A Central Limit Approach for Ring-LWE Noise Analysis

Sean Murphy and Rachel Player

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

Abstract. This paper develops Central Limit arguments for analysing the noise in ciphertexts in two homomorphic encryption schemes that are based on Ring-LWE. The first main contribution of this paper is to present an average-case noise analysis for the BGV scheme. Our approach builds upon the recent work of Costache et al. that gives the approximation of a polynomial product as a multivariate Normal distribution. We show how this result can be applied in the BGV context and experimentally verify its improvement over prior, worst-case, approaches. Our second main contribution is to develop a Central Limit framework to analyse the noise growth in the homomorphic Ring-LWE cryptosystem of Lyubashevsky, Peikert and Regev (Eurocrypt 2013, full version). Our approach is very general: apart from finite variance, no assumption on the distribution of the noise is required (in particular, the noise need not be subgaussian). We show that our approach leads to tighter bounds for the probability of decryption failure than have been obtained in prior work.

Keywords. Ring-LWE, Central Limit Theorem, δ-subgaussian, decryption failure probability, BGV cryptosystem, homomorphic encryption.

1 Introduction

The Learning with Errors or LWE problem [30, 31] has become a standard hard problem in cryptography that is at the heart of lattice-based cryptography [25, 28]. The Ring Learning with Errors or Ring-LWE problem [33, 21] is a generalisation of the LWE problem from the ring of integers to certain other number field rings that potentially give far better efficiency.

A key application area of lattice-based cryptography is (fully, somewhat or levelled) homomorphic encryption [14]. Homomorphic encryption enables an untrusted party to operate meaningfully on encrypted data belonging to a different party, without requiring access to the secret key. A large number of homomorphic encryption schemes have been proposed in the literature, for example [4, 12, 17, 22, 6, 5], many of which [4, 12, 22, 5] are based on Ring-LWE. To illustrate the ideas of this paper, we first consider the widely-used BGV scheme [4], that has been implemented in (e.g.) [19, 32]. We also consider the symmetric key homomorphic cryptosystem given by Lyubashevsky, Peikert and Regev in Section 8.3 of [22] (the full version of [23]), which we term the SymHom cryptosystem.
Ciphertexts in all homomorphic encryption schemes contain an inherent noise that is needed for security. As more homomorphic evaluation operations are performed, the noise grows, and if it exceeds a certain threshold, then decryption will fail. It is thus essential to understand the noise growth behaviour in order to choose secure and correct parameters. Ideally, we would model the noise growth as tightly as possible, so that the most performant parameters that meet the security and correctness requirements can be selected.

Prior approaches for noise analysis in BGV [15, 16, 10, 9] have been ‘worst-case’: that is, they have modelled the noise growth after every BGV evaluation operation using heuristic worst-case bounds. By tracing through the bounds after each operation, the noise growth incurred by the overall evaluation can also be bounded. However, there can be an unsatisfying gap between the final noise bound and the typical size of the noise as observed in experiments [9], with the gap growing as more computations are performed. In this work, we present for the first time an ‘average-case’ noise analysis for BGV, where average case is meant in the sense of the noise analysis for the TFHE scheme [6] as presented in [7]. That is, we show how for each homomorphic evaluation operation, the input and output noises can be modelled as a Normal random variable. This enables us to trace through the variances of the noise at each operation, and eventually arrive at the variance of the noise after the evaluation. We therefore only need to resort to a bound after the evaluation, where the Normal distribution of the given variance implies a certain tail bound on the noise (holding with a certain probability). This enables us to set parameters that are still large enough to ensure correctness, but, due to the tighter analysis, may be smaller (and thus more performant) than those that would be chosen under a worst-case analysis.

The fundamental issue with modelling the noise growth in schemes like BGV or the `SymHom` cryptosystem is that the noise growth in multiplication is nonlinear. In more detail, if two BGV ciphertexts having noise polynomials \( v_1 \) and \( v_2 \) are multiplied, then the resulting ciphertext has noise polynomial \( v_1 \cdot v_2 \). In particular, if \( X_1 \) and \( X_2 \) are subgaussian random variables arising from such noise polynomials, then the product \( X_1 \cdot X_2 \) is not necessarily subgaussian and indeed can have a much heavier tail [27]. For this reason, an average-case noise analysis for BGV, and related schemes, such as CKKS [5] and BFV [13], was believed until recently to be a challenging open question [9].

In this work, we demonstrate that a Central Limit approach can, under certain assumptions, be used to approximate the output noise of all BGV or `SymHom` operations as a Normal distribution. We now expand in more detail on our approach for each scheme.

### 1.1 A Central Limit Approach for BGV

The first main contribution of this paper is to present an average-case noise analysis for BGV, based on a Central Limit argument.

Average-case analyses for noise growth in FHE schemes have been presented previously, for example for the TFHE scheme [6]. The approach, as presented in [7], is as follows. It is assumed that the coefficients of a fresh TFHE ciphertext
are independent subgaussians, and that the coefficients of a ciphertext output of
the gate bootstrapping operation are also independent subgaussians. The latter
assumption is experimentally verified [7, Figure 10]. It is shown that every TFHE
operation can be implemented via gate bootstrapping on a linear combination
of ciphertexts. Thus, by linearity and by the assumption on gate bootstrapping,
every TFHE ciphertext noise coefficient can be modelled as a subgaussian, thus
permitting an average-case analysis.

Our approach is built upon the recent work of [8] that develops an average-
case noise analysis for the CKKS scheme [5]. To this end, the analysis relies
on Theorem 1, developed in [8], that gives the approximation of a polynomial
product as a multivariate Normal distribution. Our analyses for the noise poly-
nomials resulting from each BGV homomorphic operation follow from repeated
applications of this result and is summarised in Figure 5. We expect that a
similar approach could yield an average-case analysis for the BFV homomorphic
encryption scheme [13]. Indeed, an analysis of the distributional properties of the
multiplication of two polynomial ring elements could also be applicable in wider
contexts, such as in analysis of lattice-based key encapsulation mechanisms [2,
11].

We additionally present an experimental verification of the analysis by com-
paring with practical noise growth in HElib [19] and SEAL [32]. The results are
presented in Tables 1, 2, 3 and 4 and show that the average-case approach more
tightly models the noise growth. Moreover, we demonstrate the applicability
of our analysis by exhibiting specific computations for which the average-case
approach predicts lower parameters to support the computation than the worst-
case approach, and confirm this by successfully implementing these computations
with the smaller parameter set.

1.2 A Central Limit Approach for SymHom

The second main contribution of this paper is to develop a statistical framework,
based on a Central Limit argument, for analysing the noise in SymHom cipher-
texts. To illustrate the utility of this approach, we present in Theorem 2 and
Corollary 2 new, tighter bounds for the probabilities of incorrect decryption in
degree-1 and degree-2 SymHom ciphertexts. Our analysis can similarly be applied
for higher-degree ciphertexts [27].

In more detail, the Central Limit framework is essentially based on approx-
imating the mean vector and the covariance matrix of the noise of a ciphertext
when embedded into the complex space $H$ and transformed with respect to an
appropriate “decoding” basis, that is required during decryption [22]. We show
that the approximate Normality of this embedded noise when expressed in a
decoding basis is fundamentally a Central Limit phenomenon arising from the
weighted sum of many random variables, where the weights arise from a change
of basis matrix to the decoding basis.

For example, if $C^{(pΓ)}$ is a vector of dimension $n$ expressing the noise in a
ciphertext with respect to the decoding $pΓ$-basis for $H$ (Definition 8) and $C^{(T)}$
is a vector of dimension $n$ expressing the noise in a ciphertext with respect to the
original \( T \)-basis for \( H \) (Section 2.4), then \( C^{(p\Gamma)} = p\Delta C^{(T)} \) for an appropriate real-valued \( n \times n \) change of basis matrix \( \Delta \) and “scaling prime” \( p \) (which is the plaintext modulus in \( \text{SymHom} \)). In particular, this means that we can express a component \( c_j^{(p\Gamma)} \) of \( C^{(p\Gamma)} \) as

\[
c_j^{(p\Gamma)} = p \sum_{k=1}^{n} \Delta_{jk} c_k^{(T)}.
\]

The components \( c_1^{(T)}, \ldots, c_n^{(T)} \) of \( C^{(T)} \) are identically distributed random variables that are uncorrelated and, in general, independent, having zero mean \( \mathbb{E} \left( c_j^{(T)} \right) = 0 \) and some finite variance \( \text{Var} \left( c_j^{(T)} \right) = \rho^2 \). Thus a component \( c_j^{(p\Gamma)} \) of a noise vector in the \( p\Gamma \)-basis is a weighted sum of uncorrelated and in general independent identically distributed random variables. We will show that the weightings \( \Delta_{j1}, \ldots, \Delta_{jn} \) are of comparable size, which suggests that a Central Limit argument can be invoked to give a Normal approximation for a component \( c_j^{(p\Gamma)} \). For successful decryption, we require each component of \( C^{(p\Gamma)} \) to be bounded by an appropriate threshold. A Central Limit approach enables us to bound the probability of incorrect decryption using bounds on the tails of Normal distributions.

Theorem 2 and Corollary 2 demonstrate the improvement that can be obtained by using a Central Limit approach in comparison with prior bounds, such as those of [22], obtained using \( \delta \)-subgaussian random variables [24, 26]. For example, if \( \eta_1(n, q, \rho) = \frac{1}{2}(n^2 \rho)^{-1}q \) is moderate or large (see Section 2.2 for further discussion of this issue), Theorem 2 gives a decryption failure probability bound of

\[
\frac{2n \exp\left(-\frac{1}{2}\eta_1^2\right)}{(2\pi)^{\frac{1}{2}}\eta_1}.
\]

This is tighter than the equivalent \( \delta \)-subgaussian decryption failure probability bound of

\[
2n \exp\left(-\frac{1}{2}\eta_1^2\right)
\]

which is obtained by using the tail bound of [26, Lemma 18] in the manner of [22, Lemma 6.5].

No concrete parameter recommendations for \( \text{SymHom} \) are specified in [22], so in contrast to the situation with BGV, it is difficult to quantify the concrete improvement. Asymptotically, ignoring constants, we tighten the bound by a factor of \( \omega(\sqrt{\log n}) \), for power-of-two \( n \) and \( q \) following [22, Lemma 8.5]. However, we emphasise that using such a Central Limit approach in analysing \( \text{SymHom} \) has a number of advantages over other possible approaches, such as the subgaussian approach used in [22]. These advantages are listed below and expressed in terms of the above discussion.

1. A Central Limit approach makes no substantive distributional assumption for the components \( c_k^{(T)} \) beyond finite variance, so is potentially applicable to \( c_k^{(T)} \) that are chosen from heavy-tailed distributions. Thus a Central
Limit approach is more generally applicable than other approaches that for example have a subgaussian requirement for such random variables.

2. A Central Limit approach gives an explicit approximating distribution for the cryptographic random variable of interest which can be directly used for general calculation or simulation purposes of use in cryptography. By contrast, a subgaussian approach can never give an explicit approximating distribution and can only give tail bounds. These tail bounds are generally weaker, as is evidenced by comparing our Theorem 2 with the bound that would be obtained following [22].

3. A Central Limit approach gives not only asymptotically an approximation to a Normal distribution, but also a close approximation concretely, for practically relevant Ring-LWE dimensions $n$.

1.3 Structure of the Paper

We recall relevant background and introduce new tools in Section 2. We outline our Central Limit approach for BGV in Section 3. We then outline our Central Limit approach for the SymHom cryptosystem in Section 4.

2 Background

2.1 Notation

The value or more formally the coset representative of $(r \mod q)$ nearest to 0 is denoted by $\lceil r \rceil_q = r - q\lfloor q^{-1}r \rfloor$, and we use the same notation for a coset of $\mathbb{Z}_q$. We can also extend this idea componentwise to vectors, and we write $\lceil \cdot \rceil_B^q$ to indicate such an extension with respect to a basis $B$. We use $\dagger$ to denote the complex conjugate transpose of a matrix, so $T^\dagger = \overline{\overline{T}}$.

2.2 Central Limit Approximations

Encryption and decryption in Ring-LWE-based cryptography are inherently statistical processes, and we are giving Central Limit approximations to the distributions of cryptographic random variables of interest. Thus we use the notation $\sim$ to denote either “is exactly distributed as” or “is approximately distributed as” in the sense that we may use the approximating distribution for practical purposes without significant error, as is typically done by taking a Central Limit Normal distribution approximation in statistical analysis. Furthermore, whilst Central Limit results are formally asymptotic results concerning sums or means of random variables, such Central Limit approximations usually apply in practice with relatively few summands (except perhaps for pathological distributions) as illustrated by the Berry-Esseen conditions [34] and related multidimensional versions [35]. For example, the simplest form of these Berry-Esseen conditions occurs for independent and identically distributed random variables $X_1, X_2, \ldots$.
with mean \( \mathbf{E}(X_i) = 0 \). In this case, if \( F_n(x) = \mathbf{P}(Y_n \leq x) \) is the distribution function of \( Y_n = \frac{n^{\frac{1}{2}}(X_1 + \ldots + X_n)}{\text{Var}(X_i)^{\frac{1}{2}}} \) and \( \Phi \) is the distribution function of a standard Normal random variable \( Z \sim \mathcal{N}(0, 1) \), then
\[
|F_n(x) - \Phi(x)| < \frac{\mathbf{E}(|X_i|^3)}{\text{Var}(X_i)^{\frac{1}{2}}} n^{-\frac{1}{2}}.
\]
We therefore typically use the phrasing “for moderate or large ...” in such a Central Limit context to emphasise the usual applicability of Central Limit approximations with relatively few summands. For example, such a Central Limit approximation is used in a homomorphic encryption context as being empirically justified with as few as 30 summands [?], in line with routine statistical practice.

