Revisiting Multivariate Lattices for Encrypted Signal Processing

Alberto Pedrouzo-Ulloa
University of Vigo, Vigo, Spain
apedrouzo@gts.uvigo.es

Juan R. Troncoso-Pastoriza
EPFL, Lausanne, Switzerland
juan.troncoso-pastoriza.epfl.ch

Fernando Pérez-González
University of Vigo, Vigo, Spain
fperez@gts.uvigo.es

ABSTRACT

Multimedia contents are inherently sensitive signals that must be protected when processed in untrusted environments. The field of Secure Signal Processing addresses this challenge by developing methods which enable operating with sensitive signals in a privacy-conscious way. Recently, we introduced a hard lattice problem called m-RLWE (multivariate Ring Learning with Errors) which gives support to efficient encrypted processing of multidimensional signals. Afterwards, Bootland *et al.* presented an attack to m-RLWE that reduces the security of the underlying scheme from a lattice with dimension $\prod_i n_i$ to $\max\{n_i\}_i$. Our work introduces a new pre-/post-coding block that addresses this attack and achieves the efficient results of our initial approach while basing its security directly on RLWE with dimension $\prod_i n_i$, hence preserving the security and efficiency originally claimed. Additionally, this work provides a detailed comparison between a conventional use of RLWE, m-RLWE and our new pre-/post-coding procedure, which we denote "packed"-RLWE. Finally, we discuss a set of encrypted signal processing applications which clearly benefit from the proposed framework, either alone or in a combination of baseline RLWE, m-RLWE and "packed"-RLWE.

KEYWORDS

Secure Signal Processing, Lattice-based Cryptography, Homomorphic Encryption, Multidimensional Signal Processing

ACM Reference Format:
Alberto Pedrouzo-Ulloa, Juan R. Troncoso-Pastoriza, and Fernando Pérez-González. 2019. Revisiting Multivariate Lattices for Encrypted Signal Processing. In *ACM Information Hiding and Multimedia Security Workshop (IH&MMSec '19), July 3–5, 2019, Paris, France.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3335203.3335730

GPSC is funded by the Agencia Estatal de Investigación (Spain) and the European Regional Development Fund (ERDF) under projects WINTER (TEC2016-76409-C2-2-R) and COMONSENS (TEC2015-69648-REDC). Also funded by the Xunta de Galicia and the European Union (European Regional Development Fund - ERDF) under projects Agrupación Estratéxica Consolidada de Galicia accreditation 2016-2019 and Grupo de Referencia ED431C2017/53, and also by the FPI grant (BES-2014-069018). EPFL is funded in part by the grant #2017-201 (DPPH) of the Swiss PHRT and by the grant #2018-522 (MedCo) of the Swiss PHRT and SPHN. We would like to thank Jean-Claude Bajard, Julien Eynard, M. Anwar Hasan and Vincent Zucca for providing us with their RNS implementation of the FV cryptosystem.

IH&MMSec '19, July 3–5, 2019, Paris, France

ACM ISBN 978-1-4503-6821-6/19/06…$15.00
https://doi.org/10.1145/3335203.3335730

1 INTRODUCTION

Signal processing has become ubiquitous in our daily lives; encompassing communication and entertainment technologies, from speech and audio processing to image and video analysis, with a strong impact on emerging applications such as smart grids, autonomous driving and analysis of medical signals, among others.

Many of these applications deal with very sensitive signals, whose information cannot be leaked to non-authorized users. This is the context where Secure Signal Processing (SSP) [21] was born, as a marriage between applied cryptography and signal processing aiming at solutions that can protect the content of the involved signals in an efficient way. Since then, numerous applications have been proposed, many of them based on the use of homomorphic encryption, and specifically, the additively homomorphic Paillier cryptosytem [27], covering the encrypted realization of linear transforms and typical signal processing primitives [8, 37].

However, approaches based on Paillier present two serious limitations: (a) high overhead and cipher expansion, even when mitigated by packing and unpacking techniques [7, 35]; and (b) they require the involvement of the client (secret key holder) engaging in interactive protocols with the outsourced party [36].

Due to this lack of flexibility, lattice cryptosystems (which present a ring homomorphism) are being progressively adopted by researchers in the field [2, 3, 16, 19, 34]. In particular, cryptosystems based on RLWE (Ring Learning with Errors) present a clear advantage when dealing with signals, as its underlying polynomial structure allows for very efficient filtering and convolution operations [33]; hence, most of the applications involving correlations and filtering can benefit from recent RLWE-based schemes, which keep constantly evolving [11, 12, 14].

