Accurate BGV Parameters Selection: Accounting for Secret and Public Key Dependencies in Average-Case Analysis

Beatrice Biasioli[1], Chiara Marcolla[2], Nadir Murru[3], and Matilda Urani[4]

[1] IBM Research Europe - Zurich, Switzerland & University of Potsdam, Germany **
[2] Technology Innovation Institute, Abu Dhabi, United Arab Emirates
[3] Università degli studi di Trento, Trento, Italy
[4] Politecnico di Torino, Torino, Italy

Abstract. The Brakerski-Gentry-Vaikuntanathan (BGV) scheme is one of the most significant fully homomorphic encryption (FHE) schemes. It belongs to a class of FHE schemes whose security is based on the presumed intractability of the Learning with Errors (LWE) problem and its ring variant (RLWE). Such schemes deal with a quantity, called *noise*, which increases each time a homomorphic operation is performed. Specifically, in order for the scheme to work properly, it is essential that the noise remains below a certain threshold throughout the process. For BGV, this threshold strictly depends on the ciphertext modulus, which is one of the initial parameters whose selection heavily affects both the efficiency and security of the scheme.
In this paper, we provide a new method to estimate noise growth, closely aligning with experimental results and forming the basis for parameter selection that ensures correctness and improves efficiency.

1 Introduction

The first Fully Homomorphic Encryption (FHE) scheme was introduced in 2009 by Gentry [18]. Since then, several FHE constructions have been proposed, such as BGV [4], BFV [3,17], FHEW [16], TFHE [9,10], and CKKS [8,7].

The homomorphic encryption schemes currently in use base their security on the presumed intractability of the Learning with Errors (LWE) problem, [26], and its ring variant (RLWE) [23]. Informally, the decisional version of RLWE consists of distinguishing polynomial equations $(a, b = s \cdot a + e) \in \mathcal{R}_q \times \mathcal{R}_q$, perturbed by small noise e (also called error), from uniform random tuples from $\mathcal{R}_q \times \mathcal{R}_q$, where $\mathcal{R}_q = \mathbb{Z}_q[x]/\langle x^n + 1\rangle$ and q is a positive integer.

** Part of this work was performed while at Technology Innovation Institute, Abu Dhabi

Schemes based on the (R)LWE problem face a critical challenge related to the growth of noise during homomorphic operations, which must be carefully controlled to ensure the correct functioning of the encryption scheme. Specifically, the noise must be kept below a certain threshold, which, in the case of BGV, is directly related to the ciphertext modulus parameter q.

As homomorphic operations are performed, the noise increases, and therefore, to maintain the integrity of the scheme, the parameter q must be chosen sufficiently large. However, although increasing q allows for a greater number of operations, it simultaneously compromises both the security and efficiency of the scheme. Therefore, selecting an appropriate value for q and, in general, determining an optimal set of parameters, is critical. This process requires a balance between security and efficiency while ensuring the correctness of the scheme.

One of the key factors in achieving this balance and determining suitable parameters is providing accurate estimates of the error and its growth during the homomorphic operations in the circuit.

This issue is central to research in FHE, and over the years, various approaches have been proposed to address it. As for example, employing the Euclidean norm [4], the infinity norm [17,22], and the canonical norm, also called *worst-case* analysis [11,13,19,21,24]. The prevailing trend in the current literature adopts the *average-case analysis*, which involves treating the noise coefficients as random variables distributed according to a Gaussian distribution and studying their expected value and variance.

Interest in this method, initially applied in the TFHE scheme [9], and subsequently in the CKKS [12], BGV [14,25] and BFV [2] schemes, grew due to a recognized discrepancy between the estimates based on worst-case technique and experimental data, as highlighted in [13]. The introduction of the average-case approach, as seen in [2,14], offers a potential resolution to these disparities, indeed, with this method, it is possible to compute a tight *probabilistic* upper bound.

However, the heuristics used for the BGV [25] and CKKS [12] schemes often *underestimate* the noise growth due to the assumption of the noises independence, leading to *imprecise bounds*, as also pointed out in [1,12,25]. Such underestimates lead to two potential issues: first, the ciphertext is not correctly decrypted with non-negligible probability due to excessive noise and, second, the scheme is exposed to security vulnerabilities, as shown in recent papers [5,6].

In light of this, it becomes evident that accounting for the dependencies between the error coefficients is crucial in order to derive increasingly tighter and correct bounds. This, in turn, enables the definition of more accurate operational parameters, making the scheme both more secure and efficient, which is essential for the widespread adoption of FHE.

In this paper, we propose the first average-case noise analysis for BGV that does not provide underestimates, taking in account the dependencies introduced by the common secret and public key. We extend the approach of BFV [2], where the authors consider the fact that the errors are *not* independent among each other, and introduce a function F to "correct" the product of the variances for homomorphic multiplication. We notice the additional dependencies given by the public key and employ a second correcting function to address its contribution. The results obtained in this study suggest that this approach leads to significant improvements in noise analysis.

A related average-case analysis for the BGV scheme is presented in [14], where the authors develop a noise estimation method tailored to the specific implementation of BGV in HElib [20]. In contrast, our work proposes a general analysis that does not depend on the specific library and instead focuses on capturing the structural *dependencies* among the errors. We show that considering these dependencies is essential to derive correct, accurate and tighter bounds, independently of specific implementations.

In the BGV scheme, each ciphertext is associated with a *critical quantity* ν which is a polynomial in $\mathcal{R}$. The critical quantity of a ciphertext $\mathbf{c}$ defines whether $\mathbf{c}$ can be correctly decrypted. Specifically, if the size of ν is below a given bound (depending on q) the decryption algorithm works. Otherwise, the plaintext cannot be recovered due to excessive noise growth. Therefore, as previously mentioned, tracking the size of this critical quantity is essential to ensure correct decryption.

To provide a clearer picture of what happens to the coefficients of ν, we focus on multiplication, which is the homomorphic operation that highlights most clearly and significantly the dependencies among the critical quantities.

The BGV public key $\mathsf{pk} \in \mathcal{R}_q \times \mathcal{R}_q$ consists of two polynomials $(-a \cdot s + te, a)$, where s is the secret key, t is the plaintext modulus, $a \in \mathcal{R}_q$ is randomly chosen and $e \in \mathcal{R}_q$ is the error sampled from a discrete Gaussian distribution χ_e. Roughly speaking, when two ciphertexts are multiplied — even if they were independently computed — their noises share some common terms which affect the resulting critical quantity ν_{mult}. More specifically, we observed that the noise in the ciphertexts contains terms that include powers of the secret key s and powers of the term e. Note that these terms are common to all ciphertexts calculated using the same public key and are responsible for the dependence of the noise.

To account for these dependencies, we applied the correction function F introduced in [2]. It is important to note that the case of BGV is more complex than that of BFV. In BFV, the dependency due to e appears only in a negligible term. In contrast, for BGV, we must take into account the dependencies on both s and e. This requires the use of two distinct correction functions to accurately model and mitigate these dependencies.

The paper is structured as follows. Section 2 introduces essential definitions and fundamental properties that are instrumental for understanding both our contribution and the scheme more broadly. Section 3 provides a concise overview of the main features and structure of the BGV scheme. In Section 4, we present our key results concerning the behavior of the error term and its growth under homomorphic operations. Section 5 then demonstrates how the findings from Section 4 can be leveraged to estimate error growth in fixed-operation circuits, laying the groundwork for novel approaches to selecting the scheme's initial parameters. Finally, Section 6 concludes the paper and outlines possible directions for future research inspired by our results.

2 Preliminaries

In this section, we define the general notations that we will use in the remainder of the work.

In our analysis we will describe the leveled version of the BGV scheme, noting that this implies that *the parameters of the scheme depend (polynomially) on the depth of the circuits that the scheme is capable of evaluating* [4]. It should be noted that this version is also the most widely adopted because it does not require the usage of the bootstrapping technique, which is highly complex from a computational perspective. Before recalling the BGV scheme, some preliminary parameters must be fixed.

Let L denote the number of levels of the arithmetic circuit that the scheme must be able to evaluate. Moreover, assume that m is a suitably chosen integer. The notation $\mathcal{R}_d$, for a fixed $d \in \mathbb{Z}$, will denote the ring $\mathcal{R}_d = \mathbb{Z}_d[x]/\langle \Phi_m(x) \rangle$, where $\Phi_m(x)$ is the m-th cyclotomic polynomial, a definition of which is briefly recalled below.

Definition 1. *Given a positive integer m, the m-th cyclotomic polynomial is defined as*

$$\Phi_m(x) = \prod_{\substack{1 \le j < m \\ \gcd(j,m)=1}} (x - \zeta^j),$$

where ζ is a primitive m-th root of unity. This polynomial has degree $\phi(m)$, where ϕ denotes the Euler function.

Eventually, we will denote with $\mathcal{R}$ the ring $\mathcal{R} = \mathbb{Z}[x]/\langle \Phi_m(x) \rangle$. To define the plaintext and ciphertext spaces, $L+1$ moduli are selected as follows:

- An integer t, denoted as the *plaintext modulus*, is chosen such that $t \equiv 1 \mod m$.

– L integers q_l, for $l \in \{0, \ldots, L-1\}$, are defined as:

$$q_l = \prod_{j=0}^{l} p_j,$$

where the p_j are primes satisfying $p_j \equiv 1 \mod m$ for $j = 0, \ldots, L-1$ and $p_1, ..., p_{L-2}$ have approximately the same size. Each q_{L-1-l} is referred to as the *ciphertext modulus* for the l-th level.

According to these notations, we can define the plaintext and ciphertext spaces, respectively, as $P = \mathcal{R}_t$, $C = \mathcal{R}_{q_l} \times R_{q_l}$.

Due to the ciphertext coefficients being reduced according to different moduli at each level, BGV is commonly referred to as *scale-dependent*.

We use lowercase letters such as x to denote polynomials, and bold symbols like $\boldsymbol{x}$ to represent vectors of polynomials. Given a polynomial $x \in \mathcal{R}_n$, we use the notation $[x]_n$ to refer to the *centered representation* of x modulo n i.e., the representative of x with coefficients in $[-\frac{n}{2}, \frac{n}{2})$. In general, unless otherwise specified, we always assume the coefficients of polynomials in $\mathcal{R}_d$ to be centered with respect to the modulus d.

Moreover, given a random polynomial $p \in \mathcal{R}$ and a probabilistic distribution X, the notation $p \leftarrow X$ is used to indicate that each coefficient of p is chosen independently according to X.

Some distributions that will be frequently considered are the following:

– $\mathcal{U}_q$ as the *uniform distribution* over $\mathbb{Z}/q\mathbb{Z}$;
– $\mathcal{N}(0, \sigma^2)$ as the normal distribution, also referred to as the *Gaussian distribution*, over $\mathbb{R}$, with mean 0 and variance σ^2;
– $\mathcal{DG}_q(\sigma^2)$ as the *discrete Gaussian distribution*, which involves sampling a value according to $\mathcal{N}(0, \sigma^2)$, rounding it to the nearest integer and then reducing it modulo q.
Moreover, the representative modulo q is taken in the interval $\left[-\frac{q}{2}, \frac{q}{2}\right)$;

For the BGV scheme the notation χ_e, χ_s will be adopted in order to indicate the distribution of the error for a RLWE instance and the secret key coefficients, respectively. Typically, χ_e is a discrete Gaussian distribution with a suitable standard deviation, while for the secret key, the ternary uniform distribution $\mathcal{U}_3$ is usually considered. However, in some special cases, where bootstrapping is needed, the choice for the secret key distribution falls on the Hamming Weight distribution, a definition of which is recalled below [2].

Definition 2. *The Hamming Weight distribution $\mathcal{HWT}_{n,h}$ consists of selecting uniformly at random a vector of n entries in $\{-1, 0, 1\}$, where exactly $h < n$ entries are non-zero.*

To ensure the correctness of the scheme, it is important to underline that the error added to the plaintext during encryption must be sufficiently small [4]. This will become more apparent through the presentation of the BGV functions.

For the purposes of our subsequent analysis, it is helpful to recall that for two polynomials $r, s \in \mathcal{R}$, and denoting by $r|_i$ and $s|_i$ their coefficients with respect to x^i, the i-th coefficient of their product is given by [2]

$$rs|_i = \sum_{j=0}^{\phi(m)-1} \xi(i,j) r|_j s|_{i-j}, \tag{1}$$

where

$$\xi(i,j) = \begin{cases} 1 & \text{for } i-j \in [0, \phi(m)) \\ -1 & \text{otherwise} \end{cases}$$

Furthermore, the following notation will be adopted.

Notation 1 *Given a polynomial $p \in \mathcal{R}_q$, for a fixed integer q, the variance of its coefficients, namely $\mathsf{Var}(p|_i)$, is denoted as V_p.*

Proposition 1. *Let p, q be two independent polynomials in $\mathcal{R}_q$, where q is a fixed integer, and let k be an integer in $\mathbb{Z}/q\mathbb{Z}$. Moreover, assume that the coefficients of each polynomial are independent and identically distributed, with 0-mean. Then,*

a. $V_{p+q} = V_p + V_q$
b. $V_{kp} = k^2 V_p$
c. $V_{p \cdot q} = \phi(m) V_p \cdot V_q$

Finally, the variance values for some common distributions, which will often be employed in the BGV scheme, are:

- $V_{\mathcal{DG}_q(\sigma^2)} = \sigma^2$ for the discrete Gaussian distribution centered at 0 with standard deviation σ;
- $V_3 = \frac{2}{3}$ for the ternary distribution $\mathcal{U}_3$;
- $V_q = \frac{q^2-1}{12} \approx \frac{q^2}{12}$ for the uniform distribution over integer values in $\left[-\frac{q}{2}, \frac{q}{2}\right)$;

3 The BGV scheme

Once the parameters have been specified, the framework of the BGV scheme can be defined according to three main functions: Key Generation, Encryption and Decryption.

