Noise Distributions in Homomorphic Ring-LWE

Sean Murphy and Rachel Player

Royal Holloway, University of London, U.K.
s.murphy@rhul.ac.uk
Rachel.Player.2013@live.rhul.ac.uk
12 June 2017

Abstract. We develop a statistical framework to analyse the Ring-LWE processes of *A Toolkit for Ring-LWE Cryptography* (Eurocrypt 2013) and similar processes. We consider the δ-subgaussian random variables used in the *Toolkit* and elsewhere in the literature, and we give a simple and complete characterisation of such random variables. We then apply our results to the homomorphic cryptosystem provided as an example application in the *Toolkit*. We show that the δ-subgaussian approach as used in the *Toolkit* to argue correctness of this cryptosystem is flawed, and we also rectify this analysis using our developed statistical framework.

Keywords. Ring Learning with Errors, Subgaussian Random Variable, Homomorphic Encryption.

1 Introduction

The Learning with Errors or *LWE* problem [30, 31] has become a standard hard problem in cryptology that is at the heart of lattice-based cryptography [24, 27]. The Ring Learning with Errors or *Ring-LWE* problem [20] is a generalisation of the LWE problem from the ring of integers to certain other number field rings, and a formal statement of the Ring-LWE problem is given in Figure 1. Both the LWE problem and the Ring-LWE problem are related to well-studied lattice problems which are believed to be hard [4, 20, 21, 25, 30].

Hardness of Ring-LWE. We briefly summarise hardness results pertaining to Ring-LWE. For formal statements of theorems and reductions, we refer the reader to [20, 21, 29]. The most relevant result for our purpose is [20, Theorem 3.6], also stated as [21, Theorem 2.22]: if K is a cyclotomic number field with ring of integers R, then there is a polynomial time quantum reduction from approximate SIVP (Shortest Independent Vector Problem) on ideal lattices in K to Decision Ring-LWE in R given a fixed number of samples, where the error distribution is a fixed spherical Gaussian over the field tensor product $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$. A more general result, for any number field, is given in [29].

In more detail, there is a quantum reduction from a particular hard lattice problem to Search Ring-LWE in the ring of integers R of an arbitrary number field K [20, Theorem 4.1]. This requires a family of distributions which are Gaussian (spherical or elliptical) over $K_{\mathbb{R}}$. For the special case of rings of integers

Ring-LWE. Let R be the ring of integers of a number field K. Let $R^\vee$ be the dual fractional ideal of R. Let q be an integer modulus. Let $R_q = R/qR$ and $R_q^\vee = R^\vee/qR^\vee$. Let $K_\mathbb{R} = K \otimes_\mathbb{Q} \mathbb{R}$. Let χ be a distribution over $K_\mathbb{R}$. Let $s \in R_q^\vee$ be a secret. A sample from the Ring-LWE distribution $A_{s,\chi}$ over $R_q \times K_\mathbb{R}/qR^\vee$ is

$$(a, b = a \cdot s + e \mod qR^\vee)$$

where $a \leftarrow R_q$ is chosen uniformly at random and $e \leftarrow \chi$.
• *Decision Ring-LWE* is the problem of deciding whether samples (a_i, b_i) are chosen according to the distribution $A_{s,\chi}$ or are uniformly random.
• *Search Ring-LWE* is the problem of recovering s from (a_i, b_i) sampled according to $A_{s,\chi}$.

Fig. 1. The Ring-LWE problem [19, 21].

of cyclotomic fields, a reduction from Search Ring-LWE to Decision Ring-LWE is given in [20] and generalised in [10] and [8]. When the number of samples is bounded, we can give a reduction from Search Ring-LWE in the ring of integers of a cyclotomic field to Decision Ring-LWE for a fixed spherical Gaussian error distribution over $K_\mathbb{R}$ [20, Theorem 5.2].

Spherical gaussians. In the hardness results for Ring-LWE above, the error distributions are spherical Gaussians over $K_\mathbb{R}$. A reasonable question is whether or not one could use a different error distribution, or indeed modify the Ring-LWE instance in some other way, such that there is no longer a hardness reduction. There is some evidence to suggest that the use of a setting in which the induced Ring-LWE problem is not provably as hard as well-studied lattice problems may be dangerous from a security perspective. In particular, a number of works have given attacks on Ring-LWE when the underlying number field, error distribution, or modulus is of various special forms [6–11, 28]. Due to the presence of weaker settings vulnerable to attacks, it may make sense to consider only settings with provable hardness results. Indeed in practice, almost all works basing their hardness on Ring-LWE use cyclotomic rings, with power-of-2 cyclotomics being especially common (due also to efficiency and ease of sampling errors).

Homomorphic encryption. A key application of lattice-based cryptography is the ability to achieve (fully, somewhat or levelled) homomorphic encryption. Using homomorphic encryption means that one party (the server) can operate meaningfully on encrypted data belonging to a different party (the client), and the server does not need access to the secret key in order to do this. This allows a computationally weak client to outsource computation on their data to a powerful server, without having to share their data with the server in the clear. The server performs a homomorphic evaluation operation on input ciphertexts which produces an output ciphertext that the client can decrypt to obtain the result of some useful function on the data. For example, we can define a *homomorphic addition* operation, which takes as input two ciphertexts c_1 and c_2 encrypting m_1 and m_2 respectively and outputs a ciphertext encrypting $m_1 + m_2$. Similarly

we can also define a *homomorphic multiplication* operation which takes as input c_1 and c_2 and outputs a ciphertext encrypting $m_1 \cdot m_2$. An encryption scheme, augmented with both such a homomorphic addition and a homomorphic multiplication operation, would then enable arbitrary computation on encrypted data. Constructing such a *fully homomorphic encryption* scheme was a longstanding open problem until it was resolved in Gentry's seminal work [14]. Gentry's original scheme begins by specifying a *somewhat homomorphic encryption* scheme, in which ciphertexts have an inherent noise, which grows during homomorphic operations. Gentry then shows how to transform a somewhat homomorphic encryption scheme into a fully homomorphic encryption scheme using a technique known as bootstrapping. A large number of somewhat homomorphic cryptosystems have been proposed in the literature, for example [1–3, 5, 12, 15, 16, 18, 34]. Several of these are based on Ring-LWE, for example [2, 3, 5, 12, 15].

Noise. A common feature among all homomorphic encryption schemes is that all ciphertexts have an inherent 'noise'. This is typically small in a fresh ciphertext, but the noise grows as homomorphic evaluation operations are performed. If the noise grows too large, then decryption fails, so a good understanding of the noise growth behaviour of a homomorphic encryption scheme is essential to choose appropriate parameters to ensure correctness. Typically, the noise in a ciphertext in a Ring-LWE-based homomorphic encryption scheme is related to the error distribution used in the underlying Ring-LWE instance, but often does not directly follow a spherical gaussian distribution.

The `THRing` *cryptosystem.* Lyubashevsky, Peikert, and Regev's work *A Toolkit for Ring-LWE Cryptography* [21], which we refer to as the *Toolkit*, is a paper of particular note in Ring-LWE cryptography, and an abridged form was published at Eurocrypt 2013 [22]. The homomorphic Ring-LWE cryptosystem, or `THRing` cryptosystem, of the *Toolkit* Section 8.3 is given an example application of Ring-LWE. In the `THRing` cryptosystem, the noise in a fresh ciphertext is obtained from a perturbation of a spherical gaussian.

δ-subgaussian random variables. The *Toolkit* uses a relaxation of a subgaussian random variable (see for example [32]), called a δ-subgaussian random variable, to analyse the `THRing` cryptosystem. The use of δ-subgaussian random variables in statistical analyses in cryptography is not limited to homomorphic encryption applications. For example, they are used in the analysis of a signature scheme given by Micciancio and Peikert in [23]. They are also used in the analysis of correctness of Peikert's key exchange protocol [26] (indeed, the analysis presented in [26] also relies on results from the *Toolkit*).

A fundamental issue of the Toolkit analysis of the `THRing` *Cryptosystem.* We refer to the random variables we must consider when analysing the noise growth behaviour in the `THRing` cryptosystem as various types of *Noise* random variables. These *Noise* random variables are perturbed spherical gaussians. To determine whether the decryption of a ciphertext produced as the output of a

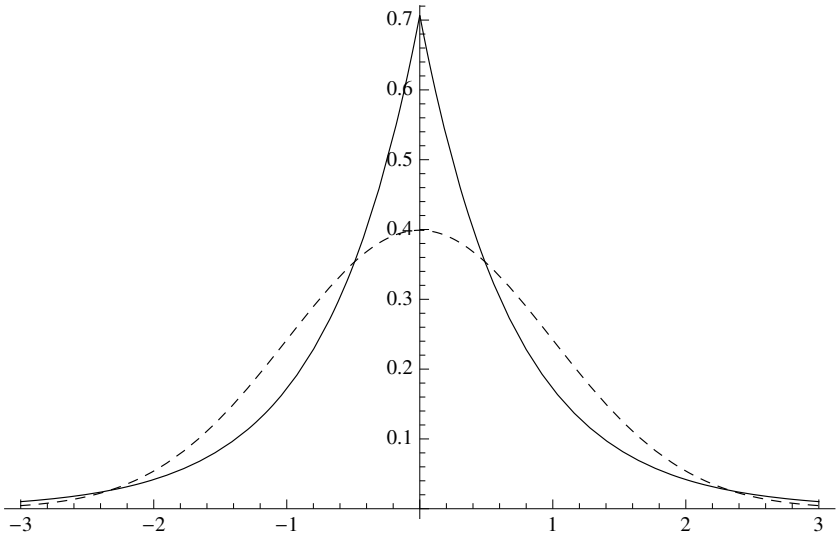

Fig. 2. Density function for the Laplace $2^{\frac{1}{2}}(\mathrm{N}(0,1)\cdot\mathrm{N}(0,1)+\mathrm{N}(0,1)\cdot\mathrm{N}(0,1))$ random variable arising as a component of a Noise product (solid line) and the density function for the corresponding standard Normal $\mathrm{N}(0,1)$ random variable (dashed line).

homomorphic multiplication of two fresh ciphertexts succeeds, we must consider a product of *Noise* random variables. The statistical argument of the *Toolkit* about a product of such Noise random variables essentially reduces to an assertion that a component of such a product of Noise random variables can be well-approximated as a corresponding Normal random variable with the same mean and variance. However, when considered as a real vector with respect to an appropriate basis, a component of such a Noise product has a Laplace distribution arising as the sum of two products of two independent Normal random variables (Section 4.5). Figure 2 illustrates that a density function of a component of such a product of Noise random variables, the Laplace random variable $2^{\frac{1}{2}}(\mathrm{N}(0,1)\cdot\mathrm{N}(0,1)+\mathrm{N}(0,1)\cdot\mathrm{N}(0,1))$, is very different to the density function of a standard Normal $\mathrm{N}(0,1)$ random variable having the same mean and variance. Figure 3 illustrates the corresponding very different tail probabilities for these two random variables.

1.1 Contributions of this Paper

A major contribution of this paper is to give a full and particularly simple characterisation of δ-subgaussian random variables, which are used extensively by the *Toolkit* and elsewhere to analyse homomorphic Ring-LWE cryptosystems and related matters. This simple characterisation allows us to improve and extend existing results for the sum and product of δ-subgaussian random variables used in cryptography, and also improve results existing for the variability of a discretisation process.

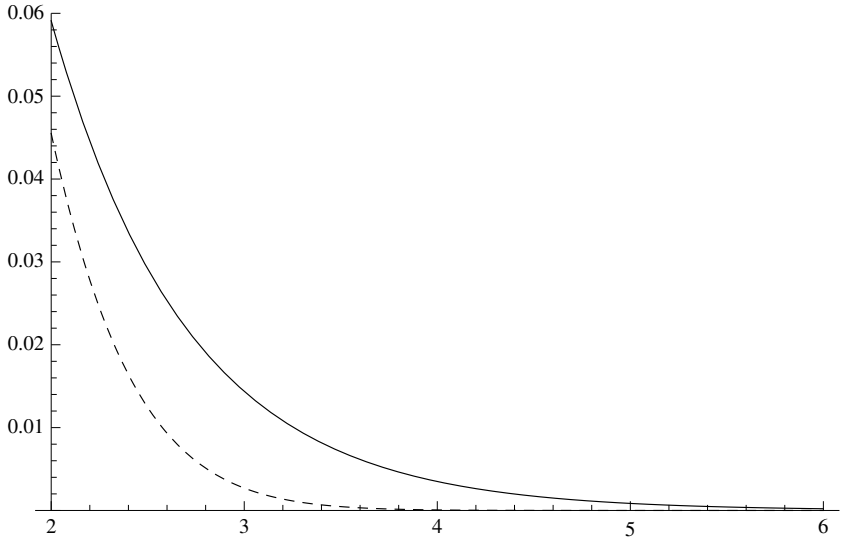

Fig. 3. Tail probability for the Laplace $2^{\frac{1}{2}}(\mathrm{N}(0,1)\cdot\mathrm{N}(0,1)+\mathrm{N}(0,1)\cdot\mathrm{N}(0,1))$ random variable arising as a component of a Noise product (solid line) and the density function for the corresponding standard Normal $\mathrm{N}(0,1)$ random variable (dashed line).

A further contribution is the use of this δ-subgaussian characterisation to provide evidence that δ-subgaussian approach of the *Toolkit* to analyse the correctness of its `THRing` cryptosystem is flawed. A final contribution is to provide a rigorous statistical analysis of the `THRing` cryptosystem. In contrast to the *Toolkit* approach, we are able to bound the probability of incorrect decryption of ciphertexts without appealing to an argument based on the use of δ-subgaussian random variables. The derivation of this bound rests on the Central Limit Theorem applied to random variables that cannot be approximated as δ-subgaussian random variables.

1.2 Structure of the Paper

We review the algebraic background for Ring-LWE in Section 2, and we analyse and characterise δ-subgaussian random variables in Section 3. We analyse the multivariate gaussian distributions used in Ring-LWE applications in Section 4, and we consider the discretisations of such random variables in Section 5. Finally, we apply results from the previous sections to the `THRing` cryptosystem in Section 6.

2 Algebraic Background for Ring-LWE

We give the algebraic background for our analysis of Ring-LWE. This background has its origins in the *Toolkit* and in part follows the *Toolkit*. We consider the

ring $R = \mathbb{Z}[X]/(\Phi_m(X))$, where $\Phi_m(X)$ is the m^{th} cyclotomic polynomial of degree n, and we let R_a denote R/aR for an integer a. For simplicity, we only consider the case where m is a large prime, so $n = \phi(m) = m - 1$, and we also let $n' = \frac{1}{2}n = \frac{1}{2}(m-1)$, though our arguments apply more generally.

There are three natural algebraic settings for the discussion of Ring-LWE: the complex space H, the n-dimensional real vector space, and the m^{th} cyclotomic number field. We move between these settings at different places in our discussion of Ring-LWE.

2.1 Cyclotomic Number Fields

Let ζ_m denote a (primitive) m^{th} root of unity, which has minimal polynomial $\Phi_m(X) = 1 + X + \ldots + X^n$. The m^{th} *cyclotomic number field*

$$K = \mathbb{Q}(\zeta_m)$$

is the field extension of the rational numbers $\mathbb{Q}$ obtained by adjoining this m^{th} root of unity ζ_m, so K has degree n.

There are n *ring embeddings* $\sigma_1, \ldots, \sigma_n \colon K \to \mathbb{C}$ that fix every element of $\mathbb{Q}$. Such a ring embedding σ_k (for $1 \leq k \leq n$) is defined by $\zeta_m \mapsto \zeta_m^k$, so $\sum_{j=1}^n a_j \zeta_m^j \mapsto \sum_{j=1}^n a_j \zeta_m^{kj}$. It is clear that such ring embeddings occur in conjugate pairs. The *canonical embedding* $\sigma : K \to \mathbb{C}^n$ is defined by

$$a \mapsto (\sigma_1(a), \ldots, \sigma_n(a))^T.$$

We can define a natural induced geometry on K with ℓ_2-norm $\|\cdot\|_2$ and ℓ_∞-norm $\|\cdot\|_\infty$ given by the element's norm under the canonical embedding σ, that is to say

$$\|a\|_2 = \|\sigma(a)\|_2 = \sum_{j=1}^{n} |\sigma_j(a)|^2 = 2\sum_{j=1}^{n'} |\sigma_j(a)|^2$$
$$\text{and } \|a\|_\infty = \|\sigma(a)\|_\infty = \max\{|\sigma_1(a)|, \ldots, |\sigma_n(a)|\}.$$

The *ring of integers* $\mathcal{O}_K$ of a number field is the ring of all elements of the number field which are roots of some monic polynomial with coefficients in $\mathbb{Z}$. The ring of integers of the m^{th} cyclotomic number field K is

$$R = \mathbb{Z}[\zeta_m] \cong \mathbb{Z}[x]/(\Phi_m).$$

The canonical embedding σ embeds R as a lattice $\sigma(R)$. The conjugate dual of this lattice corresponds to the embedding of the dual fractional ideal

$$R^\vee = \{a \in K \mid \text{Tr}(aR) \subset \mathbb{Z}\}.$$

If we define t such that $t^{-1} = m^{-1}(1 - \zeta_m)$, then $R^\vee = \langle t^{-1} \rangle$. We let $(R^\vee)^k$ denote the space of products of k elements of $R^\vee$, that is to say

$$(R^\vee)^k = \{s_1 \ldots s_k \mid s_1, \ldots, s_k \in R^\vee\} = \left\{t^{-k} r_1 \ldots r_k \mid r_1, \ldots, r_k \in R\right\}.$$

2.2 The Powerful Basis and the Decoding Basis

The analysis of Ring-LWE given by the *Toolkit* is based on various $\mathbb{Z}$-bases of K, R and $R^\vee$, and we now specify these relevant $\mathbb{Z}$-bases in the case when m is prime.

Definition 1. (*Toolkit* Definition 4.1.) The *Powerful Basis* $\overrightarrow{p}$ of $K = \mathbb{Q}(\zeta_m)$ and $R = \mathbb{Z}[\zeta_m]$ is

$$\left\{\zeta_m^0, \zeta_m^1, \ldots, \zeta_m^{n-1}\right\}. \qquad \square$$

Definition 2. (*Toolkit* Equation (6.3).) The *Decoding Basis* $\overrightarrow{d}$ of $R^\vee$ is

$$\left\{\tfrac{1}{m}(\zeta_m^0 - \zeta_m^n), \tfrac{1}{m}(\zeta_m^1 - \zeta_m^n), \ldots, \tfrac{1}{m}(\zeta_m^{n-1} - \zeta_m^n)\right\}. \qquad \square$$

Definition 3. (*Toolkit* Section 6.2.) The *Scaled Decoding Basis* of $(R^\vee)^k$ is

$$m^{-(k-1)}\overrightarrow{d} = \left\{\tfrac{1}{m^k}(\zeta_m^0 - \zeta_m^n), \tfrac{1}{m^k}(\zeta_m^1 - \zeta_m^n), \ldots, \tfrac{1}{m^k}(\zeta_m^{n-1} - \zeta_m^n)\right\}. \qquad \square$$

A drawback of these bases is that they are very generally defined and so not all basis elements occur in conjugate pairs. In the case when m is prime, we can define and use the following alternative bases where the elements do occur in conjugate pairs.

Definition 4. The *Powerful Conjugate Pair Basis* $\overrightarrow{q}$ of $K = \mathbb{Q}(\zeta_m)$ and $R = \mathbb{Z}[\zeta_m]$ is

$$\left\{\zeta_m^1, \zeta_m^2, \ldots, \zeta_m^n\right\}. \qquad \square$$

Definition 5. The *Decoding Conjugate Pair Basis* $\overrightarrow{c}$ of $R^\vee$ is

$$\left\{\tfrac{1}{m}(1 - \zeta_m^1), \tfrac{1}{m}(1 - \zeta_m^2), \ldots, \tfrac{1}{m}(1 - \zeta_m^n)\right\}. \qquad \square$$

Definition 6. The *Scaled Decoding Conjugate Pair Basis* of $(R^\vee)^k$ is

$$m^{-(k-1)}\overrightarrow{c} = \left\{\tfrac{1}{m^k}(1 - \zeta_m^1), \tfrac{1}{m^k}(1 - \zeta_m^2), \ldots, \tfrac{1}{m^k}(1 - \zeta_m^n)\right\}. \qquad \square$$

2.3 The Complex Space H

The ring embeddings $\sigma_1, \ldots, \sigma_n$ defined in Section 2.1 occur in complex conjugate pairs with $\overline{\sigma_k} = \sigma_{m-k}$, as we noted above. Accordingly, much of the analysis of Ring-LWE takes place in a space of conjugate pairs of complex numbers. We now specify the appropriate complex space for analysing Ring-LWE, which following the *Toolkit* we denote by H. In order to do so, we first define a complex matrix, the conjugate pairs matrix T. As we are working in a complex space, we use the notation † to denote the complex conjugate transpose of a matrix, so $T^\dagger = \overline{T}^T$ and so on.

Definition 7. The *conjugate pair matrix* is the $n \times n$ complex matrix T, so $T\colon \mathbb{C}^n \to \mathbb{C}^n$, given by

$$T = 2^{-\frac{1}{2}} \begin{pmatrix} 1 & 0 \dots 0 & 0 \dots & 0 & i \\ 0 & 1 \dots 0 & 0 \dots & i & 0 \\ \vdots & \vdots \ddots \vdots & \vdots & \vdots & \vdots \\ 0 & 0 \dots 1 & i \dots & 0 & 0 \\ 0 & 0 \dots 1 & -i \dots & 0 & 0 \\ \vdots & \vdots & \vdots \ddots & \vdots & \vdots \\ 0 & 1 \dots 0 & 0 \dots & -i & 0 \\ 1 & 0 \dots 0 & 0 \dots & 0 & -i \end{pmatrix}. \qquad \square$$

Lemma 1. The conjugate pair matrix T has determinant $(-i)^{n'}$ of absolute size 1 and is a unitary matrix with

$$T^{-1} = T^\dagger = 2^{-\frac{1}{2}} \begin{pmatrix} 1 & 0 \dots 0 & 1 \\ 0 & 1 \dots 1 & 0 \\ \vdots & \vdots \ddots \vdots & \vdots \\ 0 & -i \dots i & 0 \\ -i & 0 \dots 0 & i \end{pmatrix}. \qquad \square$$

Definition 8. The complex conjugate pair space $H = T(\mathbb{R}^n)$, where T is the conjugate pairs matrix. $\square$

Definition 9. The *I-basis* for H is given by the columns of the $n \times n$ identity matrix I, that is to say by standard basis vectors. $\square$

Definition 10. The *T-basis* for H is given by the columns of the conjugate pair matrix T. $\square$

The I-basis and T-basis for H give two different ways of expressing an element of H as a vector:

$$\begin{aligned} &H\text{-vectors in the } I\text{-basis} && \left\{ (z_1, \dots, z_{n'}, \overline{z}_{n'}, \dots, \overline{z}_1)^T \,\middle|\, z_1, \dots, z_{n'} \in \mathbb{C} \right\}, \\ &H\text{-vectors in the } T\text{-basis} && \left\{ (w_1, \dots, w_n)^T \,\middle|\, w_1, \dots, w_n \in \mathbb{R} \right\}. \end{aligned}$$

An element of H is expressed as a vector in the I-basis as a vector of n' conjugate pairs. Such an element of H can also be expressed (by construction) as a vector in the T-basis as a real-valued vector. We also note that the vector representing an element in the T-basis for H has the same norm as an element representing the same element in T-basis for H, as $|Tv|^2 = |v|^2$ because T is a unitary matrix. Expressing elements of H as vectors in the T-basis therefore gives the isomorphism between H and $\mathbb{R}^n$ as an inner product space. Thus the T-basis for H is a very natural basis to use for the analysis of Ring-LWE.

We have seen that the expression of an element of H in the I-basis gives a vector of complex conjugate pairs. It is sometimes convenient to consider such

a single conjugate pair in isolation, so giving rise to the H_2-space and so on of Definition 11. It is clear that the space H is isomorphic to the n'-fold product of H_2-spaces $H_2 \times \ldots \times H_2$. We therefore refer to such 2-dimensional subspaces of H that arise in the I-basis as the H_2-components of H.

Definition 11. The *single conjugate pair space* H_2 is given by

$$H_2 = T(\mathbb{R}^2) = 2^{-\frac{1}{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} (\mathbb{R}^2)\,. \qquad \square$$

We can define *conjugate pair* mappings $\widetilde{\sigma}_i$ for $1 \leq i \leq n'$ on K by

$$\widetilde{\sigma}_i(a) = (\sigma_i(a), \sigma_{m-i}(a))^T$$

where σ_i are the ring embeddings defined in Section 2.1. The conjugate pair mappings are each (by definition) an embedding $\widetilde{\sigma}_i \colon K \to H_2$. The canonical embedding σ can therefore be regarded as essentially the concatenation of the n' conjugate pair embeddings $\widetilde{\sigma}_1, \ldots, \widetilde{\sigma}_{n'}$, In particular, the canonical embedding actually embeds K into $H_2 \times \ldots \times H_2 \cong H \subset \mathbb{C}^n$, and such an embedded element is expressed as a vector (with appropriate component re-ordering) with respect to the I-basis for H.