2.3 Cyclotomic Number Fields

We consider the ring \( R = \mathbb{Z}[x]/(\Phi_m(x)) \), where \( \Phi_m(x) \) is the \( m \)-th cyclotomic polynomial of degree \( n = \phi(m) \), and we let \( R_a \) denote \( R/aR \) for an integer \( a \). We let \( \zeta_m \) denote a (primitive) \( m \)-th root of unity. 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 \( \zeta_m \), so \( K \) has degree \( n \). The tensor product \( K \otimes_{\mathbb{Q}} \mathbb{R} \) is denoted by \( K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R} \).

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

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 \( \sigma \) embeds \( R \) as a lattice \( \sigma(R) \). The conjugate dual of this lattice corresponds to the embedding of the dual fractional ideal
\[ R^\vee = \{ a \in K \mid \text{Tr}(aR) \subseteq \mathbb{Z} \}. \]
For \( m \) an odd prime, if we define \( b \) such that \( b^{-1} = m^{-1}(1 - \zeta_m) \), then [22, Corollary 2.18] shows that \( R^\vee = \langle b^{-1} \rangle \). We let \( (R^\vee)^k \) denote the space of products of \( k \) elements of \( R^\vee \), that is to say
\[ (R^\vee)^k = \{ s_1 \ldots s_k \mid s_1, \ldots, s_k \in R^\vee \} = \{ b^{-k} r_1 \ldots r_k \mid r_1, \ldots, r_k \in R \}. \]

2.4 The Complex Space \( H \)

The ring embeddings \( \sigma_1, \ldots, \sigma_n \) from \( K \) into \( \mathbb{C} \) occur in complex conjugate pairs with \( \bar{\sigma_k} = \sigma_{m-k} \). Accordingly, much of the analysis of Ring-LWE takes place in a space \( H \) of conjugate pairs of complex numbers.
Definition 1. The conjugate pairs matrix is the complex unitary $n \times n$ matrix $T$, so $T^{-1} = T^\dagger$, given by
\[
T = 2^{-\frac{1}{2}} \begin{pmatrix}
1 & 0 & \ldots & 0 & \ldots & 0 & i \\
0 & 1 & \ldots & 0 & \ldots & i & 0 \\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \ldots & 1 & i & \ldots & 0 \\
0 & 0 & \ldots & 1 & -i & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\
0 & 1 & \ldots & 0 & 0 & \ldots & -i \\
1 & 0 & \ldots & 0 & 0 & \ldots & -i
\end{pmatrix}.
\]

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

Definition 3. The I-basis for $H$ is given by the columns of the $n \times n$ identity matrix $I$, that is to say the I-basis is the standard basis.

Definition 4. The $T$-basis for $H$ is given by the columns of the conjugate pairs matrix $T$.

An element of $H$ is expressed via the I-basis as a vector of $n' = \frac{1}{2}n$ conjugate pairs. Such an element of $H$ can also be expressed (by construction) in the $T$-basis as a real-valued vector, giving the isomorphism between $H$ and $\mathbb{R}^n$ as an inner product space.

2.5 The BGV scheme

In this section we introduce the BGV scheme [4]. We generally follow the description of BGV given in [9], reproduced in Figure 1, that restricts to a power-of-two cyclotomic ring, \( \mathcal{R} = \frac{\mathbb{Z}[X]}{(X^n+1)} \) for $n$ a power of two. The plaintext space is given by \( \mathcal{R}_t = \frac{\mathbb{Z}_q[X]}{(X^n+1)} \) and the ciphertext space is given by \( \mathcal{R}_q = \frac{\mathbb{Z}_q[X]}{(X^n+1)} \). We generally regard a polynomial element of $\mathcal{R}_q$ as having coefficients in \( \{-\frac{1}{2}(q-1), \ldots, \frac{1}{2}(q-1)\} \). A polynomial $h \in \mathcal{R}$ (or $\mathcal{R}_q$ or $\mathcal{R}_t$) is given by
\[
h = h(X) = \sum_{i=0}^{n-1} h_j X^j = h_0 + h_1 X + \ldots + h_{n-1} X^{n-1},
\]
where this polynomial may also be interpreted as vector $h = (h_0, \ldots, h_{n-1})$ of coefficients in an appropriate context.

We now describe in our notation the relevant parts of the BGV scheme in order to define the noise in a BGV ciphertext.
The BGV scheme. BGV is a (levelled) FHE scheme parameterised by \( n, q, t, \chi, S, w, \ell \) and \( \lambda \). Let \( w \) be a base, then \( \ell + 1 = \lceil \log_q q \rceil + 1 \) is the number of terms in the decomposition into base \( w \) of an integer in base \( q \). The Ring-LWE error distribution is denoted \( \chi \) and is typically a discrete Normal with standard deviation \( \sigma = 3.2 \) [1]. The underlying Ring-LWE problem is parameterised by \( n, q, \sigma \) and \( S \), where the parameter \( S \) denotes the secret key distribution. In implementations (e.g [19, 32]), \( S \) is often chosen as a polynomial that has coefficients in \( \{-1, 0, 1\} \). The security parameter is \( \lambda \).

- **SecretKeyGen(\( \lambda \)):** Sample \( s \leftarrow S \) and output \( sk = s \).
- **PublicKeyGen(\( sk \)):** Set \( s = sk \) and sample \( a \leftarrow R_q \) uniformly at random and \( c \leftarrow \chi \). Output \( pk = \langle \lfloor - (as + tc) \rfloor_q, a \rangle \).
- **EvaluationKeyGen(\( sk, w \)):** Set \( s = sk \). For \( i \in \{0, \ldots, \ell \} \), sample \( b_i \leftarrow R_q \) uniformly at random and \( d_i \leftarrow \chi \). Output \( evk = \langle \lfloor - (b_is + td_i) + w_is^2 \rfloor_q, b_i \rangle \).
- **Encrypt(\( pk, m \)):** For the message \( m \in R_q \). Let \( pk = (p_0, p_1) \), sample \( u \leftarrow S \) and \( e_1, e_2 \leftarrow \chi \). Output \( ct = \langle [m + pu + te_1]_q, [pju + te_2]_q \rangle \).
- **Decrypt(\( sk, ct \)):** Let \( s = sk \) and \( ct = (c_0, c_1) \). Output \( m' = \lfloor [(c_0 + c_1)s]_q \rfloor \).
- **Add(\( ct_0, ct_1 \)):** Output \( ct = \langle [ct_0[0] + ct_1[0]]_q, [ct_0[1] + ct_1[1]]_q \rangle \).
- **Multiply(\( ct_0, ct_1 \)):** Set \( c_0 = \lfloor ct_0[0]ct_1[0] \rfloor_q \), \( c_1 = \lfloor ct_0[0]ct_1[1] + ct_0[1]ct_1[0] \rfloor_q \), and \( c_2 = \lfloor ct_0[1]ct_1[1] \rfloor_q \). Output \( ct = (c_0, c_1, c_2) \).
- **Relinearize(\( ct, evk \)):** Let \( ct[0] = c_0 \), \( ct[1] = c_1 \) and \( ct[2] = c_2 \). Let \( evk[i][0] = \lfloor - (b_is + td_i) + w_is^2 \rfloor_q \) and \( evk[i][1] = b_i \). Express \( c_2 \) in base \( w \) as \( c_2 = \sum_{i=0}^{q-1} c_2[i] w^i \). Set \( c_0 = c_0 + \sum_{i=0}^{q-1} evk[i][0]c_2[i] \), and \( c_1 = c_1 + \sum_{i=0}^{q-1} evk[i][1]c_2[i] \). Output \( ct' = (c_0', c_1') \).
- **ModSwitch(\( ct, p \)):** For \( p = q \equiv 1 \mod t \) with \( p \) dividing \( q \). Let \( ct = (c_0, c_1) \). Fix \( \delta \), such that \( \delta_i = -c_i \mod \frac{q}{p} \) and \( \delta_i = 0 \mod \ell \). Set \( c_0 = \frac{q}{p} (c_0 + \delta_0) \) and \( c_1 = \frac{q}{p} (c_1 + \delta_1) \). Output \( ct = (c_0', c_1') \).

![Fig. 1.](image-url)  

The BGV scheme as presented in [9].

**SecretKeyGen.** For emphasis, we write the secret key as \( s \in \{-1, 0, 1\}^n \), a ternary vector of length \( n \). We regard \( s \) as a constant vector known to the genuine receiver. More generally, \( s \) can be regarded as a polynomial of degree \( n - 1 \).

**PublicKeyGen.** The public key \((p_0, p_1)\) consists of two parts, with the first part \( p_0 \) a multivariate random variable and the second part \( p_1 \) a constant vector. For the second part \( p_1 \), a constant vector \( a \in \{-\frac{1}{2}(q-1), \ldots, \frac{1}{2}(q-1)\}^n \) is chosen and \( p_1 \) is set to \( a \), so \( p_1 = a \). For the first part \( p_0 \) with secret key \( s \in \{-1, 0, 1\}^n \), we have

\[
p_0 = -as - t\epsilon_0, \quad \text{where} \quad \epsilon_0 \sim \mathcal{N}(0; \sigma^2 I_n)
\]

is a spherically symmetric multivariate Normal random variable with component variance \( \sigma^2 \), where \( as \) denotes the appropriate polynomial product of \( a \) and \( s \). The distribution of the public key \((p_0, p_1)\) is therefore given by

\[
p_0 \sim \mathcal{N}(-as; t^2 \sigma^2 I_n) \quad \text{and} \quad p_1 = a.
\]
Noise in BGV. In our analysis, we will give distributions for the multivariate random variables arising in BGV before any reduction modulo \( q \). For convenience, we approximate discrete random variables in BGV by the obvious appropriate continuous random variable.

For a BGV ciphertext \((c_0, c_1)\) encrypting a message \( m \), our analysis considers the BGV Critical Value, \( W \) given by

\[
W = c_0 + sc_1,
\]

where \( sc_1 \) denotes the appropriate polynomial product of \( s \) and \( c_1 \). This BGV Critical Value is (we will show) an \( n \)-dimensional multivariate Normal random variable that arises during BGV decryption with secret key \( s \). The Noise \( V \) is then given from the Critical Value \( W \) by subtracting \( m \).

Modulus switching. The key technical tool for noise management in BGV is modulus switching. In Lemma 1 we give an alternative expression for the BGV ModSwitch operation to that given in Figure 1 that will be more convenient for our analysis. Lemma 1 can be seen as giving an explicit implementation of the Scale operation described in earlier analyses of BGV [10, 15].

**Lemma 1.** Suppose that \((c_0, c_1)\) is a BGV ciphertext with respect to a modulus \( q \) and consider a ModSwitch operation with respect to a new modulus \( p < q \). The BGV ModSwitch operation maps an input ciphertext part \( c_i \) to the nearest integer polynomial to \( \frac{p}{q}c_i \) having the same value modulo \( t \) as \( c_i \). More formally, this output ciphertext \((c'_0, c'_1)\) after the ModSwitch operation can be expressed as

\[
c'_i = \left\lfloor \frac{p}{q}c_i \right\rfloor + \left( \left( c_i - \left\lfloor \frac{p}{q}c_i \right\rfloor \right) \mod t \right) \quad [i = 0, 1].
\]

**Proof.** We let \( r = \frac{q}{p} \), so the integer \( r = 1 \mod t \). The ModSwitch operation uses \( \delta_i = -c_i \mod r \) and \( \delta_i = 0 \mod t \) for \( i = 0, 1 \). The Chinese Remainder Theorem shows that \( \delta_0 \) and \( \delta_1 \) are uniquely defined modulo \( rt \), so have coefficients lying between \(-\frac{1}{2}rt\) and \( \frac{1}{2}rt \). This specification for \( \delta_i \) also gives

\[
c_i + \delta_i = 0 \mod r \quad \text{and} \quad c_i + \delta_i = c_i \mod t \quad [i = 0, 1].
\]

In addition, the Chinese Remainder Theorem shows that \( c_0 + \delta_0 \) and that \( c_1 + \delta_1 \) have unique solutions modulo \( rt \) given by

\[
c_0 + \delta_0 = rc_0 \mod rt \quad \text{and} \quad c_1 + \delta_1 = rc_1 \mod rt.
\]

The parts of output ciphertext \((c'_0, c'_1)\) after the ModSwitch operation therefore satisfy

\[
c'_0 = \frac{c_0 + \delta_0}{r} = c_0 \mod t \quad \text{and} \quad c'_1 = \frac{c_1 + \delta_1}{r} = c_1 \mod t,
\]
so the output ciphertext parts have the same values modulo $t$ as the input ciphertext parts.

