# Improving and Automating BFV Parameters

## Selection: An Average-Case Approach

June 20, 2023

Beatrice Biasioli, Chiara Marcolla, Marco Calderini, and Johannes Mono

beatrice.biasioli@tii.ae

# Motivation

Cryptography Research Centre

This work arises from the practical need of using Homomorphic Encryption in a team project. We had to face the challenge of parameters selection in (leveled) FHE.

The problem is the noise growth . The error introduced in the encryption phase for security reasons grows as homomorphic operations are performed. In particular, it grows exponentially with multiplications .

To guarantee correctness , we need a large ciphertext modulus . However, a larger modulus also decreases the security level of the underlying scheme, requiring a larger polynomial degree at the cost of efficiency.

Our aim: an effective analysis the noise growth and a consequent a tight bound on the ciphertext modulus for correctness.

# Our Contribution

- We propose an average-case studio for the error growth in the BFV scheme . Our analysis differs from the previously proposed for other schemes in the computation of the homomorphic multiplication variance error, where we introduce a “correcting” function.

- We show how to compute the ciphertext modulus with closed formulas for generic circuits.

- We implemented an interactive tool for the parameter generation, extending the one of *Mono et al.* [13] for BGV. It combines their security formula with our theoretical findings.

---

https://eprint.iacr.org/2023/600.pdf

# Related works

- Recent works introduced the average-case analysis for the error growth for TFHE [4], CKKS [6] and BGV [14, 8].

- The state-of-the-art in establishing theoretical bounds for the BFV scheme relies on the canonical norm [5, 10, 7], which often yields overly conservative bounds.

- Regarding automation of parameters selection, Bergerat *et al.* [3] proposed a framework for efficiently selecting parameters in TFHE-like schemes; Mono *et al.* [13] developed an interactive parameter generator for the leveled BGV scheme that supports arbitrary circuit models.

# Security: the RLWE Problem

Cryptography Research Centre

Let $f(x)$ be a monic irreducible polynomial and $\mathcal{R} = \mathbb{Z}[x]/\langle f(x) \rangle$.
Let $q > 1$ be an integer, we denote $\mathbb{Z}_q = \mathbb{Z} \cap (-q/2, q/2]$ and $\mathcal{R}_q$ the set of polynomials in $\mathcal{R}$ with coefficients in $\mathbb{Z}_q$.
Let $\chi_e$ be an error distribution, usually a discrete Gaussian centered in 0 [1].
Let $\chi_s$ be any distribution.

The **(Decisional) Ring Learning with Errors** problem [12]:

Let $a \in \mathcal{R}_q$ arbitrary, sample $e \leftarrow \chi_e$ and $s \leftarrow \chi_s$ randomly.
The goal is distinguishing pairs $(a, b = [as + e]_q)$ from random ones in $\mathcal{R}_q^2$.

The RLWE problem is presumed to be intractable [15].

# Building a Scheme on top of RLWE: BFV [9, 11]

Cryptography Research Centre

The **(Decisional) Ring Learning with Errors** problem [12]:

Let $a \in \mathcal{R}_q$ arbitrary, sample $e \leftarrow \chi_e$ and $s \leftarrow \chi_s$ randomly.
The goal is distinguishing pairs $(a, b = [as + e]_q)$ from random ones in $\mathcal{R}_q^2$.

Let $f(x) = x^n + 1$ with $n$ a power of 2.
Let $\chi_s$ be a secret distribution, we consider the ternary distribution.

**Key Generation.** Sample $a \leftarrow \mathcal{U}_q$, $s \leftarrow \chi_s$ and $e \leftarrow \chi_e$.
Output sk $= s$ and pk $= (b, a) = ([-as + e]_q, a)$.

