δ-subgaussian Random Variables in Cryptography

Sean Murphy and Rachel Player

Royal Holloway, University of London, U.K.
s.murphy@rhul.ac.uk
rachel.player@rhul.ac.uk

Abstract. In the Ring-LWE literature, there are several works that use a statistical framework based on δ-subgaussian random variables. These were introduced by Miccancio and Peikert (Eurocrypt 2012) as a relaxation of subgaussian random variables. In this paper, we completely characterise δ-subgaussian random variables. In particular, we show that this relaxation from a subgaussian random variable corresponds only to the shifting of the mean. Next, we give an alternative noncentral formulation for a δ-subgaussian random variable, which we argue is more statistically natural. This formulation enables us to extend prior results on sums of δ-subgaussian random variables, and on their discretisation.

Keywords. Ring Learning with Errors, Subgaussian Random Variable.

1 Introduction

A subgaussian random variable [4] is a random variable that is bounded in a particular technical sense by a Normal random variable. Subgaussian random variables cover a wide class of random variables: for example is well known that any centred and bounded random variable is subgaussian [17]. They have many of the attractive properties of Normal random variables: for example, they form a linear space and their tails that are bounded by the tails of a Normal random variable [15]. Subgaussian random variables have been used widely in cryptography [2].

In [7], Micciancio and Peikert introduced the notion of a δ-subgaussian random variable, where δ can take a value $\delta \geq 0$, as a relaxation of a subgaussian random variable. In the formulation of [7], the case $\delta = 0$ gives a 0-subgaussian random variable, which is exactly a subgaussian random variable. Statistical arguments based on δ-subgaussian random variables have been used in Ring-LWE cryptography in many application settings including signature schemes [7], key exchange [10] and homomorphic encryption [6].

In this paper, we re-examine the relaxation in [7] of subgaussian random variables to give δ-subgaussian random variables. We completely characterise δ-subgaussian random variables by showing that this relaxation corresponds only to the shifting of the mean. This enables us to give a noncentral formulation for δ-subgaussian random variables which we argue is more statistically natural.

Amongst the prior literature using δ-subgaussian random variables, perhaps the prominent work is *A Toolkit for Ring-LWE Cryptography* [6]. This work gives an algebraic and statistical framework for Ring-LWE cryptography that is widely applicable. Using our noncentral formulation for δ-subgaussian random variables, we extend results presented in the *Toolkit* on sums of δ-subgaussian random variables, and on their discretisation.

1.1 Contributions

The first main contribution of this paper is to give a full and particularly simple characterisation of δ-subgaussian random variables. We show in Lemma 5 that any δ-subgaussian random variable with mean 0 must be a 0-subgaussian random variable. We then show in Lemma 6 that shifting a δ-subgaussian random variable by its mean gives a 0-subgaussian random variable. Finally, we show in Lemma 7 that any shift of a 0-subgaussian random variable is a δ-subgaussian random variable for some $\delta \geq 0$. These results give our main result in this section, Proposition 1, that the relaxation from 0-subgaussian random variables to δ-subgaussian random variables corresponds only to a shifting of the mean.

The second main contribution of this paper is to generalise results about δ-subgaussian random variables that have previously appeared in the literature. Firstly, we give an alternative noncentral formulation for a δ-subgaussian random variable which enables us in Theorem 1 to generalise the results in [10, 6] for sums of δ-subgaussian random variables. Secondly, in Theorem 2 we improve the result of the *Toolkit* [6] for the δ-subgaussian standard parameter of the coordinatewise randomised rounding discretisation (termed *CRR-discretisation* in our paper) of the *Toolkit* [6, Section 2.4.2] of a δ-subgaussian random variable.

1.2 Structure

We review the necessary background in Section 2. We analyse and characterise δ-subgaussian random variables in Section 3. We give a noncentral formulation for δ-subgaussian random variables in Section 4. We consider the discretisations of random variables arising in Ring-LWE in Section 5.

2 Background

2.1 Algebraic background

This section mainly follows [6]. 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 $n = \phi(m) = m - 1$, though our arguments apply more generally.

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 $1 \le k \le n$) is defined by $\zeta_m \mapsto \zeta_m^k$, so $\sum_{j=1}^n a_j \zeta_m^j \mapsto \sum_{j=1}^n a_j \zeta_m^{kj}$. The *canonical embedding* $\sigma : K \to \mathbb{C}^n$ is defined by

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

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

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

The ring embeddings $\sigma_1, \ldots, \sigma_n$ occur in conjugate pairs, and much of the analysis of Ring-LWE takes place in a space H of conjugate pairs of complex numbers. The conjugate pairs matrix T gives a basis for H that we call the T-basis.