The output ciphertext parts $c'_0$ and $c'_1$ are “modulo $p$” polynomials with coefficients lying in $\{ -\frac{1}{2}(p-1), \ldots, \frac{1}{2}(p-1) \}$ obtained as the direct contractions of “modulo $q$” polynomials as

$$c'_0 = \frac{c_0 + \delta_0}{r} = \frac{p}{q} (c_0 + \delta_0) \quad \text{and} \quad c'_1 = \frac{c_1 + \delta_1}{r} = \frac{p}{q} (c_1 + \delta_1)$$

We note that these new ciphertext parts can also be expressed as

$$c'_0 = \frac{c_0}{r} + \frac{\delta_0}{r} \quad \text{and} \quad c'_1 = \frac{c_0}{r} + \frac{\delta_1}{r},$$

where $\delta_0$ and $\delta_1$ are polynomials with coefficients between $-\frac{1}{2}t$ and $\frac{1}{2}t$. Thus the BGV ModSwitch operation maps an input ciphertext part $c_i$ to an output ciphertext part $c'_i$, where $c'_i$ is the nearest integer polynomial to $\frac{c_i}{r} = \frac{p}{q} c_i$ having the same value modulo $t$ as $c_i$, which gives the expression in the statement of the Lemma.

### 2.6 The SymHom scheme

In this section we introduce the SymHom cryptosystem. In order to do so, we first need two definitions. A description of SymHom cryptosystem, in the notation of [22], is then given in Figure 2.

**Definition 5 ([26]).** The univariate Balanced Reduction function $\mathcal{R}$ on $\mathbb{R}$ is the random function $\mathcal{R}(a) = \begin{cases} 1 - ([a] - a) & \text{with probability } [a] - a \\ -([a] - a) & \text{with probability } 1 - ([a] - a). \end{cases}$

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 6 ([26]).** Let $B$ be a (column) basis matrix for the $n$-dimensional lattice $\Lambda$ in $H$. If $\mathcal{R}$ is the Balanced Reduction function, then the coordinate-wise randomised rounding discretisation or CRR discretisation $|X|_{\Lambda + c}^B$ of the random variable $X$ on $H$ to the lattice coset $\Lambda + c$ with respect to the basis matrix $B$ is the random variable

$$|X|_{\Lambda + c}^B = X + B \ \mathcal{R} \left( B^{-1} (c - X) \right).$$

We now describe in our notation the relevant parts of the SymHom cryptosystem in order to define the noise in a SymHom ciphertext. We first recall that the SymHom secret key is an element $s \in R$, the plaintext space is $R_p$, and a plaintext $\mu \in R_p$ is encrypted to give a linear polynomial over $R_q^t$.

The first step of the encryption process is to generate a random input for a discretisation process to a coset depending on the plaintext $\mu$. Accordingly, we
The SymHom cryptosystem. Let $\psi$ be a continuous LWE error distribution over $K_R$, and let $[\cdot]$ denote any valid discretisation to cosets of some scaling of $R^\nu$ (e.g., using the decoding basis of $R^\nu$). The cryptosystem is defined formally as follows.

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

For ciphertexts $c, c'$ of arbitrary degrees $k, k'$, their homomorphic product is the degree-$(k + k')$ ciphertext $c(S) \square c'(S) = c(S) \cdot c'(S)$, that is to say standard polynomial multiplication. The noise in the result is defined to be the product of the noise terms of $c, c'$. Similarly, for ciphertexts $c, c'$ of equal degree $k$, their homomorphic sum is $c(S) \oplus c'(S) = c(S) + c'(S)$, and the noise in the resulting ciphertext is the sum of those of $c, c'$.

Fig. 2. The SymHom cryptosystem as defined in [22, Section 8.3].

Let $Y$ be a random variable on $H$ such that $TY \sim \mathcal{N}(0; p^2 \rho^2 I_n)$ is a spherically symmetric $n$-dimensional Normal random variable with component variance $p^2 \rho^2$ for an appropriately chosen $p^2$. We term $Y$ the Underlying Noise, and $Y$ is a complex-valued random vector expressed in the $I$-basis for $H$.

Specifically, we discretise $Y$ to the coset $\sigma(pR^\nu) + \sigma(b^{-1} \mu)$ of the lattice $\sigma(pR^\nu)$ obtained by the canonical embedding of the scaled dual fractional ideal $pR^\nu$. We consider the coordinate-wise randomised rounding discretisation with respect to the $pI$-basis for $H$, and following Definition 6 we denote this discretisation of $Y$ by $Y'(\mu) = [Y]_{p\sigma(pR^\nu) + \sigma(b^{-1} \mu)}$.

The Noise random variable $Y''(\mu)$ in the encryption of the plaintext $\mu$ is then defined to be $Y''(\mu) = \sigma^{-1}(Y'(\mu))$, and is an element of a coset of $pR^\nu + b^{-1} \mu$ containing information about $\mu$. For obvious reasons, we refer to $Y'(\mu)$ as the Embedded Noise, and we note that $Y''(\mu)$ expresses the Embedded Noise in the $I$-basis of $H$. We summarise this discussion in Figure 3.

In the next step of encryption, we form the ciphertext from the Noise $Y''(\mu)$ and the secret key $s$ in the following way. We choose $A$ uniformly in $R_q^\nu$, and we let $A' = -As + Y''(\mu) \in R_q^\nu$. The ciphertext $C(\theta; \mu)$ is the polynomial in $\theta$ over $R_q^\nu$ defined as $C(\theta; \mu) = A'(\mu) + A\theta$. We note that this polynomial can be expressed directly in terms of the Noise $Y''(\mu)$ and the secret key $s$ as $C(\theta; \mu) = A(\theta - s) + Y''(\mu)$. A fresh ciphertext is defined to be a degree-1 ciphertext, since the polynomial $C(\theta; \mu)$ is linear.

The output ciphertext of a homomorphic multiplication of two degree-1 ciphertext polynomials is obtained simply by multiplying these polynomials together. Thus we can obtain the degree-2 ciphertext polynomial over $R_q^\nu$ corresponding to the product $\mu_1 \mu_2$ of plaintexts $\mu_1$ and $\mu_2$ as $C(\theta; \mu_1, \mu_2) = C(\theta; \mu_1) \square C(\theta; \mu_2)$, where $C(\theta; \mu_1) = A'_1(\mu_1) + A_1 \theta$ and $C(\theta; \mu_2) = A'_2(\mu_2) + A_2 \theta$. This degree-2 ciphertext polynomial is $C(\theta; \mu_1, \mu_2) = A'_1(\mu_1)A'_2(\mu_2) + (A_2 A'_1(\mu_1) +$
Random Variable & Range of Random Variable
---
Underlying Noise & \( Y \) & Complex Space \( H \)
Embedded Noise & \( Y'(\mu) \) & Lattice Coset \( \sigma(pR^r) + \sigma(b^{-1}\mu) \)
Noise & \( Y''(\mu) \) & Number Field Coset \( pR^r + b^{-1}\mu \)

Fig. 3. Notation for the Noise-related quantities used in encryption of the plaintext \( \mu \).

\[
A_1 A_2^2(\mu_2) \theta + A_1 A_2 \theta^2, \text{ which is given in terms of the secret key } s \text{ and its constituent Noises } Y''(\mu) \text{ and } Y'''_2(\mu) \text{ by }
\]

\[
C(\theta; \mu_1, \mu_2) = A_1 A_2(\theta - s)^2 + (A_2 Y''_1(\mu_1) + A_1 Y''_2(\mu_2)) \theta - s) + Y''_1(\mu_1)Y''_2(\mu_2).
\]

The Noise in this degree-2 output ciphertext \( C(\theta; \mu_1, \mu_2) \) is defined to be the product \( Y''_1(\mu_1)Y''_2(\mu_2) \) of the Noises \( Y''_1(\mu_1) \) and \( Y''_2(\mu_2) \) of the degree-1 input ciphertexts. This process extends in the obvious way to give ciphertexts of higher degree.

3 A CLT approach to BGV noise analysis

3.1 BGV Polynomial Multiplication

Many BGV operations involve polynomial multiplication in \( R \) or \( R_q \), that is to say modulo \( X^n + 1 \), and we express such a polynomial multiplication using a modified Sign function \( \xi \) on the integers given by \( \xi(z) = \text{Sign}(z) \) for \( z \neq 0 \) with \( \xi(0) = 1 \). A term of \( (hh') \) can then be specified as

\[
(hh')_i = \sum_{j=0}^{n-1} \xi(i - j) h_{i-j} h'_{j} \quad [i = 0, \ldots, n - 1].
\]

and the subscripts are interpreted modulo \( n \) to lie in \( \{0, \ldots, n - 1\} \).

BGV requires to construct the polynomial product in \( R \) or \( R_q \) of a constant or scalar and a (discretised) multivariate Normal random variable or of two multivariate Normal random variables. We use the following result, developed for the CKKS context in [8].

**Theorem 1.** Suppose that \( Z \sim \mathcal{N}(\mu; \rho^2 I_n) \) and \( Z' \sim \mathcal{N}(\mu'; \rho^2 I_n) \), then the polynomial product \( ZZ' \) (modulo \( X^n + 1 \)) is well-approximated as a multivariate Normal distribution for large \( n \) given by

\[
ZZ' \sim \mathcal{N}(\mu \mu' ; \rho^2_\ast I_n + S),
\]

where \( \rho^2_\ast = n \rho^2 + \rho^2 |\mu|^2 + \rho^2 |\mu'|^2 \) and \( S \) is an off-diagonal matrix with \( S_{i,i'} = \rho^2 \sum_{j=0}^{n-1} \xi(i-j)\xi(i'-j)\mu_{i-j}\mu'_{i'-j} + \rho^2 \sum_{j=0}^{n-1} \xi(i-j)\xi(i'-j)\mu_{i-j}^\prime\mu'_{i'-j} \).
Following the approach of [8], we make the Small-\(S\) assumption: that this off-diagonal matrix \(S\) is negligible compared to \(\rho^2 I_N\) and we disregard it. As noted in [8], examination of the form of \(S\) this assumption may not always hold, for example if the mean vectors have large constant components (as further discussed in [8] Supplementary Material C). However, the Small-\(S\) assumption is reasonable in many circumstances of interest in BGV when the message components can be modelled as being uniform modulo \(t\).

**Corollary 1.** Suppose that \(Z \sim \mathcal{N}(\mu; \rho^2 I_n)\) and \(Z' \sim \mathcal{N}(\mu'; \rho'^2 I_n)\) are independent, \(\lambda\) is a constant vector and the Small-\(S\) assumption is valid. Approximations to the distribution of \(\lambda Z, ZZ', Z^2\) are then given by:

\[
\lambda Z \sim \mathcal{N}(\lambda \mu; \rho^2 |\lambda|^2 I_n),
\]

\[
ZZ' \sim \mathcal{N}(\mu \mu'; n \rho^2 \rho'^2 + \rho^2 |\mu|^2 + \rho'^2 |\mu'|^2) I_n
\]

and \(Z^2 \sim \mathcal{N}(\mu^2; 2 \rho^2 (n \rho^2 + 2 |\mu|^2)) I_n\).

We also add a further variant of these results, as adapted in a special case for general (i.e., not necessarily Normal) distributions \(Z\) and \(Z'\), which we use when considering the BGV ModSwitch operation.

**Lemma 2.** Suppose that \(Z = (Z_0, \ldots, Z_{n-1})^T\) and \(Z' = (Z'_0, \ldots, Z'_{n-1})^T\) are independent vectors of independent and identically distributed components with mean \(E(Z_i) = E(Z'_i) = 0\) and respective variances \(Var(Z_i) = \rho^2\) and \(Var(Z'_i) = \rho'^2\). The polynomial product \(ZZ'\) is well-approximated as a multivariate Normal distribution for large \(n\) given by

\[
ZZ' \sim \mathcal{N}(0; n \rho^2 \rho'^2 I_n).
\]

**Proof.** The proof is similar to that given for Theorem 1 given in [8]. A component \((ZZ')_i\) of \(ZZ'\) is the sum of \(n\) summands of the form \(\pm Z_j Z'_j\) with mean \(E(\pm Z_j Z'_j) = 0\) and variance \(Var(\pm Z_j Z'_j) = \rho^2 \rho'^2\). Thus the Central Limit Theorem shows that the distribution of this component \((ZZ')_i\) and be approximated for large \(n\) as \((ZZ')_i \sim \mathcal{N}(0, n \rho^2 \rho'^2)\). Furthermore, distinct components \((ZZ')_i\) and \((ZZ')_{i'}\) (\(i \neq i'\)) have covariance \(Cov((ZZ')_i, (ZZ')_{i'}) = 0\) (as they have 0 means), which gives the result.