The canonical embedding under σ of a sum in the cyclotomic number field gives a componentwise addition in H of the vectors expressing the embedded elements for any basis for H. Similarly, the canonical embedding under σ of a product in the cyclotomic number field gives rise to a componentwise $\odot$-product in H when the vectors expressing the embedded elements are in the I-basis for H, when we have

$$\begin{aligned} \sigma(aa') &= (\sigma_1(aa'), \ldots, \sigma_n(aa'))^T = (\sigma_1(a)\sigma_1(a'), \ldots, \sigma_n(a)\sigma_n(a'))^T \\ &= (\sigma_1(a), \ldots, \sigma_n(a))^T \odot (\sigma_1(a'), \ldots, \sigma_n(a'))^T \\ &= \sigma(a) \odot \sigma(a'). \end{aligned}$$

The canonical embedding of a product under σ gives other forms of "product" for the corresponding vectors expressing elements of H when other bases are used. The appropriate notion of a product of two elements of the complex space H when these elements are expressed as real vectors in the T-basis for H is given by Definition 12, which specifies the $\otimes$-product of two real vectors.

Definition 12. The $\otimes$-*product* of two real vectors $u = (u_{11}, u_{12}, \ldots, u_{n'1}, u_{n'2})^T$ and $v = (v_{11}, v_{12}, \ldots, v_{n'1}, v_{n'2})^T$ of length $n = 2n'$ is

$$u \otimes v = \begin{pmatrix} u_{11} \\ u_{12} \\ \vdots \\ u_{n'1} \\ u_{n'2} \end{pmatrix} \otimes \begin{pmatrix} v_{11} \\ v_{12} \\ \vdots \\ v_{n'1} \\ v_{n'2} \end{pmatrix} = T^{\dagger}\left(Tu \odot Tv\right) = 2^{-\frac{1}{2}} \begin{pmatrix} u_{11}v_{11} - u_{12}v_{12} \\ u_{11}v_{12} + u_{12}v_{11} \\ \vdots \\ u_{n'1}v_{n'1} - u_{n'2}v_{n'2} \\ u_{n'1}v_{n'2} + u_{n'2}v_{n'1} \end{pmatrix}.$$

The $\otimes$-product of two vectors in H expressed in the T-basis is the expression in the T-basis of the componentwise product $\odot$ of those two vectors when expressed in the I-basis. $\square$

$$H \text{ with } T\text{-basis} \quad \underset{\Delta^{-1} = T^{-1}\Gamma}{\overset{\Delta = \Gamma^{-1}T}{\longleftrightarrow}} \quad H \text{ with } \Gamma\text{-basis} \quad \underset{\Delta'^{-1} = \Gamma^{-1}\Gamma'}{\overset{\Delta' = \Gamma'^{-1}\Gamma}{\longleftrightarrow}} \quad H \text{ with } \Gamma'\text{-basis}$$

Fig. 4. Change of Basis Matrices for Bases expressing Elements of H as Real Vectors.

We now define two further bases for H, obtained by embedding certain number field bases of Section 2.2, in which elements of H are expressed as real-valued vectors. These bases are used by the decryption process of the `THRing` cryptosystem. We also give the eigenvalues of the Gram matrix [13] of these basis matrices of H and discuss the change-of-basis transformations between these various bases for H, as shown in Figure 4.

Definition 13. The *embedded decoding conjugate pair basis* $\sigma(\overrightarrow{c})$ or Γ-basis for H is the basis given by the columns of the matrix Γ, where

$$\Gamma = \frac{1}{m}\begin{pmatrix} 1-\zeta_m^{1\cdot 1} & 1-\zeta_m^{1\cdot 2} & 1-\zeta_m^{1\cdot 3} & \dots & 1-\zeta_m^{1\cdot n} \\ 1-\zeta_m^{2\cdot 1} & 1-\zeta_m^{2\cdot 2} & 1-\zeta_m^{2\cdot 3} & \dots & 1-\zeta_m^{2\cdot n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1-\zeta_m^{n\cdot 1} & 1-\zeta_m^{n\cdot 2} & 1-\zeta_m^{n\cdot 3} & \dots & 1-\zeta_m^{n\cdot n} \end{pmatrix}. \qquad \square$$

Lemma 2. The Gram matrix of Γ is $\Gamma^\dagger\Gamma = m^{-1}(I+J)$, where $J = \mathbf{1}\mathbf{1}^T$ is the all 1 matrix. This Gram matrix $\Gamma^\dagger\Gamma$ has an eigenvalue 1 with multiplicity 1 and an eigenvalue m^{-1} with multiplicity $n-1$. $\square$

Proof. We note that $\Gamma^\dagger_{jk} = m^{-1}(1-\zeta_m^{-jk})$ and that $\sum_{l=1}^n \zeta^l = -1$ and so on. Thus $\sum_{l=1}^n \zeta^{l(j-k)} = n$ if $k = j$ and -1 if $k \neq j$ (for $1 \leq k, j \leq n$), which yields

$$\begin{aligned} \left(\Gamma^\dagger\Gamma\right)_{jk} &= \sum_{l=1}^n \Gamma^\dagger_{jl}\Gamma_{lk} = \frac{1}{m^2}\sum_{l=1}^n (1-\zeta^{-jl})(1-\zeta^{lk}) \\ &= \frac{1}{m^2}\sum_{l=1}^n 1 - \frac{1}{m^2}\sum_{l=1}^n \zeta^{lk} - \frac{1}{m^2}\sum_{l=1}^n \zeta^{-jl} + \frac{1}{m^2}\sum_{l=1}^n \zeta^{l(k-j)} \\ &= \begin{cases} 2m^{-2}2(n+1) = 2m^{-1} & [k=j] \\ m^{-2}(n+1) = m^{-1} & [k \neq j]. \end{cases}, \end{aligned}$$

so $\Gamma^\dagger\Gamma = m^{-1}(I+J)$. It can then be verified by direct calculation that $\Gamma^\dagger\Gamma$ has an eigenvector $(1,\dots,1)^T$ with eigenvalue 1 and an eigenspace with eigenvalue m^{-1} of dimension $n-1$ spanned by eigenvectors $e_k - e_l$, where e_k and e_l $(k \neq l)$ are standard basis vectors. $\square$

Lemma 3. If T is the conjugate pair matrix, then $\Delta = \Gamma^{-1}T$ is a real invertible change of basis matrix from the T-basis to the Γ-basis of H. The matrix $\Delta\Delta^T = mI - J$ has an eigenvalue m with multiplicity $n-1$ and an eigenvalue 1 with multiplicity 1. $\square$

Proof. It is clear that $\Delta = \Gamma^{-1}T$ is invertible as both Γ^{-1} and T are invertible. The matrix $\Delta^{-1} = T^{-1}\Gamma = T^\dagger\Gamma$ has matrix entries

$$\Delta^{-1}_{kl} = \begin{cases} 2^{-\frac{1}{2}}\left(\left(1-\zeta_m^{kl}\right)+\left(1-\zeta_m^{-kl}\right)\right) = 2^{\frac{1}{2}}\left(1-\mathrm{Re}\left(\zeta^{kl}\right)\right) & [1 \le k \le n'] \\ 2^{-\frac{1}{2}}\left(-i\left(1-\zeta_m^{-kl}\right)+i\left(1-\zeta_m^{kl}\right)\right) = 2^{\frac{1}{2}}\mathrm{Im}\left(\zeta^{kl}\right) & [n' < k \le n], \end{cases}$$

so Δ^{-1} and hence Δ are real matrices. Thus we have

$$\Delta\Delta^T = \Delta\Delta^\dagger = (\Gamma^{-1}T)(\Gamma^{-1}T)^\dagger = \Gamma^{-1}TT^\dagger(\Gamma^{-1})^\dagger = \left(\Gamma^\dagger\Gamma\right)^{-1} = mI - J,$$

which can be verified by direct calculation as Lemma 2 shows $\Gamma^\dagger\Gamma = m^{-1}(I+J)$. Furthermore, it can also be verified by direct calculation that $\Delta\Delta^T = mI - J$ has an eigenvector $(1,\ldots,1)^T$ with eigenvalue 1 and an eigenspace with eigenvalue m of dimension $n-1$ spanned by eigenvectors $e_k - e_l$, where e_k and e_l $(k \neq l)$ are standard basis vectors. Similarly, the eigenspace results can then be verified by direct calculation. □

Definition 14. The *decoding conjugate basis* $\sigma(\overrightarrow{d})$ or Γ'-basis for H is the basis given by the columns of the matrix Γ', where

$$\Gamma' = \frac{1}{m}\begin{pmatrix} \zeta_m^{0\cdot 1} - \zeta_m^{n\cdot 1} & \zeta_m^{0\cdot 2} - \zeta_m^{n\cdot 2} & \cdots & \zeta_m^{0\cdot n} - \zeta_m^{n\cdot n} \\ \zeta_m^{1\cdot 1} - \zeta_m^{n\cdot 1} & \zeta_m^{1\cdot 2} - \zeta_m^{n\cdot 2} & \cdots & \zeta_m^{1\cdot n} - \zeta_m^{n\cdot n} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta_m^{(n-1)\cdot 1} - \zeta_m^{n\cdot 1} & \zeta_m^{(n-1)\cdot 2} - \zeta_m^{n\cdot 2} & \cdots & \zeta_m^{(n-1)\cdot n} - \zeta_m^{n\cdot n} \end{pmatrix}. \qquad \square$$

Lemma 4. The Gram matrix $\Gamma'^\dagger\Gamma'$ of Γ has an eigenvalue 1 with multiplicity 1 and an eigenvalue m^{-1} with multiplicity $n-1$. □

Proof. We first note the determinant identity $\det(\theta I - \Gamma'\Gamma'^\dagger) = \det(\theta I - \Gamma'^\dagger\Gamma')$, so $\Gamma'\Gamma^\dagger$ has the same eigenvalues as the Gram matrix $\Gamma'^\dagger\Gamma'$ of Γ'. We therefore calculate $\Gamma'\Gamma'^\dagger$, in a similar manner to Lemma 2 to obtain

$$\begin{aligned} \left(\Gamma'\Gamma'^\dagger\right)_{jk} &= \sum_{l=1}^n \Gamma'_{jl}\Gamma'^\dagger_{lk} = \frac{1}{m^2}\sum_{l=1}^n (\zeta^{(j-1)l} - \zeta_m^{nl})(\zeta^{-l(k-1)} - \zeta_m^{-nl}) \\ &= \frac{1}{m^2}\sum_{l=1}^n \zeta^{(j-k)l} - \frac{1}{m^2}\sum_{l=1}^n \zeta^{-(m-j)l} - \frac{1}{m^2}\sum_{l=1}^n \zeta^{(m-k)l} + \frac{1}{m^2}\sum_{l=1}^n 1 \\ &= \begin{cases} 2m^{-2}2(n+1) = 2m^{-1} & [k=j] \\ m^{-2}(n+1) = m^{-1} & [k \neq j]. \end{cases} \end{aligned}$$

Thus $\Gamma'\Gamma'^\dagger = m^{-1}(I+J)$, so the eigenvalues of $\Gamma'\Gamma'^\dagger$ and hence of the Gram matrix $\Gamma'^\dagger\Gamma'$ of Γ' are given by Lemma 2 □

The change of basis matrix from the Γ-basis to the Γ'-basis for H is the matrix

$$\Delta' = \Gamma'^{-1}\Gamma = \begin{pmatrix} 0 & 0 & \ldots & 0 & 1 \\ -1 & 0 & \ldots & 0 & 1 \\ 0 & -1 & \ldots & 0 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & -1 & 1 \end{pmatrix}.$$

Basis	I-Basis	T-Basis	$p\Gamma$-Basis	$p\Gamma'$-Basis
Vector or Random Variable	Z	$Z^{\ddagger}$	Z^{*}	Z^{**}
Transformation from the I-Basis	I	$T^{\dagger}$	$p^{-1}\Gamma^{-1}$	$p^{-1}\Gamma'^{-1}$

Fig. 5. Notation for the expression of an element of H as a vector in the various different vector space bases for H.

This change of basis is also illustrated in Figure 4. We also need to consider the change of basis matrix $\Delta'' = \Delta'\Delta = \Gamma'^{-1}\Gamma\Gamma^{-1}T = \Gamma'^{-1}T$ from the T-basis to the Γ'-basis for H. The relevant properties of this change of basis matrix Δ'' are given in Lemma 5.

Lemma 5. Suppose $\Delta'' = \Delta'\Delta = \Gamma'^{-1}T$. If $E = e_1 e_1^T$ denotes a matrix with a single 1, then $\Delta''\Delta''^T = m(I+J) - (m+1)E$. Furthermore, $\Delta''\Delta''^T$ has an eigenvalue that is approximately m^2 for large m with multiplicity 1, an eigenvalue m of multiplicity $n-2$ and an eigenvalue that is approximately m^{-1} for large m with multiplicity 1. □

Proof. Lemma 3 shows that $\Delta\Delta^T = mI - J$, so

$$\begin{aligned}\Delta''\Delta''^T &= \Delta'\Delta(\Delta'\Delta)^T = \Delta'\Delta\Delta^T\Delta'^T = \Delta'(mI-J)\Delta'^T = m\Delta'\Delta'^T - \Delta' J \Delta'^T \\ &= m(I+J-E) - E = m(I+J) - (m+1)E.\end{aligned}$$

The vector $(\frac{1}{2}m^{-1}(-(m^2-1)+(m^4-2m^2-4m+1)^{\frac{1}{2}}), 1, \ldots, 1)^T$ is an eigenvector of $\Delta''\Delta''^T$ with eigenvalue $\nu = \frac{1}{2}((m^2-1)+(m^4-2m^2-4m+1)^{\frac{1}{2}}) \approx m^2$ for large m. Similarly, the vector $(\frac{1}{2}m^{-1}(-(m^2-1)-(m^4-2m^2-4m+1)^{\frac{1}{2}}), 1, \ldots, 1)^T$ is an eigenvector of $\Delta''\Delta''^T$ with eigenvalue $m\nu^{-1} \approx m^{-1}$ for large m. The remaining eigenvectors lie in an eigenspace with eigenvalue m. This eigenspace is of dimension $n-2$ and is spanned by eigenvectors $e_k - e_l$, where e_k and e_l ($k \neq l$ and $k, l \neq 1$) are standard basis vectors. □

At various times in our discussion of Ring-LWE, we consider the expression of an element of H as a vector with respect to these various different bases for H, though it is convenient for later use in Section 6 to re-scale the Γ-basis and Γ'-basis. We therefore introduce the notation of Figure 5 for the purposes of clarity when dealing with an element of H expressed with respect to the various different bases for H. Thus if Z is a vector expressing an element of H as a vector of conjugate pairs in the I-basis (or standard basis) for H, then we have real vectors $Z^{\ddagger} = T^{\dagger}Z$, $Z^{*} = p^{-1}\Gamma^{-1}Z$ and $Z^{**} = p^{-1}\Gamma'^{-1}Z$ expressing this element as a vector in the T-basis, the $p\Gamma$-basis and the $p\Gamma'$-basis for H respectively.

3 Subgaussian Random Variables

A subgaussian random variable is a random variable that is bounded in some sense by a Normal random variable. The *Toolkit* analysis of Ring-LWE is "based

on *subgaussian* random variables, relaxed slightly as in [23]", and this relaxation gives the δ-subgaussian random variable ($\delta \geq 0$). In this Section, we give a complete and particularly simple characterisation of δ-subgaussian random variables. We can then give a more natural mathematical framework for the analysis of subgaussian random variables. We establish the following main results in this Section which improve or extend existing results.

- Proposition 1 shows that the δ-subgaussian random variables ($\delta \geq 0$) used by the *Toolkit* are simply a translation of 0-subgaussian random variables.
- Theorem 1 gives results for the sum of δ-subgaussian random variables that are far more general than those given by the *Toolkit*.

More generally, our results show that a stated motivation for the use of δ-subgaussian random variables in Ring-LWE, namely that "we need this relaxation when working with discrete Gaussians" [23], is of questionable relevance. For example, we show that a discretised Gaussian random variable with mean 0, usually the situation of interest in cryptographic applications, is a 0-subgaussian random variable.

3.1 An Introduction to Moment Generating Functions

The *Toolkit* analysis of the random variables in Ring-LWE is based on a subgaussian property of random variables. This subgaussian property is defined in terms of the moment generating function [17] of a random variable, and we therefore begin our discussion of subgaussian random variables by defining the moment generating function of a real-valued univariate random variable.

Definition 15. The *moment generating function* M_W of a real-valued univariate random variable W is the function from a subset of $\mathbb{R}$ to $\mathbb{R}$ defined by

$$M_W(t) = \mathbf{E}\left(\exp(tW)\right) \quad \text{for } t \in \mathbb{R} \text{ whenever this expectation exists.} \qquad \square$$

The moment generating function is a basic tool of probability theory, and the fundamental results underlying the utility of the moment generating function are given in Lemma 6 [17].

Lemma 6. If M_W is the moment generating function of a real-valued univariate random variable W, then M_W is a continuous function within its radius of convergence and the k^{th} moment of W is given by $\mathbf{E}(W^k) = M_W^{(k)}(0)$ when the k^{th} derivative of the moment generating function exists at 0. In particular (i) $M_W(0) = 1$, (ii) $\mathbf{E}(W) = M'_W(0)$ and (iii) $\text{Var}(W) = M''_W(0) - M'_W(0)^2$ where these derivatives exist. $\square$

More generally, the statistical properties of a random variable W can be determined from its moment generating function M_W, and in particular from the behaviour of this moment generating function M_W in a neighbourhood of 0 as its Taylor series expansion (where it exists) is given by

$$\begin{aligned} M_W(t) &= 1 + M'_W(0)\, t + \tfrac{1}{2} M''_W(0)\, t^2 + \ldots + \tfrac{1}{k!} M_W^{(k)}(0)\, t^k + \ldots \\ &= 1 + \ \mathbf{E}(W)\, t \ + \tfrac{1}{2}\mathbf{E}(W^2)\, t^2 + \ldots + \ \tfrac{1}{k!}\mathbf{E}(W^k)\, t^k \ + \ldots . \end{aligned}$$

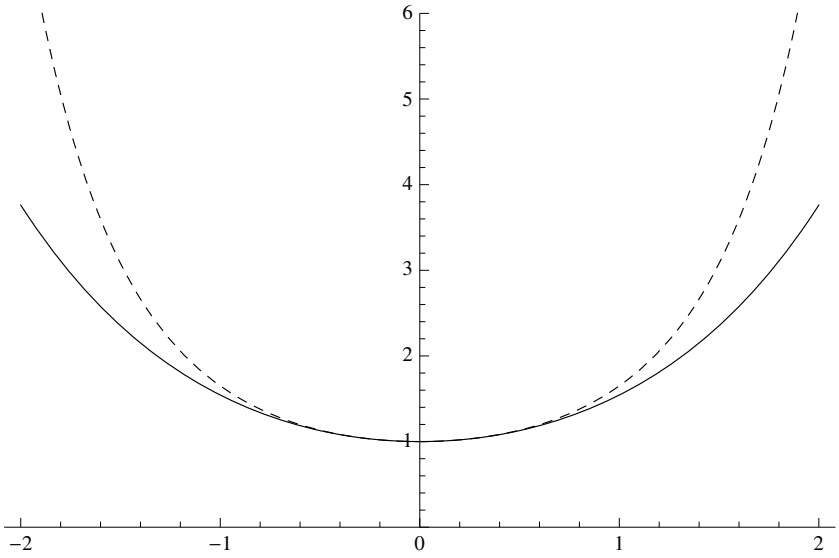

Fig. 6. Moment generating function $M_X(t) = \cosh t$ for the random variable X taking values ± 1 with probability $\frac{1}{2}$ (solid line) and 0-subgaussian bounding function $\exp(\frac{1}{2}t^2)$ (dashed line).

Lemma 7 now gives the standard result [17] for the moment generating function of a Normal random variable with mean 0.

Lemma 7. If $W \sim \mathrm{N}(0, b^2)$ is a Normal random variable with mean 0 and standard deviation $b \geq 0$, then W has moment generating function

$$M_W(t) = \mathbf{E}\left(\exp(tW)\right) = \exp(\tfrac{1}{2}b^2t^2) \qquad \text{for all } t \in \mathbb{R}. \qquad \square$$

3.2 Univariate δ-subgaussian Random Variables

Lemma 7 gives rise to the idea of considering random variables with mean 0 whose moment generating function is dominated everywhere by the moment generating function of an appropriate Normal random variable with mean 0. Such random variables are simply termed "subgaussian" by [32] and 0-subgaussian by the *Toolkit* and by [23]. This idea is illustrated in Figure 6, which shows the moment generating function $M_X(t) = \cosh t$ for the random variable X taking values ± 1 with probability $\frac{1}{2}$ (so $\mathbf{E}(X) = 0$ and $\mathrm{Var}(X) = 1$), together with the corresponding 0-subgaussian bounding function $\exp(\frac{1}{2}t^2)$, which is the moment generating function of a standard Normal $\mathrm{N}(0, 1)$ random variable having the same mean and variance.

We now give the two variants for the definition of a δ-subgaussian random variable, and for completeness (following Lemma 7) we then give the subgaussian status of a univariate Normal random variable in Lemma 8.

Definition 16. A real-valued random variable W is δ-*subgaussian* ($\delta \geq 0$) with *standard parameter* $b \geq 0$ if its moment generating function M_W satisfies

$$M_W(t) = \mathbf{E}(\exp(tW)) \leq \exp(\delta)\exp(\tfrac{1}{2}b^2t^2) \qquad \text{for all } t \in \mathbb{R}. \qquad \square$$

Definition 17. A real-valued random variable W is δ-*subgaussian* ($\delta \geq 0$) with *scaled parameter* $s \geq 0$ if its moment generating function M_W satisfies

$$M_W(2\pi t) = \mathbf{E}(\exp(2\pi tW)) \leq \exp(\delta)\exp(\pi s^2t^2). \qquad \text{for all } t \in \mathbb{R}. \qquad \square$$

Lemma 8. If $W \sim \mathrm{N}(0, b^2)$, then W is a 0-subgaussian random variable with standard parameter b. $\square$

We generally use standard parameters for δ-subgaussian random variables in our discussion of Ring-LWE as this approach corresponds with the usual probability theory of moment generating functions [17]. However, the subgaussian definition given in the *Toolkit* Section 2.3 is that of a δ-subgaussian random variable with *scaled parameter* (Definition 17), and the discussion of the *Toolkit* is phrased in these terms. The relationship between the standard parameter and scaled parameter for δ-subgaussian random variables is given in Lemma 9, which can be easily used to switch between the two parameters.

Lemma 9. A real-valued univariate random variable is δ-subgaussian with standard parameter b if and only if it is δ-subgaussian with scaled parameter $(2\pi)^{\frac{1}{2}}b$.

3.3 Multivariate δ-subgaussian Random Variables

We extend our discussion of δ-subgaussian random variables to multivariate random variables. We first note that the definition of a moment generating function generalises naturally to multivariate random variables on $\mathbb{R}^l$ by using the inner product $\langle \cdot, \cdot \rangle$ on $\mathbb{R}^l$ [17]. We then extend such the definition of a moment generating function to a random variable on the complex space H.

Definition 18. The *moment generating function* of a multivariate random variable W on $\mathbb{R}^l$ is the function from a subset of $\mathbb{R}^l$ to $\mathbb{R}$ defined by

$$M_W(t) = \mathbf{E}\left(\exp(\langle t, W\rangle\right) = \mathbf{E}\left(\exp\left(t^T W\right)\right) \text{ whenever this expectation exists. } \square$$

Lemma 10 [17] giving the moment generating function of a spherical multivariate Normal random variable enables us to give the natural extension of the univariate definition of a δ-subgaussian random variable to the multivariate case. This gives Definition 19 for a real-valued multivariate δ-subgaussian random variable phrased in terms of the multivariate moment generating function being always dominated by a multiple of the moment generating function of some spherical multivariate normal random variable. Lemmas 11 and 12 then show that Definition 19 is equivalent to that given by the *Toolkit* for a δ-subgaussian multivariate random variable.