Let $t > 1$ be an integer, called plaintext modulus, and $m \in \mathbb{Z}_t$.
**Encryption($\mathrm{m}$, pk).** Sample $e_0, e_1 \leftarrow \chi_e$, $u \leftarrow \chi_s$. Output $\mathfrak{c} = (\mathbf{c}, q)$ with

$$\mathbf{c} = (c_0, c_1) = \left( \left[ \left\lfloor \frac{q}{t} m \right\rceil + bu + e_0 \right]_q, [au + e_1]_q \right).$$

# Correctness

**Key Generation & Encryption($\mathfrak{m}$, pk).** $a \leftarrow \mathcal{U}_q$, $s, u \leftarrow \chi_s$ and $e, e_0, e_1 \leftarrow \chi_e$.

sk $= s$, $b = [-as+e]_q$, $\mathfrak{c} = (\mathbf{c}, q)$, $\mathbf{c} = (c_0, c_1) = \left(\left[\left\lfloor \frac{q}{t} m \right\rceil + bu + e_0\right]_q, [au+e_1]_q\right)$.

**Decryption($\mathfrak{c}$, sk).** Receive $\mathfrak{c} = (\mathbf{c}, q_\ell)$. Output $\left[\left\lfloor \frac{t}{q_\ell}[c_0 + c_1 s]_{q_\ell} \right\rceil\right]_t$.

**Correctness**:

$$\frac{t}{q}[c_0 + c_1 s]_q = \frac{t}{q}\left(\frac{qm}{t} - \frac{[qm]_t}{t} + eu + e_0 + e_1 s + kq\right) = m + \nu_{\text{clean}} + kt$$

for some $k \in \mathcal{R}$ and $\nu_{\text{clean}} = \frac{t}{q}\left(-\frac{[qm]_t}{t} + eu + e_0 + e_1 s\right)$.

The decryption is correct if and only if

$$\left[\left\lfloor \frac{t}{q}[c_0 + c_1 s]_q \right\rceil\right]_t = [m + \lfloor \nu_{\text{clean}} \rceil]_t = m,$$

i.e. when all the coefficients of $\nu_{\text{clean}}$ belong to $(-1/2, 1/2]$.

# Bound on the (Fresh) Error

Cryptography Research Centre

The coefficients of $\nu_{\text{clean}}$ are well-approximated by identically distributed Gaussians with mean $\mathbb{E}[\nu_{\text{clean}}|_i] = 0$ and variance

$$\text{Var}(\nu_{\text{clean}}|_i) \approx \frac{t^2}{q^2}\left(\frac{1}{12} + nV_eV_u + V_e + nV_eV_s\right).$$

For correct decryption with overwhelming probability, we bound the variance $\text{Var}(\nu_{\text{clean}}|_i) \leq \frac{1}{8D^2}$. Indeed,

$$\mathbb{P}\big(\nu_{\text{clean}}|_i \in (-1/2, 1/2]\ \forall i\big) \geq 1 - n(1 - \text{erf}(D)).$$

Usually $D = 6$, for $n = 2^{13}$, $n(1 - \text{erf}(D)) = 2^{-42}$.

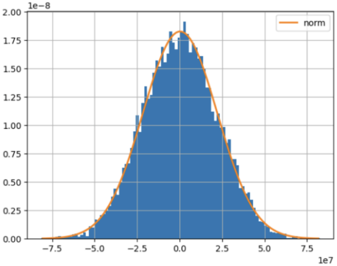



Figure 0.1: $\text{ks}_{\text{pval}} = 0.5889 \geq 0.05$.

# Characterization of the error

The important characteristics of $\nu_{\text{clean}}$ hold also after the performing of homomorphic operation. Let the **invariant noise** [10] be the “minimal" $\nu \in \mathbb{Q}[x]/\langle f(x)\rangle$ such that

$$\frac{t}{q_\ell}[c_0 + c_1 s]_{q_\ell} = m + \nu + kt$$

for some $k \in \mathcal{R}$. Then,

- its coefficients are well-approximated by identical distributed Gaussians with mean $\mathbb{E}[\nu|_i] = 0$. Thus, the same probabilistic bound holds if $\text{Var}(\nu|_i) \leq \frac{1}{8D^2}$.
- we can always write $\nu = \sum_\iota a_\iota s^\iota$ such that $\text{Var}(\nu|_i) = \sum_\iota \sum_{j=0}^{n-1} \text{Var}(a_\iota|_j) s^\iota|_{i-j}^2$.

In the following, we show how do $\nu$ and $\text{Var}(\nu|_i)$ change depending on the main operations, without going into the details.