Definition 1. The *conjugate pair matrix* is the $n \times n$ complex matrix T, so $T \colon \mathbb{C}^n \to \mathbb{C}^n$, given by

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

Definition 2. The *complex conjugate pair space* H is given by $H = T(\mathbb{R}^n)$, where T is the conjugate pairs matrix. $\square$

Our results on discretisation will rely on the spectral norm of the basis for H being considered. We note that the spectral norm for the T-basis is 1.

Definition 3. 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 *spectral norm* $\lambda(B) > 0$ of the basis matrix B is the square root of largest eigenvalue of the Gram matrix $B^\dagger B$. $\square$

2.2 The Ring-LWE problem

The Learning with Errors (LWE) problem [13, 14] has become a standard hard problem in cryptology that is at the heart of lattice-based cryptography [8, 11]. The Ring Learning with Errors (Ring-LWE) problem [16, 5] is a generalisation of the LWE problem from the ring of integers to certain other number field rings. Both the LWE problem and the Ring-LWE problem are related to well-studied lattice problems that are believed to be hard [1, 5, 6, 9, 13, 12].

Definition 4 ([16, 5]). Let R be the ring of integers of a number field K. Let $q \geq 2$ be an integer modulus. Let $R^\vee$ be the dual fractional ideal of R. 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 generated by choosing $a \leftarrow R_q$ uniformly at random, choosing $e \leftarrow \chi$ and outputting

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

Let Ψ be a family of distributions over $K_\mathbb{R}$. The *Search Ring-LWE* problem is defined as follows: given access to arbitrarily many independent samples from $A_{s,\chi}$ for some arbitrary $s \in R_q^\vee$ and $\chi \in \Psi$, find s.

Let Υ be a distribution over a family of error distributions, each over $K_\mathbb{R}$. The *average-case Decision Ring-LWE* problem is to distinguish with non-negligible advantage between arbitrarily many independent samples from $A_{s,\chi}$ for a random choice of $(s, \chi) \leftarrow \mathcal{U}\left(R_q^\vee\right) \times \Upsilon$, and the same number of uniformly random samples from $R_q \times K_\mathbb{R}/qR^\vee$. □

2.3 Moment generating functions

The moment generating function is a basic tool of probability theory, and we first give a definition for a univariate random variable.

Definition 5. 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

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

Fundamental results underlying the utility of the moment generating function are given in Lemma 1.

Lemma 1 ([3]). 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. □

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

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

The definition of a moment generating function for a real-valued univariate random variable generalises to multivariate random variables and to random variables on H, and the above results also generalise in the appropriate way.

Definition 6. The *moment generating function* M_W 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

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

Definition 7. The *moment generating function* M_W of a multivariate random variable W on H is the function from a subset of H to $\mathbb{R}$ defined by

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

2.4 Subgaussian random variables

In Lemma 2 we recall the standard result for the moment generating function of a Normal random variable with mean 0.

Lemma 2 ([3]). 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

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

Lemma 2 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 a random variable is known as a *subgaussian* random variable [15] and is specified in Definition 8.

Definition 8. A real-valued random variable W is *subgaussian* with *standard parameter* $b \geq 0$ if its moment generating function M_W satisfies

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

An example of a subgaussian random variable is illustrated in Figure 1, which shows the moment generating function $M_X(t) = \cosh t$ for the subgaussian random variable X taking values ± 1 with probability $\frac{1}{2}$ (so $\mathbf{E}(X) = 0$ and $\mathrm{Var}(X) = 1$), together with its corresponding 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.