Lemma 10. If $W \sim \mathrm{N}(0, b^2 I_l)$ is a spherically symmetric Normal random variable with mean 0 and component standard deviation $b \geq 0$, then W has moment generating function

$$M_W(t) = \mathbf{E}\left(\exp\left(t^T W\right)\right) = \exp(\tfrac{1}{2}b^2|t|^2) \qquad \text{for all } t \in \mathbb{R}^l. \qquad \square$$

Definition 19. A multivariate random variable W on $\mathbb{R}^l$ is *δ-subgaussian* ($\delta \geq 0$) with *standard parameter* $b \geq 0$ if its moment generating function M_W satisfies

$$M_W(t) = \mathbf{E}\left(\exp\left(t^T W\right)\right) \leq \exp(\delta)\exp(\tfrac{1}{2}b^2|t|^2) \qquad \text{for all } t \in \mathbb{R}^l. \qquad \square$$

Lemma 11. The moment generating function M_W of the multivariate random variable W on $\mathbb{R}^l$ satisifies $M_{\hat{t}^T W}(\alpha) = M_W\left(\alpha\hat{t}\,\right)$ for all unit vectors $\hat{t} \in \mathbb{R}^l$ and $\alpha \in \mathbb{R}$ (where this exists). $\square$

Proof. If $\hat{t} \in \mathbb{R}^l$ is a unit vector and $\alpha \in \mathbb{R}$, then the moment generating function $M_{\hat{t}^T W}$ of $\hat{t}^T W$ satisfies

$$M_{\hat{t}^T W}(\alpha) = \mathbf{E}\left(\exp\left(\alpha\left(\hat{t}^T W\right)\right)\right) = \mathbf{E}\left(\exp\left(\left(\alpha\hat{t}\right)^T W\right)\right) = M_W\left(\alpha\hat{t}\,\right). \qquad \square$$

Lemma 12. The *Toolkit* Section 2.3 definition of a δ-subgaussian real-valued multivariate random variable is equivalent to Definition 19. $\square$

Proof. Let W be a real-valued multivariate random variable on $\mathbb{R}^l$ that satisfies the *Toolkit* Section 2.3 definition of a δ-subgaussian real-valued multivariate random variable with standard parameter b. This *Toolkit* definition requires that $\hat{t}^T W$ is a (univariate) δ-subgaussian random variable with standard parameter b for all unit vectors $\hat{t} \in \mathbb{R}^l$. Thus the moment generating function $M_{\hat{t}^T W}$ of $\hat{t}^T W$ satisfies

$$M_{\hat{t}^T W}(\alpha) \leq \exp(\delta)\exp(\tfrac{1}{2}b^2\alpha^2) \qquad \text{for all unit vectors } \hat{t} \in \mathbb{R}^l.$$

Lemma 11 therefore shows that the moment generating function M_W of W is bounded as

$$\begin{aligned} M_W\left(\alpha\hat{t}\right) &\leq \exp(\delta)\exp(\tfrac{1}{2}b^2\alpha^2) \\ &= \exp(\delta)\exp\left(\tfrac{1}{2}b^2\left|\alpha\hat{t}\right|^2\right) \quad \text{for all unit vectors } \hat{t} \in \mathbb{R}^l. \end{aligned}$$

By writing $t = \alpha\hat{t}$, we can therefore show that

$$M_W(t) \leq \exp(\delta)\exp\left(\tfrac{1}{2}b^2|t|^2\right) \quad \text{for all vectors } t \in \mathbb{R}^l.$$

Thus W satisfies the Definition 19 requirements for W to be a δ-subgaussian random variable with standard parameter b. The argument is reversible, so the *Toolkit* Section 2.3 definition of a δ-subgaussian with standard parameter b is equivalent to Definition 19. $\square$

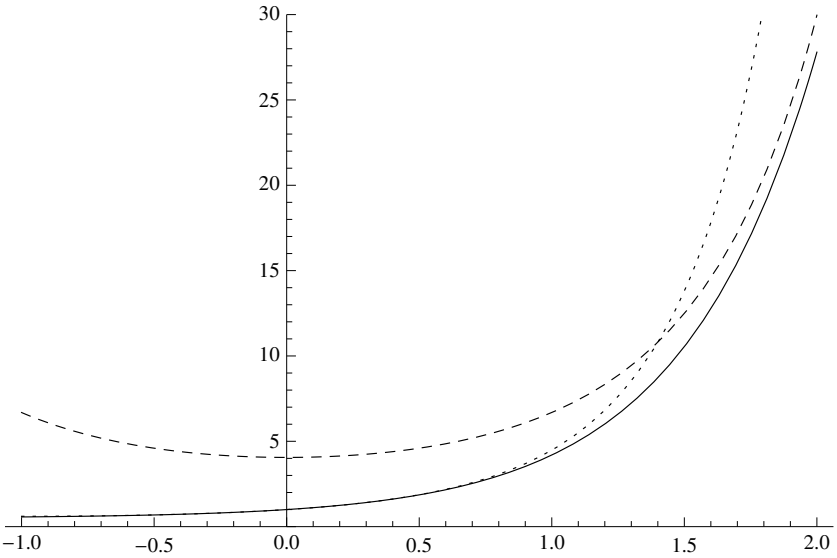

Fig. 7. Moment generating function $M_{X+1}(t) = \frac{1}{2}(1+\exp(2t))$ for the random variable $X+1$ (see Figure 6) taking values 0 and 2 with probability $\frac{1}{2}$ and having mean 1 (solid line), δ-subgaussian bounding function $\exp(\frac{7}{5} + \frac{1}{2}t^2)$ (dashed line), and "noncentral" subgaussian bounding function $\exp(t + \frac{1}{2}t^2)$ (dotted line).

Definition 20. The moment generating function M_Z of a random variable defined on H is a function from a subset of H to $\mathbb{R}$ defined by

$$M_Z(t) = \mathbf{E}\left(\exp(\langle t, Z\rangle)\right) = \mathbf{E}\left(\exp\left(t^\dagger Z\right)\right) \text{ whenever this expectation exists. } \square$$

Definition 21. A multivariate random variable Z on H is *δ-subgaussian* ($\delta \geq 0$) with *standard parameter* $b \geq 0$ if its moment generating function M_Z satisfies

$$M_Z(t) = \mathbf{E}\left(\exp\left(t^\dagger Z\right)\right) \leq \exp(\delta)\exp(\tfrac{1}{2}b^2|t|^2) \qquad \text{for all } t \in H. \qquad \square$$

Lemma 13. The *Toolkit* Section 2.3 definition of a δ-subgaussian multivariate random variable on H is equivalent to Definition 21. $\square$

3.4 Characterisation of Univariate δ-subgaussian Random Variables

We are now able to give a characterisation of a univariate δ-subgaussian random variable. We show that the "relaxation" of the 0-subgaussian condition to give the δ-subgaussian condition for a univariate random variable does not correspond to any relaxation in the fundamental statistical conditions on the random variable except for the location of its mean. Lemma 14 (proved in [32]) first shows that a 0-subgaussian random variable has mean 0, as illustrated in Figure 6, and we now give a heuristic explanation for this result. Lemma 6(i)

shows that any moment generating function must pass through $(0, 1)$. However, a 0-subgaussian bounding function $\exp(\frac{1}{2}b^2t^2)$ has derivative 0 at 0. Thus any moment generating function bound by $\exp(\frac{1}{2}b^2t^2)$ must have derivative 0 at 0. Lemma 6(ii) then shows that such a 0-subgaussian random variable with moment generating function bound by $\exp(\frac{1}{2}b^2t^2)$ must have mean 0.

Lemma 14. If W is a univariate real-valued 0-subgaussian random variable, then $\mathbf{E}(W) = 0$. □

We now give some results to show that the "relaxation" of the 0-subgaussian condition to the δ-subgaussian condition (for $\delta \geq 0$) corresponds exactly to the "relaxation" of the condition that the mean of the random variable is 0. These results are illustrated in Figure 7 for a random variable with mean 1. Relaxing the constraint that $\delta = 0$ in the δ-subgaussian bounding function $\exp(\delta)\exp(\frac{1}{2}b^2t^2)$ essentially shifts the bounding function "up the y-axis", and in particular away from the point $(0, 1)$. However, a moment generating function must pass through the point $(0, 1)$. This relaxation essentially permits us to "tilt" the moment generating function of a 0-subgaussian random variable, pivoting about the point $(0, 1)$, so that the moment generating function has a nonzero derivative at 0. This allows random variables with nonzero mean potentially to be δ-subgaussian random variables.

We now make the intuition described above and illustrated by Figure 7 more precise in a number of ways. Lemma 15 gives the basic result that any δ-subgaussian random variable with mean 0 must be a 0-subgaussian random variable. Lemmas 16 and 17 then give some technical results about shifts of random variables. These results then collectively give Proposition 1, which precisely characterise δ-subgaussian random variables as shifts of 0-subgaussian random variables.

Lemma 15. If W is a univariate real-valued δ-subgaussian random variable ($\delta \geq 0$) with mean $\mathbf{E}(W) = 0$, then W is a 0-subgaussian random variable. □

Proof. The δ-subgaussian bounding function $\exp(\delta)\exp(\frac{1}{2}b^2t^2)$ is bounded above and away from 1 when $\delta > 0$. However, the moment generating function M_W of W is continuous at 0 with $M_W(0) = 1$, so the δ-subgaussian bounding function $\exp(\delta)\exp(\frac{1}{2}b^2t^2)$ is neccesarily always a redundant bounding function for any moment generating function in some open neighbourhood of 0. The proof therefore proceeds by considering the moment generating function M_W of W in two separate regions: an open neighbourhood containing 0 and the region away from this open neighbourhood.

We first consider a region that is some open neighbourhood of 0. Taylor's Theorem (about 0) shows that the moment generating function M_W of W can be expressed in this open neighbourhood of 0 as

$$\begin{aligned} M_W(t) = \mathbf{E}\left(\exp(tW)\right) &= 1 + \mathbf{E}(W)t + \tfrac{1}{2}\mathbf{E}\left(W^2\right)t^2 + o(t^2) \\ &= 1 + \tfrac{1}{2}\mathbf{E}\left(W^2\right)t^2 + o(t^2) \end{aligned}$$

Similarly we can write $\exp(\frac{1}{2}c^2t^2) = 1 + \frac{1}{2}c^2t^2 + o(t^2)$, so we have

$$\frac{M_W(t) - \exp(\frac{1}{2}c^2t^2)}{t^2} = \tfrac{1}{2}\left(\mathbf{E}\left(W^2\right) - c^2\right) + \frac{o(t^2)}{t^2}.$$

Thus for values of c such that $c^2 > \mathbf{E}\left(W^2\right)$ we have

$$\lim_{t\to 0} \frac{M_W(t) - \exp(\frac{1}{2}c^2t^2)}{t^2} = \tfrac{1}{2}\left(\mathbf{E}\left(W^2\right) - c^2\right) < 0,$$

in which case there exists an open neighbourhood $(-\nu, \nu)$ of 0 ($\nu > 0$) such that

$$\frac{M_W(t) - \exp(\frac{1}{2}c^2t^2)}{t^2} < 0$$

in this neighbourhood, so

$$M_W(t) \leq \exp(\tfrac{1}{2}c^2t^2) \quad [|t| < \nu].$$

We now consider the other region away from the open neighbourhood $(-\nu, \nu)$ of 0. If W is δ-subgaussian with standard parameter $b \geq 0$, then its moment generating function satisfies $M_W(t) \leq \exp(\delta)\exp(\frac{1}{2}b^2t^2)$ for all $t \in \mathbb{R}$, and in particular for $|t| \geq \nu$. If we let $d^2 = b^2 + 2\nu^{-2}\delta$, then in this other region the moment generating function M_W of W satisfies

$$\begin{aligned} M_W(t) &\leq \exp(\delta)\exp(\tfrac{1}{2}b^2t^2) \leq \exp(\delta)\exp(\tfrac{1}{2}d^2t^2)\exp(-\delta\nu^{-2}t^2) \\ &\leq \exp(\delta(1-\nu^{-2}t^2))\exp(\tfrac{1}{2}d^2t^2) \leq \exp(\tfrac{1}{2}d^2t^2) \qquad [|t| \geq \nu]. \end{aligned}$$

Taking the two regions together shows that the moment generating function M_W of W satisfies

$$M_W(t) \leq \exp(\ \tfrac{1}{2}\max\{c^2, d^2\}\ t^2\ ) \qquad \text{for all } t \in \mathbb{R}.$$

Thus W is a 0-subgaussian random variable. □

Lemma 16. If W is a univariate real-valued δ-subgaussian random variable ($\delta \geq 0$), then the centred random variable $W_0 = W - \mathbf{E}(W)$ is a 0-subgaussian random variable. □

Proof. If W is a δ-subgaussian random variable with standard parameter b, then its moment generating function M_W satisifies

$$M_W(t) \leq \exp(\delta)\exp(\tfrac{1}{2}b^2t^2) \qquad \text{for all } t \in \mathbb{R}.$$

The centred random variable $W_0 = W - \mathbf{E}(W)$ with mean $\mathbf{E}(W_0) = 0$ has moment generating function M_{W_0} given by

$$\begin{aligned} M_{W_0}(t) &= \mathbf{E}\left(\exp(tW_0)\right) = \mathbf{E}\left(\exp(t(W - \mathbf{E}(W)))\right) \\ &= \exp(-\mathbf{E}(W)t)\ \mathbf{E}\left(\exp(tW)\right) \\ &= \exp(-\mathbf{E}(W)t)\ M_W(t). \end{aligned}$$

The required result can be obtained by noting that for $c > b > 0$, the inequality

$$\left(\delta + \left(\tfrac{1}{2}b^2t^2 - \mathbf{E}(W)t\right)\right) \;\leq\; \left(\left(\delta + \frac{1}{2}\frac{\mathbf{E}(W)^2}{c^2-b^2}\right) + \tfrac{1}{2}c^2t^2\right)$$

holds, which can be demonstrated as

$$\left(\left(\delta + \frac{1}{2}\frac{\mathbf{E}(W)^2}{c^2-b^2}\right) + \tfrac{1}{2}c^2t^2\right) - \left(\delta + \left(\tfrac{1}{2}b^2t^2 - \mathbf{E}(W)t\right)\right) = \frac{c^2-b^2}{2}\left(t + \frac{\mathbf{E}(W)}{c^2-b^2}\right)^2$$

is non-negative for $c > b > 0$. This inequality means that the moment generating function M_{W_0} of W_0 satisfies

$$\begin{aligned} M_{W_0}(t) &= \exp(-\mathbf{E}(W)t)\; M_W(t) \\ &\leq \exp(-\mathbf{E}(W)t)\exp(\delta)\exp(\tfrac{1}{2}b^2t^2) \\ &\leq \exp\left(\delta + (\tfrac{1}{2}b^2t^2 - \mathbf{E}(W)t)\right) \\ &\leq \exp\left(\delta + \frac{1}{2}\frac{\mathbf{E}(W)^2}{c^2-b^2}\right)\exp(\tfrac{1}{2}c^2t^2). \end{aligned}$$

Thus W_0 is a $\left(\delta + \frac{1}{2}\frac{\mathbf{E}(W)^2}{c^2-b^2}\right)$-subgaussian random variable. As W_0 has mean $\mathbf{E}(W_0) = 0$, Lemma 15 therefore shows that $W_0 = W - \mathbf{E}(W)$ is a 0-subgaussian random variable. □

Lemma 17. If W_0 is a univariate real-valued δ_0-subgaussian random variable with mean 0, then the shifted random variable $W = W_0 + d$ is a δ-subgaussian random variable for some $\delta \geq 0$. □

Proof. If W_0 is a δ_0-subgaussian random variable with mean 0, then Lemma 15 shows that W_0 is a 0-subgaussian random variable with some standard parameter $c \geq 0$. The moment generating function M_{W_0} of W_0 is therefore bounded as $M_{W_0}(t) \leq \exp(\frac{1}{2}c^2t^2)$. If $b > c \geq 0$ and $\delta \geq \dfrac{d^2}{2(b^2-c^2)}$, then we note that

$$(\tfrac{1}{2}b^2t^2 + \delta) - (\tfrac{1}{2}c^2t^2 + dt) = \frac{(b^2-c^2)}{2}\left(t - \frac{d}{b^2-c^2}\right)^2 + \delta - \frac{d^2}{2(b^2-c^2)} \geq 0.$$

In this case, the moment generating function M_W of $W = W_0 + d$ satisfies

$$M_W(t) = \exp(dt)M_{W_0}(t) \leq \exp(\tfrac{1}{2}c^2t^2 + dt) \leq \exp(\delta)\exp(\tfrac{1}{2}b^2t^2).$$

Thus $W = W_0 + d$ is δ-subgaussian with standard parameter b. □

Proposition 1. A real-valued univariate δ-subgaussian random variable can essentially be described in terms of a 0-subgaussian random variable (which must have mean 0) as:

$$\delta\text{-}\textit{subgaussian univariate RV} \;=\; 0\text{-}\textit{subgaussian univariate RV} + \textit{constant}. \qquad \square$$

Proposition 1 characterises δ-subgaussian random variables in a simple manner in terms of 0-subgaussian random variables, which must have mean 0. A thorough discussion of the properties of 0-subgaussian random variables is given by [32], where such a 0-subgaussian random variable is simply termed "subgaussian". We give the corresponding results for δ-subgaussian random variables in Lemmas 18-21, and we note that Lemma 20 is proved in [33].

Lemma 18. Suppose that W is a univariate real-valued δ-subgaussian random variable ($\delta \geq 0$) with standard parameter $b \geq 0$. Such a random variable W satisfies: (a) $\mathrm{Var}(W) \leq b^2$, (b) $\mathbf{P}\left(|W - \mathbf{E}(W)| > \alpha\right) \leq 2\exp\left(-\frac{1}{2}b^{-2}\alpha^2\right)$ and (c) $\mathbf{E}\left(\exp(a(W - \mathbf{E}(W))^2)\right) \leq 2$ for some $a > 0$. □

Lemma 19. The set of δ-subgaussian random variables form a linear space. □

Lemma 20. If W is a univariate real-valued bounded random variable with mean $\mathbf{E}(W) = 0$ and $|W| \leq b$, then W is a 0-subgaussian random variable with standard parameter b. □

Lemma 21. If W is a bounded univariate real-valued random variable, then W is a δ-subgaussian random variable for some $\delta \geq 0$. □

Proof. If W is a bounded random variable, then $W_0 = W - \mathbf{E}(W)$ is a bounded random variable with mean 0. Lemma 20 therefore shows that W_0 is a 0-subgaussian random variable, and so Lemma 17 shows that $W = W_0 + \mathbf{E}(W)$ is a δ-subgaussian random variable for some $\delta \geq 0$. □

3.5 Noncentral Subgaussian Random Variables

We have established that the class of δ-subgaussian random variables are precisely those random variables that can be obtained as shifts of 0-subgaussian random variables. This property allows us to define a δ-subgaussian random variable in an alternative way as a *noncentral subgaussian* random variable with an alternative parameterisation in Definition 22. The equivalence between these two definitions is established in Lemma 22, and Lemma 23 then follows.

Definition 22. A random variable Z (on $\mathbb{R}^l$ or H) is a *noncentral subgaussian* random variable with *noncentrality parameter* $|\mathbf{E}(Z)| \geq 0$ and *deviation parameter* $d \geq 0$ if the centred random variable $Z_0 = Z - \mathbf{E}(Z)$ is a 0-subgaussian random variable with standard parameter d. □

Lemma 22. A noncentral subgaussian random variable Z (on $\mathbb{R}^l$ or H) is a δ-subgaussian random variable and vice versa. □

Proof. The equivalence between noncentral subgaussian random variables and δ-subgaussian random variables follows from Proposition 1. □

Lemma 23. The set of noncentral subgaussian random variables (on $\mathbb{R}^l$ or H) (equivalently the set of δ-subgaussian random variables) is a linear space. □

Figure 7 illustrates such a "noncentral" subgaussian bounding function that arises from Definition 22. It can be seen that this noncentral subgaussian bounding function is a tight bounding function to the moment generating function at 0, unlike any possible δ-subgaussian bounding function for $\delta > 0$. Thus Definition 22 is a natural characterisation of shifted 0-subgaussian random variables, not least because the noncentral subgaussian bounding function is actually a moment generating function of some Normal random variable. By contrast, the δ-subgaussian bounding function is not a moment generating function of any random variable when $\delta > 0$.

We now give an equivalent specification for a noncentral subgaussian random variable in Lemma 24. The parameterisation of Lemma 24 allows us to directly compare such a random variable with the corresponding Normal random variable. It is also clear that the deviation parameter of a noncentral subgaussian random variable is invariant under translation of the random variable, so mirroring this fundamental property of standard deviation. By contrast, Example 1 shows that the parameterisation of such a random variable in the manner of Definition 16 using δ and the standard parameter does not give a standard parameter that is invariant under translation. However, Lemma 25 then gives a partial relationship between the δ-subgaussian definition and noncentral subgaussian definition for a random variable.

Lemma 24. If Z is a noncentral subgaussian random variable (on $\mathbb{R}^l$ or H) with noncentrality parameter $|\mathbf{E}(Z)|$ and deviation parameter d, then its moment generating function M_Z is bounded as

$$M_Z(t) \leq \exp\left(\langle t, \mathbf{E}(Z)\rangle\right) \exp(\tfrac{1}{2}d^2|t|^2). \qquad \square$$

Proof. By Definition 22, $Z_0 = Z - \mathbf{E}(Z)$ has moment generating function M_{Z_0} bounded as $M_{Z_0}(t) = \exp(-\langle t, \mathbf{E}(Z)\rangle)M_Z(t) \leq \exp(\frac{1}{2}d^2|t|^2)$. $\square$

Example 1. Suppose that $W \sim \mathrm{N}(0, \sigma^2)$ is a Normal random variable with mean 0 and variance σ^2, so has moment generating function $M_W(t) = \exp(\frac{1}{2}\sigma^2 t^2)$. In terms of Definiton 22, it is clear that W is a noncentral subgaussian random variable with noncentrality parameter 0 and deviation parameter σ. Similarly, the translated random variable $W + a \sim \mathrm{N}(a, \sigma^2)$ is by definition a noncentral random variable with noncentrality parameter $|a|$ and deviation parameter b.

In terms of Definition 16, W is a 0-subgaussian random variable with standard parameter σ. If $W + a$ is a δ-subgaussian random variable with the same standard parameter σ, then $M_{W+a}(t) = \exp(\frac{1}{2}\sigma t^2 + at) \leq \exp(\delta + \frac{1}{2}\sigma^2 t^2)$ so $at \leq \delta$ for all t, which is impossible for $a \neq 0$. Thus even though $W + a$ is a Normal random variable with standard deviation σ, it is not a δ-subgaussian random variable with standard parameter σ when $a \neq 0$. $\square$

Lemma 25. Suppose that Z is a noncentral subgaussian random variable with noncentrality parameter $|\mathbf{E}(Z)|$ and deviation parameter d. If $\mathbf{E}(Z) = 0$, then Z is a 0-subgaussian random variable with standard parameter d. If $|\mathbf{E}(Z)| > 0$, then Z is a δ-subgaussian random variable with standard parameter b whenever (i) $b > d$ and (ii) $\delta \geq \frac{1}{2}|\mathbf{E}(Z)|^2(b^2 - d^2)^{-1}$. $\square$

Proof. If Z is a noncentral subgaussian random variable with noncentrality parameter $|\mathbf{E}(Z)|$ and deviation parameter d, then the moment generating function M_Z of Z satisfies $M_Z(t) \leq \exp\left(\langle E(Z), t\rangle + \frac{1}{2}d^2t^2\right)$. The first case when $\mathbf{E}(Z) = 0$ follows immediately. The conditions for the other case when $|\mathbf{E}(Z)| > 0$ yields the inequality

$$\begin{aligned}\left(\delta + \tfrac{1}{2}b^2|t|^2\right) - \left(\langle E(Z), t\rangle + \tfrac{1}{2}d^2|t|^2\right) &= \tfrac{1}{2}(b^2 - d^2)|t|^2 - \langle \mathbf{E}(Z), t\rangle + \delta \\ &= \frac{b^2 - d^2}{2}\left|t - \frac{\mathbf{E}(Z)}{(b^2 - d^2)}\right|^2 + \delta - \frac{1}{2}\frac{|\mathbf{E}(Z)|^2}{b^2 - d^2} \\ &\geq \delta - \tfrac{1}{2}|\mathbf{E}(Z)|^2(b^2 - d^2)^{-1} \geq 0.\end{aligned}$$

Thus the moment generating function M_Z of Z satisfies

$$M_Z(t) \leq \exp(\langle \mathbf{E}(Z), t\rangle + \tfrac{1}{2}d^2t^2) \leq \exp(\delta)\exp(\tfrac{1}{2}b^2|t|^2),$$

and so Z is a δ-subgaussian random variable with standard parameter b. □

We have shown that the δ-subgaussian property (Definitions 16, 19 and 21) and the noncentral subgaussian property (Definition 22) for a random variable are equivalent. However, the δ-subgaussian definition is problematic for a number of reasons. In addition to the invariance issue highlighted in Example 1, the moment generating function bound $M_W(t) \leq \exp(\mathbf{E}(W)t + \frac{1}{2}d^2t^2)$ of Lemma 24 for a noncentral subgaussian random variable W actually touches the moment generating function M_W at 0, as illustrated in Figure 7. The discussion of Section 3.1 shows that the behaviour of the moment generating function M_W of a random variable W in the vicinity of 0 is of fundamental importance to the properties of the random variable W. Thus the noncentral subgaussian moment generating function bound of Lemma 24 is of immediate relevance to such properties. By contrast, the moment generating function bound $M_W(t) \leq \exp(\delta + \frac{1}{2}b^2t^2)$ of Definition 16 for a δ-subgaussian random variable W is remote from the moment generating function M_W at 0 (for $\delta > 0$), and so is not so immediately relevant.