# Additions & Modulo Switch

Cryptography Research Centre

Let $\nu = \sum_{\iota_1} a_{\iota_1} s^{\iota_1}$, $\nu' = \sum_{\iota_2} a'_{\iota_2} s^{\iota_2}$ be the noises of two ciphertexts $\mathfrak{c}$, $\mathfrak{c}'$ computed independently.

Note that $s$ is seen as a fixed vector, whose coefficients have zero mean and variance $V_s$. Hence, the errors are independent.

**Addition($\mathfrak{c}$, $\mathfrak{c}'$).** The error resulting from the addition is $\nu + \nu'$ and its coefficients variance is

$$\mathsf{Var}(\nu|_i) + \mathsf{Var}(\nu'|_i).$$

**ModSwitch($\mathfrak{c}$, $q'_\ell$).** The resulting error is $\nu + \nu_{\mathsf{ms}}(q'_\ell)$ with $\nu_{\mathsf{ms}}(q'_\ell)$ independent of $\nu$, then the variance is $\mathsf{Var}(\nu|_i) + V_{\mathsf{ms}}(q'_\ell)$ and, in particular,

$$\mathsf{Var}(\nu|_i) + \frac{B_{\mathsf{ms}}}{q'_\ell}.$$

# Multiplication [9, 11]



Let $\nu = \sum_{\iota_1=0}^{T_1} a_{\iota_1} s^{\iota_1}$, $\nu' = \sum_{\iota_2=0}^{T_2} a'_{\iota_2} s^{\iota_2}$ be the noises of two ciphertexts $\mathfrak{c}$, $\mathfrak{c}'$ computed independently with modulus $q_\ell, q'_\ell$, respectively, and $q_\ell \approx q'_\ell$.

**Multiplication($\mathfrak{c}$,$\mathfrak{c}'$).** The error becomes
$\nu_{\mathsf{mul}}(q_\ell) = -\nu\nu' + \nu\frac{t}{q'_\ell}(c'_0 + c'_1 s) + \nu'\frac{t}{q_\ell}(c_0 + c_1 s) + \frac{t}{q_\ell}(\varepsilon_0 + \varepsilon_1 s + \varepsilon_2 s^2)$.

Initially, we assumed the coefficients of each polynomials are independent among each others, obtaining

$$\begin{aligned}\mathsf{Var}(\nu_{\mathsf{mul}}(q_\ell)|_i) =& n\mathsf{Var}(\nu|_i)\mathsf{Var}(\nu'|_i) + n\mathsf{Var}(\nu|_i)\frac{t^2}{12}(1+nV_s)+\\ &+ n\mathsf{Var}(\nu'|_i)\frac{t^2}{12}(1+nV_s) + \mathsf{Var}\Big(\frac{t}{q_\ell}(\varepsilon_0 + \varepsilon_1 s + \varepsilon_2 s^2)|_i\Big).\end{aligned}$$

However, we discovered that the result was an understimation.

# The worst you will see today!

Cryptography Research Centre

Let $\nu = \sum_{\iota_1=0}^{T_1} a_{\iota_1} s^{\iota_1}$, $\nu' = \sum_{\iota_2=0}^{T_2} a'_{\iota_2} s^{\iota_2}$, then

$$\mathsf{Var}(\nu_{\mathsf{mul}}(q_\ell)|_i) = n \sum_{\iota_1} \sum_{\iota_2} \mathsf{Var}(a_{\iota_1}|_i)\mathsf{Var}(a'_{\iota_2}|_i) \sum_{j=0}^{n-1} s^{\iota_1+\iota_2}|_{i-j}^2 + \ldots$$

While what we obtained from the previous formula, $n\mathsf{Var}(\nu|_i)\mathsf{Var}(\nu'|_i) + \ldots$, is

$$n \sum_{\iota_1} \sum_{\iota_2} \mathsf{Var}(a_{\iota_1}|_i)\mathsf{Var}(a'_{\iota_2}|_i) \sum_{j_1=0}^{n-1} s^{\iota_1}|_{i-j_1}^2 \sum_{j_2=0}^{n-1} s^{\iota_2}|_{i-j_2}^2 + \ldots$$

We want to estimate the ratio

$$\frac{\sum_{j=0}^{n-1} s^{\iota_1+\iota_2}|_{i-j}^2}{\sum_{j_1=0}^{n-1} s^{\iota_1}|_{i-j_1}^2 \sum_{j_2=0}^{n-1} s^{\iota_2}|_{i-j_2}^2}$$

to get $\mathsf{Var}(\nu_{\mathsf{mul}}(q_\ell)|_i)$ from the simplified formula.

