider the induced distribution, given side-channel leakage on the input. We present three instantiations of our approach, proving that the regularity lemma holds for three natural conditional distributions.

Keywords. Lattice-based cryptography, leakage resilience, Ring-LWE, regularity lemma.

2010 Mathematics Subject Classification. 94A60,68P25,03G10.

1 Introduction

The leftover hash lemma (LHL) is used in the analysis of various lattice-based cryptosystems. Specifically, it is often useful to argue that for high-min entropy input $\mathbf{x} \in \mathbb{Z}_q^m$ and random matrix $A \leftarrow \mathbb{Z}_q^{n \times m}$, $A\mathbf{x}$ is uniform random, given A. The above fact is used in the proof of security for both the Regev and Dual-Regev encryption schemes. More sophisticated proof approaches that utilize the LHL along with the structure of the matrix A have been used to argue leakage resilience of these cryptosystems, such as in [1, 13].[1]

This work is supported in part by NSF grants #CNS-1840893, #CNS-1453045 (CAREER), by a research partnership award from Cisco and by financial assistance award 70NANB15H328 from the U.S. Department of Commerce, National Institute of Standards and Technology.

[1] example, techniques include decomposition of the matrix A into two random matrices of varying dimensions [1].

Analogues of the statement above do not necessarily hold in the ring setting. Specifically, assuming a high min-entropy input $\mathbf{x} = x_1, \ldots, x_l$, setting $a_1 = 1$, and $a_2, \ldots, a_l$ chosen uniformly at random from the ring, the uniformity of $a_{l+1} = \sum_{i \in [l]} a_i x_i$ *does not* follow from the LHL lemma, in cases where the ring is far from a field, which is the typical case for efficient cryptosystems.

Fortunately, Lyubashevsky et al. [25, 26] proved a "regularity lemma" showing that the distribution over a_{l+1} as above is (close to) *uniform random*, even given $a_2, \ldots, a_l$, but *only* for the case where the input $\mathbf{x}$ is drawn from a *discrete Gaussian* distribution of sufficiently high standard deviation. While sufficient for proving the security of certain cryptosystems, unlike the more general leftover hash lemma, the statement of the regularity lemma of [25] implies nothing about uniformity of a_{l+1} in the case that $\mathbf{x}$ is a high min-entropy input from another distribution.

The ring setting. Consider the number field $K = \mathbb{Q}[x]/\Phi_m(x)$, where $\Phi_m(x)$ is the m-th cyclotomic polynomial of degree $\varphi(m)$. The ring of integers, $R \subset K$, is defined as $R = \mathbb{Z}[x]/\Phi_m(x)$. $R_q := \mathbb{Z}_q[x]/\Phi_m(x)$ denotes the set of polynomials obtained by taking an element of $\mathbb{Z}[x]/\Phi_m(x)$ and reducing each coefficient modulo q. In this paper, we further assume that m is a power of two, so $\Phi_m(x) = x^n + 1$ has degree $n = m/2$, and set q to be a prime such that $q \equiv 1 \mod m$. In this case $\Phi_m(x)$ completely splits into n factors in $\mathbb{Z}_q[x]$. This is the setting favored in practice since it allows for optimizations in the implementation, such as fast arithmetic over the ring R_q.

A Ring Analogue of the LHL. For rings R_q such as the above, a result analogous to the leftover hash lemma—proving that $a_{l+1} = \sum_{i \in [l]} a_i x_i$ is indistinguishable from random, given $a_2, \ldots, a_l$, as long as $x_1, \ldots, x_l$ has sufficiently high min-entropy—is impossible. For example, if the j-th NTT coordinate of each ring element in $\mathbf{x} = x_1, \ldots, x_l$ is leaked, then the j-th NTT coordinate of $a_{l+1} = \sum_{i \in [l]} a_i x_i$ is known[2], and so a_{l+1} is very far from uniform. Yet this is only a $1/n$ leakage rate![3]

Nevertheless, Lyubashevsky et al. [25,26] proved a "regularity lemma" showing that for matrix $A = [I_k | \bar{A}] \in (R_q)^{k \times l}$, where $I_k \in (R_q)^{k \times k}$ is the identity matrix and $\bar{A} \in (R_q)^{k \times (l-k)}$ is uniformly random, and $\mathbf{x}$ chosen from a discrete Gaussian distribution (centered at 0) over R_q^l, the distribution over $A\mathbf{x}$ is (close to) *uniform random*. A similar result was proven by Micciancio [28], but requires super-constant dimension l, thus yielding non-compact cryptosystems. In contrast,

[2] Applying NTT to $a_i, x_i \in R_q$—resulting in n-dimensional vectors, $\widehat{a}_i, \widehat{x}_i \in \mathbb{Z}_q^n$—allows for *component-wise* multiplication/addition, so the j-th NTT coordinate of $a_i x_i, i \in [l]$ will be known and so the j-th NTT coordinate of a_{l+1} is known.

[3] We thank an anonymous reviewer for pointing out this counterexample to us.

the regularity lemma of [25] holds even for constant dimension l as small as 2. The fundamental technical question we consider in this work is:

> For which distributions $\mathcal{D}$ over $\mathbf{x} \in R_q^l$, is the distribution over $A\mathbf{x}$ (close to) *uniform random*, for R, q, A as above and constant l?

1.1 Our Results

We prove a "regularity lemma" for three conditional distributions, which we describe next. **Only the parameter s–the standard deviation of the discrete Gaussian for sampling each coordinate of $\mathbf{x}$–differs in each setting.**

Conditional Distribution I. We assume a secret key $\mathbf{x} = (x_1, \ldots, x_l)$, where each $x_i \in R_q$. Moreover, each x_i itself is represented as an n-dimensional vector. So in total, $\mathbf{x}$ is an $l \cdot n$-dimensional vector. We consider the conditional distribution on $\mathbf{x}$ when the sum of $\mathbf{x}$ and $\mathbf{e}$ is revealed, where each coordinate of $\mathbf{e}$ is a Gaussian random variable with standard deviation at least s. This setting captures leakage on $\mathbf{x}$ by an adversary who uses a fast, but inaccurate device to obtain noisy measurements of *each* sampled coordinate of the secret key (e.g. through a power or timing channel). **We prove that it is sufficient to set $s \geq \sqrt{2} \cdot 2n \cdot q^{k/l+2/(nl)}$.** See Theorem 2.1 and Corollary 2.2.

Conditional Distribution II. We consider the conditional distribution over $\mathbf{x} = (x_1, \ldots, x_l)$ when we leak ℓ coordinates from each $x_i, i \in [l]$. and we set parameters such that the fraction of leaked coordinates–$\frac{\ell \cdot l}{n \cdot l}$–is constant. The ℓ leaked coordinates are arbitrary, but the same ℓ coordinates must be leaked from each $x_i, i \in [l]$.[4] *Low noise* is added to each leaked coordinate (only $2n$ standard deviation, as opposed to $\sqrt{2} \cdot 2n \cdot q^{k/l+2/(nl)}$ standard deviation as in Conditional Distribution I). No information at all is leaked about the remaining coordinates. This setting corresponds to a side-channel attack launched during the sampling of $\mathbf{x}$, where the attacker has a slower, but more accurate device which allows it to obtain more accurate measurements for a *constant fraction* of the coordinates of the secret key, but *no* information for the remaining coordinates. [5] **We prove that it is sufficient to set $s \geq 2n \cdot q^{\frac{kn+2}{l(n-\ell)}}$, where $\ell \cdot l$ is the number of leaked coordinates.** See Theorem 2.3 and Corollary 2.6.

Conditional Distribution III. Here, we consider the conditional distribution on $\mathbf{x}$, when the magnitude of $\mathbf{x}$ with Gaussian channel error e is revealed (note that

[4] Alternatively, we can view the leakage as ℓ completely arbitrary coordinates, with leakage rate of $\ell/(n \cdot l)$, which remains constant for constant l.

[5] Here we assume that the secret key is stored as a vector in the canonical embedding (in the other leakage scenarios, the result holds when the secret key is stored in using the polynomial representation or is stored as a vector in the canonical embedding).

e is a scalar). We assume e is sampled from a univariate Gaussian with standard deviation s. A motivation for this type of leakage is that (discrete) Gaussian sampling of $\mathbf{x}$ is often implemented via rejection sampling in practice [7, 12]. E.g. a vector could be sampled from a "close" multi-dimensional binomial distribution and rejection sampling then used to obtain a sample from the correct distribution. The rejection condition depends on the weight of $\mathbf{x}$ under the target distribution, which in turn depends on the magnitude of $\mathbf{x}$, and so this information is vulnerable to leakage during computation. [6] **We prove that it is sufficient to set $s \geq \sqrt{14/5 \cdot (n'/n) \cdot \ln n'} \cdot 2n \cdot q^{k/l+2/(nl)}$, where $n' = n \cdot l + 1$.** See Theorem 2.9 and Corollary 2.10.

Applications to leakage resilience. Since applications of the LHL/Regularity Lemma in lattice-based cryptography are widespread, a number of Ring-LWE (RLWE) cryptosystems achieve certain leakage resilience properties using our results. Such cryptosystems include the ring analogues of Regev encryption [24], Dual-Regev encryption [25], and identity-based encryption (IBE) based on Dual-Regev encryption [19] (see ring version in [3]). Specifically, by substituting our "regularity lemma" for the original "regularity lemma" in the security proofs, those schemes still enjoy security guarantees even given certain leakage on the *randomness for encryption* (for Regev) the *secret key* (for Dual-Regev), and the *secret key corresponding to the challenge identity* (for IBE).

1.2 Our High-Level Approach

For a matrix $A = [I_k | \bar{A}] \in (R_q)^{k \times l}$, where $I_k \in (R_q)^{k \times k}$ is the identity matrix and $\bar{A} \in (R_q)^{k \times (l-k)}$ is uniformly random, we define $\Lambda^{\perp}(A) = \{\mathbf{z} \in R^l : A\mathbf{z} = \mathbf{0} \bmod qR\}$. If $[\mathbf{x} \mod \Lambda^{\perp}(A)]$ is uniform random (over cosets of $\Lambda^{\perp}(A)$), then the distribution of $A\mathbf{x}$ is also uniform random over cosets of $(qR)^k$. The input/output distributions can then be discretized over the ring R. Therefore, the goal is to show that when $\mathbf{x}$ is sampled from continuous distribution $\mathcal{D}$, we have that $[\mathbf{x} \mod \Lambda^{\perp}(A)]$ is uniform random. Consider the case where the distribution $\mathcal{D}$ is exactly a Gaussian distribution with mean 0 and standard deviation s. In this case, if s is greater than or equal to the *smoothing parameter* of $\Lambda^{\perp}(A)$, this by definition ensures that the distribution $[\mathbf{x} \mod \Lambda^{\perp}(A)]$ is uniform random. Thus, [25] prove their regularity lemma by showing that with high probability over choice of A, the smoothing parameter, $\eta_{\varepsilon}(\Lambda^{\perp}(A))$, is upperbounded by s.

Before presenting our approach to extending the above result, it is instructive to give a high-level recap of how to derive upper bounds on the smoothing parameter.

[6] For example, a power analysis attack on the BLISS signature scheme [18] exploited the rejection sampling procedure to recover the magnitude (norm) of certain secret values, which then led to a full break of the scheme.

Let $\rho_s := e^{-\pi \frac{\langle \mathbf{x}, \mathbf{x} \rangle}{s^2}}$ and let ψ_s (the normalization of ρ_s) correspond to the probability density function (PDF) of the normalized n-dimensional Gaussian distribution with mean 0 and standard deviation s. In the following, for a function f we concisely represent $\sum_{\mathbf{v} \in \Lambda} f(\mathbf{v})$ by $f(\Lambda)$. To show that the distribution over $[\mathbf{x} \bmod \Lambda]$ is (close to) uniform when $\mathbf{x}$ is sampled from a distribution with PDF ψ_s, one needs to show that for every coset $(\Lambda + \mathbf{c})$ of the lattice, $\psi_s(\Lambda + \mathbf{c}) \approx \frac{1}{\det(\Lambda)}$. Focusing on the zero coset, where $\mathbf{c} = \mathbf{0}$, we can prove this using the Poisson summation formula, which says that for any lattice Λ and integrable function ρ_s: $\psi_s(\Lambda) = \frac{1}{\det(\Lambda)} \cdot \widehat{\psi_s}(\Lambda^\vee)$, where for a function f, $\widehat{f}$ denotes the n-dimensional Fourier transform of f and $\Lambda^\vee$ is the dual lattice of Λ (see Appendix A.2). It remains to show that $\widehat{\psi_s}(\Lambda^\vee)$ is close to 1 (i.e. is upperbounded by $1 + \varepsilon$).

The proof approach outlined above can be applied to (integrable) normalized PDF Ψ that are not Gaussians centered at 0: To show that the distribution over $[\mathbf{x} \bmod \Lambda]$ is (close to) uniform when $\mathbf{x}$ is sampled from a distribution with PDF Ψ, it is sufficient to show that $\widehat{\Psi}(\Lambda^\vee)$ is upperbounded by $1 + \varepsilon$.

In this work, we consider PDF's, Ψ, that correspond to the PDF of $\mathbf{x}$, *from the point of view of the adversary*, given the leakage. The technical contribution of this work is to show that, for each conditional distribution, (with overwhelming probability over choice of $\bar{A}$) $\widehat{\Psi}(\Lambda^\perp(A)^\vee)$ is close to 1. Specifically, for each distribution, our approach requires: (1) Determining the PDF Ψ, (2) Computing (an upper bound for) the multi-dimensional Fourier transform of Ψ (denoted $\widehat{\Psi}$), (3) Proving that $\widehat{\Psi}((\Lambda^\perp(A))^\vee)$ is upperbounded by $1 + \varepsilon$ (or, equivalently that $\widehat{\Psi}((\Lambda^\perp(A))^\vee \setminus \{\mathbf{0}\})$ is upperbounded by ε).

1.3 Related Work

Leakage-resilient cryptography. There is a significant body of work on leakage-resilient cryptographic primitives, beginning with the work of Dziembowski and Pietrzak [16] on leakage-resilient stream-ciphers. Other constructions include [1, 5, 6, 14, 22, 22, 23, 23, 27, 30, 31]. With the exception of [1], most of these results construct new cryptosystems from the bottom up. In our work, we consider whether we can prove that an existing cryptosystem enjoys leakage resilience, without modification of the scheme.

Lattice-based & leakage-resilient cryptography. Goldwasser et al. [20] initiated the study of leakage resilience of lattice based cryptosystems. This was followed by series of works [1, 13, 15], all these papers however study leakage resilience of schemes based on standard LWE problem in both symmetric as well as public key setting.

Robustness of Ring-LWE To the best of our knowledge the ePrint version [10] of this work is the first effort to study the robustness of RLWE based cryptosystems

under leakage. Subsequent to the publishing of ePrint [10], interest has sparked in analyzing the RLWE-based schemes and their leakage resilience. Albrecht et.al [2] implemented cold boot attack on RLWE based KEM schemes and compared the number of operations required to mount the attack when secret is stored with different encodings. Recently, Bolboceanu et.al [4] studied the hardness of RLWE problem in cases where the secret is sampled from distributions other than uniform random distribution over the ring. In [11], it is shown that under specific structured leakage on the NTT encoding of secret key, it is possible to recover the entire secret key given multiple RLWE samples and they implement the attack to recover the secret in real world parameter settings.

Other variants of LHL Stehlé and Steinfeld [34] studied the leftover hash lemma in the ring setting for power of 2 cyclotomics and Rosca et.al [33] generalized their result to non-cyclotomic rings. However, both these results study the case where input is sampled from discrete Gaussian distribution.

2 Extending the Regularity Lemma

For a positive integer n, we denote by $[n]$ the set $\{1, \ldots, n\}$. We denote vectors in boldface $\mathbf{x}$ and matrices using capital letters A. For vector $\mathbf{x}$ over $\mathbb{R}^n$ or $\mathbb{C}^n$, define the ℓ_2 norm as $\|\mathbf{x}\|_2 = \left(\sum_i |x_i|^2\right)^{1/2}$. We write as $\|\mathbf{x}\|$ for simplicity. Background and standard definitions related to lattices and algebraic number theory are in Appendix A. Our results are applicable when R is the ring of integers in the m^{th} cyclotomic number field K of degree n, $m = 2n$ is a power of 2 and prime q is s.t. $q \equiv 1 \mod m$. We denote by $I_k \in (R_q)^{k \times k}$ the identity matrix.