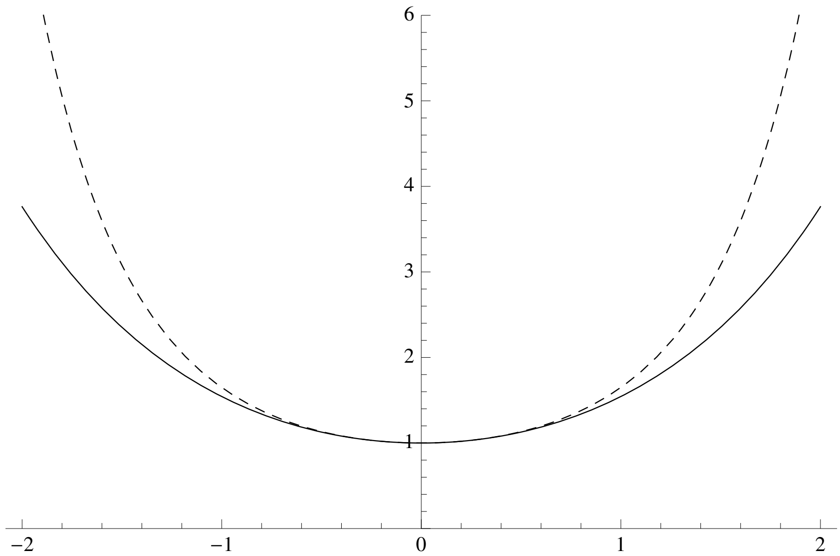

Fig. 1. Moment generating function $M_X(t) = \cosh t$ for the random variable X taking values ± 1 with probability $\frac{1}{2}$ (solid line) and subgaussian bounding function $\exp(\frac{1}{2}t^2)$ (dashed line).

3 δ-subgaussian random variables

In this section, we give a complete and particularly simple characterisation of δ-subgaussian random variables. Statistical arguments based on δ-subgaussian random variables have been widely used in Ring-LWE [7, 10, 6], as noted in Section 1. Our main result, Proposition 1, shows that a δ-subgaussian random variable (for $\delta \geq 0$) is simply a translation of some 0-subgaussian random variable.

3.1 Defining a δ-subgaussian random variable

A δ-subgaussian random variable is a generalisation of a subgaussian random variable in the following sense: δ is allowed to be any value $\delta \geq 0$, and taking the case $\delta = 0$ gives a subgaussian random variable. In other words, what is termed a 0-subgaussian random variable for example in [7, 6] is exactly a subgaussian random variable.

We now give two definitions for a univariate δ-subgaussian random variable to make this generalisation precise. Definition 9 corresponds with the usual probability theory of moment generating functions [3]. Definition 10 is used for example in [6]. Lemma 3 shows that these definitions are equivalent.

Definition 9. 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 10. 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

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

Lemma 3. A real-valued univariate random variable is δ-subgaussian with standard parameter b if and only if it is δ-subgaussian with scaled parameter $(2\pi)^{\frac{1}{2}} b$.

The definition of a univariate δ-subgaussian random variable generalises to a multivariate δ-subgaussian random variable and a δ-subgaussian random variable on H in the obvious way.

Definition 11. 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

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

Definition 12. A random variable W on H is *δ-subgaussian* ($\delta \geq 0$) with *standard parameter* $b \geq 0$ if its moment generating function M_W satisfies

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

3.2 Characterisation of univariate δ-subgaussian random variables

In this section, we give a complete 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.

We firstly recall in Lemma 4 a property of 0-subgaussian random variables proved in [15], namely that their mean is 0. This can be heuristically explained as follows. Lemma 1(i) shows that any moment generating function must pass through $(0, 1)$. However, a 0-subgaussian bounding function $\exp(\frac{1}{2} b^2 t^2)$ also passes through $(0, 1)$ and has derivative 0 at 0. Thus any moment generating function bounded by $\exp(\frac{1}{2} b^2 t^2)$ must have derivative 0 at 0. Lemma 1(ii) then shows that such a 0-subgaussian random variable with moment generating function bounded by $\exp(\frac{1}{2} b^2 t^2)$ must have mean 0.

Lemma 4 ([15]). If W is a univariate real-valued 0-subgaussian random variable, then $\mathbf{E}(W) = 0$. $\square$

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 2 for a random variable with mean 1.

Intuitively, relaxing the constraint that $\delta = 0$ in the δ-subgaussian bounding function $\exp(\delta) \exp(\frac{1}{2} b^2 t^2)$ essentially shifts the bounding function "up the

