On the Leakage Resilience of Ideal-Lattice Based Public Key Encryption

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

University of Maryland, College Park, USA
danadach@ece.umd.edu, gong@cs.umd.edu, {mukul@terpmail, ariash@terpmail}.umd.edu

Abstract. We consider the leakage resilience of the Ring-LWE analogue of the Dual-Regev encryption scheme (R-Dual-Regev for short), originally presented by Lyubashevsky et al. (Eurocrypt '13). Specifically, we would like to determine whether the R-Dual-Regev encryption scheme remains IND-CPA secure, even in the case where an attacker leaks information about the secret key.

We consider the setting where R is the ring of integers of the m-th cyclotomic number field, for m which is a power-of-two, and the Ring-LWE modulus is set to $q \equiv 1 \mod m$. This is the common setting used in practice and is desirable in terms of the efficiency and simplicity of the scheme. Unfortunately, in this setting R_q is very far from being a field so standard techniques for proving leakage resilience in the general lattice setting, which rely on the leftover hash lemma, do not apply. Therefore, new techniques must be developed.

In this work, we put forth a high-level approach for proving the leakage resilience of the R-Dual-Regev scheme, by generalizing the original proof of Lyubashevsky et al. (Eurocrypt '13). We then give three instantiations of our approach, proving that the R-Dual-Regev remains IND-CPA secure in the presence of three natural, non-adaptive leakage classes.

1 Introduction

Recently, NIST has begun the process of standardizing post-quantum cryptosystems, i.e. algorithms for public key encryption, key exchange and digital signatures that are expected to remain secure even in the presence of a universal quantum computer. One of the foremost avenues for viable post-quantum public key encryption is to construct schemes from lattices, and reduce the security of the scheme to the quantum-hardness of a well-studied lattice problem. Among cryptosystems built from lattices, so-called *ideal-lattice-based* schemes are usually preferred in practice, since *ideal-lattices* are highly structured objects that lend themselves to more efficient and compact cryptosystems. There are several *ideal-lattice-based* schemes for public key encryption that may become candidates for standardization. One of these is the Ring-LWE analogue of the Dual-Regev encryption scheme (R-Dual-Regev for short), first presented by Lyubashevsky et al. [32] and then simplified (for the case of power-of-two cyclotomics) by Alperin-Sheriff and Peikert and Crockett and Peikert [4,12].

As various candidate lattice-based schemes are being considered for standardization, it is imperative to provide evidence of their robustness and suitability for large-scale use. Indeed, it is possible that a cryptosystem enjoys a security reduction to a quantum-hard problem, but at the same time is vulnerable to far simpler attacks that can be carried out without the expertise and expense needed to launch a quantum attack. In this work, we consider the robustness of the R-Dual-Regev encryption scheme against *side-channel* attacks, where an attacker *leaks* information about the cryptographic key by measuring e.g. power consumption of a physical device during decryption. Such attacks are known to be detrimental against standard cryptosystems, such as RSA, and can be launched with reasonable costs in myriad settings (cf. [5,17,25,26,23,46,43,19]).

Lattices and LWE. An n-dimensional lattice $\mathcal{L}$ is an additive discrete subgroup of $\mathbb{R}^n$. There are several algorithmic problems relating to lattices that are believed to be hard, even for a quantum computer. The relevant one for this work will be the (approximate) shortest independent vector problem (SIVP_γ), which asks to find a set of n linearly independent vectors (where n is the dimension of the lattice) such that the length of the longest vector in the set is within a γ factor of the minimum possible length.

* This work is supported in part by an NSF CAREER Award #CNS-1453045, 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.

The learning with errors (LWE) problem was introduced by Regev [42], who showed a worst-case to average-case *quantum* reduction from SIVP_γ.[1] To solve the (decision version of the) LWE problem, an attacker must distinguish the two distributions $(A, A\boldsymbol{x} + \boldsymbol{e})$ from $(A, \boldsymbol{u})$, where A is a matrix chosen uniformly from $Z_q^{m\times n}$, $\boldsymbol{x}$ is sampled from Z_q^n, $\boldsymbol{e}$ is sampled from an "error distribution" ψ_m over Z_q^m and $\boldsymbol{u}$ is chosen uniformly from Z_q^m. Many lattice-based public-key encryption schemes are built from LWE (following the original construction of [42]) and the security of these schemes is proven by first reducing to LWE and then applying known reductions from LWE to lattice problems (cf. [20,10]).

Ideal lattices and Ring-LWE. Efficiency is a main concern in lattice-based cryptosystems. When using the LWE assumption over general lattices to build encryption schemes, the public key consists of the LWE matrix A, a random matrix over Z_q of size $m \times n$, where $m > n$ and n is security parameter. So storing the public key requires space at least $\Omega(n^2 \log q)$, and encryption requires matrix-vector multiplication. To over come this inefficiency, *ideal lattices*—lattices with additional structure—were introduced. In the ideal lattice setting, we consider the number field $K = \mathbb{Q}[x]/\Phi_m(x)$, where $\Phi_m(x)$ is the m-th cyclotomic polynomial of degree $\varphi(m)$. For m which is a power of 2, the m-th cyclotomic polynomial is simply $\Phi_m(x) = x^n + 1$, where $n = m/2$ is also a power of 2. We then consider the ring of integers, $R \subset K$ of the number field, defined as $R = \mathbb{Z}[x]/\Phi_m(x)$. R can now be viewed as a lattice via the so-called "canonical embedding" which transforms elements of K from a polynomial representation to a vector representation in an inner product space endowed with a vector norm. "Ideal lattices", therefore, correspond to fractional ideals of K, which can be viewed as lattices via the canonical embedding. We further define $R_q := \mathbb{Z}_q[x]/\Phi_m(x)$, which denotes the set of polynomials obtained by taking an element of $\mathbb{Z}[x]/\Phi_m(x)$ and reducing each coefficient modulo q.

Given the above, the Ring-LWE problem is to distinguish $(a, b = a \cdot s + e) \in R_q \times R_q$ from uniformly random pairs, where $s \in R_q$ is a random secret, the $a \in R_q$ is uniformly random and the error term $e \in R$ has small norm.

In the above formulation, the matrix A from the general lattice LWE setting is replaced with a polynomial a in the ideal lattice setting. Therefore, the public key now has dimension n instead of $m \times n$ and can be represented as a vector in Z_q^n, requiring only $O(n \log q)$ bits of storage.

In this paper, we consider ideal lattices with further structure. Specifically, we assume that m is a power of two, which means that $\Phi_m(x)$ has degree $n = m/2$. We further set q to be a prime such that $q \equiv 1 \mod m$, in which case $\Phi_m(x)$ completely splits into n factors in $\mathbb{Z}_q[x]$. This allows for additional optimizations in the implementation, such as fast arithmetic over the ring R_q.

The R-Dual-Regev encryption scheme. The key generation algorithm of the R-Dual-Regev encryption scheme proceeds as follows: The secret key corresponds to elements $x_1, \ldots, x_l$ that are chosen from a discrete Gaussian distribution over R. To generate the public key, a_1 is set to $-1 \in R_q$ and $a_2, \ldots, a_l$ are chosen uniformly at random from R_q. The public key is then set to $(a_2, \ldots, a_l, a_{l+1} = -\sum_{i\in[l]} a_i x_i)$. The key property necessary for proving the security of the Dual-Regev encryption scheme is that for public keys sampled as described above, a_{l+1} should be distributed (close to) uniform random in R_q, given $a_2, \ldots, a_l$.

When R_q is a field, not only does the above property hold, but it can be shown that a_{l+1} is distributed (close to) uniform random in R_q, as long as $x_1, \ldots, x_l$ has sufficiently high min-entropy (via the leftover hash lemma). Thus, when R_q is a field, it can be immediately argued that the R-Dual-Regev encryption scheme is inherently leakage-resilient, to (non-adaptive) leakage[2] on the secret key $x_1, \ldots, x_l$, as long as $x_1, \ldots, x_l$ has sufficiently high min-entropy conditioned on the leakage. In this work, however, recall that we consider the case where R is the ring of integers in the m^{th} cyclotomic number field K of degree n, where m is a power-of-two, and the modulus q is a prime such that $q \equiv 1 \mod m$. As discussed above, such setting of parameters is desirable since it allows for highly efficient implementation of various aspects of the cryptosystem (such as discrete Gaussian sampling, as well as representation and manipulation of elements of R and R_q). Unfortunately, when n and q are chosen as above, it implies that qR (the ideal of R generated by $\langle q \rangle$) splits completely into n distinct prime ideals, $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$, each of norm q, which in turn means that R_q is very far from being a field. In particular, this means that standard techniques for proving leakage resilience, which rely on the leftover hash lemma, cannot be used when the computations are performed over the ring R_q.

[1] Classical reductions from GapSVP were subsequently proved by Peikert [39] and Brakerski et al. [9].

[2] By non-adaptive leakage we mean that the chosen leakage function g does not depend on the public key.

Nevertheless, Lyubashevsky et al. [32,33] proved a "regularity theorem" showing that (even when q is a prime such that $q \equiv 1 \mod m$) 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 $\boldsymbol{x}$ chosen from a discrete Gaussian distribution (centered at 0) over R_q^l, the distribution over $A\boldsymbol{x}$ is (close to) *uniform random*. A similar result was proven by Micciancio [35], but requires super-constant dimension l, thus yielding non-compact cryptosystems. In contrast, the regularity theorem of [32] holds even for constant dimension l as small as 2, and thus yields compact cryptosystems. However, while sufficient for proving the security of the cryptosystem itself, unlike the more general leftover hash lemma, the statement of the regularity theorem of [32] implies nothing about the security of the cryptosystem in the leakage setting. Therefore, the key to proving the security of the R-Dual-Regev encryption scheme under leakage on the secret key seems to be extending the regularity theorem to settings in which $\boldsymbol{x}$ is chosen from a distribution $\mathcal{D}$, which is not necessarily a Gaussian distribution centered at 0. In particular, the fundamental technical question we consider in this work is:

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

Indeed, from the point of view of the adversary, the secret key $\boldsymbol{x}$ is drawn from a distribution $\mathcal{D}$, where $\mathcal{D}$ corresponds to a Gaussian distribution ***conditioned on the view of the adversary after leakage on the secret key*** $\boldsymbol{x}$. We would like to understand whether for natural distributions $\mathcal{D}$ arising from adversarial leakage, it is the case that when $\boldsymbol{x}$ is sampled according to $\mathcal{D}$, we have that $A\boldsymbol{x}$ is (close to) uniform random.

In this work, we make progress on the fundamental question above and show that for three natural classes of leakage—which give rise to three different distributions $\mathcal{D}$—when $\boldsymbol{x}$ is sampled according to $\mathcal{D}$, the distribution over $A\boldsymbol{x}$ remains (close to) uniform random. This implies that the R-Dual-Regev encryption scheme is resilient to these three types of leakage (with possibly small modifications to the scheme such as increasing the standard deviation of the Gaussian distribution under which the secret key $\boldsymbol{x}$ is sampled during key generation). In the following, we give a brief description of the three types of leakage that we consider. We then discuss our high-level technical approach as well as the particular methods we use for each of the three leakage classes under consideration.[3]

1.1 The Leakage Scenarios

In the following, we describe the three leakage scenarios considered in this work and their relation to side-channel attacks appearing in practice.

Leakage Scenario I. This scenario models an attacker who can measure the noisy version of each coordinate of secret key either through a power or timing channel. For example, the side-channel attack can be launched on the Gaussian Sampling algorithm, which is used to sample the secret key and which was shown to be vulnerable to timing attacks [43]. Recall that the secret key of the R-Dual-Regev encryption scheme is $\boldsymbol{x} = (x_1, \ldots, x_l)$, where each $x_i \in R_q$. Moreover, each x_i itself is represented as an n-dimensional vector. Thus, in total, the secret key can be viewed as an $l \cdot n$-dimensional vector. In this scenario we allow leakage on *each* coordinate of the secret key, but assume that this leakage is "noisy" in the sense that independent Gaussian noise (with sufficiently high standard deviation) is added to each leaked coordinate. More precisely, the Gaussian noise is assumed to have standard deviation at least s, where s is the standard deviation of the Gaussian distribution from which the secret key, $\boldsymbol{x}$ is sampled.

Leakage Scenario II. This scenario models a setting where an attacker obtains low-noise measurements about some (constant fraction) of coordinates of the secret key and gets no information about the remaining coordinates. As above, we can consider a side-channel attack that is launched during the Gaussian sampling of the secret key, but the attacker is unable to extract information on all coordinates, due to the low resolution of the measurement. In this scenario, the noise added to each leaked coordinate has only $2n$ standard deviation.[4] In comparison, in Leakage Scenario I the standard deviation of the noise is at least s,

[3] We note that an alternative approach is to replace the regularity lemma by a Ring-LWE assumption as in [28,29]. Leakage resilience under conditional distribution $\mathcal{D}$ would then follow by analyzing the underlying Ring-LWE problem with respect to secret key distribution $\mathcal{D}$.