In summary, the noncentral subgaussian definition is more mathematically and statistically natural for shifts of 0-subgaussian random variables than the δ-subgaussian definition and is therefore to be preferred. The fundamental issue with the δ-subgaussian definition is that its bounding function $\exp(\delta + \frac{1}{2}b^2t^2)$ is not actually a moment generating function of any random variable when $\delta > 0$.

3.6 Sums of Univariate δ_i-subgaussian Random Variables

The analysis of Ring-LWE given by the *Toolkit* relies heavily on the properties of sums of univariate δ-subgaussian or equivalently noncentral subgaussian random variables. However, the results given by the *Toolkit* for such sums of δ-subgaussian random variables are either for independent random variables (such as *Toolkit* Claim 8.6) or are based on the highly restrictive "martingale-like" setting of *Toolkit* Claim 2.1. The *Toolkit* results for the sums of δ-subgaussian random variables are therefore narrowly defined and do not describe all situations of interest in Ring-LWE.

Theorem 1 gives a result for sums of noncentral subgaussian random variables, and gives the result of Lemma 26 about the sum of δ_i-subgaussian random variables. Thus Theorem 1 extends results for the sum of δ_i-subgaussian (or equivalently noncentral subgaussian) random variables from the very narrow conditions of the *Toolkit* (see for example the preamble to *Toolkit* Claim 2.1) to the general setting.

Theorem 1. Suppose that $W_1, \ldots, W_l$ are noncentral subgaussian random variables where W_j has deviation parameter $d_j \geq 0$ for $j = 1, \ldots, l$.

- The sum $\sum_{j=1}^{l} W_j$ is a noncentral subgaussian random variable with noncentrality parameter $\left|\sum_{j=1}^{l} \mathbf{E}(W_j)\right|$ and deviation parameter $\sum_{j=1}^{l} d_j$.
- If $W_1, \ldots, W_l$ are independent, then the deviation parameter of the sum $\sum_{j=1}^{l} W_j$ can be improved to $\left(\sum_{j=1}^{l} d_j^2\right)^{\frac{1}{2}}$. □

Proof. If W_j is a noncentral subgaussian random variable with deviation parameter $d_j \geq 0$, then $W'_j = W_j - \mathbf{E}(W_j)$ is a 0-subgaussian random variable with standard parameter d_j. Theorem 2.7 of [32] therefore shows that $\sum_{j=1}^{l} W'_j = \sum_{j=1}^{l} W_j - \sum_{j=1}^{l} \mathbf{E}(W_j)$ is a 0-subgaussian random variable with standard parameter $\sum_{j=1}^{l} d_j$. Thus $\sum_{j=1}^{l} W_j$ is a noncentral subgaussian random variable with noncentrality parameter $\left|\sum_{j=1}^{l} \mathbf{E}(W_j)\right|$ and deviation parameter $\sum_{j=1}^{l} d_j$. The second (independence) result similarly follows from the independence result of Theorem 2.7 of [32]. □

Lemma 26. Suppose that W_j is a δ_j-subgaussian random variable for some $\delta_j \geq 0$ where $j = 1, \ldots, l$, then their sum $\sum_{j=1}^{l} W_j$ is a δ-subgaussian random variable for some $\delta \geq 0$. □

Proof. Lemma 22 shows that $W_1, \ldots, W_l$ are noncentral subgaussian random variables. Thus Theorem 1 shows that $\sum_{j=1}^{l} W_j$ is a noncentral subgaussian random variable, and Lemma 22 then shows that $\sum_{j=1}^{l} W_j$ is a δ-subgaussian random variable for some $\delta \geq 0$. □

3.7 The $\odot$-product of δ-subgaussian Random Variables

We conclude this Section with a cautionary example about properties of products of δ-subgaussian random variables. The final part of Example 2 considers two random variables on H whose expression as vectors Z_1 and Z_2 in the I-basis for H are δ-subgaussian random variables. This example shows that even when $Z_1 \odot Z_2$ is δ-subgaussian, the (standard) parameter of $Z_1 \odot Z_2$ can essentially be entirely unrelated to the δ-subgaussian standard parameters of Z_1 and Z_2.

Example 2. Suppose that the independent real random variables W_1 and W_2 defined for some $a > 1$ by $W_j = a - 1$ with probability $\frac{1}{2}$ and $W_j = a + 1$ with

probability $\frac{1}{2}$ $(j = 1, 2)$. These random variables have mean $\mathbf{E}(W_j) = a$, with $\mathbf{E}(W_j^2) = a^2 + 1$ and so $\mathrm{Var}(W_j) = 1$. The proof of Lemma 17 and the bound $\cosh z \leq \exp(\frac{1}{2}z^2)$ (given for example in [32]) show that we can express and bound the moment generating function M_{W_j} of W_j as

$$\begin{aligned} M_{W_j}(t) = \mathbf{E}(\exp(tW_j)) &= \tfrac{1}{2}\exp((a-1)t) + \tfrac{1}{2}\exp((a+1)t) = \exp(at)\cosh(t) \\ &\leq \exp(at + \tfrac{1}{2}t^2) \leq \exp(\delta + \tfrac{1}{2}b^2t^2), \end{aligned}$$

whenever $b^2 > 1$ and $\delta \geq \frac{1}{2}a^2(b^2-1)^{-1}$. Thus for any $b > 1$, where W_1 and W_2 have standard deviation 1, we can find $\delta > 0$ such that W_1 and W_2 are independent δ-subgaussian random variables with standard parameter b.

The product random variable W_1W_2, which takes the values $(a-1)^2$ and $(a+1)^2$ with probability $\frac{1}{4}$ and $(a-1)(a+1)$ with probability $\frac{1}{2}$. Thus W_1W_2 has mean $\mathbf{E}(W_1W_2) = a^2$ and variance $\mathrm{Var}(W_1W_2) = 2a^2 + 1$. The random variable $W_1W_2 - a^2$ is therefore a bounded variable with mean 0 and variance $2a^2+1$. Thus Lemmas 20 and 21 show that $W_1W_2 - a^2$ is a 0-subgaussian random variable, and Lemma 18 shows that the standard parameter of $W_1W_2 - a^2$ is bounded below by the standard deviation. Thus $W_1W_2 - a^2$ is 0-subgaussian with standard parameter at least $(2a^2+1)^{\frac{1}{2}} > 2^{\frac{1}{2}}a$. Lemma 17 therefore shows that W_1W_2 is a δ'-subgaussian random variable for some $\delta' > 0$ with standard parameter exceeding $2^{\frac{1}{2}}a$.

We now suppose that $W_{11}, \ldots, W_{1n'}, W_{21}, \ldots, W_{2n'}$ are independent real random variables taking the value $a-1$ with probability $\frac{1}{2}$ and $a+1$ with probability $\frac{1}{2}$ (where $a > 1$). We can define the random variables Z_1 and Z_2 on H expressed as vectors in the I-basis as

$$Z_1 = 2^{-\frac{1}{2}} \begin{pmatrix} W_{11} \\ W_{11} \\ \vdots \\ W_{1n'} \\ W_{1n'} \end{pmatrix} = T \begin{pmatrix} W_{11} \\ 0 \\ \vdots \\ W_{1n'} \\ 0 \end{pmatrix} \quad \text{and} \quad Z_2 = 2^{-\frac{1}{2}} \begin{pmatrix} W_{21} \\ W_{21} \\ \vdots \\ W_{2n'} \\ W_{2n'} \end{pmatrix} = T \begin{pmatrix} W_{21} \\ 0 \\ \vdots \\ W_{2n'} \\ 0 \end{pmatrix}.$$

The above analysis shows that Z_1 and Z_2 are δ-subgaussian random variables with standard parameter $1 + \epsilon$ for any $\epsilon > 0$ and consequent $\delta > 0$. The $\odot$-product of the random variables Z_1 and Z_2 in H is then expressed as a vector in the I-basis for H as

$$Z_1 \odot Z_2 = \frac{1}{2} \begin{pmatrix} W_{11}W_{12} \\ W_{11}W_{12} \\ \vdots \\ W_{1n'}W_{2n'} \\ W_{1n'}W_{2n'} \end{pmatrix}.$$

Applying the above analysis, we can see that $Z_1 \odot Z_2$ is a δ'-subgaussian random variable for some $\delta' > 0$ with standard parameter at least a.

In summary, we have constructed independent random variables Z_1 and Z_2 on H that (expressed in the I-basis) are δ-subgaussian with standard parameter

arbitrarily close to 1. Their product in H (expressed in the I-basis) is a δ-subgaussian random variable with a standard parameter bounded below by the arbitrary value $a > 1$. Thus the standard parameter of the product $Z_1 \odot Z_2$ can be arbitrarily large depending on the value of a chosen, whatever the value of n and n' (including $n' = 1$). □

4 Spherical H-Normal Random Variables

The Ring-LWE error distributions are formally defined over the field tensor product $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$ (see also for example Figures 1 and 8). In particular, we saw that the distributions of most relevance are spherical Gaussians over $K_{\mathbb{R}}$. However, $K_{\mathbb{R}}$ is isomorphic to H [20], so we can equivalently consider spherical Gaussian distributions over H, which we term a Spherical H-Normal distribution. Such a distribution can be described in terms of its H_2-component distributions. Our approach is initially to consider such random variables on H or H_2 as real-valued multivariate vectors expressed in the T-basis, and then use the conjugate pair matrix T to derive the equivalent results in the I-basis for H or H_2. This allows us to derive distributional results for both the Spherical H-Normal random variables and the componentwise product of two independent such Spherical H-Normal random variables. In particular, we give the following main result in this Section relating to the *Toolkit* analysis of homomorphic Ring-LWE.

– Theorem 2 shows that the componentwise product of two independent Spherical H-Normal random variables is not a δ-subgaussian random variable.

4.1 Spherical H-Normal Random Variables

The Spherical H-Normal distribution of Definition 23 is the natural definition for the (conjugate pair) random vector expressing a random variable on H in the I-basis for H to be considered Gaussian as it mirrors the definition of H.

Definition 23. The random variable Z has a *Spherical H-Normal* distribution on H with component variance b^2 if $T^\dagger Z \sim \mathrm{N}(0; b^2 I_n)$ has a spherical Normal distribution on R^n with component variance b^2, where T is the conjugate pair matrix (Definition 7). Such a random variable is denoted $Z \sim N_H(b^2)$. □

We begin this discussion of Spherical H-Normal random variables with two technical Lemmas. Lemmas 27 and 28 shows that an appropriate random variable can essentially have the same moment generating function or density function whether expressed in the I-basis or the T-basis for H. These results allow us to give the basic properties of such a Spherical H-Normal distribution in Lemma 29.

Lemma 27. Suppose W is a random variable on H with moment generating function $M_W(t)$ that is defined on a subset $S \subset H$ and is a function of $|t|$ alone, say $M_W(t) = \Phi_{\mathrm{mgf}}(|t|)$ for an appropriate function Φ_{mgf}. The random variable TW on H then has moment generating function $M_{TW}(t) = \Phi_{\mathrm{mgf}}(|t|)$ defined on a subset $T(S) \subset H$. The converse result is also true. □

Proof. We note that T and hence $T^\dagger$ is a unitary matrix, so

$$\begin{aligned} M_{TW}(t) &= \mathbf{E}\left(\exp\left(t^\dagger TW\right)\right) = \mathbf{E}\left(\exp\left((T^\dagger t)^\dagger W\right)\right) \\ &= M_W(T^\dagger t) = \Phi_{\mathrm{mgf}}(|T^\dagger t|) = \Phi_{\mathrm{mgf}}(|t|), \end{aligned}$$

whenever $T^\dagger t \in S$, that is to say $t \in T(S)$. The converse proof is similar. □

Lemma 28. Suppose W is a random variable on H with density function $f_W(z)$ that is a function of $|z|$ alone, say $f_W(z) = \Phi_{\mathrm{df}}(|z|)$ for an appropriate function Φ_{df}. The random variable TW on H then has density function $f_{TW}(z) = \Phi_{\mathrm{df}}(|z|)$. The converse result is also true. □

Proof. The transformation from W to TW has Jacobian $|\det(T)| = 1$, so TW has density function $f_{TW}(z) = f_W(T^\dagger z) = \Phi_{\mathrm{df}}(|T^\dagger z|) = \Phi_{\mathrm{df}}(|z|)$, as $T^\dagger$ is a unitary matrix. The converse proof is similar. □

Lemma 29. If $Z \sim \mathrm{N}_H(b^2)$ has a Spherical H-Normal distribution, then Z has density function $f_Z(z) = (2\pi b^2)^{-n'} \exp\left(-\frac{1}{2}b^{-2}|z|^2\right)$ on H and moment generating function $M_Z(t) = \exp(\frac{1}{2}b^2|t|^2)$ for all $v \in H$. Thus Z is a 0-subgaussian random variable on H with standard parameter b. □

Proof. If $Z \sim \mathrm{N}_H(b^2)$, then $T^\dagger Z$ has density function $f_{T^\dagger Z}$ given for $w \in \mathbb{R}^n$ by $f_{T^\dagger Z}(w) = (2\pi b^2)^{-\frac{1}{2}n} \exp(-\frac{1}{2}b^{-2}|w|^2)$. Lemma 28 then gives the density function f_Z of Z as $f_Z(z) = (2\pi b^2)^{-\frac{1}{2}n} \exp(-\frac{1}{2}b^{-2}|z|^2)$ for $z \in H$. Similarly, we note that Lemma 10 shows that $T^\dagger Z$ has moment generating function $M_{T^\dagger Z}(t) = \exp(\frac{1}{2}b^2|t|^2)$, so Lemma 27 shows that Z has moment generating function $M_Z(t) = \exp(\frac{1}{2}b^2|t|^2)$ for all t in H. The subgaussian result then follows immediately. □

4.2 Spherical H-Normal Distributions in Various Bases for H

We extend this discussion of Spherical H-Normal random variables by considering the distribution of the real vectors expressing such a random variable in the various bases for H given in Section 2.3. Thus Lemmas 30, 31 and 32 give such distributional results when such a Spherical H-Normal conjugate pair random vector in the I-basis for H is expressed as a real vector in the T-basis, the $p\Gamma$-basis and the $p\Gamma'$-basis respectively. We use the notation of Section 2.3, which is summarised in Figure 5. For later convenience in Section 6, we express the component variance as $p^2\rho^2$ in these results.

Lemma 30. Suppose that $Z \sim N_H(p^2\rho^2)$ is a Spherical H-Normal random variable expressed as a vector in the I-basis for H, and that $Z^\ddagger = T^\dagger Z$ expresses this random variable as a vector in the T-basis for H.
(i) The real vector $Z^\ddagger \sim \mathrm{N}(0; p^2\rho^2 I_n)$.
(ii) $Z^\ddagger$ is a 0-subgaussian random variable with standard parameter $p\rho$.
(iii) A component $Z_j^\ddagger$ of $Z^\ddagger$ is distributed as $Z^\ddagger \sim \mathrm{N}(0, p^2\rho^2)$ for $j = 1, \ldots, n$.
(iv) $Z_j^\ddagger$ is a 0-subgaussian random variable with standard parameter $p\rho$. □

Proof. If $Z \sim N_H(p^2\rho^2)$, then $Z^\ddagger = T^\dagger Z \sim \mathrm{N}(0; p^2\rho^2)$ (by Definition 23). This gives part (i), and parts (ii)-(iv) then follow automatically. □

Lemma 31. Suppose that $Z \sim N_H(p^2\rho^2)$ is a Spherical H-Normal random variable expressed as a vector in the I-basis for H, and that $Z^* = p^{-1}\Gamma^{-1}Z$ expresses this random variable as a vector in the $p\Gamma$-basis for H.
(i) The real vector $Z^* \sim \mathrm{N}(0; \rho^2(mI - J))$, where $J = \mathbf{1}\mathbf{1}^T$ is the all 1 matrix.
(ii) Z^* is a 0-subgaussian random variable with standard parameter $m^{\frac{1}{2}}\rho$.
(iii) A component Z_j^* of Z^* is distributed as $Z_j^* \sim \mathrm{N}(0, n\rho^2)$ for $j = 1, \ldots n$.
(iv) Z_j^* is a 0-subgaussian random variable with standard parameter $n^{\frac{1}{2}}\rho$. □

Proof. The change of basis matrix from the T-basis to the $p\Gamma$-basis for H is given by $p^{-1}\Delta = p^{-1}\Gamma^{-1}T$ (Figure 4). Thus $Z^* = p^{-1}\Gamma^{-1}Z = p^{-1}\Delta Z^\ddagger$ has mean 0. Furthermore, Lemma 3 shows that the covariance matrix of Z^* is $\mathrm{Cov}(Z^*) = p^{-2}\Delta\mathrm{Cov}(Z^\ddagger)\Delta^T = \rho^2\Delta\Delta^T = \rho^2(mI - J)$, so giving part (i). Lemma 3 also immediately gives that maximal eigenvalue of $\mathrm{Cov}(Z^*)$ is $m\rho^2$, so giving part (ii). We note that $\mathrm{Var}(Z_j^*) = \mathrm{Cov}(Z^*)_{jj} = \rho^2(m-1) = n\rho^2$ for $j = 1, \ldots, n$, so giving parts (iii) and (iv). □

Lemma 32. Suppose that $Z \sim N_H(p^2\rho^2)$ is a Spherical H-Normal random variable expressed as a vector in the I-basis for H, and that $Z^{**} = p^{-1}\Gamma'^{-1}Z$ expresses this random variable as a vector in the $p\Gamma'$-basis for H.
(i) The real vector $Z^{**} \sim \mathrm{N}(0; \rho^2(m(I + J) - (m + 1)E))$, where $J = \mathbf{1}\mathbf{1}^T$ is the all 1 matrix and $E = e_1 e_1^T$ is the matrix with a single 1.
(ii) Z^{**} is a 0-subgaussian random variable with standard parameter approximately $m\rho$ for large m.
(iii) The component Z_1^{**} of Z^{**} is distributed as $Z^{**} \sim \mathrm{N}(0, n\rho^2)$. The other components $Z_2^{**}, \ldots, Z_n^{**}$ of Z^{**} are distributed as $Z_j^{**} \sim \mathrm{N}(0, 2m\rho^2)$ for $j = 2, \ldots n$.
(iv) Z_1^{**} is a 0-subgaussian random variable with standard parameter $n^{\frac{1}{2}}\rho$, and $Z_2^{**}, \ldots Z_n^{**}$ are 0-subgaussian random variables with standard parameter $2^{\frac{1}{2}}m^{\frac{1}{2}}\rho$. □

Proof. The change of basis matrix from the T-basis to the $p\Gamma'$-basis for H is given by $p^{-1}\Delta'' = p^{-1}\Delta'\Delta = p^{-1}\Gamma'^{-1}T$ (Figure 4). Thus $Z^{**} = p^{-1}\Gamma'^{-1}Z = p^{-1}\Delta''Z^\ddagger$ has mean 0. Furthermore, Lemma 5 shows that its covariance matrix of Z^* is $\mathrm{Cov}(Z^{**}) = p^{-2}\Delta''\mathrm{Cov}(Z^\ddagger)\Delta''^T = \rho^2\Delta''\Delta''^T = \rho^2(m(I + J) - (m + 1)E)$, so giving part (i). Lemma 5 also shows that maximal eigenvalue of $\mathrm{Cov}(Z^{**})$ is approximately $m^2\rho^2$, so giving part (ii). We note that $\mathrm{Var}(Z_1^{**}) = \mathrm{Cov}(Z^*)_{11} = n\rho^2$ and that $\mathrm{Var}(Z_j^{**}) = \mathrm{Cov}(Z^*)_{jj} = 2m\rho^2$ for $j = 2, \ldots, n$, so giving parts (iii) and (iv). □

4.3 The Covariance Matrix of the ⊗-product of Random Vectors

We begin our discussion of the ⊗-product of vectors expressing random variables in the T-basis for H by specifying the technical Lemmas 33 and 34, which give the mean vector and the covariance matrix for the ⊗-product of general real random vectors.

Lemma 33. Suppose that U and V are real-valued $n = 2n'$-dimensional independent random variables with mean vectors $\mathbf{E}(U) = \mathbf{E}(V) = 0$ and respective diagonal covariance matrices $\beta_U^2 I_n$ and $\beta_V^2 I_n$, then their $\otimes$-product $U \otimes V$ has mean vector $\mathbf{E}(U \otimes V) = 0$ and covariance matrix $\mathrm{Cov}(U \otimes V) = \beta_U^2 \beta_V^2 I_n$.

Proof. As the $\otimes$-product is defined in terms of H_2-components, it suffices to demonstrate the results for $n' = 1$, so $n = 2$. Accordingly, we consider the 2-dimensional real-valued random variable

$$W = \begin{pmatrix} W_1 \\ W_2 \end{pmatrix} = U \otimes V = \begin{pmatrix} U_1 \\ U_2 \end{pmatrix} \otimes \begin{pmatrix} V_1 \\ V_2 \end{pmatrix} = 2^{-\frac{1}{2}} \begin{pmatrix} U_1 V_1 - U_2 V_2 \\ U_1 V_2 + U_2 V_1 \end{pmatrix},$$

where $U = (U_1, U_2)^T$ and $V = (V_1, V_2)^T$ are independent 2-dimensional real-valued random variables with $\mathbf{E}(U) = \mathbf{E}(V) = 0$ and respective covariance matrices $\beta_U^2 I_2$ and $\beta_V^2 I_2$. We first note that $\mathbf{E}(W) = 0$ as

$$\mathbf{E}(W_1) = 2^{-\frac{1}{2}} \mathbf{E}(U_1 V_1 - U_2 V_2) = 2^{-\frac{1}{2}} \mathbf{E}(U_1)\mathbf{E}(V_1) - 2^{-\frac{1}{2}} \mathbf{E}(U_2)\mathbf{E}(V_2) = 0$$

and similarly $\mathbf{E}(W_2) = 0$. Thus the variance of a component W_1 of W is given by

$$\begin{aligned} \mathrm{Var}(W_1) = \mathbf{E}(W_1^2) &= \tfrac{1}{2}\mathbf{E}((U_1 V_1 - U_2 V_2)^2) \\ &= \tfrac{1}{2}\mathbf{E}(U_1^2 V_1^2) + \tfrac{1}{2}\mathbf{E}(U_2^2 V_2^2) - \mathbf{E}(U_1 U_2 V_1 V_2) \\ &= \tfrac{1}{2}\mathbf{E}(U_1^2)\mathbf{E}(V_1^2) + \tfrac{1}{2}\mathbf{E}(U_2^2)\mathbf{E}(V_2^2) - \mathbf{E}(U_1 U_2)\mathbf{E}(V_1 V_2) \\ &= \tfrac{1}{2}\beta_U^2 \beta_V^2 + \tfrac{1}{2}\beta_U^2 \beta_V^2 = \beta_U^2 \beta_V^2, \end{aligned}$$

as U_1 and U_2 are uncorrelated, so $\mathbf{E}(U_1 U_2) = 0$, and so on. We similarly have $\mathrm{Var}(W_2) = \beta_U^2 \beta_V^2$. The covariance of W_1 and W_2 is given by

$$\begin{aligned} \mathrm{Cov}(W_1, W_2) = \mathbf{E}(W_1 W_2) &= \tfrac{1}{2}\mathbf{E}\left((U_1 V_1 - U_2 V_2)(U_1 V_2 + U_2 V_1)\right) \\ &= \tfrac{1}{2}\mathbf{E}(U_1 U_2)\mathbf{E}(V_1^2 - V_2^2) + \tfrac{1}{2}\mathbf{E}(V_1 V_2)\mathbf{E}(U_1^2 - U_2^2) = 0, \end{aligned}$$

again as U_1 and U_2 are uncorrelated and so on. Thus $W = U \otimes V$ has mean vector $\mathbf{E}(U \otimes V) = 0$ and covariance matrix $\mathrm{Cov}(U \otimes V) = \beta_U^2 \beta_V^2 I_2$. □

Lemma 34. Suppose that $U_1, \ldots, U_k$ are real-valued $n = 2n'$-dimensional independent random variables with mean vectors $\mathbf{E}(U_j) = 0$ and diagonal covariance matrices $\beta_j^2 I_n$ $(j = 1, \ldots k)$, then their $\otimes$-product $U_1 \otimes \ldots \otimes U_k$ has mean vector $\mathbf{E}(U_1 \otimes \ldots \otimes U_k) = 0$ and covariance matrix $\mathrm{Cov}(U_1 \otimes \ldots \otimes U_k) = \beta_1^2 \ldots \beta_k^2 I_n$. □

Proof. The result follows inductively from Lemma 33. □

4.4 The $\otimes$-Product of Bivariate Normal Random Variables

The analysis of the $\otimes$-product of bivariate spherical random variables requires us to consider the (central) Laplace distribution of Definition 24. Such a Laplace distribution can thought of as two Exponential distributions sitting back-to-back, and its moment generating function is given in Lemma 35. Thus a Laplace random variable is not a δ-subgaussian random variable. However, Lemmas 36 - 38

give a series of results about the $\otimes$-product of bivariate spherical random variables, including establishing that any projection of this product has a Laplace distribution. Figure 2 illustrates the density function of such a Laplace random variable and also gives the density function of a standard Normal $\mathrm{N}(0,1)$ random variable for comparison. This latter Normal distribution is a heavy-tailed subgaussian distribution with the same mean and variance as the Laplace distribution. The corresponding tail probabilities for these two distributions are then given in Figure 3. These figures illustrate that such a Laplace distribution obtained as an $\otimes$-product of bivariate spherical Normal random variable is fundamentally very different to the corresponding subgaussian distribution.