# The "correcting" function f

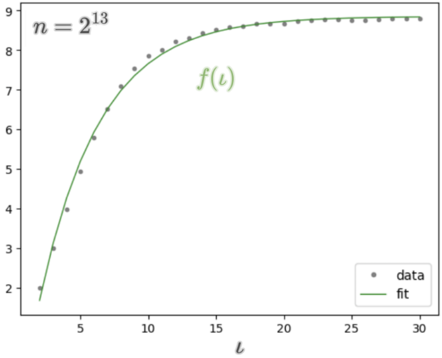
We start analyzing computationally the average value of the particular case

$$\frac{\sum_{i=0}^{n-1} s^{\iota}|_i^2}{\sum_{i_1=0}^{n-1} s|_{i_1}^2 \sum_{i_2=0}^{n-1} s^{\iota-1}|_{i_2}^2},$$

for $\iota \geq 2$. It is well-approximated by the function

$$f(\iota) = -\frac{1}{e^{a\iota-b}} + c,$$

where $a, b, c$ depend only on the ring dimension $n$ and are computed with Python function *curve_fit*.




For $n = 2^{13}$, $a = 0.2240$, $b = 2.4181$ and $c = 8.8510$.

# Variance estimation exploiting $f$

We define $g(\iota) = \prod_{i=0}^{\iota} f(i)$. It can be proven by induction that, for $\iota \geq 1$,

$$\sum_{i=0}^{n-1} s^{\iota}|_i^2 \approx (nV_s)^{\iota} g(\iota).$$

It follows that

$$\mathsf{Var}(\nu_{\mathsf{mul}}(q_\ell)|_i) = n \sum_{\iota_1} \sum_{\iota_2} \mathsf{Var}(a_{\iota_1}|_i)\mathsf{Var}(a'_{\iota_2}|_i) \sum_{j=0}^{n-1} s^{\iota_1+\iota_2}|_{i-j}^2 + \dots$$

can be approximated by

$$n \sum_{\iota_1} \sum_{\iota_2} \mathsf{Var}(a_{\iota_1}|_i)\mathsf{Var}(a'_{\iota_2}|_i) \sum_{j_1=0}^{n-1} s^{\iota_1}|_{i-j_1}^2 \sum_{j_2=0}^{n-1} s^{\iota_2}|_{i-j_2}^2 \frac{g(\iota_1+\iota_2)}{g(\iota_1)g(\iota_2)} + \dots$$

# Bound on $g$

By monotonicity of $f$, we can prove that $\frac{g(\iota_1+\iota_2)}{g(\iota_1)g(\iota_2)} \leq \frac{g(T_1+T_2)}{g(T_1)g(T_2)}$. Therefore

$$\mathsf{Var}(\nu_{\mathsf{mul}}(q_\ell)|_i) \approx n \sum_{\iota_1} \sum_{\iota_2} \mathsf{Var}(a_{\iota_1}|_i)\mathsf{Var}(a'_{\iota_2}|_i) \sum_{j_1=0}^{n-1} s^{\iota_1}|_{i-j_1}^2 \sum_{j_2=0}^{n-1} s^{\iota_2}|_{i-j_2}^2 \frac{g(\iota_1+\iota_2)}{g(\iota_1)g(\iota_2)} + \dots$$

$$\leq n\mathsf{Var}(\nu|_i)\mathsf{Var}(\nu'|_i)\frac{g(T_1+T_2)}{g(T_1)g(T_2)} + \dots$$

