Discretisation and Product Distributions in Ring-LWE

Sean Murphy and Rachel Player

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

Abstract. A statistical framework applicable to Ring-LWE was outlined by Murphy and Player (IACR eprint 2019/452). Its applicability was demonstrated with an analysis of the decryption failure probability for degree-1 and degree-2 ciphertexts in the homomorphic encryption scheme of Lyubashevsky, Peikert and Regev (IACR eprint 2013/293). In this paper, we clarify and extend results presented by Murphy and Player. Firstly, we make precise the approximation of the discretisation of a Normal random variable as a Normal random variable, as used in the encryption process of Lyubashevsky, Peikert and Regev. Secondly, we show how to extend the analysis given by Murphy and Player to degree-k ciphertexts, by precisely characterising the distribution of the noise in these ciphertexts.

Keywords. Ring-LWE, Discretisation, Homomorphic Encryption.

1 Introduction

The Ring-LWE problem [12, 6] has become a standard hard problem underlying lattice-based cryptography. In [7], a detailed algebraic background for Ring-LWE was given, together with a statistical framework based on δ-subgaussian random variables [9, 10]. Another statistical framework applicable to Ring-LWE, based on a Central Limit approach, was outlined in [11]. It is argued in [11] that this is a more natural approach than one using δ-subgaussian arguments, when considering the important application setting of homomorphic encryption [5].

Ciphertexts in all homomorphic encryption schemes have an inherent *noise* which is small in fresh ciphertexts and grows during homomorphic evaluation operations. If the noise grows too large, decryption will fail. A thorough understanding of the statistical properties of the noise is therefore essential for choosing efficient parameters while ensuring correctness. Rather than analysing the noise directly, we consider the embedding of the noise via the *canonical embedding* (see e.g. [7]) in a complex space H.

In this paper, we present results on discretisation and product distributions applicable to Ring-LWE cryptography, which clarify and extend results presented in [11]. For concreteness, these results could be applied to the homomorphic encryption scheme of Section 8.3 of [7], termed `SymHom` by [11] and analysed there.

In a Ring-LWE discretisation, an element of the complex space H is rounded to some randomly determined nearby element of H in a lattice coset $\Lambda + c$. We require that all components of the vector expressing this discretisation in an appropriate basis for H are bounded by an appropriate threshold in order for a successful decryption to take place. The statistical properties of the discretisation process are therefore of fundamental importance in determining correctness. Our results demonstrate how we can obtain a good multivariate Normal approximation for (embedded) noise of a degree-1 (fresh) ciphertext vector expressed in a decryption basis after a change of basis transformation. This justifies the approach used in [11, Theorem 1] for bounding the decryption failure probability of such ciphertexts.

In homomorphic Ring-LWE cryptosystems such as SymHom, for $k = k_1 + k_2$, a degree-k ciphertext c_{mult} is formed as the result of the homomorphic multiplication of two ciphertexts c_1 and c_2 of degrees k_1 and k_2 respectively. The noise in c_{mult} is defined to be the product of the noises in the input ciphertexts c_1 and c_2. We show that using the Central Limit Framework of [11], the distribution of a vector expressing the (embedded) noise in a degree-k SymHom ciphertext in an appropriate decryption basis can be approximated by a multivariate Normal distribution. This extends the analysis for degree-2 ciphertexts given in [11, Theorem 2].

1.1 Contributions

In Section 3 we make precise the approximation of the *CRR discretisation* (Definition 5) of a Normal random variable as a Normal random variable, so potentially allowing a more direct and powerful approach to CRR discretisation than a δ-subgaussian approach. Moreover, our techniques are potentially generalisable to other randomised discretisation methods. Our first main result is Proposition 1, which describes the distribution of the *Balanced Reduction* (Definition 4) of a Normal random variable. To obtain Proposition 1, we first show in Lemma 1 that the Balanced Reduction of a Normal random variable gives a Triangular distribution, which is itself approximately by a Normal distribution (Lemma 2).

In Section 4 we extend the analysis of degree-2 ciphertexts given in [11] to degree-k ciphertexts. Our second main result is Lemma 6, which shows that a component $Z_j^{(k)}$ of the k-fold $\otimes$-product $Z^{(k)}$ has a $\mathcal{K}$ *distribution* (Section 4.1).

2 Background

In this section, we give the relevant background for our discussion. In Section 2.1 we recall the necessary algebraic background to Ring-LWE, following [7]. In Section 2.2 we recall results on discretisation following [10]. In Section 2.3 we recall the definition and basic properties of the Meijer G-Function [2–4].

2.1 Algebraic Background

The mathematical structure underlying Ring-LWE is the polynomial quotient ring obtained from the m^{th} cyclotomic polynomial of degree n. For simplicity, we consider the case where m is a large prime, so $n = \phi(m) = m - 1$, and we let $n' = \frac{1}{2}n$. Our focus is solely on the vector space aspects of Ring-LWE, and in particular our discussion is based on the complex space H (Definition 1).

Definition 1. *The* conjugate pair space H *is* $H = T(\mathbb{R}^n)$, *where* T *is the* $n \times n$ *unitary* conjugate pairs matrix *given by* $T = 2^{-\frac{1}{2}} \left(\begin{array}{c|c} I_{n'} & iJ_{n'} \\ \hline J_{n'} & -iI_{n'} \end{array}\right)$, *where* $I_{n'}$ *is the* $n' \times n'$ *identity matrix and* $J_{n'}$ *is the* $n' \times n'$ *reverse diagonal matrix of* 1*s.*

We note that $T^{-1} = T^\dagger$, where $T^\dagger$ denotes the conjugate transpose of T. We can represent elements of H as vectors with respect to a basis for H, and two such bases of H of direct relevance are specified in Definition 2.

Definition 2. *The* I-basis *for* H *is given by the columns of the* $n \times n$ *identity matrix* I_n*, that is to say by standard basis vectors. The* T-basis *for* H *is given by the columns of the conjugate pair matrix* T*.*

We note that an element of H is expressed as a vector in the I-basis as a vector of n' conjugate pairs and by construction in the T-basis as a *real-valued* vector. A vector expressing the same element of H in the I-basis has the same norm as a vector expressing the same element in the T-basis as T is a unitary matrix ($|Tv|^2 = |v|^2$). Furthermore, the complex space H has a natural well-defined multiplication operation, and Definition 3 specifies this multiplication operation for vector expressing an element of H in the I-basis and in the T-basis.

Definition 3. *If* $a = (a_1 \ldots a_n)^T$ *and* $b = (b_1, \ldots, b_n)^T$ *are vectors expressing elements of* H *in the* I*-basis for* H*, then the* $\odot$*-product* $a \odot b = (a_1 b_1, \ldots, a_n b_n)^T$ *is their componentwise product. If* u *and* v *are (real-valued) vectors expressing elements of* H *in the* T*-basis for* H*, then the* $\otimes$*-product* $u \otimes v = T^\dagger\,(Tu \odot Tv)$*.*

The $\otimes$-product of two real-valued vectors can be expressed by considering appropriate pairs of components. The space H can be regarded as $H_2 \times \ldots \times H_2$, where $H_2 = T(\mathbb{R}^2)$. For two real-valued vectors $u, v \in \mathbb{R}^2$ expressing elements of H_2 in the T-basis for H_2, their $\otimes$-product is given by

$$u \otimes v = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} \otimes \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = 2^{-\frac{1}{2}} \begin{pmatrix} u_1 v_1 - u_2 v_2 \\ u_1 v_2 + u_2 v_1 \end{pmatrix} .$$

2.2 Discretisation Background

The discretisation process in (for example) a homomorphic Ring-LWE cryptosystem "rounds" an element of H to some randomly determined nearby element of H in a lattice coset $\Lambda + c$ of some lattice Λ in H. As an illustration of a discretisation process, we use the coordinate-wise randomised rounding method of discretisation or *CRR discretisation* given in the first bullet point of Section 2.4.2 of [7]. We give a formal statistical description of CRR discretisation in terms of a random *Balanced Reduction* function following [10].