3.1 Key Generation

The key generation function is responsible for producing:

- the *secret key*, represented by a polynomial in $\mathcal{R}_{q_{L-1}}$;
- the *public key*, which consists of a pair of polynomials, each belonging to $\mathcal{R}_{q_{L-1}}$;

To achieve this, three polynomials in $\mathcal{R}_{q_{L-1}}$ are generated according to the following distributions: $s \leftarrow \chi_s$, $a \leftarrow \mathcal{U}_{q_{L-1}}$ and $e \leftarrow \chi_e$. The resulting keys are given by

$$\begin{cases} sk & = s \\ pk & = (b, a) \equiv (-a \cdot s + te, a) \mod q_{L-1} \end{cases}$$

3.2 Encryption

Given the plaintext $m \in \mathcal{R}_t$ and the public key $pk = (b, a)$, the encryption function returns as output $(\boldsymbol{c}, q_l, \nu_{clean})$ where:

- $\boldsymbol{c} \in \mathcal{R}_{q_l} \times \mathcal{R}_{q_l}$ is the actual ciphertext defined as

$$\boldsymbol{c} = (c_0, c_1) \equiv (b \cdot u + te_0 + m, a \cdot u + te_1) \mod q_l,$$

  where $u, e_0, e_1 \in \mathcal{R}_{q_l}$, with coefficients distributed as $u \leftarrow \chi_s$ and $e_0, e_1 \leftarrow \chi_e$.
- q_l represents the ciphertext modulus for the level at which computations are performed. Specifically, as the encryption function is computed in the first level 0, the corresponding q_l is q_{L-1}.
- ν is the *critical quantity* associated to the ciphertext and is defined as

$$\nu = [c_0 + c_1 \cdot s]_{q_l}.$$

We refer to the triple $\tilde{c} = (\boldsymbol{c}, q_l, \nu_{clean})$ with the term *extended ciphertext*.

Broadly speaking, the encryption of the plaintext message results in a pair of ciphertext values: the first encodes the masked plaintext using the public key, while the second supplies auxiliary information necessary for the receiver to recover the original message, provided they possess the secret key.

Regarding the critical quantity, it is important to emphasize that this value is strictly related to the error introduced by the encryption operator. Thus, it essentially determines whether the ciphertext can be correctly decrypted or not. For this reason, its behavior is analyzed to gain a clear understanding of the functioning of the scheme.

3.3 Decryption

At any level, it should be possible to recover the original plaintext using the decryption function.
Given the extended ciphertext $(\boldsymbol{c}, q_l, \nu)$ and the secret key $sk = s$, the plaintext is recovered performing the following computations

$$m = \Big[[c_0 + c_1 \cdot s]_{q_l} \Big]_t .$$

Using the previously established notation, the critical quantity can be rewritten as

$$[c_0 + c_1 \cdot s]_{q_l} = [m + t(e \cdot u + e_1 \cdot s + e_0)]_{q_l} = [m + t\epsilon]_{q_l} ,$$

where $t\epsilon$ denotes the *error* introduced during encryption.
By considering the reduction modulo t of the critical quantity, it is possible to verify that the plaintext is successfully recovered. However, if the error is too large, the value $m + t(e \cdot u + e_1 \cdot s + e_0)$ could wrap around the modulus, resulting in an incorrect decryption.
So, decryption is correct only if the error magnitude remains below a certain threshold, as previously emphasized. In addition, the error associated to the ciphertext $\boldsymbol{c}$ at level l increases each time the homomorphic circuit is evaluated. Therefore, for constructing a leveled homomorphic encryption scheme, it is crucial to estimate and manage this error properly. To deal with the error effectively, the magnitude of the critical quantity, often referred to as *noise*, is typically analyzed using its norm. In the context of homomorphic encryption, the infinity and the canonical norm, a definition of which are briefly recalled below [19], assume a central role.

Definition 3. *The infinity norm of a polynomial $p \in \mathcal{R}$, of the form $p = p|_0 + p|_1 x + ... + p|_{\phi(m)-1} x^{\phi(m)-1}$ is defined as*

$$\|p\|_\infty = \max_{0 \le i < \phi(m)} | \, p|_i \, |.$$

Definition 4. *The canonical embedding norm of a polynomial $p \in \mathcal{R}$ is defined as*

$$\|p\|_{can} = \max_{\substack{1 \le j < m \\ \gcd(j,m)=1}} |p(\zeta^j)|,$$

where ζ is a primitive m-th root of unity.

Essentially, it corresponds to the infinity norm of the canonical embedding of p, denoted as $\sigma(p)$, which is the $\phi(m)$-vector defined as

$$\sigma(p) = (p(\zeta^i))_i,$$

where $1 \le i < m$ and $\gcd(j, m) = 1$.

A relationship between these two norms is given by the following property

$$||p||_\infty \leq \alpha_m ||p||_{can} \qquad \forall p \in \mathcal{R},$$

where α_m is a constant related to the ring $\mathcal{R}$, which depends exclusively on m. Another property, which will be useful in the context of the noise growth analysis, is recalled below [15].

Proposition 2. *Let p, q be two polynomials in $\mathcal{R}$. Then,*

$$\begin{aligned} ||p \cdot q||_\infty &\leq \phi(m)||p||_\infty \cdot ||q||_\infty \\ ||p \cdot q||_{can} &\leq ||p||_{can} \cdot ||q||_{can} \end{aligned}$$

In light of this, to guarantee the correctness of the decryption, the condition on the critical quantity can be expressed as follow

$$||\nu||_\infty \leq \alpha_m ||\nu||_{can} < \frac{q_l}{2},$$

which allows to avoid the error wrapping around the modulus [24]. Naturally, in order to bound the noise, any type of norm could be used. Nevertheless, in the state-of-the-art analysis of noise growth for homomorphic schemes, the canonical norm is typically preferred, due to its properties, as it permits obtaining more accurate estimates. Finally, another concept that is often introduced for the error growth estimation is the noise budget.

Definition 5. *Let $(\boldsymbol{c}, q_l, \nu)$ be an extended ciphertext. The noise budget associated to $\boldsymbol{c}$ is the quantity*

$$\log_2(q_l) - \log_2(||\nu||) - 1,$$

where $||\cdot||$ refers to a fixed norm.

The key operations involved in the BGV scheme are briefly summarized in the following.

3.4 Ciphertext Addition and Constant Multiplication

Assume that $\boldsymbol{c} = (c_0, c_1)$ and $\boldsymbol{c'} = (c'_0, c'_1)$ are two ciphertexts defined with respect to the same modulus q_l and computed encrypting two plaintexts m and m', respectively, using the same key. Their homomorphic sum is defined as

$$\mathsf{Add}(\boldsymbol{c}, \boldsymbol{c'}) := (c_0 + c'_0,\ c_1 + c'_1) \mod q_l.$$

The resulting ciphertext encrypts the sum $m + m'$, and the corresponding noise grows additively. In fact, the resulting critical quantity is defined as

$$\nu_{\mathsf{add}} = \nu + \nu',$$

where $\nu = c_0 + c_1 s$ and $\nu' = c'_0 + c'_1 s$ denote the critical quantities of $\boldsymbol{c}$ and $\boldsymbol{c'}$, respectively.

Similarly, let $\boldsymbol{c} = (c_0, c_1)$ be a ciphertext and $k \in R_t$ a constant polynomial. The homomorphic multiplication by k is performed as follows

$$\mathsf{Mul}_k(\boldsymbol{c}) := (kc_0,\ kc_1) \mod q_l,$$

and the corresponding critical quantity scales by k, yielding

$$\nu_{\mathsf{const}} = k \cdot \nu.$$

In both cases, decryption correctness is preserved as long as the resulting noise does not cause the message to wrap around the modulus.

3.5 Homomorphic multiplication and Key switching

Homomorphic multiplication is one of the fundamental operations supported by the BGV scheme. Given two ciphertexts $\boldsymbol{c} = (c_0, c_1)$ and $\boldsymbol{c'} = (c'_0, c'_1)$, and assuming that both are defined with respect to the same modulus q_l, their product is given by

$$\mathsf{Mul}(\boldsymbol{c}, \boldsymbol{c'}) := (c_0^{\mathsf{mul}}, c_1^{\mathsf{mul}}, c_2^{\mathsf{mul}}) = (c_0 \cdot c'_0, c_0 \cdot c'_1 + c_1 \cdot c'_0, c_1 \cdot c'_1) \mod q_l.$$

As a result, the ciphertext expands from two to three polynomials, which violates the compactness property and makes subsequent operations more costly. This phenomenon becomes even more problematic when performing multiple multiplications. Recovering the message from $\mathsf{Mul}(\boldsymbol{c}, \boldsymbol{c'})$ requires computing the reduction modulo t of the resulting critical quantity given by $\nu_{\mathsf{mul}} = c_0^{\mathsf{mul}} + c_1^{\mathsf{mul}} s + c_2^{\mathsf{mul}} s^2$.

It is significant to note that, unlike other operations, multiplication causes the noise to grow multiplicatively, making it the most critical case to handle among the basic homomorphic operations in terms of error growth.

To address this, a technique known as *relinearization*, or *key switching*, is employed. The key idea is to reduce the ciphertext back to its original size while preserving its correctness. In practice, this means converting a ciphertext of the form (c_0, c_1, c_2) into a new, equivalent one of the form $(\hat{c}_0, \hat{c}_1)$, using auxiliary data called the *key switching key*. More intuitively, key switching allows the expression $c_0 + c_1 s + c_2 s^2$ to be re-expressed as a linear polynomial in s, restoring the standard noise form.

Although the relinearization step introduces additional noise, it is essential for maintaining the practicality of the scheme. Several key switching techniques have been proposed in the literature, each aiming to optimize this trade-off between correctness and noise growth. The most commonly used are the Brakerski Vaikuntanathan (BV) variant, the Gentry Halevi Smart (GHS) variant and the Hybrid variant, which can be considered as a combination of the previous ones.

3.6 Modulus switching

The primary aim of the modulus switching technique is to reduce the noise resulting from homomorphic evaluations. In practical circuits, modulus switching is typically applied only after homomorphic multiplications, due to their higher cost in terms of error growth. Similarly to the bootstrapping technique, the main purpose is to transition from an extended ciphertext $(\boldsymbol{c}, q_l, \nu)$ to another $(\boldsymbol{c}', q_{l'}, \nu')$ such that the error associated to the latter is smaller, while preserving the fact that, using the same key, both can be decrypted to the same original message. The key difference lies in how this is achieved, and it is in this aspect that modulus switching demonstrates greater efficiency compared to bootstrapping.

Let $(\boldsymbol{c}, q_l, \nu)$ be the extended ciphertext, whose error we want to reduce, and let l' be an integer, such that $q_{l'} < q_l$. The new ciphertext produced by the modulus switch is given by

$$\boldsymbol{c}' = \frac{q_{l'}}{q_l}(\boldsymbol{c} + \boldsymbol{\delta}) \mod q_{l'},$$

where $\boldsymbol{\delta} = t[-\boldsymbol{c}t^{-1}]_{\frac{q_l}{q_{l'}}}$. The $\boldsymbol{\delta}$ value can be interpreted as a correction required to ensure that the ciphertext is divisible by $\frac{q_l}{q_{l'}}$ and does not affect the original message. In fact, it only influences the error since $\boldsymbol{\delta} \equiv 0 \mod t$. Therefore, the new ciphertext $\boldsymbol{c}'$ will still decrypt to the original plaintext (scaled by a factor of $\frac{q_l}{q_{l'}}$), provided that the necessary conditions are met.

The critical quantity associated to the new ciphertext $\boldsymbol{c}'$ can be expressed in terms of that of $\boldsymbol{c}$, namely ν, as

$$\nu_{\mathsf{modswitch}} = [c'_0 + c'_1 \cdot s]_{q_{l'}} = \frac{q_{l'}}{q_l}([c_0 + c_1 \cdot s]_{q_l} + \delta_0 + \delta_1 \cdot s) = \frac{q_{l'}}{q_l}(\nu + \delta_0 + \delta_1 \cdot s).$$

To conclude, it is worth noting that this correctness verification implicitly relies on the common value h in the two equalities

$$\begin{aligned}[c_0 + c_1 \cdot s]_{q_l} &= c_0 + c_1 \cdot s - hq_l \\ [c'_0 + c'_1 \cdot s]_{q_{l'}} &= c'_0 + c'_1 \cdot s - hq_{l'}\end{aligned}$$

The reason why the value h is the same for both the expressions can be found in [4, Lemma 1].

4 Average-Case Noise Analysis for BGV

The aim of this section is to investigate the behavior of the noise resulting from the main homomorphic operations supported by the BGV scheme. Throughout this analysis, we consider ciphertexts that are mutually independent, obtained by encrypting independently generated random messages under the same public key.

As previously mentioned, the novel approach introduced in this paper seeks to analyze noise growth by accounting for dependencies among the coefficients of the critical quantities involved. Before delving into the details, it is important to highlight that in BGV, the critical quantity resulting from homomorphic operations can be affected by such dependencies, even when the ciphertexts involved are independent. These dependencies stem from the fact that the noise in the ciphertexts includes terms involving powers of the secret key s and powers of the error term e, which makes it necessary to explicitly consider these contributions when analyzing the variance of the noise.

To study the impact of s and e, we isolate their contribution in the expression of the critical quantity ν, using the following notation:

$$\nu = \sum_{\iota} a_\iota s^\iota = \sum_{\iota} \sum_{\mu} b_\mu(\iota) e^\mu s^\iota,$$

where $a_\iota = \sum_\mu b_\mu(\iota) e^\mu$, and $b_\mu(\iota)$ contains no powers of s or e.

To enhance clarity, for the critical quantity ν of a fresh ciphertext $\boldsymbol{c}$, this notation yields

$$\nu = a_0 + a_1 s = b_0(0) + b_1(0)e + b_0(1)s,$$

where

$$\begin{cases} a_0 = b_0(0) + b_1(0) \cdot e = (m + te_0) + tu \cdot e \\ a_1 = b_0(1) = te_1 \end{cases}$$

Before introducing our method for studying the growth of error through its variance in fixed circuits, we begin by presenting some considerations and results we have derived regarding the distribution of the coefficients of a generic error term, along with certain properties related to their variances. We then proceed to describe how these properties are used to estimate the variance of the error coefficients after homomorphic multiplications, and finally how such estimates can be applied to circuits consisting of fixed sequences of operations.