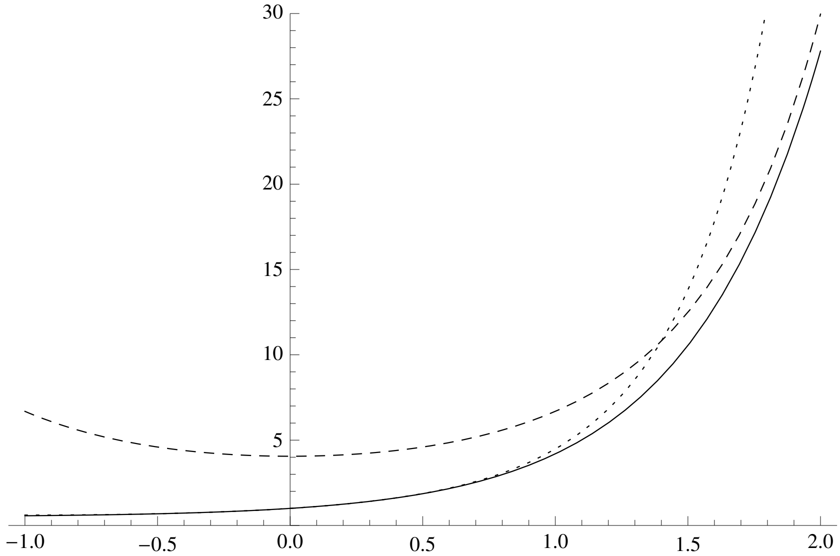

Fig. 2. Moment generating function $M_{X+1}(t) = \frac{1}{2}(1+\exp(2t))$ for the random variable $X+1$ (for $X \sim \text{Uni}(\{-1,1\})$ of Figure 1) taking values 0 and 2 with probability $\frac{1}{2}$ and having mean 1 (solid line), δ-subgaussian bounding function $\exp(\frac{7}{5} + \frac{1}{2}t^2)$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

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 2 more precise in a number of ways. First, Lemma 5 shows that any δ-subgaussian random variable with mean 0 must be a 0-subgaussian random variable.

Lemma 5. 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

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

where a function $g(t) = o(t^2)$ in the infinitesimal sense near 0 if $t^{-2}g(t) \to 0$ as $t \to 0$. 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

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

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

$$M_W(t) \le \exp(\delta)\exp(\tfrac{1}{2}b^2t^2) = \exp(\delta)\exp(\tfrac{1}{2}d^2t^2)\exp(-\delta\nu^{-2}t^2)$$
$$\le \exp(\delta(1-\nu^{-2}t^2))\exp(\tfrac{1}{2}d^2t^2) \le \exp(\tfrac{1}{2}d^2t^2) \qquad [|t| \ge \nu].$$

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

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

Thus W is a 0-subgaussian random variable. □

Next, Lemma 6 shows that shifting a δ-subgaussian random variable by its mean results in a 0-subgaussian random variable.

Lemma 6. If W is a univariate real-valued δ-subgaussian random variable ($\delta \ge 0$), 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 5 therefore shows that $W_0 = W - \mathbf{E}(W)$ is a 0-subgaussian random variable. □

Finally, Lemma 7 shows that any shift of a δ_0-subgaussian random variable with mean 0 is a δ-subgaussian random variable for some $\delta \geq 0$.

Lemma 7. If W_0 is a univariate real-valued δ_0-subgaussian random variable with mean $\mathbf{E}(W_0) = 0$, then for $\beta \in \mathbb{R}$ the real-valued shifted random variable $W = W_0 + \beta$ 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 5 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 $\delta \geq \dfrac{\beta^2}{2(b^2 - c^2)}$, then we note that

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

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

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

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

Lemmas 5, 6 and 7 collectively give the main result Proposition 1 of this section. Proposition 1 precisely characterises δ-subgaussian random variables as shifts of 0-subgaussian random variables, which must have mean 0.

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:

δ*-subgaussian univariate RV* $=$ 0*-subgaussian univariate RV* $+$ *constant.* □

3.3 Properties of δ-subgaussian random variables

In this section, we give some basic properties of δ-subgaussian random variables. These are analogous to well-known properties of subgaussian random variables, given for example in [15].

Lemma 8. 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) $\text{Var}(W) \leq b^2$, (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 9. The set of δ-subgaussian random variables form a linear space. □

Lemma 10. 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. However, Theorem 2.5 of [15] or Theorem 9.9 of [17] shows that a bounded random variable with mean 0, such as W_0, is a 0-subgaussian random variable. Thus Lemma 7 shows that $W = W_0 + \mathbf{E}(W)$ is a δ-subgaussian random variable for some $\delta \geq 0$. □

4 Noncentral Subgaussian Random Variables

Proposition 1 shows that the class of δ-subgaussian random variables are precisely those random variables that can be obtained as shifts of 0-subgaussian random variables. In this section, we use this characterisation to give an alternative noncentral formulation for a δ-subgaussian random variable. We then use this formulation to analyse sums and products of δ-subgaussian random variables. Our main result is Theorem 1, which generalises a result of [6] on sums of δ-subgaussian random variables.

4.1 A noncentral formulation for δ-subgaussian random variables

Proposition 1 enables us to see a δ-subgaussian random variable as a shifted 0-subgaussian random variable. This motivates the following definition.

Definition 13. A random variable Z (on $\mathbb{R}^l$ or H) is a *noncentral subgaussian* random variable with *standard parameter* $d \geq 0$ if the centred random variable $Z - \mathbf{E}(Z)$ is a 0-subgaussian random variable with standard parameter d. $\square$

Lemma 11 establishes the equivalence of the δ-subgaussian and noncentral subgaussian definitions. Lemma 11 also gives a basic property of noncentral subgaussian random variables, which follows from Lemma 9.