Definition 4. *The univariate* Balanced Reduction *function $\mathcal{R}$ on $\mathbb{R}$ is the random function* $\mathcal{R}(a) = \begin{cases} 1-(\lceil a\rceil - a) & \textit{with probability} \quad \lceil a\rceil - a \\ -(\lceil a\rceil - a) & \textit{with probability} \;\; 1-(\lceil a\rceil - a). \end{cases}$

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

Definition 5. *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 on H to the lattice coset $\Lambda + c$ with respect to the basis matrix B is the random variable*

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

The CRR discretisation $\lfloor X\rceil^B_{\Lambda+c}$ of the random variable X with respect to the basis B of Λ is a random variable on the lattice coset $\Lambda + c$, and is a valid (does not depend on the chosen coset representative c) discretisation [7, 10].

2.3 Meijer *G*-Functions

Our analysis in Section 4 will be most easily expressed in terms of Meijer G-functions [2–4], which are specified in general in Definition 6. Definition 7 gives three classes of Meijer G-functions that are of direct relevance to us.

Definition 6. *The* Meijer G-Function $G^{\xi\;\nu}_{p\;q}\left(\begin{smallmatrix} a_1\ldots a_p \\ b_1\ldots b_q\end{smallmatrix}\middle|\, x\right)$ *is defined for $x \neq 0$ and integers ξ,ν,p,q with $0 \le \xi \le q$ and $0 \le \nu \le p$ by the line integral*

$$G^{\xi\;\nu}_{p\;q}\left(\begin{smallmatrix} a_1\ldots a_p \\ b_1\ldots b_q\end{smallmatrix}\middle|\, x\right) = \frac{1}{2\pi i}\int_L \frac{\prod_{j=1}^{\xi}\Gamma(b_j - s)\prod_{j=1}^{\nu}\Gamma(1-a_j+s)}{\prod_{j=\xi+1}^{q}\Gamma(1-b_j+s)\prod_{j=\nu+1}^{p}\Gamma(a_j - s)} x^s\, ds$$

in the complex plane, where Γ denotes the gamma function and $a_k - b_j \neq 1,2,\ldots$ (for $j = 1,\ldots,\xi$ and $k = 1,\ldots,\nu$). The integral path L runs from $-i\infty$ to $i\infty$ such that all poles of $\Gamma(b_j - s)$ are to the right of the path (for $j = 1,\ldots,\xi$) and all the poles of $\Gamma(1-a_k+s)$ are to the left of the path (for $k = 1,\ldots,\nu$), though other paths are possible.

Definition 7. *For a positive integer k and the integral path L of Definition 6, the functions $\mathcal{G}_k$, $\mathcal{H}_k$ and $\mathcal{J}_k$ are the Meijer-G functions given by*

$$\begin{aligned} \mathcal{G}_k(x) = {}& G^{k\;0}_{0\;k}\left(\,{}_{00\ldots0}\middle|\, x\right) &&= \frac{1}{2\pi i}\int_L \Gamma(-s)^k x^s\, ds, \\ \mathcal{H}_k(x) = {}& G^{k-1\;1}_{1\;k-1}\left(\begin{smallmatrix} 1 \\ 11\ldots1\end{smallmatrix}\middle|\, x\right) &&= \frac{1}{2\pi i}\int_L \Gamma(1-s)^{k-1}\Gamma(s) x^s\, ds \\ \textit{and } \mathcal{J}_k(x) = {}& G^{k\;0}_{0\;k}\left(\,{}_{0\frac{1}{2}\ldots\frac{1}{2}}\middle|\, x\right) &&= \frac{1}{2\pi i}\int_L \Gamma(-s)\Gamma(\tfrac{1}{2}-s)^{k-1} x^s\, ds. \end{aligned}$$

For small k, we note that $\mathcal{G}_1(x) = \exp(-x)$ and $\mathcal{G}_2(x) = 2K_0\left(2x^{\frac{1}{2}}\right)$, where $K_0(x) = \displaystyle\int_0^\infty \exp(-x\cosh t)\ dt$ is a modified Bessel function of the second kind [1]. Similarly, we also have $\mathcal{H}_1(x) = \exp(-x^{-1})$ and $H_2(x) = \dfrac{x}{1+x}$, as well as $\mathcal{J}_1(x) = \exp(-x)$ and $\mathcal{J}_2(x) = \pi^{\frac{1}{2}}\exp(-2x^{\frac{1}{2}})$.

3 Discretisation Distributions in Ring-LWE

In Section 3.1, we show that the Balanced Reduction of a Gaussian random variable underlying a degree-1 ciphertext in situations of interest is essentially a Triangular random variable, which can itself be approximated by a Normal random variable. In Section 3.2, we make precise the multivariate Normal approximation of the CRR discretisation of the embedded noise in a degree-1 `SymHom` ciphertext.

3.1 The Balanced Reduction of a Normal Random Variable

A Ring-LWE encryption process is based on the discretisation of Normal random variables in H. We therefore consider the discretisation $\lfloor X \rceil^B_{\Lambda+c}$ of a random variable $X = TX'$ (in the I-basis) which is the image of some real-valued multivariate Normal random variable X' under T. However, $B^{-1}(c-X)$ is a real-valued multivariate Normal random variable. Thus we must consider the Balanced Reduction of $\mathcal{R}\left(B^{-1}(c-X)\right)$ of the Normal random variable $B^{-1}(c-X)$, and Lemma 1 essentially shows that such a Balanced Reduction gives a Triangular distribution.

Lemma 1. *If $Y \sim N(\mu, \sigma^2)$, then its Balanced Reduction $\mathcal{R}(Y) \to \triangle$ has the Triangular distribution $\triangle$ (density function $1 - |z|$ for $|z| < 1$ and 0 otherwise) as its limiting distribution as the standard deviation $\sigma \to \infty$.*

Sketch Proof. We can express the density function $f_{\mathcal{R}(Y)}$ of $\mathcal{R}(Y)$ in terms of the density function $f_{Y'}$ of $Y' = Y - \lfloor Y \rfloor$, the "modulo 1" reduction of Y. By considering the Fourier series for $f_{Y'}$ on $[0,1)$, we can obtain a Fourier series for $f_{\mathcal{R}(Y)}$ on $(-1,1)$ and hence show that $f_{\mathcal{R}(Y)}(y) \to 1 - |y|$ on $(-1,1)$ as $\sigma \to \infty$. A full proof is given in Appendix A. □

The Fourier form shown in the proof of Lemma 1 (Appendix A) in fact shows that the Balanced Reduction of a Normal $\mathrm{N}(\mu, \sigma^2)$ random variable with *any* mean μ is very close to a Triangular distribution $\triangle$ with mean $\mathbf{E}(\triangle) = 0$ and variance $\mathrm{Var}(\triangle) = \frac{1}{6}$ for even a moderate standard deviation σ, as illustrated in Figure 1 for the small standard deviation $\sigma = 0.50$. Ring-LWE applications typically use a larger standard deviation than 0.5, so giving an even closer approximation.