From this point onward, we adopt the notation n to denote $\phi(m)$, in order to simplify the presentation. It is interesting to point out that when n is a power of two, $m = 2n$.

4.1 Distribution Analysis

As previously mentioned, the noise coefficients are treated as random variables. We observed that their distributions are well-approximated by identically distributed, dependent Gaussian variables centered at zero. This empirical observation was validated through experiments using the Python *fitter* package, which confirmed the Gaussian nature of the noise coefficients. This property is particularly advantageous, as it allows us to bound the maximum absolute value of the noise coefficients with high probability by simply controlling their variance V.

In particular, we recall the following fundamental property of Gaussian random variables.

Proposition 3. *Let Z be a real-valued, zero-mean Gaussian random variable with variance V. Then, for any fixed value $z > 0$, the probability that Z lies within the interval $(-z, z)$ is given by*

$$\mathbb{P}(|Z| < z) = erf\left(\frac{z}{\sqrt{2V}}\right),$$

where $erf(z)$ is the error function, defined as

$$erf(z) = \frac{2}{\sqrt{\pi}} \int_0^z e^{-t^2}\, dt.$$

Extending this result to a vector $\boldsymbol{Z} \in \mathbb{R}^n$, whose entries are distributed as Z, we obtain the following bound on the tail probability of the infinity norm

$$\mathbb{P}(\|\boldsymbol{Z}\|_\infty > z) \leq n\left(1 - \operatorname{erf}\left(\frac{z}{\sqrt{2V}}\right)\right). \tag{2}$$

This implies that, in order to ensure that a noise vector ν satisfies the correctness condition $\|\nu\|_\infty < q/2$, we can use Proposition 3 to bound the failure probability as

$$\mathbb{P}\left(\|\nu\|_\infty > \frac{q}{2}\right) \leq n\left(1 - \operatorname{erf}\left(\frac{q}{2\sqrt{2V}}\right)\right),$$

where V denotes the estimated variance of the noise coefficients. To express this bound more conveniently, we introduce a *security parameter* D such that

$$D \leq \frac{q}{2\sqrt{2V}},$$

from which it follows, using the monotonicity of the error function, that

$$\mathbb{P}\left(\|\nu\|_\infty > \frac{q}{2}\right) \leq n\left(1 - \operatorname{erf}(D)\right).$$

Thus, by appropriately choosing the security parameter D, we can ensure that the probability of decryption failure remains negligibly small. For instance, setting $D = 6$ and $n = 2^{13}$ yields a failure probability of approximately 2^{-42}. For practical applications, $D = 8$ should be preferred, resulting in a probability of approximately 2^{-83}, when the ring dimension is $n = 2^{13}$.

Consequently, the ciphertext modulus q can be selected according to the inequality

$$q \geq 2D\sqrt{2V}, \tag{3}$$

which highlights the importance of accurately estimating V.

It is important to emphasize that the bounds derived in our analysis provide insight into the *minimum* ciphertext modulus q required to guarantee the correctness of the scheme. Although larger values of q may be used in practice, identifying the minimal admissible value is essential for optimizing performance and efficiency. This is particularly relevant in the context of the BGV scheme, where our results can serve as a guideline for carefully selecting the setting parameters. By determining tight lower bounds on q, it is possible to lay the foundation for sound and efficient parameter selection that ensures correctness without over-provisioning resources.

4.2 Mean and Variance Analysis

As previously discussed, we have demonstrated that the coefficients of the error term are centered at zero. Furthermore, we have shown that the coefficients of the b_μ terms are uncorrelated, meaning that their pairwise covariance is zero.

Lemma 1. *Let $\nu = \sum_\iota \sum_\mu b_\mu(\iota) e^\mu s^\iota$ be the critical quantity associated with a given ciphertext. Then, the following properties hold*

a) $\mathsf{Cov}(b_{\mu_1}(\iota_1)|_{j_1}, b_{\mu_2}(\iota_2)|_{j_2}) = 0$ *for* $\mu_1 \neq \mu_2$ *or* $j_1 \neq j_2$, $\forall \iota_1, \iota_2$;
b) $\mathbb{E}[b_\mu(\iota)|_i] = 0$, $\forall \iota, \mu, i$;

A proof of Lemma 1 can be found in Appendix A

Lemma 2. *Let $\nu = \sum_\iota a_\iota s^\iota$ represent the critical quantity associated with a given ciphertext, where, for a fixed ι, $a_\iota = \sum_\mu b_\mu(\iota) e^\mu$. Then, the following equivalence holds*

$$\mathsf{Var}(a_\iota s^\iota|_i) = \sum_{\mu \geq 0} \mathsf{Var}(b_\mu(\iota)|_i) \sum_{k=0}^{n-1} \mathbb{E}[e^\mu|_k^2] \sum_{j=0}^{n-1} \mathbb{E}[s^\iota|_j^2]$$

A proof of Lemma 2 can be found in Appendix B.

4.3 Homomorphic multiplications

The main goal of our analysis is to provide estimates on the growth of the error resulting from homomorphic multiplications, which are the most complex operations and therefore the most interesting to study. It thus becomes crucial to account for the dependencies that arise among the noise coefficients as a consequence of these multiplications. To this end, the approach we adopted relies on the correction functions introduced in [2].

Therefore, before stating the theorem, some of the key properties of F will be recalled. Unlike the BFV scheme, the BGV scheme requires additional care in the use of the correction function F, as not only the impact of the term s must be taken into account, but also that of the term e, which is negligible in BFV. Consequently, our analysis requires the introduction of two distinct correction functions, which will be denoted as F_e and F_s. To define these two functions, we need the following

Heuristic 1 *Let x be a polynomial whose coefficients are independent and identically distributed according to a fixed distribution. The function f_x defined as*

$$f_x(\iota) = -e^{\alpha - \beta\iota - \gamma\iota^2} + \delta, \tag{4}$$

where $\alpha, \beta, \gamma, \delta$ depend only on the coefficient distribution of x and the ring dimension n, satisfies the following

$$f_x(\iota) \approx \frac{\sum_{i=0}^{n-1} \mathbb{E}[x^\iota|_i^2]}{\sum_{i_1=0}^{n-1} \mathbb{E}[x^{\iota-1}|_{i_1}^2] \sum_{i_2=0}^{n-1} \mathbb{E}[x|_{i_2}^2]}.$$

In Table 1, we report the values of $\alpha, \beta, \gamma, \delta$ required to define the function f_s, where s denotes the secret key with coefficients sampled from the ternary distribution $\chi_s = \mathcal{U}_3$, as in [2].

n	α	β	γ	δ
2^{12}	2.8732	0.0160	0.0049	19.1895
2^{13}	2.9644	0.0196	0.0046	20.4747
2^{14}	2.9578	0.0386	0.0032	19.5755
2^{15}	2.9765	0.0197	0.0043	20.7760

Table 1: Parameters for $\chi_s = \mathcal{U}_3$

Similarly, it is possible to define the function f_e for the error term e, whose coefficients are distributed according to a discrete Gaussian distribution. For completeness, a table containing the parameters depending on the distribution χ_e can be found in Table 2 [2].

Definition 6. *Let $g_x(\iota) = \prod_{i=0}^{\iota} f_x(i)$ with f_x defined as in (4) and $f_x(0) = f_x(1) = 1$. The correction function F_x is*

$$F_x(\iota_1, \iota_2) := \frac{g_x(\iota_1 + \iota_2)}{g_x(\iota_1) \cdot g_x(\iota_2)}$$

n	α	β	γ	δ
2^{12}	2.9000	0.0157	0.0051	19.5356
2^{13}	2.9340	0.0042	0.0055	20.7063
2^{14}	2.9138	0.0290	0.0039	19.2973
2^{15}	2.9511	0.0129	0.0046	20.7263

Table 2: Parameters for $\chi_e = \mathcal{DG}_q(\sigma^2)$, $\sigma = 3.19$

Moreover, this function satisfies

$$F_x(\iota_1, \iota_2) \approx \frac{\sum_{i=0}^{n-1} \mathbb{E}[x^{\iota_1+\iota_2}|_i^2]}{\sum_{i_1=0}^{n-1} \mathbb{E}[x^{\iota_1}|_{i_1}^2] \sum_{i_2=0}^{n-1} \mathbb{E}[x^{\iota_2}|_{i_2}^2]}$$

A proof of this result can be found in [2]. For the purposes of our study, we denote by F_e the correction function required to account for the dependencies induced by the term e, and by F_s the correction function associated with the term s.

We can now introduce our main theorem.

Theorem 1. *Let $\nu = \sum_\iota a_\iota s^\iota, \nu' = \sum_\iota a'_\iota s^\iota$ be the critical quantities of two independently computed ciphertexts defined with respect to the same modulus q. Then*

$$\mathsf{Var}((a_{\iota_1} s^{\iota_1} a'_{\iota_2} s^{\iota_2})|_i) \leq n\mathsf{Var}((a_{\iota_1} s^{\iota_1})|_i)\mathsf{Var}((a'_{\iota_2} s^{\iota_2})|_i)F_s(\iota_1, \iota_2)F_e(K_1, K_2),$$

where K_1, K_2 arise from the expansions

$$a_{\iota_1} = \sum_{\mu_1=0}^{K_1} b_{\mu_1}(\iota_1)e^{\mu_1}, \quad a'_{\iota_2} = \sum_{\mu_2=0}^{K_2} b'_{\mu_2}(\iota_2)e^{\mu_2}$$

and represent the highest power of e appearing in $a_{\iota_1}, a'_{\iota_2}$, respectively.

Proof. From lemma 2 it is possible to express the variance of two generic terms $a_{\iota_1} s^{\iota_1}|_i$ and $a'_{\iota_2} s^{\iota_2}|_i$ as

$$\begin{cases} \mathsf{Var}(a_{\iota_1} s^{\iota_1}|_i) = \sum_{\mu_1=0}^{K_1} \mathsf{Var}(b_{\mu_1}(\iota_1)|_i) \sum_{j_1=0}^{n-1} \mathbb{E}[e^{\mu_1}|_{j_1}^2] \sum_{j_2=0}^{n-1} \mathbb{E}[s^{\iota_1}|_{j_2}^2] \\ \mathsf{Var}(a'_{\iota_2} s^{\iota_2}|_i) = \sum_{\mu_2=0}^{K_2} \mathsf{Var}(b'_{\mu_2}(\iota_2)|_i) \sum_{j_3=0}^{n-1} \mathbb{E}[e^{\mu_2}|_{j_3}^2] \sum_{j_4=0}^{n-1} \mathbb{E}[s^{\iota_2}|_{j_4}^2] \end{cases}$$

By observing that

$$a_{\iota_1} s^{\iota_1} \cdot a'_{\iota_2} s^{\iota_2} = \left(\sum_\mu \sum_{\mu_1+\mu_2=\mu} b_{\mu_1}(\iota_1) b'_{\mu_2}(\iota_2) e^\mu \right) s^{\iota_1+\iota_2},$$

and using lemma 2, it is possible to write the variance $\mathsf{Var}((a_{\iota_1} s^{\iota_1} \cdot a'_{\iota_2} s^{\iota_2})|_i)$ as

$$\sum_\mu \mathsf{Var}\left(\sum_{\mu_1+\mu_2=\mu} (b_{\mu_1}(\iota_1) b'_{\mu_2}(\iota_2))|_i \right) \sum_{j_1=0}^{n-1} \mathbb{E}[e^\mu|_{j_1}^2] \sum_{j_2=0}^{n-1} \mathbb{E}[s^{\iota_1+\iota_2}|_{j_2}^2]$$

$$= n \sum_{\mu} \sum_{\mu_1+\mu_2=\mu} \mathsf{Var}\left(b_{\mu_1}(\iota_1)|_i\right) \mathsf{Var}\left(b'_{\mu_2}(\iota_2)|_i\right) \sum_{j_1=0}^{n-1} \mathbb{E}[e^{\mu}|_{j_1}^2] \sum_{j_2=0}^{n-1} \mathbb{E}[s^{\iota_1+\iota_2}|_{j_2}^2],$$

where the second equality follows from the independence of $b_{\mu_1}(\iota_1), b'_{\mu_2}(\iota_2)$ and from $\mathsf{Cov}(b_{\mu_1}(\iota)|_{j_1}, b_{\mu_2}(\iota)|_{j_2}) = 0$ for $\mu_1 \neq \mu_2$ or $j_1 \neq j_2$.