Definition 24. A random variable W has a (central) *Laplace* distribution with scale parameter $\beta > 0$ if its density function $f_W(w) = (2\beta)^{-1}\exp(-\beta^{-1}|w|)$. Such a random variable is denoted by $W \sim \mathrm{Lap}(\beta)$. □

Lemma 35. If $W \sim \mathrm{Lap}(\beta)$, then $\mathbf{E}(W) = 0$ and $\mathrm{Var}(W) = 2\beta^2$. The moment generating function M_U of U is given by $M_W(t) = (1-\beta^2t^2)^{-1}$ for $|t| < \beta^{-1}$. □

Proof. The mean and variance of W can be verified by direct calculation to be $\mathbf{E}(W) = \displaystyle\int_{-\infty}^{\infty} w f_W(u)\ du = 0$ and $\mathrm{Var}(W) = \displaystyle\int_{-\infty}^{\infty} w^2 f_U(w)\ dw = 2\beta^2$. The moment generating function M_W of W is given for $|t| < \beta^{-1}$ by

$$\begin{aligned}
M_W(t) = \mathbf{E}(\exp(tW)) &= \int_{-\infty}^{\infty} \exp(tw) f_W(w)\ dw \\
&= \frac{1}{2\beta}\int_{-\infty}^{\infty} \exp(tw - \beta^{-1}|w|)\ dw \\
&= \frac{1}{2\beta}\int_{-\infty}^{0} \exp((t+\beta^{-1})w)\ dw + \frac{1}{2\beta}\int_{0}^{\infty} \exp((t-\beta^{-1})w)\ dw \\
&= \frac{1}{2\beta}\int_{0}^{\infty} \exp(-(\beta^{-1}+t)w) + \exp(-(\beta^{-1}-t)w)\ dw \\
&= \frac{1}{2\beta(\beta^{-1}+t)} + \frac{1}{2\beta(\beta^{-1}-t)} = \frac{1}{1-\beta^2t^2}.
\end{aligned}$$

□

Lemma 36. Suppose that $U \sim \mathrm{N}(0, b^2I_2)$ is a bivariate spherical Normal random variable with component variance b^2 and that $\alpha \in \mathbb{R}^2$ is a constant, then the $\otimes$-product $\alpha \otimes U \sim \mathrm{N}(0; \frac{1}{2}b^2|\alpha|^2I_2)$ is a bivariate spherical Normal random variable with component variance $\frac{1}{2}b^2|\alpha|^2$. □

Proof. The $\otimes$-product $\alpha \otimes U = M_\alpha U$, where $M_\alpha = 2^{-\frac{1}{2}}\begin{pmatrix}\alpha_1 & -\alpha_2 \\ \alpha_2 & \alpha_1\end{pmatrix}$. However, $M_\alpha M_\alpha^T = \frac{1}{2}|\alpha|^2I_2$, so we have $\alpha \otimes U = M_\alpha U \sim \mathrm{N}(0; \frac{1}{2}b^2|\alpha|^2I_2)$. □

Lemma 37. Suppose that $U \sim \mathrm{N}(0; b_U^2I_2)$ and $V \sim \mathrm{N}(0; b_V^2I_2)$ are independent spherical bivariate Normal random variables, then $U \otimes V$ has moment generating function $M_{U\otimes V}(t_0) = (1 - \frac{1}{2}b_U^2b_V^2|t_0|^2)^{-1}$ for $|t_0|^2 < 2(b_Ub_V)^{-2}$. Thus $U \otimes V$ is not a δ-subgaussian random variable for any $\delta \geq 0$. □

Proof. We assume without loss of generality that $b_U = b_V = 1$. In this case, Lemma 36 shows that $(U \otimes V | V = v) \sim \mathrm{N}(0; \frac{1}{2}|v|^2 I_2)$, so this conditional random variable has moment generating function

$$\mathbf{E}\left(\exp\left(t_0^T (U \otimes V)\right) \middle| V = v\right) = \exp\left(\tfrac{1}{2}\tfrac{1}{2}|t_0|^2|v|^2\right),$$

which means that the corresponding conditional expectation random variable is given by

$$\mathbf{E}\left(\exp\left(t^T (U \otimes V)\right) \middle| V\right) = \exp\left(\tfrac{1}{2}\tfrac{1}{2}|t_0|^2|V|^2\right).$$

The Law of Total Expectation [17] therefore gives the moment generating function $M_{U\otimes V}$ of $U \otimes V$ as

$$\begin{aligned} M_{U\otimes V}(t_0) &= \mathbf{E}(\exp(t_0^T (U \otimes V)) = \mathbf{E}\left(\mathbf{E}\left(\exp\left(t_0^T (U \otimes V)\right) \middle| V\right)\right) \\ &= \mathbf{E}\left(\exp(\tfrac{1}{4}|t_0|^2|V|^2)\right) = M_{|V|^2}(\tfrac{1}{4}|t_0|^2), \end{aligned}$$

where $M_{|V|^2}$ is the moment generating function of $|V|^2$. However, $|V|^2 \sim \chi_2^2$ has a χ^2 distribution with 2 degrees of freedom as $|V|^2 = V_1^2 + V_2^2$ is the sum of the squares of two independent standard Normal $\mathrm{N}(0,1)$ random variables. Thus $|V|^2$ has moment generating function $M_{|V|^2}(s) = (1-2s)^{-1}$ for $s < \frac{1}{2}$, so the moment generating function $M_{U\otimes V}$ of $U \otimes V$ is given by

$$M_{U\otimes V}(t_0) = (1 - \tfrac{1}{2}|t_0|^2)^{-1} \qquad \left[|t_0|^2 < \tfrac{1}{2}\right].$$

A simple rescaling then gives the required result for the moment generating function $M_{U\otimes V}$ of $U \otimes V$. The subgaussian result then follows as this moment generating function is not defined everywhere. □

Lemma 38. Suppose that $U \sim \mathrm{N}(0; b_U^2 I_2)$ and $V \sim \mathrm{N}(0; b_V^2 I_2)$ are independent spherical bivariate Normal random variables. Any projection of their $\otimes$-product $U \otimes V$ has a Laplace distribution with scale parameter $2^{-\frac{1}{2}} b_U b_V$. In particular, $(U \otimes V)_1, (U \otimes V)_2 \sim \mathrm{Lap}(2^{-\frac{1}{2}} b_U b_V)$ are uncorrelated Laplace random variables with scale parameter $2^{-\frac{1}{2}} b_U b_V$ □

Proof. We can express the $\otimes$-product of U and V as

$$W = \begin{pmatrix} W_1 \\ W_2 \end{pmatrix} = U \otimes V = \begin{pmatrix} U_1 \\ U_2 \end{pmatrix} \otimes \begin{pmatrix} V_1 \\ V_2 \end{pmatrix} = 2^{-\frac{1}{2}} \begin{pmatrix} U_1 V_1 - U_2 V_2 \\ U_1 V_2 + U_2 V_1 \end{pmatrix}.$$

Lemma 37 shows that the projection $W^{(\theta)} = W_1 \cos\theta + W_2 \sin\theta$ of W in the "θ-direction" is a real-valued univariate random variable with moment generating function $M_{W^{(\theta)}}$ given by

$$\begin{aligned} M_{W^{(\theta)}}(s) &= \mathbf{E}\left(\exp(tW^{(\theta)})\right) = \mathbf{E}\left(\exp(s\cos\theta\, W_1 + s\sin\theta\, W_2)\right) \\ &= M_W((s\cos\theta, s\sin\theta)) = (1 - \tfrac{1}{2} b_U^2 b_V^2 |s|^2)^{-1} \end{aligned}$$

for real-valued s with $s^2 < 2(b_U b_V)^{-2}$ This moment generating function $M_{W^{(\theta)}}$ is well-defined in an open neighbourhood of 0 and Lemma 35 shows that it is the moment generating function of a Laplace random variable with scale parameter

$2^{-\frac{1}{2}} b_U b_V$. Thus the projection $W^{(\theta)} \sim \text{Lap}(2^{-\frac{1}{2}} b_U b_V)$ of W in the θ-direction has a Laplace distribution with scale parameter $2^{-\frac{1}{2}} b_U b_V$. Thus in particular the two components (projections along the co-ordinate axes) $(U \otimes V)_1, (U \otimes V)_2 \sim \text{Lap}(2^{-\frac{1}{2}} b_U b_V)$ have a Laplace distribution. Lemma 33 shows that these two components are uncorrelated. □

4.5 The ⊗-Product of Spherical Normal Random Variables

We are now in a position to give results for the ⊗-product of two independent n-dimensional spherical Normal random variables by extending the bivariate results of Section 4.4. We begin in Lemma 39 by giving the moment generating function of such an ⊗-product.

Lemma 39. Suppose that $U \sim \text{N}(0; b_U^2 I_n)$ and $V \sim \text{N}(0; b_V^2 I_n)$ are independent spherical n-dimensional Normal random variables. If $t = (t_1, \ldots, t_{n'})^T \in \mathbb{R}^{2n'}$ expresses t in terms of its n' $\mathbb{R}^2$-components $t_1, \ldots, t_{n'}$, then the ⊗-product $U \otimes V$ has moment generating function $M_{U \otimes V}(t) = \prod_{j=1}^{n'} (1 - \frac{1}{2} b_U^2 b_V^2 |t_j|^2)^{-1}$ for $|t_1|, \ldots, |t_{n'}| < 2^{\frac{1}{2}} (b_U b_V)^{-1}$. □

Proof. This result follows directly from Lemma 37 as the 2-dimensional components (corresponding to the H_2-components) of ⊗-product are independent. □

Lemma 39 shows that the moment generating function of the ⊗-product of two spherical Normal random variables is not spherically symmetric. In particular, the form of this moment generating function shows that a 1-dimensional projection of such an ⊗-product does not in general have a Laplace distribution. However, Lemma 40 gives a partial analogue to Lemma 38 by recovering a Laplace distribution for projections along the co-ordinates axes.

Lemma 40. Suppose that $U \sim \text{N}(0; b_U^2 I_n)$ and $V \sim \text{N}(0; b_V^2 I_n)$ are independent spherical n-dimensional Normal random variables. The components $(U \otimes V)_1, \ldots, (U \otimes V)_n \sim \text{Lap}(2^{-\frac{1}{2}} b_U b_V)$ of the ⊗-product $U \otimes V$ are uncorrelated Laplace random variables with scale parameter $2^{-\frac{1}{2}} b_U b_V$, so these components are not δ-subgaussian. □

Proof. The moment generating function $(1 - \frac{1}{2} b_U^2 b_V^2 |t_j|^2)^{-1}$ of an $\mathbb{R}^2$-component of $U \otimes V$ is of the form considered in Lemma 38. □

Lemma 40 shows that a component of the ⊗-product of two spherical Normal random variables has a Laplace distribution, so such a component is not δ-subgaussian and in fact has an exponential tail. Thus such a product distribution has a far heavier tail than such an approximating subgaussian distribution, as illustrated a particular projection in Figure 3. However, it is essentially the approach of the *Toolkit* to approximate such a component with a Laplace distribution by a heavy-tailed subgaussian random variable, such as the Normal distribution, with the same mean and variance.

4.6 The $\odot$-Product of Spherical H-Normal Random Variables

We can now extend the results of Sections 4.4 and 4.5 directly to (conjugate pair) vectors expressing products in the complex space H in the I-basis. Thus we consider the $\odot$-product of two independent Spherical H-Normal random variables, and we give the moment generating function for such an $\odot$-product in Lemma 41. This allows us to show in Theorem 2 that the $\odot$-product of two independent Spherical H-Normal random variables is not a δ-subgaussian random variable.

Lemma 41. Suppose that $Z_1 \sim \mathrm{N}_H(b_1^2)$ and $Z_1 \sim \mathrm{N}_H(b_2^2)$ are independent Spherical H-Normal random variables (in the I-basis for H). The $\odot$-product $Z_1 \odot Z_2$ has moment generating function $M_{Z_1 \odot Z_2}(t) = \prod_{j=1}^{n'}(1 - \frac{1}{2}b_1^2 b_2^2 |t_j|^2)^{-1}$ for $|t_1|, \ldots, |t_{n'}| < 2^{\frac{1}{2}}(b_1 b_2)^{-1}$, where $v = (t_1, \ldots, t_{n'})^T \in H$ expresses t in terms of its H_2-components $t_1, \ldots, t_{n'}$. □

Proof. If $Z_j \sim \mathrm{N}_H(b_j^2)$, then $T^\dagger Z_j \sim \mathrm{N}(0; b_j^2 I_n)$ for $j = 1, 2$. The moment generating function for $T^\dagger Z_1 \otimes T^\dagger Z_2$ is given in Lemma 39 and for each of the n' independent $\mathbb{R}^2$-components of $T^\dagger Z_1 \otimes T^\dagger Z_2$ in Lemma 37. The independence of Z_1 and Z_2 and the application of Lemma 27 to the identity $Z_1 \odot Z_2 = T(T^\dagger Z_1 \otimes T^\dagger Z_2)$ then gives the required result. □

Theorem 2. The $\odot$-product of two independent Spherical H-Normal random variables (in the I-basis for H) is not a δ-subgaussian random variable. □

Proof. This result immediately follows from Lemma 41, which shows that the moment generating function of such an $\odot$-product is not defined everywhere. □

5 Discretisation

Discretisation is a fundamental part of Ring-LWE. It is a process where a point is "rounded" to a nearby point in a lattice coset. In fact, such a discretisation process usually involves randomisation, so discretisation typically gives rise to a random variable on the elements of the coset. We consider the *coordinate-wise randomised rounding* method of discretisation, which is described in the first bullet point of *Toolkit* Section 2.4.2, as an illustration of a discretisation process, though most of our comments apply more generally. We establish the following two main results in this Section.

- Theorem 3 improves the *Toolkit* results for the variability of the coordinate-wise randomised rounding discretisation process used in Ring-LWE.
- Theorem 4 shows that the componentwise product of the coordinatewise randomised rounding discretisation of two independent Spherical H-Normal random variables is not a δ-subgaussian random variable.

5.1 Coordinate-wise Randomised Rounding Discretisation

The details of the *coordinate-wise randomised rounding* method of discretisation depend on the lattice basis used. One particular property of interest is the *elongation* of a lattice basis matrix of Definition 25, and we give the elongation of the basis matrices for H discussed in Section 2.3 in Lemma 42.

Definition 25. Suppose that the lattice Λ has (column) basis matrix B. The *Gram matrix* of the basis matrix B is $B^\dagger B$, where $B^\dagger = \overline{B}^T$ is the complex conjugate of B. The *elongation* $\lambda(B) > 0$ of the basis matrix B is the square root of largest eigenvalue of the Gram matrix $B^\dagger B$. □

Lemma 42. The lattice basis matrices T, Γ and Γ' of the T-basis, the Γ-basis and the Γ'-basis for H have elongation $\lambda(T) = \lambda(\Gamma) = \lambda(\Gamma') = 1$. □

Proof. The results immediately follow from Lemmas 1, 2 and 4. □

We now give a formal description of the coordinate-wise randomised rounding discretisation method. This description is based on the univariate Reduction random variable of Definition 26. Such a Reduction random variable is a translation of the basic "coin-flip" Bernoulli random variable [17], and so we can give its immediate basic properties in Lemma 43. For the purposes of discussing discretisation, it is convenient to consider the multivariate generalisation of a Reduction random variable given by Definition 27. Lemma 44 then gives a technical result about such a multivariate Reduction random variable that we use later.

Definition 26. If Bern denotes the Bernoulli distribution, then the univariate *Reduction* distribution $\mathrm{Red}(a) = \mathrm{Bern}(\lceil a \rceil - a) - (\lceil a \rceil - a)$ is the discrete probability distribution defined for parameter $a \in \mathbb{R}$ as taking the values

$$\begin{array}{rlll} \text{(i)} & 1 + a - \lceil a \rceil & \text{with probability} & \lceil a \rceil - a \\ \text{and (ii)} & a - \lceil a \rceil & \text{with probability} & 1 - (\lceil a \rceil - a). \end{array}$$ □

Lemma 43. If $R_0 \sim \mathrm{Red}(a)$ is a (univariate) Reduction random variable for parameter $a \in \mathbb{R}$, then R_0 satisifies (i) $|R_0| \leq 1$, (ii) $\mathbf{E}(R_0) = 0$, (iii) $\mathrm{Var}(R_0) \leq \frac{1}{4}$ and (iv) $a - R_0 \in \{\lfloor a \rfloor, \lceil a \rceil\} \subset \mathbb{Z}$. □

Definition 27. A random variable $R = (R_1, \ldots, R_l)^T$ has a multivariate Reduction distribution $R \sim \mathrm{Red}(a)$ on $\mathbb{R}^l$ for parameter $a = (a_1, \ldots, a_l)^T \in \mathbb{R}^l$ if its components $R_j \sim \mathrm{Red}(a_j)$ for $j = 1, \ldots, l$ are independent univariate Reduction random variables. □

Lemma 44. Suppose that the lattice Λ has (column) basis matrix B with elongation $\lambda(B)$ and that R is a Reduction random variable of appropriate dimension, then $|BR|^2 \leq n\lambda(B)^2$ and $\mathbf{E}(|BR|^2) \leq \frac{1}{4}n\lambda(B)^2$. □

Proof. We note that $|R|^2 \leq n$, so

$$|BR|^2 = (BR)^\dagger BR = R^T(B^\dagger B)R \leq \lambda(B)^2|R|^2 \leq n\lambda(B)^2.$$

Furthermore, $\mathbf{E}(|BR|^2) \leq \lambda(B)^2\mathbf{E}(|R|^2) = n\lambda(B)^2\mathbf{E}(R_j^2) = \frac{1}{4}n\lambda(B)^2$. □

We are now able to specify the coordinate-wise randomised rounding discretisation method in a vector form in Definition 28. Lemma 45 then shows that coordinate-wise randomised rounding is well-defined, and Lemma 46 gives some basic properties of this method of discretisation.

Definition 28. Suppose B is a (column) basis matrix for the l-dimensional lattice Λ. The *coordinate-wise randomised rounding discretisation* $\lfloor x \rceil^B_{\Lambda+c}$ of the point x to the lattice coset $\Lambda + c$ with respect to the basis B can then be defined in terms of the multivariate Reduction random variable $Q_{x,c}$ by the random variable

$$\lfloor x \rceil^B_{\Lambda+c} = x + BQ_{x,c}, \qquad \text{where } Q_{x,c} \sim \text{Red}\left(B^{-1}(c-x)\right). \ \square$$

Lemma 45. The coordinate-wise randomised rounding discretisation $\lfloor x \rceil^B_{\Lambda+c}$ is a random variable on the lattice coset $\Lambda + c$ and is *valid* (does not depend on the chosen coset representative c). $\square$

Proof. We can express the Reduction random variable $Q_{x,c} \sim \text{Red}\left(B^{-1}(c-x)\right)$ as $Q_{x,c} = P_{x,c} + \lceil B^{-1}(c-x) \rceil - B^{-1}(c-x)$, where $P_{x,c}$ is a vector of independent Bernoulli random variables. We note that $P_{x,c} + \lceil B^{-1}(c-x) \rceil$ is an integer vector, so the coordinate-wise randomised rounding discretisation $\lfloor x \rceil^B_{\Lambda+c}$ is therefore a random variable on the lattice coset $\Lambda + c$ as

$$\begin{aligned} \lfloor x \rceil^B_{\Lambda+c} &= x + BQ_{x,c} = x + BP_{x,c} + B\lceil B^{-1}(c-x) \rceil - (c-x) \\ &= c + B\left(P_{x,c} + \lceil B^{-1}(c-x) \rceil\right) \\ &\in \Lambda + c. \end{aligned}$$

Furthermore, if $c' \in \Lambda + c$, so $c - c' \in \Lambda$, then there exists an integer vector z such that $c' - c = Bz$, so $B^{-1}(x-c) - B^{-1}(x-c') = z$, that is to say $B^{-1}(x-c)$ and $B^{-1}(x-c')$ differ by an integer vector. Thus $\text{Red}\left(B^{-1}(c-x)\right)$ and $\text{Red}\left(B^{-1}(c-x)\right)$ are identical distributions. The distribution of $\lfloor x \rceil^B_{\Lambda+c}$ on the lattice coset $\Lambda + c$ does not therefore depend on the chosen coset representative c and so the discretisation is *valid*. $\square$

Lemma 46. Suppose that the lattice Λ has (column) basis matrix B with elongation $\lambda(B)$, then the coordinate-wise randomised rounding $\lfloor x \rceil^B_{\Lambda+c}$ of the point x satisfies $\mathbf{E}\left(\lfloor x \rceil^B_{\Lambda+c}\right) = x$ and $\mathbf{E}\left(\left|\lfloor x \rceil^B_{\Lambda+c} - x\right|^2\right) \leq n\lambda(B)^2$. $\square$

Proof. Lemma 43 shows that $\mathbf{E}\left(\lfloor x \rceil^B_{\Lambda+c}\right) = x + \mathbf{E}(BR_{x,c}) = x + B\mathbf{E}(Q_{x,c}) = x$. Lemma 44 shows that $\mathbf{E}\left(\left|\lfloor x \rceil^B_{\Lambda+c} - x\right|^2\right) = \mathbf{E}(|BQ_{x,c}|^2) \leq n\lambda(B)^2$. $\square$

We now consider the coordinate-wise randomised rounding discretisation of a random variable to a lattice in H, when the natural extension of Definition 28 gives Definition 29. Lemma 47 then shows that the mean of a random variable is invariant under such a discretisation. We conclude with Lemma 52 which gives the covariance matrix of a real vector expressing such a discretisation of a random variable expressed in the T-basis for H.

Definition 29. Suppose B is a (column) basis matrix for the n-dimensional lattice Λ in H. The *coordinate-wise randomised rounding discretisation* $\lfloor X \rceil_{\Lambda+c}^{B}$ of the random variable X to the lattice coset $\Lambda + c$ with respect to the basis matrix B is then defined by the conditional random variable

$$\left(\lfloor X \rceil_{\Lambda+c}^{B} \middle| X = x \right) = \lfloor x \rceil_{\Lambda+c}^{B} = x + BQ_{x,c}, \text{ where } Q_{x,c} \sim \text{Red}\left(B^{-1}(c-x)\right). \quad \square$$

Lemma 47. Suppose B is a (column) basis matrix for the n-dimensional lattice Λ in H. The coordinate-wise randomised rounding discretisation $\lfloor X \rceil_{\Lambda+c}^{B}$ of the random variable X to the lattice coset $\Lambda + c$ with respect to the basis matrix B has mean vector $\mathbf{E}\left(\lfloor X \rceil_{\Lambda+c}^{B}\right) = \mathbf{E}(X)$. $\square$

Proof. Lemma 43 shows that the mean of the multivariate Reduction random variable $Q_{x,c} \sim \text{Red}(B^{-1}(c-x))$ is given by $\mathbf{E}(Q_{x,c}) = 0$. Thus we have

$$\mathbf{E}\left(\lfloor X \rceil_{\Lambda+c}^{B} \middle| X = x \right) = x + \mathbf{E}(BQ_{x,c}) = x + B\mathbf{E}(Q_{x,c}) = x,$$

so we obtain the conditional expectation random variable $\mathbf{E}\left(\lfloor X \rceil_{\Lambda+c}^{B} \middle| X \right) = X$. The Law of Total Expectation [17] then gives the required result as

$$\mathbf{E}\left(\lfloor X \rceil_{\Lambda+c}^{B}\right) = \mathbf{E}\left(\mathbf{E}\left(\lfloor X \rceil_{\Lambda+c}^{B} \middle| X \right)\right) = \mathbf{E}(X). \quad \square$$

5.2 Subgaussian Properties of Discretisation Random Variables

We next consider the subgaussian properties of the random variable given by this discretisation process. We give two preliminary results in Lemmas 48 and 49, which lead to Theorem 3. These results allow us to bound the deviation parameter of a random variable obtained by such a discretisation of a point. Lemmas 50 and 51 then extend these results to allow us to bound the deviation parameter of a random variable obtained by such a discretisation of a 0-subgaussian random variable, which is a perturbation of this 0-subgaussian random variable. In particular, Lemma 51 is a multivariate version of the final part of Theorem 1.