Lemma 11. A noncentral subgaussian random variable Z (on $\mathbb{R}^l$ or H) is a δ-subgaussian random variable and vice versa, and the set of noncentral subgaussian random variables (on $\mathbb{R}^l$ or H) is a linear space. $\square$

4.2 Motivation for the noncentral formulation

In this section, we motivate the alternative noncentral formulation. We begin by specifying a noncentral subgaussian random variable in terms of its moment generating function.

Lemma 12. The random variable Z is a noncentral subgaussian random variable (on $\mathbb{R}^l$ or H) with standard parameter d if and only if the moment generating function M_Z of Z satisfies $M_Z(t) \leq \exp\left(\langle t, \mathbf{E}(Z)\rangle\right) \exp(\frac{1}{2}d^2|t|^2)$. $\square$

Proof. If Z is a noncentral subgaussian random variable, then $Z - \mathbf{E}(Z)$ is a 0-subgaussian random variable with standard parameter d and so has moment generating function $M_{Z-\mathbf{E}(Z)}$ satisfying $M_{Z-\mathbf{E}(Z)}(t) \leq \exp(\frac{1}{2}d^2|t|^2)$. Thus M_Z satisfies $M_Z(t) = M_{\mathbf{E}(Z)}(t)\, M_{Z-\mathbf{E}(Z)}(t) \leq \mathbf{E}(\exp(\langle t, \mathbf{E}(Z)\rangle))\, \exp(\frac{1}{2}d^2|t|^2)$.

Conversely, if $M_Z(t) \leq \exp\left(\langle t, \mathbf{E}(Z)\rangle\right) \exp(\frac{1}{2}d^2|t|^2) = M_{\mathbf{E}(Z)}(t) \exp(\frac{1}{2}d^2|t|^2)$, then $Z - \mathbf{E}(Z)$ has moment generating function $M_{Z-\mathbf{E}(Z)} = M_Z M_{-\mathbf{E}(Z)}$ satisfying $M_{Z-\mathbf{E}(Z)}(t) = M_{\mathbf{E}(Z)}(t) \exp(\frac{1}{2}d^2|t|^2) M_{-\mathbf{E}(Z)}(t) \leq \exp(\frac{1}{2}d^2|t|^2)$. Thus $Z - \mathbf{E}(Z)$ is a 0-subgaussian random variable with standard parameter d, and so Z is a noncentral subgaussian random variable with standard parameter d. $\square$

We now argue that the noncentral subgaussian formulation is more natural from a statistical point of view, for the following reasons.

Firstly, the bounding function of Lemma 12 allows us to directly compare such a noncentral subgaussian random variable with a corresponding Normal random variable. Figure 2 illustrates an example of a noncentral subgaussian bounding function and a δ-subgaussian bounding function. It can be seen that this noncentral subgaussian bounding function is a tight bounding function to the moment generating function at 0, and hence captures better the behaviour at 0. Moreover, the noncentral subgaussian bounding function is actually a moment generating function of some Normal random variable.

Secondly, the standard parameter of a noncentral subgaussian random variable is invariant under translation of the random variable, mirroring a fundamental property of standard deviation. By contrast, in Example 1 we show that the standard parameter of a δ-subgaussian random variable is not necessarily invariant under translation.

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 13, it is clear that W is a noncentral subgaussian random variable with mean 0 and standard parameter σ. Similarly, the translated random variable $W + a \sim \mathrm{N}(a, \sigma^2)$ is by definition a noncentral random variable with mean a and standard parameter σ.

In terms of Definition 9, 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 $a \neq 0$. □

4.3 Sums of univariate noncentral subgaussian random variables

In this section, we give our main result, Theorem 1, on sums of noncentral subgaussian (equivalently δ-subgaussian) random variables. This a far more general result than previous results [10, 6] on sums of δ-subgaussian random variables, which apply only in restricted settings. For example, [10, Fact 2.1] applies when the summands are independent, and [6, Claim 2.1] applies in a martingale-like setting.