Moreover, it can be noted that $n\mathsf{Var}(a_{\iota_1} s^{\iota_1}|_i)\mathsf{Var}(a'_{\iota_2} s^{\iota_2}|_i)$ can be written as

$$n \left(\sum_{\mu_1=0}^{K_1} \mathsf{Var}(b_{\mu_1}(\iota_1)|_i) \sum_{j_1=0}^{n-1} \mathbb{E}[e^{\mu_1}|_{j_1}^2] \sum_{j_2=0}^{n-1} \mathbb{E}[s^{\iota_1}|_{j_2}^2] \right) \cdot \\ \cdot \left(\sum_{\mu_2=0}^{K_2} \mathsf{Var}(b'_{\mu_2}(\iota_2)|_i) \sum_{j_3=0}^{n-1} \mathbb{E}[e^{\mu_2}|_{j_3}^2] \sum_{j_4=0}^{n-1} \mathbb{E}[s^{\iota_2}|_{j_4}^2] \right),$$

which can be reordered as

$$n \sum_{\mu} \sum_{\mu_1+\mu_2=\mu} \mathsf{Var}(b_{\mu_1}(\iota_1)|_i)\mathsf{Var}(b'_{\mu_2}(\iota_2)|_i) \\ \cdot \sum_{j_1=0}^{n-1} \mathbb{E}[e^{\mu_1}|_{j_1}^2] \sum_{j_3=0}^{n-1} \mathbb{E}[e^{\mu_2}|_{j_3}^2] \sum_{j_2=0}^{n-1} \mathbb{E}[s^{\iota_1}|_{j_2}^2] \sum_{j_4=0}^{n-1} \mathbb{E}[s^{\iota_2}|_{j_4}^2],$$

Recalling that the correction function F approximates the following quantities

$$\begin{cases} F_e(\iota_1, \iota_2) \approx \frac{\sum_{i=0}^{n-1} \mathbb{E}[e^{\iota_1+\iota_2}|_i^2]}{\sum_{i_1=0}^{n-1} \mathbb{E}[e^{\iota_1}|_{i_1}^2] \sum_{i_2=0}^{n-1} \mathbb{E}[e^{\iota_2}|_{i_2}^2]} \\ F_s(\iota_1, \iota_2) \approx \frac{\sum_{i=0}^{n-1} \mathbb{E}[s^{\iota_1+\iota_2}|_i^2]}{\sum_{i_1=0}^{n-1} \mathbb{E}[s^{\iota_1}|_{i_1}^2] \sum_{i_2=0}^{n-1} \mathbb{E}[s^{\iota_2}|_{i_2}^2]} \end{cases}$$

It is possible to use these functions in order to express $\mathsf{Var}((a_{\iota_1} s^{\iota_1} \cdot a'_{\iota_2} s^{\iota_2})|_i)$ in terms of $\mathsf{Var}(a_{\iota_1} s^{\iota_1}|_i)\mathsf{Var}(a'_{\iota_2} s^{\iota_2}|_i)$. In fact, $\mathsf{Var}((a_{\iota_1} s^{\iota_1} \cdot a'_{\iota_2} s^{\iota_2})|_i)$ can be written as

$$n \sum_{\mu} \sum_{\mu_1+\mu_2=\mu} \mathsf{Var}\left(b_{\mu_1}(\iota_1)|_i\right) \mathsf{Var}\left(b'_{\mu_2}(\iota_2)|_i\right) \sum_{j=0}^{n-1} \mathbb{E}[e^{\mu_1+\mu_2}|_j^2] \sum_{j'=0}^{n-1} \mathbb{E}[s^{\iota_1+\iota_2}|_{j'}^2].$$

Thus, by leveraging the properties of the correction functions

$$\begin{aligned} nF_s(\iota_1, \iota_2) \sum_{\mu} \sum_{\mu_1+\mu_2=\mu} & \mathsf{Var}\left(b_{\mu_1}(\iota_1)|_i\right) \mathsf{Var}\left(b'_{\mu_2}(\iota_2)|_i\right) F_e(\mu_1, \mu_2) \cdot \\ & \cdot \sum_{j_1=0}^{n-1} \mathbb{E}[e^{\mu_1}|_{j_1}^2] \sum_{j_2=0}^{n-1} \mathbb{E}[e^{\mu_2}|_{j_2}^2] \sum_{j_3=0}^{n-1} \mathbb{E}[s^{\iota_1}|_{j_3}^2] \sum_{j_4=0}^{n-1} \mathbb{E}[s^{\iota_2}|_{j_4}^2] \\ \approx \quad nF_s(\iota_1, \iota_2) \sum_{\mu} \sum_{\mu_1+\mu_2=\mu} & \mathsf{Var}\left(b_{\mu_1}(\iota_1)|_i\right) \mathsf{Var}\left(b'_{\mu_2}(\iota_2)|_i\right) F_e(\mu_1, \mu_2) \cdot \\ & \cdot \sum_{j_1=0}^{n-1} \mathbb{E}[e^{\mu_1}|_{j_1}^2] \sum_{j_2=0}^{n-1} \mathbb{E}[e^{\mu_2}|_{j_2}^2] \sum_{j_3=0}^{n-1} \mathbb{E}[s^{\iota_1}|_{j_3}^2] \sum_{j_4=0}^{n-1} \mathbb{E}[s^{\iota_2}|_{j_4}^2]. \end{aligned}$$

Then, by exploiting the monotonicity of F_e and F_s [2], it is possible to derive an upper bound given by

$$nF_s(\iota_1,\iota_2)F_e(K_1,K_2)\sum_{\mu}\sum_{\mu_1+\mu_2=\mu}\mathsf{Var}\left(b_{\mu_1}(\iota_1)|_i\right)\mathsf{Var}\left(b'_{\mu_2}(\iota_2)|_i\right)\cdot \\ \cdot\sum_{j_1=0}^{n-1}\mathbb{E}[e^{\mu_1}|_{j_1}^2]\sum_{j_2=0}^{n-1}\mathbb{E}[e^{\mu_2}|_{j_2}^2]\sum_{j_3=0}^{n-1}\mathbb{E}[s^{\iota_1}|_{j_3}^2]\sum_{j_4=0}^{n-1}\mathbb{E}[s^{\iota_2}|_{j_4}^2],$$

where K_1, K_2 represent the highest power of e appearing in $a_{\iota_1}, a'_{\iota_2}$, respectively. It is straightforward to verify that this concludes our proof, yielding

$$\mathsf{Var}((a_{\iota_1}s^{\iota_1}\cdot a'_{\iota_2}s^{\iota_2})|_i) = nF_s(\iota_1,\iota_2)F_e(K_1,K_2)\mathsf{Var}(a_{\iota_1}s^{\iota_1}|_i)\mathsf{Var}(a'_{\iota_2}s^{\iota_2}|_i).$$

□

Remark 1 *Theorem 1 provides an upper bound on the variance of the product $a_{\iota_1}s^{\iota_1}\cdot a'_{\iota_2}s^{\iota_2}$. However, it is significant to point out that this estimate can be regarded as a faithful approximation, i.e.,*

$$\mathsf{Var}((a_{\iota_1}s^{\iota_1}a'_{\iota_2}s^{\iota_2})|_i) \approx n\mathsf{Var}((a_{\iota_1}s^{\iota_1})|_i)\mathsf{Var}((a'_{\iota_2}s^{\iota_2})|_i)F_s(\iota_1,\iota_2)F_e(K_1,K_2).$$

The reason behind this statement can be immediately found in the distributions of the b_μ-terms in the noise of a fresh ciphertext. In fact, for a fresh ciphertext, the critical quantity can be expressed as

$$\nu = a_0 + a_1 s = (b_0(0) + b_1(0)\cdot e) + b_0(1)s,$$

where

$$\begin{cases} a_0 = b_0(0) + b_1(0)\cdot e = (m + te_0) + tu\cdot e \\ a_1 = b_0(1) = te_1 \end{cases}$$

Then, it can be observed that the variance of the b_μ-values is given by

$$\begin{cases} \mathsf{Var}(b_0(0)|_i) = V_m + t^2V_e \\ \mathsf{Var}(b_1(0)|_i) = nt^2V_eV_u \\ \mathsf{Var}(b_0(1)|_i) = nt^2V_eV_s \end{cases}$$

where n typically assumes values in $\{2^{13}, 2^{14}, 2^{15}, 2^{16}\}$. Consequently,

$$\mathsf{Var}(b_0(0)|_i) \ll \mathsf{Var}(b_1(0)|_i), \mathsf{Var}(b_0(1)|_i).$$

Therefore, $b_0(0)$ becomes negligible in our analysis, and we can assume $a_0 \approx b_1(0)\cdot e$, obtaining the approximated version of the theorem.

However, in order to maintain our results as general as possible, our next analysis will refer to the upper bound version of the theorem, still knowing that it corresponds to a reliable approximation.

5 Application of Our Variance Estimation Method to Fixed Circuits

This section employs the results of Section 4 to propose an effective method for tracking the error growth in circuits with a fixed number of operation. As previously highlighted, obtaining bounds sufficiently tight with respect to the experimental values of the error coefficients' variance is crucial for development and real use of homomorphic encryption.

These bounds, in fact, allow one to construct new techniques for efficiently finding initial scheme parameters that improve performance and security simultaneously. Naturally, the behavior of the error is very dependent on the specific circuit under consideration, that is, the sequence of operations that the scheme must accommodate.

We analyze a circuit in which pairs of ciphertexts are progressively multiplied. We focus on circuits that primarily involves homomorphic multiplication, since, as previously mentioned, it is the most complex and therefore the most significant operation to study.

For clarity, we divide the analysis into two distinct scenarios. In the first scenario, only theoretical, the modulus switch technique is not applied, resulting in a very rapid increase of the error. Instead, in the second case, the modulus switch is performed after each multiplication.

Typically, the first scenario is not taken into account, as the error magnitude, without modulus switching, quickly becomes unmanageable, making the scheme impractical for real-world applications. In contrast, with modulus switching, error growth is significantly diminished, and the noise remains within a manageable range. This is, in fact, one of the primary goals pursued in designing practical FHE schemes.

However, the application of modulus switch drastically reduces the differences in estimates derived from even significantly distant approaches. Instead, by studying circuits without the modulus switch, we believe that the necessity of considering the dependencies in the coefficients of the error polynomial becomes unequivocal.

For this reason, although the absence of modulus switching does not reflect a realistic scenario, we decided to start our analysis in this simplified context. This allows us to highlight the key structural aspects of error growth, which are then carried over and extended to the more realistic case involving modulus switching.

Again, we want to stress that circuits without modulo switch are not practicable and do not have real world applications. The choice to describe this scenario is purely to complete the explanation of our method, further emphasizing the differences between our approach and others considered.

The remainder of this section is structured as follows. In the first part, we present circuits without modulus switching. Subsequently, we focus on practical circuits that employ modulus switching, showing how the results from Section 4 can be applied in this setting.

Based on the results, we are confident that our estimates represent a tangible improvement over the current state of the art. Our bounds closely match the experimental results, while consistently avoiding underestimation, which affects instead the existing approaches and must be avoided for the proper functioning of the scheme together with its security.

5.1 Circuits without Modulo Switch

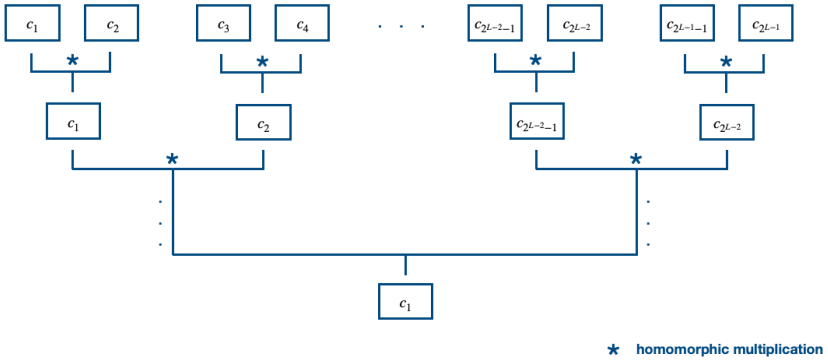

Fig. 1: Reference circuit

Figure 1 provides a schematic representation of the circuit used as a reference for our analysis. Let M denote the multiplicative depth of the circuit, that is, the number of multiplications to be supported. To facilitate the analysis, we divide the circuit into $L = M + 1$ levels.

For the considered circuit, we assume the independent and random generation of 2^{L-1} plaintexts, which are then encrypted using the same public key, resulting in 2^{L-1} fresh ciphertexts, denoted by $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_{2^{L-1}}$.

At each level $l \in [0, \ldots, L-1]$, pairs of ciphertexts are multiplied, yielding the corresponding ciphertexts of the $(l+1)$-th level, and then the process is repeated until the final ciphertext is computed.

Our study aims to estimate the variance of the coefficients of the critical quantity $\nu^{(l)}|_i$, denoted as V_l, which corresponds to the ciphertexts of the circuit at level l.

According to the current average-case approach, the variance at level l can be approximated as

$$V_l \leq nV_{l-1}^2.$$

However, as pointed out by the authors of [25], this estimation tends to underestimate the variance observed in experimental evaluations. Such underestimation may lead to security vulnerabilities, as previously discussed, and, therefore, must be avoided.

In contrast, in our investigation, we proved that

$$V_l \leq nh(l)V_{l-1}^2, \tag{5}$$

where h is a function specifically designed to account for the dependencies among the coefficients of the error polynomial. This construction is based on the correction function F introduced in [2] and represents the crucial difference compared to the current approach [25].

Section 4 has laid the groundwork for deriving this bound. Thus, the construction of our bound can now be presented, beginning with the initial levels and subsequently extending the reasoning to the general case for a level l.

First Multiplication Let $\boldsymbol{c}, \boldsymbol{c'}$ be two fresh ciphertexts with critical quantities $\nu = a_0 + a_1 s$, $\nu' = a'_0 + a'_1 s$, respectively, where

$$\begin{cases} a_0 = b_0(0) + b_1(0) \cdot e = (m + te_0) + tu \cdot e \\ a_1 = b_0(1) = te_1 \end{cases}$$

$$\begin{cases} a'_0 = b'_0(0) + b'_1(0) \cdot e = (m' + te'_0) + tu' \cdot e \\ a'_1 = b'_0(1) = te'_1 \end{cases}$$

Let V_0 be the variance of the critical quantity associated with the fresh ciphertexts. Then, it can be observed that

$$\begin{cases} V(a_0|_i) = V(a'_0|_i) = t^2(\frac{1}{12} + V_e + nV_eV_u) \\ V(a_1 s|_i) = V(a'_1 s|_i) = t^2 nV_eV_s \end{cases}$$

Therefore, it is possible to assume that

$$V(a_0|_i) \approx V(a_1 s|_i) \approx \frac{V_0}{2}, \tag{6}$$

since $V_u = V_s$, due to the choice of the distributions of s and u, and

$$\frac{1}{12} + V_e \ll nV_eV_u,$$

which is then negligible, as highlighted in Remark 1.