2.1 Conditional Distribution I

Recall that $\mathbf{x} = (x_1, \ldots, x_l)$, where each coordinate of each $x_i \in R_q$ is sampled from a discrete Gaussian with standard deviation s and each x_i is represented as a vector in either the polynomial or canonical basis.[7] We assume leakage of all coordinates, with Gaussian noise of standard deviation $v = \tau \cdot s$ added. It turns out that this conditional distribution is fairly simple to handle since if X and Y are independent Gaussian random variables, then the distribution of X conditioned on $X + Y$ is also a Gaussian that is *not* centered at 0. Fortunately, the regularity lemma of [26] straightforwardly extends to Gaussians that are not centered at 0. We discuss formal details next, however, we mainly view Conditional Distribution I as a warm-up to the more difficult Conditional Distributions II and III.

See Appendix D for background on manipulating Gaussian random variables. Specifically, Lemma D.1 shows that, conditioned on leakage, each coordinate x_i

[7] Either representation works since for power-of-two cyclotomics, spherical Gaussians in the polynomial basis correspond to spherical Gaussians in the canonical basis.

of the secret key is sampled from a multivariate Gaussian distribution $\rho_{\sigma,\mathbf{c}^i}$ with mean $\mathbf{c}^i := (c_1^i, \ldots, c_n^i)$, where $c_j^i := \frac{z_j}{\tau^2+1}$ and $\sigma = s\sqrt{\frac{\tau^2}{\tau^2+1}}$. The entire secret key is then sampled from $\rho_{\sigma,\mathbf{c}}$, where $\mathbf{c} = [\mathbf{c}^i]_{i\in l}$. We have the following theorem:

Theorem 2.1. *For positive integers $k \le l \le \mathrm{poly}(n)$, let $A = [I_k|\bar{A}] \in (R_q)^{k\times l}$, where $\bar{A} \in (R_q)^{k\times(l-k)}$ is uniformly random. Then for all $\sigma \ge 2n \cdot q^{k/l+2/(nl)}$ and $\mathbf{c} \in \mathbb{R}^{n\cdot l}$ then*

$$\widehat{\rho_{\sigma,\mathbf{c}}}\left(\Lambda^{\perp}(A)^{\vee}\right) \le 1 + 2^{-\Omega(n)},$$

except with probability at most $2^{-\Omega(n)}$ over choice of $\bar{A}$.

Proof. The theorem follows from Lemma B.7 and the regularity lemma from [26]. □

The following corollary follows from Lemmas B.12 and B.13 and Theorem 2.1.

Corollary 2.2. Let $R, n, q, k, l, \mathbf{c}, \sigma$ be as in Theorem 2.1. Assume that $A = [I_k|\bar{A}] \in (R_q)^{k\times l}$ is chosen as in Theorem 2.1. Then, with probability $1 - 2^{-\Omega(n)}$ over the choice of $\bar{A}$, the distribution of $A\mathbf{x} \in R_q^k$, where $\mathbf{x} \in R^l$ is chosen from $D_{\Lambda,\sigma,\mathbf{c}}$, the discrete Gaussian probability distribution over R^l with parameter σ and center $\mathbf{c}$, satisfies that the probability of each of the q^{nk} possible outcomes is in the interval $(1 \pm 2^{-\Omega(n)})q^{-nk}$ (and in particular is within statistical distance $2^{-\Omega(n)}$ of the uniform distribution over R_q^k).

In particular, this means that the standard deviation used to sample $\mathbf{x}$ should be increased from $2n \cdot q^{k/l+2/(nl)}$ (as in [26]) to $\sqrt{\frac{1+\tau^2}{\tau^2}} \cdot 2n \cdot q^{k/l+2/(nl)}$. Setting $\tau = 1$, we obtain the parameters described in the introduction.

2.2 Conditional Distribution II

Recall that $\mathbf{x} = (x_1, \ldots, x_l)$, where each $x_i \in R_q$ and each x_i is represented as a vector in the canonical embedding. We assume leakage of ℓ coordinates—with low noise added—of each x_i for $i \in [l]$ and restrict the coordinates leaked across each x_i to be the same. Let $\mathcal{S} \subseteq [n]$, where $|\mathcal{S}| = \ell$ denote the set of positions (from each x_i) that are leaked. Lemma D.1 shows that, conditioned on leakage, each component x_i^j, $i \in [l], j \in \mathcal{S}$, (resp. $\notin \mathcal{S}$) is sampled from Gaussian distribution with mean $c_i^j := \frac{nz_i^j}{n+\frac{1}{s^2}}$ (resp. 0), and variance $\sigma_j^2 \ge 4n^2$ (resp. $\sigma_j^2 = s^2$).

Theorem 2.3. *For positive integers $k \le l \le \mathrm{poly}(n)$, let $A = [I_k|\bar{A}] \in (R_q)^{k\times l}$, where $\bar{A} \in (R_q)^{k\times(l-k)}$ is uniformly random. Let $\sigma := (\sigma_1, \ldots, \sigma_n) \in \mathbb{R}_{>0}^n$ and*

$\mathbf{c} := (c_1, \ldots, c_{ln}) \in \mathbb{R}^{ln}$ *be vectors, where* ℓ *positions in* σ *are set to* $2n$*, and all others are set to* s*. Let* k, l, ℓ *be such that* $l - k - l \cdot \ell/n > 0$ *and* $l - k - 1 \geq 1$*, and let* $s \geq 2n \cdot q^{\frac{kn+2}{l(n-\ell)}}$ *then* $\widehat{\rho_{\sigma^l,\mathbf{c}}}\left(\Lambda^{\perp}(A)^{\vee}\right) \leq 1 + 2^{-\Omega(n)}$ *except with probability at most* $2^{-\Omega(n)}$ *over choice of* $\bar{A}$*.*

For proving Theorem 2.3, we begin with exposition on the forms of the Ideals $qR^{\vee} \subseteq \mathcal{J} \subseteq R^{\vee}$ in power-of-two cyclotomics as well as some lemmas.

To generate the set T of ideals $\mathcal{J}$ such that $qR^{\vee} \subseteq \mathcal{J} \subseteq R^{\vee}$ we take each ideal $\mathcal{I}$ s.t. $qR \subseteq \mathcal{I} \subseteq R$ and set $\mathcal{J} := q\mathcal{I}^{\vee}$. Recall from Fact A.3 that $\langle q \rangle$ splits completely into n distinct ideals of norm q, i.e. $qR = \Pi_{i \in [n]} \mathfrak{p}_i$. Therefore, the set of all ideals $\mathcal{I}$ such that $qR \subseteq \mathcal{I} \subseteq R$, is exactly the set $\mathcal{S} := \{\Pi_{i \in S} \mathfrak{p}_i \mid S \subseteq [n]\}$. Thus, the number of ideals $\mathcal{I}$ such that $qR \subseteq \mathcal{I} \subseteq R$ (and hence also the number of ideals $\mathcal{J} \in T$) is exactly 2^n. Moreover, note that for each ideal $\mathcal{J} \in T$,

$$|\mathcal{J}/qR^{\vee}| = |R/q\mathcal{J}^{\vee}| = N(q\mathcal{J}^{\vee}).$$

Thus, we see that for each $\mathcal{J} \in T$, $1 \leq |\mathcal{J}/qR^{\vee}| \leq q^n$.

Let T_1 denote the set of ideals $\mathcal{J} \in T$ such that $|\mathcal{J}/qR^{\vee}| < 2^n$. Let T_2 denote the set of ideals $\mathcal{J}$ such that $|\mathcal{J}/qR^{\vee}| \geq 2^n$. Furthermore, let T_2^1 be the set of $\mathcal{J} \in T_2$ such that $s \geq \eta_{2^{-2n}}((\frac{1}{q}\mathcal{J})^{\vee})$ (where $\eta_{2^{-2n}}$ denotes the smoothing parameter and s is fixed as above). Let $T_2^2 := T_2 \setminus T_2^1$. Let $\sigma := (\sigma_1, \ldots, \sigma_n) \in \mathbb{R}^n_{>0}$ be a vector with ℓ positions are set to $2n$, while the other positions are set to value s.

Lemma 2.4. For ideals $\mathcal{J} \in T_1$,

$$\eta_{2^{-2n}}\left((\frac{\mathcal{J}}{q})^{\vee}\right) \leq 2n.$$

The proof of Lemma 2.4 can be found in Appendix E.1.

Lemma 2.5. For ideals $\mathcal{J} \in T_2^1$

$$|\mathcal{J}/qR^{\vee}|^{-(l-k)} \left(\rho_{1/\sigma_1,\ldots,1/\sigma_n}\left(\frac{1}{q}\mathcal{J}\right)^l\right) \leq 2^{-n(l-k)},$$

where $\rho_{1/\sigma_1,\ldots,1/\sigma_n}$ is an n-dimensional Gaussian function with coordinate-wise standard deviation $1/\sigma_i, i \in [n]$ and center 0 (see beginning of Appendix B).

The proof of Lemma 2.5 can be found in Appendix E.1. We now conclude the proof of Theorem 2.3.

Proof of Theorem 2.3. Since by Lemma B.7 we have that for any $(n \cdot l)$-dimensional vectors, $\mathbf{c}$, $\mathbf{x}$ and any n-dimensional vector $\sigma = (\sigma_1, \ldots, \sigma_n)$:

$$\widehat{\rho_{\sigma^l,\mathbf{c}}}(\mathbf{x}) \leq \widehat{\rho_{\sigma^l}}(\mathbf{x}) = \rho_{(1/\sigma_1,\ldots,1/\sigma_n)^l}(\mathbf{x}),$$

then following the proof of [26] step-by-step, it is sufficient to show that

$$\sum_{\mathcal{J}\in T} |\mathcal{J}/qR^\vee|^{-(l-k)} \cdot \left(\rho_{(1/\sigma_1,\ldots,1/\sigma_n)}\left(\frac{1}{q}\mathcal{J}\right)^l - 1\right) \leq 2^{-\Omega(n)}.$$

We will show that

$$\sum_{\mathcal{J}\in T_2^1} |\mathcal{J}/qR^\vee|^{-(l-k)} \left(\rho_{(1/\sigma_1,\ldots,1/\sigma_n)}\left(\frac{1}{q}\mathcal{J}\right)^l - 1\right) \leq 2^{-\Omega(n)}, \tag{2.1}$$

and that

$$\sum_{\mathcal{J}\in(T_1\cup T_2^2)} |\mathcal{J}/qR^\vee|^{-(l-k)} \left(\rho_{1/\sigma_1,\ldots,1/\sigma_n}\left(\frac{1}{q}\mathcal{J}\right)^l - 1\right) \leq 2^{-\Omega(n)} \tag{2.2}$$

To show (2.2), note that by Lemma 2.4, for ideals $\mathcal{J} \in T_1$ (we have that $\eta_{2^{-2n}}((\frac{\mathcal{J}}{q})^\vee) \leq 2n$. This means that for each $i \in [n]$, $\sigma_i \geq \eta_{2^{-2n}}$, which implies that $\rho_{1/\sigma_1,\ldots,1/\sigma_n}\left(\frac{1}{q}\mathcal{J}\right)^l \leq (1+2^{-2n})^l$.

On the other hand, by definition of T_2^2, for ideals $\mathcal{J} \in T_2^2$, we have that $\sigma_i < \eta_{2^{-2n}}$, for each $i \in [n]$. Thus, by Lemma B.6 we have that $\rho_{1/\sigma_1,\ldots,1/\sigma_n}\left(\frac{1}{q}\mathcal{J}\right) \leq \left(\frac{\eta_{2^{-2n}}((\frac{\mathcal{J}}{q})^\vee)}{\sigma_1} \cdots \frac{\eta_{2^{-2n}}((\frac{\mathcal{J}}{q})^\vee)}{\sigma_n}\right) \cdot (1+2^{-2n})$. Since $\eta_{2^{-2n}}((\frac{\mathcal{J}}{q})^\vee)^n \leq |\mathcal{J}/qR^\vee|\Delta_K$, and plugging in the proper values for $\sigma_1, \ldots, \sigma_n$, we have that $\rho_{1/\sigma_1,\ldots,1/\sigma_n}\left(\frac{1}{q}\mathcal{J}\right)^l \leq (|\mathcal{J}/qR^\vee|\Delta_K s^{-n+\ell} \cdot (2n)^{-\ell})^l \cdot (1+2^{-2n})^l$. Combining the above, we get that for $\mathcal{J} \in T_1 \cup T_2^2$,

$$\rho_{1/\sigma_1,\ldots,1/\sigma_n}\left(\frac{1}{q}\mathcal{J}\right)^l \leq \max(1, (|\mathcal{J}/qR^\vee|\Delta_K s^{-n+\ell} \cdot (2n)^{-\ell})^l) \cdot (1+2^{-2n})^l.$$

Similarly to [26], using the lower bound of s from Theorem 2.3, we bound

$$\begin{aligned}
&\sum_{\mathcal{J}\in(T_1\cup T_2^2)} |\mathcal{J}/qR^\vee|^{-(l-k)} \left(\rho_{1/\sigma_1,\ldots,1/\sigma_n}\left(\frac{1}{q}\mathcal{J}\right)^l - 1\right) \\
&\leq \sum_{\mathcal{J}\in(T_1\cup T_2^2)} |\mathcal{J}/qR^\vee|^{-(l-k)} \cdot \max(1, (|\mathcal{J}/qR^\vee|\Delta_K s^{-n+\ell}\cdot(2n)^{-\ell})^l)\cdot(1+\varepsilon)^l \\
&\leq \sum_{\mathcal{J}\in T} |\mathcal{J}/qR^\vee|^{-(l-k)} \cdot \max(1, (|\mathcal{J}/qR^\vee|\Delta_K s^{-n+\ell}\cdot(2n)^{-\ell})^l)\cdot(1+\varepsilon)^l \\
&\leq 2^{-\Omega(n)} + 2(s/n)^{-nl} q^{kn+2}\left(\frac{s}{2n}\right)^{l\cdot\ell} \in 2^{-\Omega(n)}.
\end{aligned}$$

Moreover, by Lemma 2.5 and the fact that $|T_2^1| \leq |T| = 2^n$, we can bound

$$\sum_{\mathcal{J}\in T_2^1} |\mathcal{J}/qR^\vee|^{-(l-k)} \left(\rho_{1/\sigma_1,\ldots,1/\sigma_n}\left(\frac{1}{q}\mathcal{J}\right)^l - 1\right) \leq 2^n \cdot 2^{-n(l-k)} \in 2^{-\Omega(n)},$$

where the last line follows from the setting of parameters in Theorem 2.3.

This completes the proof. □

The following corollary follows from Lemmas B.12 and B.13 and Theorem 2.3.

Corollary 2.6. Let k, l, ℓ, σ and $\mathbf{c}$ be as in Theorem 2.3. Assume that $A = [I_k|\bar{A}] \in (R_q)^{k\times l}$ is chosen as in Theorem 2.3. Then, with probability $1 - 2^{-\Omega(n)}$ over the choice of $\bar{A}$, the distribution of $A\mathbf{x} \in R_q^k$, where $\mathbf{x} \in R^l$ is chosen from $D_{R^l,\sigma^l,\mathbf{c}}$, the discrete Gaussian probability distribution over R^l with parameter σ^l and center $\mathbf{c}$, satisfies that the probability of each of the q^{nk} possible outcomes is in the interval $(1 \pm 2^{-\Omega(n)})q^{-nk}$ (and in particular is within statistical distance $2^{-\Omega(n)}$ of the uniform distribution over R_q^k).

In particular, this means that the standard deviation used to sample $\mathbf{x}$ should be increased from $2n \cdot q^{k/l+2/(nl)}$ (as in [26]) to $2n \cdot q^{\frac{kn+2}{l(n-\ell)}}$.