Then

$$\mathsf{Var}(\nu_{\mathsf{mul}}(q_\ell)|_i) \leq n\mathsf{Var}(\nu|_i)\mathsf{Var}(\nu'|_i)\frac{g(T_1+T_2)}{g(T_1)g(T_2)} + n\mathsf{Var}(\nu|_i)\frac{t^2}{12}\big(1 + nV_s f(T_1+1)\big) +$$
$$+ n\mathsf{Var}(\nu'|_i)\frac{t^2}{12}\big(1 + nV_s f(T_2+1)\big) + \frac{t^2}{12q_\ell^2}\big(1 + nV_s + (nV_s)^2 f(2)\big).$$

# Closed formulas for Base Circuit

Cryptography Research Centre

Finally, the first and last terms are negligible, then

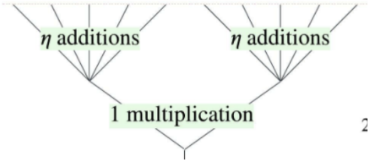
$$\mathsf{Var}(\nu_{\mathsf{mul}}|_i) \approx \frac{t^2 n^2 V_s}{12}\left(\mathsf{Var}(\nu|_i) f(T_1+1) + \mathsf{Var}(\nu'|_i) f(T_2+1)\right).$$

**Base Circuit:**

$$V_\ell \approx \frac{t^2 n^2 V_s}{12}\left(2\eta V_{\ell-1} + V_{\mathsf{ms}}\right) f(\ell+1)$$
$$\approx (AV_{\ell-1} + C) f(\ell+1)$$

$$V_{L-1} \approx \frac{A^{L-2}(AB_{\mathsf{clean}} + C) g(L)}{q^2} < 1/8D^2$$

$$q^2 \geq 8D^2 A^{L-2}(AB_{\mathsf{clean}} + C) g(L)$$



# Results - Single Functions

Cryptography Research Centre

We compare encryption, addition and multiplication of fresh ciphertexts through the noise budget, [16]

$$-\log_2(2\cdot||\nu||) = \log_2\left(\tfrac{1}{2}\right) - \log_2(||\nu||).$$

| | Encryption | | | | Addition | | | | Multiplication | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | maximum value | | | mean | maximum value | | | mean | maximum value | | | mean |
| $n$ | can | our | exp | exp | can | our | exp | exp | can | our | exp | exp |
| $2^{12}$ | 26.5 | 32.0 | 32.7 | 35.4 | 86.0 | 91.5 | 92.1 | 94.9 | 57.0 | 65.1 | 65.9 | 68.7 |
| $2^{13}$ | 25.5 | 31.5 | 32.2 | 34.9 | 85.0 | 91.0 | 91.6 | 94.4 | 55.0 | 63.6 | 64.3 | 66.2 |
| $2^{14}$ | 24.5 | 31.0 | 31.5 | 34.4 | 84.0 | 90.5 | 91.1 | 93.9 | 53.0 | 62.1 | 62.8 | 65.7 |
| $2^{15}$ | 23.5 | 30.5 | 31.0 | 33.9 | 83.0 | 90.0 | 90.5 | 93.4 | 51.0 | 60.6 | 61.2 | 64.2 |

# Results - Base circuits

We consider Base circuits of depth 2 and 3, taking $\eta = 8$.

| | 2 multiplications | | | | | 3 multiplications | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | maximum value | | | mean value | | maximum value | | | mean value | |
| $n$ | can | our | exp | our | exp | can | our | exp | our | exp |
| $2^{12}$ | 21.5 | 35.0 | 35.9 | 38.1 | 38.6 | - | - | - | - | - |
| $2^{13}$ | 18.5 | 32.5 | 33.6 | 35.6 | 36.1 | 45.0 | 62.5 | 63.6 | 65.6 | 66.3 |
| $2^{14}$ | 15.5 | 30.0 | 30.9 | 33.1 | 33.6 | 41.0 | 59.1 | 60.1 | 62.2 | 62.7 |
| $2^{15}$ | 12.5 | 27.6 | 28.4 | 30.7 | 31.1 | 37.0 | 55.6 | 56.4 | 58.7 | 59.2 |

# Results - Ciphertext

We compare the resulting bound on the ciphertext modulus.

| $n$ | $2^{12}$ | $2^{13}$ | $2^{14}$ | $2^{15}$ |
|---|---|---|---|---|
| can | 75.0 | 79.0 | 83.0 | 87.0 |
| our | 56.7 | 60.2 | 63.7 | 67.2 |

Table 1: Comparison of $\log_2(q)$ in the Base Model circuit of depth 3 and $\eta = 8$.