[4] Note that in this leakage scenario 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).

where s is the standard deviation of the Gaussian distribution from which the secret key, $\boldsymbol{x}$ is sampled. To give an idea of how big s is, when instantiating the R-Dual-Regev encryption scheme with $q = \Theta(n^3)$ and $l = 5$, the standard deviation of s is at least $n^{1.6}$.

Leakage Scenario III. In this scenario, the adversary learns the magnitude of the secret key with channel error, where both secret key and error are sampled from Gaussian distributions. The motivation for this type of leakage is that (discrete) Gaussian sampling of the secret key is often implemented via rejection sampling in practice [13,9]. Briefly, in rejection sampling we have a distribution D' that is sufficiently close to the target distribution D (i.e. $D(\boldsymbol{x}) \leq M \cdot D'(\boldsymbol{x})$, where $D(\boldsymbol{x})$, resp. $D'(\boldsymbol{x})$, denotes the probability of $\boldsymbol{x}$ under distribution D, resp. D'). We sample $\boldsymbol{x}$ according to D', output $\boldsymbol{x}$ with probability $p = \frac{D(\boldsymbol{x})}{M \cdot D'(\boldsymbol{x})}$ and reject with probability $1 - p$. In case of rejection the procedure is repeated. Concretely, in our setting, D' can correspond to a multi-dimensional binomial distribution (with parameters set such that the one-dimensional binomial distribution is $(1 - \delta)$-close to the one-dimensional Gaussian distribution), for which sampling is straightforward. Note that the probability p of accept will depend on the probability of $\boldsymbol{x}$ under the Gaussian distribution, $D(\boldsymbol{x})$, which in turn depends only on the *magnitude* of $\boldsymbol{x}$. Indeed, a recent attack on the BLISS signature scheme [19] exploited the fact that—due to optimizations—the computation of the probability of a secret value under the target distribution during the rejection sampling procedure allowed for the magnitude (norm) of this secret value to be recovered via a power analysis attack, which then led to a full break of the scheme. In the encryption setting, our result for Leakage Scenario III suggests that it may be better (from a security perspective) to sample the entire $\boldsymbol{x}$ from a multi-dimensional distribution D' and then apply rejection sampling to the entire vector at once, as opposed to performing the rejection sampling coordinate-by-coordinate, since in this case there is only one opportunity for leakage.[5].

1.2 Our Results

We show that in each of Leakage Scenarios I, II and III, the R-Dual-Regev encryption scheme can be proven secure, as long as the parameter s—corresponding to the standard deviation of the Gaussian from which the secret key is sampled—is slightly increased. Specifically, in the original analysis of the R-Dual-Regev encryption scheme by Lyubashevsky et al. [32], it was shown that it is sufficient to set $s \geq 2n \cdot q^{1/l+2/(nl)}$, where n is the dimension of R_q, q is the modulus and l is a constant representing the number of ring elements in the secret key, public key and ciphertext and k is set to 1. We next describe the setting of s in each of the leakage scenarios:

- For **Leakage Scenario I**, we show that it is sufficient to set $s \geq \sqrt{2} \cdot 2n \cdot q^{1/l+2/(nl)}$, an increase of a multiplicative factor of $\sqrt{2}$. (see Theorem 5.2, Corollary 5.3 and the discussion following the corollary).
- For **Leakage Scenario II**, we show that it is sufficient to set $s \geq 2n \cdot q^{\frac{n+2}{l(n-\ell)}}$, where ℓ is the number of leaked coordinates of the secret key. (see Theorem 5.4, Corollary 5.7 and the discussion following the corollary). Surprisingly, even if leaked coordinates of secret key $\boldsymbol{x}$ have standard deviation $2n$, which is much smaller than smoothing parameter of the lattice, distribution of $a_{l+1} = -\sum_{i \in [l]} a_i x_i$ can still be (close to) uniform random.
- For **Leakage Scenario III**, we show that it is sufficient to set $s \geq \sqrt{14/5 \cdot (n'/n) \cdot \ln n'} \cdot 2n \cdot q^{1/l+2/(nl)}$, where $n' = n \cdot l + 1$, an increase of a multiplicative factor of $\sqrt{14/5 \cdot (n'/n) \cdot \ln n'}$. (see Theorem 5.9, Corollary 5.10 and the discussion following the corollary).

Note that keeping n, q, l fixed while increasing s will make it necessary to decrease ξ, the standard deviation of the noise for the Ring-LWE samples, and this, in turn, will make it necessary to increase γ, the approximation factor of the SIVP problem, in the underlying lattice. Alternatively, one can fix n, q, γ (which together determine the security level of the cryptosystem) and then slightly increase the parameter l (the number of ring elements in the secret key, public key and ciphertext) accordingly.

We illustrate our parameter settings in the following two tables. Our goal in these charts is not to suggest concrete parameters for practical implementations, but rather to illustrate the required increase in parameters for Leakage Scenarios I, II and III, given a fixed setting of parameters for the original scheme.

[5] Note that this only works if $(1-\delta)^n$ is non-negligible, where $1 - \delta$ is the closeness of the one-dimensional binomial and Gaussian distributions. Since, $(1-\delta)^{1/\delta}$ approaches e^{-1} as $1/\delta$ goes to infinity, this can be achieved by setting $\delta \leq 1/n$.

In Figure 1, we fix concrete settings for n, q, l for the original R-Dual-Regev encryption scheme and each leakage scenario and then calculate the corresponding settings of s, ξ and γ.

Scenario	s	ξ	γ
Original	1.89e+04	354.74	2.08e+09
I	2.67e+04	250.84	2.94e+09
II	2.12e+04	315.58	2.34e+09
III	3.04e+05	22.06	3.35e+10

Fig. 1: The table shows the amount of standard deviation of the Gaussian which the secret key (s) and error (ξ) is sampled from. For each scenario the obtained approximation factor (γ) is provided. The table is for the case where $n = 1024$, $q = 4290937559$, $l = 10$ and $\ell = n/20$.

In Figure 2, we fix concrete settings for n, q and γ, thus fixing the desired level of hardness of the cryptosystem. We must then increase l in order to achieve the desired hardness. We record the resulting settings of l, s and ξ for the original R-Dual-Regev encryption scheme and each leakage scenario.

Scenario	l	s	ξ	γ
Original	4	5.3e+05	20.01	3.1e+10
I	5	2.47e+05	38.44	1.68e+10
II	5	2.20+05	43.02	1.50e+10
III	11	2.62e+05	24.42	3.08e+10

Fig. 2: The table shows how much l should be increased to achieve at least the same level of security as the original (no leakage allowed). For each scheme then, the new value for standard deviation of the Gaussian which the secret key (s) and error (ξ) is sampled from is given. For each scenario the obtained approximation factor (γ) is provided. The table is for the case where $n = 1024$, $q = 4290937559$ and $\ell = n/20$.

1.3 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 $\Lambda^{\perp}(A) = \{\boldsymbol{z} \in R^l : A\boldsymbol{z} = \boldsymbol{0} \bmod qR\}$. By the definition of A and $\Lambda^{\perp}(A)$, if, when $\boldsymbol{x}$ is sampled from some continuous distribution $\mathcal{D}$, we have that $[\boldsymbol{x} \mod \Lambda^{\perp}(A)]$ is uniform random (over cosets of $\Lambda^{\perp}(A)$), then when $\boldsymbol{x}$ is sampled from $\mathcal{D}$, the distribution of $A\boldsymbol{x}$ is also uniform random over cosets of $(qR)^k$. Both the input distribution $\mathcal{D}$ and the output distribution can then be discretized over the ring R to achieve the desired results. Therefore, the goal is to show that when $\boldsymbol{x}$ is sampled from continuous distribution $\mathcal{D}$, we have that $[\boldsymbol{x} \mod \Lambda^{\perp}(A)]$ 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 $[\boldsymbol{x} \mod \Lambda^{\perp}(A)]$ is uniform random. Thus, [32] prove their Regularity Theorem by showing that with high probability over choice of A, the smoothing parameter, $\eta_{\varepsilon}(\Lambda^{\perp}(A))$, is upperbounded by s.

In order to understand 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, i.e. how to directly prove the uniformity of $[\boldsymbol{x} \mod \Lambda]$ (for n-dimensional lattice Λ) when $\boldsymbol{x}$ is sampled from a (discrete) Gaussian distribution with mean 0 and sufficiently high standard deviation.

Let $\rho_s := e^{-\pi\frac{\langle \boldsymbol{x},\boldsymbol{x}\rangle}{s^2}}$ 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. To show that the distribution over $[\boldsymbol{x} \mod \Lambda]$ is (close to) uniform when $\boldsymbol{x}$ is sampled from a distribution with pdf ψ_s, one needs to show that for every coset $(\Lambda + \boldsymbol{c})$ of the lattice, $\psi_s(\Lambda + \boldsymbol{c}) \approx \frac{1}{\det(\Lambda)}$. Let us focus on showing this for the zero coset, where $\boldsymbol{c} = \boldsymbol{0}$ (extending the argument is straightforward due to properties of the

Fourier transform). In other words, we would like to show that

$$\sum_{\boldsymbol{v}\in\Lambda} \psi_s(\boldsymbol{v}) \approx \frac{1}{\det(\Lambda)}. \tag{1}$$

In the following, for a function f we concisely represent $\sum_{\boldsymbol{v}\in\Lambda} f(\boldsymbol{v})$ by $f(\Lambda)$.

In order to show (1), we use the Poisson summation formula, which says that for any lattice Λ and integrable function ρ_s, the following equation holds:

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

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 Section 2.2). Therefore, the task that remains is to show that $\widehat{\psi_s}(\Lambda^\vee)$ is close to 1 (i.e. is upperbounded by $1+\varepsilon$).

The general proof approach outlined above can be applied to (integrable) normalized pdf Ψ that are not Gaussians centered at 0. Namely, to show that the distribution over $[\boldsymbol{x} \mod \Lambda]$ is (close to) uniform when $\boldsymbol{x}$ is sampled from a distribution with pdf Ψ, one can follow the above template, which implies that it is sufficient to show that $\widehat{\Psi}(\Lambda^\vee)$ is upperbounded by $1+\varepsilon$.

In this work, we consider pdf's other than spherical Gaussian distributions centered at 0. In more detail, the pdf, Ψ, we consider corresponds to the probability density function of the secret key, *from the point of view of the adversary*, given the leakage that is obtained. The technical contribution of this work is then to show that, in each leakage scenario, (with overwhelming probability over choice of $\bar{A}$) $\widehat{\Psi}(\Lambda(A)^\vee)$ is close to 1. Specifically, for each scenario, 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).

Leakage Scenario I, is fairly simple to handle (given sufficient noise) since if X and Y are multi-dimensional, independent Gaussian random variables, then the distribution of X conditioned on $X+Y$ is also a multidimensional Gaussian that is *not* centered at 0. Fortunately, the regularity theorem of [32] straightforwardly extends to Gaussians that are not centered at 0. We mainly view Leakage Scenario I as a warmup to the more difficult Leakage Scenarios II and III.

The analysis for Leakage Scenario II follows from the observation that the distribution of X conditioned on $X+Y$ is now a non-spherical Gaussian, where leaked coordinates correspond to independent Gaussians with very small standard deviation and unleaked coordinates correspond to independent Gaussians with high standard deviation. The key to analyzing this scenario is noting that the matrix $\bar{A}$ is chosen at random, independently of which coordinates are leaked. This allows us to analyze the expectation of $\widehat{\Psi}((\Lambda^\perp(A))^\vee)$ (correspondingly, the expectation of $\widehat{\Psi}((\Lambda^\perp(A))^\vee \setminus \{\mathbf{0}\})$), over choice of $\bar{A}$ and show that if not too many coordinates are leaked then the expectation of $\widehat{\Psi}((\Lambda^\perp(A))^\vee \setminus \{\mathbf{0}\})$ remains low. In order for this analysis to go through, the proof of the Regularity Theorem of [32] must be carefully adapted to our setting.

Our key observation for the analysis of Leakage Scenario III is that the probability of a particular secret key vector $\boldsymbol{x}$ under the conditional distribution corresponding to the view of the adversary who sees a "noisy" version of the magnitude of $\boldsymbol{x}$, *depends only on the magnitude of* $\boldsymbol{x}$. This allows us to show that the pdf corresponding to the distribution over $\boldsymbol{x}$, conditioned on the leakage has the form of a one-dimensional Gaussian (not centered at 0), when viewing the pdf as a *radial* function over a single variable $r = \|\boldsymbol{x}\|$. Using properties of the *radial Fourier transform*, we are then able to analyze this setting.