The Triangular distribution can obviously itself be approximated by a Normal $\mathrm{N}(0, \frac{1}{6})$ distribution with the same mean $\mathbf{E}(\triangle) = 0$ and variance $\mathrm{Var}(\triangle) = \frac{1}{6}$

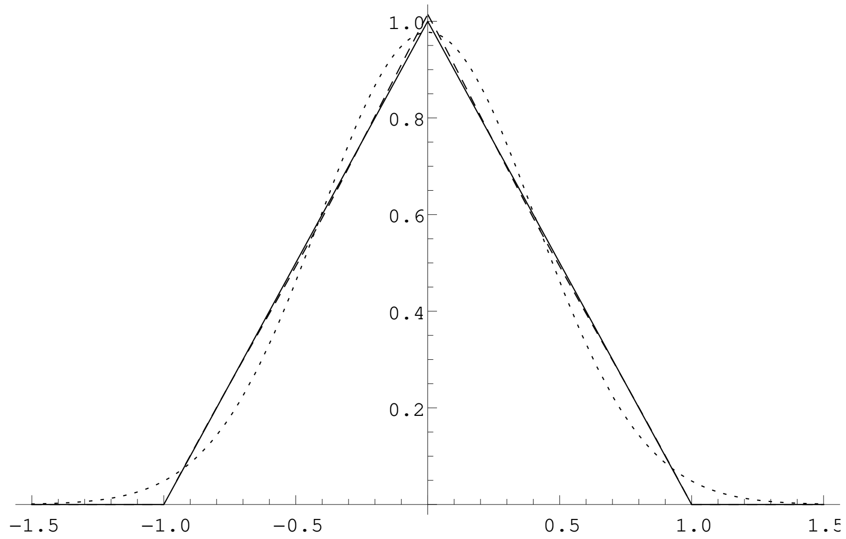

Fig. 1. The density functions of a Triangular ($\triangle$) random variable (solid line), a Balanced Reduction $\mathcal{R}(\mathrm{N}(0, 0.50^2))$ of a Normal random variable with standard deviation 0.50 (dashed line) and a Normal random variable $\mathrm{N}(0, \frac{1}{6})$ with standard deviation $(\frac{1}{6})^{\frac{1}{2}}$ (dotted line).

in the manner outlined in Lemma 2. This closeness of this approximating $\mathrm{N}(0, \frac{1}{6})$ distribution to a Triangular distribution, and essentially also to a Balanced Reduction of an $\mathrm{N}(0, \sigma^2)$ Normal random variable for $\sigma > 0.50$, is illustrated in Figure 1.

Lemma 2. *Suppose that $W \sim \triangle$ has a Triangular distribution with distribution function $F_W(w) = \mathbf{P}(W \leq w) = \frac{1}{2}\left(w + 2w - sign(w)w^2\right)$ for $|w| \leq 1$. If Φ is the distribution function of a standard Normal $N(0, 1)$ random variable, then the random variable $W' = (\frac{1}{6})^{\frac{1}{2}}\, \Phi^{-1}\left(F_W(W)\right) \sim N(0, \frac{1}{6})$ has a Normal distribution with mean 0 and variance $\frac{1}{6}$.*

Proof. If $Z \sim \mathrm{N}(0, \frac{1}{6})$, then $F_Z^{-1}(z) = (\frac{1}{6})^{\frac{1}{2}}\Phi^{-1}(z)$ is the inverse distribution function of Z. Thus the distribution function $F_{W'}$ of W' is

$$\begin{aligned} F_{W'}(w) &= \mathbf{P}\left(W' = (\tfrac{1}{6})^{\frac{1}{2}}\Phi^{-1}\left(F_W(W)\right) = F_Z^{-1}(F_W(W)) \leq w\right) \\ &= \mathbf{P}\left(W \leq F_W^{-1}(F_Z(w))\right) = F_W\left(F_W^{-1}(F_Z(w))\right) = F_Z(w). \end{aligned}$$

Thus W' and Z have the same distribution function and so $W' \sim \mathrm{N}(0, \frac{1}{6})$.

The discrepancy between the Triangular random variable $W \sim \triangle$ and the approximating Normal random variable $W' \sim \mathrm{N}(0, \frac{1}{6})$, and hence between the Balanced Reduction of an appropriate Normal distribution and an $\mathrm{N}(0, \frac{1}{6})$ distribution, is a very small distribution. This small distribution is formally specified

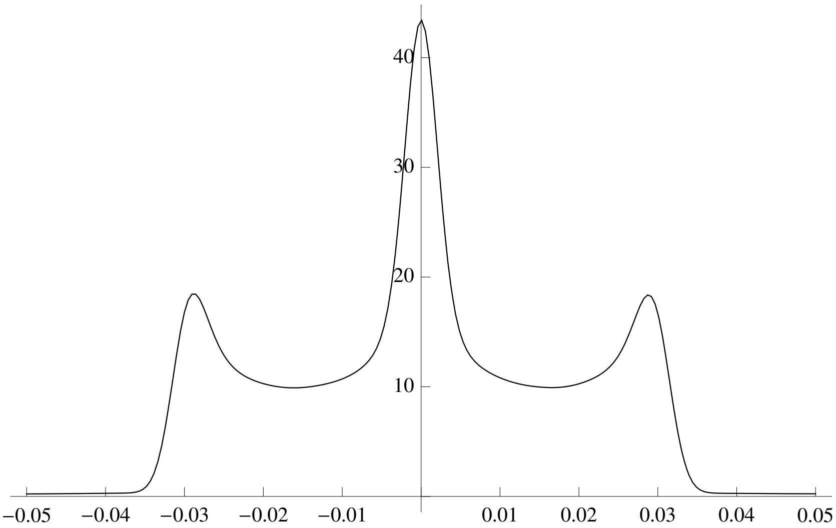

Fig. 2. The density function of a Ghost random variable.

in Definition 8 and illustrated in Figure 2, and we term this distribution the *Ghost* distribution 👻 because of its shape and elusive nature. Lemma 3 gives the statistical properties of the Ghost distribution. Proposition 1 summarises the distribution of the Balanced Reduction of a Normal random variable, using the notation $\overset{\cdot}{\sim}$ to denote "is approximately distributed as".

Definition 8. *Suppose that $W \sim \triangle$ has a Triangular distribution with distribution function $F_W(w) = \mathbf{P}(W \leq w) = \frac{1}{2}\left(w + 2w - sign(w)w^2\right)$ for $|w| \leq 1$. If Φ is the distribution function of a standard Normal $N(0,1)$ random variable, then the random variable $W'' = W - W' = W - (\frac{1}{6})^{\frac{1}{2}}\ \Phi^{-1}\left(F_W(W)\right)$ has a* Ghost *distribution. Such a random variable W'' is denoted $W'' \sim$ 👻.*

Lemma 3. *A Ghost random variable $W'' \sim$ 👻 has mean $\mathbf{E}\left(W''\right) = 0$ and variance $Var(W'') = 0.0012$, so has standard deviation $St\ Dev(W'') = 0.035$. Furthermore, the tail probabilities of W'' are given by the following Table.*

θ	0.03	0.15	0.37	0.62	0.84
$\mathbf{P}(\lvert W''\rvert > \theta)$	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}

Proof. The results can be obtained by numerical integration and so on.