### 3.2 BGV Noise Analysis

We now give a series of results showing how the noise in a ciphertext output from each BGV operation follows a Normal distribution with zero mean and a specified component variance. We begin with Lemma 3 about the noise of a fresh BGV ciphertext obtained under a secret key \(s\) and an ephemeral encryption key \(u\). Heuristic 1 then gives a Normal distribution that accurately approximates the noise random variable for a fresh BGV ciphertext. We note that a similar result can be inferred from Lemma 1 of [9].
Lemma 3. [Fresh] The noise random variable $V_{\text{fresh}(s,u)}$ for a fresh BGV ciphertext obtained under a secret key $s$ and an ephemeral encryption key $u$ has a Normal distribution given by $V_{\text{fresh}(s,u)} \sim \mathcal{N}(0; \rho^2_{\text{fresh}(s,u)} I_N)$, where the component variance $\rho^2_{\text{fresh}(s,u)}$ is given by

$$\rho^2_{\text{fresh}(s,u)} = (|s|^2 + |u|^2 + 1)t^2\sigma^2.$$  

Proof. The first part of the public key $p_0 = [-(as + te)]_q$ (in the notation of Figure 1) can be expressed as $p_0 = -as - te + qa$ for an appropriate integer vector $a$. For the second part of the public key $p_1 = a$, we therefore have $p_0 + sp_1 = -te + qa$. The BGV Critical Value $W_{\text{fresh}(s,u)}$ used for decryption of the fresh ciphertext $(c_0, c_1)$ given by $c_0 = m + p_0 u + te_1$ and $c_1 = p_1 u + te_2$ corresponding to message $m$ is given by

$$W_{\text{fresh}(s,u)} = c_0 + sc_1 = m + p_0 u + te_1 + s(p_1 u + te_2) = m + u(-as - te + qa) + te_1 + s(au + te_2) = m + qu_0 + t(-ue + e_1 + se_2).$$

If the standard deviation of $t(-ue + e_1 + se_2)$ is not too large, reducing the BGV Critical Value $W$ modulo $q$ and then modulo $t$ gives the message $m$. Thus the noise random variable corresponding to the BGV Critical Value $W_{\text{fresh}(s,u)}$ is

$$V_{\text{fresh}(s,u)} = t(-ue + e_1 + se_2).$$

Corollary 1 shows that $-ue \sim \mathcal{N}(0; |u|^2\sigma^2 I_n)$ and that $se_2 \sim \mathcal{N}(0; |s|^2\sigma^2 I_n)$, so the distribution of the fresh noise random variable $V_{\text{fresh}(s,u)}$ is

$$V_{\text{fresh}(s,u)} \sim \mathcal{N}(0; \rho^2_{\text{fresh}(s,u)} I_n), \text{ where } \rho^2_{\text{fresh}(s,u)} = (1 + |u|^2 + |s|^2)t^2\sigma^2.$$  

Heuristic 1 [Fresh] The noise random variable $V_{\text{fresh}}$ for a fresh BGV ciphertext is accurately approximated as $V_{\text{fresh}} \sim \mathcal{N}(0; \rho^2_{\text{fresh}} I_N)$ by a Normal distribution with component variance $\rho^2_{\text{fresh}}$, given by

$$\rho^2_{\text{fresh}} = (\frac{3}{4}n + 1)t^2\sigma^2.$$  

Justification. Lemma 3 shows that $\rho^2_{\text{fresh}(s,u)} = (1 + |u|^2 + |s|^2)t^2\sigma^2$, where $s$ is the secret key and $u$ is an ephemeral key. However $s$ and $u$ are random vectors of length $n$ with components uniformly distributed in $\{-1, 0, 1\}$, so $|s|^2, |u|^2 \sim \text{Bin}(n, \frac{2}{3})$ are independent Binomial random variables each with mean $\frac{4}{3}n$ and variance $\frac{2}{3}n$, giving $|s|^2 + |u|^2 \sim \text{Bin}(2n, \frac{2}{3})$ with mean $\frac{4}{3}n$ and variance $\frac{2}{3}n$. The fresh noise random variable $V_{\text{fresh}}$ is therefore the mixture of Normal distributions

$$\sum_{k=0}^{n} \mathbf{P}(\text{Bin}(2n, \frac{2}{3}) = k) \mathcal{N}(0; (k + 1)t^2\sigma^2 I_n),$$

weighted by the Binomial probabilities $\mathbf{P}(\text{Bin}(2n, \frac{2}{3}) = k) = \binom{2n}{k} \left(\frac{2}{3}\right)^k \left(\frac{1}{3}\right)^{2n-k}$. Thus $V_{\text{fresh}}$ is a mixture of Normal distributions in which the high weight summand distributions are very similar, all having mean 0 and component variance
Fig. 4. Density function of Normal Mixture distribution for $V_{\text{fresh}}$ (dashed line) and the essentially coincident approximating Normal distribution (solid line) in dimension $n = 256$

Close to $(\frac{4}{3}n + 1)t^2\sigma^2$, as the standard deviation of $|s|^2 + |u|^2$ is $\frac{2}{3}n^\frac{1}{2}$. The Normal mixture distribution for $V_{\text{fresh}}$ can therefore be approximated as a Normal distribution as

$$V_{\text{fresh}} \sim \mathcal{N}(0; \rho_{\text{fresh}}^2 I_n), \quad \text{where } \rho_{\text{fresh}}^2 = (\frac{4}{3}n + 1)t^2\sigma^2.$$  

Figure 4 illustrates that the Normal mixture distribution and the approximating Normal distribution have essentially coincident density functions for $n = 256$. In this $n = 256$ case, the Kolmogorov-Smirnov distance between the Normal mixture distribution and the approximating Normal distribution is $7.9 \times 10^{-6}$, and this Kolmogorov-Smirnov distance decreases as the dimension $n$ increases.

We now give a series of results about the noise distribution resulting from the application of BGV operations to BGV ciphertexts. We start with Lemma 4 giving the distribution of the noise random variable following the application of the BGV $\text{Add}$ operation to two BGV ciphertexts.

**Lemma 4.** [Add] Suppose that the noise random variables $V$ and $V'$ for two independent BGV ciphertexts have 0-mean multivariate Normal distributions given by $V \sim \mathcal{N}(0; \rho^2 I_n)$ and $V' \sim \mathcal{N}(0; \rho'^2 I_n)$. Let $V_{\text{add}}$ be the noise random variable for the ciphertext output from the BGV $\text{Add}$ operation applied to these two ciphertexts, then $V_{\text{add}} \sim \mathcal{N}(0; \rho_{\text{add}}^2 I_n)$, where the component variance $\rho_{\text{add}}^2$ is given by

$$\rho_{\text{add}}^2 = \rho^2 + \rho'^2.$$

**Proof.** Suppose that $(c_0, c_1)$ and $(c'_0, c'_1)$ are the independent BGV ciphertexts having respective underlying messages $m$ and $m'$ respectively and having the given noise random variables

$$V = (c_0 + sc_1) - m \sim \mathcal{N}(0; \rho^2 I_n) \quad \text{and} \quad V' = (c'_0 + sc'_1) - m' \sim \mathcal{N}(0; \rho'^2 I_n).$$
The BGV Add operation gives the new ciphertext \((c_0 + c_1, c_0' + c_1')\) with message \(m + m'\) and noise random variable

\[
V_{\text{add}} = (c_0 + c_0') + s(c_1 + c_1') - (m + m') = V + V' \sim \mathcal{N}(0; (\rho^2 + \rho'^2)I_n).
\]

The BGV Add operation can also be used to add a ciphertext to itself. For completeness, we also give (without proof) the distribution of the noise random variable for such an integer multiple of a ciphertext in Lemma 5.

**Lemma 5. [Integer Multiple]** Suppose that the noise random variable \(V\) of a BGV ciphertext \((c_0, c_1)\) has 0-mean multivariate Normal distribution given by \(V \sim \mathcal{N}(0; \rho^2I_n)\). The noise random variable of the integer multiple \(k(c_0, c_1)\) of the BGV ciphertext \((c_0, c_1)\) for an integer \(k\) is \(kV \sim \mathcal{N}(0; k^2\rho^2I_n)\).

The application of the BGV Multiply operation to the BGV ciphertexts \((c_0, c_1)\) and \((c_0', c_1')\) gives a 3-part ciphertext

\[
(c_0^*, c_1^*, c_2^*) = (c_0c_0', c_0c_1' + c_1c_0', c_1c_1').
\]

This 3-part ciphertext can potentially be decrypted by considering the 3-part Multiply Critical Value

\[
W_{\text{mult}} = c_0^* + sc_1^* + s^2c_2^* = c_0 + s(c_0'c_1' + c_1c_0') + s^2c_1c_1' = (c_0 + sc_1)(c_0' + sc_1') = WW',
\]

where \(W = c_0 + sc_1\) and \(W' = c_0' + sc_1'\) are the BGV Critical Values of the original ciphertexts \((c_0, c_1)\) and \((c_0', c_1')\). If \(m\) and \(m'\) are the messages corresponding to the ciphertexts \((c_0, c_1)\) and \((c_0', c_1')\), then the message \(m \cdot m'\) corresponding to this 3-part ciphertext can be found by reducing this Critical Value \(W_{\text{mult}}\) modulo \(q\) and then modulo \(t\). The distribution of the noise random variable following the application of the BGV Multiply operation is given in Lemma 6, and Heuristic 2 then gives a method for using this result by giving an expression for the component variance in circumstances of practical interest.

**Lemma 6. [Multiply]** Suppose that the noise random variables \(V\) and \(V'\) for two independent BGV ciphertexts have 0-mean multivariate Normal distributions given by \(V \sim \mathcal{N}(0; \rho^2I_n)\) and \(V' \sim \mathcal{N}(0; \rho'^2I_n)\). Further suppose that the Small-S assumption is valid for the product distribution \((m + V)(m' + V')\), where \(m\) and \(m'\) are the underlying messages. Let \(V_{\text{mult}}\) be the noise random variables for the ciphertext output from the BGV Multiply operation applied to these two ciphertexts, then \(V_{\text{mult}} \sim \mathcal{N}(0; \rho^2_{\text{mult}}I_n)\), where the component variance \(\rho^2_{\text{mult}}\) is given by

\[
\rho^2_{\text{mult}} = n\rho^2 + \rho^2|m|^2 + \rho'^2|m'|^2.
\]

**Proof.** Suppose that \((c_0, c_1)\) and \((c_0', c_1')\) are the independent BGV ciphertexts having respective underlying messages \(m\) and \(m'\) respectively and having the given noise random variables

\[
V = (c_0 + sc_1) - m \sim \mathcal{N}(0; \rho^2I_n) \quad \text{and} \quad V' = (c_0' + sc_1') - m' \sim \mathcal{N}(0; \rho'^2I_n).
\]
The BGV multiplication operation gives the new 3-part ciphertext
\[(c_0c'_0, c_0c'_1 + c_1c'_0, c_1c'_1)\] with corresponding message \(m \cdot m'\).

The corresponding BGV Critical Value is
\[W_{\text{mult}(m,m')} = (c_0 + sc_1)(c'_0 + sc'_1) = (m + V)(m' + V').\]

The corresponding noise random variable \(V_{\text{mult}}\) therefore has the same covariance matrix as the product of \(m + V \sim \mathcal{N}(m; \rho^2I_n)\) and \(m' + V' \sim \mathcal{N}(m'; \rho^2I_n)\). The result then follows from Theorem 1 and Corollary 1.

**Heuristic 2 [Multiply]** In practice, we need to approximate \(|m|^2\) and \(|m'|^2\) to use Lemma 6. If the components of \(m\) and \(m'\) can be regarded as being independently and uniformly distributed on \(T = \{-\frac{1}{2}(t-1), \ldots, \frac{1}{2}(t-1)\}\), then the overall noise random variable \(V_{\text{mult}}\) for a BGV Multiply ciphertext is accurately approximated as \(V_{\text{mult}} \sim \mathcal{N}(0; \rho^2_{\text{mult}}I_n)\) by a Normal distribution with component variance \(\rho^2_{\text{mult}}\) given by
\[\rho^2_{\text{mult}} = n (\rho^2 \rho^2 + \frac{1}{12} (t^2 - 1)(\rho^2 + \rho'^2)).\]

**Justification** If the components \(m_i\) and \(m'_i\) are uniformly distributed on \(T\), then \(Var(m_i) = Var(m'_i) = \frac{1}{12} (t^2 - 1)\). In this case, we have \(|m|^2, |m'|^2 \approx \frac{1}{12} n(t^2 - 1)\), and so a similar argument to the Justification for Heuristic 1 shows that the Normal mixture distribution for \(V_{\text{mult}}\) can be accurately approximated as a Normal distribution as
\[V_{\text{mult}} \sim \mathcal{N}(0; \rho^2_{\text{mult}}I_n), \quad \text{where} \quad \rho^2_{\text{mult}} \approx n (\rho^2 \rho^2 + \frac{1}{12} (t^2 - 1)(\rho^2 + \rho'^2)).\]

The BGV Relinearize operation is used to convert a 3-part ciphertext arising after a BGV Multiply operation to a standard 2-part BGV ciphertext. The distribution of the Noise random variable following the application of a BGV Relinearize operation of the form described in Figure 1 is given in Lemma 7. The result is analogous to prior results [9, 20, 29] about the BGV and BFV Relinearize operations.

We note that well-known implementations of BGV use more extensively optimised variants of this basic BGV Relinearize operation, so this result may need adapting for such optimised variants.

**Lemma 7. [Relinearize]** Suppose that a 3-part BGV ciphertext arising from a BGV Multiply operation has a 0-mean multivariate Normal noise random variable given by \(V \sim \mathcal{N}(0; \rho^2I_n)\). Consider a BGV Relinearize operation with \(\ell + 1\) terms in the decomposition into base \(w\) of an integer in base \(q\) with \(\ell = \lfloor \log_w q \rfloor\) in which a coefficient in \(-\frac{1}{2}(q-1), \ldots, \frac{1}{2}(q-1)\) is represented as vector with \((\ell + 1)\) components lying between \(\frac{-1}{2}w\) and \(\frac{1}{2}w\). Let \(V_{\text{relin}}\) be the noise random variable for the ciphertext output from such a BGV Relinearize operation, then \(V_{\text{relin}} \sim \mathcal{N}(0; \rho^2_{\text{relin}}I_n)\), where the component variance \(\rho^2_{\text{relin}}\) is given by
\[\rho^2_{\text{relin}} = \rho^2 + \frac{1}{12} n(\ell + 1) w^2 \sigma^2.\]
Proof. We consider the 3-part ciphertext \((c_0^s, c_1^s, c_2^s) = (c_0 c_0', c_0 c_1' + c_1 c_0', c_1 c_1')\) arising from the application of the BGV Multiply operation to the ciphertext \((c_0, c_1)\) and the ciphertext \((c_0', c_1')\). For a BGV scheme with parameter \(\ell\), the ciphertext component \(c_2^s\), a polynomial with coefficients between \(\frac{1}{2}(q - 1)\) and \(\frac{1}{2}q\), is expressed as
\[
c_2^s = \sum_{i=0}^{\ell} g_i w^i, \quad \text{for decomposition polynomials } g_i(x) = \sum_{j=0}^{n-1} g_{ij} x^j.
\]
The integer coefficients \(g_{ij}\) of these decomposition polynomials \(g_i\) can be regarded as independent random variables lying uniformly between \(-\frac{1}{2}w\) and \(\frac{1}{2}w\), so we have \(E(g_{ij}) = 0\) and \(\text{Var}(g_{ij}) = \frac{1}{12}w^2\).