1.4 Related Work

Lattice-based cryptography. Regev introduced the *Learning with Errors* or LWE, problem in his seminal work [42], and showed a *quantum* reduction from hardness of solving LWE problem to that of solving GapSVP and SIVP and Peikert [39] showed a *classical* reduction to GapSVP (but not SIVP). While Regev's reduction worked for polynomial modulus q, Peikert's reduction required exponentially large modulus q, and the subsequent work of Brakerski et al. [9] extended the classical reduction to the case of polynomial modulus $q = \mathrm{poly}(n)$. Regev [42] also presented a public-key encryption scheme based on the hardness of LWE problem. The work of Gentry et al. [20] presented "trapdoor" cryptographic tools from lattices, which then led to new constructions of cryptographic primitives such as digital signatures and identity-based encryption. This work also introduced the so-called "Dual-Regev" public key encryption scheme.

Ideal-lattice-based cryptography. Micciancio's [35] modified Ajtai's one-way function [1] to the setting of polynomial rings and reduced its security to the hard problem known as the *ring-SIS* problem. Early works used the integer coefficients of the polynomial to represent an element of the ring R, and the norm of this vector was used as norm on R. Lyubashevsky et al. [31] used the notion of the *canonical embedding* from algebraic number theory to represent ring elements which facilitates much simpler analysis and tighter bounds on the norm of ring elements. In the same work [31], introduced the *ring*-LWE problem and proved its hardness by proving a *quantum* reduction to SVP on arbitrary ideal lattices arising from the ring R. In an independent work, Stehlé et al. [44] also considered a special case of ring-LWE and proved the hardness for only search problem for the specific ring. Analogously to the LWE-problem, the ring-LWE problem can then be used to construct public key encryption [31,32,33]. In particular, Lyubashevsky et al. [32,33] presented the analogue of the "Dual-Regev" public key encryption scheme for the ring-LWE setting.

Leakage-resilient cryptography. There is a significant body of work on leakage-resilient cryptographic primitives, beginning with the work of Dziembowski and Pietrzak [18] on leakage-resilient stream-ciphers. Other constructions include: leakage resilient block-ciphers [40]; public key encryption (cf. [2,37,8,27,24]); and digital signatures (cf. [24,7,34,15,27]). With the exception of [2], most of these results construct new cryptosystems from the bottom up, using different techniques from those of standard cryptosystems used in practice. 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. There is an important line of work considering the leakage resilience of general-lattice-based cryptosystems, beginning with the work of Goldwasser et al. [21] who showed that LWE with "weak" secrets (where attacker learns some bounded leakage on secret key in form of some hard to invert function) is as hard as LWE with "perfect" secrets but with smaller dimension and error rate. Akavia et al. [2] analyzed the robustness of Regev's scheme and showed that the encryption scheme of [41] is secure even when any arbitrary function of the secret key of bounded output length is given to the adversary. Dodis et al. [16] presented secret key encryption schemes secure against an adversary learning any computationally uninvertible function of the secret key, relying on an assumption related to the LWE assumption. Subsequently, Dodis et al. [14] presented a construction of public-key encryption scheme based on LWE which is secure against an adversary learning any computationally uninvertible function of the secret key, however their techniques require superpolynomial modulus. Other works [6,38,3,9,30] showed that the LWE problem is hard with small losses in dimension and error rate even if one or more *linear* relations on the secret and the error are revealed. These can then be combined with the work of [14] to obtain leakage resilient, public-key encryptions schemes based on LWE with polynomial modulus.

In cases where R_q is (close to) a field, prior results on leakage resilience in the general lattice setting should carry over the the polynomial ring setting in a straightforward manner. In our work, however, we consider the commonly used setting in practice, where R is the ring of integers in the m^{th} cyclotomic number field K of degree n, where m is a power-of-two, and the modulus q is a prime such that $q \equiv 1 \mod m$. In this setting R_q is very far from being a field and so prior techniques do not carry over. To the best of our knowledge, our work is the first to consider the leakage resilience of a cryptosystem in this setting.

2 Notation and Preliminaries

2.1 Notation

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

2.2 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 $m \geq 2$),

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

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 $B = \{\boldsymbol{b}_j\} \subset H$:

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

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.

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

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 section 3) into a discrete Gaussian distribution (definition 3.8). Given a lattice $\Lambda = \mathcal{L}(B)$ represented by some "good" basis $B = \{\boldsymbol{b}_i\}$, a point $\boldsymbol{x} \in H$, and a point $\boldsymbol{c} \in H$ representing a lattice coset $\Lambda + \boldsymbol{c}$, the discretization process outputs a point $\boldsymbol{y} \in \Lambda + \boldsymbol{c}$ such that the length of $\boldsymbol{y} - \boldsymbol{x}$ is not too large. This is denoted as $\boldsymbol{y} \leftarrow \lfloor \boldsymbol{x} \rceil_{\Lambda + \boldsymbol{c}}$. A discretization procedure is called *valid* if it is efficient; and depends only on the lattice coset $\Lambda + (\boldsymbol{c} - \boldsymbol{x})$, not on particular representative used to specify it. Note that for a valid discretization, $\lfloor \boldsymbol{z} + \boldsymbol{x} \rceil_{\Lambda + \boldsymbol{c}}$ and $\boldsymbol{z} + \lfloor \boldsymbol{x} \rceil_{\Lambda + \boldsymbol{c}}$ are identically distributed for any $\boldsymbol{z} \in \Lambda$. For more details and actual description of algorithms used for discretization we refer the interested reader to [33].

2.3 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:

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

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.

2.4 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 2.1 ([33]). *For any fractional ideal $\mathcal{I}$ in a number field K of degree n,*

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

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 2.2. *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 2.3. *[33] 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.*

2.5 Ring-LWE

In this section, we present the formal definition of the ring-LWE problem as given in [33].

Definition 2.4 (**Ring-LWE Distribution**). *For a "secret" $s \in R_q^\vee$ (or just $R^\vee$) and a distribution ψ over $K_\mathbb{R}$, a sample from the ring-*LWE *distribution $A_{s,\psi}$ over $R_q \times (K_\mathbb{R}/qR^\vee)$ is generated by choosing $a \leftarrow R_q$ uniformly at random, choosing $e \leftarrow \psi$, and outputting $(a, b = a \cdot s + e \bmod qR^\vee)$.*

Definition 2.5 (**Ring-LWE, Average-Case Decision**). *The* average-case decision *version of the ring-*LWE *problem, denoted R-*DLWE$_{q,\psi}$*, is to distinguish with non-negligible advantage between independent samples from $A_{s,\psi}$, where $s \leftarrow R_q^\vee$ is uniformly random, and the same number of uniformly random and independent samples from $R_q \times (K_\mathbb{R}/qR^\vee)$.*

In [4], it is shown that an equivalent "tweaked" form of the Ring-LWE problem can be used in cryptographic applications without loss in security or efficiency. This is convenient since the "tweaked" version does not involve $R^\vee$. The "tweaked" ring-LWE problem can be obtained by implicitly multiplying the noisy products b_i by the "tweak" factor $t = \hat{m}/g \in R$ as defined in definition 2.2. Note that, $t \cdot R^\vee = R$. This yields new values

$$b_i' = t \cdot b_i = (t \cdot s) \cdot a_i + (t \cdot e_i) = s' \cdot a_i + e_i' \bmod qR,$$

where $a_i, s' = t \cdot s \in R_q$, and the errors $e_i' = t \cdot e_i$ come from the "tweaked" error distribution $t \cdot \psi$. Note that when ψ corresponds to spherical Gaussian, its tweaked form $t \cdot \psi$ may be *highly non-spherical.*

Theorem 2.6. *[33, Theorem 2.22] Let K be the m^{th} cyclotomic number field having dimension $n = \varphi(m)$ and $R = \mathcal{O}_K$ be its ring of integers. Let $\alpha = \alpha(n) > 0$, and $q = q(n) \geq 2$, $q = 1 \bmod m$ be a* poly(n)*-bounded prime such that $\alpha q \geq \omega(\sqrt{\log n})$. Then there is a polynomial-time quantum reduction from $\tilde{O}(\sqrt{n}/\alpha)$-approximate* SIVP *(or* SVP*) on ideal lattices in K to the problem of solving R-*DLWE$_{q,\psi}$ *given only l samples, where ψ is the Gaussian distribution D_ξ for $\xi = \alpha \cdot q \cdot (nl/\log(nl))^{1/4}$.*

Lemma 2.7. *[33, 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 ring-*LWE *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 2.8. *[33, 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-$\mathsf{DLWE}_{q,\psi}$ is hard given l samples, then so is the variant of R-$\mathsf{DLWE}_{q,\psi}$ in which the secret is sampled from $\chi := \lfloor p \cdot \psi \rceil_{w+pR^\vee}$, given $l-1$ samples.*

2.6 Security Definitions for Leakage Resilient Public Key Encryption

A public key encryption scheme $\mathcal{E}$ consists of three algorithms: $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$.

- $\mathsf{Gen}(1^n) \to (\mathsf{pk}, \mathsf{sk})$. The key generation algorithm takes in the security parameter and outputs a public key pk and a secret key sk.
- $\mathsf{Enc}(\mathsf{pk}, m) \to c$. The encryption algorithm takes in a public key pk and a message m. It outputs a ciphertext c.
- $\mathsf{Dec}(\mathsf{sk}, c) \to m$. The decryption algorithm takes in a ciphertext c and a secret key sk. It outputs a message m.

Correctness. The PKE scheme satisfies correctness if $\mathsf{Dec}(\mathsf{sk}, c) = m$ with all but negligible probability whenever pk, sk is produced by Gen and c is produced by $\mathsf{Enc}(\mathsf{pk}, m)$.

Security. We define IND-CPA security under non-adaptive, one-time leakage for PKE schemes in terms of the following game between a challenger and an attacker (this extends the usual notion of IND-CPA security to our leakage setting). We let n denote the security parameter, and the class $\mathcal{F}$ denotes the class of allowed leakage functions.

Setup Phase. The game begins with a setup phase. The challenger calls $\mathsf{Gen}(1^n)$ to create the initial secret key sk and public key pk.

Query Phase. The attacker specifies an efficiently computable leakage function $f \in \mathcal{F}$ (note that f may be probabilistic).

Challenge Phase. The attacker receives $(\mathsf{pk}, f(\mathsf{sk}))$ from the challenger. The attacker chooses two messages m_0, m_1 which it gives to the challenger. The challenger chooses a random bit $b \in \{0, 1\}$, encrypts m_b, and gives the resulting ciphertext to the attacker. The attacker then outputs a guess b' for b. The attacker wins the game if $b = b'$. We define the advantage of the attacker in this game as $\left|\frac{1}{2} - \Pr[b' = b]\right|$.

Definition 2.9 (IND-CPA security under Non-Adaptive, One-Time Leakage)**.** *We say a Public Key Encryption scheme $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is IND-CPA secure under non-adaptive, one-time key leakage from leakage class $\mathcal{F}$ if any probabilistic polynomial time attacker only has a negligible advantage (negligible in n) in the above game.*

3 Regularity and Fourier Transforms

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

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

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

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

By normalizing this function we obtain the *continuous* Gaussian probability distribution $\psi_{s,c}^1$ (resp. ψ_s^1) of parameter s, whose density is given by $s^{-1} \cdot \rho_{s,c}^1(x)$ (resp. $s^{-1} \cdot \rho_s^1(x)$).

Let $\rho_{s,c}^1$ 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:

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

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 3.1 (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*

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

Theorem 3.2 (Poisson Summation Formula). *Let $f : \mathbb{R}^n \to \mathbb{C}$ be an integrable function and Λ a lattice of dimension n. Then*

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

where $\Lambda^\vee$ is the dual lattice of Λ.

Definition 3.3. *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 3.4. *[36,11] 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 ([33]). 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 3.5. *For any n-dimensional lattice Λ and $\varepsilon > 0$, $\boldsymbol{s} := (s_1, \ldots, s_n) \in \mathbb{R}^n_{>0}$, and $\boldsymbol{c} := (c_1, \ldots, c_n) \in \mathbb{R}^n$, 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. Details can be found in Section A in supplementary material. □

Lemma 3.6. *[36, 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 3.7. *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:*

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

Definition 3.8. *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*

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

Remark 1. 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 3.9. *[36, Lemma 4.4] For any n'-dimensional lattice Λ, and reals $0 < \varepsilon < 1, s \geq \eta_\varepsilon(\Lambda)$, we have*

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

The following is a modified version of Lemma 3.8 from [42] and the proof can be found in Section B in supplementary material.

Lemma 3.10. *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 $\boldsymbol{c} \in \mathbb{R}^n$, $\Psi(\Lambda + \boldsymbol{c}) \in \det(\Lambda^\vee)(1 \pm \varepsilon)$.*

The proof of the following lemma proceeds as the proof of Corollary 2.8 in [20].