Clearly, the same reasoning can be applied to $V(a'_0|_i), V(a'_1 s|_i)$, obtaining

$$V(a'_0|_i) \approx V(a'_1 s|_i) \approx \frac{V_0}{2}. \tag{7}$$

Our goal is to estimate the coefficients variance of $\nu_{\mathsf{mul}} = \nu \cdot \nu'$, which will be referred to as V_1, following the level notation introduced at the beginning. Moreover, according to the previously introduced notation, it is possible to write ν_{mul} as

$$\nu_{\mathsf{mul}} = a_0 a'_0 + (a_0 a'_1 + a_1 a'_0) \cdot s + a_1 a'_1 \cdot s^2.$$

Consequently, when the variance is considered, applying Theorem 1 and using that the covariance of this addends is zero, it follows that

$$\begin{aligned} V_1 := \mathsf{Var}(\nu_{\mathsf{mul}}|_i) \leq\ & n\mathsf{Var}(a_0|_i)\mathsf{Var}(a'_0|_i)F_s(0,0)F_e(1,1) \\ & + n\mathsf{Var}(a_0|_i)\mathsf{Var}((a'_1 s)|_i)F_s(0,1)F_e(1,0) \\ & + n\mathsf{Var}((a_1 s)|_i)\mathsf{Var}(a'_0|_i)F_s(1,0)F_e(0,1) \\ & + n\mathsf{Var}((a_1 s)|_i))\mathsf{Var}((a'_1 s)|_i)F_s(1,1)F_e(0,0). \end{aligned}$$

Moreover, this bound can be simplified, observing that $F_s(0,0) = F_s(1,0) = F_s(0,1) = 1$ and $F_e(0,0) = F_e(1,0) = F_e(0,1) = 1$. Therefore, it follows that

$$\begin{aligned} V_1 \leq\ & n\mathsf{Var}(a_0|_i)\mathsf{Var}(a'_0|_i)F_e(1,1) + n\mathsf{Var}(a_0|_i)\mathsf{Var}((a'_1 s)|_i) \\ & + n\mathsf{Var}((a_1 s)|_i)\mathsf{Var}(a'_0|_i) + n\mathsf{Var}((a_1 s)|_i))\mathsf{Var}((a'_1 s)|_i)F_s(1,1). \end{aligned}$$

Again, this can be reformulated using (6) and (7) as

$$V_1 \leq \frac{nV_0^2}{4}\left(F_e(1,1) + F_s(1,1) + 2\right).$$

Hence, the first value of the function h we aim to construct, can be fixed as

$$h(1) = \frac{F_s(1,1) + F_e(1,1) + 2}{4}.$$

Thus, for the first level, the following inequality has been proven

$$V_1 \leq nh(1)V_0^2.$$

Second Multiplication In the second multiplication, the ciphertexts involved will have an associated critical quantity of the form

$$\nu = a_0 + a_1 \cdot s + a_2 \cdot s^2,$$

where, according to our study, each coefficient has variance

$$\begin{cases} \mathsf{Var}(a_0|_i) \approx \frac{F_e(1,1)V_1}{F_s(1,1)+F_e(1,1)+2} \\ \mathsf{Var}(a_1 s|_i) \approx \frac{2V_1}{F_s(1,1)+F_e(1,1)+2} \\ \mathsf{Var}(a_2 s^2|_i) \approx \frac{F_s(1,1)V_1}{F_s(1,1)+F_e(1,1)+2} \end{cases}$$

Therefore, by repeating the same procedure depicted above, the critical quantity after the second multiplication will be of the form

$$\nu \cdot \nu' = a_0 a_0' + (a_0 a_1' + a_0' a_1)s + (a_1 a_1' + a_0 a_2' + a_0' a_2)s^2 + (a_1 a_2' + a_1' a_2)s^3 + a_2 a_2' s^4$$

Thus, its coefficients' variance can be estimated as

$$\begin{aligned} V_2 \leq \frac{nV_1^2}{(2 + F_s(1,1) + F_e(1,1))^2} \big[& F_e(1,1)^2 \cdot F_s(0,0) F_e(2,2) \\ & + 4F_e(1,1) \cdot F_s(0,1) F_e(1,2) + 4 \cdot F_s(1,1) F_e(1,1) \\ & + 2F_s(1,1) F_e(1,1) \cdot F_s(0,2) F_e(0,2) + 4F_s(1,1) \cdot F_s(1,2) F_e(0,1) \\ & + F_s(1,1)^2 \cdot F_s(2,2) F_e(0,0) \big], \end{aligned}$$

where this inequality follows from the fact that a_0 contains a term multiplied by e^2, a_1 contains a term multiplied by e and a_2 does not contain any powers of e. As a result, $h(2)$ can be chosen as

$$\begin{aligned} h(2) = \frac{1}{(2 + F_s(1,1) + F_e(1,1))^2} \big[& F_e(1,1)^2 \cdot F_s(0,0) F_e(2,2) \\ & + 4F_e(1,1) \cdot F_s(0,1) F_e(1,2) + 4 \cdot F_s(1,1) F_e(1,1) \\ & + 2F_s(1,1) F_e(1,1) \cdot F_s(0,2) F_e(0,2) \\ & + 4F_s(1,1) \cdot F_s(1,2) F_e(0,1) + F_s(1,1)^2 \cdot F_s(2,2) F_e(0,0) \big]. \end{aligned}$$

Consequently, $V_2 \leq nh(2)V_1^2$.

Generalization Finally, this procedure can be easily generalized in order to compute all the necessary values for h, therefore proving our bound in (5), i.e.,

$$V_l \leq nh(l)V_{l-1}^2, \qquad l = 1, \ldots, L-1.$$

5.2 Circuits with Modulo Switch

In the present section, the reasoning previously introduced is adapted to circuits where the modulus switching technique is employed, in order to exploit the advantages of the method in practical scenarios.

Let L denote the number of levels in the circuit, and $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_{2^{L-1}}$ the initial fresh ciphertexts, generated by encrypting 2^{L-1} independent and randomly generated messages, using the same key. The reference circuit for our analysis is depicted in Fig. 2.

We consider a model in which, at each level, homomorphic multiplication of pairs of ciphertexts is carried out. The key difference is that at the beginning of each level $l \in \{1, \ldots, L-1\}$ the input ciphertexts are switched to a smaller modulus,

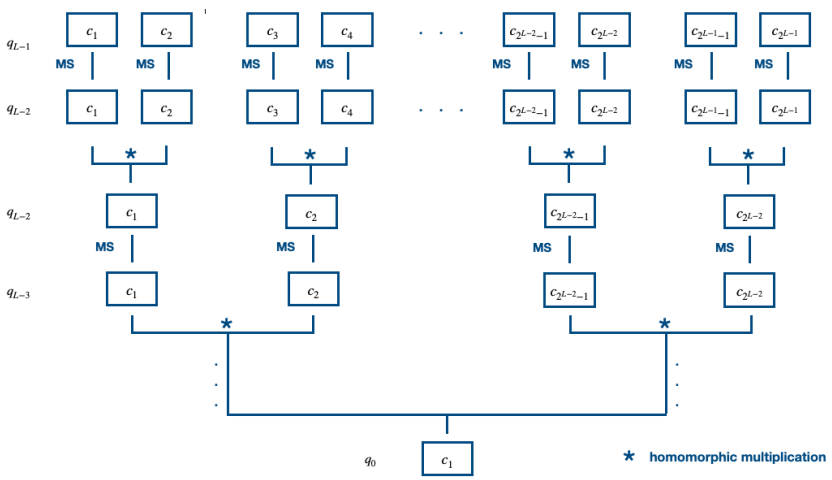

Fig. 2: Reference circuit

to maintain the error almost constant throughout the process. In particular, following the previously defined notion, let q_l be the ciphertexts moduli of each level, defined as

$$q_l = \prod_{j=0}^{l} p_j,$$

where p_j are primes such that $\gcd(p_i, p_j) = 1$ for $i \neq j$.

The process represented by the circuit can be resumed as follows:

- At level 0, all the fresh ciphertexts are defined in $\mathcal{R}_{q_{L-1}} \times \mathcal{R}_{q_{L-1}}$;
- At level 1, modulo switch to q_{L-2} is applied to each of the initial fresh ciphertexts. After that, the first homomorphic multiplication is performed in $\mathcal{R}_{q_{L-2}}$, yielding 2^{L-2} resulting ciphertexts in $\mathcal{R}^3_{q_{L-2}}$. Finally, these ciphertexts are relinearized to obtain equivalent ones in $\mathcal{R}^2_{q_{L-2}}$, which constitutes the input of the next level;
- At level 2, each input ciphertext undergoes a modulo switch from q_{L-2} to q_{L-3}, which is again followed by the homomorphic multiplication of pairs of them. To conclude, a relinearization step is carried out;
- This process is repeated until level $L-1$, where a final ciphertext, which constitutes the output of the circuit, is returned;

It should be noted that, in the circuit represented in Fig. 2, the relinearization step is not explicated. In fact, as for the case of the circuit without modulus switching, we decided to omit its contribution from our error analysis, since it is negligible compared to the impact of modulus switch and multiplication.

Before discussing the results, it should be noted that, in contrast to the case without the modulus switching, in this scenario, L ciphertext moduli are required for

the operation of the circuit. Therefore, the selection of parameters will consist in choosing all the q_l values, i.e., all the primes p_j, such that the correct functioning of the scheme is ensured while still choosing sufficiently small moduli in order to improve efficiency, which is crucial for practical usage of BGV.

For better understanding, we will divide our analysis according to the level l considered. Specifically, an in-depth explanation of the noise estimates for the first three levels will be provided. Then, these results will be generalized for a fixed level l, thus delineating our bound.

Level 0 Let $\boldsymbol{c} \in \mathcal{R}_{q_{L-1}} \times \mathcal{R}_{q_{L-1}}$ be a fresh ciphertext, obtained encrypting a random message $m \in \mathcal{R}_t$.
Let $\nu_{\mathsf{clean}} = a_0 + a_1 s$ be the critical quantity associated with $\boldsymbol{c}$.
As for the circuits without modulo switching, it is possible to assume that

$$\mathsf{Var}(a_0|_i) \approx \mathsf{Var}((a_1 s)|_i) \approx \frac{V_0}{2}, \tag{8}$$

where the notation V_0 is used to denote the variance of the coefficients of the critical quantity ν_{clean}. In general, the notation V_l will be used to represent the variance of the coefficients of the critical quantity at the end of level l. It is significant to observe that the assumption in (8) applies to all initial 2^{L-1} ciphertexts. In fact, the estimate of V_l is the same for all ciphertexts belonging to the same level.

Level 1 As mentioned above, at the beginning of level 1, all ciphertexts are subject to a modulus switch from q_{L-1} to q_{L-2}.
Therefore, the error and the modulus of $\boldsymbol{c}$ are rescaled by a factor of $q_{L-2}/q_{L-1} = 1/p_{L-1}$. Thus, the critical quantity associated to the resulting ciphertext is given by

$$\nu_{\mathsf{modswitch}} = \frac{\nu_{\mathsf{clean}} + \nu_{\mathsf{ms}}(p_{L-1})}{p_{L-1}}, \tag{9}$$

where $\nu_{\mathsf{ms}}(p_{L-1})$ is defined as

$$\nu_{\mathsf{ms}}(p_{L-1}) = \delta_0 + \delta_1 s \qquad \delta_i = t[-c_i t^{-1}]_{p_{L-1}}$$

In particular, for the following analysis we will use the notation

$$\frac{\nu_{\mathsf{ms}}(p_{L-1})}{p_{L-1}} = a_0^{\mathsf{ms}} + a_1^{\mathsf{ms}} s,$$

with

$$\begin{cases} a_0^{\mathsf{ms}} = \frac{\delta_0}{p_{L-1}} \\ a_1^{\mathsf{ms}} = \frac{\delta_1}{p_{L-1}} \end{cases}$$

Moreover, we will denote with V_{ms} the following variance

$$V_{\mathsf{ms}} = \mathsf{Var}\left(\frac{\nu_{\mathsf{ms}}(p_{L-1})}{p_{L-1}} \bigg|_i \right).$$

For our analysis, it is possible to assume that $V_{\mathsf{ms}} \approx \mathsf{Var}(a_1^{\mathsf{ms}} s|_i)$. This is a consequence of the fact that, observing the distributions of the coefficients in a_0^{ms} and a_1^{ms}, it is evident that $\mathsf{Var}(a_0^{\mathsf{ms}}|_i) \ll \mathsf{Var}(a_1^{\mathsf{ms}} s|_i)$. In fact, noting that $c_i \leftarrow \mathcal{U}_{q_{L-1}}$, it is possible to estimate the variance of $a_0^{\mathsf{ms}}|_i$ and $a_1^{\mathsf{ms}}|_i$ as

$$\begin{cases} \mathsf{Var}(a_0^{\mathsf{ms}}|_i) = \mathsf{Var}(a_1^{\mathsf{ms}}|_i) = t^2/12 \\ \mathsf{Var}(a_1^{\mathsf{ms}} s|_i) = t^2 n V_s/12, \end{cases}$$

where n is typically in $\{2^{12}, 2^{13}, 2^{14}, 2^{15}\}$. With this in mind, we can proceed with the analysis of the noise growth related to the multiplication of two ciphertexts, whose associated critical quantity is as in (9).

We start by observing that the critical quantity in (9) can be written as

$$\nu_{\mathsf{modswitch}} = \hat{a_0} + \hat{a_1} s = \frac{a_0}{p_{L-1}} + a_0^{\mathsf{ms}} + \left(\frac{a_1}{p_{L-1}} + a_1^{\mathsf{ms}} \right) s.$$

Moreover, it is possible to further simplify the notation by using the fact that $\mathbb{E}[a_0^{\mathsf{ms}}] = 0$ and its variance is negligible. Therefore, we rewrite this value as

$$\nu_{\mathsf{modswitch}} = \hat{a_0} + \hat{a_1} s = \frac{a_0}{p_{L-1}} + \left(\frac{a_1}{p_{L-1}} + a_1^{\mathsf{ms}} \right) s.$$

Then, it can be derived that

$$\begin{cases} \mathsf{Var}(\hat{a_0}|_i) \approx \frac{V_0}{2p_{L-1}^2} \\ \mathsf{Var}(\hat{a_1} s|_i) \approx \frac{V_0}{2p_{L-1}^2} + V_{\mathsf{ms}} \end{cases}$$

since

$$\mathsf{Var}\left(\frac{a_0}{p_{L-1}} \Big|_i \right) = \mathsf{Var}\left(\frac{a_1}{p_{L-1}} s \Big|_i \right) = \frac{V_0}{2p_{L-1}^2}.$$

In order to estimate the variance of the critical quantity resulting from multiplication, we will rely on Theorem 1. In particular, in this analysis, we will try to avoid explicitly writing the terms $b_\mu(\iota)$ involved in the expression of a generic $a_\iota = \sum_{\mu=0}^{K} b_\mu(\iota) e^\mu$, to avoid the notation becoming cumbersome. However, it is crucial to keep in mind the highest power of e, namely K, present in the terms a_ι involved in the multiplications, as the correction of the function F depends on this value. Precisely, for fresh ciphertexts at level 0, it can be seen that for a_0 the associated K is 1, while for a_1 we have $K = 0$. Instead, for the terms $a_0^{\mathsf{ms}}, a_1^{\mathsf{ms}}$ the case is quite different. In fact, these values can be assumed to be randomly distributed over $\mathcal{R}_t$, i.e. $a_0^{\mathsf{ms}}, a_1^{\mathsf{ms}} \leftarrow \mathcal{U}_t$ for every level of the circuit. This makes the analysis slightly more complicated, since, in order to derive tight estimates, it will be necessary to distinguish the contribution of a_0, a_1 from the one of $a_0^{\mathsf{ms}}, a_1^{\mathsf{ms}}$.