The BGV Relinearize operation transforms this 3-part ciphertext into a standard 2-part BGV ciphertext by using the Evaluation Keys
\[
\alpha_i = -(\beta_is + td_i) + w's^2 \quad \text{and} \quad \beta_i = [i = 0, \ldots, \ell],
\]
where \(\beta_0, \ldots, \beta_\ell\) are independent random elements of \(\mathcal{R}_q\) and \(d_0, \ldots, d_\ell\) are independent random variables with the error distribution \(\chi\), and we note that \(\alpha_i + s\beta_i = s^2w' - td_i\). The output of the BGV Relinearize operation is the 2-part ciphertext \((\overline{c}_0, \overline{c}_1)\) given by
\[
\overline{c}_0 = c_0^s + \sum_{i=0}^{\ell} \alpha_i g_i \quad \text{and} \quad \overline{c}_1 = c_1^s + \sum_{i=0}^{\ell} \beta_i g_i.
\]
The BGV Critical Value \(W_{\text{relin}}\) of this 2-part ciphertext \((\overline{c}_0, \overline{c}_1)\) is given by
\[
W_{\text{relin}} = \overline{c}_0 + \overline{c}_1 = c_0^s + \sum_{i=0}^{\ell} \alpha_i g_i + s c_1^s + s \sum_{i=0}^{\ell} \beta_i g_i
= c_0^s + s c_1^s + \sum_{i=0}^{\ell} (\alpha_i + s\beta_i) g_i = c_0^s + s c_1^s + s^2 \sum_{i=0}^{\ell} w^i g_i - t \sum_{i=0}^{\ell} d_i g_i
= c_0^s + s c_1^s + s^2 c_2^s - t \sum_{i=0}^{\ell} d_i g_i = W - t \sum_{i=0}^{\ell} d_i g_i,
\]
where \(W = c_0^s + s c_1^s + s^2 c_2^s\) is the BGV Critical Value for the 3-part ciphertext \((c_0^s, c_1^s, c_2^s)\). Thus the BGV Relinearize operation has noise random variable \(V_{\text{relin}}\) given by
\[
V_{\text{relin}} = V - t \sum_{i=0}^{\ell} d_i g_i.
\]
A component \(d_{ij}\) of \(d\) has mean \(E(d_{ij}) = 0\) and variance \(\text{Var}(d_{ij}) = \sigma^2\), and a component \(g_{ij}\) has mean \(E(g_{ij}) = 0\) and variance \(\text{Var}(g_{ij}) = \frac{1}{12}w^2\) as \(g_{ij}\) is uniformly distributed between \(-\frac{1}{2}w\) and \(\frac{1}{2}w\). Thus Lemma 2 shows that \(d_i g_i \sim N(0; \frac{1}{12}nw^2\sigma^2)\), and hence that
\[
t \sum_{i=0}^{\ell} d_i g_i \sim N(0; \frac{1}{12}n(\ell + 1)w^2t^2\sigma^2 I_n).
\]
Thus the BGV Relinearize operation has a noise random variable \(V_{\text{relin}}\) with a distribution
\[
V_{\text{relin}} \sim N(0; (\rho^2 + \frac{1}{12}n(\ell + 1)w^2t^2\sigma^2) I_n),
\]
with component variance \(\rho_{\text{relin}}^2 = \rho^2 + \frac{1}{12}n(\ell + 1)w^2t^2\sigma^2\).
The BGV ModSwitch operation is, as we noted earlier, the key technical tool for noise management in BGV and is used to move from a modulus $q$ to a smaller modulus $p$. We first give in Lemma 8 a technical result that we will rely on in the following lemma. Lemma 9 then gives an expression for the component variance $\rho^2_{\text{mod-sw}(s)}$ of the noise random variable for the BGV ModSwitch operation for a ciphertext with respect to a secret key $s$. Heuristic 3 then gives a Normal distribution that accurately approximates the noise random variable for a ciphertext obtained from a BGV ModSwitch operation.

We note that in Lemma 9, the first term $\gamma^2 \rho^2 = \left( \frac{p}{q} \right)^2 \rho^2$ is much smaller than the second term $\frac{1}{12}(|s|^2 + 1)(t^2 - 1)$ in many situations of interest, in which case the noise component variance $\rho^2_{\text{mod-sw}} \approx \frac{1}{12} \left( \frac{2n + 1}{3} \right)(t^2 - 1)$ does not depend on the input noise variance $\rho^2$ or the ratio of $p$ and $q$.

**Lemma 8.** Suppose that $q$ and $t$ are odd positive integers with $q \gg t$, and let $Q = \{-\frac{1}{2}(q-1), \ldots, \frac{1}{2}(q-1)\}$ and $T = \{-\frac{1}{2}(t-1), \ldots, \frac{1}{2}(t-1)\}$. If $Z \sim \text{Uni}(Q)$ and $|\gamma| \ll 1$ then the random variable $(Z - \lfloor \gamma Z \rfloor) \mod t$ has a distribution very close to Uniform on $T$.

**Proof.** We address the distribution of $((Z - \lfloor \gamma Z \rfloor) \mod t)$ by considering the mapping $g: Q \to T$ given by $g(x) = (x - \lfloor \gamma x \rfloor) \mod t$.

We first consider the restriction of the mapping $g$ to the set $Q_k = \{z \in Q \mid z = k \mod t\}$ of “modulo $q$” values that have the value $k$ modulo $t$, that is to say the mapping $g_k: Q_k \to T$ given by $g_k(x) = (x - \lfloor \gamma x \rfloor) \mod t$.

For $|\gamma| \ll 1$, the mapping $g_k$ can be regarded as a random mapping of the finite set $Q_k$ to the finite set $T$, so for $x \in Q_k$ and $y \in T$ the random variable

$$Z_{k,x,y} = \begin{cases} 1 & \text{if } g_k(x) = y \\ 0 & \text{if } g_k(x) \neq y \end{cases}$$

has a Bernoulli distribution with parameter $\frac{1}{\#T} = \frac{1}{t}$. The number the pre-images under $g_k$ in $Q_k$ of a given $y \in T$ is the random variable

$$R_{k,y} = \sum_{x \in Q_k} Z_{k,x,y} = \#\{x \in Q_k \mid g^{-1}(y) = x\}.$$

Thus the number the pre-images of $y \in T$ under $g_k$ has a Binomial distribution as it is the sum of independent Bernoulli random variables, so we have

$$R_{k,y} \sim \text{Bin}(\#Q_k, t^{-1}).$$
The number of pre-images under $g$ in $Q$ of an element $y \in T$ is the random variable
\[ P_y = \sum_{k \in T} R_{k,y} = \sum_{k \in T} \sum_{x \in Q_k} Z_{k,x,y} = \# \{ x \in Q \mid g^{-1}(y) = x \}. \]

The number of pre-images of $y \in T$ under $g$ in $Q$ is therefore the sum of Binomial random variables with the same probability parameter, so has a Binomial distribution (noting that $\sum_{k \in T} \#Q_k = \#Q = q$) given by
\[ P_y \sim \text{Bin}(q,t^{-1}) \]
with mean $E(P_y) = \frac{q}{t}$ and variance $\text{Var}(P_y) = \frac{q}{t} \left( 1 - \frac{1}{t} \right)$. This Binomial distribution for $P_y$ can be approximated using the standard technique of approximating such a Binomial distribution by an appropriate Normal distribution, given for example by the Central Limit approximation to the sum of $Z_{k,x,y}$. Thus we can write
\[ P_y \sim N \left( \frac{q}{t}, \frac{q}{t} \left( 1 - \frac{1}{t} \right) \right). \]

The distribution of $g(Z) = ((Z - \lceil \gamma Z \rceil) \mod t)$ for $Z \sim \text{Uni}(Q)$ is therefore given by $P(g(Z) = k)$ for $k \in T$, where
\[ P(g(Z) = k) \text{ is given by } \frac{P_y}{q} \sim N \left( \frac{1}{t}, \frac{1}{tq} \left( 1 - \frac{1}{t} \right) \right), \]
This random variable has mean $E \left( \frac{P_y}{q} \right) = \frac{1}{t}$ and standard deviation satisfying
\[ \text{St Dev} \left( \frac{P_y}{q} \right) = \frac{1}{(tq)^{\frac{1}{2}}} \left( 1 - \frac{1}{t} \right)^{\frac{1}{2}} < \left( \frac{t}{q} \right)^{\frac{1}{2}} \frac{1}{t}. \]

However, $t \ll q$, so $\left( \frac{t}{q} \right)^{\frac{1}{2}}$ is very small, showing that $P(g(Z) = k)$ is very close to $\frac{1}{t}$. Thus $g(Z)$ is approximated by a Uniform distribution on $T$.

**Lemma 9. [ModSwitch]** Suppose that a BGV ciphertext $(c_0, c_1)$ with respect to a modulus $q$ has a 0-mean multivariate Normal noise random variable given by $V \sim N(0; \rho^2 I_n)$. Then the output ciphertext $(c'_0, c'_1)$ after a ModSwitch operation of this ciphertext to a modulus $p \ll q$ has noise random variable $V_{\text{mod-sw}(s)} \sim N(0; \rho_{\text{mod-sw}(s)}^2 I_n)$, where the component variance $\rho_{\text{mod-sw}(s)}^2$ is given in terms of the contraction factor $\gamma = \frac{p}{q}$ as
\[ \rho_{\text{mod-sw}(s)}^2 = \gamma^2 \rho^2 + \frac{1}{12} \left( |s|^2 + 1 \right) (t^2 - 1). \]
Proof. Lemma 1 shows that the output ciphertext \((c'_0, c'_1)\) (with modulus \(p\)) following the application of the BGV \texttt{ModSwitch} to the input ciphertext \((c_0, c_1)\) (with modulus \(q\)) is given by
\[
c'_i = [\rho c_i] + ((c_i - [\rho c_i]) \mod t) \quad [i = 0, 1],
\]
In order to analyse the BGV \texttt{ModSwitch} operation, we define
\[
U_i = ((c_i - [\rho c_i]) \mod t) = c'_i - [\rho c_i] \quad [i = 0, 1],
\]
which we can regard as integer random variables with independent components \(U_{ij}\) taking values in the set \(\mathcal{T} = \{\frac{1}{2}(t - 1), \ldots, \frac{1}{2}(t - 1)\}\) of modulo \(t\) values (where \(t\) is odd). Lemma 8 shows that these integer random variables \(U_{ij}\) have a distribution very close to Uniform \(T\) for BGV moduli \(p < q\) (as \(|\gamma| \ll 1\)).

The BGV Critical Value \(W_{\text{mod-sw}}\) for the decryption of this ciphertext \((c'_0, c'_1)\) obtained from the BGV \texttt{ModSwitch} operation is
\[
W_{\text{mod-sw}(s)} = c'_0 + s c'_1 = [\rho c_0] + s|\rho c_1| + (U_0 + sU_1)
= \gamma (c_0 + s c_1) + (U_0 + sU_1) + ([\rho c_0] + s|\rho c_1| - \gamma(c_0 + s c_1))
= \gamma W + (U_0 + sU_1) + (([\rho c_0] - \gamma c_0) + s([\rho c_1] - \gamma c_1)),
\]
We note that the final term \((c_0 - \gamma c_0) + s|\gamma c_1| - \gamma c_1)\) arises from rounding components to the nearest integers. Thus this term is negligible as each component consists of the sum of \((1 + |s|) \approx (\frac{2}{3}n + 1) \text{Unif}((\frac{1}{2}, \frac{1}{2}))\) rounding random variables, and so for practical purposes the BGV \texttt{ModSwitch} Critical Value is given by
\[
W_{\text{mod-sw}(s)} = \gamma W + (U_0 + sU_1).
\]

The BGV \texttt{ModSwitch} noise random variable \(V_{\text{mod-sw}}\) corresponding to this BGV \texttt{ModSwitch} Critical Value is is given by
\[
V_{\text{mod-sw}(s)} = \gamma V + (U_0 + sU_1).
\]

The first term \(\gamma V \sim \mathcal{N}(0; \gamma^2 \rho^2 I_n)\) in this expression has a symmetric multivariate Normal distribution with mean 0 and component variance \(\gamma^2 \rho^2\). A component \((U_0 + sU_1)_j\) of the second term \(U_0 + sU_1\) is a sum of \((1 + |s|^2)\) independent \text{Unif}(-\frac{1}{2}t, \frac{1}{2}t)\) random variables, so the Central Limit Theorem shows that the component \((U_0 + sU_1)_j\) can be regarded as having a Normal distribution with \(\mathcal{N}(0, \frac{1}{12}(1 + |s|^2)(t^2 - 1))\) for large \(n\) with component variance \(\frac{1}{12}(1 + |s|^2)(t^2 - 1)\). Thus the noise random variable \(V_{\text{mod-sw}}\) of BGV \texttt{ModSwitch} operation has a distribution given by
\[
V_{\text{mod-sw}(s)} \sim \mathcal{N}\left(0; \rho^2_{\text{mod-sw}(s)} I_n\right), \text{ where } \rho^2_{\text{mod-sw}(s)} = \gamma^2 \rho^2 + \frac{1}{12}(1 + |s|^2)(t^2 - 1).
\]

Heuristic 3 [\texttt{ModSwitch}] The noise random variable \(V_{\text{mod-sw}}\) for a BGV ciphertext after a \texttt{ModSwitch} operation can be accurately approximated \(V_{\text{mod-sw}} \sim \mathcal{N}(0; \rho^2_{\text{mod-sw}} I_n)\) by a Normal distribution with component variance \(\rho^2_{\text{mod-sw}}\) given by
\[
\rho^2_{\text{mod-sw}} = \gamma^2 \rho^2 + \frac{1}{12}(\frac{2}{3}n + 1)(t^2 - 1).
\]
The result can be obtained by approximating the Normal mixture distribution for $V_{\text{mod-sw}}$ by the stated Normal distribution using the argument given in the Justification for Heuristic 1.