2.3 Conditional Distribution III

We slightly change the dimensions so that $\mathbf{x}$ is represented by a vector of dimension $n' := l \cdot n + 1$. When n is a power of two, a spherical Gaussian in the coefficient representation is also a spherical Gaussian in the canonical embedding representation [24]. So we can assume that $\mathbf{x}$ is generated using the coefficient representation, where each coordinate is sampled independently from a discrete

Gaussian, $D_{Z,s'}$. During sampling of $\mathbf{x}$, an additional coordinate is sampled and stored together with the remainder of the secret. We compute the PDF corresponding to the conditional distribution on $\mathbf{x}$, given $z = |r + e|$, where $r = \|\mathbf{x}\|$ as:

$$F_{X\left|\|\|X\|+E\right|=z}(\|X\| = r) = \frac{e^{-\left(\frac{\pi}{s^2}+\frac{\pi}{v^2}\right)\left(r-\frac{zs^2}{v^2+s^2}\right)^2} + e^{-\left(\frac{\pi}{s^2}+\frac{\pi}{v^2}\right)\left(r+\frac{zs^2}{v^2+s^2}\right)^2}}{N}, \tag{2.3}$$

where N is the normalization factor. For details on how the PDF is computed, see Appendix E.2. $F_{X\left|\|\|X\|+E\right|=z}(\|X\| = r)$ is the sum of two Gaussian functions centered at $\frac{zs^2}{v^2+s^2}$ and $-\frac{zs^2}{v^2+s^2}$ respectively with the same standard deviation σ. Suppose $v = s$, we have $\sigma = \frac{s}{\sqrt{2}}$.

Lemma 2.7. Suppose $v = s$, we bound the center $\frac{zs^2}{v^2+s^2}$ from Equation 2.3 by $\Pr\left(\frac{zs^2}{v^2+s^2} \geq s\sqrt{n'}\right) \in 2^{-\Omega(n)}$, where the probability is taken over choice of $\mathbf{x}$ and e.

The proof is found in Appendix E.2.

Let $\Psi_{\sigma,c}(\mathbf{x}) := F_{X\left|\|\|X\|+E\right|=z}(\|X\| = \|\mathbf{x}\|)$ be the normalization of the function $f(\mathbf{x}) := e^{-\frac{\pi(\|\mathbf{x}\|-c)^2}{\sigma^2}} + e^{-\frac{\pi(\|\mathbf{x}\|+c)^2}{\sigma^2}}$. By Lemma 2.7, we have that with all but negligible probability, $c := \frac{zs^2}{v^2+s^2} \leq \sqrt{2} \cdot \sigma\sqrt{n'}$.

For the proof, we will require certain properties of the Fourier transform of $\Psi_{\sigma,c}$, when c is bounded as above. We state those properties in the following theorem, which is proved in Appendix C.

Theorem 2.8. *Let $n' := l \cdot 2^a + 1$, where l, a are positive integers and $a > 2$, and $c \leq \sqrt{2} \cdot \sigma \cdot \sqrt{n'}$. Let $\Psi_{\sigma,c}$ denote the normalized pdf corresponding to the non-normalized function $f(\mathbf{x}) := e^{-\frac{\pi(\|\mathbf{x}\|-c)^2}{\sigma^2}} + e^{-\frac{\pi(\|\mathbf{x}\|+c)^2}{\sigma^2}}$, where $\mathbf{x}$ is a vector over n' dimensions. and let $\widehat{\Psi_{\sigma,c}}(\mathbf{y})$ denote the n'-dimensional Fourier transform of $\Psi_{\sigma,c}$. Then $|\widehat{\Psi_{\sigma,c}}(\mathbf{y})| \leq n'^{n'} \cdot e^{-\pi\|\mathbf{y}\|^2\sigma^2}$ for $\|\mathbf{y}\| > 1/\sigma$.*

We next present the main theorem of this section.

Theorem 2.9. *For positive integers $k \leq l \leq \text{poly}(n)$, let $A = [I_k|\bar{A}] \in (R_q)^{k\times l}$, where $\bar{A} \in (R_q)^{k\times(l-k)}$ is uniformly random. Let $c \leq \sqrt{2} \cdot \sqrt{n'} \cdot \sigma$ and let $\sigma \geq \sqrt{\frac{7}{5} \cdot \frac{n'}{n} \ln n'} \cdot 2n \cdot q^{k/l+2/(nl)}$. Define $\Lambda^\perp(A)^+$ as a direct product of $\Lambda^\perp(A)$ and $\mathbb{Z}$, written as $\Lambda^\perp(A)^+ := \Lambda^\perp(A) \times \mathbb{Z}$. Then $\Psi_{\sigma,c}\left(\Lambda^\perp(A)^+\right) \leq \frac{1}{det(\Lambda^\perp(A)^+)}(1 + 2^{-\Omega(n)})$ except with probability at most $2^{-\Omega(n)}$.*

Proof. Note that $\Lambda^{\perp}(A)$ is a lattice of even dimension $l \cdot n$ (where n is a power of two), but Theorem 2.8 holds only for n' equal to $l \cdot 2^a + 1$. Therefore, we define $n' := l \cdot n + 1$, and we have the n'-dimensional lattice $\Lambda^{\perp}(A)^+ := \Lambda^{\perp}(A) \times \mathbb{Z}$. We have the following properties of $\Lambda^{\perp}(A)^+$, which can be verified by inspection:

(a) $(\Lambda^{\perp}(A)^+)^{\vee} := \Lambda^{\perp}(A)^{\vee} \times \mathbb{Z}$;

(b) the shortest non-zero vector in $(\Lambda^{\perp}(A)^+)^{\vee}$ is at least $\min(\lambda_1(\Lambda^{\perp}(A)^{\vee}), 1)$, where $\lambda_1(\Lambda^{\perp}(A)^{\vee})$ denotes the shortest non-zero vector in $\Lambda^{\perp}(A)^{\vee}$;

By Poisson summation formula, it is sufficient to show that with probability $1-2^{-\Omega(n)}$ over choice of A, $|\widehat{\Psi_{\sigma,c}}|((\Lambda^{\perp}(A)^+)^{\vee}) \leq 1+2^{-\Omega(n)}$, where $\widehat{\Psi_{\sigma,c}}$ denotes the Fourier transform of $\Psi_{\sigma,c}$ over n' dimensions and the notation $|\widehat{\Psi_{\sigma,c}}|$ means the summation of the absolute value of the function over the lattice $\Lambda^{\perp}(A)^+)^{\vee}$.

We first note that, over n' dimensions, $\widehat{\Psi_{\sigma,c}}(\mathbf{0}) = 1$. This follows due to the fact that by definition of Fourier transform, $\widehat{\Psi_{\sigma,c}}(\mathbf{0}) := \int_{\mathbb{R}^{n'}} \Psi_{\sigma,c}(\mathbf{x})\, d\mathbf{x}$. Since $\Psi_{\sigma,c}$ is a normalized PDF, it must be the case that $\int_{\mathbb{R}^{n'}} \Psi_{\sigma,c}(\mathbf{x})\, d\mathbf{x} = 1$.

Thus, it remains to show that $\left|\widehat{\Psi_{\sigma,c}}\right| \left((\Lambda^{\perp}(A)^+)^{\vee} \setminus \{\mathbf{0}\}\right) \leq 2^{-\Omega(n)}$.

Towards showing this, we first let $\beta = 2n \cdot q^{k/l+2/(nl)}$ for simplicity, and then use Theorem 2.8 to show that, when $\kappa = |\mathbf{y}| \geq \frac{\sqrt{n/\pi}}{\beta}$,

$$|\widehat{\Psi_{\sigma,c}}(\mathbf{y})| \leq n'^{n'} \cdot e^{-(\sigma^2 \cdot \pi \cdot \kappa^2)} \leq n'^{n'} \cdot e^{-5(\sigma^2 \cdot \pi \cdot \kappa^2)/7} \cdot e^{-2(\sigma^2 \cdot \pi \cdot \kappa^2)/7} \leq e^{-2(\sigma^2 \cdot \pi \cdot \kappa^2)/7},$$

where the last line follows since $\sigma := \sqrt{\frac{7n'}{5n} \ln n'} \cdot 2n \cdot q^{k/l+2/(nl)} = \sqrt{\left(\frac{7n'}{5n}\right) \ln n'} \cdot \beta$ is chosen so that when $\kappa \geq \frac{\sqrt{n/\pi}}{\beta}$, $e^{5(\sigma^2 \cdot \pi \cdot \kappa^2)/7} \geq n'^{n'} = e^{n' \ln n'}$.

Let $Q := \sum_{\mathbf{y} \in (\Lambda^{\perp}(A)^+)^{\vee} \setminus \{\mathbf{0}\}} e^{-2(\sigma^2 \cdot \pi \cdot \kappa^2)/7}$. Combining the above inequalities which hold when $\kappa \geq \frac{\sqrt{n/\pi}}{\beta}$, together with (b) and Corollary B.17, which states that with probability $1 - 2^{-\Omega(n)}$ over choice of A, the shortest non-zero vector in $\Lambda^{\perp}(A)^{\vee}$ has length $\kappa \geq \frac{\sqrt{n/\pi}}{\beta}$, we conclude that an upper bound on Q yields an upper bound on the desired quantity, $\left|\widehat{\Psi_{\sigma,c}}\right| \left((\Lambda^{\perp}(A)^+)^{\vee} \setminus \{\mathbf{0}\}\right)$.

Additionally note that when $\kappa \geq \frac{\sqrt{n/\pi}}{\beta}$, then

$$e^{-2(\sigma^2 \cdot \pi \cdot \kappa^2)/7} = e^{-(\sigma^2 \cdot \pi \cdot \kappa^2)/7} \cdot e^{-(\sigma^2 \cdot \pi \cdot \kappa^2)/7} \leq e^{-1/5 \cdot n' \ln n'} \cdot e^{-(\sigma^2 \cdot \pi \cdot \kappa^2)/7}, \quad (2.4)$$

where the inequality follows since (by above) $e^{5(\sigma^2 \cdot \pi \cdot \kappa^2)/7} \geq n'^{n'} = e^{n' \ln n'}$. so $e^{-(\sigma^2 \cdot \pi \cdot \kappa^2)/7} \leq n'^{-1/5 \cdot n'} = e^{-1/5 \cdot n' \ln n'}$. Moreover, recall that two applications of Poisson summation give:

$$\sum_{\mathbf{y} \in (\Lambda^{\perp}(A)^+)^{\vee}} e^{-(\sigma^2 \cdot \pi \cdot \kappa^2)/7} \leq 2^{n'} \cdot \sum_{\mathbf{y} \in (\Lambda^{\perp}(A)^+)^{\vee}} e^{-2(\sigma^2 \cdot \pi \cdot \kappa^2)/7} \quad (2.5)$$

Combining the above, we have that

$$\begin{aligned} Q &\leq \sum_{\mathbf{y} \in (\Lambda^{\perp}(A)^{+})^{\vee}} e^{-1/5 \cdot n' \ln n'} \cdot e^{-(\sigma^2 \cdot \pi \cdot \kappa^2)/7} \\ &\leq e^{-1/5 \cdot n' \ln n'} \cdot 2^{n'} \cdot \sum_{\mathbf{y} \in (\Lambda^{\perp}(A)^{+})^{\vee}} e^{-2(\sigma^2 \cdot \pi \cdot \kappa^2)/7} \\ &= e^{-1/5 \cdot n' \ln n'} \cdot 2^{n'} (1 + Q), \end{aligned}$$

where the first inequality follows from (2.4) and the definition of Q, the second inequality from (2.5), and the final equality from the definition of Q.

Thus we have that $(1 - e^{-1/5 \cdot n' \ln n'} \cdot 2^{n'})Q \leq e^{-1/5 \cdot n' \ln n'} \cdot 2^{n'}$ which implies that $Q \leq 2 \cdot e^{-1/5 n' \ln n'} \cdot 2^{n'} \leq 2^{-n'+1} \leq 2^{-\Omega(n)}$, assuming n' is at least 2^{10}. □

Corollary 2.10. Let k, l, σ and $\mathbf{c}$ be as in Theorem 2.9. Assume that $A = [I_k | \bar{A}] \in (R_q)^{k \times l}$ is chosen as in Theorem 2.9. Then, with probability $1 - 2^{-\Omega(n)}$ over the choice of $\bar{A}$, the distribution of $A\mathbf{x} \in R_q^k$, where $(\mathbf{x}, x_{n'}) \in R^l \times Z$ is chosen from $D_{R^l \times Z, \Psi_{\sigma,c}}$ satisfies that the probability of each of the q^{nk} possible outcomes is in the interval $(1 \pm 2^{-\Omega(n)})q^{-nk}$ (and in particular is within statistical distance $2^{-\Omega(n)}$ of the uniform distribution over R_q^k).

The proof appears in Appendix E.2.

Given the corollary, the analysis of Conditional Distribution III is complete. In particular, this means that the standard deviation used to sample $\mathbf{x}$ should be increased from $2n \cdot q^{k/l+2/(nl)}$ (as in [26]) to $\sqrt{14/5 \cdot n'/n \cdot \ln n'} \cdot 2n \cdot q^{k/l+2/(nl)}$.

3 Conclusions and Future Directions

In this work, we present a general approach for analyzing the leakage resilience of RLWE-based cryptosystems, by determining and analyzing the explicit PDF resulting from the conditional distribution of the RLWE secret given the leakage. Our approach can be used to provide a security analysis for existing cryptosystems in the presence of leakage, with appropriate choice of parameters (and *without* any modifications to the scheme). We instantiate our approach by considering three leakage settings and corresponding conditional distributions I, II and III.

A key technical tool in the analysis of conditional distribution II is extending the regularity lemma of [25]; to cases where $\mathbf{x}$ is drawn from a non-spherical Gaussian with standard deviation significantly *smaller* than the smoothing parameter in a constant fraction of the dimensions and larger than the smoothing parameter in the remaining dimensions. In the analysis of conditional distribution III we find applications of the Radial Fourier Transform to lattice-based cryptography.

Future Directions. We believe that our approach of generalizing the regularity lemma to conditional distributions can be used as an important tool in the security analysis of RLWE-based cryptosystems. In future work, we plan to extend our analysis to other conditional distributions, with implications for other leakage settings. A first candidate is generalizing conditional distribution II to (certain types of) multivariate Gaussians with covariance matrices that are not diagonal. Such a generalization would allow us to capture leakage of coordinates in the polynomial instead of canonical representation.

Bibliography

[1] Adi Akavia, Shafi Goldwasser and Vinod Vaikuntanathan, Simultaneous Hardcore Bits and Cryptography against Memory Attacks, in: *TCC 2009* (Omer Reingold, ed.), LNCS 5444, pp. 474–495, Springer, Heidelberg, March 2009.

[2] Martin R. Albrecht, Amit Deo and Kenneth G. Paterson, Cold Boot Attacks on Ring and Module LWE Keys Under the NTT, *IACR TCHES* **2018** (2018), 173–213, `https://tches.iacr.org/index.php/TCHES/article/view/7273`.

[3] Pauline Bert, Pierre-Alain Fouque, Adeline Roux-Langlois and Mohamed Sabt, Practical Implementation of Ring-SIS/LWE Based Signature and IBE, in: *Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018* (Tanja Lange and Rainer Steinwandt, eds.), pp. 271–291, Springer, Heidelberg, 2018.

[4] Madalina Bolboceanu, Zvika Brakerski, Renen Perlman and Devika Sharma, *Order-LWE and the Hardness of Ring-LWE with Entropic Secrets*, Cryptology ePrint Archive, Report 2018/494, 2018, `https://eprint.iacr.org/2018/494`.

[5] Elette Boyle, Gil Segev and Daniel Wichs, Fully Leakage-Resilient Signatures, *Journal of Cryptology* **26** (2013), 513–558.

[6] Zvika Brakerski, Yael Tauman Kalai, Jonathan Katz and Vinod Vaikuntanathan, Overcoming the Hole in the Bucket: Public-Key Cryptography Resilient to Continual Memory Leakage, in: *51st FOCS*, pp. 501–510, IEEE Computer Society Press, October 2010.

[7] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev and Damien Stehlé, Classical hardness of learning with errors, in: *45th ACM STOC* (Dan Boneh, Tim Roughgarden and Joan Feigenbaum, eds.), pp. 575–584, ACM Press, June 2013.

[8] Dong Pyo Chi, Jeong Woon Choi, Jeong San Kim and Taewan Kim, *Lattice Based Cryptography for Beginners*, Cryptology ePrint Archive, Report 2015/938, 2015, `https://eprint.iacr.org/2015/938`.

[9] Kai-Min Chung, Daniel Dadush, Feng-Hao Liu and Chris Peikert, On the lattice smoothing parameter problem, in: *Computational Complexity (CCC), 2013 IEEE Conference on*, IEEE, pp. 230–241, 2013.