Lemma 3.11. *Let Λ' be an n-dimensional lattice and Ψ a probability distribution over $\mathbb{R}^n$. Assume that for all $\boldsymbol{c} \in \mathbb{R}^n$ it is the case that*

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

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

Definition 3.12. *For a matrix $A \in R_q^{k \times l}$ we define*

$$\Lambda^\perp(A) = \{\boldsymbol{z} \in R^l : A\boldsymbol{z} = 0 \bmod qR\},$$

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 3.13. *[33] 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 [33].

Corollary 3.14. *Let R, n, q, k and l be as in Theorem 3.13. Assume that $A = [I_k | \bar{A}] \in (R_q)^{k \times l}$ is chosen as in Theorem 3.13. Then, with probability $1 - 2^{-\Omega(n)}$ over the choice of $\bar{A}$, the distribution of $A\boldsymbol{x} \in R_q^k$, where each coordinate of $\boldsymbol{x} \in R_q^l$ 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 [33] and can be deduced from Lemma 3.4.

Corollary 3.15. *Let R, n, q, k and l be as in Theorem 3.13. Assume that $A = [I_k | \bar{A}] \in (R_q)^{k \times l}$ is chosen as in Theorem 3.13. 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 $\frac{\sqrt{n/\pi}}{2n \cdot q^{k/l+2/(nl)}}$.*

The following lemma computes a lower bound of the normalization factor of the pdf in Theorem 3.17. The proof can be found in Section C of supplementary material.

Lemma 3.16. *Let $n' \in \mathbb{N}$ be odd, $\boldsymbol{x} \in \mathbb{R}^{n'}$, $c \in \mathbb{R}$. Then*

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

The next theorem provides an upper bound on the Fourier transform of a pdf for the subsequent analysis of Leakage Scenario III in Section 5.3. We refer to Section D of supplementary material for the detailed proof.

Theorem 3.17. *Let $\Psi_{\sigma,c}$ denote the normalized pdf corresponding to the non-normalized function $f(\boldsymbol{x}) := e^{-\frac{\pi(\|\boldsymbol{x}\|-c)^2}{\sigma^2}} + e^{-\frac{\pi(\|\boldsymbol{x}\|+c)^2}{\sigma^2}}$, where $\boldsymbol{x}$ is a vector over n' dimensions. and let $\widehat{\Psi_{\sigma,c}}(\boldsymbol{y})$ denote the n'-dimensional Fourier transform of $\Psi_{\sigma,c}$. Let $n' := l \cdot 2^a + 1$, where l, a are positive integers and $a > 2$, and $c \leq \sigma \cdot \sqrt{2} \cdot \sqrt{n'}$. Then $\widehat{\Psi_{\sigma,c}}(\boldsymbol{y}) \leq {n'}^{n'} \cdot e^{-\pi\|\boldsymbol{y}\|^2\sigma^2}$ for $\|\boldsymbol{y}\| > 1/\sigma$.*

4 Dual-Style Encryption Scheme

In this section we present a dual-style encryption scheme from [33], however we use the result from [4,12], which applies to power-of-two cyclotomics, to avoid usage of $R^\vee$. The system is parameterized by l, which is the number of R-LWE samples which attacker gets to see; q is the modulus of the ring R_q; s, ξ are the parameters for the continuous Gaussian distributions ψ_s, and ψ_ξ over $K_\mathbb{R}$ respectively. Also, let $D_{R,s}$ be the discrete Gaussian distribution obtained from ψ_s, where R denotes m^{th} cyclotomic ring (of degree $n = \varphi(m)$). Also, let p, q be coprime integers[6]

Let $\lfloor \cdot \rceil$ be a valid discretization to (cosets of) R or pR. Then the corresponding "tweaked" distribution over R or pR is defined as $\psi^{pR} = \lfloor t \cdot p \cdot \psi_\xi \rceil_{pR}$. Similarly, $\psi^{\mu+pR} = \lfloor t \cdot p \cdot \psi_\xi \rceil_{\mu+pR}$. Authors of [4,12] noted that using the "tweaked" distributions for sampling the LWE errors is equivalent to ring LWE.

The dual-style encryption scheme consists of three algorithm as follows:

Key-Generation Algorithm Gen: It outputs private/public key pair by following steps.

1. Choose $a_1 = -1 \in R_q$, and generate uniformly random and independent element $a_2, \ldots, a_l \in R_q$.
2. Generate independent $x_1, \ldots, x_l \leftarrow D_{R,s}$.
3. Set the public key $\boldsymbol{a} = (a_2, \ldots, a_l, a_{l+1} = -\sum_{i\in[l]} a_i x_i) \in R_q^l$, and the secret key $\boldsymbol{x} = (x_2, \ldots, x_l, x_{l+1} = 1) \in R_q^l$. Note that $\langle \boldsymbol{a}, \boldsymbol{x} \rangle = x_1 \in R_q$ by construction.

Encryption Algorithm Enc: It takes as input a public key $\boldsymbol{a} \in R_q^l$, and a message $\mu \in R_p$, returns a ciphertext $\boldsymbol{c}$ by proceeding the following steps.

1. Generate independent $e_1, \ldots, e_l \leftarrow \psi^{pR}$ and $e_{l+1} \leftarrow \psi^{\mu+pR}$.
   Set $\boldsymbol{e} = (e_2, \ldots e_{l+1}) \in R^l$.
2. Compute $\boldsymbol{c} = e_1 \cdot \boldsymbol{a} + \boldsymbol{e} \in R_q^l$.

Decryption Algorithm Dec: It takes as input a private key $\boldsymbol{x} \in R_q^l$, and a ciphertext $\boldsymbol{c} \in R_q^l$, returns a plaintext μ by proceeding the following steps.

1. Compute $d = \langle \boldsymbol{c}, \boldsymbol{x} \rangle \in R$.
2. Output $\mu = d \bmod pR$.

Lemma 4.1. *Let the view of the adversary be* $\mathsf{view}_\mathcal{A} = (\boldsymbol{a}, \mathsf{leak})$*, where* leak *is the leakage obtained by the adversary as defined in section 2.6. If the public key element* a_{l+1} *is close to uniform given* $\mathsf{view}_\mathcal{A}$*, then the above encryption scheme is IND-CPA secure assuming the hardness of* $R\text{-DLWE}_{q,\psi_\xi}$ *given* $l+1$ *samples.*

Note that if a_{l+1} is close to uniform then $\boldsymbol{a}$ is close to uniform random vector since all $a_i, i \in [l]$ are uniform random. Given that $\boldsymbol{a}$ is indistinguishable from a uniform vector, it follows that $\boldsymbol{c}$ is indistinguishable from a uniform random value in R_q^l, from lemma 2.7 and lemma 2.8.

The following lemma shows that the decryption is correct with high probability. Here we present the analysis where ciphertext $c \in R_p^\vee$ for better readability and to preserve the proof structure of lemma 8.2 in [33]. Authors of [4,12] noted that using the "tweaked" distributions for sampling the LWE errors is equivalent to ring LWE since the tweak is reversible. This allows for the analysis to be conducted in either dual of the ring $R^\vee$ or the ring R.

Lemma 4.2. *Suppose that for any* $c \in R_p^\vee$*,* $\lfloor p \cdot \psi_\xi \rceil_{c+pR^\vee}$ *is* δ*-subgaussian with parameter* $\xi' = O(p \cdot \xi)$ *for some* $\delta = O(1/l)$*, and* $q \geq \xi' \cdot \sqrt{(s^2 \cdot l + 1) \cdot n} \cdot \omega(\sqrt{\log n})$*. Then decryption is correct with probability* $1 - \mathsf{negl}(n)$ *over all the randomness of key generation and encryption.*

Proof. We know that, ψ is a continuous Gaussian with parameter $\xi \geq 1$, then $\lfloor p \cdot \psi_\xi \rceil_{c+pR^\vee}$ is 0-subgaussian with parameter $\xi' = p\sqrt{\xi^2 + \pi} = O(p \cdot \xi)$.

$$\langle \boldsymbol{c}, \boldsymbol{x} \rangle = e_1 \cdot \langle \boldsymbol{a}, \boldsymbol{x} \rangle + \langle \boldsymbol{e}, \boldsymbol{x} \rangle$$

$$\langle \boldsymbol{c}, \boldsymbol{x} \rangle = e_1 \cdot x_1 + \langle \boldsymbol{e}, \boldsymbol{x} \rangle$$

Let $\boldsymbol{e'} = (e_1, \boldsymbol{e})$ and $\boldsymbol{x'} = (x_1, \boldsymbol{x})$. Then, $\langle \boldsymbol{e'}, \boldsymbol{x'} \rangle = \mu \bmod pR$ as long as $(\langle \boldsymbol{e'}, \boldsymbol{x'} \rangle \bmod qR) \in R$.

[6] In this work we consider $p = 2$, while computing the parameters presented in tables 1 and 2. Note that, the encryption scheme and analysis holds for any general p coprime with q.

We now present a proof sketch for the claim that $(\langle \boldsymbol{e'}, \boldsymbol{x'} \rangle \bmod qR) \in R$ with probability $1 - \mathsf{negl}(n)$. Using previous work, there exists a decoding function (similar to the decoding function of [33] section 6.2) which takes $\langle \boldsymbol{e'}, \boldsymbol{x'} \rangle$ to the closest element in R, as long as the following conditions are satisfied: For each $i \in [l]$, $\|x_i\| \leq s \cdot \sqrt{n}$, $\|x_{l+1}\| = \|1\| = \sqrt{n}$, and each coefficient of $e_i x_i$ is δ'-subgaussian with parameter $\xi' \cdot s \cdot \sqrt{n}$ and each coefficient of $e_{l+1} x_{l+1}$ is δ'-subgaussian with parameter $\xi' \cdot \sqrt{n}$, for $\delta' \in O(1)$. To see that these conditions are satisfied, first, note that by Lemma 3.9, for each $i \in [l]$, $\|x_i\| \leq s \cdot \sqrt{n}$ except with probability at most $2^{-n} = \mathsf{negl}(n)$, and $\|x_{l+1}\| = \|1\| = \sqrt{n}$. Moreover, note that the e_i are mutually independent and each coefficient of e_i is δ-subgaussian with parameter ξ', therefore each coefficient of $\langle \boldsymbol{e'}, \boldsymbol{x'} \rangle$ is $\delta(l+1)$-subgaussian with parameter $\xi' \cdot \sqrt{(s^2 \cdot l + 1) \cdot n}$. Since $\delta(l+1) \in O(1)$, we have that all the conditions are satisfied. □

5 Security against Auxiliary Inputs

The key step in proving the security of the dual-style encryption scheme presented in Section 4 (without auxiliary inputs) is to show that the public key component a_{l+1} constructed during key generation is distributed (close to) uniform random. To show this, [33], in fact, prove a more general theorem, which we refer to as the *Regularity Theorem* (see Corollary 7.5). Essentially, what this theorem says is that for $A = [I_k | \bar{A}] \in (R_q)^{k \times l}$, if $\bar{A}$ is chosen uniformly at random and $\boldsymbol{x}$ is chosen from a discrete Gaussian distribution with sufficiently large standard deviation, then $A\boldsymbol{x}$ is (close to) uniform random.

In this section, we analyze security against auxiliary inputs under three scenarios. For each leakage scenario, we argue that the encryption scheme defined in Section 4 still achieves semantic security. To prove this, it is sufficient to show, in each scenario, that *conditioned on the view of the leakage adversary*, the distribution over $A\boldsymbol{x}$ remains (close to) *uniform random*. In other words, we show that the distribution over $A\boldsymbol{x}$ remains *uniform random*, even when $\boldsymbol{x}$ is drawn from a conditional distribution corresponding to the knowledge the adversary has about $\boldsymbol{x}$, conditioned on the leakage that was obtained. This informal statement is made formal in Corollaries 5.3, 5.7 and 5.10 for each of the leakage scenarios I, II and III, below.

5.1 Leakage Scenario I

Recall that the secret key of the encryption scheme defined in Section 4 is $(x_1, \ldots, x_l)$, where each $x_i \in R_q$ is chosen from a discrete Gaussian distribution $D_{R,s}$, where $s > 2n \cdot q^{k/l+2/(nl)}$. In this scenario we can assume that each x_i is stored using the polynomial representation (powerful basis) and allow leakage on *each* coefficient or assume that each x_i is stored using the canonical embedding (CRT basis) and allow leakage on *each* coordinate (this is because for power-of-two cyclotomics, spherical Gaussians in the powerful basis representation correspond to spherical Gaussians in the CRT basis representation). We assume, however, that the leakage is "noisy" in the sense that independent Gaussian noise (with sufficiently high standard deviation) is added to each leaked coordinate. More precisely, adversary learns a "noisy" version of secret key, where independent Gaussian noise with standard deviation v is added to each coordinate of the secret key.

It turns out that this scenario is actually quite simple to handle (given sufficient noise) 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 theorem of [33] straightforwardly extends to Gaussians that are not centered at 0.