The results of this Section typically use a factor of $\frac{1}{2}$ with the standard parameter or deviation parameter of a random variable obtained by discretisation. By contrast, any comparable result of the *Toolkit* uses a factor of 1 (see for example the first bullet point of *Toolkit* Section 2.4.2). Thus the results of this Section improve and extend any comparable result of the *Toolkit* about coordinate-wise randomised rounding discretisation.

Lemma 48. A multivariate Reduction random variable (Definition 27) is a 0-subgaussian random variable with standard parameter $\frac{1}{2}$. $\square$

Proof. We first consider the univariate Reduction random variable $R_j \sim \text{Red}(p)$ (Definition 26) for $0 \leq p \leq 1$ (without loss of generality), so R_j takes the value p with probability $1 - p$ and the value $p - 1$ with probability p. Thus R_j has moment generating function

$$M_{R_j}(t) = \mathbf{E}(\exp(tR_j)) = (1-p)\exp(pt) + p\exp((p-1)t) = \exp(pt)h(t),$$

where $h(t) = (1-p) + p\exp(-t)$. We consider the logarithm of the moment generating function given by the function

$$g(t) = \log M_{R_j}(t) = pt + \log h(t).$$

The first three derivatives of g are given by

$$g'(t) = \frac{p(1-p)(1-\exp(-t))}{h(t)}, \qquad g''(t) = \frac{p(1-p)\exp(-t)}{h(t)^2}$$
$$\text{and } \; g'''(t) = \frac{-p(1-p)\exp(-t)\,((1-p)-p\exp(-t))}{h(t)^3}.$$

We see that $g''(t) \geq 0$ and that solving $g'''(t) = 0$ shows that the maximum of g'' occurs at $t_0 = \log\left(\frac{p}{1-p}\right)$ with a maximum value of $g''(t_0) = \frac{1}{4}$, so $0 \leq g''(t) \leq \frac{1}{4}$ for all $t \in \mathbb{R}$, and we also note that $g(0) = g'(0) = 0$. The Lagrange remainder form of Taylor's Theorem shows that there exists ξ between 0 and t such that $g(t) = \frac{1}{2}g''(\xi)t^2$, so $0 \leq g(t) \leq \frac{1}{8}t^2$. Thus $M_{R_j}(t) = \exp(f(t)) \leq \exp(\frac{1}{2}(\frac{1}{2})^2t^2)$, so R_j is a 0-subgaussian random variable with standard parameter $\frac{1}{2}$.

We now consider the moment generating function M_R of the multivariate Reduction random variable $R = (R_1, \ldots, R_l)^T$, which is given by

$$\begin{aligned} M_R(t) &= \mathbf{E}(\exp(t^T R)) = \mathbf{E}\left(\exp\left(\textstyle\sum_{j=1}^l t_j R_j\right)\right) = \mathbf{E}\left(\prod_{j=1}^l \exp(t_j R_j)\right) \\ &= \prod_{j=1}^{l} \mathbf{E}(\exp(t_j R_j)) = \prod_{j=1}^{l} M_{R_j}(t_j) \\ &\leq \prod_{j=1}^{l} \exp(\tfrac{1}{2}(\tfrac{1}{2})^2 t_j^2) = \exp\left(\tfrac{1}{2}(\tfrac{1}{2})^2 \textstyle\sum_{j=1}^l t_j^2\right) = \exp(\tfrac{1}{2}(\tfrac{1}{2})^2|t|^2). \end{aligned}$$

Thus R is a 0-subgaussian random variable with standard parameter $\frac{1}{2}$. □

Lemma 49. Suppose that B is a (column) basis matrix for a lattice in H with elongation $\lambda(B)$ and that R is a multivariate Reduction random variable (Definition 27) of appropriate dimension. The random variable BR is a 0-subgaussian random variable with standard parameter $\frac{1}{2}\lambda(B)$. □

Proof. As we noted in the proof of Lemma 44, both $BB^\dagger$ and the Gram matrix $B^\dagger B$ are positive definite Hermitian matrices sharing the same eigenvalues. Lemma 48 therefore shows that the moment generating function M_{BR} of BR satisfies

$$\begin{aligned} M_{BR}(v) &= \mathbf{E}(\exp(v^\dagger BT)) = \mathbf{E}\left(\exp\left(\left(B^\dagger v\right)^\dagger R\right)\right) = M_R\left(B^\dagger v\right) \\ &\leq \exp\left(\tfrac{1}{2}(\tfrac{1}{2})^2|B^\dagger v|^2\right) = \exp\left(\tfrac{1}{2}(\tfrac{1}{2})^2\left(v^\dagger BB^\dagger v\right)\right) \\ &\leq \exp\left(\tfrac{1}{2}(\tfrac{1}{2})^2\lambda(B)^2|v|^2\right), \end{aligned}$$

as $\lambda(B)^2 > 0$ is the largest eigenvalue of the Gram matrix $BB^\dagger$. Thus BR is a 0-subgaussian random variable with standard parameter $\frac{1}{2}\lambda(B)$. □

Theorem 3. Suppose that B is a (column) basis matrix for a lattice in H with elongation $\lambda(B)$. The coordinate-wise randomised rounding discretisation of z to $\lfloor z \rceil_{\Gamma+c}^{B}$ is a noncentral subgaussian random variable with noncentrality parameter $|z|$ and deviation parameter $\frac{1}{2}\lambda(B)$. □

Proof. The discretisation $\lfloor z \rceil_{\Gamma+c}^{B} = z + BQ_{z,c}$ of z has moment generating function

$$\begin{aligned} M_{\lfloor z \rceil_{\Gamma+c}^{B}}(v) &= M_{z+BQ_{z,c}}(v) = M_z(v) M_{BQ_{z,c}}(v) \\ &\leq \exp\left(\langle v, z\rangle\right) \exp\left(\tfrac{1}{2}(\tfrac{1}{2})^2 \lambda(B)^2 |v|^2\right), \end{aligned}$$

so $\lfloor z \rceil_{\Gamma+c}^{B}$ is a noncentral subgaussian random variable with noncentrality parameter $|z|$ and standard parameter $\frac{1}{2}\lambda(B)$. □

Lemma 50. Suppose that B is a (column) basis matrix for a lattice in H with elongation $\lambda(B)$ and that Z is an independent noncentral subgaussian random variable with deviation parameter d_Z. The coordinate-wise randomised rounding discretisation of Z to $\lfloor Z \rceil_{\Gamma+c}^{B}$ is a noncentral subgaussian random variable with noncentrality parameter $|\mathbf{E}(Z)|$ and deviation parameter $(d_Z^2 + (\frac{1}{2})^2 \lambda(B)^2)^{\frac{1}{2}}$. □

Proof. Theorem 3 gives a conditional expectation bound of

$$\mathbf{E}\left(\exp\left(v^\dagger \lfloor Z \rceil_{\Gamma+c}^{B}\right) \middle| Z = z\right) \leq \exp\left(\langle v, z\rangle\right) \exp\left(\tfrac{1}{2}(\tfrac{1}{2})^2 \lambda(B)^2 |v|^2\right),$$

so the corresponding conditional expectation random variable is bounded as

$$\mathbf{E}\left(\exp\left(v^\dagger \lfloor Z \rceil_{\Gamma+c}^{B}\right) \middle| Z\right) \leq \exp\left(\langle v, Z\rangle\right) \exp\left(\tfrac{1}{2}(\tfrac{1}{2})^2 \lambda(B)^2 |v|^2\right).$$

The Law of Total Expectation [17] then allows us to bound the moment generating function $M_{\lfloor Z \rceil_{\Gamma+c}^{B}}$ of the discretisation $\lfloor Z \rceil_{\Gamma+c}^{B}$ as

$$\begin{aligned} M_{\lfloor Z \rceil_{\Gamma+c}^{B}}(v) &= \mathbf{E}\left(\exp\left(v^\dagger \lfloor Z \rceil_{\Gamma+c}^{B}\right)\right) = \mathbf{E}\left(\mathbf{E}\left(\exp\left(v^\dagger \lfloor Z \rceil_{\Gamma+c}^{B}\right) \middle| Z\right)\right) \\ &\leq \mathbf{E}\left(\exp\left(\langle v, Z\rangle\right)\right) \exp\left(\tfrac{1}{2}(\tfrac{1}{2})^2 \lambda(B)^2 |v|^2\right) \\ &= M_Z(v) \exp\left(\tfrac{1}{2}(\tfrac{1}{2})^2 \lambda(B)^2 |v|^2\right) \\ &= \exp\left(\langle v, \mathbf{E}(Z)\rangle\right) \exp\left(\tfrac{1}{2}(d_Z^2 + (\tfrac{1}{2})^2 \lambda(B)^2) |v|^2\right). \end{aligned}$$

Thus $\lfloor Z \rceil_{\Gamma+c}^{B}$ is a noncentral subgaussian random variable with noncentrality parameter $|\mathbf{E}(Z)|$ and deviation parameter $(d_Z^2 + (\frac{1}{2})^2 \lambda(B)^2)^{\frac{1}{2}}$. □

Lemma 51. Suppose that B is a (column) basis matrix for a lattice in H with elongation $\lambda(B)$ and that Z is an independent 0-subgaussian random variable with standard parameter b_Z. The coordinate-wise randomised rounding discretisation $\lfloor Z \rceil_{\Gamma+c}^{B}$ of this random variable Z is a 0-subgaussian random variable with standard parameter $(b_Z^2 + (\frac{1}{2})^2 \lambda(B)^2)^{\frac{1}{2}}$, □

Proof. If Z is a 0-subgaussian random variable with standard parameter b_Z, then Z has mean $\mathbf{E}(Z) = 0$ and so is a (noncentral) subgaussian random variable with noncentrality parameter 0 and deviation parameter b_Z. Lemma 50 therefore shows that coordinate-wise randomised rounding discretisation of Z to $\lfloor Z \rceil_{\Gamma+c}^{B}$ is a (noncentral) subgaussian random variable with noncentrality parameter 0 and deviation parameter $(b_Z^2 + (\frac{1}{2})^2 \lambda(B)^2)^{\frac{1}{2}}$. Thus $\lfloor Z \rceil_{\Gamma+c}^{B}$ is a 0-subgaussian random variable with standard parameter $(b_Z^2 + (\frac{1}{2})^2 \lambda(B)^2)^{\frac{1}{2}}$. □

5.3 Discretised Spherical H-Normal Distributions in Various Bases

We now extend the results of Section 4.2 by considering the distributional properties of a random variable with a discretised Spherical H-Normal distribution for a lattice on H as vectors with a general basis matix B. We again use the notation of Section 2.3, which is summarised in Figure 5. We begin with Lemma 52 which gives the covariance matrix of such a discretisation when expressed in the T-basis for H.

Lemma 52. Suppose B is a (column) basis matrix for the n-dimensional lattice Λ in H. The coordinate-wise randomised rounding discretisation $\lfloor X \rceil_{\Lambda+c}^{B}$ of the random variable X on H to the lattice coset $\Lambda+c$ with respect to the basis B with elongation $\lambda(B)$ when expressed in the T-basis for H as $(\lfloor X \rceil_{\Lambda+c}^{B})^{\ddagger} = T^{\dagger} \lfloor X \rceil_{\Lambda+c}^{B}$ has covariance matrix

$$\operatorname{Cov}\left((\lfloor X \rceil_{\Lambda+c}^{B})^{\ddagger}\right) = \operatorname{Cov}\left(X^{\ddagger}\right) + \widehat{B}\widehat{B}^{T},$$

where $\operatorname{Cov}\left(X^{\ddagger}\right)$ is the covariance matrix of the real random variable $X^{\ddagger} = T^{\dagger}X$ and $\widehat{B}$ is a real matrix with elongation $\lambda(\widehat{B})$ bounded as $\lambda(\widehat{B}) \leq \frac{1}{2}\lambda(B)$. □

Proof. We suppose without loss of generality that $\mathbf{E}(\lfloor X \rceil_{\Lambda+c}^{B}) = 0$. In this case, the covariance matrix of $(\lfloor X \rceil_{\Lambda+c}^{B})^{\ddagger} = T^{\dagger} \lfloor X \rceil_{\Lambda+c}^{B}$ is given by

$$\operatorname{Cov}\left(\lfloor X \rceil_{\Lambda+c}^{B})^{\ddagger}\right) = \operatorname{Cov}\left(T^{\dagger} \lfloor X \rceil_{\Lambda+c}^{B}\right) = \mathbf{E}\left(\left(T^{\dagger} \lfloor X \rceil_{\Lambda+c}^{B}\right)\left(T^{\dagger} \lfloor X \rceil_{\Lambda+c}^{B}\right)^{T}\right).$$

We first consider the covariance matrix of the conditional random variable $\left(T^{\dagger} \lfloor X \rceil_{\Lambda+c}^{B} \middle| X = x\right)$, which is given by

$$\begin{aligned}
\operatorname{Cov}\left(T^{\dagger} \lfloor X \rceil_{\Lambda+c}^{B} \middle| X = x\right) &= \mathbf{E}\left(\left(T^{\dagger} \lfloor X \rceil_{\Lambda+c}^{B}\right)\left(T^{\dagger} \lfloor X \rceil_{\Lambda+c}^{B}\right)^{T} \middle| X = x\right) \\
&= \mathbf{E}\left(\left(T^{\dagger}x + T^{\dagger}BQ_{x,c}\right)\left(T^{\dagger}x + T^{\dagger}BQ_{x,c}\right)^{T}\right) \\
&= \left(T^{\dagger}x\right)\left(T^{\dagger}x\right)^{T} + \left(T^{\dagger}B\right)\mathbf{E}(Q_{x,c}Q_{x,c}^{T})\left(T^{\dagger}B\right)^{T} \\
&= \left(T^{\dagger}x\right)\left(T^{\dagger}x\right)^{T} + \left(T^{\dagger}B\right)\operatorname{Cov}(Q_{x,c})\left(T^{\dagger}B\right)^{T}
\end{aligned}$$

as the multivariate Reduction random variable $Q_{x,c}$ has mean $\mathbf{E}(Q_{x,c}) = 0$ and $\mathbf{E}\left(Q_{x,c}Q_{x,c}^{T}\right) = \operatorname{Cov}(Q_{x,c})$ is the diagonal covariance matrix of $Q_{x,c}$. However, Lemma 43 and Definition 27 show that the components of $Q_{x,c}$ are independent with maximum variance $\frac{1}{4}$, so its covariance matrix can be written as $\operatorname{Cov}\left(Q_{x,c}\right) = D_{x,c}^{2}$, where $D_{x,c}$ is a diagonal matrix with non-negative diagonal entries at most $\frac{1}{2}$. If we therefore write $\widehat{B}_{x,c} = \left(T^{\dagger}B\right)D_{x,c}$, then $\widehat{B}_{x,c}$ is a real matrix with elongation $\lambda(\widehat{B}_{x,c})$ bounded as $\lambda(\widehat{B}_{x,c}) \leq \frac{1}{2}\lambda(T^{\dagger}B) = \frac{1}{2}\lambda(B)$ for all x and c as $T^{\dagger}$ is a unitary matrix. Thus the conditional covariance matrix is given by

$$\operatorname{Cov}\left(T^{\dagger} \lfloor X \rceil_{\Lambda+c}^{B} \middle| X = x\right) = \left(T^{\dagger}x\right)\left(T^{\dagger}x\right)^{T} + \widehat{B}_{x,c}\widehat{B}_{x,c}^{T}.$$

We can obtain an unconditional covariance matrix for $T^\dagger \lfloor X \rceil_{\Lambda+c}^B$. We can first obtain the conditional expectation random variable

$$\mathrm{Cov}\left(T^\dagger \lfloor X \rceil_{\Lambda+c}^B \middle| X\right) = \left(T^\dagger X\right)\left(T^\dagger X\right)^T + \widehat{B}_{X,c}\widehat{B}_{X,c}^T,$$

where $\widehat{B}_{X,c}$ is a random matrix with elongation $\lambda(\widehat{B}_{X,c}) \leq \frac{1}{2}\lambda(B)$. The Law of Total Expectation [17] then gives the unconditional covariance matrix for $T^\dagger \lfloor X \rceil_{\Lambda+c}^B$ as

$$\begin{aligned}\mathrm{Cov}\left((\lfloor X \rceil_{\Lambda+c}^B)^\ddagger\right) = \mathrm{Cov}\left(T^\dagger \lfloor X \rceil_{\Lambda+c}^B\right) &= \mathbf{E}\left(\mathrm{Cov}\left(T^\dagger \lfloor X \rceil_{\Lambda+c}^B \middle| X\right)\right) \\ &= \mathbf{E}\left(\left(T^\dagger X\right)\left(T^\dagger X\right)^T\right) + \mathbf{E}\left(\widehat{B}_{X,c}\widehat{B}_{X,c}^T\right) \\ &= \mathrm{Cov}\left(X^\ddagger\right) + \widehat{B}\widehat{B}^T,\end{aligned}$$

where $\widehat{B}$ is a matrix satisfying $\widehat{B}\widehat{B}^T = \mathbf{E}\left(\widehat{B}_{X,c}\widehat{B}_{X,c}^T\right)$ and has elongation $\lambda(\widehat{B})$ bounded as $\lambda(\widehat{B}) \leq \frac{1}{2}\lambda(B)$. □

Lemma 53 now gives a more detailed result for the distributional properties of a random variable with a discretised Spherical H-Normal distribution $\lfloor N_H(p^2\rho^2) \rceil_{\Lambda+c}^B$ for a lattice on H as vectors with basis matrix B, where as before we express the component variance as $p^2\rho^2$.

Lemma 53. Suppose that $Z \sim N_H(p^2\rho^2)$ is a Spherical H-Normal random variable expressed as a vector in the I-basis for H, and that $\lfloor Z \rceil_{\Lambda+c}^B$ is the discretisation of Z to a lattice coset $\Lambda + c$ of the lattice Λ with respect to the basis B. Suppose also that $\left(\lfloor Z \rceil_{\Lambda+c}^B\right)^\ddagger = T^\dagger \lfloor Z \rceil_{\Lambda+c}^B$ expresses this random variable as a real vector in the T-basis for H, and that $\widehat{B}$ is the real matrix defined in Lemma 52 with elongation $\lambda(\widehat{B}) \leq \frac{1}{2}\lambda(B)$.
(i) $\left(\lfloor Z \rceil_{\Lambda+c}^B\right)^\ddagger$ has mean $\mathbf{E}\left(\left(\lfloor Z \rceil_{\Lambda+c}^B\right)^\ddagger\right) = 0$.
(ii) $\left(\lfloor Z \rceil_{\Lambda+c}^B\right)^\ddagger$ has covariance matrix $\mathrm{Cov}\left(\left(\lfloor Z \rceil_{\Lambda+c}^B\right)^\ddagger\right) = p^2\rho^2\left(I + \dfrac{\widehat{B}\widehat{B}^T}{(p\rho)^2}\right)$.
(iii) $\left(\lfloor Z \rceil_{\Lambda+c}^B\right)^\ddagger$ is 0-subgaussian with standard parameter $p\rho\left(1 + \left(\frac{\lambda(B)}{2p\rho}\right)^2\right)^{\frac{1}{2}}$.
□

Proof. Lemma 47 gives part (i), and Lemma 52 gives part (ii). Lemma 51 shows that $\lfloor Z \rceil_{\Lambda+c}^B$, and hence $\left(\lfloor Z \rceil_{\Lambda+c}^B\right)^\ddagger = T^\dagger \lfloor Z \rceil_{\Lambda+c}^B$ as $T^\dagger$ unitary, is 0-subgaussian with standard parameter $(p^2\rho^2 + (\frac{1}{2})^2\lambda(B)^2)^{\frac{1}{2}}$. Part (iii) then follows. □

We finish this discussion of discretisations with Lemmas 54 and 55, which specify a good asymptotic approximation as a Normal distribution for the vectors $\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^*$ and $\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma'}\right)^{**}$ expressing such discretisations in the $p\Gamma$-basis and $p\Gamma'$-basis for H, that is to say in the "decoding bases" for H. We note that these results depend only on Central Limit arguments and so only depend on the moments of $\lfloor N_H(p^2\rho^2) \rceil_{\Lambda+c}^B$ and not on the fully specified distribution of $\lfloor N_H(p^2\rho^2) \rceil_{\Lambda+c}^B$.

Lemma 54. Suppose that $Z \sim N_H(p^2\rho^2)$ is a Spherical H-Normal random variable expressed as a vector in the I-basis for H, and that $\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}$ is the discretisation of Z to a lattice coset $\Lambda + c$ for the lattice $\Lambda = \sigma(pR^\vee)$ in H with respect to the $p\Gamma$-basis. Suppose also that $\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^* = p^{-1}\Gamma^{-1}\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}$ expresses this random variable as a real vector in the $p\Gamma$-basis for H.
(i) $\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^*$ is well-approximated as a $\mathrm{N}(0; \rho^2(mI - J))$ multivariate Normal random variable for large m and large ρ.
(ii) $\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^*$ is well-approximated by some 0-subgaussian random variable with standard parameter $m^{\frac{1}{2}}\rho$ for large m and large ρ.
(iii) A component $\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^*_j$ of $\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^*$ can be well-approximated as a $\mathrm{N}(0; n\rho^2)$ random variable for large $n = m - 1$ and large ρ.
(iv) A component $\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^*_j$ of $\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^*$ can be well-approximated by some 0-subgaussian random variable with standard parameter $n^{\frac{1}{2}}\rho$ for large $n = m-1$ and large ρ. □

Proof. We use the results of Lemma 53 with the basis matrix $B = p\Gamma$ for the $p\Gamma$-basis for H. This shows that the real random variable $\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^\ddagger$ has mean vector 0 and covariance matrix $\mathrm{Cov}\left(\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^\ddagger\right) = p^2\rho^2\left(I + \rho^{-2}\widehat{\Gamma}\widehat{\Gamma}^T\right)$. Lemmas 42 and 52 show that $\widehat{\Gamma}$ has elongation bounded as $\lambda(\widehat{\Gamma}) \leq \frac{1}{2}\lambda(\Gamma) = \frac{1}{2}$, so the components of $\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}$ are weakly correlated for large ρ.

The random variable $\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^* = p^{-1}\Delta\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^\ddagger$ is a linear transformation of $\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^*$ (see for example Figure 4). Thus $\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^*$ has mean vector 0 and covariance matrix

$$\begin{aligned}
\mathrm{Cov}\left(\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^*\right) &= p^{-2}\Delta\,\mathrm{Cov}\left(\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^*\right)\,\Delta^T = \rho^2\Delta\left(I + \rho^{-2}\widehat{\Gamma}\widehat{\Gamma}^T\right)\Delta^T \\
&= \rho^2\left(\Delta\Delta^T + \rho^{-2}(\Delta\widehat{\Gamma})(\Delta\widehat{\Gamma})^T\right) \\
&= \rho^2\left((mI - J) + \rho^{-2}(\Delta\widehat{\Gamma})(\Delta\widehat{\Gamma})^T\right) \\
&= \rho^2(mI - J)\left(I + m^{-1}\rho^{-2}(I + J)(\Delta\widehat{\Gamma})(\Delta\widehat{\Gamma})^T\right) \\
&\approx \rho^2(mI - J).
\end{aligned}$$

for large m and large ρ. We can the use an appropriate form of the Central Limit Theorem for weakly correlated random variables with similar variances [17] to give a Central Limit argument that $\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^* = p^{-1}\Delta\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^\ddagger$ is very well-approximated by a multivariate $\mathrm{N}\left(\mathbf{E}\left(\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^*\right); \mathrm{Cov}\left(\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^*\right)\right)$ multivariate Normal random variable. Thus we have shown that $\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^*$ is very well-approximated as a multivariate $\mathrm{N}(0; \rho^2(mI - J)$ Normal random variable

for large ρ and large m, so giving part (i). Lemma 3 then gives part (ii). Consideration of a component of the $\mathrm{N}(0; m\rho^2(I - m^{-1}J)$ distribution with variance $(m-1)\rho^2$ then gives parts (iii) and (iv). □

Lemma 55. Suppose that $Z \sim N_H(p^2\rho^2)$ is a Spherical H-Normal random variable expressed as a vector in the I-basis for H, and that $\lfloor Z \rceil_{\Lambda+c}^{p\Gamma'}$ is the discretisation of Z to a lattice coset $\Lambda + c$ for the lattice $\Lambda = \sigma(pR^{\vee})$ in H with respect to the $p\Gamma'$-basis. Suppose also that $\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma'}\right)^{**} = p^{-1}\Gamma'^{-1}\lfloor Z \rceil_{\Lambda+c}^{p\Gamma'}$ expresses this random variable as a real vector in the $p\Gamma$-basis for H.
(i) $\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^{**}$ is well-approximated as a $\mathrm{N}(0; m\rho^2(I + J - (1-m^{-1})E))$ multivariate Normal random variable for large m and large ρ, where $J = \mathbf{1}\mathbf{1}^T$ and $E = e_1 e_1^T$.
(ii) $\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^{**}$ is well-approximated by some 0-subgaussian random variable with standard parameter $m\rho$ for large m and large ρ.
(iii) A component $\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)_j^{**}$ of $\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^{**}$ can be well-approximated as a $\mathrm{N}(0; (m+1)\rho^2)$ random variable (when $j = 1$) or as a $\mathrm{N}(0; 2m\rho^2)$ random variable (when $j = 2, \ldots, n$) for large m and large ρ.
(iv) A component $\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)_j^{**}$ of $\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^{**}$ can be well-approximated by some 0-subgaussian random variable with standard parameter $(m+1)^{\frac{1}{2}}\rho$ (when $j = 1$) or $2^{\frac{1}{2}}m^{\frac{1}{2}}\rho$ (when $j = 2, \ldots, n$) for large m and large ρ. □

Proof. The random variable $\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^{**} = p^{-1}\Delta''\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^{\ddagger}$ is a linear transformation of $\left(\lfloor Z \rceil_{\Lambda+c}^{p\Gamma}\right)^{*}$ (see for example Figure 4). We can then use Lemma 5 and the same Central Limit argument of the proof of Lemma 54 to obtain these results. □

5.4 The $\odot$-product of Discretisations in the I-basis for H

We conclude this Section by considering the $\odot$-product of vectors expressing the discretisations of Spherical H-Normal random variables in the I-basis for H. We show in Theorem 4 by generalising Theorem 2 that such an $\odot$-product of discretisations in the I-basis is not a δ-dubgaussian random variable.