### 3.3 Experimental verification

The analysis of the previous subsections shows that the noise in a BGV ciphertext can, under certain assumptions, be expressed as a multivariate Normal random variable after every homomorphic operation. The analysis is summarised in Figure 5. This enables us to model the noise growth throughout a BGV homomorphic evaluation in an 'average-case' manner, as was done for TFHE in [7], that is, tracing through the variances at each operation, in order to find the variance of the noise in the output ciphertext. The variance can then be used to determine a bound on the noise in the output ciphertext to set parameters for correctness. Such an average-case approach is in contrast to a 'worst-case' analysis, as employed in prior studies on BGV [16, 10, 9]; that is, tracing through a bound on the noise at each operation in order to determine a bound on the noise in the output ciphertext. Since worst-case bounds are used in these prior studies at each step, we expect that the final bound could be very loose. This was confirmed by experiments in [9], which compared the observed noise growth in the HElib [19] implementation of BGV to the predicted noise growth from worst-case analyses.

<table>
<thead>
<tr>
<th>BGV Operation</th>
<th>Component variance of input noise(s)</th>
<th>Component variance of output noise(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt</td>
<td>$\rho^2, \rho^2$</td>
<td>$(\frac{3}{2}n + 1) t^2 \sigma^2$</td>
</tr>
<tr>
<td>Add</td>
<td>$\rho^2, \rho^2$</td>
<td>$\rho^2 + \rho^2$</td>
</tr>
<tr>
<td>Multiply</td>
<td>$\rho^2$</td>
<td>$n \rho^2 \rho^2 + \rho^2</td>
</tr>
<tr>
<td>Relinearize</td>
<td>$\rho^2$</td>
<td>$\rho^2 + \frac{1}{12} n (k + 1) w^2 t^2 \sigma^2$</td>
</tr>
<tr>
<td>ModSwitch</td>
<td>$\rho^2$</td>
<td>$\gamma^2 \rho^2 + \frac{1}{12} (\frac{3}{2}n + 1) (t^2 - 1)$</td>
</tr>
</tbody>
</table>

**Fig. 5.** Component variances in the zero-mean Normal random variable giving the noise in the output ciphertext after homomorphic evaluation operations on input ciphertexts with input noises given by the zero-mean Normal random variables of the given component variances. (Other notation as given in Lemmas 3-9.)

In this section, we illustrate the efficacy of our average-case approach by comparing the noise growth predicted by these with observed noise growth in both HElib [19] and SEAL [32] and with the noise growth predicted by worst-case bounds as developed in [9] following Iliashenko [20]. Our experiments use HElib version 2.2.1 and SEAL version 4.0. We show that our average-case analysis can better estimate the practical noise growth, thus narrowing the gap between worst-case predicted noise and practically observed noise highlighted in [9]. To do so, we consider the homomorphic evaluation of two circuits. The results for
HElib are displayed in Tables 1 and 2 respectively. The results for SEAL are displayed in Tables 3 and 4 respectively.

The first circuit considered is the same circuit as was used in [9]. The evaluation is as follows in the $i$-th trial. First, fresh ciphertexts $ct_1$ and $ct_2$ encrypting $i+1$ and $i$ are generated. Next, $ct_3$ is generated as the homomorphic addition of $ct_1$ and $ct_2$. Next, $ct_4$ is generated as the homomorphic multiplication of $ct_3$ and $ct_2$. For $n > 2048$, $ct_5$ is generated by modulus switching $ct_4$ down to the next prime in the chain (for $n = 2048$ the parameters are too small to support this operation). We measure the noise budget after each operation and output an average over 10000 trials. The results for HElib and SEAL are presented in Table 1 and Table 3 respectively.

We also explore the noise growth in a second deeper circuit, using the same parameter settings as the previous experiment. The evaluation is as follows in the $i$-th trial. First, fresh ciphertexts $ct_1, \ldots, ct_8$ encrypting $i+1, \ldots, i+8$ respectively are generated. Next, ciphertexts $ct_9, \ldots, ct_{12}$ are generated as the multiplication of $ct_1$ and $ct_2; \ldots; ct_7$ and $ct_8$ respectively. Next ciphertexts $ct_{13}$ and $ct_{14}$ are generated as the multiplication of $ct_9$ and $ct_{10}$; and $ct_{11}$ and $ct_{12}$ respectively. Finally, ciphertext $ct_{15}$ is generated as the multiplication of $ct_{13}$ and $ct_{14}$. We measure the noise budget after each multiplication and output an average over 10000 trials. The results for HElib and SEAL are presented in Table 2 and Table 4 respectively.

For both circuits, the HElib parameters were chosen as follows. The standard deviation of the error distribution was set to $\sigma = 3.2$, the ring dimension was set to $n \in \{2048, 4096, 8192, 16384\}$ and the corresponding maximal ciphertext modulus $q$ was set so that $\log q \in \{54, 109, 218, 438\}$. The plaintext modulus was set as $t = 3$. Other parameters are set according to HElib default parameter settings, detailed in [9]. The parameter set $n = 2048$ is omitted in Table 2 as it is too small to support the homomorphic evaluation of the circuit.

For both circuits, the SEAL parameters were chosen as follows. The standard deviation of the error distribution was set to $\sigma = 3.2$, the ring dimension was set to $n \in \{4096, 8192, 16384, 32768\}$ and the corresponding maximal ciphertext modulus $q$ was set so that $\log q \in \{109, 218, 438, 881\}$. The plaintext modulus was set to be a suitable integer of 20 bits, a default choice in the SEAL examples. In SEAL, the parameter sets with $n \in \{4096, 8192\}$ were too small to support the deeper circuit.

We present average case bounds for each operation as follows: we trace through the component variance of the noise polynomial after each operation, using the formulae in Figure 5. We model the variance after multiplication as in Heuristic 2. We then translate the variance after each operation into a bound on the noise after each operation following the approach described in [8]. That is, we allow an error tolerance $\alpha$ (we set $\alpha = 0.001$ in the experiments), such that our noise bound is exceeded with probability $\alpha$.

**Lemma 10 ([8]).** Suppose a noise polynomial is distributed as $\mathcal{N}(0, \rho^2 I_n)$. For a threshold $T > 0$, the error tolerance $\alpha = \mathbb{P}(\|Z\|_\infty > T)$ satisfies

$$T = \sqrt{2} \cdot \rho \cdot \text{erf}^{-1}(\sqrt{1 - \alpha})^\frac{1}{2}. \)
We express our results in terms of the noise budget (Definition 7). Loosely speaking, the noise budget is the number of bits left for homomorphic computation before a wraparound modulo \( q \) that would lead to decryption failure.

**Definition 7 ([9]).** Let \( ct \) be a BGV ciphertext with respect to modulus \( q \) having Critical Value \( W \) modulo \( q \). The noise budget for this ciphertext is defined as

\[
\log_2 (q) - \log_2 (\|W\|) - 1.
\]

The HElib results in Tables 1 and 2 show that the average-case approach much more closely models the observed noise growth for fresh ciphertexts, addition, and multiplication. While the average-case modelling does not completely close the heuristic-to-practical gap identified in [9], the improvement is still significant. For example, the gap is reduced by as much as 25 bits in the case of the deeper circuit.

The SEAL results of Tables 3 and 4 are even more promising and show that the average-case heuristics more closely model the observed noise growth for fresh ciphertexts, addition, and multiplication, including deeper multiplication. In several cases, the heuristic-to-practical gap is reduced to only 3-5 bits.

There are some discrepancies between the SEAL implementation and the heuristic estimates that may account for differences between the observed and predicted behaviour. For example, in Table 4, for \( n = 16384 \), after the third multiplication, the average-case heuristic overestimates the remaining noise budget by one bit. We do not relinearize (in doing so, diverging from the SEAL recommendations), so by the third multiplication in the second circuit, the ciphertexts are much larger. This introduces additional noise not accounted for in the heuristics. We would expect such an additional noise to increase as \( n \) increases, and this expectation is confirmed by the results for \( n = 32768 \). Moreover, modifying our experiments to relinearize inputs before the next multiplication significantly reduces (but does not totally account for) the overestimation.

For modulus switching, in both libraries, the remaining noise budget is overestimated by the average-case approach. This may also be due to specificities in the libraries. For example, in our HElib implementation we modulus switch to the ‘natural’ prime set following the expected usage of the library, whereas the heuristic analyses are for a general situation of modulus switching to any \( p \). Modifying HElib to explore this further is beyond the scope of this work.

Both our worst-case and average-case heuristic estimates assume that the secret distribution is uniform ternary, as is done in our analysis of Section 3.2, and as is the distribution used in SEAL. The secret distribution implemented in HElib is also ternary, but with a slightly different variance\(^1\). We found that this discrepancy impacts the heuristic-to-practical gap only minimally. Indeed, adapting the heuristics for the HElib secret distribution made no difference in the predicted remaining average-case noise budget in low-depth computation, while

\(^1\) https://github.com/homenc/HElib/blob/f0e3e010009c592cd411ba96baa8376eb485247a/src/keys.cpp#L1145
The column $\tau$ gives the observed mean of the noise budget in HElib ciphertexts over 10000 trials of the homomorphic evaluation described in the first circuit and in [9] for parameter sets with dimension $n \in \{2048, 4096, 8192, 16384\}$. The column $W$ gives an estimate of the noise budget using worst-case heuristic bounds following [9]. The column $A$ gives an estimate of the noise budget using an average case approach.

<table>
<thead>
<tr>
<th>$n$</th>
<th>Enc</th>
<th>Add</th>
<th>Multi</th>
<th>ModSwitch</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$W$</td>
<td>$A$</td>
<td>$\tau$</td>
<td>$W$</td>
</tr>
<tr>
<td>2048</td>
<td>35.0</td>
<td>41.0</td>
<td>48.7</td>
<td>34.0</td>
</tr>
<tr>
<td>4096</td>
<td>89.0</td>
<td>96.0</td>
<td>104</td>
<td>88.0</td>
</tr>
<tr>
<td>8192</td>
<td>199</td>
<td>206</td>
<td>213</td>
<td>198</td>
</tr>
<tr>
<td>16384</td>
<td>417</td>
<td>425</td>
<td>433</td>
<td>416</td>
</tr>
</tbody>
</table>

Table 1. The column $\tau$ gives the observed mean of the noise budget in HElib ciphertexts over 10000 trials of the homomorphic evaluation described in the first circuit and in [9] for parameter sets with dimension $n \in \{2048, 4096, 8192, 16384\}$. The column $W$ gives an estimate of the noise budget using worst-case heuristic bounds following [9]. The column $A$ gives an estimate of the noise budget using an average case approach.

for larger $n$, and after two or more multiplications, the predicted remaining noise budget was 2 bits closer to the observed remaining noise budget.

The results for $n = 4096$ in Table 3 give an interesting example where the worst-case approach predicts that there is no remaining noise budget after the multiplication, suggesting that the parameter set is too small to support the evaluation of this circuit. In contrast, the average-case analysis predicts there are 6 bits remaining, and indeed there is an observed average remaining noise budget of 8 bits. Following a worst-case analysis in this context would suggest to perform the computation in dimension at least $n = 8192$, leading to a consequent performance slowdown, as (e.g.) more coefficients must be processed during each homomorphic operation. In fact, as suggested by the average-case analysis, the computation can be performed for $n = 4096$. This illustrates that the use of an average-case approach can lead to a practical improvement when it comes to parameter selection, e.g., if $n$ were to be chosen in an automated way based on the predicted noise growth by an FHE compiler.

To further illustrate the utility of the average-case approach, we now exhibit additional specific computations for which the average-case approach predicts lower parameters to support the computation than the worst-case approach. The examples here are illustrative and we expect that many other such circuits could be found. To characterise a broad range of circuits, we focus on an $L$-level circuit with $\zeta$ additions and one multiplication at each level. We fix ciphertext moduli $q$ that achieve 128-bit security according to the Homomorphic Encryption Security Standard [1] for error distribution standard deviation $\sigma = 3.2$, uniform ternary secret, and $n \in \{4096, 8192, 16384\}$; and allow to vary the plaintext modulus $t$.

Given a circuit parameterised by $L$, $\zeta$ and $t$, we investigate the predicted noise growth for different parameter sets according to the average-case and worst-case approaches.