Proposition 1. *The distribution of the Balanced Reduction $\mathcal{R}(N(\mu, \sigma^2))$ of a univariate Normal distribution for standard deviations σ of interest in Ring-LWE can essentially be approximated (with a slight abuse of notation) as*

$$\mathcal{R}(N(\mu, \sigma^2)) \overset{\cdot}{\sim} N(0, \tfrac{1}{6}) + 👻.$$

3.2 The Distribution of a CRR Discretisation

We consider the CRR discretisation $\lfloor X \rceil^{B}_{\Lambda+c}$ of a complex-valued random vector $X = TX'$ that is the image under T of a spherically symmetric real-valued Normal random variable $X' \sim \mathrm{N}(0; \rho^2 I_n)$ with component standard deviation ρ. This component standard deviation ρ is typically larger than the length of the basis vectors, that is to say the column lengths of B or equivalently of the real matrix $T^{\dagger}B$. We can express this CRR discretisation as either a complex-valued random vector $\lfloor X \rceil^{B}_{\Lambda+c}$ in the I-basis for H or as a real-valued random vector $T^{\dagger} \lfloor X \rceil^{B}_{\Lambda+c}$ in the T-basis for H. Following Proposition 1, the distributions of these vectors are essentially given by

$$\begin{aligned} \lfloor X \rceil^{B}_{\Lambda+c} &\mathrel{\overset{\cdot}{\underset{\cdot}{\sim}}} T(\mathrm{N}(0; \rho^2 I_n)) + B(\mathrm{N}(0; \tfrac{1}{6} I_n)) + B(\text{👻}^{n}) \\ \text{and } T^{\dagger}(\lfloor X \rceil^{B}_{\Lambda+c}) &\mathrel{\overset{\cdot}{\underset{\cdot}{\sim}}} \mathrm{N}(0; \rho^2 I_n) + T^{\dagger}B(\mathrm{N}(0; \tfrac{1}{6} I_n)) + T^{\dagger}B(\text{👻}^{n}). \end{aligned}$$

We observe that the first of these three distributions is typically the dominating distribution. For example, the real-valued distribution of $T^{\dagger}(\lfloor X \rceil^{B}_{\Lambda+c})$ differs from a Normal distribution by $T^{\dagger}B(\text{👻}^{n})$. The distribution $T^{\dagger}B(\text{👻}^{n})$ is usually negligible for the lattice basis matrices B in Ring-LWE. Similarly, the variance matrix of $T^{\dagger}B(\mathrm{N}(0; \frac{1}{6} I_n))$ is usually negligible in comparison with $\rho^2 I_n$. For practical purposes we can therefore consider that $T^{\dagger}(\lfloor X \rceil^{B}_{\Lambda+c})$ has an $\mathrm{N}(0; \rho^2 I_n)$ distribution or equivalently that $\lfloor X \rceil^{B}_{\Lambda+c}$ has a $T(\mathrm{N}(0; \rho^2 I_n))$ distribution.

In the decryption of a degree-1 ciphertext, such a discretisation (that is, the noise in the ciphertext embedded in H) is considered as a real-valued vector in a "decryption basis". An appropriate change of basis matrix C to such a decryption basis can be expressed as $C = C'T^{\dagger}$ for a real matrix C'. We therefore consider the real-valued vector $C(\lfloor X \rceil^{B}_{\Lambda+c})$ which can be expressed as

$$C(\lfloor X \rceil^{B}_{\Lambda+c}) \mathrel{\overset{\cdot}{\underset{\cdot}{\sim}}} C'(\mathrm{N}(0; \rho^2 I_n)) + CB(\mathrm{N}(0; \tfrac{1}{6} I_n)) + CB(\text{👻}^{n}) \, ,$$

where $C' = CT$ and CB are real matrices. The decryption is successful if every component of $C(\lfloor X \rceil^{B}_{\Lambda+c})$ is less than an appropriate threshold.

In summary, this discussion justifies the approach used in [11, Theorem 1] for obtaining a bound for a decryption failure probability for $C(\lfloor X \rceil^{B}_{\Lambda+c})$ by using the distributional approximation

$$C(\lfloor X \rceil^{B}_{\Lambda+c}) \mathrel{\overset{\cdot}{\underset{\cdot}{\sim}}} \mathrm{N}\left(0; \rho^2 CC'^{T}\right) \, .$$

4 Product Distributions in Ring-LWE

The noise in a degree-k ciphertext in `SymHom` can be seen as the k-fold $\odot$-product of the noises of k degree-1 ciphertexts in the I-basis for H. We are interested in the k-fold $\odot$-product of the form $\lfloor X_1 \rceil^{B}_{\Lambda+c} \odot \ldots \odot \lfloor X_k \rceil^{B}_{\Lambda+c}$ of the discretisation vectors $\lfloor X_1 \rceil^{B}_{\Lambda+c}, \ldots, \lfloor X_k \rceil^{B}_{\Lambda+c}$ given by degree-1 ciphertexts. The discussion of Section 3.2 shows that this distribution can be approximated as

$$\lfloor X_1 \rceil^{B}_{\Lambda+c} \odot \ldots \odot \lfloor X_k \rceil^{B}_{\Lambda+c} \mathrel{\overset{\cdot}{\underset{\cdot}{\sim}}} T(\mathrm{N}(0; \rho_1^2 I_n)) \odot \ldots \odot T(\mathrm{N}(0; \rho_k^2 I_n)) \, .$$

We consider the equivalent $\otimes$-product $T^\dagger(\lfloor X_1 \rceil^B_{\Lambda+c}) \otimes \ldots \otimes T^\dagger(\lfloor X_k \rceil^B_{\Lambda+c})$ expressing the embedded noises as real vectors in the T-basis, with approximate distribution

$$T^\dagger(\lfloor X_1 \rceil^B_{\Lambda+c}) \otimes \ldots \otimes T^\dagger(\lfloor X_k \rceil^B_{\Lambda+c}) \mathrel{\dot{\sim}} \mathrm{N}(0;\rho_1^2 I_n) \otimes \ldots \otimes \mathrm{N}(0;\rho_k^2 I_n).$$

The $\otimes$-product in $\mathbb{R}^n$ decomposes into $n' = \frac{1}{2}n$ independent $\otimes$-products in $\mathbb{R}^2$. Thus we consider the distribution on $\mathbb{R}^2$ given by the k-fold $\otimes$-product of spherical bivariate Normal random variables

$$\mathrm{N}(0;\rho_1^2 I_2) \otimes \ldots \otimes \mathrm{N}(0;\rho_k^2 I_2)\,.$$

In particular, we consider the distribution of a 1-dimensional component of this 2-dimensional distribution. This approach allows us to construct an approximate multivariate distribution for the vector expressing the embedded noise in an appropriate decryption basis.

4.1 The $\mathcal{K}$ Distribution

We use the $\mathcal{K}$ *distribution*, which we now introduce, to analyse the component distribution of a k-fold $\otimes$-product.

Definition 9. *A symmetric continuous univariate random variable X has a $\mathcal{K}$ distribution with* shape *k (positive integer) and* variance *$\nu^2 > 0$ if it has density function $f_X(x) = (2\pi\nu^2)^{-\frac{1}{2}} \mathcal{J}_k(\frac{1}{2}\nu^{-2}x^2)$, where $\mathcal{J}_k$ is the Meijer G-function of Definition 7. We write $X \sim \mathcal{K}(k,\nu^2)$ to denote that X has such a distribution.*

We note that an $\mathcal{K}(1,1)$ distribution is a standard Normal $\mathrm{N}(0,1)$ distribution and that $\mathcal{K}(2,1)$ is a univariate Laplace distribution. The density functions of the $\mathcal{K}(1,1)$, $\mathcal{K}(2,1)$ and $\mathcal{K}(4,1)$ distributions are shown in Figure 3, and tail probabilities are tabulated in Figure 4 for the $\mathcal{K}(k,1)$ distributions for shape $k = 1,\ldots,6$. The tail probability functions for the $\mathcal{K}(1,1)$, $\mathcal{K}(2,1)$ and $\mathcal{K}(4,1)$ distributions are illustrated in Figure 5 in Appendix B. It can be seen that $\mathcal{K}(k,1)$ is far more highly weighted around 0 and in the tails for shape $k > 1$ than the comparable standard Normal distribution $\mathrm{N}(0,1) = \mathcal{K}(1,1)$ with the same mean 0 and variance 1.

4.2 The $\otimes$-product of Spherical Bivariate Normal Distributions

We now establish the distribution of a component $Z_j^{(k)}$ of the k-fold $\otimes$-product $Z^{(k)}$ of spherical bivariate Normal distributions. Lemma 4 gives the density function $f_{Z^{(k)}}$ of the bivariate random variable $Z^{(k)}$. Lemma 5 then gives the associated characteristic function $\phi_{Z^{(k)}}$ of $Z^{(k)}$. Finally, Lemma 6 shows that a component $Z_j^{(k)}$ of the k-fold $\otimes$-product $Z^{(k)}$ has the $\mathcal{K}$ distribution with shape k. Full proofs of these results are provided in Appendix C.