Theorem 4. Suppose Z_1 and Z_2 are independent Spherical H-Normal random variables (in the I-basis for H) and that $\lfloor Z_1 \rceil_{\Gamma+c_1}^{B}$ and $\lfloor Z_2 \rceil_{\Gamma+c_2}^{B}$ are their coordinate-wise randomised rounding discretisations, then their componentwise product $\lfloor Z_1 \rceil_{\Gamma+c_1}^{B} \odot \lfloor Z_2 \rceil_{\Gamma+c_2}^{B}$ is not a δ-subgaussian random variable. □

Proof. Without loss of generality, we suppose that $Z_1, Z_2 \sim N_H(1)$ both have component variance 1. Their coordinate-wise randomised rounding discretisations $\lfloor Z_1 \rceil_{\Gamma+c_1}^{B}$ and $\lfloor Z_2 \rceil_{\Gamma+c_2}^{B}$ of Z_1 and Z_2 to cosets of the lattice with (column) basis matrix B are given by

$$\lfloor Z_1 \rceil_{\Gamma+c_1}^{B} = Z_1 + BQ_{Z_1,c_1} \quad \text{and} \quad \lfloor Z_2 \rceil_{\Gamma+c_2}^{B} = Z_2 + BQ_{Z_2,c_2},$$

where Q_{Z_1,c_1} is defined by the conditional multivariate Reduction (Definition 27) random variable $(Q_{Z_1,c_1}|Z_1 = z_1) = Q_{z_1,c_1} \sim \mathrm{Red}(B^{-1}(c_1 - z_1))$ and so on. The componentwise product of these discretisations is therefore given by

$$\lfloor Z_1 \rceil^B_{\Gamma+c_1} \odot \lfloor Z_2 \rceil^B_{\Gamma+c_2} = (Z_1 + BQ_{Z_1,c_1}) \odot (Z_2 + BQ_{Z_2,c_2}),$$

which can be expanded to give

$$\lfloor Z_1 \rceil^B_{\Gamma+c_1} \odot \lfloor Z_2 \rceil^B_{\Gamma+c_2} = Z_1 \odot Z_2 + Z_1 \odot BQ_{Z_2,c_2} + Z_2 \odot BQ_{Z_1,c_1} + BQ_{Z_1,c_1} \odot BQ_{Z_2,c_2}.$$

We consider the term $Z_1 \odot BQ_{Z_2,c_2} = T(T^\dagger Z_1 \otimes T^\dagger BQ_{Z_2,c_2})$ in the above sum. Lemma 44 shows that $|BQ_{Z_2,c_2}| \leq n^{\frac{1}{2}}\lambda(B)$, where $\lambda(B)$ is the elongation of B (Definition 25). Thus $|T^\dagger BQ_{Z_2,c_2}| \leq n^{\frac{1}{2}}\lambda(B)$ is a bounded random variable as $T^\dagger$ is unitary. The natural generalisation of Lemma 36 shows that the conditional random variable

$$(T^\dagger Z_1 \otimes T^\dagger BQ_{Z_2,c_2} | T^\dagger BQ_{Z_2,c_2} = \alpha) = \alpha \otimes T^\dagger Z_1$$

is a 0-subgaussian random variable with standard parameter α bounded by $|\alpha| \leq n^{\frac{1}{2}}\lambda(B)$, as $T^\dagger Z_1 \sim \mathrm{N}(0, b_1^2 I_n)$. Thus the unconditional random variable $Z_1 \odot BQ_{Z_2,c_2}$, and similarly $Z_2 \odot BQ_{Z_1,c_1}$ is a 0-subgaussian random variable. Furthermore, the componentwise product $BQ_{Z_1,c_1} \odot BQ_{Z_2,c_2}$ of the bounded random variables BQ_{Z_1,c_1} and BQ_{Z_2,c_2} is bounded, and so Lemma 21 can be used to show that $BQ_{Z_1,c_1} \odot BQ_{Z_2,c_2}$ is also a 0-subgaussian random variable.

We can now consider the random variable $\lfloor Z_1 \rceil^B_{\Gamma+c_1} \odot \lfloor Z_2 \rceil^B_{\Gamma+c_2}$ and note that we can express the componentwise product of Spherical H-Normal random variables as

$$Z_1 \odot Z_2 = \lfloor Z_1 \rceil^B_{\Gamma+c_1} \odot \lfloor Z_2 \rceil^B_{\Gamma+c_2} - Z_1 \odot BQ_{Z_2,c_2} - Z_2 \odot BQ_{Z_1,c_1} - BQ_{Z_1,c_1} \odot BQ_{Z_2,c_2}.$$

If we suppose (for a contradiction) that $\lfloor Z_1 \rceil^B_{\Gamma+c_1} \odot \lfloor Z_2 \rceil^B_{\Gamma+c_2}$ is a δ-subgaussian random variable, then $Z_1 \odot Z_2$ would be the sum of δ-subgaussian random variables and so Lemma 23 shows that $Z_1 \odot Z_2$ would be a δ-subgaussian random variable itself. However, Theorem 2 shows that $Z_1 \odot Z_2$ is not a δ-subgaussian random variable, which gives a contradiction. Thus the componentwise product $\lfloor Z_1 \rceil^B_{\Gamma+c_1} \odot \lfloor Z_2 \rceil^B_{\Gamma+c_2}$ of discretisations cannot be a δ-subgaussian random variable. □

5.5 The $\odot$-product of Discretisations in a Decoding Basis for H

Theorem 4 shows that $\odot$-product of vectors expressing the discretisations of Spherical H-Normal random variables in the I-basis for H is not a δ-dubgaussian random variable. Indeed, as these discretisations of Spherical H-Normal random variables are in general small perturbations of Spherical H-Normal random variables, the discussion of Section 4.5 and Figures 2 and 3 show that the distribution of such an $\odot$-product in the I-basis is very different to a δ-subgaussian or Spherical H-Normal random variable. However, Lemma 56 shows that we can recover

a good Normal approximation for a scaled decoding $m^{-1}p\Gamma$-basis for H, and we could give a similar result for the $m^{-1}p\Gamma'$-basis.

We note that Lemma 56 is fundamentally given by a Central Limit argument applied to the "highly non-Normal" distribution of an $\odot$-product of vectors expressing discretised Spherical H-Normal random variables in the I-basis for H. Thus only the mean vector and covariance matrix of the $\odot$-product in the I-basis are essentially relevant to the Normal approximation. Other matters, such as the δ-subgaussian properties of this $\odot$-product in the I-basis (or its two factors) are not relevant to this Normal approximation.

Lemma 56. Suppose that $Z_1 \sim N_H(p^2\rho_1^2)$ and $Z_2 \sim N_H(p^2\rho_2^2)$ are independent Spherical H-Normal random variables expressed as vectors in the I-basis for H. The vector expressing the product of their discretisations $\lfloor Z_1 \rceil_{\Lambda+c_1}^{p\Gamma}$ and $\lfloor Z_2 \rceil_{\Lambda+c_2}^{p\Gamma}$ in the scaled decoding $m^{-1}p\Gamma$-basis for H is well-approximated as a real multivariate $\mathrm{N}(0; m^2p^2\rho_1^2\rho_2^2(mI - J))$ has mean vector 0 and covariance matrix $m^2p^2\rho_1^2\rho_2^2(mI - J)$. □

Proof. Lemma 53 shows that that the real vector $(\lfloor Z_j \rceil_{\Lambda+c_j}^{p\Gamma})^\ddagger$ expressing the the discretisation of Z_j to the lattice coset $\Lambda + c_j$ with respect to the $p\Gamma$-basis in the T-basis, that is to say the real vector expressing the Embedded Noise in the T-basis, has mean vector $\mathbf{E}\left((\lfloor Z_j \rceil_{\Lambda+c_j}^{p\Gamma})^\ddagger\right) = 0$ and covariance matrix well-approximated as

$$\mathrm{Cov}\left((\lfloor Z_j \rceil_{\Lambda+c_j}^{p\Gamma})^\ddagger\right) = p^2\rho_j^2\left(I + \rho_j^{-2}\widehat{\Gamma}\widehat{\Gamma}^T\right) \approx p^2\rho_j^2 I$$

for large ρ_j (where $j = 1, 2$). Thus Lemma 33 shows that the $\otimes$-product of these two real random vectors expressing the Embedded Noise in the T-basis has mean vector

$$\mathbf{E}\left((\lfloor Z_1 \rceil_{\Lambda+c_j}^{p\Gamma})^\ddagger \otimes (\lfloor Z_2 \rceil_{\Lambda+c_j}^{p\Gamma})^\ddagger\right) = 0$$

and covariance matrix well-approximated for large ρ_1 and ρ_2 by

$$\mathrm{Cov}\left((\lfloor Z_1 \rceil_{\Lambda+c_j}^{p\Gamma})^\ddagger \otimes (\lfloor Z_2 \rceil_{\Lambda+c_j}^{p\Gamma})^\ddagger\right) \approx p^4\rho_1^2\rho_2^2 I.$$

We now consider the real vector expressing this product in the $m^{-1}p\Gamma$-basis for H. Accordingly, we use the change of basis matrix $mp^{-1}\Delta$ to move from the T-basis for H to the $m^{-1}p\Gamma$-basis for H. Thus we see that

$$\mathbf{E}\left(mp^{-1}\Delta\left((\lfloor Z_1 \rceil_{\Lambda+c_j}^{p\Gamma})^\ddagger \otimes (\lfloor Z_2 \rceil_{\Lambda+c_j}^{p\Gamma})^\ddagger\right)\right) = 0,$$

and the covariance matrix for the vector expressing the product in the $m^{-1}p\Gamma$-basis is well-approximated as

$$\begin{aligned}\mathrm{Cov}\left(mp^{-1}\Delta\left((\lfloor Z_1 \rceil_{\Lambda+c_j}^{p\Gamma})^\ddagger \otimes (\lfloor Z_2 \rceil_{\Lambda+c_j}^{p\Gamma})^\ddagger\right)\right) &\approx m^2p^{-2}\Delta\left(p^4\rho_1^2\rho_2^2 I\right)\Delta^T \\ &= m^2p^2\rho_1^2\rho_2^2\Delta\Delta^T \\ &= m^2p^2\rho_1^2\rho_2^2(mI - J).\end{aligned}$$

for large ρ_1 and ρ_2. We can the use an appropriate form of the Central Limit Theorem for weakly correlated random variables with similar variances [17] to give a Central Limit argument in the manner of the proof of Lemma 54 to show that this product $mp^{-1}\Delta\left((\lfloor Z_1 \rceil_{\Lambda+c_j}^{p\Gamma})^{\ddagger} \otimes (\lfloor Z_2 \rceil_{\Lambda+c_j}^{p\Gamma})^{\ddagger}\right)$ has a multivariate Normal distribution with mean 0 and the above covariance matrix. □

6 The THRing Cryptosystem

We now apply the ideas developed in this paper to analyse the *Symmetric-Key Homomorphic Cryptosystem* of *Toolkit* Section 8.3. We refer to this homomorphic Ring-LWE cryptosystem as the THRing cryptosystem and a specification is given in Figure 8. Our analysis of the THRing cryptosystem begins with a full description of the THRing cryptosystem in our notation. We then give a full statistical description of the various types of "Noise" used by the THRing cryptosystem. This allows us to apply our results to the *Toolkit* discussion of the THRing cryptosystem, and in particular we obtain the following result.

- Proposition 2 shows that the assertion of *Toolkit* Lemma 8.7 about the distribution of the product of δ-subgaussian random variables is not correct. The *Toolkit* uses this assertion to attempt to justify the correctness of the THRing cryptosystem.

We then use our ideas to develop a method that gives a rigorous analysis of the THRing cryptosystem and allows us to derive the following results.

- Theorem 5 gives a bound for the probability of incorrect decryption of a degree-1 ciphertext in the THRing cryptosystem.
- Theorem 6 gives a bound for the probability of incorrect decryption of a degree-2 ciphertext in the THRing cryptosystem.

6.1 The Encryption Process in the THRing Cryptosystem

We now give a description of the relevant parts of the encryption process of the THRing cryptosystem. The secret key for the THRing cryptosystem is an element $s \in R$. The plaintext space in the THRing cryptosystem is R_p, and a plaintext $\mu \in R_p$ is encrypted to give a linear polynomial over $R_q^{\vee}$. The encryption process for the THRing cryptosystem for a plaintext μ requires us to generate a *Noise* random variable that is the result of a discretisation process involving the plaintext μ and some random input. The main notation and terminology we use in discussing this encryption process is summarised in Figure 9.

The first step of the encryption process is to generate a random input for the discretisation process involving the plaintext μ. Accordingly, we let

$$Y \sim \mathrm{N}_H(p^2\rho^2)$$

The `THRing` cryptosystem. Let ψ be a continuous LWE error distribution over $K_{\mathbb{R}}$, and let $\lfloor \cdot \rceil$ denote any valid discretisation to cosets of some scaling of $R^\vee$ (e.g. using the decoding basis $\overrightarrow{d}$ of $R^\vee$). The cryptosystem is defined formally as follows.

- Gen: choose $s' \leftarrow \lfloor \psi \rceil_{R^\vee}$, and output $s = t \cdot s' \in R$ as the secret key.
- $\mathrm{Enc}_s(\mu \in R_p)$: choose $e \leftarrow \lfloor p\psi \rceil_{t^{-1}\mu + pR^\vee}$. Let $c_0 = -c_1 \cdot s + e \in R_q^\vee$ for uniformly random $c_1 \leftarrow R_q^\vee$, and output the ciphertext $c(S) = c_0 + c_1 S$. The "noise" in $c(S)$ is defined to be e.
- $\mathrm{Dec}_s(c(S))$ for c of degree k: compute $c(s) \in (R^\vee)_q^k$, and decode it to $e = [\![c(s)]\!] \in (R^\vee)^k$. Output $\mu = t^k \cdot e \bmod pR$.

For ciphertexts c, c' of arbitrary degrees k, k', their homomorphic product is the degree-$(k+k')$ ciphertext $c(S) \boxdot c'(S) = c(S) \cdot c'(S)$ (that is to say standard polynomial multiplication). The noise in the result is defined to be the product of the noise terms of c, c'. Similarly, for ciphertexts c, c' of *equal* degree k, their homomorphic sum is $c(S) \boxplus c'(S) = c(S) + c'(S)$, and the noise in the resulting ciphertext is the sum of those of c, c'. (Observe that any degree-k ciphertext resulting from these operations has coefficients in $(R^\vee)_q^k$, as required). To homomorphically add two ciphertexts of different degrees, we must first homomorphically multiply the one having smaller degree by a fixed public encryption of $1 \in R_p$ enough times to match the larger degree.

Fig. 8. The `THRing` Cryptosystem as stated in *Toolkit* Section 8.3.

be a Spherical H-Normal random variable with component variance $p^2\rho^2$ for an appropriately chosen ρ. We term Y the *Underlying Noise*, and Y is a random vector expressed in the I-basis for H. We can therefore essentially regard Y as having a $p\Psi$ distribution, where Ψ is a continuous LWE Gaussian error distribution over $K_{\mathbb{R}}$ having component variance ρ^2. In order to encrypt the plaintext $\mu \in R_p$, we have to discretise Y to the coset $\sigma(pR^\vee) + \sigma(t^{-1}\mu)$ of the lattice $\sigma(pR^\vee)$ obtained by the canonical embedding of the scaled dual fractional ideal $pR^\vee$. We consider such a discretisation with respect to the Decoding Conjugate Pair Basis with basis matrix $p\Gamma$ (Definition 5), so we can define the discretisation of Y to a coset of $\sigma(pR^\vee)$ determined by the plaintext μ by

$$Y'(\mu) = \lfloor\!\lfloor Y \rceil\!\rceil^{p\Gamma}_{\sigma(pR^\vee)+\sigma(t^{-1}\mu)} .$$

The *Noise* random variable $Y''(\mu)$ in the encryption of the plaintext μ is then defined by the *Toolkit* to be

$$Y''(\mu) = \sigma^{-1}(Y'(\mu)),$$

an element of a coset of $pR^\vee + t^{-1}\mu$ containing information about the plaintext μ. For obvious reasons, we refer to $Y'(\mu) = \sigma(Y''(\mu))$ as the *Embedded Noise*, and we note that $Y'(\mu)$ is a vector with respect to the I-basis of H.

We can form a linear polynomial $C(\theta, \mu)$ over $R_q^\vee$ from the Noise $Y''(\mu)$ that depends on the secret key s in the following way. We choose A uniformly in $R_q^\vee$, so $A \sim \mathrm{Uni}(R_q^\vee)$, and we let $A'(\mu) = -As + Y''(\mu) \in R_q^\vee$. The linear polynomial $C(\theta; \mu)$ over $R_q^\vee$ is then defined as

$$C(\theta; \mu) = A'(\mu) + A\theta.$$

Description	Random Variable	Range of Random Variable
Underlying Noise	Y	Complex Space H
Embedded Noise	$Y'(\mu)$	Lattice Coset $\sigma(pR^\vee) + \sigma(t^{-1}\mu)$
Noise	$Y''(\mu)$	Number Field Coset $pR^\vee + t^{-1}\mu$

Fig. 9. Notation for the Noise-related quantities used in the `THRing` encryption of the plaintext μ.

We note that this linear polynomial over $R_q^\vee$ can be expressed directly in terms of the Noise $Y''(\mu)$ and the secret key s as

$$C(\theta;\mu) = A(\theta - s) + Y''(\mu).$$

The encryption process of the `THRing` cryptosystem then defines this linear polynomial to be the degree-1 ciphertext corresponding to the plaintext μ, that is to say

$$\mathrm{Enc}_s(\mu) = C(\theta;\mu).$$

6.2 Homomorphic Multiplication in the `THRing` Cryptosystem

The homomorphic product of two degree-1 ciphertext polynomials is obtained simply by multiplying these polynomials together. Thus we can obtain the degree-2 ciphertext polynomial over $R_q^\vee$ corresponding to the product $\mu_1\mu_2$ of plaintexts μ_1 and μ_2 as

$$C(\theta;\mu_1,\mu_2) = C(\theta;\mu_1) \boxdot C(\theta;\mu_2),$$

where $C(\theta;\mu_1) = A_1'(\mu_1) + A_1\theta$ and $C(\theta;\mu_2) = A_2'(\mu_2) + A_2\theta$. This degree-2 ciphertext polynomial can be expressed directly as

$$C(\theta;\mu_1,\mu_2) = A_1'(\mu_1)A_2'(\mu_2) + \left(A_2A_1'(\mu_1) + A_1A_2'(\mu_2)\right)\theta + A_1A_2\theta^2,$$

and in terms of the secret key s and its constituent Noises $Y_1''(\mu)$ and $Y_2''(\mu)$ as

$$C(\theta;\mu_1,\mu_2) = A_1A_2(\theta - s)^2 + \left(A_2Y_1''(\mu_1) + A_1Y_2''(\mu_2)\right)(\theta - s) + Y_1''(\mu_1)Y_2''(\mu_2).$$

The *Noise* in this degree-2 ciphertext polynomial $C(\theta;\mu_1,\mu_2)$ is defined to be the product $Y_1''(\mu_1)Y_2''(\mu_2)$ of the Noises $Y_1''(\mu_1)$ and $Y_2''(\mu_2)$ of the constituent degree-1 ciphertexts, that is to say the constant term in the above formulation of $C(\theta;\mu_1,\mu_2)$. This process extends in the obvious way to give ciphertexts of higher degree.

6.3 The Decryption Process in the `THRing` Cryptosystem

The *Toolkit* uses a scaled embedded decoding basis, that is to say a $p\Gamma'$-basis (Definition 14), to specify a decryption process for the `THRing` cryptosystem,

Lemma 8.5. Suppose the noise e in a degree-k ciphertext c is δ-subgaussian with parameter r for some $\delta = O(1)$, and $q \geq r \cdot \hat{m}^{k-1}\sqrt{n} \cdot \omega(\sqrt{\log n})$. Then $\mathrm{Dec}_s(c)$ recovers e with probability $1-\mathrm{negl}(n)$. Alternatively, if $q > 2\|e\|_2 \hat{m}^{k-1}\sqrt{n}$, then $\mathrm{Dec}_s(c)$ recovers e with certainty.

Fig. 10. *Toolkit* Lemma 8.5 (as stated).

though any appropriate basis can be used. We therefore describe for simplicity an alternative decryption process for our case when m is prime in which we simply replace the $p\Gamma'$-basis with a scaled embedded decoding conjugate pair basis or $p\Gamma$-basis (Definition 13) in an otherwise identical process.

In our discussion of the `THRing` cryptosystem, it is necessary to consider the expression of an element of H as a vector with respect to various different bases for H. We therefore recall the notation of of Section 2.3 and illustrated in Figure 5. If Z is a vector expressing an element of H as a vector of conjugate pairs in the I-basis (or standard basis) for H, then we have real vectors $Z^\ddagger = T^\dagger Z$, $Z^* = p^{-1}\Gamma^{-1}Z$ and $Z^{**} = \Gamma'^{-1}Z$ expressing this element as a vector in the T-basis, the $p\Gamma$-basis and the $p\Gamma'$-basis for H respectively. The change of basis transformations between these latter three bases are also summarised in Figure 4

Decryption of the degree-1 ciphertext polynomial $C(\theta, \mu)$ is performed by evaluating this polynomial at the secret s to obtain information about the Noise as

$$C(s;\mu) = Y''(\mu) \bmod R_q^\vee.$$

We let $[\![r]\!]_q = r - q[q^{-1}r]$ for $r \in \mathbb{Z}$ to denote the coset representative of $(r \bmod q)$ nearest to 0, and we can use the same notation for a coset of $\mathbb{Z}_q$. We can also extend this idea componentwise to vectors, and we write $[\![\cdot]\!]_q^B$ to indicate such an extension with respect to the basis B. If we embed $C(s,\mu)$ in H under σ and perform such a reduction modulo q with respect to to this $p\Gamma$-basis, then we obtain an integer vector $[\![\sigma(C(s,\mu))]\!]_q^{p\Gamma}$ with entries in $[-\frac{1}{2}q, \frac{1}{2}q)$.

The Embedded Noise $Y'(\mu)$ is expressed in the I-basis for H, so $Y'(\mu)$ is expressed with respect to the T-basis of H as the real vector $Y'(\mu)^\ddagger = T^\dagger Y(\mu)$. However, the change of basis from this T-basis to the $p\Gamma$-basis of H is given by $p^{-1}\Delta = p^{-1}\Gamma^{-1}T$, so there is a real transformation $Y'(\mu)^* = p^{-1}\Delta Y(\mu)^\ddagger$ that gives a real vector $Y'(\mu)^*$ specifying the Embedded Noise expressed with respect to the $p\Gamma$-basis for H. This allows us to write

$$Y'(\mu)^* = [\![\sigma(C(s,\mu))]\!]_q^{p\Gamma} \quad \text{if the Embedded Noise is small enough.}$$

In this case, we can recover the real vector $Y'(\mu)^*$ and hence the real Embedded Noise vector $Y'(\mu)^\ddagger$ with respect to the T-Basis. This allows us to determine the coset representative $\sigma(t^{-1}\mu)$ for the coset of the lattice $\sigma(pR^\vee)$ corresponding to the plaintext $\mu \in R_p$. Thus if the Embedded Noise is small enough with high probability, then we can recover the plaintext μ with high probability. In this case, we can express the decryption process as $\mathrm{Dec}_s(C(\theta;\mu)) = \mu$.