We exhibit in Table 5 an example for $L = 3$, $\zeta = 8$, and $t = 256$, following parameter choices in [9]. It can be seen that the worst-case approach indicates that the $n = 16384$ parameter set is required, while the average-case approach indicates that $n = 8192$ suffices. In Table 6, we see another example, for $L = 2$, $\zeta = 3$, and $t = 257$. In this situation, the average-case approach predicts that
Table 2. The column $\bar{x}$ gives the observed mean of the noise budget in HElib ciphertexts over 10000 trials of the homomorphic evaluation described above in the second circuit for parameter sets with dimension $n \in \{4096, 8192, 16384\}$. The column $W$ gives an estimate of the noise budget using worst-case heuristic bounds following [9]. The column $A$ gives an estimate of the noise budget using an average case approach.

<table>
<thead>
<tr>
<th>$n$</th>
<th>Enc</th>
<th>Mult1</th>
<th>Mult2</th>
<th>Mult3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$W$</td>
<td>$A$</td>
<td>$\bar{x}$</td>
<td>$W$</td>
</tr>
<tr>
<td>4096</td>
<td>89.0</td>
<td>96.0</td>
<td>104</td>
<td>71.0</td>
</tr>
<tr>
<td>8192</td>
<td>199</td>
<td>206</td>
<td>213</td>
<td>180</td>
</tr>
<tr>
<td>16384</td>
<td>417</td>
<td>425</td>
<td>433</td>
<td>397</td>
</tr>
</tbody>
</table>

Table 3. The column $\bar{x}$ gives the observed mean of the noise budget in SEAL ciphertexts over 10000 trials of the homomorphic evaluation described in the first circuit and in [9] for parameter sets with dimension $n \in \{2048, 4096, 8192, 16384\}$. The column $W$ gives an estimate of the noise budget using worst-case heuristic bounds following [9]. The column $A$ gives an estimate of the noise budget using an average case approach.

<table>
<thead>
<tr>
<th>$n$</th>
<th>Enc</th>
<th>Add</th>
<th>Mult</th>
<th>ModSwitch</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$W$</td>
<td>$A$</td>
<td>$\bar{x}$</td>
<td>$W$</td>
</tr>
<tr>
<td>4096</td>
<td>34.0</td>
<td>40.0</td>
<td>44.0</td>
<td>33.0</td>
</tr>
<tr>
<td>8192</td>
<td>135</td>
<td>142</td>
<td>146</td>
<td>134</td>
</tr>
<tr>
<td>16384</td>
<td>349</td>
<td>357</td>
<td>360</td>
<td>348</td>
</tr>
<tr>
<td>32768</td>
<td>784</td>
<td>792</td>
<td>796</td>
<td>783</td>
</tr>
</tbody>
</table>

Table 4. The column $\bar{x}$ gives the observed mean of the noise budget in SEAL ciphertexts over 10000 trials of the homomorphic evaluation described above in the second circuit for parameter sets with dimension $n \in \{4096, 8192, 16384\}$. The column $W$ gives an estimate of the noise budget using worst-case heuristic bounds following [9]. The column $A$ gives an estimate of the noise budget using an average case approach.

<table>
<thead>
<tr>
<th>$n$</th>
<th>Enc</th>
<th>Mult1</th>
<th>Mult2</th>
<th>Mult3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$W$</td>
<td>$A$</td>
<td>$\bar{x}$</td>
<td>$W$</td>
</tr>
<tr>
<td>16384</td>
<td>349</td>
<td>357</td>
<td>361</td>
<td>341</td>
</tr>
<tr>
<td>32768</td>
<td>784</td>
<td>792</td>
<td>796</td>
<td>745</td>
</tr>
</tbody>
</table>

The $n = 4096$ parameter set suffices to support the computation, while the worst-case approach suggests $n = 8192$ is required. We implemented this latter circuit in HElib, and found indeed that the computation could be supported with $n = 4096$.

4 A CLT approach to SymHom noise analysis

In this section, we present a Central Limit approach to SymHom noise analysis. For simplicity, we restrict our discussion to the situation where $m$ is prime, though our arguments apply more generally.
<table>
<thead>
<tr>
<th>( n )</th>
<th>( W )</th>
<th>( A )</th>
</tr>
</thead>
<tbody>
<tr>
<td>8192</td>
<td>0</td>
<td>17</td>
</tr>
<tr>
<td>16384</td>
<td>183</td>
<td>229</td>
</tr>
</tbody>
</table>

Table 5. The column \( W \) gives an estimate of the noise budget for the circuit parameterised by \( L = 3, \zeta = 8, t = 256 \), for the parameter set determined by the ring dimension \( n \), using worst-case heuristic bounds following [9]. The column \( A \) gives an estimate of the noise budget for the same circuit using an average case approach.

<table>
<thead>
<tr>
<th>( n )</th>
<th>( W )</th>
<th>( A )</th>
</tr>
</thead>
<tbody>
<tr>
<td>4096</td>
<td>0</td>
<td>19</td>
</tr>
<tr>
<td>8192</td>
<td>105</td>
<td>124</td>
</tr>
</tbody>
</table>

Table 6. The column \( W \) gives an estimate of the noise budget for the circuit parameterised by \( L = 2, \zeta = 3, t = 257 \), for the parameter set determined by the ring dimension \( n \), using worst-case heuristic bounds following [9]. The column \( A \) gives an estimate of the noise budget for the same circuit using an average case approach.

4.1 Additional background

In this section, we introduce some relevant definitions. Definition 8 specifies the \( p\Gamma \)-basis for \( H \) in which elements of \( H \) are expressed as real-valued vectors. The \( p\Gamma \)-basis arises as the embedding of a basis of conjugate pairs for \( R^\vee \). The \( p\Gamma \)-basis is a more convenient basis for \( H \) in the case when \( m \) is prime, and is a suitable basis for decryption.

**Definition 8.** The \( p\Gamma \)-basis for \( H \) is given by the columns of the matrix \( p\Gamma \) (for \( p \) prime), where

\[
\Gamma = \frac{1}{m} \begin{pmatrix}
1 - \zeta_m^1 & 1 - \zeta_m^2 & 1 - \zeta_m^3 & \ldots & 1 - \zeta_m^n \\
1 - \zeta_m^2 & 1 - \zeta_m^4 & 1 - \zeta_m^6 & \ldots & 1 - \zeta_m^{2n} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 - \zeta_m^n & 1 - \zeta_m^{2n} & 1 - \zeta_m^{3n} & \ldots & 1 - \zeta_m^{n^2}
\end{pmatrix},
\]

and is the embedding of the basis \( \{ \frac{p}{m}(1 - \zeta_m^1), \frac{p}{m}(1 - \zeta_m^2), \ldots, \frac{p}{m}(1 - \zeta_m^n) \} \) of conjugate pairs for \( R^\vee \) in \( H \).

In Figure 6, we summarise our notation for elements of \( H \) expressed with respect to the various bases. If \( Z \) is a vector expressing an element of \( H \) as a vector of conjugate pairs in the \( I \)-basis (or standard basis) for \( H \), then we have real-valued vectors \( Z^T = T^T Z \) and \( Z^* = (p\Gamma)^{-1} Z \) expressing this element as a vector in the \( T \)-basis and the \( p\Gamma \)-basis for \( H \) respectively.

The change of basis transformations between the \( T \)-basis and the \( p\Gamma \)-basis are summarised in Figure 7, and the relevant properties of the (scaled) change-of-basis matrix \( \Delta = \Gamma T^{-1} \) are given in Lemma 11.

**Lemma 11.** The change of basis matrix from the \( T \)-basis to the \( p\Gamma \)-basis of \( H \) is the real invertible matrix \( p^{-1} \Delta \), where \( \Delta = \Gamma^{-1} T \) satisfies \( \Delta \Delta^T = mI - J \).
<table>
<thead>
<tr>
<th>Basis for $H$</th>
<th>$I$-Basis</th>
<th>$T$-Basis</th>
<th>$pI$-Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vector or Random Variable</td>
<td>$Z$</td>
<td>$Z^I$</td>
<td>$Z^*$</td>
</tr>
<tr>
<td>Transformation from the $I$-Basis</td>
<td>$I$</td>
<td>$T^I$</td>
<td>$p^{-1}I^{-1}$</td>
</tr>
</tbody>
</table>

*Fig. 6.* Notation for the expression of an element of $H$ as a vector in the various different vector space bases for $H$. Note that $p$ is a scaling factor.

$$H \text{ with } T\text{-basis} \leftrightarrow \frac{p^{-1}\Delta = (pI)^{-1}T}{p\Delta^{-1} = T^{-1}(pI)} \rightarrow H \text{ with } pI\text{-basis}$$

*Fig. 7.* Change of Basis Matrices for the $T$-basis and $pI$-basis for $H$ in which elements of $H$ are expressed as real-valued vectors.

**Proof.** It is clear that $\Delta = I^{-1}T$ is invertible as both $I^{-1}$ and $T$ are invertible. The matrix $\Delta^{-1} = I^{-1}T = T^I I^\dagger$ has matrix entries $\Delta^{-1}_{kl}$ satisfying

$$m \Delta^{-1}_{kl} = \begin{cases} 2^{-\frac{1}{2}} ((1 - \zeta^{kl}_m) + (1 - \zeta^{-kl}_m)) & \text{if } k \leq n' \leq n \\ 2^{-\frac{1}{2}} (-i (1 - \zeta^{kl}_m) + i (1 - \zeta^{-kl}_m)) & \text{if } n' < k \leq n, \end{cases}$$

so $\Delta^{-1}$ and hence $\Delta$ are real matrices. Thus we have

$$\Delta \Delta^T = \Delta \Delta^I = (I^{-1}T) (I^{-1}T)^I = I^{-1}TT^I (I^{-1})^I = (I^\dagger I)^{-1}.$$ 

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

$$(I^\dagger I)_{jk} = \sum_{l=1}^n I^\dagger_{jl} I_{lk} = \frac{1}{m^2} \sum_{l=1}^n (1 - \zeta^{-jl})(1 - \zeta^{lk})$$

$$= \frac{1}{m^2} \sum_{l=1}^n 1 - \frac{1}{m^2} \sum_{l=1}^n \zeta^{lk} - \frac{1}{m^2} \sum_{l=1}^n \zeta^{-jl} + \frac{1}{m^2} \sum_{l=1}^n \zeta^{l(k-j)}$$

$$= \begin{cases} 2m^{-2}(n + 1) = 2m^{-1} & \text{if } k = j \\ m^{-2}(n + 1) = m^{-1} & \text{if } k \neq j, \end{cases}$$

so $I^\dagger I = m^{-1}(I + J)$. Thus $\Delta \Delta^T = (I^\dagger I)^{-1} = mI - J$.

The noise in a SymHom ciphertext obtained as the output of a homomorphic multiplication of two fresh ciphertexts is the product of the noises in the input ciphertexts. We will therefore be interested in the $\otimes$-product (Definition 9) of two elements of $H$ expressed in the $T$-basis.
Definition 9. The ⊗-product of two real vectors $u = (u_{11}, u_{12}, \ldots, u_{n'1}, u_{n'2})$ and $v = (v_{11}, v_{12}, \ldots, v_{n'1}, v_{n'2})$ of length $n = 2n'$ is

\[
\begin{pmatrix}
  u_{11} \\
  u_{12} \\
  \vdots \\
  u_{n'1} \\
  u_{n'2}
\end{pmatrix} \otimes
\begin{pmatrix}
  v_{11} \\
  v_{12} \\
  \vdots \\
  v_{n'1} \\
  v_{n'2}
\end{pmatrix} = T^\dagger (TuTv) = 2^{-\frac{1}{2}}
\begin{pmatrix}
  u_{11}v_{11} - u_{12}v_{12} \\
  u_{11}v_{12} + u_{12}v_{11} \\
  \vdots \\
  u_{n'1}v_{n'1} - u_{n'2}v_{n'2} \\
  u_{n'1}v_{n'2} + u_{n'2}v_{n'1}
\end{pmatrix}.
\]

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

4.2 A Central Limit approach to approximate the distribution of $C(p\Gamma)$

To obtain a Normal approximation for a weighted sum $\sum_{j=1}^{n} a_j X_j$ of the form encountered in SymHom, we need a general form of the Central Limit Theorem formally given by the Lindeberg condition [3, 34]. We state such a Central Limit result in Lemma 12. However, Lemma 12 can be informally expressed as that the weighted sum $\sum_{j=1}^{n} a_j X_j$ of the form encountered in Ring-LWE has an approximate Normal distribution for moderate or large $n$ provided that the absolute weights $a_j$ are not dominated by just a few values.

Lemma 12. Suppose $X_1, X_2, \ldots$ are independent and identically distributed continuous random variables that are symmetric about 0 with mean $E(X_j) = 0$ and variance $\text{Var}(X_j) = 1$, and that have common density function $f_{X_j}$, and suppose that for constants $a_1, a_2, \ldots$ the sum $\sum_{j=1}^{l} a_j X_j$ has variance function $a(l)^2 = \sum_{j=1}^{l} a_j^2$, and that the functions $\tilde{a}_j$ are defined by $\tilde{a}_j(l) = \frac{|a_j|}{a(l)}$. In this case, Lindeberg’s condition is that for any given $\epsilon > 0$, the sum

\[
\sum_{j=1}^{l} \tilde{a}_j(l)^2 \Psi_{X_j} \left( \frac{\epsilon}{\tilde{a}_j(l)} \right) \rightarrow 0 \quad \text{as} \quad l \rightarrow \infty,
\]

where $\Psi_{X_j}(\theta) = \int_{-\infty}^{\infty} x^2 f_{X_j}(x) \, dx$.