Theorem 1. Suppose that $W_1, \ldots, W_l$ are noncentral subgaussian, or equivalently δ-subgaussian, random variables where W_j has standard parameter $d_j \geq 0$ for $j = 1, \ldots, l$.
(i) The sum $\sum_{j=1}^{l} W_j$ is a noncentral subgaussian random variable with mean $\sum_{j=1}^{l} \mathbf{E}(W_j)$ and standard parameter $\sum_{j=1}^{l} d_j$.
(ii) If $W_1, \ldots, W_l$ are independent, then the standard 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 standard 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 [15] 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 mean $\sum_{j=1}^{l} \mathbf{E}(W_j)$ and standard parameter $\sum_{j=1}^{l} d_j$. The second (independence) result similarly follows from the independence result of Theorem 2.7 of [15]. □

5 Discretisation

Discretisation is a fundamental part of Ring-LWE cryptography in which 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 [6, Section 2.4.2] or *CRR-discretisation*, as an illustration of a discretisation process, though most of our comments apply more generally.

We begin by giving a formal definition of CRR-discretisation in terms of a Balanced Reduction function. This allows us to establish general results about the CRR-discretisation of δ-subgaussian random variables. In particular, our main result is Theorem 2, which improves prior results [6] for the δ-subgaussian standard parameter of the CRR-discretisation of a δ-subgaussian random variable.

5.1 Coordinate-wise Randomised Rounding Discretisation

In this section we describe the coordinate-wise randomised rounding discretisation method of the first bullet point of [6, Section 2.4.2], which we term CRR-discretisation. We first introduce the Balanced Reduction function in Definition 14, and give its basic properties in Lemma 13.

Definition 14. The univariate *Balanced Reduction* function $\mathcal{R}$ on $\mathbb{R}$ is the random function with support on $[-1,1]$ given by

$$\mathcal{R}(a) = \begin{cases} 1-(\lceil a\rceil - a) & \text{with probability} \quad \lceil a\rceil - a \\ -(\lceil a\rceil - a) & \text{with probability} \;\; 1-(\lceil a\rceil - a). \end{cases}$$

The multivariate *Balanced Reduction* function $\mathcal{R}$ on $\mathbb{R}^l$ with support on $[-1,1]^l$ is the random function $\mathcal{R} = (\mathcal{R}_1, \dots, \mathcal{R}_l)$ with component functions $\mathcal{R}_1, \dots, \mathcal{R}_l$ that are independent univariate Balanced Reduction functions. □

Lemma 13. The random variable $\mathcal{R}(a) + (\lceil a\rceil - a) \sim \mathrm{Bern}(\lceil a\rceil - a)$ has a Bernoulli distribution for any $a \in \mathbb{R}$, and the random variable $\mathcal{R}(a)$ satisifies (i) $\mathbf{E}(\mathcal{R}(a)) = 0$, (iii) $\mathrm{Var}(\mathcal{R}(a)) \le \frac{1}{4}$ and (iii) $a - \mathcal{R}(a) \in \{\lfloor a\rfloor, \lceil a\rceil\} \subset \mathbb{Z}$. □

We are now in a position to define CRR-discretisation in terms of the Balanced Reduction function.

Definition 15. Suppose B is a (column) basis matrix for the n-dimensional lattice Λ in H. If $\mathcal{R}$ is the Balanced Reduction function, then the *coordinate-wise randomised rounding discretisation* or *CRR-discretisation* $\lfloor X \rceil^B_{\Lambda+c}$ of the random variable X to the lattice coset $\Lambda + c$ with respect to the basis matrix B is the random variable

$$\lfloor X \rceil^B_{\Lambda+c} = X + B\,\mathcal{R}\left(B^{-1}(c-X)\right). \qquad \square$$

In Lemma 14 we show that the specification of coordinate-wise randomised rounding in Definition 15 is well-defined.

Lemma 14. The CRR-discretisation $\lfloor X \rceil^B_{\Lambda+c}$ of the random variable X with resect to the (column) basis B is (i) a random variable on the lattice coset $\Lambda+c$, (ii) is *valid* (does not depend on the chosen coset representative c) and (iii) has mean $\mathbf{E}(\lfloor X \rceil^B_{\Lambda+c}) = \mathbf{E}(X)$. □

Proof. For part (i), the CRR-discretisation can be expressed as

$$\begin{aligned}\lfloor X \rceil^B_{\Lambda+c} &= X + B\mathcal{R}\left(B^{-1}(c-X)\right) = B\left(B^{-1}X + \mathcal{R}\left(B^{-1}(c-X)\right)\right) \\ &= c - B\left(B^{-1}(c-X) - \mathcal{R}\left(B^{-1}(c-X)\right)\right) \\ &\in \Lambda + c,\end{aligned}$$

as Lemma 13(iii) shows that $B^{-1}(c-X) - \mathcal{R}\left(B^{-1}(c-X)\right)$ is a random variable on $\mathbb{Z}^n$. For part (ii), if $c' \in \Lambda+c$, so $c-c' \in \Lambda$, then there exists an integer vector z such that $c-c' = Bz$, so $B^{-1}(c-X) - B^{-1}(c'-X) = z$, that is to say $B^{-1}(c-X)$ and $B^{-1}(c'-X)$ differ by an integer vector. Thus $\mathcal{R}\left(B^{-1}(c-X)\right)$ and $\mathcal{R}\left(B^{-1}(c'-X)\right)$ have 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*. Finally, for part (iii), Lemma 13(i) shows that $\mathbf{E}(\lfloor X \rceil^B_{\Lambda+c}) = \mathbf{E}(X) + B\mathbf{E}\left(\mathcal{R}\left(B^{-1}(c-X)\right)\right) = \mathbf{E}(X)$. □