This decryption process generalises to degree-2 and higher degree ciphertexts by using a scaled decoding conjugate pair basis (Definition 6) and so on. Thus

Lemma 6.5. Let $\mathcal{I} = (R^\vee)^k$ for some $k \geq 1$, let $a \in \mathcal{I}$ and write $a = \langle \hat{m}^{1-k}\overrightarrow{d}, \mathbf{a}\rangle$ for some integral coefficient vector $\mathbf{a}$, and let $q \geq 1$ be an integer. If every coefficient $a_j \in [-q/2, q/2)$, then $[\![a \bmod q\mathcal{I}]\!] = a$. In particular, if every a_j is δ-subgaussian with parameter s, then $[\![a \bmod q\mathcal{I}]\!] = a$ except with probability at most $2n\exp(\delta - \pi q^2/(2s)^2)$.

Fig. 11. *Toolkit* Lemma 6.5 (as stated).

if $C(\theta;\mu_1)$ and $C(\theta;\mu_2)$ are two degree-1 ciphertexts with respective Embedded Noise $Y_1'(\mu_1)$ and $Y_2'(\mu_2)$, then we clearly have

$$C(s;\mu_1,\mu_2) = Y''(\mu_1)Y''(\mu_2) = C(s;\mu_1)C(s;\mu_2) \bmod (R^\vee)_q^2.$$

With the obvious extension of notation to the appropriate scaled conjugate decoding basis (Definition 6), we have

$$(Y_1'(\mu_1) \odot Y_2'(\mu_2))^* = [\![\sigma(C(s;\mu_1,\mu_2))]\!]_q^{m^{-1}p\Gamma} \quad \text{for small Embedded Noise.}$$

If the Embedded Noise is small enough with high probability, then we can recover the plaintext product $\mu_1\mu_2 \in R_p$ with high probability. The generalisation of the decryption process to decrypt higher degree ciphertexts is also clear.

6.4 Issues in the *Toolkit* Analysis of the `THRing` Cryptosystem

We begin our discussion of the *Toolkit* analysis of the `THRing` cryptosystem by considering the decryption of degree-1 ciphertext. *Toolkit* Lemma 8.5 (see Figure 10) states a result for the probability of correct decryption for degree-1 (and higher degree) `THRing` ciphertexts, where the result is justified as following directly from *Toolkit* Lemma 6.5 (see Figure 11).

Some care is needed with this *Toolkit* approach to degree-1 ciphertexts as the subgaussian standard parameter for vector random variable expressing the Embedded Noise varies greatly depending on the basis used. It seems that *Toolkit* Lemmas 8.5-8.7 of Section 8.3 use a subgaussian standard (or scaled) parameter of random vectors expressed in the I-basis (or equivalently the T-basis) for H, but *Toolkit* Lemma 6.5 uses a subgaussian standard (or scaled) parameter for random vectors expressed in a decoding basis, such as the $p\Gamma$-basis or the $p\Gamma'$-basis. However, Lemmas 53 - 55 show how the subgaussian standard parameter changes considerably when moving between these bases.

We now consider the decryption of higher degree ciphertexts in the `THRing` cryptosystem, focussing (without loss of generality) on degree-2 ciphertexts. The *Toolkit* analysis of such a degree-2 ciphertext is based on *Toolkit* Lemma 8.7 (see Figure 12). We note that $\sigma(Y_1''(\mu_1)Y_2''(\mu_2)) = Y_1'(\mu_1) \odot Y_2'(\mu_2)$, so we can restate *Toolkit* Lemma 8.7 using our terminology in terms of the Embedded Noise in the following way.

Lemma 8.7. Let e, e' be the noise terms in ciphertexts c, c', respectively. Then the noise $e \cdot e'$ in the ciphertext $c \boxdot c'$ satisfies $\|e \cdot e'\| \leq \|e\| \cdot \|e'\|_\infty$, where $\|\cdot\|$ denotes either the ℓ_2 or ℓ_∞ norm. Moreover, if e is δ-subgaussian with [scaled] parameter r, then the noise $e \cdot e'$ is δ-subgaussian with [scaled] parameter $r \cdot \|e'\|_\infty$. In particular, if e' is δ-subgaussian with [scaled] parameter r' and is independent of e. then $e \cdot e'$ is within $\texttt{negl}(n)$ statistical distance of a δ-subgaussian with [scaled] parameter $r \cdot r'$ $\omega((\log n)^{\frac{1}{2}})$.

Fig. 12. *Toolkit* Lemma 8.7 (as stated).

Restated *Toolkit* Lemma 8.7 for Two Degree-1 Ciphertexts.
Let $Y_1'(\mu_1) = \sigma(Y_1''(\mu_1))$ and $Y_2'(\mu_2) = \sigma(Y_2''(\mu_2))$ be the Embedded Noise terms (in the I-basis) of two degree-1 ciphertexts $C(\theta; \mu_1)$ and $C(\theta; \mu_2)$ given by the encryption of the plaintexts μ_1 and μ_2 respectively.
(i) The Embedded Noise $Y_1'(\mu_1) \odot Y_2'(\mu_2)$ in the ciphertext $C(\theta; \mu_1) \boxdot C(\theta; \mu_2)$ satisfies $\|Y_1'(\mu_1) \odot Y_2'(\mu_2)\| \leq \|Y_1'(\mu_1)\| \cdot \|Y_2'(\mu_2)\|_\infty$, where $\|\cdot\|$ denotes either the ℓ_2 or ℓ_∞ norm.
(ii) If the Embedded Noise $Y_1'(\mu_1)$ is a δ-subgaussian random variable with standard parameter b_1, then the Embedded Noise product $Y_1'(\mu_1) \odot Y_2'(\mu_2)$ of $C(\theta; \mu_1) \boxdot C(\theta; \mu_2)$ is a δ-subgaussian random variable with standard parameter $b_1 \|Y_2'(\mu)\|_\infty$.
(iii) If the Embedded Noise $Y_2'(\mu_2)$ is a δ-subgaussian random variable with standard parameter b_2 and the Embedded Noises $Y_2'(\mu_2)$ and $Y_1'(\mu_1)$ are independent, then the Embedded Noise $Y_1'(\mu_1) \odot Y_2'(\mu_2)$ is within $\texttt{negl}(n)$ statistical distance of a δ-subgaussian random variable with standard parameter $b_1 b_2$ $\omega((\log n)^{\frac{1}{2}})$.
□

Toolkit Lemma 8.7 is highly problematic, as the following three remarks demonstrate. Firstly, Theorem 4 shows that a product $Y_1'(\mu_1) \odot Y_2'(\mu_2)$ of Embedded Noise is not a δ-subgaussian random variable (or even close to one). Secondly, the claim of part (ii) that the Embedded Noise product $Y_1'(\mu_1) \odot Y_2'(\mu_2)$ is a δ-subgaussian random variable with standard parameter $b_1 \|Y_2'(\mu_2)\|_\infty$ is not correct as $b_1 \|Y_2'(\mu_2)\|_\infty$ is itself a random variable. Thirdly, Example 2 shows that the $\odot$-product of two independent δ-subgaussian random variables on H each with a fixed standard parameter can have an arbitrarily large standard parameter even for small n, contrary to the claim of part (iii).

More generally, the application of *Toolkit* Lemma 8.7 to the analysis of the `THRing` cryptosystem is justified in the preamble by the assertion that this Lemma provides "... (*nearly*) *tight bounds on the subgaussian parameter of the noise under* [componentwise multiplication]". However, Theorem 4 shows that degree-2 Noise is not a δ-subgaussian random variable, that is to say that standard parameter of degree-2 Noise must formally be regarded as infinite in any statement about such a standard parameter. Thus it is simply not possible to construct a "(nearly) tight bound" for the standard parameter of the Noise of a higher degree `THRing` ciphertext, contrary to this assertion of the *Toolkit*. These observations give Proposition 2.

Proposition 2. The proof of *Toolkit* Lemma 8.7(ii) and (iii) is not correct. The use of *Toolkit* Lemma 8.7 to provide justification that degree-2 Noise in `THRing` can be regarded as approximately δ-subgaussian and to provide an approximate standard parameter is not sustainable. □

6.5 Decryption of Degree-1 Ciphertexts in the `THRing` Cryptosystem

We now give a rigorous approach to analysing the decryption of a degree-1 ciphertext in the `THRing` cryptosystem. The `THRing` decryption process for the degree-1 ciphertext $C(\theta;\mu)$ using the $p\Gamma$-basis for H (for example) processes this ciphertext as $[\![\sigma(C(s;\mu))]\!]_q^{p\Gamma}$. The processing of a degree-1 ciphertext in this way therefore fundamentally involves a change of basis transformation between bases for H ultimately to the $p\Gamma$-basis. Analysing this change of basis transformation yields Theorem 5, which gives a bound for the probability of the incorrect decryption of a `THRing` degree-1 ciphertext when using the $p\Gamma$-basis for H.

Theorem 5. The probability of the incorrect decryption of a `THRing` degree-1 ciphertext using the $p\Gamma$-basis for H is bounded for moderate or large $\frac{1}{2}(n^{\frac{1}{2}}\rho)^{-1}q$ by

$$\mathbf{P}(\text{Incorrect decryption of degree-1 ciphertext}) \leq \frac{4n^{\frac{3}{2}}\rho}{(2\pi)^{\frac{1}{2}}q}\exp\left(-\frac{q^2}{8n\rho^2}\right). \quad \square$$

Proof. Lemma 54 shows that the vector $\left(\lfloor Z\rceil_{\Lambda_c}^{p\Gamma}\right)^*$ expressing the Embedded Noise in the $p\Gamma$-basis for H is very well-approximated by a multivariate Normal random variable $U \sim \mathrm{N}(0;\rho^2(mI-J))$, with components $U_1,\ldots,U_n \sim \mathrm{N}(0,n\rho^2)$. Thus these components have upper tail probability given for $\alpha > 0$ by

$$\mathbf{P}(U_j > \alpha) = \mathbf{P}\left((n^{\frac{1}{2}}\rho)^{-1}U_j > (n^{\frac{1}{2}}\rho)^{-1}\alpha\right) = Q\left((n^{\frac{1}{2}}\rho)^{-1}\alpha\right),$$

where Q is the "Q-function" giving the upper tail probability for a standard Normal $\mathrm{N}(0,1)$ distribution. This tail probability $Q(x)$ is bounded by its asymptotic expansion as $Q(x) \leq (2\pi x^2)^{-\frac{1}{2}}\exp(-\frac{1}{2}x^2)$, and we note that this bound is extremely tight for even moderate values of $x > 0$. We can now obtain a bound for the tail probability for the maximum of $U_1,\ldots,U_n$ for moderate $(n^{\frac{1}{2}}\rho)^{-1}\alpha$ by using the union bound [17] (also used in a similar way in *Toolkit* Lemma 6.5) to obtain

$$\begin{aligned}\mathbf{P}\left(\max\{U_1,\ldots,U_n\} > \alpha\right) &\leq n\mathbf{P}(U_j > \alpha) = nQ\left((n^{\frac{1}{2}}\rho)^{-1}\alpha\right)\\ &\leq \frac{n^{\frac{3}{2}}\rho}{(2\pi)^{\frac{1}{2}}\alpha}\exp\left(-\frac{\alpha^2}{2n\rho^2}\right).\end{aligned}$$

Thus we obtain a bound for the tail probability for the maximum absolute size of a component of

$$\mathbf{P}\left(\max\{|U_1|,\ldots,|U_n|\} > \alpha\right) \leq \frac{2n^{\frac{3}{2}}\rho}{(2\pi)^{\frac{1}{2}}\alpha}\exp\left(-\frac{\alpha^2}{2n\rho^2}\right).$$

We can now give a bound for the probability of decryption failure for a degree-1 ciphertext using the Γ-basis. In this case, decryption fails if the absolute size of any component of exceeds $\frac{1}{2}q$, so taking $\alpha = \frac{1}{2}q$ for moderate and large $\frac{1}{2}(n^{\frac{1}{2}}\rho)^{-1}q$ gives

$$\mathbf{P}(\text{Incorrect decryption of degree-1 ciphertext}) \leq \frac{4n^{\frac{3}{2}}\rho}{(2\pi)^{\frac{1}{2}}q}\exp\left(-\frac{q^2}{8n\rho^2}\right). \quad \square$$

We note that using the subgaussian tail bound of Lemma 18 in the manner of *Toolkit* Lemma 6.5 for the $p\Gamma$-basis gives an equivalent bound for the probability of incorrect decryption of $2n\exp(-\frac{1}{8}(n\rho^2)^{-1}q^2)$, but this bound is less tight than Theorem 5. For a `THRing` degree-1 ciphertext, applying the Theorem 5 bound gives $\mathbf{P}(\text{Incorrect decryption}) \to 0$ as $q \to \infty$ if n is fixed. If q and n are both allowed to become large together, the situation is more complicated. For example, if we set $q = A\rho n^{\frac{1}{2}}(\log n)^{\frac{1}{2}}$ in the spirit of *Toolkit* Lemma 8.5 for some constant $A > 0$, then this bound for the probability of incorrect decryption becomes

$$\mathbf{P}(\text{Incorrect decryption of degree-1 ciphertext}) \leq \frac{4n^{1-\frac{1}{8}A^2}}{(2\pi)^{\frac{1}{2}}A(\log n)^{\frac{1}{2}}} \to 0$$

as $n \to \infty$ for $A^2 \geq 8$. This bounding function is a "negligible" function of n for large enough A. We also note that using Lemma 55 gives related bounds for the probability of incorrect decryption of a `THRing` degree-1 ciphertext when using the $p\Gamma'$-basis for H.

6.6 Decryption of Degree-2 Ciphertexts in the `THRing` Cryptosystem

We now give a rigorous approach to the analysis of the `THRing` decryption process for a degree-2 ciphertext, though we note these ideas can easily be extended to higher degree ciphertexts by using Lemma 34 and so on. We have seen that the distribution of the Embedded Noise expressed in the I-basis or the T-basis for H for such a degree-2 ciphertext has component distributions cannot therefore be approximated in any meaningful way as δ-subgaussian random variables. As noted above, the *Toolkit* approach based on such an approximation cannot be regarded as sustainable. However, we have also seen that it is possible to recover a multivariate Normal approximation for the distribution of the Embedded Noise when expressed as a vector in a scaled Γ-basis or Γ'-basis for H by using a Central Limit approach.

In more detail, the decryption of a `THRing` degree-2 ciphertext $C(\theta; \mu_1, \mu_2)$ involves processing this ciphertext as $[\![\sigma(C(s; \mu_1, \mu_2))]\!]_q^{m^{-1}p\Gamma}$, that is to say by regarding this Embedded Noise expressed as a vector with respect to the rescaled decoding conjugate pair $m^{-1}p\Gamma$-basis. Thus the processing of a degree-2 ciphertext fundamentally involves change of basis transformations for bases for H ultimately to the $m^{-1}p\Gamma$-basis. Lemma 56 demonstrates that the embedded Noise of a degree-2 ciphertext expressed as a vector is well-approximated as a multivariate Normal random distribution by invoking (as before) a Central Limit

argument. This approach allows us to give a bound for incorrect decryption of a degree-2 ciphertext in Theorem 6.

Theorem 6. The probability of the incorrect decryption of a `THRing` degree-2 ciphertext using the $m^{-1}p\Gamma$-basis for H is bounded for moderate or large $\frac{1}{2}(n^{\frac{1}{2}}mp\rho_1\rho_2)^{-1}q$ by

$$\mathbf{P}(\text{Degree-2 Incorrect decryption}) \leq \frac{4n^{\frac{3}{2}}mp\rho_1\rho_2}{(2\pi)^{\frac{1}{2}}q}\exp\left(-\frac{q^2}{8nm^2p^2\rho_1^2\rho_2^2}\right). \quad \square$$

Proof. We can adapt the argument of the proof of Theorem 5 simply by using Lemma 56 to give the appropriate moments and so replacing ρ with $mp\rho_1\rho_2$. $\square$

For a `THRing` degree-2 ciphertext, as for a degree-1 ciphertext, the Theorem 6 bound gives $\mathbf{P}(\text{Incorrect decryption}) \to 0$ as $q \to \infty$ if m and $n = m - 1$ are fixed. However, as before, if q and n are both allowed to become large together, the situation is more complicated. For example, if in the spirit of *Toolkit* Lemma 8.5, we set $q = A\rho_1\rho_2 n^{\frac{1}{2}}(\log n)^{\frac{1}{2}}$ for some constant $A > 0$, then this incorrect decryption bound becomes

$$\mathbf{P}(\text{Incorrect decryption of degree-2 ciphertext}) \leq \frac{4mp\, n^{1-\frac{1}{8mp^2}A^2}}{(2\pi)^{\frac{1}{2}}A(\log n)^{\frac{1}{2}}}.$$

It is clear that this bounding function for the probability for the incorrect decryption of a `THRing` degree-2 ciphertext when using the $m^{-1}p\Gamma$-basis for H becomes arbitrarily large as $m \to \infty$ (and hence $n = m - 1 \to \infty$), so cannot meaningfully be used to bound a probability. Similarly, the equivalent bounding function for the probability for the incorrect decryption of a degree-2 ciphertext when using the $m^{-1}p\Gamma'$-basis for H cannot meaningfully be used to bound a probability as $m \to \infty$. Thus it is not possible to use this *Toolkit* approach to obtain a meaningful bound for the probability of incorrect decryption of a degree-2 ciphertext in the $q = A\rho_1\rho_2 n^{\frac{1}{2}}(\log n)^{\frac{1}{2}}$ situation of *Toolkit* Lemma 8.5.

6.7 Summary of the Issues in the Analysis of `THRing` cryptosystem

Our analysis of the `THRing` cryptosystem shows that the approximate normality of Embedded Noise is fundamentally a Central Limit phenomenon arising from the sum of many random variables. As such, the essential issue is the first two moments of the summand random variables, namely the mean vector and the covariance matrix. A full rigorous statistical analysis of the `THRing` cryptosystem can be made using this standard statistical approach.

By contrast, the *Toolkit* δ-subgaussian approach to the analysis of `THRing` cryptosystem does not really address the fundamental statistical in the decryption process for the following two reasons.

- The *Toolkit* asserts incorrectly (for degree-2 and higher degree ciphertexts) that the summand random variables in this Central Limit sum are or can be well-approximated as δ-subgaussian random variables.

– It is not relevant to the approximation and bounding process required to justify the correctness of the `THRing` cryptosystem that the summand random variables are or can be well-approximated as δ-subgaussian random variables.

The δ-subgaussian approach of the *Toolkit* to the analysis of the `THRing` cryptosystem is therefore in general neither accurate nor relevant.

Acknowledgements

Rachel Player was supported by an ACE-CSR Ph.D. grant.

References

1. J.W. Bos, K.E. Lauter, J. Loftus, and M. Naehrig. Improved Security for a Ring-Based Fully Homomorphic Encryption Scheme. In M. Stam, editor, *Cryptography and Coding - 14th IMA International Conference*, volume 8308 of *LNCS*, pages 45–64. Springer, 2013.
2. Z. Brakerski. Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP. In R. Safavi-Naini and R. Canetti, editors, *Advances in Cryptology - CRYPTO 2012*, volume 7417 of *LNCS*, pages 868–886. Springer, 2012.
3. Z. Brakerski, C. Gentry, and V. Vaikuntanathan. (Leveled) Fully Homomorphic Encryption without Bootstrapping. In *Innovations in Theoretical Computer Science 2012*, pages 309–325, 2012.
4. Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehlé. Classical Hardness of Learning with Errors. In D. Boneh, T. Roughgarden, and J. Feigenbaum, editors, *45th Annual ACM Symposium on Theory of Computing*, 2013.
5. Z. Brakerski and V. Vaikuntanathan. Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. In P. Rogaway, editor, *Advances in Cryptology - CRYPTO 2011*, volume 6841 of *LNCS*, pages 505–524. Springer, 2011.
6. W. Castryck, I. Iliashenko, and F. Vercauteren. On the Tightness of the Error Bound in Ring-LWE. *IACR Cryptology ePrint Archive*, 2016:240, 2016.
7. W. Castryck, I. Iliashenko, and F. Vercauteren. Provably Weak Instances of Ring-LWE Revisited. In M. Fischlin and J-S. Coron, editors, *Advances in Cryptology - EUROCRYPT 2016*, volume 9665 of *LNCS*, pages 147–167. Springer, 2016.
8. H Chen, K.E. Lauter, and K.E. Stange. Attacks on Search-RLWE. *IACR Cryptology ePrint Archive*, 2015:971, 2015.
9. H. Chen, K.E. Lauter, and K.E. Stange. Vulnerable Galois RLWE Families and Improved Attacks. *IACR Cryptology ePrint Archive*, 2016:193, 2016.
10. K. Eisenträger, S. Hallgren, and K.E. Lauter. Weak Instances of PLWE. In *Selected Areas in Cryptography - SAC 2014*, volume 8741 of *LNCS*, pages 183–194. Springer, 2014.
11. Y. Elias, K.E. Lauter, E. Ozman, and K.E. Stange. Provably Weak Instances of Ring-LWE. In R. Gennaro and M. Robshaw, editors, *Advances in Cryptology - CRYPTO 2015*, volume 9215 of *LNCS*, pages 63–92. Springer, 2015.
12. J. Fan and F. Vercauteren. Somewhat Practical Fully Homomorphic Encryption. *IACR Cryptology ePrint Archive*, 2012:144, 2012.

13. S. Galbraith. *The Mathematics of Public Key Cryptography.* Cambridge University Press, 2012.
14. C. Gentry. Fully Homomorphic Encryption using Ideal Lattices. In M. Mitzenmacher, editor, *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009*, ACM, pages 169–178, 2009.
15. C. Gentry, S. Halevi, and N.P. Smart. Fully Homomorphic Encryption with Polylog Overhead. In D. Pointcheval and T. Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 465–482. Springer, 2012.
16. C. Gentry, A. Sahai, and B. Waters. Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based. In R. Canetti and J.A. Garay, editors, *Advances in Cryptology - CRYPTO 2013*, volume 8042 of *LNCS*, pages 75–92. Springer, 2013.
17. G. Grimmett and D. Stirzaker. *Probability And Random Processes.* Oxford University Press, third edition, 2001.
18. A. López-Alt, E. Tromer, and V. Vaikuntanathan. On-the-fly Multiparty Computation on the Cloud via Multikey Fully Homomorphic Encryption. In *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012*, pages 1219–1234. ACM, 2012.
19. V. Lyubashevsky, C. Peikert, and O. Regev. On Ideal Lattices and Learning with Errors over Rings. In H. Gilbert, editor, *Advances in Cryptology - EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 1–23. Springer, 2010.
20. V. Lyubashevsky, C. Peikert, and O. Regev. On Ideal Lattices and Learning with Errors Over Rings. *IACR Cryptology ePrint Archive*, 2012:230, 2012.
21. V. Lyubashevsky, C. Peikert, and O. Regev. A Toolkit for Ring-LWE Cryptography. *IACR Cryptology ePrint Archive*, 2013:293, 2013.
22. V. Lyubashevsky, C. Peikert, and O. Regev. A Toolkit for Ring-LWE Cryptography. In T. Johansson and P. Nguyen, editors, *Advances in Cryptology - EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 35–54. Springer, 2013.
23. D. Micciancio and C. Peikert. Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller. In D.Pointcheval and T. Johansson, editors, *Eurocrypt 2012*, volume 7237 of *LNCS*, pages 700–718. Springer, 2012.
24. D. Micciancio and O. Regev. Lattice-based Cryptography. In D.J. Bernstein and J. Buchmann and E. Dahmen, editor, *Post-Quantum Cryptography*, pages 147–191. Springer, 2009.
25. C. Peikert. Public-Key Cryptosystems from the worst-case Shortest Vector Problem. In M. Mitzenmacher, editor, *41st Annual ACM Symposium on Theory of Comuting*, 2009.
26. C. Peikert. Lattice Cryptography for the Internet. In M. Mosca, editor, *PQCrypto 2014*, volume 8772 of *LNCS*, pages 197–219, Springer, 2014.
27. C. Peikert. A Decade of Lattice Cryptography. *IACR Cryptology ePrint Archive*, 2015:939, 2016.
28. C. Peikert. How (Not) to Instantiate Ring-LWE. In V.Zikas and R. De Prisco, editors, *Security and Cryptography for Networks - 10th International Conference, SCN 2016*, volume 9841 of *LNCS*, pages 411–430. Springer, 2016.
29. C. Peikert, O. Regev, and N. Stephens-Davidowitz. Pseudorandomness of Ring-LWE for any Ring and Modulus. *IACR Cryptology ePrint Archive*, 2017:258, 2017.
30. O. Regev. On Lattices, Learning with Errors, Random Linear Codes and Cryptography. In H. Gabow and R. Fagin, editors, *37th Annual ACM Symposium of Theory of Computing*, 2005.
31. O. Regev. The Learning with Errors Problem (Invited Survey). In *IEEE Conference on Computational Complexity*, pages 191–204, 2010.

32. O. Rivasplata. Subgaussian Random Variables: An Expository Note. Available at `http://www.stat.cmu.edu/~arinaldo/36788/subgaussians.pdf`, 2015.
33. K.R. Stromberg. *Probability for Analysts*. Chapman and Hall, 1994.
34. M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan. Fully Homomorphic Encryption over the Integers. In H. Gilbert, editor, *Advances in Cryptology - EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 24–43. Springer, 2010.