[10] Dana Dachman-Soled, Huijing Gong, Mukul Kulkarni and Aria Shahverdi, *On the Leakage Resilience of Ideal-Lattice Based Public Key Encryption*, Cryptology ePrint Archive, Report 2017/1127, 2017, `https://eprint.iacr.org/2017/1127`.

[11] Dana Dachman-Soled, Huijing Gong, Mukul Kulkarni and Aria Shahverdi, *Partial Key Exposure in Ring-LWE-Based Cryptosystems: Attacks and Resilience*, Cryptology ePrint Archive, Report 2018/1068, 2018, `https://eprint.iacr.org/2018/1068`.

[12] Luc Devroye, Sample-based non-uniform random variate generation, in: *Proceedings of the 18th conference on Winter simulation*, ACM, pp. 260–265, 1986.

[13] Yevgeniy Dodis, Shafi Goldwasser, Yael Tauman Kalai, Chris Peikert and Vinod Vaikuntanathan, Public-Key Encryption Schemes with Auxiliary Inputs, in: *TCC 2010* (Daniele Micciancio, ed.), LNCS 5978, pp. 361–381, Springer, Heidelberg, February 2010.

[14] Yevgeniy Dodis, Kristiyan Haralambiev, Adriana López-Alt and Daniel Wichs, Cryptography against Continuous Memory Attacks, in: *51st FOCS*, pp. 511–520, IEEE Computer Society Press, October 2010.

[15] Yevgeniy Dodis, Yael Tauman Kalai and Shachar Lovett, On cryptography with auxiliary input, in: *41st ACM STOC* (Michael Mitzenmacher, ed.), pp. 621–630, ACM Press, May / June 2009.

[16] Stefan Dziembowski and Krzysztof Pietrzak, Leakage-Resilient Cryptography, in: *49th FOCS*, pp. 293–302, IEEE Computer Society Press, October 2008.

[17] Wolfgang Ebeling, *Lattices and codes*, Lattices and Codes, Springer, 2013, pp. 1–32.

[18] Thomas Espitau, Pierre-Alain Fouque, Benoit Gerard and Mehdi Tibouchi, *Side-Channel Attacks on BLISS Lattice-Based Signatures – Exploiting Branch Tracing Against strongSwan and Electromagnetic Emanations in Microcontrollers*, Cryptology ePrint Archive, Report 2017/505, 2017, `http://eprint.iacr.org/2017/505`.

[19] Craig Gentry, Chris Peikert and Vinod Vaikuntanathan, Trapdoors for hard lattices and new cryptographic constructions, in: *40th ACM STOC* (Richard E. Ladner and Cynthia Dwork, eds.), pp. 197–206, ACM Press, May 2008.

[20] Shafi Goldwasser, Yael Tauman Kalai, Chris Peikert and Vinod Vaikuntanathan, Robustness of the Learning with Errors Assumption, in: *ICS 2010* (Andrew Chi-Chih Yao, ed.), pp. 230–240, Tsinghua University Press, January 2010.

[21] Loukas Grafakos and Gerald Teschl, On Fourier Transforms of Radial Functions and Distributions, *Journal of Fourier Analysis and Applications* **19** (2013), 167–179.

[22] Jonathan Katz and Vinod Vaikuntanathan, Signature Schemes with Bounded Leakage Resilience, in: *ASIACRYPT 2009* (Mitsuru Matsui, ed.), LNCS 5912, pp. 703–720, Springer, Heidelberg, December 2009.

[23] Allison B. Lewko, Mark Lewko and Brent Waters, How to leak on key updates, in: *43rd ACM STOC* (Lance Fortnow and Salil P. Vadhan, eds.), pp. 725–734, ACM Press, June 2011.

[24] Vadim Lyubashevsky, Chris Peikert and Oded Regev, On Ideal Lattices and Learning with Errors over Rings, *J. ACM* **60** (2013), 43:1–43:35.

[25] Vadim Lyubashevsky, Chris Peikert and Oded Regev, A Toolkit for Ring-LWE Cryptography, in: *EUROCRYPT 2013* (Thomas Johansson and Phong Q. Nguyen, eds.), LNCS 7881, pp. 35–54, Springer, Heidelberg, May 2013.

[26] Vadim Lyubashevsky, Chris Peikert and Oded Regev, *A Toolkit for Ring-LWE Cryptography*, Cryptology ePrint Archive, Report 2013/293, 2013, `http://eprint.iacr.org/2013/293`.

[27] Tal Malkin, Isamu Teranishi, Yevgeniy Vahlis and Moti Yung, Signatures Resilient to Continual Leakage on Memory and Computation, in: *TCC 2011* (Yuval Ishai, ed.), LNCS 6597, pp. 89–106, Springer, Heidelberg, March 2011.

[28] Daniele Micciancio, Generalized Compact Knapsacks, Cyclic Lattices, and Efficient One-Way Functions, *Computational Complexity* **16** (2007), 365–411.

[29] Daniele Micciancio and Oded Regev, Worst-case to average-case reductions based on Gaussian measures, *SIAM Journal on Computing* **37** (2007), 267–302.

[30] Moni Naor and Gil Segev, Public-Key Cryptosystems Resilient to Key Leakage, *SIAM J. Comput.* **41** (2012), 772–814.

[31] Krzysztof Pietrzak, A Leakage-Resilient Mode of Operation, in: *EUROCRYPT 2009* (Antoine Joux, ed.), LNCS 5479, pp. 462–482, Springer, Heidelberg, April 2009.

[32] Oded Regev, On lattices, learning with errors, random linear codes, and cryptography, *Journal of the ACM (JACM)* **56** (2009), 34.

[33] Miruna Rosca, Damien Stehlé and Alexandre Wallet, On the Ring-LWE and Polynomial-LWE Problems, in: *EUROCRYPT 2018, Part I* (Jesper Buus Nielsen and Vincent Rijmen, eds.), LNCS 10820, pp. 146–173, Springer, Heidelberg, April / May 2018.

[34] Damien Stehlé and Ron Steinfeld, Making NTRU as Secure as Worst-Case Problems over Ideal Lattices, in: *EUROCRYPT 2011* (Kenneth G. Paterson, ed.), LNCS 6632, pp. 27–47, Springer, Heidelberg, May 2011.

[35] G.N. Watson, *A Treatise on the Theory of Bessel Functions*, Cambridge Mathematical Library, Cambridge University Press, 1995.

A Preliminaries and Definitions

A.1 Notation

For a positive integer n, we denote by $[n]$ the set $\{1, \ldots, n\}$. We denote vectors in boldface $\mathbf{x}$ and matrices using capital letters A. For vector $\mathbf{x}$ over $\mathbb{R}^n$ or $\mathbb{C}^n$, define the ℓ_2 norm as $\|\mathbf{x}\|_2 = \left(\sum_i |x_i|^2\right)^{1/2}$. We write as $\|\mathbf{x}\|$ for simplicity.

A.2 Lattices and background

Let $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ denote the cycle, i.e. the additive group of reals modulo 1. We also denote by $\mathbb{T}_q$ its cyclic subgroup of order q, i.e., the subgroup given by $\{0, 1/q, \ldots, (q-1)/q\}$.

Let H be a subspace, defined as $H \subseteq \mathbb{C}^{\mathbb{Z}_m^*}$, (for some integer $m \geq 2$),

$$H = \{\mathbf{x} \in \mathbb{C}^{\mathbb{Z}_m^*} : x_i = \overline{x_{m-i}}, \forall i \in \mathbb{Z}_m^*\}.$$

A *lattice* is a discrete additive subgroup of H. We exclusively consider the full-rank lattices, which are generated as the set of all linear integer combinations of some set of n linearly independent *basis* vectors $B = \{\mathbf{b}_j\} \subset H$:

$$\Lambda = \mathcal{L}(B) = \left\{ \sum_j z_j \mathbf{b}_j : z_j \in \mathbb{Z} \right\}.$$

The *determinant* of a lattice $\mathcal{L}(B)$ is defined as $|\det(B)|$, which is independent of the choice of basis B. The *minimum distance* $\lambda_1(\Lambda)$ of a lattice Λ (in the Euclidean norm) is the length of a shortest nonzero lattice vector.

The *dual lattice* of $\Lambda \subset H$ is defined as following, where $\langle \cdot, \cdot \rangle$ denotes the inner product.

$$\Lambda^\vee = \{\mathbf{y} \in H : \forall \mathbf{x} \in \Lambda, \langle \mathbf{x}, \overline{\mathbf{y}} \rangle = \sum_i x_i y_i \in \mathbb{Z}\}.$$

Note that, $(\Lambda^\vee)^\vee = \Lambda$, and $\det(\Lambda^\vee) = 1/\det(\Lambda)$.

Discretization

Discretization is an important procedure used in applications based on lattices, such as converting continuous Gaussian distribution (defined in Appendix B) into a discrete Gaussian distribution (Definition B.9). Given a lattice $\Lambda = \mathcal{L}(B)$ represented by some "good" basis $B = \{\mathbf{b}_i\}$, a point $\mathbf{x} \in H$, and a point $\mathbf{c} \in H$ representing a lattice coset $\Lambda + \mathbf{c}$, the discretization process outputs a point $\mathbf{y} \in \Lambda + \mathbf{c}$ such that the length of $\mathbf{y} - \mathbf{x}$ is not too large. This is denoted as $\mathbf{y} \leftarrow \lfloor \mathbf{x} \rceil_{\Lambda + \mathbf{c}}$. A discretization procedure is called *valid* if it is efficient; and depends only on the lattice coset $\Lambda + (\mathbf{c} - \mathbf{x})$, not on particular representative used to specify it.

Note that for a valid discretization, $\lfloor \mathbf{z} + \mathbf{x} \rceil_{\Lambda+\mathbf{c}}$ and $\mathbf{z} + \lfloor \mathbf{x} \rceil_{\Lambda+\mathbf{c}}$ are identically distributed for any $\mathbf{z} \in \Lambda$. For more details and actual description of algorithms used for discretization we refer the interested reader to [26].

A.3 Algebraic Number Theory

For a positive integer m, the m^{th} *cyclotomic number field* is a field extension $K = \mathbb{Q}(\zeta_m)$ obtained by adjoining an element ζ_m of order m (i.e. a primitive m^{th} root of unity) to the rationals. The minimal polynomial of ζ_m is the m^{th} *cyclotomic polynomial*

$$\Phi_m(X) = \prod_{i \in \mathbb{Z}_m^*} (X - \omega_m^i) \in \mathbb{Z}[X],$$

where $\omega_m \in \mathbb{C}$ is any primitive m^{th} root of unity in $\mathbb{C}$.

For every $i \in \mathbb{Z}_m^*$, there is an embedding $\sigma_i : K \to \mathbb{C}$, defined as $\sigma_i(\zeta_m) = \omega_m^i$. Let $n = \varphi(m)$, the totient of m. The *trace* $\mathrm{Tr} : K \to \mathbb{Q}$ and *norm* $\mathrm{N} : K \to \mathbb{Q}$ can be defined as the sum and product, respectively, of the embeddings:

$$\mathrm{Tr}(x) = \sum_{i \in [n]} \sigma_i(x) \text{ and } \mathrm{N}(x) = \prod_{i \in [n]} \sigma_i(x).$$

For any $x \in K$, the l_p *norm* of x is defined as $\|x\|_p = \|\sigma(x)\|_p = (\sum_{i \in [n]} |\sigma_i(x)|^p)^{1/p}$. We omit p when $p = 2$. Note that the appropriate notion of norm $\|\cdot\|$ is used throughout this paper depending on whether the argument is a vector over $\mathbb{C}^n$, or whether the argument is an element from K; whenever the context is clear.

A.4 Ring of Integers and Its Ideals

Let $R \subset K$ denote the set of all algebraic integers in a number field K. This set forms a ring (under the usual addition and multiplication operations in K), called the *ring of integers* of K. Ring of integers in K is written as $R = \mathbb{Z}[\zeta_m]$.

The (absolute) discriminant Δ_K of K measures the geometric sparsity of its ring of integers. The discriminant of the m^{th} cyclotomic number field K is

$$\Delta_K = \left(\frac{m}{\prod_{\text{prime } p|m} p^{1/(p-1)}} \right)^n \leq n^n,$$

in which the product in denominator runs over all the primes dividing m.

An (*integral*) *ideal* $\mathcal{I} \subseteq R$ is a non-trivial (i.e. $\mathcal{I} \neq \varnothing$ and $\mathcal{I} \neq \{0\}$) additive subgroup that is closed under multiplication by R, i,e., $r \cdot a \in \mathcal{I}$ for any $r \in R$

and $a \in \mathcal{I}$. The *norm* of an ideal $\mathcal{I} \subseteq R$ is the number of cosets of $\mathcal{I}$ as an addictive subgroup in R, defined as *index* of $\mathcal{I}$, i.e., $\mathrm{N}(\mathcal{I}) = |R/\mathcal{I}|$. Note that $\mathrm{N}(\mathcal{I}\mathcal{J}) = \mathrm{N}(\mathcal{I})\mathrm{N}(\mathcal{J})$.

A *fractional* ideal $\mathcal{I}$ in K is defined as a subset such that $\mathcal{I} \subseteq R$ is an integral ideal for some nonzero $d \in R$. Its norm is defined as $\mathrm{N}(\mathcal{I}) = \mathrm{N}(d\mathcal{I})/\mathrm{N}(d)$. An *ideal lattice* is a lattice $\sigma(\mathcal{I})$ embedded from a fractional ideal $\mathcal{I}$ by σ in H. The determinant of an ideal lattice $\sigma(\mathcal{I})$ is $\det(\sigma(\mathcal{I})) = \mathrm{N}(\mathcal{I}) \cdot \sqrt{\Delta_K}$. For simplicity, however, most often when discussing about ideal lattice, we omit mention of σ since no confusion is likely to arise.

Lemma A.1 ([26]). For any fractional ideal $\mathcal{I}$ in a number field K of degree n,

$$\sqrt{n} \cdot \mathrm{N}^{1/n}(\mathcal{I}) \leq \lambda_1(\mathcal{I}) \leq \sqrt{n} \cdot \mathrm{N}^{1/n}(\mathcal{I}) \cdot \sqrt{\Delta_K^{1/n}}.$$

For any *fractional* ideal $\mathcal{I}$ in K, its *dual* ideal is defined as

$$\mathcal{I}^\vee = \{a \in K : \mathrm{Tr}(a\mathcal{I}) \subset \mathbb{Z}\}.$$

Definition A.2. For $R = \mathbb{Z}[\zeta_m]$, define $g = \prod_p (1 - \zeta_p) \in R$, where p runs over all odd primes dividing m. Also, define $t = \frac{\hat{m}}{g} \in R$, where $\hat{m} = \frac{m}{2}$ if m is even, otherwise $\hat{m} = m$.

The dual ideal $R^\vee$ of R is defined as $R^\vee = \langle t^{-1} \rangle$, satisfying $R \subseteq R^\vee \subseteq \hat{m}^{-1}R$. For any fractional ideal $\mathcal{I}$, its dual is $\mathcal{I}^\vee = \mathcal{I}^{-1} \cdot R^\vee$. The quotient $R_q^\vee$ is defined as $R_q^\vee = R^\vee / qR^\vee$.

Fact A.3 ([26]). Assume that q is a prime satisfying $q = 1 \mod m$, so that $\langle q \rangle$ splits completely into n distinct ideals of norm q. The prime ideal factors of $\langle q \rangle$ are $\mathfrak{q}_i = \langle q \rangle + \langle \zeta_m - \omega_m^i \rangle$, for $i \in \mathbb{Z}_m^*$. By Chinese Reminder Theorem, the natural ring homomorphism $R/\langle q \rangle \to \prod_{i \in \mathbb{Z}_m^*} (R/\mathfrak{q}_i) \cong (\mathbb{Z}_q^n)$ is an isomorphism.

Lemma A.4. [26, Lemma 2.23] Let p and q be positive coprime integers, and $\lfloor \cdot \rceil$ be a valid discretization to (cosets of) $pR^\vee$. There exists an efficient transformation that on input $w \in R_p^\vee$ and a pair in $(a', b') \in R_q \times (K_\mathbb{R}/qR^\vee)$, outputs a pair $(a = pa' \bmod qR, b) \in R_q \times R_q^\vee$ with the following guarantees: if the input pair is uniformly distributed then so is the output pair; and if the input pair is distributed according to the RLWE distribution $A_{s,\psi}$ for some (unknown) $s \in R^\vee$ and distribution ψ over $K_\mathbb{R}$, then the output pair is distributed according to $A_{s,\chi}$, where $\chi = \lfloor p \cdot \psi \rceil_{w+pR^\vee}$.