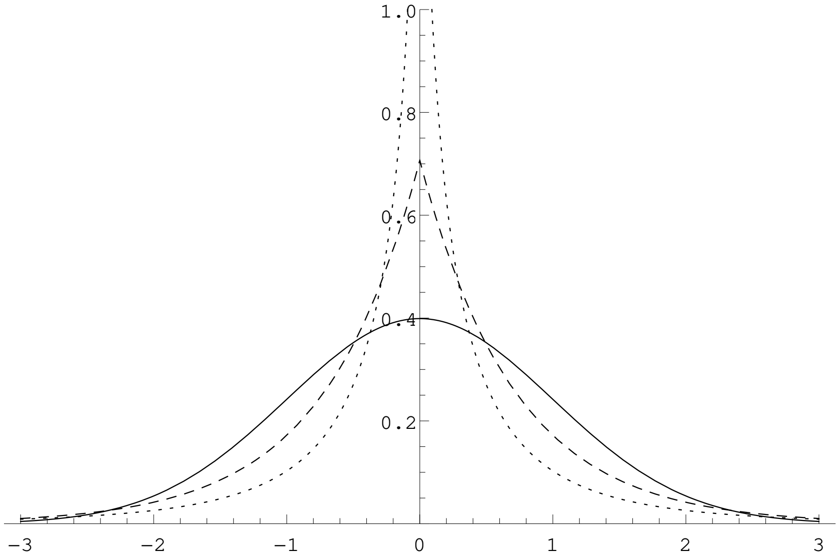

Fig. 3. The density function of a $\mathcal{K}(1,1) = \mathrm{N}(0,1)$ distribution (solid line), the density function of a $\mathcal{K}(2,1)$ distribution (dashed line) and the density function of a $\mathcal{K}(4,1)$ distribution (dotted line).

Lemma 4. *Suppose that $Z_1 \sim N(0;\rho_1^2 I_2), \ldots, Z_k \sim N(0;\rho_k^2 I_2)$ are independent spherical bivariate Normal random variables and that $\mathcal{G}_k$ is the Meijer G-function of Definition 7. Their k-fold $\otimes$-product $Z^{(k)} = Z_1 \otimes \ldots \otimes Z_k$ has density function $f_{Z^{(k)}}$ on $\mathbb{R}^2$ given by $f_{Z^{(k)}}(z) = (2\pi\rho^2)^{-1}\, \mathcal{G}_k\left(\frac{1}{2}\rho^{-2}|z|^2\right)$, where $\rho^2 = \rho_1^2 \ldots \rho_k^2$.*

Sketch Proof. The proof establishes the density function $f_{|Z^{(k)}|}$ of $|Z^{(k)}|$ by an inductive argument based on the multiplicative convolution of particular Meijer G-functions. The final form of the density function $f_{Z^{(k)}}$ of $Z^{(k)}$ then follows from a polar transformation. □

Lemma 5. *Suppose that $Z_1 \sim N(0;\rho_1^2 I_2), \ldots, Z_k \sim N(0;\rho_k^2 I_2)$ are independent spherical bivariate Normal random variables and that $\mathcal{H}_k$ is the Meijer G-function of Definition 7. Their k-fold $\otimes$ product $Z^{(k)} = Z_1 \otimes \ldots \otimes Z_k$ has characteristic function $\phi_{Z^{(k)}}$ on $\mathbb{R}^2$ given by $\phi_{Z^{(k)}}(t) = \mathcal{H}_k\left(2\rho^2|t|^{-2}\right)$, where $\rho^2 = \rho_1^2 \ldots \rho_k^2$.*

Sketch Proof. The characteristic function $\phi_{Z^{(k)}}$ is evaluated by means of polar co-ordinates to give a multiplicative convolution of Meijer G-functions. □

Lemma 6. *Suppose that $Z_1 \sim N(0;\rho_1^2 I_2), \ldots, Z_k \sim N(0;\rho_k^2 I_2)$ are independent spherical bivariate Normal random variables, and let $Z^{(k)} = Z_1 \otimes \ldots \otimes Z_k$ be their k-fold $\otimes$-product. A component $Z_j^{(k)}$ of $Z^{(k)}$ has a $\mathcal{K}(k,\rho^2)$ distribution (Definition 9) with shape k and variance $\rho^2 = \rho_1^2 \ldots \rho_k^2$.*

θ	2.0	3.0	4.0	5.0	6.0	7.0
$\mathbf{P}(\lvert\mathcal{K}(1,1)\rvert > \theta)$	0.0455	0.0027	0.0001	0.0000	0.0000	0.0000
$\mathbf{P}(\lvert\mathcal{K}(2,1)\rvert > \theta)$	0.0591	0.0144	0.0035	0.0008	0.0002	0.0001
$\mathbf{P}(\lvert\mathcal{K}(3,1)\rvert > \theta)$	0.0578	0.0201	0.0077	0.0031	0.0013	0.0006
$\mathbf{P}(\lvert\mathcal{K}(4,1)\rvert > \theta)$	0.0530	0.0217	0.0100	0.0050	0.0026	0.0015
$\mathbf{P}(\lvert\mathcal{K}(5,1)\rvert > \theta)$	0.0473	0.0213	0.0109	0.0061	0.0036	0.0022
$\mathbf{P}(\lvert\mathcal{K}(6,1)\rvert > \theta)$	0.0417	0.0201	0.0110	0.0065	0.0041	0.0027

Fig. 4. The tail probabilities for a $\mathcal{K}(k,1)$ distribution with shape $k = 1, \ldots, 6$.

Sketch Proof. The characteristic function corresponding to the density function f_Y is the appropriate marginal characteristic function derived from Lemma 5. □

4.3 Application to Homomorphic Multiplication Noise Growth

By considering repeated multiplication of degree-1 ciphertexts we can see that the (embedded) noise in a degree-k ciphertext is an element of H that can be expressed as a real valued random vector $W^{(k)} = (W_1^{(k)}, \ldots, W_n^{(k)})^T$ in the T-basis formed by a k-fold $\otimes$-product. The discussion of Section 4.2 shows that the distribution of a component $W_j^{(k)} \dot{\sim} \mathcal{K}(k, \rho^2)$ can be approximated by a $\mathcal{K}$ distribution with shape k and some variance ρ^2 obtained as the product of individual variances. Furthermore, a component $W_j^{(k)}$ is independent of every other component, except its complex conjugate "twin" component to which it is uncorrelated.

For decryption, we consider the embedded noise of a degree-k ciphertext expressed as the real random vector $C'W^{(k)}$ in an appropriate decryption basis. We can use a Central Limit framework [11] to approximate the distribution of $C'W^{(k)}$ as a multivariate Normal distribution under mild conditions on C' for "product variance" ρ^2 as

$$C'W^{(k)} \dot{\sim} \mathrm{N}(0; \rho^2 C'C'^T) .$$

This Normal approximation can then be used to obtain information about the probability of decryption failure, as was done for $k = 2$ in [11, Theorem 2].

The quality of the approximation will decrease as the degree k increases due to the heavier tails of $\mathcal{K}(k, \rho^2)$ as k increases. In the case of a somewhat homomorphic encryption scheme, requiring to support only a few multiplications, this may not be problematic. Moreover, the quality of this approximation can be checked empirically if required.