5.2 The CRR-Discretisation of δ-Subgaussian Random Variables

In this section we examine the subgaussian properties of the CRR-discretisation of a noncentral subgaussian random variable. Our main result is Theorem 2, which gives a subgaussian standard parameter for such a CRR-discretisation arising in Ring-LWE, that is to say discretisation for a lattice in H. Theorem 2 uses a factor of $\frac{1}{2}$ with the standard parameter of a random variable obtained by such a CRR-discretisation. By contrast, any comparable result in [6] uses a factor of 1 (see for example the first bullet point of [6, Section 2.4.2]). Thus the results of this Section improve and extend any comparable result in [6] about a CRR-discretisation of a δ-subgaussian random variable.

We first give in Lemma 15 the subgaussian property of the (multivariate) Balanced Reduction function.

Lemma 15. The (multivariate) Balanced Reduction $\mathcal{R}(v)$ (Definition 14) is a 0-subgaussian random variable with standard parameter $\frac{1}{2}$ for all $v \in \mathbb{R}^l$. □

Proof. We first consider the univariate random variable $R_j = \mathcal{R}(p)$ given by the Balanced Reduction of the constant p, where $0 \leq p \leq 1$ without loss of generality. Thus R_j takes the value p with probability $1-p$ and the value $p-1$ with probability p, so 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

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

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 $M_{R_j}(t) = \exp(g(t)) \leq \exp(\frac{1}{2}(\frac{1}{2})^2 t^2)$, so R_j is a 0-subgaussian random variable with standard parameter $\frac{1}{2}$.

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

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

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

We now give in Theorem 2 a subgaussian standard parameter for a CRR-discretisation. The details of the CRR-discretisation depend on the lattice basis used, and in particular on the spectral norm of a lattice basis matrix.

Theorem 2. Suppose that B is a (column) basis matrix for a lattice Λ in H with spectral norm $\lambda(B)$. If Z is a noncentral subgaussian random variable with standard parameter b, then its CRR-discretisation $\lfloor Z \rceil^B_{\Lambda+c}$ is a noncentral subgaussian random variable with mean $\mathbf{E}(Z)$ and standard parameter $\left(b^2 + (\frac{1}{2}\lambda(B))^2\right)^{\frac{1}{2}}$. □

Proof. Lemma 14(iii) shows that $\lfloor Z \rceil^B_{\Lambda+c} = Z + B\mathcal{R}(B^{-1}(c - Z))$ has mean $\mathbf{E}(Z)$. For $v \in H$, Lemma 15 allows us to bound the relevant conditional expectation as

$$\begin{aligned}
\mathbf{E}\left(\exp\left(v^\dagger \lfloor Z \rceil^B_{\Lambda+c}\right) \big|\, Z=z\right) &= \mathbf{E}\left(\exp\left(v^\dagger \left(z + B\mathcal{R}(B^{-1}(c-z))\right)\right)\right) \\
&= \exp(v^\dagger z)\ \mathbf{E}\left(\exp\left(v^\dagger B\mathcal{R}(B^{-1}(c-z))\right)\right) \\
&= \exp(v^\dagger z)\ \mathbf{E}\left(\exp\left((B^\dagger v)^\dagger \mathcal{R}(B^{-1}(c-z))\right)\right) \\
&= \exp(v^\dagger z)\ M_{\mathcal{R}(B^{-1}(c-z))}\left(B^\dagger v\right) \\
&\leq \exp(v^\dagger z)\ \exp\left(\tfrac{1}{2}(\tfrac{1}{2})^2 |B^\dagger v|^2\right) \\
&\leq \exp(v^\dagger z)\ \exp\left(\tfrac{1}{2}(\tfrac{1}{2}\lambda(B))^2 |v|^2\right),
\end{aligned}$$

so the corresponding conditional expectation random variable is bounded as

$$\mathbf{E}\left(\exp\left(v^\dagger \lfloor Z \rceil^B_{\Lambda+c}\right) \big|\, Z\right) \leq \exp(v^\dagger Z)\ \exp\left(\tfrac{1}{2}(\tfrac{1}{2}\lambda(B))^2 |v|^2\right).$$