Lemma A.5. [26, Lemma 2.24] Let p and q be positive coprime integers, $\lfloor \cdot \rceil$ be a valid discretization to (cosets of) $pR^\vee$, and w be an arbitrary element in $R_p^\vee$. If R-DLWE$_{q,\psi}$ is hard given l samples, then so is the variant of R-DLWE$_{q,\psi}$ in which the secret is sampled from $\chi := \lfloor p \cdot \psi \rceil_{w+pR^\vee}$, given $l-1$ samples.

B Regularity and Fourier Transforms

Let $\rho_{\mathbf{s},\mathbf{c}}$ denote an n-dimensional Gaussian function with standard deviation $\mathbf{s}$ and mean $\mathbf{c}$.

One and Multi-Dimensional Gaussians. For $s > 0$, $c \in \mathbb{R}$, $x \in \mathbb{R}$, define the Gaussian function $\rho^1_{s,c} : \mathbb{R} \to (0, 1]$ as

$$\rho^1_{s,c}(x) := e^{\frac{-\pi(x-c)^2}{s^2}}.$$

When $c = 0$, we write for simplicity,

$$\rho^1_{s}(x) := e^{\frac{-\pi(x)^2}{s^2}}.$$

By normalizing this function we obtain the *continuous* Gaussian probability distribution $\psi^1_{s,c}$ (resp. ψ^1_s) of parameter s, whose density is given by $s^{-1} \cdot \rho^1_{s,c}(x)$ (resp. $s^{-1} \cdot \rho^1_s(x)$).

We denote by $\rho_{(s_1,\ldots,s_n),(c_1,\ldots,c_n)}$ the distribution over $\mathbb{R}^n$ with the following pdf:

Let $\rho^1_{s,c}$ denote a one-dimensional Gaussian function as above with standard deviation s and mean c.We denote by $\rho_{(s_1,\ldots,s_n),(c_1,\ldots,c_n)}$ the distribution over $\mathbb{R}^n$ with the following pdf:

$$\rho_{(s_1,\ldots,s_n),(c_1,\ldots,c_n)}(x_1,\ldots,x_n) := \rho^1_{s_1,c_1}(x_1)\cdots\rho^1_{s_n,c_n}(x_n).$$

When $c = \mathbf{0}$, we again write for simplicity, $\rho_{(s_1,\ldots,s_n)}$. Moreover, when $s_1 = \cdots = s_n$ and the dimension is clear from context we write for simplicity $\rho_{s,(c_1,\ldots,c_n)}$ (resp. ρ_s). Normalizing as above, we obtain the corresponding *continuous* Gaussian probability distribution $\psi_{(s_1,\ldots,s_n),(c_1,\ldots,c_n)}$ (resp. $\psi_{(s_1,\ldots,s_n)}$, $\psi_{s,(c_1,\ldots,c_n)}$, ψ_s).

Definition B.1 (**Fourier Transform**). Given an integrable function $f : \mathbb{R}^n \to \mathbb{C}$, we denote by $\widehat{f} : \mathbb{R}^n \to \mathbb{C}$ the Fourier transform of f, defined as

$$\widehat{f}(\mathbf{y}) := \int_{\mathbb{R}^n} f(\mathbf{x}) e^{-2\pi i \langle x,y \rangle}\, \mathrm{d}\mathbf{x}.$$

Theorem B.2 (Poisson Summation Formula). *:Let $\Lambda \subset \mathbb{R}^n$ be an arbitrary lattice of dimension n, and let $f : \mathbb{R}^n \to \mathbb{C}$ be an appropriate function* [8] *Then*

$$f(\Lambda) = \frac{1}{\det(\Lambda)} \widehat{f}(\Lambda^\vee),$$

where $\Lambda^\vee$ is the dual lattice of Λ and $\widehat{f}$ is a Fourier transform of f.

Definition B.3. For an n-dimensional lattice Λ, and positive real $\varepsilon > 0$, we define its smoothing parameter $\eta_\varepsilon(\Lambda)$ to be the smallest s such that $\rho_{1/s}(\Lambda^\vee \setminus \{\mathbf{0}\}) \leq \varepsilon$.

Lemma B.4. [9, 29] For any n-dimensional lattice Λ, we have $\frac{\sqrt{\ln(1/\varepsilon)}}{\sqrt{\pi}\lambda_1(\Lambda^\vee)} \leq \eta_\varepsilon(\Lambda) \leq \frac{\sqrt{n}}{\lambda_1(\Lambda^\vee)}$, for $\varepsilon \in [2^{-n}, 1]$.

Claim B.5 ([26]). *For any n-dimensional lattice Λ and $\varepsilon, s > 0$,*

$$\rho_{1/s}(\Lambda) \leq \max\left(1, \left(\frac{\eta_\varepsilon(\Lambda^\vee)}{s}\right)^n\right)(1+\varepsilon).$$

Lemma B.6. For any n-dimensional lattice Λ and $\varepsilon > 0$, $\mathbf{s} := (s_1, \ldots, s_n) \in \mathbb{R}^n_{>0}$, and $\mathbf{c} := (c_1, \ldots, c_n) \in \mathbb{R}^n$, if all of $s_1, \ldots, s_n < \eta_\varepsilon(\Lambda^\vee)$ then

$$\rho_{(1/s_1,\ldots,1/s_n),(c_1,\ldots,c_n)}(\Lambda) \leq \left(\frac{\eta_\varepsilon(\Lambda^\vee)}{s_1} \cdots \frac{\eta_\varepsilon(\Lambda^\vee)}{s_n}\right)(1+\varepsilon).$$

Proof. Applying Poisson summation formula twice, using the fact that for all vectors $\mathbf{x} \in \mathbb{R}^n$, $\widehat{\rho}_{(1/s_1,\ldots,1/s_n),(c_1,\ldots,c_n)}(\mathbf{x}) \leq (s_1)^{-1} \cdots (s_n)^{-1} \cdot \rho_{(s_1,\ldots,s_n)}(\mathbf{x})$, and the fact that $\widehat{\rho}_{\eta_\varepsilon(\Lambda^\vee)} = \eta_\varepsilon(\Lambda^\vee)^n \cdot \rho_{1/\eta_\varepsilon(\Lambda^\vee)}$, we have:

$$\begin{aligned}
\rho_{(1/s_1,\ldots,1/s_n),(c_1,\ldots,c_n)}(\Lambda) &\leq \det(\Lambda)^{-1}(s_1)^{-1} \cdots (s_n)^{-1} \cdot \rho_{(s_1,\ldots,s_n)}(\Lambda^\vee) \\
&\leq \det(\Lambda)^{-1}(s_1)^{-1} \cdots (s_n)^{-1} \cdot \rho_{\eta_\varepsilon(\Lambda^\vee)}(\Lambda^\vee) \\
&= (s_1)^{-1} \cdots (s_n)^{-1} \cdot \eta_\varepsilon(\Lambda^\vee)^n \cdot \rho_{1/\eta_\varepsilon(\Lambda^\vee)}(\Lambda) \\
&\leq \left(\frac{\eta_\varepsilon(\Lambda^\vee)}{s_1} \cdots \frac{\eta_\varepsilon(\Lambda^\vee)}{s_n}\right)(1+\varepsilon).
\end{aligned}$$

where the last inequality follows from the definition of $\eta_\varepsilon(\Lambda^\vee)$.

□

[8] Assume that (1). $\int_{\mathbb{R}^n} |f(x)|dx < \infty$. (2). Function $f(\Lambda + u)$ is continuous on $\mathbb{R}^n$. (3). The series $\widehat{f}(\Lambda^\vee)$ is absolutely convergent. (See [17] for details)

Lemma B.7. [29, Lemma 3.6] For any lattice Λ, positive real $s > 0$ and a vector $\mathbf{c}$, $\rho_{s,\mathbf{c}}(\Lambda) \leq \rho_s(\Lambda)$.

Definition B.8. Let Λ be an n-dimensional lattice and Ψ a probability distribution over $\mathbb{R}^n$. Define the discrete probability distribution of Ψ over Λ to be:

$$D_{\Lambda,\Psi}(\mathbf{x}) = \frac{\Psi(\mathbf{x})}{\Psi(\Lambda)}, \forall \mathbf{x} \in \Lambda.$$

Definition B.9. Let Λ be an n-dimensional lattice, define the discrete Gaussian probability distribution over Λ with parameter $(s_1, \ldots, s_n)$ and center $(c_1, \ldots, c_n)$ as

$$D_{\Lambda,(s_1,\ldots,s_n),(c_1,\ldots,c_n)}(\mathbf{x}) = \frac{\rho_{(s_1,\ldots,s_n),(c_1,\ldots,c_n)}(\mathbf{x})}{\rho_{(s_1,\ldots,s_n),(c_1,\ldots,c_n)}(\Lambda)}, \forall \mathbf{x} \in \Lambda.$$

Remark B.10. Whenever Ψ is Gaussian with parameter $(s_1, \ldots, s_n)$ and center $(c_1, \ldots, c_n)$ we denote it's discrete Gaussian probability by $D_{\Lambda,(s_1,\cdots,s_n),(c_1,\ldots,c_n)}$. If $s = s_1 = \cdots = s_n$ (resp. $c = c_1 = \cdots = c_n$) we write $D_{\Lambda,s,(c_1,\ldots,c_n)}$ (resp. $D_{\Lambda,(s_1,\ldots,s_n),c}$). If $c_1 = \cdots = c_n = 0$ we write $D_{\Lambda,(s_1,\cdots,s_n)}$.

Lemma B.11. [29, Lemma 4.4] For any n'-dimensional lattice Λ, and reals $0 < \varepsilon < 1, s \geq \eta_\varepsilon(\Lambda)$, we have

$$\Pr_{\mathbf{x} \sim D_{\Lambda,\psi_s}} \left(\|\mathbf{x}\| > s\sqrt{n'} \right) \leq \frac{1+\varepsilon}{1-\varepsilon} \cdot 2^{-n'}.$$

The following is a modified version of Lemma 3.8 from [32].

Lemma B.12. Let Λ be an n-dimensional lattice and Ψ a probability distribution over $\mathbb{R}^n$. If $|\widehat{\Psi}|(\Lambda^\vee \setminus \{\mathbf{0}\}) \leq \varepsilon$, then for any $\mathbf{c} \in \mathbb{R}^n$, $\Psi(\Lambda + \mathbf{c}) \in \det(\Lambda^\vee)(1 \pm \varepsilon)$, where $|\widehat{\Psi}|(\Lambda^\vee \setminus \{\mathbf{0}\})$ denotes the summation of the absolute value of the function at each point in $\Lambda^\vee \setminus \{\mathbf{0}\}$.

Proof. First, since Ψ is a pdf, we have that $\widehat{\Psi}(\mathbf{0}) = 1$. We have:

$$\begin{aligned}
\Psi(\Lambda + \mathbf{c}) &= \det(\Lambda^\vee) \sum_{\mathbf{y}\in\Lambda^\vee} \widehat{\Psi}(\mathbf{y}) e^{2\pi i <\mathbf{c},\mathbf{y}>} \\
&\in \det(\Lambda^\vee) \left(1 \pm \sum_{\mathbf{y}\in\Lambda^\vee\setminus\{\mathbf{0}\}} |\widehat{\Psi}(\mathbf{y}) e^{2\pi i <\mathbf{c},\mathbf{y}>}|\right) \\
&\subseteq \det(\Lambda^\vee) \left(1 \pm \sum_{\mathbf{y}\in\Lambda^\vee\setminus\{\mathbf{0}\}} \widehat{\Psi}(\mathbf{y})\right) \\
&\subseteq \det(\Lambda^\vee)(1 \pm \varepsilon),
\end{aligned}$$

where the equality follows from properties of the Fourier transform. □

The proof of the following lemma proceeds as the proof of Corollary 2.8 in [19].

Lemma B.13. Let Λ' be an n-dimensional lattice and Ψ a probability distribution over $\mathbb{R}^n$. Assume that for all $\mathbf{c} \in \mathbb{R}^n$ it is the case that

$$\Psi(\Lambda' + \mathbf{c}) \in \left[\frac{1-\varepsilon}{1+\varepsilon}, \frac{1+\varepsilon}{1-\varepsilon}\right] \cdot \Psi(\Lambda'),$$

Let Λ be an n-dimensional lattice such that $\Lambda' \subseteq \Lambda$ then the distribution of $(D_{\Lambda,\Psi} \bmod \Lambda')$ is within statistical distance of at most 4ε of uniform over $(\Lambda \bmod \Lambda')$.

Definition B.14. For a matrix $A \in R_q^{k\times l}$ we define $\Lambda^\perp(A) = \{\mathbf{z} \in R^l : A\mathbf{z} = 0 \bmod qR\}$, which we identify with a lattice in H^l. Its dual lattice (which is again a lattice in H^l) is denoted by $\Lambda^\perp(A)^\vee$.

Theorem B.15. [26] *Let R be the ring of integers in the m^{th} cyclotomic number field K of degree n, and $q \geq 2$ an integer. For positive integers $k \leq l \leq \mathrm{poly}(n)$, let $A = [I_k|\bar{A}] \in (R_q)^{k\times l}$, where $I_k \in (R_q)^{k\times k}$ is the identity matrix and $\bar{A} \in (R_q)^{k\times(l-k)}$ is uniformly random. Then for all $s \geq 2n$,*

$$\mathbb{E}_{\bar{A}}\left[\rho_{1/s}\left(\Lambda^\perp(A)^\vee\right)\right] \leq 1 + 2(s/n)^{-nl} q^{kn+2} + 2^{-\Omega(n)}.$$

In particular, if $s > 2n \cdot q^{k/l+2/(nl)}$ then $\mathbb{E}_{\bar{A}}\left[\rho_{1/s}\left(\Lambda^\perp(A)^\vee\right)\right] \leq 1 + 2^{-\Omega(n)}$, and so by Markov's inequality, $\eta_{2^{-\Omega(n)}}(\Lambda^\perp(A)) \leq s$ except with probability at most $2^{-\Omega(n)}$.

The following corollary was presented in [26].

Corollary B.16. Let R, n, q, k and l be as in Theorem B.15. Assume that $A = [I_k|\bar{A}] \in (R_q)^{k\times l}$ is chosen as in Theorem B.15. Then, with probability $1-2^{-\Omega(n)}$ over the choice of $\bar{A}$, the distribution of $A\mathbf{x} \in R_q^k$, where each coordinate of $\mathbf{x} \in R_q^l$ is chosen from a discrete Gaussian distribution of parameter $s > 2n\cdot q^{k/l+2/(nl)}$ over R, satisfies that the probability of each of the q^{nk} possible outcomes is in the interval $(1 \pm 2^{-\Omega(n)})q^{-nk}$ (and in particular is within statistical distance $2^{-\Omega(n)}$ of the uniform distribution over R_q^k).

We next state an additional corollary of the regularity theorem from [26].

Corollary B.17. Let R, n, q, k and l be as in Theorem B.15. Assume that $A = [I_k|\bar{A}] \in (R_q)^{k\times l}$ is chosen as in Theorem B.15. Then, with probability $1-2^{-\Omega(n)}$ over the choice of $\bar{A}$, the shortest non-zero vector in $\Lambda^{\perp}(A)^{\vee}$ has length at least $\frac{\sqrt{n/\pi}}{2n\cdot q^{k/l+2/(nl)}}$.

C Proof of Theorem 2.8

In this section, we prove the following theorem, which provides an upper bound on the Fourier transform of a pdf for the analysis of Conditional Distribution III in Section 2.3.