If Lindeberg’s condition is satisfied, then $a(l)^{-1} \sum_{j=1}^{l} a_j X_j$ tends in distribution to a standard Normal $\mathcal{N}(0, 1)$ distribution as $l \rightarrow \infty$.

Proposition 1 gives a Central Limit approximation to a weighted multivariate sum of the form for independent and identically distributed random variables $X_1, \ldots, X_n$. This proposition is a summary of the Lindeberg condition for a Central Limit Theorem and essentially states that a good Normal approximation exists for the weighted sum if enough of the largest (in absolute value) weights are of comparable size. Concretely, in a typical parameter situation of Ring-LWE where we have $n > 10^2$, (or $n > 10^3$ in the case of homomorphic encryption), we can expect Proposition 1 to give a good approximation when as few as (for example) about 20 of the largest weights are comparable.
Proposition 1. Suppose that \( X = (X_1, \ldots, X_n) \) has components \( X_1, \ldots, X_n \) that are independent and identically distributed random variables with mean \( \mathbf{E}(X_j) = 0 \) and finite variance \( \text{Var}(X_j) = \rho^2 \), so \( X \) has covariance matrix \( \rho^2 I_n \).

If \( A \) is a \( n \times n \) matrix whose entries \( A_{jk} \) are not dominated by just a few of these entries, then the transformed random variable \( AX \sim \mathcal{N}(0, \rho^2 AA^T) \) can be approximated as a multivariate Normal distribution for moderate or large \( n \).

In Proposition 2, we apply Proposition 1 to approximate the distribution of the noise in a SymHom ciphertext expressed in an appropriate decryption basis. We note the proof of Proposition 2 is complicated by the fact that a pair of random variables in the \( T \)-basis arising as the image of a conjugate pair in the \( I \)-basis are uncorrelated but not independent (see for example Lemma 11).

Proposition 2. Suppose that \( C^{(T)} \) is a vector expressing the noise in a Ring-LWE ciphertext in the \( T \)-basis for \( H \), so a component \( c^{(T)}_j \) of \( C^{(T)} \) has mean \( \mathbf{E}\left(c^{(T)}_j\right) = 0 \) and finite variance \( \text{Var}\left(c^{(T)}_j\right) = \rho^2 \). Suppose further that the \( S \)-basis given by the columns of the \( n \times n \) matrix \( S \) is an appropriate basis of \( H \) for decryption, and that \( \Psi = ST^{-1} \) is the change of basis matrix from the \( T \)-basis to the \( S \)-basis for \( H \). If the entries \( \Psi_{jk} \) of \( \Psi \) are not dominated by just a few values, then the distribution of the noise \( C^{(S)} \) in this ciphertext in the (decryption) \( S \)-basis for \( H \) can be approximated as

\[
C^{(S)} \sim \mathcal{N}(0; \rho^2 \Psi \Psi^T)
\]

for moderate or large \( n \).

In particular, the \( p \Gamma \)-basis for \( H \) yields \( C^{(p\Gamma)} \sim \mathcal{N}(0; p^2 \rho^2 (mI - J)) \).

Proof. We can split \( \Psi = (\Psi' \Psi'') \) into two \( n \times n' \) submatrices and we similarly split \( C^{(T)} = \left( C^{(T)'}, C^{(T)''} \right)^T \) into the first \( n' \) components \( C^{(T)'} \) and the final \( n' \) components \( C^{(T)''} \). Furthermore, their conjugate pairs origin means that \( C^{(T)'} \) and \( C^{(T)''} \) are uncorrelated. The components \( c^{(T)'}_1, \ldots, c^{(T)'}_{n'} \) of \( C^{(T)'} \) are independent and identically distributed with mean 0 and variance \( \rho^2 \), so Proposition 1 gives \( \Psi' C^{(T)'} \sim \mathcal{N}(0; \rho^2 \Psi' \Psi'') \), and we similarly have \( \Psi'' C^{(T)''} \sim \mathcal{N}(0; \rho^2 \Psi'' \Psi'') \).

Thus

\[
C^{(S)} = \Psi C^{(T)} = \Psi' C^{(T)'} + \Psi'' C^{(T)''} \sim \mathcal{N}(0; \rho^2 \Psi \Psi^T)
\]

as \( C^{(S)} \) is the sum of two uncorrelated approximate multivariate Normal random variables, so has an approximate Normal distribution with covariance matrix

\[
\rho^2 \Psi' \Psi'^T + \rho^2 \Psi'' \Psi''^T = \rho^2 \Psi \Psi^T.
\]

The Central Limit Theorem is formally a statement about the convergence (in distribution) of an appropriate weighted sum of random variables to a Normal distribution in the limit as the number of summands \( n \) tends to infinity. When such a result is applied in a concrete setting with a fixed finite \( n \), it is reasonable to question the speed of this convergence, and in particular how accurate the approximation is. This issue is made more precise in a companion work [27], and can be verified empirically.
4.3 SymHom decryption using the $p\Gamma$-basis

We now specify a decryption process for the SymHom cryptosystem using the $p\Gamma$-basis of $H$ (though any appropriate basis can be used). We recall (see Figure 6) that we write $Z^\dagger$ and $Z^*$ to express an element of $H$ as a vector in the $T$-basis and the $p\Gamma$-basis respectively.

Decryption of a degree-1 ciphertext polynomial $C(\theta; \mu)$ begins by evaluating this polynomial at the secret $s$. We obtain information about the Noise since $C(s; \mu) = Y''(\mu) \mod R_q^\ast$. If we embed $C(s; \mu)$ in $H$ under $\sigma$ and perform a reduction modulo $q$ with respect to to the $p\Gamma$-basis, then we obtain an integer $\|\sigma(C(s; \mu))\|_{p\Gamma}$ with entries in $[-\frac{1}{2}q, \frac{1}{2}q]$.

The Embedded Noise $Y'(\mu)$ is expressed in the $I$-basis for $H$, so $Y'(\mu)$ is expressed with respect to the $T$-basis of $H$ as the real vector $Y'(\mu)^\dagger = T^\dagger Y'(\mu)$. However, the change of basis from this $T$-basis to the $p\Gamma$-basis of $H$ is given by $p^{-1}\Delta = p^{-1}\Gamma^{-1}T$, so there is a real transformation $Y'(\mu)^* = p^{-1}\Delta Y'(\mu)^\dagger$ that gives a real vector $Y'(\mu)^*$ specifying the Embedded Noise expressed in the $p\Gamma$-basis for $H$. This allows us to write $Y'(\mu)^* = \|\sigma(C(s, \mu))\|_{p\Gamma}$ if the Embedded Noise is small enough. In this case, we can recover the real vector $Y'(\mu)^*$ and hence the real Embedded Noise vector $Y'(\mu)^\dagger$ with respect to the $T$-Basis. This allows us to determine the coset representative $\sigma(b_s^{-1}\mu)$ for the coset of the lattice $\sigma(pR^\dagger)$ corresponding to the plaintext $\mu \in R_p$. Thus if the Embedded Noise is small enough with high probability, then we can recover the plaintext $\mu$ with high probability.

This decryption process generalises to degree-2 and higher degree ciphertexts in a natural way. For example, if $C(\theta; \mu_1)$ and $C(\theta; \mu_2)$ are two degree-1 ciphertexts with respective Embedded Noises $Y'_1(\mu_1)$ and $Y'_2(\mu_2)$, then the degree-2 ciphertext $C(s; \mu_1, \mu_2) = Y''(\mu_1)Y''(\mu_2) = C(s; \mu_1)C(s; \mu_2) \mod (R^\dagger)_q^2$ and so we obtain $(Y'_1(\mu_1)Y'_2(\mu_2))^* = \|\sigma(C(s; \mu_1, \mu_2))\|_{p\Gamma}$ for small Embedded Noise. Thus if this Embedded Noise is small enough with high probability, we can recover the plaintext product $\mu_1\mu_2 \in R_p$ with high probability.

4.4 Decryption Failure Probabilities in the SymHom cryptosystem

We now present in Theorem 2 and Corollary 2 our main results of this section, which give (respectively) bounds for the probability of the incorrect decryption of degree-1 and degree-2 SymHom ciphertexts. Both results follow from the fact that SymHom decryption using (for example) the $p\Gamma$-basis for $H$ fundamentally involves a change of basis transformation between bases for $H$ ultimately to the $p\Gamma$-basis.

In the following, we denote by $Q$ the “$Q$-function” giving the upper tail probability for a standard Normal $\mathcal{N}(0, 1)$ distribution, so

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp(-\frac{1}{2}z^2) \, dz.$$ 

This tail probability $Q(x)$ is bounded by its asymptotic expansion, so

$$Q(x) \leq (2\pi x^2)^{-\frac{1}{2}} \exp(-\frac{1}{2}x^2),$$
and we note that this bound is very tight even for moderate values of $x > 0$.

**Theorem 2.** If $\eta_1(n,q,\rho) = \frac{1}{2}(n^{\frac{3}{2}}\rho)^{-1}q$ is moderate or large, then the probability of the incorrect decryption of a SymHom degree-1 ciphertext in the $p\Gamma$-basis for $H$ is bounded by

$$P\left(\text{Incorrect decryption of SymHom degree-1 ciphertext in } p\Gamma\text{-basis}\right) \leq \frac{2n \exp(-\frac{1}{2}\eta_1^2)}{(2\pi)^{\frac{3}{2}}\eta_1}.$$  

**Proof.** The vector expressing the Embedded Noise in the $p\Gamma$-basis for $H$ is of the form $\left([Z]^{p\Gamma}_{J_n}\right)^*$, where $Z = T\Theta^T$ and $p^{-1}\Theta^T = (p^{-1}T^T)Z \sim N(0, \rho^2I_n)$. However, $\left([Z]^{p\Gamma}_{J_n}\right)^* = (p\Gamma)^{-1}[Z]^{p\Gamma}_{J_n} \approx \Delta(p^{-1}T^T)Z$, so Lemma 11 shows that $\left([Z]^{p\Gamma}_{J_n}\right)^* \sim N(0; \rho^2\Delta\Delta^T) = N(0; \rho^2(mI - J))$.

Thus $\left([Z]^{p\Gamma}_{J_n}\right)^*$ is well-approximated by a multivariate Normal random variable $U \sim N(0; \rho^2(mI - J))$, with components $U_1, \ldots, U_n \sim N(0, \rho^2)$. These components therefore have an upper tail probability function given for $\alpha > 0$ by

$$P(U_j > \alpha) = P\left((n^{\frac{3}{2}}\rho)^{-1}U_j > (n^{\frac{3}{2}}\rho)^{-1}\alpha\right) = Q\left((n^{\frac{3}{2}}\rho)^{-1}\alpha\right),$$

where the $Q$-function is as defined above. We can now obtain a bound for the tail probability for the maximum of $|U_1|, \ldots, |U_n|$ for moderate $(n^{\frac{3}{2}}\rho)^{-1}$ by using the union bound [18] to obtain

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

We can now give a bound for the probability of decryption failure for a degree-1 ciphertext using the $\Gamma$-basis. In this case, decryption fails if the absolute size of any component of exceeds $\frac{1}{2}q$, so taking $\alpha = \frac{1}{2}q$ for moderate and large $\eta_1(n,q,\rho) = \frac{1}{2}(n^{\frac{3}{2}}\rho)^{-1}q$ gives

$$P\left(\text{Incorrect decryption of SymHom degree-1 ciphertext in } p\Gamma\text{-basis}\right) \leq \frac{2n \exp(-\frac{1}{2}\eta_1^2)}{(2\pi)^{\frac{3}{2}}\eta_1}.$$  

**Corollary 2.** If $\eta_2 = \frac{1}{2}(n^{\frac{3}{2}}mp\rho_2)^{-1}q$ is moderate or large, then the probability of the incorrect decryption of a SymHom degree-2 ciphertext in the $p\Gamma$-basis for $H$ is bounded by

$$P\left(\text{Incorrect decryption of SymHom degree-2 ciphertext in } p\Gamma\text{-basis}\right) \leq \frac{2n \exp(-\frac{1}{2}\eta_2^2)}{(2\pi)^{\frac{3}{2}}\eta_2}.$$
Proof. The decryption of a \textsf{SymHom} degree-2 ciphertext $C(\theta; \mu_1, \mu_2)$ involves processing this ciphertext as $[\sigma(C(s; \mu_1, \mu_2))]^{m^{-1}p\Gamma}$, that is to say by regarding this Embedded Noise expressed as a vector with respect to the rescaled decoding conjugate pair $m^{-1}p\Gamma$-basis. The processing of a degree-2 ciphertext fundamentally therefore simply involves change of basis transformations for bases for $H$ ultimately to the $m^{-1}p\Gamma$-basis. Thus we can adapt the argument of the proof of Theorem 2 simply by using the appropriate moments, and so we can replace $\rho$ in $\eta_1$ with $mpp_1\rho_2$ in to give $\eta_2 = \eta_1(n, q, mpp_1\rho_2) = \frac{1}{2}(n^2mpp_1\rho_2)^{-1}q$.

Conflict of interest

The authors declare that they have no conflict of interest.

Availability of Data

The simulation methods used and the public libraries used to generate the experimental data referred to in this paper are fully described in this paper. The code used to generate data in all results tables will be made available so that the results can be reproduced.

Acknowledgements

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