References

1. M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions*, Dover Publications, 1965.

2. R. Askey and A. Daalhuis and A. Olde, *Meijer G-function*, NIST Handbook of Mathematical Functions (F. Olver *et al.*, ed.), Cambridge University Press, 2010.
3. H. Bateman and A. Erdélyi, *Higher Transcendental Functions*, 1, McGraw-Hill, 1953.
4. R. Beals and J. Szmiglieski, Meijer G-Functions: A Gentle Introduction, *Notices Amer. Math. Soc.* **60** (2013), 886–872.
5. C. Gentry, Fully Homomorphic Encryption using Ideal Lattices, in: *41st Annual ACM Symposium on Theory of Computing, STOC 2009*, Proceedings, ACM, (2009), 169–178.
6. V. Lyubashevsky and C. Peikert and O. Regev, On Ideal Lattices and Learning with Errors over Rings, in: *Advances in Cryptology - EUROCRYPT 2010*, Lecture Notes in Comput. Sci. 6110, Springer, (2010), 1–23.
7. V. Lyubashevsky and C. Peikert and O. Regev, *A Toolkit for Ring-LWE Cryptography*, preprint (2013), `https://eprint.iacr.org/2013/293`.
8. V. Lyubashevsky and C. Peikert and O. Regev, A Toolkit for Ring-LWE Cryptography, in: *Advances in Cryptology - EUROCRYPT 2013*, Lecture Notes in Comput. Sci. 7881, Springer, (2013), 35–54.
9. D. Micciancio and C. Peikert, Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller, in: *Advances in Cryptology - EUROCRYPT 2012*, Lecture Notes in Comput. Sci. 7237, Springer, (2012), 700–718.
10. S. Murphy and R. Player, *δ-subgaussian Random Variables in Cryptography*, preprint (2019), `https://eprint.iacr.org/2017/698`.
11. S. Murphy and R. Player, *A Central Limit Framework for Ring-LWE Decryption*, preprint (2019), `https://eprint.iacr.org/2019/452`.
12. D. Stehlé and R. Steinfeld and K. Tanaka and K. Xagawa, Efficient Public Key Encryption Based on Ideal Lattices, in: *Advances in Cryptology - ASIACRYPT 2009*, Lecture Notes in Comput. Sci. 5912, Springer, (2009), 617–635.

A Proof of a Result of Section 3 about a Normal Balanced Reduction

Lemma 1.
If $Y \sim \mathrm{N}(\mu, \sigma^2)$, then its Balanced Reduction $\mathcal{R}(Y) \to \triangle$ has the Triangular distribution $\triangle$ (density function $1-|z|$ for $|z| < 1$ and 0 otherwise) as its limiting distribution as the standard deviation $\sigma \to \infty$.

Proof. Let f_Y denote the density function of $Y \sim \mathrm{N}(\mu, \sigma^2)$, and let $f_{Y'}(y) = \sum\limits_{k=-\infty}^{\infty} f_Y(y+k)$ denote the density function of $Y' = Y - \lfloor Y \rfloor$, the "modulo 1" reduction of Y to $[0, 1)$. By construction, $\mathcal{R}(Y) = \mathcal{R}(Y')$, so the distribution function $F_{\mathcal{R}(Y)}$ of $\mathcal{R}(Y)$ is given by

$$\begin{aligned} F_{\mathcal{R}(Y)}(y) = \mathbf{P}(\mathcal{R}(Y) = \mathcal{R}(Y') \leq y) &= \int_0^1 \mathbf{P}(\mathcal{R}(Y') \leq y | Y' = z) f_{Y'}(z) dz \\ &= \int_0^1 \mathbf{P}\left(\mathcal{R}(z) \leq y\right) f_{Y'}(z)\, dz = \int_0^1 F_{\mathcal{R}(z)}(y) f_{Y'}(z)\, dz. \end{aligned}$$

The distribution function $F_{\mathcal{R}(z)}(y) = \mathbf{P}(\mathcal{R}(z) \leq y)$ of $\mathcal{R}(z)$ takes the value 0 for $y < -(\lceil z \rceil - z)$, the value $1 - (\lceil z \rceil - z)$ for $-(\lceil z \rceil - z) \leq y < 1 - (\lceil z \rceil - z)$ and the value 1 for $y \geq 1 - (\lceil z \rceil - z)$. Thus this distribution function $F_{\mathcal{R}(z)}(y)$ can be expressed for $-1 \leq y < 1$ as

$$F_{\mathcal{R}(z)}(y) = \begin{cases} z & [0 \leq z < y+1] \\ 0 & [y+1 < z \leq 1] \end{cases} \quad \text{for } -1 \leq y < 0$$
$$\text{and } F_{\mathcal{R}(z)}(y) = \begin{cases} 1 & [0 \leq z < y] \\ z & [y < z \leq 1] \end{cases} \quad \text{for } 0 \leq y < 1.$$

For $-1 \leq y < 0$ this distribution function $F_{\mathcal{R}(Y)}$ of $\mathcal{R}(Y)$ therefore evaluates as

$$F_{\mathcal{R}(Y)}(y) = \int_0^{y+1} z f_{Y'}(z)\, dz = \int_{-1}^{y} (1+z) f_{Y'}(1+z)\, dz,$$

whereas, for $0 \leq y < 1$ and noting that $\mathbf{E}(Y') = \displaystyle\int_0^1 y f_{Y'}(y)\, dy$, we have

$$F_{\mathcal{R}(Y)}(y) = \int_0^y f_{Y'}(z)\, dz + \int_y^1 z f_{Y'}(z)\, dz = \mathbf{E}(Y') + \int_0^y (1-z) f_{Y'}(z)\, dz.$$

Thus the density function $f_{\mathcal{R}(Y)}$ of $\mathcal{R}(Y)$ is given by

$$f_{\mathcal{R}(Y)}(y) = F'_{\mathcal{R}(Y)}(y) = \begin{cases} (1+y) f_{Y'}(1+y) & [-1 \leq y < 0] \\ (1-y) f_{Y'}(y) & [0 \leq y < 1]. \end{cases}$$

The density function $f_{Y'}(y) = \displaystyle\sum_{k=-\infty}^{\infty} c_k \exp(i2\pi k(y-\mu))$ of Y' on $[0,1)$ can be expressed as a Fourier series in $(y-\mu)$ (of period 1) with coefficients

$$\begin{aligned} c_k &= \int_0^1 f_{Y'}(z+\mu) \exp(-i2\pi k z)\, dz \\ &= \int_0^1 \sum_{l=-\infty}^{\infty} f_Y(z+l+\mu) \exp(-i2\pi k z)\, dz \\ &= \sum_{l=-\infty}^{\infty} \int_l^{l+1} f_Y(z+\mu) \exp(-i2\pi k z) dz \\ &= \int_{-\infty}^{\infty} \exp(-i2\pi k(z-\mu)) f_Y(z)\, dz \\ &= \mathbf{E}(-i2\pi k(Y-\mu)) = \phi_{Y-\mu}(-2\pi k) = \exp(-2\pi^2\sigma^2 k^2), \end{aligned}$$

where $\phi_{Y-\mu}(t) = \exp(-\frac{1}{2}\sigma^2 t^2)$ is the characteristic function of $Y - \mu \sim \mathrm{N}(0, \sigma^2)$. The density function $f_{\mathcal{R}(Y)}$ of $\mathcal{R}(Y)$ on $(-1,1)$ is therefore given by

$$f_{\mathcal{R}(Y)}(y) = (1 - |y|) \left(1 + 2 \sum_{k=1}^{\infty} \exp(-2\pi^2\sigma^2)^{k^2} \cos(2k\pi(y-\mu)) \right).$$

Thus $f_{\mathcal{R}(Y)}(y) \to (1 - |y|)$ on $(-1,1)$ as $\sigma \to \infty$, so $\mathcal{R}(Y) \to \triangle$ as $\sigma \to \infty$.