Theorem 2.8. Let $n' := l \cdot 2^a + 1$, where l, a are positive integers and $a > 2$, and $c \leq \sigma \cdot \sqrt{2} \cdot \sqrt{n'}$. Let $\Psi_{\sigma,c}$ denote the normalized pdf corresponding to the non-normalized function $f(\mathbf{x}) := e^{-\frac{\pi(\|\mathbf{x}\|-c)^2}{\sigma^2}} + e^{-\frac{\pi(\|\mathbf{x}\|+c)^2}{\sigma^2}}$, where $\mathbf{x}$ is a vector over n' dimensions. and let $\widehat{\Psi_{\sigma,c}}(\mathbf{y})$ denote the n'-dimensional Fourier transform of $\Psi_{\sigma,c}$. Then $|\widehat{\Psi_{\sigma,c}}(\mathbf{y})| \leq n'^{n'} \cdot e^{-\pi\|\mathbf{y}\|^2\sigma^2}$ for $\|\mathbf{y}\| > 1/\sigma$.

The following lemma computes a lower bound of the normalization factor of the pdf in Theorem 2.8. Once we prove the lemma, we proceed to the proof of Theorem 2.8.

Lemma C.1. Let $n' \in \mathbb{N}$ be odd, $\mathbf{x} \in \mathbb{R}^{n'}$, $c \in \mathbb{R}$. Then

$$\int_{R^{n'}} e^{-\frac{\pi(\|\mathbf{x}\|-c)^2}{\sigma^2}} + e^{-\frac{\pi(\|\mathbf{x}\|+c)^2}{\sigma^2}} \, \mathrm{d}\mathbf{x} \geq \sigma^{n'}.$$

Proof. Let $f(\mathbf{x}) := e^{-\frac{\pi(\|\mathbf{x}\|-c)^2}{\sigma^2}} + e^{-\frac{\pi(\|\mathbf{x}\|+c)^2}{\sigma^2}}$. Let $r = \|\mathbf{x}\|$. Since f is a radial function, we slightly abuse notation and denote by $f(r) := e^{-\frac{\pi(r-c)^2}{\sigma^2}} + e^{-\frac{\pi(r+c)^2}{\sigma^2}}$.

Now, we have that

$$\int_{R^{n'}} f(\mathbf{x})\,\mathrm{d}\mathbf{x} = n' V_{n'} \int_0^\infty r^{n'-1} f(r)\,\mathrm{d}r, \tag{C.1}$$

where $V_{n'}$ denotes the volume of n'-dimensional ball $V_{n'} = \frac{\pi^{n'/2}}{\Gamma(1+n'/2)}$. Since f is an even function and n' is odd, so $r^{n'-1}$ is an even function, we have that $r^{n'-1} f(r)$ is even and so

$$\int_0^\infty r^{n'-1} f(r)\,\mathrm{d}r = 1/2 \int_{-\infty}^\infty r^{n'-1} f(r)\,\mathrm{d}r. \tag{C.2}$$

Let $a = \pi/\sigma^2$. Since n' is odd, we now have that

$$\begin{aligned}
&\int_{-\infty}^{\infty} e^{-a(r-c)^2} r^{n'-1}\,\mathrm{d}r \\
&= \int_{-\infty}^{\infty} e^{-at^2} (t+c)^{n'-1}\,\mathrm{d}t = \int_{-\infty}^{\infty} e^{-at^2} \sum_{j=0}^{n'-1} \binom{n'-1}{j} c^j t^{n'-1-j}\,\mathrm{d}t \\
&= \sum_{j=0}^{n'-1} \binom{n'-1}{j} c^j \int_{-\infty}^{\infty} e^{-at^2} t^{n'-1-j}\,\mathrm{d}t \\
&= \sum_{j=0}^{n'-1} \binom{n'-1}{j} c^j \frac{1}{2}(-1)^j \left((-1)^{n'+1} + (-1)^j\right) a^{\frac{1}{2}(-n'+j)} \Gamma\left(\frac{n'-j}{2}\right) \\
&= \sum_{j=0}^{\frac{n'-1}{2}} \binom{n'-1}{2j} c^{2j} a^{\frac{1}{2}(-n'+2j)} \Gamma\left(\frac{n'-2j}{2}\right) \\
&\geq a^{-\frac{1}{2}n'} \Gamma\left(\frac{n'}{2}\right)
\end{aligned}$$

Combining the above with (C.1) and (C.2) and substituting for a, we get that $\int_{R^{n'}} f(\mathbf{x})\,\mathrm{d}\mathbf{x} \geq \sigma^{n'}$, which completes the proof of the lemma. □

Proof of Theorem 2.8. Let N be the normalization of $f(\mathbf{x})$ over n' dimensions. We have from Lemma C.1 that $N \geq \sigma^{n'}$ Thus, it remains to show that for $n' := l \cdot 2^a + 1$ and $c \leq \sigma \cdot \sqrt{2} \cdot \sqrt{n'}$, $\widehat{f}(\mathbf{y}) \leq \sigma^{n'} \cdot n'^{5/4} \cdot e^{-\pi \|\mathbf{y}\|^2 \sigma^2}$.

Let $r := \|\mathbf{x}\|$, we slightly abuse notation and view f as a function of r, $f(r) := e^{-\frac{\pi(r-c)^2}{\sigma^2}} + e^{-\frac{\pi(r+c)^2}{\sigma^2}}$. Since $\Psi_{\sigma,c}$ is a radial function, so is its Fourier transform, thus, we again slightly abuse notation and view $F := \widehat{f}$ as a function of $\kappa := \|\mathbf{y}\|$.

We may now use the formula for the radial Fourier transform of an n'-dimensional, radial function f to find F [21]:

$$F(\kappa) = \kappa^{\frac{-(n'-2)}{2}}(2\pi)\int_0^\infty r^{\frac{n'-2}{2}} f(r) J_{\frac{n'-2}{2}}(2\pi\kappa r) r \, \mathrm{d}r, \tag{C.3}$$

where $J_{\frac{n'-2}{2}}$ denotes the Bessel function of the first kind of order $\frac{n'-2}{2}$. The Bessel function of first kind of order ν is defined as [35, Page 40]:

$$J_\nu(z) := \sum_{j=0}^{\infty} \frac{(-1)^j (\frac{1}{2}z)^{\nu+2j}}{\Gamma(\nu+j+1)j!}. \tag{C.4}$$

For half-integer order $\nu := n + \frac{1}{2}$, there is a closed-form representation of J_ν. Specifically, it can be expressed as [35, Page 298]:

$$J_{n+\frac{1}{2}}(z) := R_{n,\frac{1}{2}}(z)\left(\frac{2}{\pi z}\right)^{\frac{1}{2}} \sin z - R_{n-1,\frac{3}{2}}(z)\left(\frac{2}{\pi z}\right)^{\frac{1}{2}} \cos z. \tag{C.5}$$

where $R_{n,\frac{1}{2}}(z)$ and $R_{n-1,\frac{3}{2}}(z)$ are Lommel polynomials defined as [35, Page 296]:

$$R_{n,\nu}(z) = \sum_{j=0}^{[n/2]} \frac{(-1)^j (n-j)!\Gamma(\nu+n-j)}{j!(n-2j)!\Gamma(\nu+j)} \left(\frac{z}{2}\right)^{2j-n}, \tag{C.6}$$

where the $[x]$ means the largest integer not exceeding x.

We now have:

$$\begin{aligned}
|F(\kappa)| &= \left|\kappa^{\frac{-(n'-2)}{2}}(2\pi)\int_0^\infty r^{\frac{n'-2}{2}} f(r) J_{\frac{n'-2}{2}}(2\pi\kappa r) r \, \mathrm{d}r\right| \\
&= \left|\kappa^{\frac{-(n'-2)}{2}}(2\pi)\left(\int_0^\infty r^{\frac{n'-2}{2}} f(r)\left(\sum_{j=0}^{[\frac{n'-3}{4}]} c_j \left(\frac{2\pi\kappa r}{2}\right)^{2j-\frac{n'-3}{2}}\right)\left(\frac{2}{2\pi^2\kappa r}\right)^{\frac{1}{2}} \sin(2\pi\kappa r) r \, \mathrm{d}r - \right.\right. \\
&\quad \left.\left. \int_0^\infty r^{\frac{n'-2}{2}} f(r)\left(\sum_{j=0}^{[\frac{n'-5}{4}]} c'_j \left(\frac{2\pi\kappa r}{2}\right)^{2j-\frac{n'-5}{2}}\right)\left(\frac{2}{2\pi^2\kappa r}\right)^{\frac{1}{2}} \cos(2\pi\kappa r) r \, \mathrm{d}r\right)\right| \\
&\leq \kappa^{\frac{-(n'-2)}{2}}(2\pi)\left(\left|\int_0^\infty r^{\frac{n'-2}{2}} f(r)\left(\sum_{j=0}^{[\frac{n'-3}{4}]} c_j \left(\frac{2\pi\kappa r}{2}\right)^{2j-\frac{n'-3}{2}}\right)\left(\frac{2}{2\pi^2\kappa r}\right)^{\frac{1}{2}} \sin(2\pi\kappa r) r \, \mathrm{d}r\right| + \right. \\
&\quad \left.\left|\int_0^\infty r^{\frac{n'-2}{2}} f(r)\left(\sum_{j=0}^{[\frac{n'-5}{4}]} c'_j \left(\frac{2\pi\kappa r}{2}\right)^{2j-\frac{n'-5}{2}}\right)\left(\frac{2}{2\pi^2\kappa r}\right)^{\frac{1}{2}} \cos(2\pi\kappa r) r \, \mathrm{d}r\right|\right),
\end{aligned} \tag{C.7}$$

where the first equality follows from (C.3), the second equality follows from (C.5), (C.6) and the settings of $c_j := \frac{(-1)^j(\frac{n'-3}{2}-j)!\Gamma(\frac{1}{2}+\frac{n'-3}{2}-j)}{j!(\frac{n'-3}{2}-2j)!\Gamma(\frac{1}{2}+j)}$ and $c'_j := \frac{(-1)^j(\frac{n'-5}{2}-j)!\Gamma(\frac{1}{2}+\frac{n'-3}{2}-j)}{j!(\frac{n'-5}{2}-2j)!\Gamma(\frac{1}{2}+1+j)}$.

In order to bound (C.7), we will individually upper bound

$$\text{I:} \left| \int_0^\infty r^{\frac{n'-2}{2}} f(r) \left(\sum_{j=0}^{[\frac{n'-3}{4}]} c_j \left(\frac{2\pi\kappa r}{2}\right)^{2j-\frac{n'-3}{2}} \right) \left(\frac{2}{2\pi^2\kappa r}\right)^{\frac{1}{2}} \sin(2\pi\kappa r) r \, \mathrm{d}r \right|$$

and

$$\text{II:} \left| \int_0^\infty r^{\frac{n'-2}{2}} f(r) \left(\sum_{j=0}^{[\frac{n'-5}{4}]} c'_j \left(\frac{2\pi\kappa r}{2}\right)^{2j-\frac{n'-5}{2}} \right) \left(\frac{2}{2\pi^2\kappa r}\right)^{\frac{1}{2}} \cos(2\pi\kappa r) r \, \mathrm{d}r \right|.$$

Recalling that $f(r) = e^{-\frac{\pi(r-c)^2}{\sigma^2}} + e^{-\frac{\pi(r+c)^2}{\sigma^2}}$, we have that

$$\begin{aligned}
\text{II} &= \left| \int_0^\infty r^{\frac{n'-2}{2}} f(r) \left(\sum_{j=0}^{[\frac{n'-5}{4}]} c'_j \left(\frac{2\pi\kappa r}{2}\right)^{2j-\frac{n'-5}{2}} \right) \left(\frac{2}{2\pi^2\kappa r}\right)^{\frac{1}{2}} \cos(2\pi\kappa r) r \, \mathrm{d}r \right| \\
&= 1/2 \left| \int_{-\infty}^\infty r^{\frac{n'-2}{2}} f(r) \left(\sum_{j=0}^{[\frac{n'-5}{4}]} c'_j \left(\frac{2\pi\kappa r}{2}\right)^{2j-\frac{n'-5}{2}} \right) \left(\frac{2}{2\pi^2\kappa r}\right)^{\frac{1}{2}} \left(\frac{e^{i2\pi\kappa r} + e^{-i2\pi\kappa r}}{2}\right) r \, \mathrm{d}r \right| \\
&= 1/2 \left(\frac{1}{4\pi^2\kappa}\right)^{\frac{1}{2}} \left| \int_{-\infty}^\infty r^{\frac{n'-1}{2}} f(r) \left(\sum_{j=0}^{[\frac{n'-5}{4}]} c'_j \left(\frac{2\pi\kappa r}{2}\right)^{2j-\frac{n'}{2}+\frac{5}{2}} \right) (e^{i2\pi\kappa r} + e^{-i2\pi\kappa r}) \, \mathrm{d}r \right| \\
&\leq 1/2 \left(\frac{1}{4\pi^2\kappa}\right)^{\frac{1}{2}} \sum_{j=0}^{[\frac{n'-5}{4}]} |c'_j| \left(\pi\kappa\right)^{2j-\frac{n'}{2}+\frac{5}{2}} \left| \int_{-\infty}^\infty r^{2j+2} \left(e^{-\frac{\pi(r-c)^2}{\sigma^2}} + e^{-\frac{\pi(r+c)^2}{\sigma^2}} \right) (e^{i2\pi\kappa r} + e^{-i2\pi\kappa r}) \, \mathrm{d}r \right|,
\end{aligned} \tag{C.8}$$

where the second equality follows since $f(r)$ is an even function, $\cos(2\pi\kappa r)$ is an even function and for $n' = l \cdot 2^a + 1$, all powers of r in the integrand are even, which means that the entire integrand is an even function.

To compute an upper bound on

$$\left| \int_{-\infty}^\infty r^{2j+2} \left(e^{-\frac{\pi(r-c)^2}{\sigma^2}} + e^{-\frac{\pi(r+c)^2}{\sigma^2}} \right) (e^{i2\pi\kappa r} + e^{-i2\pi\kappa r}) \, \mathrm{d}r \right| \tag{C.9}$$

as above, we integrate each term separately. Since the analysis is essentially the same for each term, we focus on upper bounding the term $A := \left| \int_{-\infty}^\infty e^{-\frac{\pi(r-c)^2}{\sigma^2}} e^{i2\pi\kappa r} \, \mathrm{d}r \right| = \left| e^{-\pi\kappa^2\sigma^2 + 2\pi i\kappa c} \int_{-\infty}^\infty e^{-\pi\sigma^{-2}(r-(c+i\kappa\sigma^2))^2} \, \mathrm{d}r \right|$:

$$
\begin{aligned}
A &= \left|e^{-\pi\kappa^2\sigma^2+2\pi i\kappa c}\right| \cdot \left|\int_{-\infty}^{\infty} r^{2j+2} e^{-\pi\sigma^{-2}(r-(c+i\kappa\sigma^2))^2}\,\mathrm{d}r\right| \\
&\leq e^{-\pi\kappa^2\sigma^2}\left|\int_{-\infty}^{\infty}\Big(\frac{\sigma}{\sqrt{\pi}}r' + (c+i\kappa\sigma^2)\Big)^{2j+2} e^{-r'^2}\frac{\sigma}{\sqrt{\pi}}\,\mathrm{d}r'\right| \\
&= e^{-\pi\kappa^2\sigma^2}\left|\int_{-\infty}^{\infty}\sigma^{2j+2}\Big(\frac{1}{\sqrt{\pi}}r' + (\frac{c}{\sigma}+i\kappa\sigma)\Big)^{2j+2} e^{-r'^2}\frac{\sigma}{\sqrt{\pi}}\,\mathrm{d}r'\right| \\
&\leq e^{-\pi\kappa^2\sigma^2}\left|\int_{-\infty}^{\infty}\sigma^{2j+2}\Big(\frac{1}{\sqrt{\pi}}r' + (\frac{c}{\sigma}+\kappa\sigma)\Big)^{2j+2} e^{-r'^2}\frac{\sigma}{\sqrt{\pi}}\,\mathrm{d}r'\right| \\
&\leq e^{-\pi\kappa^2\sigma^2}\Big(\frac{\sigma}{\sqrt{\pi}}\Big)^{2j+3}\Big(\frac{c}{\sigma}+\kappa\sigma\Big)^{2j+2}\binom{2j+2}{j+1}\int_{-\infty}^{\infty} r'^{2j+2}e^{-r'^2}\,\mathrm{d}r \\
&\leq e^{-\pi\kappa^2\sigma^2}\Big(\frac{\sigma}{\sqrt{\pi}}\Big)^{2j+3}\Big(\frac{c}{\sigma}+\kappa\sigma\Big)^{2j+2}\binom{2j+2}{j+1}\frac{1}{2}(1+(-1)^{2j})\Gamma\Big(\frac{3}{2}+j\Big) \\
&\leq e^{-\pi\kappa^2\sigma^2}\Big(\frac{\sigma}{\sqrt{\pi}}\Big)^{2j+3}\Big(\frac{c}{\sigma}+\kappa\sigma\Big)^{2j+2}\binom{2j+2}{j+1}\Gamma\Big(\frac{3}{2}+j\Big)
\end{aligned}
$$