# Parameter Generator

To make our work more valuable and approachable for practical purposes, we provide automated parameter generation implemented in Python and publicly available on GitHub [1]. We integrated our theoretical work for the BFV scheme in the tool of Mono[13]. The generator interactively prompts the user with a list of required and optional inputs, then outputs code snippets with the obtained parameters for multiple state-of-the-art libraries.

[1] `https://github.com/Crypto-TII/fhegen`

. . . Thank you!

# References I

[1] Martin R Albrecht, Melissa Chase, Hao Chen, Jintai Ding, Shafi Goldwasser, Sergey Gorbunov, Shai Halevi, Jeffrey Hoffstein, Kim Laine, Kristin Lauter, Satya Lokam, Daniele Micciancio, Dustin Moody, Travis Morrison, Amit Sahai, and Vinod Vaikuntanathan. Homomorphic encryption security standard. Technical report, `HomomorphicEncryption.org`, Toronto, Canada, November 2018.

[2] Martin R Albrecht, Benjamin R Curtis, Amit Deo, Alex Davidson, Rachel Player, Eamonn W Postlethwaite, Fernando Virdia, and Thomas Wunderer. Estimate all the { LWE, NTRU } schemes! In *International Conference on Security and Cryptography for Networks*, pages 351–367. Springer, 2018.

[3] Loris Bergerat, Anas Boudi, Quentin Bourgerie, Ilaria Chillotti, Damien Ligier, Jean-Baptiste Orfila, and Samuel Tap. Parameter Optimization & Larger Precision for (T) FHE. *Cryptology ePrint Archive*, 2022.

# References II

Cryptography Research Centre


[4] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In *international conference on the theory and application of cryptology and information security*, pages 3–33. Springer, 2016.

[5] Ana Costache and Nigel P Smart. Which ring based somewhat homomorphic encryption scheme is best? In *Cryptographers' Track at the RSA Conference*, pages 325–340. Springer, 2016.

[6] Anamaria Costache, Benjamin R Curtis, Erin Hales, Sean Murphy, Tabitha Ogilvie, and Rachel Player. On the precision loss in approximate homomorphic encryption. *Cryptology ePrint Archive*, 2022.

[7] Anamaria Costache, Kim Laine, and Rachel Player. Evaluating the effectiveness of heuristic worst-case noise analysis in FHE. In *European Symposium on Research in Computer Security*, pages 546–565. Springer, 2020.

# References III


[8] Anamaria Costache, Lea Nürnberger, and Rachel Player. Optimisations and tradeoffs for helib. In *Topics in Cryptology–CT-RSA 2023: Cryptographers' Track at the RSA Conference 2023, San Francisco, CA, USA, April 24–27, 2023, Proceedings*, pages 29–53. Springer, 2023.

[9] Junfeng Fan and Frederik Vercauteren. Somewhat practical fully homomorphic encryption. *IACR Cryptology ePrint Archive*, 2012.

[10] Ilia Iliashenko. Optimisations of fully homomorphic encryption. PhD thesis, 2019.

[11] Andrey Kim, Yuriy Polyakov, and Vincent Zucca. Revisiting homomorphic encryption schemes for finite fields, 2021.

[12] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, pages 1–23, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

# References IV

Cryptography Research Centre


[13] Johannes Mono, Chiara Marcolla, Georg Land, Tim Güneysu, and Najwa Aaraj. Finding and Evaluating Parameters for BGV. *Africacrypt*, 2023.

[14] Sean Murphy and Rachel Player. A central limit approach for ring-lwe noise analysis.

[15] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*, pages 84–93, 2005.

[16] Microsoft SEAL (release 3.4). `https://github.com/Microsoft/SEAL`, October 2019. Microsoft Research, Redmond, WA.

Technology Innovation Institute

Cryptography Research Centre

tii.ae