We discuss formal details next, however, we mainly view Leakage Scenario I as a warm-up to the more difficult Leakage Scenarios II and III discussed below.

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

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

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

independent, can be written as

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

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

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

Lemma 5.1. *Given two independent random variables X and Y. Suppose that the distribution of X is a n-dimensional Gaussian distribution with mean $\boldsymbol{u}$ and standard deviation $\boldsymbol{s}$, each component of X pairwise independent, and the distribution of Y is a n-dimensional Gaussian distribution with mean $\boldsymbol{\mu}$ and standard deviation $\boldsymbol{v}$, 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 $\boldsymbol{c} := (c_1, \ldots, c_n)$ 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 $\boldsymbol{\sigma} := (\sigma_1, \ldots, \sigma_n)$, 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 $\boldsymbol{z} = (z_1, \ldots, z_n)$ of $X + Y$ by computing

$$\begin{aligned}
F_{X|X+Y=\boldsymbol{z}}(X = \boldsymbol{x}) &= \frac{G_X(\boldsymbol{x}, \boldsymbol{u}, \boldsymbol{s}) G_Y(\boldsymbol{z} - \boldsymbol{x}, \boldsymbol{\mu}, \boldsymbol{v})}{\int_{R^n} G_X(\boldsymbol{x}, \boldsymbol{u}, \boldsymbol{s}) G_Y(\boldsymbol{z} - \boldsymbol{x}, \boldsymbol{\mu}, \boldsymbol{v})\, \mathrm{d}\boldsymbol{x}} \\
&= \frac{\prod_{i\in[n]} \frac{1}{s_i v_i} e^{-\frac{\pi(x_i-u_i)^2}{v^2}} e^{-\frac{\pi(z_i-x_i-\mu)^2}{{v_i}^2}}}{\prod_{i\in[n]} \int_{-\infty}^{\infty} \frac{1}{s_i v_i} e^{-\frac{\pi(x_i-u_i)^2}{v^2}} e^{-\frac{\pi(z_i-x_i-\mu)^2}{{v_i}^2}}\, \mathrm{d}x} \\
&= \prod_{i\in[n]} \sqrt{\frac{1}{s_i^2} + \frac{1}{v_i^2}} \exp\left(-\pi\left(\frac{1}{s_i^2} + \frac{1}{v_i^2}\right)\left(x_i - \frac{\frac{u_i}{s_i^2} - \frac{\mu_i}{v_i^2} + \frac{z_i}{v_i^2}}{\frac{1}{s_i^2} + \frac{1}{v_i^2}}\right)^2\right)
\end{aligned}$$

Hence $F_{X|X+Y=\boldsymbol{z}}(X = \boldsymbol{x})$ 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 $\frac{1}{\frac{1}{s_i^2} + \frac{1}{v_i^2}}$.

□

Let $\boldsymbol{v} := (v, \ldots, v)$ and $\boldsymbol{s} := (s, \ldots, s)$ and let $v = \tau \cdot s$. Suppose the distribution of secret key is $G_X(\boldsymbol{x}, \boldsymbol{0}, \boldsymbol{s})$ and the distribution of noise is $G_Y(\boldsymbol{y}, \boldsymbol{0}, \boldsymbol{v})$, on the condition that adversary learns some fixed leakage $\boldsymbol{z}$ (corresponding to the "noisy" secret key), Lemma 5.1 shows that the distribution of secret key, in the view of adversary who has obtained $\boldsymbol{z}$, is

$$\prod_{i\in[n\times l]} \frac{1}{\sigma} \exp\left(\frac{-\pi\left(x_i - \frac{z_i}{\tau^2+1}\right)^2}{\sigma^2}\right)$$

Thus, from the viewpoint of the adversary, each coordinate x_i of the secret key is sampled from a multivariate Gaussian distribution $\rho_{\sigma,\boldsymbol{c}^i}$ with mean $\boldsymbol{c}^i := (c_1^i, \ldots, c_n^i)$, 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 $\rho_{\sigma,\boldsymbol{c}}$, where $\boldsymbol{c} = [\boldsymbol{c}^i]_{i\in l}$.

We have the following theorem:

Theorem 5.2. *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 $\sigma \geq 2n \cdot q^{k/l+2/(nl)}$ and $\boldsymbol{c} \in \mathbb{R}^{n\cdot l}$ then*

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

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

Proof. It follows from Lemma 3.6 and regularity theorem from [33]. □

The following corollary follows from Lemmas 3.10 and 3.11 and Theorem 5.2.

We finally, present the following corollary of Theorem 5.2, which completes the analysis for Leakage Scenario I:

Corollary 5.3. *Let* $R, n, q, k, l, \boldsymbol{c}, \sigma$ *be as in Theorem 5.2. Assume that* $A = [I_k|\bar{A}] \in (R_q)^{k\times l}$ *is chosen as in Theorem 5.2. Then, with probability* $1 - 2^{-\Omega(n)}$ *over the choice of* $\bar{A}$*, the distribution of* $A\boldsymbol{x} \in R_q^k$*, where* $\boldsymbol{x} \in R^l$ *is chosen from* $D_{\Lambda,\sigma,\boldsymbol{c}}$*, the discrete Gaussian probability distribution over* R^l *with parameter* σ *and center* $\boldsymbol{c}$*, 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 above corollary (with $k = 1$), implies that the encryption scheme is secure under Leakage Scenario I assuming $\sigma \geq 2n \cdot q^{1/l+2/(nl)}$. Since $s = \sqrt{\frac{1+\tau^2}{\tau^2}} \cdot \sigma$, it means that in order for the encryption scheme to be secure under Leakage Scenario I, we must simply sample the secret key from $D_{R^l,\sqrt{\frac{1+\tau^2}{\tau^2}}\cdot 2n\cdot q^{1/l+2/(nl)}}$, as opposed to $D_{R^l,2n\cdot q^{1/l+2/(nl)}}$. In particular, this means that the standard deviation should be increased by a factor of $\sqrt{\frac{1+\tau^2}{\tau^2}}$, beyond the parameters required by [33].

5.2 Leakage Scenario II

Recall that this scenario models a setting where an attacker obtains noisy measurements about some (constant fraction) of coordinates of the secret key and gets no information at all about the remaining coordinates. Specifically, we leak a constant fraction of the coordinates ($\ell/(l \cdot n)$-fraction) with low noise 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 Leakage Scenario I, when $v = s$). Recall that the secret key of the encryption scheme defined in Section 4 is $(x_1, \ldots, x_l)$, where each $x_i \in R_q$. We assume that each x_i will be stored as a vector in the canonical embedding (CRT basis). Thus, this scenario allows leakage of ℓ out of the total of $l \cdot n$ coordinates, when viewing the secret key as a vector in the canonical embedding. Since conditioned on the leakage, the distribution over the secret key is no longer a spherical Gaussian, we can no longer switch between the powerful and CRT basis as before.[7]

The analysis for this leakage scenario follows from a careful adaptation of the proof of the Regularity Theorem of [33] to our setting.

Suppose the distribution of secret key is $G_X(\boldsymbol{x}, \boldsymbol{0}, \boldsymbol{s})$ and the distribution of noise is $G_Y(\boldsymbol{y}, \boldsymbol{\mu}, \boldsymbol{v})$. The adversary learns the leaked "noisy" secret key $\boldsymbol{z}$ in ℓ positions, where mean of the noise is 0 and standard deviation is $\approx 2n$ Let $\mathcal{S} \subseteq [n]$, where $|\mathcal{S}| = \ell$ denote the set of positions (from each x_i) that are leaked. Lemma 5.1 shows that, conditioned on leakage, each component x_i^j, $i \in [l], j \in \mathcal{S}$, of secret key is sampled from Gaussian distribution with mean $c_i^j := \frac{nz_i^j}{n+\frac{1}{s^2}}$, and variance $\sigma_j^2 \geq 4n^2$. Conditioned on leakage, each component x_i^j, $i \in [l], j \notin \mathcal{S}$, of the secret key is sampled from Gaussian distribution with mean $c_i^j = 0$, and variance $\sigma_j^2 = s^2$.

We have the following Theorem.

Theorem 5.4. *Let* R *be the ring of integers in the* m^{th} *cyclotomic number field* K *of degree* n*, where* n *is a power of* 2*,* q *is a prime satisfying* $q = 1 \mod m$*. For positive integers* $k \leq l \leq \text{poly}(n)$*, 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. Let* $\boldsymbol{\sigma} := (\sigma_1, \ldots, \sigma_n) \in \mathbb{R}^n_{>0}$ *and* $\boldsymbol{c} := (c_1, \ldots, c_{ln}) \in \mathbb{R}^{ln}$ *be vectors, where* $\boldsymbol{\sigma}$ *is such that* ℓ *positions are set to* $2n$*, while the other positions 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* $\widehat{\rho_{\boldsymbol{\sigma}^l,\boldsymbol{c}}}\left(\Lambda^{\perp}(A)^{\vee}\right) \leq 1 + 2^{-\Omega(n)}$ *except with probability at most* $2^{-\Omega(n)}$*.*

[7] If we leak the information on the secret while it is stored in the polynomial representation, then when we switch to the canonical embedding representation this will yield a multivariate Gaussian distribution, but there will be covariances not equal to zero between pairs of random variables. Not having independence across coordinates means that it will be difficult to analyze the Fourier transform.

For proving Theorem 5.4, 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. These will then be useful in the proof of Theorem 5.4.

To generate the set T of ideals $\mathcal{J}$ such that $qR^\vee \subseteq \mathcal{J} \subseteq R^\vee$ we can take each ideal $\mathcal{I}$ such that $qR \subseteq \mathcal{I} \subseteq R$ and set $\mathcal{J} := q\mathcal{I}^\vee$.

Recall from Fact 2.3 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 $s \geq \eta_{2^{-2n}}((\frac{1}{q}\mathcal{J})^\vee)$. Let $T_2^2 := T_2 \setminus T_2^1$.

Let $\boldsymbol{\sigma} := (\sigma_1, \ldots, \sigma_n) \in \mathbb{R}^n_{>0}$ be a vector with ℓ positions are set to $2n$, while the other positions are set to value s.

Lemma 5.5. *For ideals $\mathcal{J} \in T_1$,*

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

Proof.

$$\begin{aligned}
\eta_{2^{-2n}}\left((\frac{\mathcal{J}}{q})^\vee\right) &\leq (|\mathcal{J}/qR^\vee| \cdot n^n)^{1/n} && (2)\\
&\leq (2^n \cdot n^n)^{1/n} && (3)\\
&= 2n,
\end{aligned}$$

where (2) follows from Lemmas 2.1 and 3.4, (3) follows from the definition of T_1. □

Lemma 5.6. *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 $\boldsymbol{\sigma} := (\sigma_1, \ldots, \sigma_n) \in \mathbb{R}^n_{>0}$ 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:

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

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. □

We now conclude the proof of Theorem 5.4.

Proof of Theorem 5.4. Since by Lemma 3.6 we have that for any $(n \cdot l)$-dimensional vectors, $\boldsymbol{c}$, $\boldsymbol{x}$ and any n-dimensional vector $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_n)$:

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

then following the proof of [33] 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

$$\sum_{\mathcal{J} \in T_1^2} |\mathcal{J}/qR^\vee|^{-(l-k)} \left(\rho_{(1/\sigma_1, \ldots, 1/\sigma_n)} \left(\frac{1}{q} \mathcal{J} \right)^l - 1 \right) \leq 2^{-\Omega(n)}, \tag{4}$$

and that

$$\sum_{\mathcal{J} \in (T_1 \cup T_2^2)} |\mathcal{J}/qR^\vee|^{-(l-k)} \left(\rho_{1/\sigma_1, \ldots, 1/\sigma_n} \left(\frac{1}{q} \mathcal{J} \right)^l - 1 \right) \leq 2^{-\Omega(n)} \tag{5}$$

To show (5), note that by Lemma 5.5, 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 3.5 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 $\mathcal{J} \in T_1 \cup T_2^2$,

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

Thus, similarly to [33], using the lower bound of s from the setting, we can bound

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

Moreover, by Lemma 5.6 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.

This completes the proof. □

The following corollary follows from Lemmas 3.10 and 3.11 and Theorem 5.4.