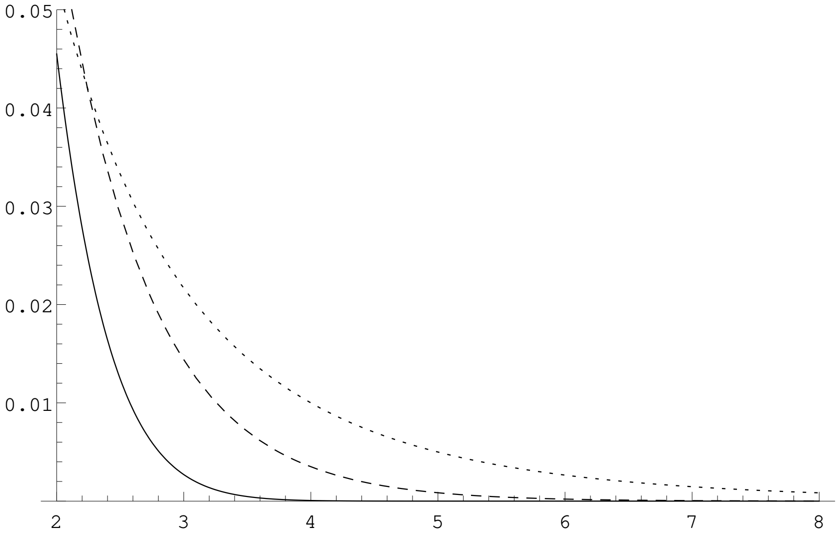

Fig. 5. The tail probability functions $\mathbf{P}(|\mathcal{K}(1,1)| > x)$ of a $\mathcal{K}(1,1) = \mathrm{N}(0,1)$ distribution (solid line), $\mathbf{P}(|\mathcal{K}(2,1)| > x)$ of a $\mathcal{K}(2,1)$ distribution (dashed line) $\mathbf{P}(|\mathcal{K}(4,1)| > x)$ of a $\mathcal{K}(4,1)$ distribution (dotted line).

B Illustration of tail probability functions of $\mathcal{K}$ distributions

The tail probability functions for the $\mathcal{K}(1,1)$, $\mathcal{K}(2,1)$ and $\mathcal{K}(4,1)$ distributions are illustrated in Figure 5.

C Proofs of Results of Section 4 about the $\otimes$-product

Lemma 4.
Suppose that $Z_1 \sim \mathrm{N}(0; \rho_1^2 I_2), \ldots, Z_k \sim \mathrm{N}(0; \rho_k^2 I_2)$ are independent spherical bivariate Normal random variables and that $\mathcal{G}_k$ is the Meijer G-function of Definition 7. Their k-fold $\otimes$-product $Z^{(k)} = Z_1 \otimes \ldots \otimes Z_k$ has density function $f_{Z^{(k)}}$ on $\mathbb{R}^2$ given by $f_{Z^{(k)}}(z) = (2\pi\rho^2)^{-1}\, \mathcal{G}_k\left(\frac{1}{2}\rho^{-2}|z|^2\right)$, where $\rho^2 = \rho_1^2 \ldots \rho_k^2$.

Proof. For simplicity, we suppose $\rho_1^2 = \ldots = \rho_k^2 = 1$ as this gives a direct rescaling of the stated result. We first show that the density function $f_{|Z^{(k)}|}$ for the length $|Z^{(k)}|$ of this k-fold $\otimes$-product $Z^{(k)}$ is $f_{|Z^{(k)}|}(r) = r\mathcal{G}_k(\frac{1}{2}r^2)$ for $r \geq 0$, which we demonstrate by induction. When $k = 1$, the length $|Z^{(1)}| = |Z_1|$ has the distribution of the length $|\mathrm{N}(0; I_2)| = \chi_2$ of a χ-distribution with 2 degrees of freedom. Thus the density function $f_{|Z^{(1)}|}(r) = r\exp(-\frac{1}{2}r^2) = r\mathcal{G}_1(\frac{1}{2}r^2)$ is given by the appropriate Meijer G-function.

We now assume inductively that the length $|Z^{(k-1)}|$ of the $(k-1)$-fold $\otimes$-product $Z^{(k-1)} = Z_1 \otimes \ldots \otimes Z_{k-1}$ has density function $f_{|Z^{(k-1)}|}(r) = r\mathcal{G}_{k-1}(\frac{1}{2}r^2)$.

Direct calculation shows that $|Z^{(k)}| = 2^{-\frac{1}{2}}|Z^{(k-1)}||Z_k|$, so $|Z^{(k)}|$ has density function

$$\begin{aligned} f_{|Z^{(k)}|}(r) &= f_{2^{-\frac{1}{2}}|Z^{(k-1)}||Z_k|}(r) = 2^{\frac{1}{2}} f_{|Z^{(k-1)}||Z_k|}\left(2^{\frac{1}{2}} r\right) \\ &= 2^{\frac{1}{2}} \int_0^\infty z^{-1}\, f_{|Z^{(k-1)}|}\left(2^{\frac{1}{2}} r z^{-1}\right)\, f_{|Z_k|}(z)\, dz \\ &= 2^{\frac{1}{2}} \int_0^\infty z^{-1}\, 2^{\frac{1}{2}} r z^{-1} \mathcal{G}_{k-1}\left(r^2 z^{-2}\right)\, z G_1\left(\tfrac{1}{2} z^2\right)\, dz \\ &= 2r \int_0^\infty z^{-1}\, \mathcal{G}_{k-1}\left(r^2 z^{-2}\right)\, \mathcal{G}_1\left(\tfrac{1}{2} z^2\right)\, dz \\ &= r \int_0^\infty y^{-1}\, \mathcal{G}_{k-1}\left(\tfrac{1}{2} r^2 y^{-1}\right)\, \mathcal{G}_1\left(y\right)\, dy \end{aligned}$$

However, $y^{-1}\mathcal{G}_1(y) = y^{-1} G^{1\,0}_{0\,1}\left({}_{0}\middle|\, y\right) = G^{1\,0}_{0\,1}\left({}_{-1}\middle|\, y\right)$ in the Meijer G-function notation of Definition 7, so

$$\begin{aligned} f_{|Z^{(k)}|}(r) &= r \int_0^\infty G^{k-1\,0}_{0\;k-1}\left({}_{00\ldots0}\middle|\, \tfrac{1}{2} y^{-1} r^2\right)\, G^{1\,0}_{0\,1}\left({}_{-1}\middle|\, y\right)\, dy \\ &= r\, G^{k\,0}_{0\,k}\left({}_{00\ldots0}\middle|\, \tfrac{1}{2} r^2\right) = r\, \mathcal{G}_k\left(\tfrac{1}{2} r^2\right), \end{aligned}$$

as the final integral is a multiplicative convolution of Meijer G-functions. Thus $f_{|Z^{(k)}|}$ has the appropriate form and the inductive demonstration is complete.

The result for the density function $f_{Z^{(k)}}$ of the spherically symmetric $Z^{(k)}$ then follows immediately from the polar transformation linking $f_{Z^{(k)}}$ and $f_{|Z^{(k)}|}$.

Lemma 5.
Suppose that $Z_1 \sim \mathrm{N}(0; \rho_1^2 I_2), \ldots, Z_k \sim \mathrm{N}(0; \rho_k^2 I_2)$ are independent spherical bivariate Normal random variables and that $\mathcal{H}_k$ is the Meijer G-function of Definition 7. Their k-fold $\otimes$ product $Z^{(k)} = Z_1 \otimes \ldots \otimes Z_k$ has characteristic function $\phi_{Z^{(k)}}$ on $\mathbb{R}^2$ given by $\phi_{Z^{(k)}}(t) = \mathcal{H}_k\left(2\rho^2|t|^{-2}\right)$, where $\rho^2 = \rho_1^2 \ldots \rho_k^2$.