Thus the Law of Total Expectation shows that the moment generating function $M_{\lfloor Z \rceil^B_{\Lambda+c}}$ of the discretisation $\lfloor Z \rceil^B_{\Lambda+c}$ is bounded by

$$\begin{aligned}
M_{\lfloor Z \rceil^B_{\Lambda+c}}(v) = \mathbf{E}\left(\exp\left(v^\dagger \lfloor Z \rceil^B_{\Lambda+c}\right)\right) &= \mathbf{E}\left(\mathbf{E}\left(\exp\left(v^\dagger \lfloor Z \rceil^B_{\Lambda+c}\right) \big|\, Z\right)\right) \\
&\leq \exp\left(\tfrac{1}{2}(\tfrac{1}{2}\lambda(B))^2 |v|^2\right)\ \mathbf{E}\left(\exp(v^\dagger Z)\right) \\
&= \exp\left(\tfrac{1}{2}(\tfrac{1}{2}\lambda(B))^2 |v|^2\right) M_Z(v) \\
&\leq \exp\left(\tfrac{1}{2}(\tfrac{1}{2}\lambda(B))^2 |v|^2\right) \exp(v^\dagger \mathbf{E}(Z)) \exp(\tfrac{1}{2} b^2 |v|^2) \\
&\leq \exp(v^\dagger \mathbf{E}(Z)) \exp\left(\tfrac{1}{2}\left(b^2 + (\tfrac{1}{2}\lambda(B))^2\right)\right)
\end{aligned}$$

as Z is a noncentral subgaussian random variable with standard parameter b. Thus its discretisation $\lfloor Z \rceil^B_{\Lambda+c}$ is a noncentral subgaussian random variable with standard parameter $\left(b^2 + (\frac{1}{2}\lambda(B))^2\right)^{\frac{1}{2}}$. □

Acknowledgements

We thank the anonymous referees for their comments on previous versions of this paper, and we thank Carlos Cid for his interesting discussions about this paper. Rachel Player was supported by an ACE-CSR Ph.D. grant, by the French Programme d'Investissement d'Avenir under national project RISQ P141580, and by the European Union PROMETHEUS project (Horizon 2020 Research and Innovation Program, grant 780701).

References

1. 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.
2. N. Genise, D. Micciancio, and Y. Polyakov. Building an Efficient Lattice Gadget Toolkit: Subgaussian Sampoling and More. In Y. Ishai and V. Rijmen, editors, *Eurocrypt 2019*, volume 11478 of *LNCS*. Springer, 2019.
3. G. Grimmett and D. Stirzaker. *Probability And Random Processes.* Oxford University Press, third edition, 2001.
4. J. Kahane. Propriétés locales des fonctions à séries de Fourier aléatoires. *Studia Mathematica*, 19:1–25, 1960.

5. V. Lyubashevsky, C. Peikert, and O. Regev. On Ideal Lattices and Learning with Errors Over Rings. *IACR Cryptology ePrint Archive*, 2012:230, 2012.
6. V. Lyubashevsky, C. Peikert, and O. Regev. A Toolkit for Ring-LWE Cryptography. *IACR Cryptology ePrint Archive*, 2013:293, 2013.
7. 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.
8. 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.
9. 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.
10. C. Peikert. Lattice Cryptography for the Internet. In M. Mosca, editor, *PQCrypto 2014*, volume 8772 of *LNCS*, pages 197–219, Springer, 2014.
11. C. Peikert. A Decade of Lattice Cryptography. *IACR Cryptology ePrint Archive*, 2015:939, 2016.
12. C. Peikert, O. Regev, and N. Stephens-Davidowitz. Pseudorandomness of Ring-LWE for any Ring and Modulus. In H. Hatami, P. McKenzie, and V. King, editors, *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017*, pages 461–473, 2017.
13. 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.
14. O. Regev. The Learning with Errors Problem (Invited Survey). In *IEEE Conference on Computational Complexity*, pages 191–204, 2010.
15. O. Rivasplata. Subgaussian Random Variables: An Expository Note. Available at `http://www.stat.cmu.edu/~arinaldo/36788/subgaussians.pdf`, 2015.
16. D. Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa. Efficient Public Key Encryption Based on Ideal Lattices. In M. Matsui, editor, *Advances in Cryptology - ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 617–635, 2009.
17. K.R. Stromberg. *Probability for Analysts*. Chapman and Hall, 1994.