Corollary 5.7. *Let $R, n, q, k, l, \ell, \boldsymbol{\sigma}$ and $\boldsymbol{c}$ be as in Theorem 5.4. Assume that $A = [I_k|\bar{A}] \in (R_q)^{k\times l}$ is chosen as in Theorem 5.4. Then, with probability $1-2^{-\Omega(n)}$ over the choice of $\bar{A}$, the distribution of $A\boldsymbol{x} \in R_q^k$, where $\boldsymbol{x} \in R^l$ is chosen from $D_{R^l,\boldsymbol{\sigma}^l,\boldsymbol{c}}$, the discrete Gaussian probability distribution over R^l with parameter $\boldsymbol{\sigma}^l$ and center $\boldsymbol{c}$, 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).*

Specifically, the above corollary (with $k = 1$), implies that the encryption scheme is secure under Leakage Scenario II assuming $s \geq 2n \cdot q^{\frac{n+2}{l(n-\ell)}}$ Since $\sigma := s$, where σ is the standard deviation of the secret key, it means that in order for the encryption scheme to be secure under Leakage Scenario II, we must simply sample the secret key from $D_{R,2n\cdot q^{\frac{n+2}{l(n-\ell)}}}$, as opposed to $D_{R,2n\cdot q^{1/l+2/(nl)}}$. In particular, this means that the standard deviation should be increased from $2n \cdot q^{1/l+2/(nl)}$ (as in [33]) to $2n \cdot q^{\frac{n+2}{l(n-\ell)}}$.

5.3 Leakage Scenario III

We slightly change the encryption scheme from Section 4 so that the secret key is represented by a vector of dimension $n' := l \cdot n + 1$, where n is a power of two. Note that when n is a power of two, a spherical Gaussian in the coefficient representation is also a spherical Gaussian in the canonical embedding representation [31]. Thus, we can assume that the secret key is generated using the coefficient representation, where each coordinate is sampled independently from a discrete Gaussian, $D_{Z,s'}$. During key sampling, an additional coordinate is sampled and stored together with the remainder of the secret key.

In this scenario, the adversary learns the magnitude of the secret key with channel error, where both secret key and error are sampled from Gaussian distributions. The motivation for this type of leakage is the following: Recall that each coordinate x_i of the secret key $\boldsymbol{x}$ is sampled from a discrete Gaussian distribution $D_{R,s}$. When n is a power-of-two, this corresponds to sampling each coefficient of each x_i from a discrete Gaussian distribution $D_{Z,s'}$ over the integers. To avoid large pre-computed tables, discrete Gaussian sampling is often implemented via rejection sampling [13,9]. Briefly, in rejection sampling we have a distribution D' that is sufficiently close to the target distribution $D_{R,s}$ ($D_{R,s}(\boldsymbol{x}) \leq M \cdot D'(\boldsymbol{x})$, where $D_{R,s}(\boldsymbol{x})$, resp. $D'(\boldsymbol{x})$, denotes the probability of $\boldsymbol{x}$ under distribution $D_{R,s}$, resp. D'). We sample $\boldsymbol{x}$ according to D', output $\boldsymbol{x}$ with probability $p = \frac{D_{R,s}(\boldsymbol{x})}{M\cdot D'(\boldsymbol{x})}$ and reject with probability $1-p$. In case of rejection the procedure is repeated. Concretely, in our setting, D' can correspond to a multi-dimensional binomial distribution (with parameters set such that D' is sufficiently close to $D_{R,s}$), for which sampling is straightforward. Note that the probability p of accept will depend on the probability of $\boldsymbol{x}$ under the Gaussian distribution, $D_{R,s}(\boldsymbol{x})$, which in turn depends only on the *magnitude* of $\boldsymbol{x}$. Indeed, a recent attack on the BLISS signature scheme [19] exploited the fact that—due to optimizations—the computation of the probability of a secret value under the target distribution during the rejection sampling procedure allowed for the magnitude (norm) of this secret value to be recovered via a side-channel attack, which then led to a full break of the scheme. In the encryption setting, our result for Leakage Scenario III, which shows that the scheme from Section 4 is secure under leakage of a noisy version of $\|\boldsymbol{x}\|$, suggests that it may be better (from a security perspective) to sample the entire $\boldsymbol{x}$ from a multi-dimensional distribution D' and then apply rejection sampling to the entire vector at once, as opposed to performing the rejection sampling coordinate-by-coordinate, since in this case there is only one opportunity for leakage.

Our key observation for the analysis of Leakage Scenario III is that the probability of a particular secret key vector $\boldsymbol{x}$ under the conditional distribution corresponding to the view of the adversary still *depends only on the magnitude of* $\boldsymbol{x}$. This allows us to show that the pdf corresponding to the conditional distribution over $\boldsymbol{x}$, conditioned on the leakage has the form of a one-dimensional Gaussian, when viewing the pdf as a *radial* function over a single variable $r = \|\boldsymbol{x}\|$. Using properties of radial Fourier transforms, we are then able to analyze this setting.

Recall that a generic probability density function (PDF) of one dimensional Gaussian distribution is defined as:

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

where u is mean, and s is standard deviation of the distribution.

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

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

where r is the magnitude of $\boldsymbol{x}$. It also can be viewed as probability density function of secret key magnitude R, denoted as $G_R(r, s)$. 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

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

Let $F_{Z|A}(Z = b)$ 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 secret key magnitude R given the value z of $|R + E|$. In other words, the weight placed on a value $\boldsymbol{x} = (x_1, \ldots, x_{n'})$ by the conditional distribution depends *only* on the magnitude of $\boldsymbol{x}$ (i.e. $r = \|\boldsymbol{x}\|$) and can be computed as:

$$\begin{aligned}
&F_{R\big||R+E|=z}(R = r) = \frac{G_R(r,s)G_E(z-r,v) + G_R(r,s)G_E(-z-r,v)}{F_{R+E}(R+E=z) + F_{R+E}(R+E=-z)} \\
=&\frac{G_R(r,s)G_E(z-r,v) + G_R(r,s)G_E(-z-r,v)}{\int_{R^{n'}} G_R(|\boldsymbol{x}|,s)G_E(z-|\boldsymbol{x}|,v)\,\mathrm{d}\boldsymbol{x} + \int_{R^{n'}} G_R(|\boldsymbol{x}|,s)G_E(-z-|\boldsymbol{x}|,v)\,\mathrm{d}\boldsymbol{x}} \\
=&\frac{e^{-\frac{\pi r^2}{s^2}} e^{-\frac{\pi(z-r)^2}{v^2}} + e^{-\frac{\pi r^2}{s^2}} e^{-\frac{\pi(z+r)^2}{v^2}}}{\int_{R^{n'}} e^{-\frac{\pi|\boldsymbol{x}|^2}{s^2}} e^{-\frac{\pi(z-|\boldsymbol{x}|)^2}{v^2}}\,\mathrm{d}\boldsymbol{x} + \int_{R^{n'}} e^{-\frac{\pi|\boldsymbol{x}|^2}{s^2}} e^{-\frac{\pi(z+|\boldsymbol{x}|)^2}{v^2}}\,\mathrm{d}\boldsymbol{x}} \\
=&\frac{e^{-\left(\frac{\pi}{s^2}+\frac{\pi}{v^2}\right)\left(r-\frac{zs^2}{v^2+s^2}\right)^2} + e^{-\left(\frac{\pi}{s^2}+\frac{\pi}{v^2}\right)\left(r+\frac{zs^2}{v^2+s^2}\right)^2}}{N},
\end{aligned} \tag{6}$$

where N is the normalization factor.

It is easy to see that the probability density function $F_{R\big||R+E|=z}(R = r)$ is the sum of two Gaussian probability density functions center 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 5.8. *Suppose $v = s$, we can bound a center $\frac{zs^2}{v^2+s^2}$ from Equation 6 by $\Pr\left(\frac{zs^2}{v^2+s^2} \geq s\sqrt{n'}\right) \in 2^{-\Omega(n)}$.*

Proof. Details can be found in Section E of supplementary material. □

Recall that conditioned on the leakage, the weight placed by the conditional distribution on a vector $\boldsymbol{x} \in \mathbb{R}^{n'}$ is equivalent to $F_{R\big||R+E|=z}(R = r)$, where $r = \|\boldsymbol{x}\|$. Let $\Psi_{\sigma,c}(\boldsymbol{x}) := F_{R\big||R+E|=z}(R = \|\boldsymbol{x}\|)$ be the normalization of the function $f(\boldsymbol{x}) := e^{-\frac{\pi(\|\boldsymbol{x}\|-c)^2}{\sigma^2}} + e^{-\frac{\pi(\|\boldsymbol{x}\|+c)^2}{\sigma^2}}$. As shown in Lemma 5.8 above, we have that with all but negligible probability, $c := \frac{zs^2}{v^2+s^2} \leq \sqrt{2} \cdot \sigma\sqrt{n'}$. We next present the following Theorem.

Theorem 5.9. *Let R be the ring of integers in the m^{th} cyclotomic number field K of degree n, where n is a power of two. 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. 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 3.17 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, $\widehat{\Psi_{\sigma,c}}((\Lambda^\perp(A)^+)^\vee) \le 1 + 2^{-\Omega(n)}$, where $\widehat{\Psi_{\sigma,c}}$ denotes the Fourier transform of $\Psi_{\sigma,c}$ over n' dimensions.

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, $\widehat{\Psi_{\sigma,c}}(\mathbf{0}) := \int_{\mathbb{R}^{n'}} \Psi_{\sigma,c}(\boldsymbol{x})\,\mathrm{d}\boldsymbol{x}$. Since $\Psi_{\sigma,c}$ is a normalized pdf, it must be the case that $\int_{\mathbb{R}^{n'}} \Psi_{\sigma,c}(\boldsymbol{x})\,\mathrm{d}\boldsymbol{x} = 1$.

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

Towards showing this, we first let $\beta = 2n \cdot q^{k/l+2/(nl)}$ for simplicity, and then use Theorem 3.17 to show that, when $\kappa = |\boldsymbol{y}| \ge \frac{\sqrt{n/\pi}}{\beta}$,

$$\begin{aligned}\widehat{\Psi_{\sigma,c}}(\boldsymbol{y}) &\le {n'}^{n'} \cdot e^{-(\sigma^2\cdot\pi\cdot\kappa^2)} \\ &\le {n'}^{n'} \cdot e^{-5(\sigma^2\cdot\pi\cdot\kappa^2)/7} \cdot e^{-2(\sigma^2\cdot\pi\cdot\kappa^2)/7} \\ &\le e^{-2(\sigma^2\cdot\pi\cdot\kappa^2)/7},\end{aligned}$$

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 $\kappa \ge \frac{\sqrt{n/\pi}}{\beta}$, $e^{5(\sigma^2\cdot\pi\cdot\kappa^2)/7} \ge {n'}^{n'} = e^{n'\ln n'}$.

Let $Q := \sum_{\boldsymbol{y}\in(\Lambda^\perp(A)^+)^\vee\setminus\{\mathbf{0}\}} e^{-2(\sigma^2\cdot\pi\cdot\kappa^2)/7}$. Combining the above inequalities which hold when $\kappa \ge \frac{\sqrt{n/\pi}}{\beta}$, together with (b) and Corollary 3.15, 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 $\kappa \ge \frac{\sqrt{n/\pi}}{\beta}$, we conclude that an upper bound on Q yields an upper bound on the desired quantity, $\widehat{\Psi_{\sigma,c}}\left((\Lambda^\perp(A)^+)^\vee \setminus \{\mathbf{0}\}\right)$.

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

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

where the inequality follows since (by above) $e^{5(\sigma^2\cdot\pi\cdot\kappa^2)/7} \ge {n'}^{n'} = e^{n'\ln n'}$. so $e^{-(\sigma^2\cdot\pi\cdot\kappa^2)/7} \le {n'}^{-1/5\cdot n'} = e^{-1/5\cdot n'\ln n'}$

Moreover, recall that two applications of Poisson summation give:

$$\sum_{\boldsymbol{y}\in(\Lambda^\perp(A)^+)^\vee} e^{-(\sigma^2\cdot\pi\cdot\kappa^2)/7} \le 2^{n'} \cdot \sum_{\boldsymbol{y}\in(\Lambda^\perp(A)^+)^\vee} e^{-2(\sigma^2\cdot\pi\cdot\kappa^2)/7} \tag{8}$$

Combining the above, we have that

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

where the first inequality follows from (7) and the definition of Q, the second inequality follows from (8), and the final equality follows from the definition of Q.