Proof. For simplicity, we set $\rho_1^2 = \ldots = \rho_k^2 = 1$, so $\rho^2 = 1$. The density function $f_{Z^{(k)}}$ of $Z^{(k)}$ is $f_{Z^{(k)}}(z) = (2\pi)^{-1}\mathcal{G}_k(\frac{1}{2}|z|^2)$, so the characteristic function $\phi_{Z^{(k)}}$ of $Z^{(k)}$ is given by

$$\phi_{Z^{(k)}}(t) = \mathbf{E}\left(\exp\left(it^T Z^{(k)}\right)\right) = \frac{1}{2\pi}\int_{\mathbb{R}^2} \exp\left(it^T z\right) \mathcal{G}_k\left(\tfrac{1}{2}|z|^2\right)\, dz$$

We can write $t = r(\cos\theta, \sin\theta)^T$ and $z = s(\cos\alpha, \sin\alpha)^T$ for t and z in polar co-ordinates, so $t^T z = rs\cos(\alpha - \theta)$. In terms of these polar co-ordinates, the characteristic function $\phi_{Z^{(k)}}(r, \theta) = \phi_{Z^{(k)}}(t)$ of $Z^{(k)}$ can be expressed as

$$\begin{aligned} \phi_{Z^{(k)}}(r, \theta) &= \frac{1}{2\pi}\int_0^\infty \int_0^{2\pi} \exp(irs\cos(\alpha - \theta))\, r\mathcal{G}_k\left(\tfrac{1}{2} r^2\right)\, d\alpha\, ds \\ &= \frac{1}{2\pi}\int_0^\infty \int_0^{2\pi} \cos(rs\cos(\alpha - \theta))\, r\mathcal{G}_k\left(\tfrac{1}{2} r^2\right)\, d\alpha\, ds \\ &\quad + i\, \frac{1}{2\pi}\int_0^\infty \int_0^{2\pi} \sin(rs\cos(\alpha - \theta))\, r\mathcal{G}_k\left(\tfrac{1}{2} r^2\right)\, d\alpha\, ds \\ &= \int_0^\infty J_0(rs)\, s\mathcal{G}_k\left(\tfrac{1}{2} s^2\right)\, ds, \end{aligned}$$

where $J_0(x) = \dfrac{1}{\pi}\displaystyle\int_0^{\pi} \cos(-x\cos\tau)\ d\tau$ is a Bessel function of the first kind [1]. However, both terms $J_0(rs) = J_0(|t|s) G^{1\,0}_{0\,2}\left({}_{00}\middle|\,\tfrac{1}{4}r^2s^2\right) = G^{1\,0}_{0\,2}\left({}_{00}\middle|\,\tfrac{1}{4}|t|^2s^2\right)$ and $\mathcal{G}_k(\tfrac{1}{2}s^2) = G^{k\,0}_{0\,k}\left({}_{00}\middle|\,\tfrac{1}{2}s^2\right)$ making up the integrand are Meijer G-functions. Thus the characteristic function $\phi_{Z^{(k)}}(t) = \phi_{Z^{(k)}}(r,\theta)$ of $Z^{(k)}$ can be evaluated as a multiplicative convolution to give

$$\begin{aligned}
\phi_{Z^{(k)}}(t) &= \int_0^{\infty} G^{1\,0}_{0\,2}\left({}_{00}\middle|\,\tfrac{1}{4}|t|^2s^2\right)\ r\ G^{k\,0}_{0\,k}\left({}_{00\ldots\,0}\middle|\,\tfrac{1}{2}s^2\right)\ ds \\
&= \int_0^{\infty} G^{1\,0}_{0\,2}\left({}_{00}\middle|\,\tfrac{1}{2}|t|^2u\right)\ G^{k\,0}_{0\,k}\left({}_{00\ldots\,0}\middle|\,u\right)\ du \\
&= \int_0^{\infty} G^{0\,1}_{2\,0}\left({}^{11}\middle|\,2|t|^{-2}u^{-1}\right)\ G^{k\,0}_{0\,k}\left({}_{00\ldots0}\middle|\,u\right)\ du \\
&= G^{k-1\,1}_{1\,k-1}\left({}^{\ 1}_{11\ldots1}\middle|\,2|t|^{-2}\right) = \mathcal{H}_k\left(2|t|^{-2}\right).
\end{aligned}$$

Lemma 6.
Suppose that $Z_1 \sim \mathrm{N}(0;\rho_1^2 I_2), \ldots, Z_k \sim \mathrm{N}(0;\rho_k^2 I_2)$ are independent spherical bivariate Normal random variables, and let $Z^{(k)} = Z_1 \otimes \ldots \otimes Z_k$ be their k-fold $\otimes$-product. A component $Z_j^{(k)}$ of $Z^{(k)}$ has a $\mathcal{K}(k,\rho^2)$ distribution (Definition 9) with shape k and variance $\rho^2 = \rho_1^2 \ldots \rho_k^2$.

Proof. For simplicity, we set $\rho_1^2 = \ldots = \rho_k^2 = 1$, so $\rho^2 = 1$. Suppose $Z^{(k)}$ has orthogonal components $Z_1^{(k)}$ and $Z_2^{(k)}$, so we can write $Z = \left(Z_1^{(k)}, Z_2^{(k)}\right)^T$. Thus the joint characteristic function $\phi_{Z_1^{(k)},Z_2^{(k)}}(t_1,t_2) = \phi_{Z^{(k)}}(t)$, where $t = (t_1,t_2)$, so Lemma 5 shows that

$$\phi_{Z_1^{(k)},Z_2^{(k)}}(t_1,t_2) = \mathbf{E}\left(\exp\left(i\left(t_1Z_1^{(k)} + t_2Z_2^{(k)}\right)\right)\right) = \mathcal{H}_k(2(t_1^2+t_2^2)^{-2}).$$

The characteristic function $\phi_{Z_1^{(k)}}$ of a component $Z_1^{(k)}$ say of $Z^{(k)}$ is therefore given by $\phi_{Z_1^{(k)}}(t_1) = \mathbf{E}(\exp(it_1Z_1^{(k)})) = \phi_{Z_1^{(k)},Z_2^{(k)}}(t_1,0) = \mathcal{H}_k(2t_1^{-2})$.

Suppose $X \sim \mathcal{K}(k,1)$, so X has density function $f_X(x) = (2\pi)^{-\frac{1}{2}}\ \mathcal{J}_k\left(\tfrac{1}{2}x^2\right)$. The characteristic function ϕ_X of X is given by

$$\begin{aligned}
\phi_X(u) = \mathbf{E}(\exp(iuX)) &= (2\pi)^{-\frac{1}{2}} \int_{-\infty}^{\infty} \cos(ux)\mathcal{J}_k(\tfrac{1}{2}x^2)\ dx \\
&= (2\pi)^{-\frac{1}{2}} \int_{-\infty}^{\infty} \cos(ux)\ G^{k\,0}_{0\,k}\left({}_{0\frac{1}{2}\ldots\,\frac{1}{2}}\middle|\,\tfrac{1}{2}x^2\right)\ dx \\
&= 2^{\frac{1}{2}}u^{-1}G^{k-1\,1}_{1\,k-1}\left(\begin{smallmatrix}\frac{1}{2}\\ \frac{1}{2}\,\frac{1}{2}\cdots\frac{1}{2}\end{smallmatrix}\middle|\,\frac{2}{u^2}\right) = G^{k-1\,1}_{1\,k-1}\left({}^{\ 1}_{11\ldots1}\middle|\,2u^{-2}\right) = \mathcal{H}_k(2u^{-2}).
\end{aligned}$$

Thus $\phi_{Z_j^{(k)}}(u) = \phi_X(u) = \mathcal{H}_k(2u^{-2})$ are the same characteristic function, and $Z_j^{(k)}$ therefore has the same distribution as $X \sim \mathcal{K}(k,1)$.

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).