Thus, we have that

$$
(\text{C.9}) \leq \Big(\frac{\sigma}{\sqrt{\pi}}\Big)^{2j+3} e^{-\pi\kappa^2\sigma^2}\Gamma(\frac{3}{2}+j)\binom{2j+2}{j+1}\left[4(\frac{c}{\sigma}+\kappa\sigma)^{2j+2}\right]
$$

Plugging the above back into (C.8), and recalling that $|c'_j| = \frac{(\frac{n'-5}{2}-j)!\Gamma(\frac{1}{2}+\frac{n'-3}{2}-j)}{j!(\frac{n'-5}{2}-2j)!\Gamma(\frac{1}{2}+1+j)}$, we have that

$$
\begin{aligned}
\text{II} &\leq 1/2\Big(\frac{1}{4\pi^2\kappa}\Big)^{\frac{1}{2}}\sum_{j=0}^{[\frac{n'-5}{4}]}|c'_j|\Big(\pi\kappa\Big)^{2j-\frac{n'}{2}+\frac{5}{2}}\Big(\frac{\sigma}{\sqrt{\pi}}\Big)^{2j+3}e^{-\pi\kappa^2\sigma^2}\Gamma(\frac{3}{2}+j)\binom{2j+2}{j+1}^2\Big(\frac{c}{\sigma}\Big)^{2j+2}\Big(\kappa\sigma\Big)^{2j+2} \\
&\leq 1/2\Big(\frac{1}{2\pi}\Big)e^{-\pi\kappa^2\sigma^2}\sum_{j=0}^{[\frac{n'-5}{4}]}(\pi)^{j-\frac{n'}{2}+1}\binom{\frac{n'-5}{2}-j}{j}\binom{2j+2}{j+1}^2\Gamma\Big(\frac{n'}{2}-1-j\Big)\,\sigma^{2j+3}\,c^{2j+2}\,\Big(\kappa\Big)^{4j-\frac{n'}{2}+4} \\
&\leq 1/2\Big(\frac{1}{2\pi}\Big)e^{-\pi\kappa^2\sigma^2}\,\Big(n'\cdot 2^{\frac{n'}{2}}\cdot n'^{\frac{n'}{2}}\Big)\sum_{j=0}^{[\frac{n'-5}{4}]}\sigma^{2j+3}\,c^{2j+2}\,\Big(\kappa\Big)^{4j-\frac{n'}{2}+4}
\end{aligned}
$$

Where the last inequality follows since $\binom{n}{i} \leq 2^n$ and $n! \leq n^n$. We now turn to

upper-bounding I. Recalling that $f(r) = e^{-\frac{\pi(r-c)^2}{\sigma^2}} + e^{-\frac{\pi(r+c)^2}{\sigma^2}}$, we have that

$$\begin{aligned}
\mathrm{I} &= \left| \int_0^\infty r^{\frac{n'-2}{2}} f(r) \left(\sum_{j=0}^{[\frac{n'-3}{4}]} c_j \left(\frac{2\pi\kappa r}{2}\right)^{2j-\frac{n'-3}{2}} \right) \left(\frac{2}{2\pi^2\kappa r}\right)^{\frac{1}{2}} \sin(2\pi\kappa r) r \,\mathrm{d}r \right| \\
&= 1/2 \left| \int_{-\infty}^\infty r^{\frac{n'-2}{2}} f(r) \left(\sum_{j=0}^{[\frac{n'-3}{4}]} c_j \left(\frac{2\pi\kappa r}{2}\right)^{2j-\frac{n'-3}{2}} \right) \left(\frac{2}{2\pi^2\kappa r}\right)^{\frac{1}{2}} \left(\frac{e^{i2\pi\kappa r} - e^{-i2\pi\kappa r}}{2i}\right) r \,\mathrm{d}r \right| \\
&\leq 1/2 \cdot \left(\frac{1}{4\pi^2\kappa}\right)^{\frac{1}{2}} \left| \int_{-\infty}^\infty r^{\frac{n'-1}{2}} f(r) \left(\sum_{j=0}^{[\frac{n'-3}{4}]} c_j \left(\frac{2\pi\kappa r}{2}\right)^{2j-\frac{n'-3}{2}} \right) (e^{i2\pi\kappa r} - e^{-i2\pi\kappa r}) \,\mathrm{d}r \right| \\
&\leq 1/2 \cdot \left(\frac{1}{4\pi^2\kappa}\right)^{\frac{1}{2}} \sum_{j=0}^{[\frac{n'-3}{4}]} |c_j| \left(\pi\kappa\right)^{2j-\frac{n'}{2}+\frac{3}{2}} \left| \int_{-\infty}^\infty r^{2j+1} \left(e^{-\frac{\pi(r-c)^2}{\sigma^2}} + e^{-\frac{\pi(r+c)^2}{\sigma^2}} \right) (e^{i2\pi\kappa r} - e^{-i2\pi\kappa r}) \,\mathrm{d}r \right|,
\end{aligned} \tag{C.10}$$

where the second equality follows since $f(r)$ is an even function, $\sin(2\pi\kappa r)$ is an odd function and for $n' = l \cdot 2^a + 1$, all powers of r in the integrand are odd, which means that the entire integrand is an even function.

To compute an upper bound on

$$\int_{-\infty}^\infty r^{2j+1} \left(e^{-\frac{\pi(r-c)^2}{\sigma^2}} + e^{-\frac{\pi(r+c)^2}{\sigma^2}} \right) (e^{i2\pi\kappa r} - e^{-i2\pi\kappa r}) \,\mathrm{d}r \tag{C.11}$$

as above, we integrate each term separately. Since the analysis is essentially the same for each term, we focus on the term $B := \left| \int_{-\infty}^\infty e^{-\frac{\pi(r-c)^2}{\sigma^2}} e^{i2\pi\kappa r} \,\mathrm{d}r \right| = \left| e^{-\pi\kappa^2\sigma^2 + i2\pi\kappa c} \int_{-\infty}^\infty e^{-\pi\sigma^{-2}(r-(c+i\kappa\sigma^2))^2} \,\mathrm{d}r \right|$:

$$
\begin{aligned}
B &= \left|e^{-\pi\kappa^2\sigma^2+i2\pi\kappa c}\right| \cdot \left|\int_{-\infty}^{\infty} r^{2j+1} e^{-\pi\sigma^{-2}(r-(c+i\kappa\sigma^2))^2}\,\mathrm{d}r\right| \\
&\leq e^{-\pi\kappa^2\sigma^2}\left|\int_{-\infty}^{\infty} r^{2j+1} e^{-\pi\sigma^{-2}(r-(c+i\kappa\sigma^2))^2}\,\mathrm{d}r\right| \\
&= e^{-\pi\kappa^2\sigma^2}\left|\int_{-\infty}^{\infty} \Big(\frac{\sigma}{\sqrt{\pi}}r' + (c+i\kappa\sigma^2)\Big)^{2j+1} e^{-r'^2}\frac{\sigma}{\sqrt{\pi}}\,\mathrm{d}r'\right| \\
&\leq e^{-\pi\kappa^2\sigma^2}\left|\int_{-\infty}^{\infty} \Big(\frac{\sigma}{\sqrt{\pi}}r' + (c+\kappa\sigma^2)\Big)^{2j+1} e^{-r'^2}\frac{\sigma}{\sqrt{\pi}}\,\mathrm{d}r'\right| \\
&\leq e^{-\pi\kappa^2\sigma^2}\Big(\frac{\sigma}{\sqrt{\pi}}\Big)^{2j+2}\Big(\frac{c}{\sigma}+\kappa\sigma\Big)^{2j+1}\binom{2j+1}{j+1}\int_{-\infty}^{\infty} r'^{2j} e^{-r'^2}\,\mathrm{d}r \\
&\leq e^{-\pi\kappa^2\sigma^2}\Big(\frac{\sigma}{\sqrt{\pi}}\Big)^{2j+2}\Big(\frac{c}{\sigma}+\kappa\sigma\Big)^{2j+1}\binom{2j+1}{j+1}\frac{1}{2}(1+(-1)^{2j})\Gamma\Big(\frac{1}{2}+j\Big) \\
&\leq e^{-\pi\kappa^2\sigma^2}\Big(\frac{\sigma}{\sqrt{\pi}}\Big)^{2j+2}\Big(\frac{c}{\sigma}+\kappa\sigma\Big)^{2j+1}\binom{2j+1}{j+1}\Gamma\Big(\frac{1}{2}+j\Big)
\end{aligned}
$$

Thus, we have that

$$
\text{(C.11)} \leq \Big(\frac{\sigma}{\sqrt{\pi}}\Big)^{2j+2} e^{-\pi\kappa^2\sigma^2}\Gamma(\frac{1}{2}+j)\binom{2j+1}{j+1}\left[4(\frac{c}{\sigma}+\kappa\sigma)^{2j+1}\right]
$$

Plugging the above back into (C.10), and recalling that $|c_j| = \frac{(\frac{n'-3}{2}-j)!\Gamma(\frac{1}{2}+\frac{n'-3}{2}-j)}{j!(\frac{n'-3}{2}-2j)!\Gamma(\frac{1}{2}+j)}$, we have that

$$
\begin{aligned}
\mathrm{I} &\leq 1/2\Big(\frac{1}{4\pi^2\kappa}\Big)^{\frac{1}{2}}\sum_{j=0}^{[\frac{n'-3}{4}]}|c_j|\Big(\pi\kappa\Big)^{2j-\frac{n'}{2}+\frac{3}{2}}\Big(\frac{\sigma}{\sqrt{\pi}}\Big)^{2j+2} e^{-\pi\kappa^2\sigma^2}\Gamma(\frac{1}{2}+j)\Big(\frac{2j+1}{j+1}\Big)^2\Big(\frac{c}{\sigma}\Big)^{2j+1}\Big(\kappa\sigma\Big)^{2j+1} \\
&\leq 1/2\Big(\frac{1}{2\pi}\Big)e^{-\pi\kappa^2\sigma^2}\sum_{j=0}^{[\frac{n'-3}{4}]}(\pi)^{j-\frac{n'-1}{2}}\Big(\frac{\frac{n'-3}{2}}{j}-j\Big)\Big(\frac{2j+1}{j+1}\Big)^2\Gamma\Big(\frac{n'}{2}-1-j\Big)\,\sigma^{2j+2}\,c^{2j+1}\,\Big(\kappa\Big)^{4j-\frac{n'}{2}+3} \\
&\leq 1/2\Big(\frac{1}{2\pi}\Big)e^{-\pi\kappa^2\sigma^2}\,\Big(n'\cdot 2^{\frac{n'}{2}}\cdot n'^{\frac{n'}{2}}\Big)\sum_{j=0}^{[\frac{n'-3}{4}]}\sigma^{2j+2}\,c^{2j+1}\,\Big(\kappa\Big)^{4j-\frac{n'}{2}+3}
\end{aligned}
$$

Where the last inequality follows since $\binom{n}{i} \leq 2^n$ and $n! \leq n^n$. Finally, plugging

into (C.7), and recalling that $c \leq \sigma \cdot \sqrt{2} \cdot \sqrt{n'}$ and $\kappa > \frac{1}{\sigma}$, we obtain:

$$|F(\kappa)| \leq 1/2\, e^{-\pi\kappa^2\sigma^2} \left(n' \cdot 2^{\frac{n'}{2}} \cdot {n'}^{\frac{n'}{2}}\right) \left(\sum_{j=0}^{[\frac{n'-5}{4}]} \sigma^{2j+3}\, c^{2j+2}\, \kappa^{4j-n'+5} + \sum_{j=0}^{[\frac{n'-3}{4}]} \sigma^{2j+2}\, c^{2j+1}\, \kappa^{4j-n'+4} \right)$$

$$\leq \sigma^{n'} \cdot {n'}^{n'} \cdot e^{-\pi\kappa^2\sigma^2}$$

□

D Manipulating Gaussians

We begin by defining some notation, which will be useful in all of the Conditional Distributions when manipulating Gaussian-distributed random variables. We write probability density function of random variable X at value $\mathbf{x}$, sampled from n-dimensional Gaussian distribution with each component of variable pairwise independent, as

$$\psi_{\mathbf{s},\mathbf{u}}(X = \mathbf{x}) = \prod_{i \in [n]} \frac{1}{s_i} \exp\left(\frac{-\pi(x_i - u_i)^2}{s_i^2}\right),$$

with mean $\mathbf{u} = (u_1, \ldots, u_n)$ and standard deviation $\mathbf{s} = (s_1, \ldots, s_n)$. The probability density function of Y at value $\mathbf{y}$, sampled from n-dimensional Gaussian distribution with each component of variable pairwise independent, can be written as

$$\psi_{\mathbf{v},\boldsymbol{\mu}}(Y = \mathbf{y}) = \prod_{i \in [n]} \frac{1}{v_i} \exp\left(\frac{-\pi(y_i - \mu_i)^2}{v_i^2}\right),$$

with mean $\boldsymbol{\mu} = (\mu_1, \ldots, \mu_n)$ and standard deviation $\mathbf{v} = (v_1, \ldots, v_n)$.

We now consider the distribution of X, conditioned on knowledge of $X + Y$. We proceed with the following straightforward lemma:

Lemma D.1. Given two independent random variables X and Y. Suppose that the distribution of X is a n-dimensional Gaussian distribution with mean $\mathbf{u}$ and standard deviation $\mathbf{s}$, each component of X pairwise independent, and the distribution of Y is a n-dimensional Gaussian distribution with mean $\boldsymbol{\mu}$ and standard deviation $\mathbf{v}$, each component of Y pairwise independent. Then the distribution of X conditioned on $X + Y$ is also a n-dimensional Gaussian distribution, where each component of X is pairwise-independent with mean $\mathbf{c} := (c_1, \ldots, c_n)$ where $c_i := \frac{\frac{u_i}{s_i^2} - \frac{\mu_i}{v_i^2} + \frac{z_i}{v_i^2}}{\left(\frac{1}{s_i^2} + \frac{1}{v_i^2}\right)}$ and standard deviation $\sigma := (\sigma_1, \ldots, \sigma_n)$, where $\sigma_i := \sqrt{\frac{1}{\frac{1}{s_i^2} + \frac{1}{v_i^2}}}$.

Proof. We have $F_{Z|A}(Z = b)$ generically represent the probability density function of random variable Z at value b, conditioned on event A.

We can then derive the density function of X given the value $\mathbf{z} = (z_1, \ldots, z_n)$ of $X + Y$ by computing

$$F_{X|X+Y=\mathbf{z}}(X = \mathbf{x}) = \frac{\psi_{\mathbf{s},\mathbf{u}}(X = \mathbf{x})\psi_{\mathbf{v},\boldsymbol{\mu}}(Y = \mathbf{y}),}{\int_{R^n} \psi_{\mathbf{s},\mathbf{u}}(X = \mathbf{x})\psi_{\mathbf{v},\boldsymbol{\mu}}(Y = \mathbf{y})\,\mathrm{d}\mathbf{x}}$$

$$= \frac{\prod_{i\in[n]} \frac{1}{s_i v_i} e^{-\frac{\pi(x_i-u_i)^2}{v^2}} e^{-\frac{\pi(z_i-x_i-\mu)^2}{{v_i}^2}}}{\prod_{i\in[n]} \int_{-\infty}^{\infty} \frac{1}{s_i v_i} e^{-\frac{\pi(x_i-u_i)^2}{v^2}} e^{-\frac{\pi(z_i-x_i-\mu)^2}{{v_i}^2}} \mathrm{d}x}$$

$$= \prod_{i\in[n]} \sqrt{\frac{1}{s_i^2} + \frac{1}{v_i^2}} \exp\left(-\pi\left(\frac{1}{s_i^2} + \frac{1}{v_i^2}\right)\left(x_i - \frac{\frac{u_i}{s_i^2} - \frac{\mu_i}{v_i^2} + \frac{z_i}{v_i^2}}{\frac{1}{s_i^2} + \frac{1}{v_i^2}}\right)^2\right)$$

Hence $F_{X|X+Y=\mathbf{z}}(X = \mathbf{x})$ is also in the form of probability density function of X on value x sampled n-dimensional Gaussian distribution, where each component x_i is generated independently with mean $\frac{\frac{u_i}{s_i^2} - \frac{\mu_i}{v_i^2} + \frac{z_i}{v_i^2}}{\left(\frac{1}{s_i^2} + \frac{1}{v_i^2}\right)}$, and variance parameter $\frac{1}{\frac{1}{s_i^2} + \frac{1}{v_i^2}}$.