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

Corollary 5.10. *Let R, n, q, k, l, σ and $\boldsymbol{c}$ be as in Theorem 5.9. Assume that $A = [I_k|\bar{A}] \in (R_q)^{k\times l}$ is chosen as in Theorem 5.4. Then, with probability $1 - 2^{-\Omega(n)}$ over the choice of $\bar{A}$, the distribution of $A\boldsymbol{x} \in R_q^k$, where $(\boldsymbol{x}, x_{n'}) \in R^l \times Z$ 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. Theorem 5.9 and Lemma 3.10 implies $\forall(\boldsymbol{b}, b_{n'}) \in R^l\times Z, \Psi_{\sigma,c}\left(\Lambda^\perp(A)^+ + (\boldsymbol{b},\ b')\right) \in \det((\Lambda^\perp(A)^+)^\vee)(1\pm 2^{-\Omega(n)}$, which means that if we choose a n'-dimensional vector from distribution $D_{R^l\times Z,\Psi_{\sigma,c}}$, written as $\boldsymbol{x'} = (\boldsymbol{x}, x_{n'})$, and let $(\boldsymbol{b}, b_{n'}) = \boldsymbol{x'} \mod (\Lambda^\perp(A)^+)$, 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 $\boldsymbol{b}$ is uniform over (R^l) modulo $(\Lambda^\perp(A))$. Moreover, we can easily see that for $\boldsymbol{x'} = (\boldsymbol{x}, x_{n'})$, if $\boldsymbol{x'} \mod (\Lambda^\perp(A)^+) = (\boldsymbol{b},\ b_{n'})$, then $A\boldsymbol{x} = A\boldsymbol{b}$. Finally, since when $\boldsymbol{b}$ is uniform random over R^l modulo $\Lambda^\perp(A)$, we have that $A\boldsymbol{b}$ is uniform random over R_q^k, the corollary follows. □

Given the corollary, the analysis of Leakage Scenario III is complete. Specifically, the above corollary (with $k = 1$), implies that the encryption scheme is secure under Leakage Scenario III assuming $\sigma \geq \sqrt{7/5 \cdot n'/n \cdot \ln n'} \cdot 2n \cdot q^{1/l+2/(nl)}$. Since $s = \sqrt{2}\sigma$, where s is the standard deviation of the secret key, it means that in order for the encryption scheme to be secure under Leakage Scenario III, we must simply sample the ($n' = (l \cdot n + 1)$-dimensional) secret key from $D_{R,\sqrt{14/5\cdot n'/n\cdot\ln n'}\cdot 2n\cdot q^{1/l+2/(nl)}}$, as opposed to $D_{R,2n\cdot q^{1/l+2/(nl)}}$. In particular, this means that the standard deviation should be increased by a factor of $\sqrt{14/5 \cdot n'/n \cdot \ln n'}$, beyond the parameters required by [33].

References

1. Ajtai, M.: Generating hard instances of lattice problems (extended abstract). In: 28th ACM STOC, ACM Press (May 1996) 99–108
2. Akavia, A., Goldwasser, S., Vaikuntanathan, V.: Simultaneous hardcore bits and cryptography against memory attacks. In Reingold, O., ed.: TCC 2009. Volume 5444 of LNCS., Springer, Heidelberg (March 2009) 474–495
3. Alperin-Sheriff, J., Peikert, C.: Circular and KDM security for identity-based encryption. In Fischlin, M., Buchmann, J., Manulis, M., eds.: PKC 2012. Volume 7293 of LNCS., Springer, Heidelberg (May 2012) 334–352
4. Alperin-Sheriff, J., Peikert, C.: Practical bootstrapping in quasilinear time. In Canetti, R., Garay, J.A., eds.: CRYPTO 2013, Part I. Volume 8042 of LNCS., Springer, Heidelberg (August 2013) 1–20
5. Boneh, D., DeMillo, R.A., Lipton, R.J.: On the importance of checking cryptographic protocols for faults (extended abstract). In Fumy, W., ed.: EUROCRYPT'97. Volume 1233 of LNCS., Springer, Heidelberg (May 1997) 37–51
6. Boneh, D., Freeman, D.M.: Linearly homomorphic signatures over binary fields and new tools for lattice-based signatures. In Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A., eds.: PKC 2011. Volume 6571 of LNCS., Springer, Heidelberg (March 2011) 1–16
7. Boyle, E., Segev, G., Wichs, D.: Fully leakage-resilient signatures. Journal of Cryptology **26**(3) (July 2013) 513–558
8. Brakerski, Z., Kalai, Y.T., Katz, J., Vaikuntanathan, V.: Overcoming the hole in the bucket: Public-key cryptography resilient to continual memory leakage. In: 51st FOCS, IEEE Computer Society Press (October 2010) 501–510
9. Brakerski, Z., Langlois, A., Peikert, C., Regev, O., Stehlé, D.: Classical hardness of learning with errors. In Boneh, D., Roughgarden, T., Feigenbaum, J., eds.: 45th ACM STOC, ACM Press (June 2013) 575–584
10. Brakerski, Z., Vaikuntanathan, V.: Efficient fully homomorphic encryption from (standard) LWE. In Ostrovsky, R., ed.: 52nd FOCS, IEEE Computer Society Press (October 2011) 97–106
11. Chung, K.M., Dadush, D., Liu, F.H., Peikert, C.: On the lattice smoothing parameter problem. In: Computational Complexity (CCC), 2013 IEEE Conference on, IEEE (2013) 230–241
12. Crockett, E., Peikert, C.: $\Lambda \circ \lambda$ functional lattice cryptography. In Weippl, E.R., Katzenbeisser, S., Kruegel, C., Myers, A.C., Halevi, S., eds.: ACM CCS 16, ACM Press (October 2016) 993–1005
13. Devroye, L.: Sample-based non-uniform random variate generation. In: Proceedings of the 18th conference on Winter simulation, ACM (1986) 260–265
14. Dodis, Y., Goldwasser, S., Kalai, Y.T., Peikert, C., Vaikuntanathan, V.: Public-key encryption schemes with auxiliary inputs. In Micciancio, D., ed.: TCC 2010. Volume 5978 of LNCS., Springer, Heidelberg (February 2010) 361–381

15. Dodis, Y., Haralambiev, K., López-Alt, A., Wichs, D.: Cryptography against continuous memory attacks. In: 51st FOCS, IEEE Computer Society Press (October 2010) 511–520
16. Dodis, Y., Kalai, Y.T., Lovett, S.: On cryptography with auxiliary input. In Mitzenmacher, M., ed.: 41st ACM STOC, ACM Press (May / June 2009) 621–630
17. Dusart, P., Letourneux, G., Vivolo, O.: Differential fault analysis on a.e.s. In: ACNS. (2003) 293–306
18. Dziembowski, S., Pietrzak, K.: Leakage-resilient cryptography. In: 49th FOCS, IEEE Computer Society Press (October 2008) 293–302
19. Espitau, T., Fouque, P.A., Gerard, B., Tibouchi, M.: 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.
20. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In Ladner, R.E., Dwork, C., eds.: 40th ACM STOC, ACM Press (May 2008) 197–206
21. Goldwasser, S., Kalai, Y.T., Peikert, C., Vaikuntanathan, V.: Robustness of the learning with errors assumption. In Yao, A.C.C., ed.: ICS 2010, Tsinghua University Press (January 2010) 230–240
22. Grafakos, L., Teschl, G.: On fourier transforms of radial functions and distributions. Journal of Fourier Analysis and Applications **19**(1) (Feb 2013) 167–179
23. Halderman, J.A., Schoen, S.D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J.A., Feldman, A.J., Appelbaum, J., Felten, E.W.: Lest we remember: cold-boot attacks on encryption keys. Commun. ACM **52**(5) (2009) 91–98
24. Katz, J., Vaikuntanathan, V.: Signature schemes with bounded leakage resilience. In Matsui, M., ed.: ASIACRYPT 2009. Volume 5912 of LNCS., Springer, Heidelberg (December 2009) 703–720
25. Kocher, P.C.: Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In Koblitz, N., ed.: CRYPTO'96. Volume 1109 of LNCS., Springer, Heidelberg (August 1996) 104–113
26. Kocher, P.C., Jaffe, J., Jun, B.: Differential power analysis. In Wiener, M.J., ed.: CRYPTO'99. Volume 1666 of LNCS., Springer, Heidelberg (August 1999) 388–397
27. Lewko, A.B., Lewko, M., Waters, B.: How to leak on key updates. In Fortnow, L., Vadhan, S.P., eds.: 43rd ACM STOC, ACM Press (June 2011) 725–734
28. Lindner, R., Peikert, C.: Better key sizes (and attacks) for LWE-Based encryption. Cryptology ePrint Archive, Report 2010/613 (2010) http://eprint.iacr.org/2010/613.
29. Lindner, R., Peikert, C.: Better key sizes (and attacks) for LWE-based encryption. In Kiayias, A., ed.: CT-RSA 2011. Volume 6558 of LNCS., Springer, Heidelberg (February 2011) 319–339
30. Ling, S., Phan, D.H., Stehlé, D., Steinfeld, R.: Hardness of k-LWE and applications in traitor tracing. In Garay, J.A., Gennaro, R., eds.: CRYPTO 2014, Part I. Volume 8616 of LNCS., Springer, Heidelberg (August 2014) 315–334
31. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. J. ACM **60**(6) (2013) 43:1–43:35
32. Lyubashevsky, V., Peikert, C., Regev, O.: A toolkit for ring-LWE cryptography. In Johansson, T., Nguyen, P.Q., eds.: EUROCRYPT 2013. Volume 7881 of LNCS., Springer, Heidelberg (May 2013) 35–54
33. Lyubashevsky, V., Peikert, C., Regev, O.: A toolkit for ring-LWE cryptography. Cryptology ePrint Archive, Report 2013/293 (2013) http://eprint.iacr.org/2013/293.
34. Malkin, T., Teranishi, I., Vahlis, Y., Yung, M.: Signatures resilient to continual leakage on memory and computation. In Ishai, Y., ed.: TCC 2011. Volume 6597 of LNCS., Springer, Heidelberg (March 2011) 89–106
35. Micciancio, D.: Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. Computational Complexity **16**(4) (2007) 365–411
36. Micciancio, D., Regev, O.: Worst-case to average-case reductions based on gaussian measures. SIAM Journal on Computing **37**(1) (2007) 267–302
37. Naor, M., Segev, G.: Public-key cryptosystems resilient to key leakage. SIAM J. Comput. **41**(4) (2012) 772–814
38. O'Neill, A., Peikert, C., Waters, B.: Bi-deniable public-key encryption. In Rogaway, P., ed.: CRYPTO 2011. Volume 6841 of LNCS., Springer, Heidelberg (August 2011) 525–542
39. Peikert, C.: Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In Mitzenmacher, M., ed.: 41st ACM STOC, ACM Press (May / June 2009) 333–342
40. Pietrzak, K.: A leakage-resilient mode of operation. In Joux, A., ed.: EUROCRYPT 2009. Volume 5479 of LNCS., Springer, Heidelberg (April 2009) 462–482
41. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In Gabow, H.N., Fagin, R., eds.: 37th ACM STOC, ACM Press (May 2005) 84–93
42. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM (JACM) **56**(6) (2009) 34
43. Roy, S.S., Reparaz, O., Vercauteren, F., Verbauwhede, I.: Compact and side channel resistant discrete gaussian sampling. IEEE Transactions on Circuits and Systems I: Regular Papers **62**(1) (2014) 157–166

44. Stehlé, D., Steinfeld, R., Tanaka, K., Xagawa, K.: Efficient public key encryption based on ideal lattices. In Matsui, M., ed.: ASIACRYPT 2009. Volume 5912 of LNCS., Springer, Heidelberg (December 2009) 617–635
45. Watson, G.: A Treatise on the Theory of Bessel Functions. Cambridge Mathematical Library. Cambridge University Press (1995)
46. Zhang, Y., Juels, A., Reiter, M.K., Ristenpart, T.: Cross-VM side channels and their use to extract private keys. In Yu, T., Danezis, G., Gligor, V.D., eds.: ACM CCS 12, ACM Press (October 2012) 305–316

Appendix

A Proof of Lemma 3.5

Lemma 3.5. *For any n-dimensional lattice Λ and $\varepsilon > 0$, $\boldsymbol{s} := (s_1, \ldots, s_n) \in \mathbb{R}^n_{>0}$, and $\boldsymbol{c} := (c_1, \ldots, c_n) \in \mathbb{R}^n$, 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 $\boldsymbol{x} \in \mathbb{R}^n$, $\widehat{\rho}_{(1/s_1,\ldots,1/s_n),(c_1,\ldots,c_n)}(\boldsymbol{x}) \leq (s_1)^{-1} \cdots (s_n)^{-1} \cdot \rho_{(s_1,\ldots,s_n)}(\boldsymbol{x})$, 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 $\eta_\varepsilon(\Lambda^\vee)$. □

B Proof of Lemma 3.10

Lemma 3.10. *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 $\boldsymbol{c} \in \mathbb{R}^n$, $\Psi(\Lambda + \boldsymbol{c}) \in \det(\Lambda^\vee)(1 \pm \varepsilon)$.*

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

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

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

C Proof of Lemma 3.16

Lemma 3.16. *Let $n' \in \mathbb{N}$ be odd, $\boldsymbol{x} \in \mathbb{R}^{n'}$, $c \in \mathbb{R}$. Then*

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

Proof. Let $f(\boldsymbol{x}) := e^{-\frac{\pi(\|\boldsymbol{x}\|-c)^2}{\sigma^2}} + e^{-\frac{\pi(\|\boldsymbol{x}\|+c)^2}{\sigma^2}}$. Let $r = \|\boldsymbol{x}\|$. 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

$$\int_{R^{n'}} f(\boldsymbol{x}) \, \mathrm{d}\boldsymbol{x} = n' V_{n'} \int_0^\infty r^{n'-1} f(r) \, \mathrm{d}r, \tag{9}$$