Now, assume that $\boldsymbol{c}, \boldsymbol{c}' \in \mathcal{R}_{q_{L-2}} \times \mathcal{R}_{q_{L-2}}$ are two ciphertexts at level 1, after modulus switching has been carried out. Their associated critical quantity is

given, respectively, by

$$\begin{cases} \nu_{\mathsf{modswitch}} = \frac{1}{p_{L-1}} a_0 + \left(\frac{1}{p_{L-1}} a_1 + a_1^{\mathsf{ms}} \right) s \\ \nu'_{\mathsf{modswitch}} = \frac{1}{p_{L-1}} a'_0 + \left(\frac{1}{p_{L-1}} a'_1 + a_1'^{\,\mathsf{ms}} \right) s \end{cases}$$

Therefore, the critical quantity obtained after their multiplication is of the form

$$\nu_{\mathsf{mul}}^{(1)} = a_0^{\mathsf{mul}} + a_1^{\mathsf{mul}} s + a_2^{\mathsf{mul}} s^2,$$

namely,

$$\begin{aligned} \nu_{\mathsf{mul}}^{(1)} = & \frac{1}{p_{L-1}^2} a_0 a'_0 + \frac{1}{p_{L-1}^2} \left(a'_0 a_1 + a_0 a'_1 \right) s + \frac{1}{p_{L-1}} (a'_0 a_1^{\mathsf{ms}} + a_0 a_1'^{\,\mathsf{ms}}) s \\ & + \frac{1}{p_{L-1}^2} a_1 a'_1 s^2 + \frac{1}{p_{L-1}} (a_1 a_1'^{\,\mathsf{ms}} + a'_1 a_1^{\mathsf{ms}}) s^2 + a_1'^{\,\mathsf{ms}} a_1^{\mathsf{ms}} s^2. \end{aligned}$$

So, we are now able to provide an estimate of the variance $V_1 = \mathsf{Var}(\nu_{\mathsf{mul}}|_i)$, applying Theorem 1, as follows

$$\begin{aligned} V_1 \leq & \frac{n}{p_{L-1}^4} V(a_0|_i) V(a'_0|_i) F_e(1,1) \\ & + \frac{n}{p_{L-1}^4} V(a'_0|_i) V(a_1 s|_i) + \frac{n}{p_{L-1}^4} V(a_0|_i) V(a'_1 s|_i) \\ & + \frac{n}{p_{L-1}^2} V(a'_0|_i) V(a_1^{\mathsf{ms}} s|_i) + \frac{n}{p_{L-1}^2} V(a_0|_i) V(a_1'^{\,\mathsf{ms}} s|_i) \\ & + \frac{n}{p_{L-1}^4} V(a_1 s|_i) V(a'_1 s|_i) F_s(1,1) + \frac{n}{p_{L-1}^2} V(a_1 s|_i) V(a_1'^{\,\mathsf{ms}} s|_i) F_s(1,1) \\ & + \frac{n}{p_{L-1}^2} V(a'_1 s|_i) V(a_1^{\mathsf{ms}} s|_i) F_s(1,1) + n V(a_1^{\mathsf{ms}} s|_i) V(a_1'^{\,\mathsf{ms}} s|_i) F_s(1,1). \end{aligned}$$

which, recalling that $\mathrm{Var}(a_\iota|_i) = \mathrm{Var}(a'_\iota|_i)$ and that $V(a_1^{\mathsf{ms}} s|_i) = V(a_1'^{\,\mathsf{ms}} s|_i) = V_{\mathsf{ms}}$, can be rewritten as

$$\begin{aligned} V_1 \leq & \frac{n}{p_{L-1}^4} V(a_0|_i)^2 F_e(1,1) + \\ & + \frac{2n}{p_{L-1}^4} V(a_0|_i) V(a_1 s|_i) + \frac{2n}{p_{L-1}^2} V_{\mathsf{ms}} V(a_0|_i) \\ & + \frac{n}{p_{L-1}^4} V(a_1 s|_i)^2 F_s(1,1) + \frac{2n}{p_{L-1}^2} V_{\mathsf{ms}} V(a_1 s|_i) + n F_s(1,1) V_{\mathsf{ms}}^2. \end{aligned}$$

By substituting to $V(a_0|_i)$,$V(a_1 s|_i)$ the value $\frac{V_0}{2}$, our bound on V_1 is derived. To conclude, it is possible to observe that the following estimate holds

$$\begin{cases} V(a_0^{\mathsf{mul}}|_i) \approx \frac{n}{p_{L-1}^4} V(a_0|_i)^2 F_e(1,1) \\ V(a_1^{\mathsf{mul}} s|_i) \approx \frac{2n}{p_{L-1}^4} V(a_0|_i) V(a_1 s|_i) + \frac{2n}{p_{L-1}^2} V_{\mathsf{ms}} V(a_0|_i) \\ V(a_2^{\mathsf{mul}} s^2|_i) \approx \frac{n}{p_{L-1}^4} V(a_1 s|_i)^2 F_s(1,1) + \frac{2n}{p_{L-1}^2} V_{\mathsf{ms}} V(a_1 s|_i) + n F_s(1,1) V_{\mathsf{ms}}^2 \end{cases} \tag{10}$$

These values are needed in order to bound the variance V_2 at the end of the next level.

Level 2 The first computation at level 2 is the modulo switch from q_{L-2} to q_{L-3}. It should be noted that, for our theoretical analysis, we chose to avoid considering the key switching step. Therefore, the ciphertexts which will be subject to modulo switch have critical quantity of the form

$$\nu^{(1)} = a_0 + a_1 s + a_2 s^2,$$

with a_0, a_1, a_2 having variances as in (10).

After the modulo switch, the critical quantity associated to the resulting ciphertexts will be as follows

$$\nu_{\mathsf{modswitch}} = \frac{\nu^{(1)} + \nu_{\mathsf{ms}}(p_{L-2})}{p_{L-2}}.$$

Therefore, it is possible to express this quantity as

$$\nu_{\mathsf{modswitch}} = \frac{a_0}{p_{L-2}} + \left(\frac{a_1}{p_{L-2}} + a_1^{\mathsf{ms}}\right) s + \frac{a_2}{p_{L-2}} s^2.$$

For this level, the maximum power of e contained in each a_i has changed.
In fact, a_0 contains a term multiplied by e^2, a_1 a term multiplied by e, while a_2 does not contain any power of e as for the term a_1^{ms}.
This distinction is crucial in order to correctly apply Theorem 1.
In light of this, given two ciphertexts with critical quantities, respectively,

$$\begin{cases} \nu_{\mathsf{modswitch}} = \frac{a_0}{p_{L-2}} + \left(\frac{a_1}{p_{L-2}} + a_1{}^{\mathsf{ms}}\right) s + \frac{a_2}{p_{L-2}} s^2 \\ \nu'_{\mathsf{modswitch}} = \frac{a'_0}{p_{L-2}} + \left(\frac{a'_1}{p_{L-2}} + a'_1{}^{\mathsf{ms}}\right) s + \frac{a'_2}{p_{L-2}} s^2 \end{cases}$$

the resulting $\nu^{(2)}_{\mathsf{mul}}$ that follows by their multiplication will be of the form

$$\nu^{(2)}_{\mathsf{mul}} = \nu_{\mathsf{modswitch}} \cdot \nu'_{\mathsf{modswitch}} = a_0^{\mathsf{mul}} + a_1^{\mathsf{mul}} s + a_2^{\mathsf{mul}} s^2 + a_3^{\mathsf{mul}} s^3 + a_4^{\mathsf{mul}} s^4,$$

which can be written as

$$\begin{aligned} \nu^{(2)}_{\mathsf{mul}} = {} & \frac{a_0 a'_0}{p^2_{L-2}} + \frac{a'_0}{p_{L-2}} \left(\frac{a_1}{p_{L-2}} + a_1{}^{\mathsf{ms}}\right) s + \frac{a_0}{p_{L-2}} \left(\frac{a'_1}{p_{L-2}} + a'_1{}^{\mathsf{ms}}\right) s \\ & + \left(\frac{a_1}{p_{L-2}} + a_1{}^{\mathsf{ms}}\right) \left(\frac{a'_1}{p_{L-2}} + a'_1{}^{\mathsf{ms}}\right) s^2 + \frac{a_0 a'_2}{p^2_{L-2}} s^2 + \frac{a'_0 a_2}{p^2_{L-2}} s^2 \\ & + \frac{a'_2}{p_{L-2}} \left(\frac{a_1}{p_{L-2}} + a_1{}^{\mathsf{ms}}\right) s^3 + \frac{a_2}{p_{L-2}} \left(\frac{a'_1}{p_{L-2}} + a'_1{}^{\mathsf{ms}}\right) s^3 + \frac{a_2 a'_2}{p^2_{L-2}} s^4. \end{aligned}$$

A bound over V_2 can then be deduced, by applying Theorem 1 and recalling that $\mathsf{Var}(a_\iota|_i) = \mathsf{Var}(a'_\iota|_i)$, resulting in

$$\begin{aligned} V_2 \leq & \frac{n}{p_{L-2}^4}\mathsf{Var}(a_0|_i)^2 F_e(2,2) + \frac{2n}{p_{L-2}^4}\mathsf{Var}(a_0|_i)\mathsf{Var}(a_1 s|_i)F_e(1,2) \\ & + \frac{n}{p_{L-2}^4}\mathsf{Var}(a_1 s|_i)^2 F_s(1,1)F_e(1,1) + \frac{2n}{p_{L-2}^4}\mathsf{Var}(a_0|_i)\mathsf{Var}(a_2 s^2|_i) \\ & + \frac{2n}{p_{L-2}^4}\mathsf{Var}(a_1 s|_i)\mathsf{Var}(a_2 s^2|_i)F_s(1,2) + \frac{n}{p_{L-2}^4}\mathsf{Var}(a_2 s^2|_i)^2 F_s(2,2) \\ & + \frac{2n}{p_{L-2}^2}V_{\mathsf{ms}}\mathsf{Var}(a_0|_i) + \frac{2n}{p_{L-2}^2}V_{\mathsf{ms}}\mathsf{Var}(a_1 s|_i)F_s(1,1) \\ & + \frac{2n}{p_{L-2}^2}V_{\mathsf{ms}}\mathsf{Var}(a_2 s^2|_i)F_s(1,2) + nV_{\mathsf{ms}}^2 F_s(1,1), \end{aligned}$$

where the values for $V(a_\iota s^\iota|_i)$ follows by (10). Moreover, similar to level 1, it is possible to deduce the contribution, in terms of variance, of each a_ι^{mul} of $\nu_{\mathsf{mul}}^{(2)}$, which will then be needed for the successive levels.

Level l For a generic level l, with $l \in \{1, \ldots, L-1\}$, the same reasoning applied in the first levels can be reiterated. Assume that two ciphertexts with critical quantity of the form

$$\nu^{(l-1)} = \sum_{\iota=0}^{2^{l-1}} a_\iota s^\iota,$$

are given as input. Let V_l be the variance of the coefficients of $\nu^{(l)}$, which is the critical quantity obtained after modulo switch and multiplication.
Following the notation adopted in the precedent levels, this quantity can be indicated as

$$\nu^{(l)} = \sum_{\iota=0}^{2^l} a_\iota^{\mathsf{mul}} s^\iota.$$

Then, V_l is bounded by the sum of

$$\begin{aligned} V_l \leq & \frac{n}{p_{L-l}^4}\sum_{\iota=0}^{2^l}\sum_{k+\mu=\iota}\mathsf{Var}(a_k s^k|_i)\mathsf{Var}(a_\mu s^\mu|_i)F_s(\iota,\mu)F_e(2^{l-1}-\iota, 2^{l-1}-\mu) \\ & + \frac{2n}{p_{L-l}^2}\sum_{\iota=0}^{2^{l-1}} V_{\mathsf{ms}}\mathsf{Var}(a_\iota s^\iota|_i)F_s(1,\iota) + nV_{\mathsf{ms}}^2 F_s(1,1) \end{aligned} \tag{11}$$