□

E Additional Proofs for Section 2

E.1 Additional Proofs in Conditional Distribution II

Lemma 2.4. For ideals $\mathcal{J} \in T_1$,

$$\eta_{2^{-2n}}\left((\frac{\mathcal{J}}{q})^\vee\right) \leq 2n.$$

Proof.

$$\eta_{2^{-2n}}\left((\frac{\mathcal{J}}{q})^\vee\right) \leq \frac{\sqrt{n}}{\lambda_1\left((\frac{\mathcal{J}}{q})^\vee\right)} \tag{E.1}$$

$$\leq \left(N\left(\frac{\mathcal{J}}{q}\right)\right)^{-1/n} \tag{E.2}$$

$$\leq \left(|\mathcal{J}/qR^\vee| \cdot n^n\right)^{1/n} \tag{E.3}$$

$$\leq (2^n \cdot n^n)^{1/n} \tag{E.4}$$

$$= 2n,$$

where (E.1) follows from Lemma B.4, (E.2) follows from Lemma A.1, and (E.3) follows from the fact that $\left(N\left(\frac{\mathcal{J}}{q}\right)\right)^{-1} = |\mathcal{J}/qR| = |R^\vee/R| \cdot |\mathcal{J}/qR^\vee| = \Delta_K|\mathcal{J}/qR|$ (for example, see [8, page. 63]), and (E.4) follows from the definition of T_1. □

Lemma 2.5. For ideals $\mathcal{J} \in T_2^1$

$$|\mathcal{J}/qR^\vee|^{-(l-k)} \left(\rho_{1/\sigma_1,\ldots,1/\sigma_n}\left(\frac{1}{q}\mathcal{J}\right)^l\right) \leq 2^{-n(l-k)}$$

Proof. Recall that $\sigma := (\sigma_1, \ldots, \sigma_n) \in \mathbb{R}^n_{>0}$ is defined as a vector such that ℓ positions are set to $2n$, while the other positions are set to s. Define $z_1, \ldots, z_n$ in the following way: For $i \in [n]$, if $\sigma_i = s$ then $z_i = \sigma_i$. Otherwise, $z_i = \eta_{2^{-2n}}\left((\frac{1}{q}\mathcal{J})^\vee\right)$. Applying Poisson summation twice we arrive at:

$$\begin{aligned}
\rho_{1/\sigma_1,\ldots,1/\sigma_n}\left(\frac{1}{q}\mathcal{J}\right) &= 1/\det(\frac{1}{q}\mathcal{J}) \cdot (1/\sigma_1 \cdots 1/\sigma_n)\rho_{\sigma_1,\ldots,\sigma_n}\left((\frac{1}{q}\mathcal{J})^\vee\right) && \text{(E.5)}\\
&\leq 1/\det(\frac{1}{q}\mathcal{J}) \cdot (1/\sigma_1 \cdots 1/\sigma_n)\rho_{z_1,\ldots,z_n}\left((\frac{1}{q}\mathcal{J})^\vee\right) && \text{(E.6)}\\
&= \left(\frac{\eta_{2^{-2n}}((\frac{1}{q}\mathcal{J})^\vee)}{2n}\right)^\ell \cdot \rho_{1/z_1,\ldots,1/z_n}\left(\frac{1}{q}\mathcal{J}\right) && \text{(E.7)}\\
&\leq (1+2^{-2n}) \cdot \left(\frac{\eta_{2^{-2n}}((\frac{1}{q}\mathcal{J})^\vee)}{2n}\right)^\ell, && \text{(E.8)}
\end{aligned}$$

where (E.6) follows from definitions of ρ and z_i. To derive (E.7), let us first introduce the following claim.

Claim E.1. *For any lattice $L^\vee$,*

$$\rho_{s_1,\ldots,s_n}(L) = s_1 \cdot s_2 \cdot \ldots \cdot s_n \cdot \frac{1}{\det(L)} \cdot \rho_{1/s_1,\ldots,1/s_n}(L^\vee)$$

Proof. It can be easily verified by combining Poisson Summation formula and the fact that $\hat{\rho}_{s_1,\ldots,s_n} = s_1 \cdots s_n \rho_{1/s_1,\ldots,1/s_n}$. □

By replacing s_i with $1/z_i$ for all i and replacing L with $\frac{1}{q}\mathcal{J}$, we have

$$1/\det(\frac{1}{q}\mathcal{J}) \cdot \rho_{z_1,\ldots,z_n}\left((\frac{1}{q}\mathcal{J})^\vee\right) = z_1 \cdots z_n \cdot \rho_{1/z_1,\ldots,1/z_n}\left(\frac{1}{q}\mathcal{J}\right).$$

By plugging into (E.6), we have

$$\left(\frac{z_1}{\sigma_1}\cdots\frac{z_n}{\sigma_n}\right)\cdot\rho_{1/z_1,\ldots,1/z_n}\left(\frac{1}{q}\mathcal{J}\right)$$

By definition of z_i, $\frac{z_i}{\sigma_i}=1$ when $\sigma_i=s$ and $\frac{z_i}{\sigma_i}=\frac{\eta_{2^{-2n}}((\frac{1}{q}\mathcal{J})^\vee)}{2n}$, when $\sigma_i=2n$. Since there are ℓ positions in σ when $\sigma_i=2n$, we obtain (E.7). Finally (E.8) follows by definition of smoothing parameter $\eta_{2^{-2n}}((\frac{1}{q}\mathcal{J})^\vee)$.

Now, using the fact that $\eta_{2^{-2n}}\leq(\Delta_K|\mathcal{J}/qR^\vee|)^{1/n}$, the fact that $\Delta_K=n^n$ and the fact that $|\mathcal{J}/qR^\vee|\geq 2^n$, and the set of parameters, we have that

$$\begin{aligned}|\mathcal{J}/qR^\vee|^{-(l-k)}\left(\rho_{1/\sigma_1,\ldots,1/\sigma_n}\left(\frac{1}{q}\mathcal{J}\right)^l\right)&\leq|\mathcal{J}/qR^\vee|^{-(l-k-l\cdot\ell/n)}(1+2^{-2n})^l\cdot 2^{-\ell\cdot l}\\&\leq 2^{-n(l-k)}\end{aligned}$$

which completes the proof of the lemma. □

E.2 Additional Proofs in Conditional Distribution III

Recall that a generic PDF of one dimensional Gaussian distribution is defined as:

$$\psi_{s,u}(x)=\frac{1}{s}\exp\left(\frac{-\pi(x-u)^2}{s^2}\right),$$

where u is mean, and s is standard deviation of the distribution. We write probability density function of secret key X at value $\mathbf{x}=(x_1,\ldots,x_{n'})$, of which each coordinate is independently sampled from a Gaussian distribution with center at 0 and standard deviation s, as

$$\psi_s(X=\mathbf{x})=\prod_{i\in[n']}\frac{1}{s}\exp\left(\frac{-\pi x_i^2}{s^2}\right)=\frac{1}{s^{n'}}\exp\left(\frac{-\pi r^2}{s^2}\right)=\psi_s(\|X\|=r),$$

where r is the magnitude of $\mathbf{x}$. It also can be viewed as probability density function of secret key for its magnitude $\|X\|=r$, denoted as $\psi_s(\|X\|=r)$. The error is sampled from a 1-dimensional Gaussian distribution with center at 0. We write probability density function of error E at value y is

$$\psi_v(E=y)=\frac{1}{v}\exp\left(\frac{-\pi y^2}{v^2}\right).$$

Let $F_{Z|A}(f(Z) = b)$ generically represent the probability density function of random variable Z at value b of $f(Z)$, conditioned on event A.

We now derive the density function of secret key X given the value z of $|\|X\| + E|$. The weight placed on a value $\mathbf{x} = (x_1, \ldots, x_{n'})$ by the conditional distribution depends *only* on the magnitude of $\mathbf{x}$ (i.e. $r = \|\mathbf{x}\|$) and can be computed as:

$$\begin{aligned}
&F_{X\left||\|X\|+E|=z\right.}(\|X\| = r) = \frac{F_{X,E}(\|X\| = r, \|X\| + E| = z)}{F_{X,E}(\|X\| + E| = z)} \\
=&\frac{\psi_s(\|X\| = r)\psi_v(E = z - r) + \psi_s(\|X\| = r)\psi_v(E = -z - r)}{F_{X,E}(\|X\| + E = z) + F_{X,E}(\|X\| + E = -z)} \\
=&\frac{\psi_s(\|X\| = r)\psi_v(E = z - r) + \psi_s(\|X\| = r)\psi_v(E = -z - r)}{\int_{R^{n'}} \psi_s(\|X\| = \|\mathbf{x}\|)\psi_v(E = z - \|\mathbf{x}\|) + \psi_s(\|X\| = \|\mathbf{x}\|)\psi_v(E = -z - \|\mathbf{x}\|)\,\mathbf{dx}} \\
=&\frac{e^{-\left(\frac{\pi}{s^2}+\frac{\pi}{v^2}\right)\left(r-\frac{zs^2}{v^2+s^2}\right)^2} + e^{-\left(\frac{\pi}{s^2}+\frac{\pi}{v^2}\right)\left(r+\frac{zs^2}{v^2+s^2}\right)^2}}{nV_n \int_{-\infty}^{\infty} e^{-\left(\frac{\pi}{s^2}+\frac{\pi}{v^2}\right)\left(r-\frac{zs^2}{v^2+s^2}\right)^2} r^{n-1} dr} \\
=&\frac{e^{-\left(\frac{\pi}{s^2}+\frac{\pi}{v^2}\right)\left(r-\frac{zs^2}{v^2+s^2}\right)^2} + e^{-\left(\frac{\pi}{s^2}+\frac{\pi}{v^2}\right)\left(r+\frac{zs^2}{v^2+s^2}\right)^2}}{N},
\end{aligned} \tag{E.9}$$

where N is the normalization factor.

Lemma E.2. Given a random variable Y chosen from a Gaussian distribution $G_E(y, v) = \frac{1}{v}\exp\left(\frac{-\pi y^2}{v^2}\right)$, Y is upper bounded by $v\sqrt{n'}$ except for negligible probability, written as $\Pr\left(Y \geq v\sqrt{n'}\right) \in 2^{-\Omega(n)}$.

Proof. $\Pr(Y \geq y) = \Pr(X \geq x)$, where $X = \frac{\sqrt{2\pi}Y}{v}$ is a standard normal, $x = \frac{\sqrt{2\pi}y}{v}$. By using Chernoff bound and calculating exponential moment of standard normal distribution, we have, for any $\lambda > 0$.

$$\Pr(X \geq x) \leq \frac{\mathbb{E}\left[e^{\lambda X}\right]}{e^{\lambda x}} = \frac{e^{\lambda^2/2}}{e^{\lambda x}},$$

Set $\lambda = x$ and $y = v\sqrt{n'}$, then $\Pr\left(Y \geq v\sqrt{n'}\right) \leq e^{-x^2/2} = e^{-\pi n'}$. The lemma follows. □

We now restate and prove Lemma 2.7.

Lemma 2.7. Suppose $v = s$, we can bound a center $\frac{zs^2}{v^2+s^2}$ from Equation E.9 by $\Pr\left(\frac{zs^2}{v^2+s^2} \geq s\sqrt{n'}\right) \in 2^{-\Omega(n)}$.

Proof. Using union bound, we have

$$\begin{aligned}
&\Pr\left(\frac{zs^2}{v^2+s^2} \geq s\sqrt{n'}\right) = \Pr\left(\frac{z}{2} \geq s\sqrt{n'}\right) \\
\leq &\Pr\left(R+E \geq 2s\sqrt{n'}\right) + \Pr\left(-R-E \geq 2s\sqrt{n'}\right) \\
\leq &\Pr\left(R \geq s\cdot\sqrt{n'}\right) + \Pr\left(E \geq v\sqrt{n'}\right) + \Pr\left(E \geq v\sqrt{n'}\right)
\end{aligned}$$

Note that since $s > n$, and using the fact that $\lambda_1((R^l \times \mathbb{Z})^\vee) \geq \lambda_1(R^\vee) \geq \sqrt{n}N^{\frac{1}{n}}(R^\vee) = \sqrt{n}\cdot(\Delta_k^{-1})^{\frac{1}{n}} \geq \sqrt{n}\left(\frac{1}{n^n}\right)^{\frac{1}{n}} = \frac{1}{\sqrt{n}}$ (See Lemma A.1), by Lemma B.4, we ensure $s > \eta_{2^{-n}}(R^l \times \mathbb{Z})$. Then by Lemma B.11 and Lemma E.2, we deduce that $\Pr\left(\frac{zs^2}{v^2+s^2} \geq s\sqrt{n'}\right) \in 2^{-\Omega(n)}$. □

Corollary 2.10. Let k, l, σ and $\mathbf{c}$ be as in Theorem 2.9. Assume that $A = [I_k|\bar{A}] \in (R_q)^{k\times l}$ is chosen as in Theorem 2.9. Then, with probability $1 - 2^{-\Omega(n)}$ over the choice of $\bar{A}$, the distribution of $A\mathbf{x} \in R_q^k$, where $(\mathbf{x}, x_{n'}) \in R^l \times Z$ is chosen from $D_{R^l\times Z,\Psi_{\sigma,c}}$ satisfies that the probability of each of the q^{nk} possible outcomes is in the interval $(1\pm 2^{-\Omega(n)})q^{-nk}$ (and in particular is within statistical distance $2^{-\Omega(n)}$ of the uniform distribution over R_q^k).

Proof. $\Psi_{\sigma,c}\left(\Lambda^\perp(A)^+ + (\mathbf{b},\ b')\right) \in \det((\Lambda^\perp(A)^+)^\vee)(1 \pm 2^{-\Omega(n)})$, which means that if we choose a n'-dimensional vector from distribution $D_{R^l\times Z,\Psi_{\sigma,c}}$, written as $\mathbf{x}' = (\mathbf{x}, x_{n'})$, and let $(\mathbf{b}, b_{n'}) = \mathbf{x}' \mod (\Lambda^\perp(A)^+)$, then the resulting distribution is within statistical distance $2^{-\Omega(n)}$ to uniform distribution over $(R^l \times Z)$ modulo $(\Lambda^\perp(A)^+)$. Due to the structure of $\Lambda^\perp(A)^+$, this also implies that the marginal distribution over $\mathbf{b}$ is uniform over (R^l) modulo $(\Lambda^\perp(A))$. Moreover, we can easily see that for $\mathbf{x}' = (\mathbf{x}, x_{n'})$, if $\mathbf{x}' \mod (\Lambda^\perp(A)^+) = (\mathbf{b},\ b_{n'})$, then $A\mathbf{x} = A\mathbf{b}$. Finally, since when $\mathbf{b}$ is uniform random over R^l modulo $\Lambda^\perp(A)$, we have that $A\mathbf{b}$ is uniform random over R_q^k, the corollary follows. □

Received **???**.

Author information

Dana Dachman-Soled, Department of Electrical and Computer Engineering and UMIACS, University of Maryland, 8125 Paint Branch Dr., College Park, MD 20742, USA.
E-mail: `danadach@ece.umd.edu`

Huijing Gong, Department of Computer Science and UMIACS, University of Maryland, 8125 Paint Branch Dr., College Park, MD 20742, USA.
E-mail: gong@cs.umd.edu

Mukul Kulkarni, Department of Electrical and Computer Engineering and UMIACS, University of Maryland, 8125 Paint Branch Dr., College Park, MD 20742, USA.
E-mail: mukul@terpmail.umd.edu

Aria Shahverdi, Department of Electrical and Computer Engineering and UMIACS, University of Maryland, 8125 Paint Branch Dr., College Park, MD 20742, USA.
E-mail: ariash@umd.edu