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

$$\int_0^\infty r^{n'-1} f(r)\,\mathrm{d}r = 1/2 \int_{-\infty}^\infty r^{n'-1} f(r)\,\mathrm{d}r. \tag{10}$$

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 (9) and (10) and substituting for a, we get that $\int_{R^{n'}} f(\boldsymbol{x})\,\mathrm{d}\boldsymbol{x} \geq \sigma^{n'}$, which completes the proof of the lemma. □

D Proof of Theorem 3.17

Theorem 3.17. *Let $\Psi_{\sigma,c}$ denote the normalized pdf corresponding to the non-normalized function $f(\boldsymbol{x}) := e^{-\frac{\pi(\|\boldsymbol{x}\|-c)^2}{\sigma^2}} + e^{-\frac{\pi(\|\boldsymbol{x}\|+c)^2}{\sigma^2}}$, where $\boldsymbol{x}$ is a vector over n' dimensions. and let $\widehat{\Psi_{\sigma,c}}(\boldsymbol{y})$ denote the n'-dimensional Fourier transform of $\Psi_{\sigma,c}$. Let $n' := l \cdot 2^a + 1$, where l, a are positive integers and $a > 2$, and $c \leq \sigma \cdot \sqrt{2} \cdot \sqrt{n'}$. Then $\widehat{\Psi_{\sigma,c}}(\boldsymbol{y}) \leq n'^{n'} \cdot e^{-\pi\|\boldsymbol{y}\|^2\sigma^2}$ for $\|\boldsymbol{y}\| > 1/\sigma$.*

Proof. Let N be the normalization of $f(\boldsymbol{x})$ over n' dimensions. We have from Lemma 3.16 that $N \geq \sigma^{n'}$ Thus, it remains to show that for $n' := l \cdot 2^a + 1$ and $c \leq \sigma \cdot \sqrt{2} \cdot \sqrt{n'}$, $\widehat{f}(\boldsymbol{y}) \leq \sigma^{n'} \cdot n'^{5/4} \cdot e^{-\pi\|\boldsymbol{y}\|^2\sigma^2}$.

Let $r := \|\boldsymbol{x}\|$, 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 $\kappa := \|\boldsymbol{y}\|$. We may now use the formula for the radial Fourier transform of an n'-dimensional, radial function f to find F [22]:

$$F(\kappa) = \kappa^{\frac{-(n'-2)}{2}} (2\pi) \int_0^\infty r^{\frac{n'-2}{2}} f(r) J_{\frac{n'-2}{2}}(2\pi\kappa r) r\,\mathrm{d}r, \tag{11}$$

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 [45, Page 40]:

$$J_\nu(z) := \sum_{j=0}^\infty \frac{(-1)^j (\frac{1}{2}z)^{\nu+2j}}{\Gamma(\nu+j+1)j!}. \tag{12}$$

For half-integer order $\nu := n + \frac{1}{2}$, there is a closed-form representation of J_ν. Specifically, it can be expressed as [45, Page 298]:

$$J_{n+\frac{1}{2}}(z) := R_{n,\frac{1}{2}}(z) \left(\frac{2}{\pi z}\right)^{\frac{1}{2}} \sin z - R_{n-1,\frac{3}{2}}(z) \left(\frac{2}{\pi z}\right)^{\frac{1}{2}} \cos z. \tag{13}$$

where $R_{n,\frac{1}{2}}(z)$ and $R_{n-1,\frac{3}{2}}(z)$ are Lommel polynomials defined as [45, Page 296]:

$$R_{n,\nu}(z) = \sum_{j=0}^{[n/2]} \frac{(-1)^j (n-j)! \Gamma(\nu+n-j)}{j!(n-2j)!\Gamma(\nu+j)} \left(\frac{z}{2}\right)^{2j-n}, \tag{14}$$

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

We now have:

$$\begin{aligned}
F(\kappa) &= \kappa^{\frac{-(n'-2)}{2}} (2\pi) \int_0^\infty r^{\frac{n'-2}{2}} f(r) J_{\frac{n'-2}{2}}(2\pi\kappa r) r \,\mathrm{d}r \\
&= \kappa^{\frac{-(n'-2)}{2}} (2\pi) \Bigg(\int_0^\infty r^{\frac{n'-2}{2}} f(r) \Bigg(\sum_{j=0}^{[\frac{n'-3}{4}]} c_j \Big(\frac{2\pi\kappa r}{2}\Big)^{2j-\frac{n'-3}{2}} \Bigg) \Big(\frac{2}{2\pi^2\kappa r}\Big)^{\frac{1}{2}} \sin(2\pi\kappa r) r \,\mathrm{d}r - \\
&\qquad \int_0^\infty r^{\frac{n'-2}{2}} f(r) \Bigg(\sum_{j=0}^{[\frac{n'-5}{4}]} c'_j \Big(\frac{2\pi\kappa r}{2}\Big)^{2j-\frac{n'-5}{2}} \Bigg) \Big(\frac{2}{2\pi^2\kappa r}\Big)^{\frac{1}{2}} \cos(2\pi\kappa r) r \,\mathrm{d}r \Bigg) \\
&\leq \kappa^{\frac{-(n'-2)}{2}} (2\pi) \Bigg(\left| \int_0^\infty r^{\frac{n'-2}{2}} f(r) \Bigg(\sum_{j=0}^{[\frac{n'-3}{4}]} c_j \Big(\frac{2\pi\kappa r}{2}\Big)^{2j-\frac{n'-3}{2}} \Bigg) \Big(\frac{2}{2\pi^2\kappa r}\Big)^{\frac{1}{2}} \sin(2\pi\kappa r) r \,\mathrm{d}r \right| + \\
&\qquad \left| \int_0^\infty r^{\frac{n'-2}{2}} f(r) \Bigg(\sum_{j=0}^{[\frac{n'-5}{4}]} c'_j \Big(\frac{2\pi\kappa r}{2}\Big)^{2j-\frac{n'-5}{2}} \Bigg) \Big(\frac{2}{2\pi^2\kappa r}\Big)^{\frac{1}{2}} \cos(2\pi\kappa r) r \,\mathrm{d}r \right| \Bigg),
\end{aligned} \tag{15}$$

where the first equality follows from (11), the second equality follows from (13), (14) 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 (15), we will individually upper bound

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

and

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

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

$$
\begin{aligned}
\mathrm{II} &= \left| \int_0^\infty r^{\frac{n'-2}{2}} f(r) \left(\sum_{j=0}^{[\frac{n'-5}{4}]} c'_j \Big(\frac{2\pi\kappa r}{2}\Big)^{2j-\frac{n'-5}{2}} \right) \Big(\frac{2}{2\pi^2\kappa r}\Big)^{\frac{1}{2}} \cos(2\pi\kappa r) r \,\mathrm{d}r \right| \\
&= 1/2 \left| \int_{-\infty}^\infty r^{\frac{n'-2}{2}} f(r) \left(\sum_{j=0}^{[\frac{n'-5}{4}]} c'_j \Big(\frac{2\pi\kappa r}{2}\Big)^{2j-\frac{n'-5}{2}} \right) \Big(\frac{2}{2\pi^2\kappa r}\Big)^{\frac{1}{2}} \Big(\frac{e^{i2\pi\kappa r}+e^{-i2\pi\kappa r}}{2}\Big) r \,\mathrm{d}r \right| \\
&= 1/2 \Big(\frac{1}{4\pi^2\kappa}\Big)^{\frac{1}{2}} \left| \int_{-\infty}^\infty r^{\frac{n'-1}{2}} f(r) \left(\sum_{j=0}^{[\frac{n'-5}{4}]} c'_j \Big(\frac{2\pi\kappa r}{2}\Big)^{2j-\frac{n'}{2}+\frac{5}{2}} \right) (e^{i2\pi\kappa r}+e^{-i2\pi\kappa r}) \,\mathrm{d}r \right| \\
&\leq 1/2 \Big(\frac{1}{4\pi^2\kappa}\Big)^{\frac{1}{2}} \sum_{j=0}^{[\frac{n'-5}{4}]} |c'_j| \Big(\pi\kappa\Big)^{2j-\frac{n'}{2}+\frac{5}{2}} \left| \int_{-\infty}^\infty r^{2j+2} \left(e^{-\frac{\pi(r-c)^2}{\sigma^2}} + e^{-\frac{\pi(r+c)^2}{\sigma^2}} \right) (e^{i2\pi\kappa r}+e^{-i2\pi\kappa r}) \,\mathrm{d}r \right|, \quad (16)
\end{aligned}
$$

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

$$
\left| \int_{-\infty}^\infty r^{2j+2} \left(e^{-\frac{\pi(r-c)^2}{\sigma^2}} + e^{-\frac{\pi(r+c)^2}{\sigma^2}} \right) (e^{i2\pi\kappa r}+e^{-i2\pi\kappa r}) \,\mathrm{d}r \right| \quad (17)
$$

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

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

Plugging the above back into (16), 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

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

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

$$\begin{aligned}
\text{I} &= \left|\int_0^\infty r^{\frac{n'-2}{2}} f(r)\left(\sum_{j=0}^{[\frac{n'-3}{4}]} c_j\left(\frac{2\pi\kappa r}{2}\right)^{2j-\frac{n'-3}{2}}\right)\left(\frac{2}{2\pi^2\kappa r}\right)^{\frac{1}{2}}\sin(2\pi\kappa r) r\,\mathrm{d}r\right| \\
&= 1/2\left|\int_{-\infty}^\infty r^{\frac{n'-2}{2}} f(r)\left(\sum_{j=0}^{[\frac{n'-3}{4}]} c_j\left(\frac{2\pi\kappa r}{2}\right)^{2j-\frac{n'-3}{2}}\right)\left(\frac{2}{2\pi^2\kappa r}\right)^{\frac{1}{2}}\left(\frac{e^{i2\pi\kappa r}-e^{-i2\pi\kappa r}}{2i}\right) r\,\mathrm{d}r\right| \\
&\leq 1/2\cdot\left(\frac{1}{4\pi^2\kappa}\right)^{\frac{1}{2}}\left|\int_{-\infty}^\infty r^{\frac{n'-1}{2}} f(r)\left(\sum_{j=0}^{[\frac{n'-3}{4}]} c_j\left(\frac{2\pi\kappa r}{2}\right)^{2j-\frac{n'-3}{2}}\right)(e^{i2\pi\kappa r}-e^{-i2\pi\kappa r})\,\mathrm{d}r\right| \\
&\leq 1/2\cdot\left(\frac{1}{4\pi^2\kappa}\right)^{\frac{1}{2}}\sum_{j=0}^{[\frac{n'-3}{4}]}|c_j|\left(\pi\kappa\right)^{2j-\frac{n'}{2}+\frac{3}{2}}\left|\int_{-\infty}^\infty r^{2j+1}\left(e^{-\frac{\pi(r-c)^2}{\sigma^2}}+e^{-\frac{\pi(r+c)^2}{\sigma^2}}\right)(e^{i2\pi\kappa r}-e^{-i2\pi\kappa r})\,\mathrm{d}r\right|, \quad (18)
\end{aligned}$$

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

$$\int_{-\infty}^\infty r^{2j+1}\left(e^{-\frac{\pi(r-c)^2}{\sigma^2}}+e^{-\frac{\pi(r+c)^2}{\sigma^2}}\right)(e^{i2\pi\kappa r}-e^{-i2\pi\kappa r})\,\mathrm{d}r \quad (19)$$

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

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

Thus, we have that

$$
(19) \le \left(\frac{\sigma}{\sqrt{\pi}}\right)^{2j+2} e^{-\pi\kappa^2\sigma^2}\Gamma(\frac{1}{2}+j)\binom{2j+1}{j+1}\left[4(\frac{c}{\sigma}+\kappa\sigma)^{2j+1}\right]
$$

Plugging the above back into (18), 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

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

Where the last inequality follows since $\binom{n}{i} \le 2^n$ and $n! \le n^n$. Finally, plugging into (15), and recalling that $c \le \sigma\cdot\sqrt{2}\cdot\sqrt{n'}$ and $\kappa > \frac{1}{\sigma}$, we obtain:

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

□

E Proof of Lemma 5.8

Theorem E.1. *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* $\Pr\left(Y \ge v\sqrt{n'}\right) \in 2^{-\Omega(n)}$.

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. □

Lemma 5.8. *Suppose $v = s$, we can bound a center $\frac{zs^2}{v^2+s^2}$ from Equation 6 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

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

By Lemma 3.9 and Lemma E.1, we deduce that $\Pr\left(\frac{zs^2}{v^2+s^2} \geq s\sqrt{n'}\right) \in 2^{-\Omega(n)}$. □