Moreover, each term of $\nu^{(l)}$ has variance

$$\begin{cases} \mathsf{Var}(a_0^{\mathsf{mul}}|_i) = \frac{n}{p_{L-l}^4} \sum_{k+\mu=0} \mathsf{Var}(a_k s^k|_i)\mathsf{Var}(a_\mu s^\mu|_i) F_s(k,\mu) F_e(2^{l-1}-k, 2^{l-1}-\mu) \\ \mathsf{Var}(a_1^{\mathsf{mul}} s|_i) = \frac{n}{p_{L-l}^4} \sum_{k+\mu=1} \mathsf{Var}(a_k s^k|_i)\mathsf{Var}(a_\mu s^\mu|_i) F_s(k,\mu) F_e(2^{l-1}-k, 2^{l-1}-\mu) \\ \qquad + \frac{2n}{p_{L-l}^2} V_{\mathsf{ms}} \mathsf{Var}(a_0|_i) F_s(1,0) \\ \mathsf{Var}(a_2^{\mathsf{mul}} s^2|_i) = \frac{n}{p_{L-l}^4} \sum_{k+\mu=2} \mathsf{Var}(a_k s^k|_i)\mathsf{Var}(a_\mu s^\mu|_i) F_s(k,\mu) F_e(2^{l-1}-k, 2^{l-1}-\mu) \\ \qquad + \frac{2n}{p_{L-l}^2} V_{\mathsf{ms}} \mathsf{Var}(a_1 s|_i) F_s(1,1) + n F_s(1,1) V_{\mathsf{ms}}^2 \\ \mathsf{Var}(a_\iota^{\mathsf{mul}} s^\iota|_i) = \frac{n}{p_{L-l}^4} \sum_{k+\mu=\iota} \mathsf{Var}(a_k s^k|_i)\mathsf{Var}(a_\mu s^\mu|_i) F_s(k,\mu) F_e(2^{l-1}-k, 2^{l-1}-\mu) \\ \qquad + \frac{2n}{p_{L-l}^2} V_{\mathsf{ms}} \mathsf{Var}(a_{\iota-1} s^{\iota-1}|_i) F_s(1,\iota-1) \mathbb{I}_{\{0,\ldots,2^{l-1}+1\}}(\iota) \end{cases}$$

where $\mathbb{I}_{\{0,\ldots,2^{l-1}+1\}}(\iota)$ is the indicator function, i.e.,

$$\mathbb{I}_{\{0,\ldots,2^{l-1}+1\}}(\iota) = \begin{cases} 1, & \text{if } \iota \in \{0,\ldots,2^{l-1}+1\} \\ 0, & \text{if } \iota \notin \{0,\ldots,2^{l-1}+1\} \end{cases}$$

6 Conclusions

In this work, we focused on improving the current average-case approach for tracking the error and its growth under homomorphic operations. In particular, we demonstrated that the primary reason for the underestimation of noise in existing average-case methods lies in the fact that the coefficients of the error polynomial are treated as independent. However, to obtain accurate bounds that never underestimate the actual values observed in practice, it is crucial to account for the dependencies among these coefficients.

Accurate noise estimation plays a key role in the proper selection of scheme parameters, especially the ciphertext modulus q, to ensure correctness, security, and improved efficiency. To evaluate the effectiveness of our analysis, we applied our results to specific homomorphic circuits, comparing our estimations with both experimental data and those obtained from the current average-case approach. The circuits were implemented using the MAGMA language.

Our findings show that the proposed method effectively overcomes the limitations of existing average-case techniques, particularly their tendency to underestimate noise variance. Furthermore, in the context of initial parameter selection, the high accuracy of our estimations, consistently close to experimental results, represents a significant improvement over the worst-case methods that currently dominate state-of-the-art parameter generation. This leads to tighter bounds and thus enables more efficient configurations of the scheme, which is especially critical for promoting the practical adoption of homomorphic encryption, and in particular of the BGV scheme, in real-world applications.

Future work will include extending our approach to other cryptographic schemes, such as CKKS, as well as studying scenarios in which ciphertexts are generated in a dependent manner. We are currently developing a comprehensive framework for modulus selection that is fully aligned with the new approach introduced in this paper.

Acknowledgment

The third author was partially supported by the Italian Ministry of University and Research in the framework of the Call for Proposals for scrolling of final rankings of the PRIN 2022 call - Protocol no. 2022RFAZCJ and by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

References

1. Bai, S., D. Galbraith, S.: Lattice decoding attacks on binary LWE. In: Australasian Conference on Information Security and Privacy. pp. 322–337. Springer, Cham (2014)
2. Biasioli, B., Marcolla, C., Calderini, M., Mono, J.: Improving and automating BFV parameters selection: An average-case approach. Cryptology ePrint Archive, Paper 2023/600 (2023), https://eprint.iacr.org/2023/600
3. Brakerski, Z.: Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP. In: Advances in Cryptology – CRYPTO 2012. pp. 868–886 (2012)
4. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (Leveled) fully homomorphic encryption without bootstrapping. ACM Transactions on Computation Theory (TOCT) **6**(3), 1–36 (2014)
5. Checri, M., Sirdey, R., Boudguiga, A., Bultel, J.P., Choffrut, A.: On the practical cpad security of "exact" and threshold fhe schemes and libraries. Cryptology ePrint Archive (2024)
6. Cheon, J.H., Choe, H., Passelègue, A., Stehlé, D., Suvanto, E.: Attacks against the indcpa-d security of exact fhe schemes. Cryptology ePrint Archive (2024)
7. Cheon, J.H., Han, K., Kim, A., Kim, M., Song, Y.: A full RNS variant of approximate homomorphic encryption. In: International Conference on Selected Areas in Cryptography – SAC 2018. pp. 347–368. Springer (2018)
8. Cheon, J.H., Kim, A., Kim, M., Song, Y.: Homomorphic Encryption for Arithmetic of Approximate Numbers. In: Advances in Cryptology – ASIACRYPT 2017. pp. 409–437 (2017)
9. Chillotti, I., Gama, N., Georgieva, M., Izabachène, M.: Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In: Advances in Cryptology – ASIACRYPT 2016. pp. 3–33 (2016)
10. Chillotti, I., Gama, N., Georgieva, M., Izabachène, M.: TFHE: Fast Fully Homomorphic Encryption over the Torus. Journal of Cryptology **33**(1), 34–91 (2020)
11. Costache, A., Smart, N.P.: Which ring based somewhat homomorphic encryption scheme is best? In: Topics in Cryptology – CT-RSA 2016. pp. 325–340 (2016)

12. Costache, A., Curtis, B.R., Hales, E., Murphy, S., Ogilvie, T., Player, R.: On the precision loss in approximate homomorphic encryption pp. 325–345 (2023)
13. Costache, A., Laine, K., Player, R.: Evaluating the effectiveness of heuristic worst-case noise analysis in FHE. In: Computer Security – ESORICS 2020. pp. 546–565 (2020)
14. Costache, A., Nürnberger, L., Player, R.: Optimisations and Tradeoffs for HElib. In: Topics in Cryptology – CT-RSA 2023. pp. 29–53 (2023)
15. Damgård, I., Pastro, V., Smart, N., Zakarias, S.: Multiparty computation from somewhat homomorphic encryption. In: Annual Cryptology Conference. pp. 643–662. Springer (2012)
16. Ducas, L., Micciancio, D.: FHEW: Bootstrapping Homomorphic Encryption in Less Than a Second. In: Oswald, E., Fischlin, M. (eds.) Advances in Cryptology – EUROCRYPT 2015. pp. 617–640. Springer Berlin Heidelberg, Berlin, Heidelberg (2015)
17. Fan, J., Vercauteren, F.: Somewhat practical fully homomorphic encryption. ePrint Archive (2012)
18. Gentry, C.: A fully homomorphic encryption scheme. Stanford university (2009)
19. Gentry, C., Halevi, S., Smart, N.P.: Homomorphic Evaluation of the AES Circuit. In: Advances in Cryptology – CRYPTO 2012. pp. 850–867 (2012)
20. Halevi, S., Shoup, V.: Design and implementation of HElib: a homomorphic encryption library. ePrint Archive (2020)
21. Iliashenko, I.: Optimisations of fully homomorphic encryption. PhD thesis (2019)
22. Kim, A., Polyakov, Y., Zucca, V.: Revisiting homomorphic encryption schemes for finite fields. In: Advances in Cryptology–ASIACRYPT 2021. pp. 608–639 (2021)
23. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Advances in Cryptology – EUROCRYPT 2010. pp. 1–23 (2010)
24. Mono, J., Marcolla, C., Land, G., Güneysu, T., Aaraj, N.: Finding and evaluating parameters for BGV. In: International Conference on Cryptology in Africa. pp. 370–394 (2023)
25. Murphy, S., Player, R.: A central limit approach for ring-LWE noise analysis. IACR Communications in Cryptology **1**(2) (2024)
26. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM (JACM) **56**(6), 1–40 (2009)

A Proof of Lemma 1

In order to prove this lemma, we will first demonstrate that these properties hold for the critical quantity of a fresh ciphertext ν_{clean}.
Then, we will show that any operation involved in the BGV circuit does not affect these properties.

Fresh ciphertexts For ν_{clean}, the coefficients $b_\iota(\mu)$ are defined as

$$\begin{cases} b_0(0) = m + te_0 \\ b_1(0) = tu \end{cases} \qquad \begin{cases} b_0(1) = te_1 \end{cases}$$

Therefore, the first property follows immediately from the independence of $b_{\mu_1}(\iota_1)|_{j_1}, b_{\mu_2}(\iota_2)|_{j_2}$ when $\mu_1 \neq \mu_2$ or $j_1 \neq j_2$.

As for the second property, it holds since
- $\mathbb{E}[b_0(0)|_i] = \mathbb{E}[m|_i] + t\mathbb{E}[e_0|_i] = 0$, due to the linearity of the expected value and the distributions considered, i.e. $m \leftarrow \mathcal{U}_t, e_0 \leftarrow \mathcal{DG}_q(\sigma^2)$;
- $\mathbb{E}[b_1(0)|_i] = t\mathbb{E}[u|_i] = 0$, as $u \leftarrow \chi_s$;
- $\mathbb{E}[b_0(1)|_i] = t\mathbb{E}[e_1|_i] = 0$, as $e_1 \leftarrow \mathcal{DG}_q(\sigma^2)$;

We will therefore show that the remaining homomorphic operations do not alter these properties.

Let $\nu = \sum_{\iota_1}\sum_{\mu_1} b_{\mu_1}(\iota_1)e^{\mu_1}s^{\iota_1}$, $\nu' = \sum_{\iota_2}\sum_{\mu_2} b'_{\mu_2}(\iota_2)e^{\mu_2}s^{\iota_2}$ be the respective critical quantities of two generic ciphertexts, for which the properties stated above are assumed to hold.

Addition of two ciphertexts The critical quantity after the addition of the two BGV ciphertexts is given by

$$\nu_{\text{add}} = \nu + \nu' = \sum_{\iota}\sum_{\mu} b^{\text{add}}_{\mu}(\iota)e^{\mu}s^{\iota},$$

where $b^{\text{add}}_{\mu}(\iota) = b_{\mu}(\iota) + b'_{\mu}(\iota)$.

Therefore, if $\mathbb{E}[b_{\mu}(\iota)|_i] = \mathbb{E}[b'_{\mu}(\iota)|_i] = 0$ then

$$\mathbb{E}[b^{\text{add}}_{\mu}(\iota)|_i] = 0,$$

according to the linearity of the expected value.

Moreover, using the bilinearity of the covariance, we have that, for $\mu_1 \neq \mu_2$ or $j_1 \neq j_2$

$$\mathsf{Cov}(b^{\text{add}}_{\mu_1}(\iota_1)|_{j_1}, b^{\text{add}}_{\mu_2}(\iota_2)|_{j_2}) = 0,$$

since

$$\begin{aligned}\mathsf{Cov}(b_{\mu_1}(\iota_1) + b'_{\mu_1}(\iota_1)|_{j_1}, b_{\mu_2}(\iota_2) + b'_{\mu_2}(\iota_2)|_{j_2}) = {} & \mathsf{Cov}(b_{\mu_1}(\iota_1)|_{j_1}, b_{\mu_2}(\iota_2)|_{j_2}) \\ & + \mathsf{Cov}(b_{\mu_1}(\iota_1)|_{j_1}, b'_{\mu_2}(\iota_2)|_{j_2}) \\ & + \mathsf{Cov}(b'_{\mu_1}(\iota_1)|_{j_1}, b_{\mu_2}(\iota_2)|_{j_2}) \\ & + \mathsf{Cov}(b'_{\mu_1}(\iota_1)|_{j_1}, b'_{\mu_2}(\iota_2)|_{j_2}),\end{aligned}$$

where all the summands vanish because:
- $\mathsf{Cov}(b_{\mu_1}(\iota_1)|_{j_1}, b_{\mu_2}(\iota_2)|_{j_2}) = \mathsf{Cov}(b'_{\mu_1}(\iota_1)|_{j_1}, b'_{\mu_2}(\iota_2)|_{j_2}) = 0$ holds by assumption for $\mu_1 \neq \mu_2$ or $j_1 \neq j_2$;
- $\mathsf{Cov}(b_{\mu_1}(\iota_1)|_{j_1}, b'_{\mu_2}(\iota_2)|_{j_2}) = \mathsf{Cov}(b'_{\mu_1}(\iota_1)|_{j_1}, b_{\mu_2}(\iota_2)|_{j_2}) = 0$ since $b_{\mu_1}(\iota_1)$ and $b'_{\mu_2}(\iota_2)$ are independent $\forall \mu_1, \mu_2$;

Multiplication by a constant Given a ciphertext with $\nu = \sum_\iota \sum_\mu b_\mu(\iota) e^\mu s^\iota$ and a constant α, the critical quantity obtained after their homomorphic multiplication, according to the BGV scheme, is as follows

$$\nu_{\text{const}} = \alpha\nu = \alpha \sum_\iota \sum_\mu b_\mu(\iota) e^\mu s^\iota = \sum_\iota \sum_\mu \alpha b_\mu(\iota) e^\mu s^\iota.$$

Therefore, we can define $b_\mu^{\text{const}}(\iota) = \alpha b_\mu(\iota)$ from which, according to the linearity of the expected value

$$\mathbb{E}[b_\mu^{\text{const}}(\iota)|_i] = \mathbb{E}[\alpha b_\mu(\iota)|_i] = \alpha \mathbb{E}[b_\mu(\iota)|_i] = 0,$$

which proves property b).

Property a) follows directly by assumption from the bilinearity of the covariance

$$\begin{aligned}\mathsf{Cov}(b_{\mu_1}^{\text{const}}(\iota_1)|_{j_1}, b_{\mu_2}^{\text{const}}(\iota_2)|_{j_2}) &= \mathsf{Cov}(\alpha b_{\mu_1}(\iota_1)|_{j_1}, \alpha b_{\mu_2}(\iota_2)|_{j_2}) = \\ &= \alpha^2 \mathsf{Cov}(b_{\mu_1}(\iota_1)|_{j_1}, b_{\mu_2}(\iota_2)|_{j_2}) = 0.\end{aligned}$$

Multiplication of two ciphertexts The critical quantity arising from the multiplication of two ciphertexts, whose associated noise is defined as above, can be expressed as

$$\nu_{\mathsf{mul}} = \nu \cdot \nu' = \sum_\iota a_\iota^{\mathsf{mul}} s^\iota = \sum_\iota \sum_\mu b_\mu^{\mathsf{mul}}(\iota) e^\mu s^\iota,$$

where $a_\iota^{\mathsf{mul}} = \sum_{\iota_1+\iota_2=\iota} a_{\iota_1} a'_{\iota_2}$.

Moreover

$$\begin{cases} a_{\iota_1} = \sum_{\mu_1} b_{\mu_1}(\iota_1) e^{\mu_1} \\ a'_{\iota_2} = \sum_{\mu_2} b'_{\mu_2}(\iota_2) e^{\mu_2} \end{cases}$$

From which it follows that

$$b_\mu^{\mathsf{mul}}(\iota) = \sum_{\iota_1+\iota_2=\iota} \sum_{\mu_1+\mu_2=\mu} b_{\mu_1}(\iota_1) b'_{\mu_2}(\iota_2).$$

From the independence of $b_{\mu_1}(\iota_1)$ and $b'_{\mu_2}(\iota_2)$ $\forall \mu_1, \mu_2, \iota_1, \iota_2$, and for the linearity of the expected value, one can deduce that

$$\begin{aligned}\mathbb{E}[b_\mu^{\mathsf{mul}}(\iota)] &= \sum_{\iota_1+\iota_2=\iota} \sum_{\mu_1+\mu_2=\mu} \mathbb{E}[b_{\mu_1}(\iota_1) b'_{\mu_2}(\iota_2)] \\ &= \sum_{\iota_1+\iota_2=\iota} \sum_{\mu_1+\mu_2=\mu} \mathbb{E}[b_{\mu_1}(\iota_1)] \mathbb{E}[b'_{\mu_2}(\iota_2)] = 0,\end{aligned}$$

which easily proves property b).

The expression of the covariance $\mathsf{Cov}(b^{\mathsf{mul}}_{\mu_1}(\iota_1)|_{i_1}, b^{\mathsf{mul}}_{\mu_2}(\iota_2)|_{i_2})$ can be reduced, using its bilinearity, to a sum of terms of the form

$$\mathsf{Cov}(b_{\mu_1}(\iota_1)|_{l_1} b'_{\mu_2}(\iota_2)|_{i_1-l_1}, b_{\mu_3}(\iota_3)|_{l_2} b'_{\mu_4}(\iota_4)|_{i_2-l_2}),$$

which are all zero, using the property of the covariance stated below.

Property 1. Let X_1, X_2, X_3, X_4 be some fixed random variables.
If X_2, X_4 are independent with respect to X_1, X_3, $\mathsf{Cov}(X_2, X_4) = 0$ and $\mathbb{E}[X_2] = 0$ then

$$\mathsf{Cov}(X_1 \cdot X_2, X_3 \cdot X_4) = 0.$$

Thus, property *a*) follows by observing that, for $\mu_2 \neq \mu_4$ or $i_2 \neq i_4$:
- $\mathsf{Cov}(b'_{\mu_2}(\iota_2)|_{i_1-l_1}, b'_{\mu_4}(\iota_4)|_{i_2-l_2}) = 0$ e $\mathbb{E}[b'_{\mu_2}(\iota_2)|_{i_1-l_1}] = 0$ based on the hypotheses made;
- $b'_{\mu_2}(\iota_2)|_{i_1-l_1}, b'_{\mu_4}(\iota_4)|_{i_2-l_2}$ are independent with respect to $b_{\mu_1}(\iota_1)|_{l_1}, b_{\mu_3}(\iota_3)|_{l_2}$;

Therefore, thanks to the property 1, this implies that

$$\mathsf{Cov}(b_{\mu_1}(\iota_1)|_{l_1} b'_{\mu_2}(\iota_2)|_{i_1-l_1}, b_{\mu_3}(\iota_3)|_{l_2} b'_{\mu_4}(\iota_4)|_{i_2-l_2}) = 0.$$

Modulus and Key Switching Let $\boldsymbol{c} = (c_0, c_1)$ be a ciphertext in $R_{q_l} \times R_{q_l}$ and suppose that the modulus switch to $q_{l'}$ is applied, in order to reduce the error.
The resulting ciphertext is defined as

$$\boldsymbol{c'} = \frac{q_{l'}}{q_l}(\boldsymbol{c} + \boldsymbol{\delta}) \mod q_{l'},$$

where $\boldsymbol{\delta} = t[-\boldsymbol{c}t^{-1}]_{\frac{q_l}{q_{l'}}}$.
The critical quantity associated to $\boldsymbol{c'}$ can be expressed as

$$\nu' = \frac{q_{l'}}{q_l}(\nu + \nu_{\mathsf{ms}}) \quad \text{where} \quad \nu_{\mathsf{ms}} = \delta_0 + \delta_1 s$$

It is possible to observe that the ciphertext components c_0, c_1 can be thought as randomly distributed over R_{q_l}, $c_0, c_1 \leftarrow \mathcal{U}_{q_l}$, and therefore the δ_i can be treated as independent polynomials with coefficients chosen randomly over $I = (-\frac{tq_l}{2q_{l'}}, \frac{tq_l}{2q_{l'}})$, i.e. $\delta_0, \delta_1 \leftarrow \mathcal{U}_I$.
Moreover, it should be noted that the values δ_i exclusively influence $b_0(0), b_0(1)$, and that they have an expected value equal to zero, because of their distributions.
Therefore, referring back to the case of the homomorphic sum, we can deduce that the expected value of $b'_\mu(\iota)$ for the new ciphertext $\boldsymbol{c'}$ remains zero, as do the covariances.
In the same way, by reducing the problem to the case of homomorphic addition, it is possible to show that these properties remain valid also after the relinearization process.
We decided not to report all the technical details but to provide only the key underlying idea, as there are multiple relinearization variants and including them would have required too much space. However, all the calculations can be derived in a very straightforward manner by simply adapting the approach in [2].

B Proof of Lemma 2

In order to prove the statement, we start by writing the term $a_\iota s^\iota|_i$, according to 1, as

$$a_\iota s^\iota|_i = \sum_\mu (b_\mu(\iota) e^\mu s^\iota)|_i = \sum_\mu \sum_{j=0}^{n-1} \xi(i,j) b_\mu(\iota) e^\mu|_j s^\iota|_{i-j}.$$

Recall that, given two random variables X and Y, the following properties hold:

a. $\mathsf{Var}(XY) = (\mathsf{Var}(X) + \mathbb{E}[X]^2)(\mathsf{Var}(Y) + \mathbb{E}[Y]^2) + \mathsf{Cov}(X^2, Y^2)$
$\quad - (\mathsf{Cov}(X,Y) + \mathbb{E}[X]\mathbb{E}[Y])^2$
b. $\mathsf{Var}(X+Y) = \mathsf{Var}(X) + \mathsf{Var}(Y) + 2\mathsf{Cov}(X,Y)$

where the second property can be generalized for k random variables $\{X_i\}_{i=0}^k$ as follows

$$\mathsf{Var}\left(\sum_{i=0}^k X_i\right) = \sum_{i=0}^k \mathsf{Var}(X_i) + \sum_{i_1 \neq i_2} \mathsf{Cov}(X_{i_1}, X_{i_2}).$$

Then, it is possible to compute the variance of $a_\iota s^\iota|_i$ as

$$\mathsf{Var}(a_\iota s^\iota|_i) = \sum_\mu \sum_{j=0}^{n-1} \mathsf{Var}(b_\mu(\iota) e^\mu|_j s^\iota|_{i-j}) + \sum_{\mu_1 \neq \mu_2 \text{ or } j_1 \neq j_2} \xi(i,j_1)\xi(i,j_2)\mathsf{Cov}(b_{\mu_1}(\iota) e^{\mu_1}|_{j_1} s^\iota|_{i-j_1}, b_{\mu_2}(\iota) e^{\mu_2}|_{j_2} s^\iota|_{i-j_2}),$$

where the covariances vanishes based on property 1.
Thus, the following equality holds

$$\mathsf{Var}(a_\iota s^\iota|_i) = \sum_\mu \sum_{j=0}^{n-1} \mathsf{Var}(b_\mu(\iota) e^\mu|_j s^\iota|_{i-j}). \tag{12}$$

Moreover, according to property (a.), it follows that

$$\begin{aligned}\mathsf{Var}(b_\mu(\iota) e^\mu|_j s^\iota|_{i-j}) = {} & (\mathsf{Var}(b_\mu(\iota) e^\mu|_j) + \mathbb{E}[b_\mu(\iota) e^\mu|_j]^2)(\mathsf{Var}(s^\iota|_{i-j}) + \mathbb{E}[s^\iota|_{i-j}]^2) \\ & + \mathsf{Cov}(b_\mu(\iota) e^\mu|_j^2, s^\iota|_{i-j}^2) \\ & - (\mathsf{Cov}(b_\mu(\iota) e^\mu|_j, s^\iota|_{i-j}) + \mathbb{E}[b_\mu(\iota) e^\mu|_j]\mathbb{E}[s^\iota|_{i-j}])^2 .\end{aligned}$$

At this point, it should be noted that
- $\mathbb{E}[b_\mu(\iota) e^\mu|_j] = 0$ according to lemma 1;
- $\mathsf{Cov}(b_\mu(\iota) e^\mu|_j, s^\iota|_{i-j}) = \mathsf{Cov}(b_\mu(\iota) e^\mu|_j^2, s^\iota|_{i-j}^2) = 0$ as $b_\mu(\iota) e^\mu|_j, s^\iota|_{i-j}$ are independent;

This results in

$$\mathsf{Var}(b_\mu(\iota)e^\mu|_j s^\iota|_{i-j}) = \mathsf{Var}(b_\mu(\iota)e^\mu|_j)(\mathsf{Var}(s^\iota|_{i-j}) + \mathbb{E}[s^\iota|_{i-j}]^2).$$

In addition, for a random variable X, it holds that

$$\mathsf{Var}(X) = \mathbb{E}[X^2] - \mathbb{E}[X]^2.$$

Therefore,

$$\mathsf{Var}(b_\mu(\iota)e^\mu|_j s^\iota|_{i-j}) = \mathsf{Var}(b_\mu(\iota)e^\mu|_j)\mathbb{E}[s^\iota|^2_{i-j}]. \tag{13}$$

Finally, the same reasoning can be applied in order to derive

$$\mathsf{Var}(b_\mu(\iota)e^\mu|_j) = \sum_{k=0}^{n-1} \mathsf{Var}(b_\mu(\iota)|_k)\mathbb{E}[e^\mu|^2_{j-k}]. \tag{14}$$

In fact, using (1) and property (b.), it follows that

$$\begin{aligned}\mathsf{Var}(b_\mu(\iota)e^\mu|_j) &= \mathsf{Var}\left(\sum_{k=0}^{n-1} b_\mu(\iota)|_k e^\mu|_{j-k}\right) \\ &= \sum_{k=0}^{n-1} \mathsf{Var}(b_\mu(\iota)|_k e^\mu|_{j-k}) \\ &\quad + \sum_{k_1\neq k_2} \xi(j,k_1)\xi(j,k_2)\mathsf{Cov}(b_\mu(\iota)|_{k_1} e^\mu|_{j-k_1}, b_\mu(\iota)|_{k_2} e^\mu|_{j-k_2}),\end{aligned}$$

where the covariances are null thanks to property 1.
Moreover, according to property (a.), it follows that

$$\begin{aligned}\mathsf{Var}(b_\mu(\iota)|_k e^\mu|_{j-k}) &= (\mathsf{Var}(b_\mu(\iota)|_k) + \mathbb{E}[b_\mu(\iota)|_k]^2)(\mathsf{Var}(e^\mu|_{j-k}) + \mathbb{E}[e^\mu|_{j-k}]^2) \\ &\quad + \mathsf{Cov}(b_\mu(\iota)|^2_k, e^\mu|^2_{j-k}) \\ &\quad - (\mathsf{Cov}(b_\mu(\iota)|_k, e^\mu|_{j-k}) + \mathbb{E}[b_\mu(\iota)|_k]\mathbb{E}[e^\mu|_{j-k}])^2.\end{aligned}$$

Thus, (13) is proven observing that $\mathbb{E}[b_\mu(\iota)|_k] = 0$, according to lemma 1, and that $b_\mu(\iota)|_k$ and $e^\mu|_{j-k}$ are independent.
By substituting (13) and (14) in (12), it follows that

$$\begin{aligned}\mathsf{Var}(a_\iota s^\iota|_i) &= \sum_\mu \sum_{j=0}^{n-1} \mathsf{Var}(b_\mu(\iota)e^\mu|_j s^\iota|_{i-j}) = \sum_\mu \sum_{j=0}^{n-1} \mathsf{Var}(b_\mu(\iota)e^\mu|_j)\mathbb{E}[s^\iota|^2_{i-j}] \\ &= \sum_\mu \sum_{j=0}^{n-1}\sum_{k=0}^{n-1} \mathsf{Var}(b_\mu(\iota)|_k)\mathbb{E}[e^\mu|^2_{j-k}]\mathbb{E}[s^\iota|^2_{i-j}].\end{aligned}$$

Finally, observing that $\mathsf{Var}(b_\mu(\iota)|_i), \mathbb{E}[e^\mu|^2_i]$ and $\mathbb{E}[s^\iota|^2_i]$ do not depend on i, the thesis is demonstrated, i.e.,

$$\mathsf{Var}(a_\iota s^\iota|_i) = \sum_\mu \mathsf{Var}(b_\mu(\iota)|_i) \sum_{k=0}^{n-1} \mathbb{E}[e^\mu|^2_k] \sum_{j=0}^{n-1} \mathbb{E}[s^\iota|^2_j].$$