Nevertheless, applications working with images or higher dimensional signals are much more demanding. One example is multimedia forensics, which deals with high volumes of signals with an inherent multidimensional structure [23]. For this scenario, several solutions have been proposed to adapt the structure of RLWE cryptosystems for efficiently dealing with this multi-dimensionality [29, 30, 32]. These works propose a generalization of RLWE called multivariate RLWE (m-RLWE), and their results show improved efficiency/space tradeoffs. Actually, the authors of [32] show the flexibility of these structures and their advantages in several conventional signal processing operations, such as block-processing and multidimensional convolutions/transforms. These schemes have been used in even more complex applications inside the field of multimedia forensics, namely camera attribution in the encrypted domain [28].

Recently, Bootland *et al.* [9] introduced an attack that reduces the security of schemes based on m-RLWE. This attack has important consequences on the validity of the results presented in [29, 30, 32] and a careful analysis is needed to correctly reevaluate the security of these schemes.

This work carries out this analysis and recalculates the correct security estimates for m-RLWE applications in light of this new attack. Additionally, we introduce a novel pre-/post-coding paradigm for RLWE cryptosystems, which we denote "packed"-RLWE, that preserves all the security properties of previous works based on m-RLWE, but now basing their security directly on RLWE, which is not affected by Bootland's attack.

We also provide an extensive comparison between a conventional use of an RLWE cryptosystem (baseline RLWE), an m-RLWE cryptosystem and an RLWE cryptosystem equipped with our proposed pre-/post-coding. For the sake of clarity and space, we focus on applications based on multidimensional filtering, but all the solutions previously presented for m-RLWE can be adapted to our new packed-RLWE. Finally, we analyze the optimal combination of the three approaches, baseline RLWE, m-RLWE and packed-RLWE, depending on the efficiency/space trade-offs required by the target application.

1.1 Main Contributions

This work features the following contributions:

- We revisit the security analysis of previous m-RLWE cryptosystems in light of the recent attack introduced in [9].
- We survey the best existing algorithms to homomorphically evaluate multidimensional convolutions with an RLWE cryptosystem (denoted as baseline RLWE), noting that some of the best solutions in one dimension (as the use of FFT algorithms) result in a much worse performance in a multidimensional setting, due to the increase of the circuit depth.
- We propose a new pre-/post-coding paradigm over RLWE cryptosystems (we denote it packed-RLWE), that directly "emulates" multidimensional convolutions over the encrypted signals, and comprises very efficient element-wise products and FFT operations on the plaintext ring.
- We show how previous solutions based on m-RLWE can be adapted to our packed-RLWE version, hence getting all the advantages of these structures while still preserving the high security of a lattice with dimension equal to the full length of the involved signals.
- We provide an extensive comparison between a baseline RLWE, an m-RLWE based solution (with non-"coprime" modular functions, which is a "worst-case" for security) and our packed-RLWE proposal. Our results show that m-RLWE and packed-RLWE still outperform those results of baseline RLWE.
- We briefly discuss how the three approaches can be combined to fit the specific requirements of a real application, optimizing the space/efficiency trade-offs. Additionally, we describe several practical applications which can greatly benefit from the use of these tools.

1.2 Notation and Structure

Vectors and matrices are represented by boldface lowercase and uppercase letters, respectively. Polynomials are denoted with regular lowercase letters and the polynomial variable is ignored whenever there is no ambiguity (e.g., a instead of $a(z)$). For the sake of clarity, we indicate the variable(s) of polynomial rings: $R_q[z]=\mathbb{Z}_q[z]/(f(z))$ denotes the polynomial ring in the variable z modulo $f(z)$ with coefficients belonging to $\mathbb{Z}_q$. In general, $R_q[z_1,...,z_l]$ (resp. $R[z_1,...,z_l]$) represents the corresponding multivariate polynomial ring with coefficients in $\mathbb{Z}_q$ (resp. $\mathbb{Z}$) and the l modular functions $f_i(z_i)$ with $1\leq i\leq l$. We also represent polynomials as column vectors of their coefficients $\boldsymbol{a}$. Finally $\boldsymbol{a}\circ\boldsymbol{b}$ is the Hadamard product between vectors, and $\boldsymbol{a}\circledast\boldsymbol{b}$ (resp. $\boldsymbol{a}*\boldsymbol{b}$) is the circular (resp. linear) convolution.

The rest of the paper is organized as follows: in Section 2, we briefly revisit the used RLWE-based cryptosystems, their security and the use of NTT/INTT transforms. Section 3 includes a description of the different approaches for both baseline and multivariate RLWE solutions. We introduce the main contribution of this work in Section 4, comprising our new pre-/post-coding blocks for packed-RLWE. Section 5 includes an extensive comparison between the different proposed approaches in terms of security, efficiency and cipher expansion. Finally, we discuss a set of example encrypted applications that greatly benefit from our solutions in Section 6.

2 PRELIMINARIES

In this section, we revisit the RLWE problem and RLWE-based cryptosystems, together with their multivariate RLWE counterparts. We also summarize the recent attack [9] to multivariate RLWE and detail its effects on the choice of security parameters. Finally, we briefly revisit the use of Number Theoretic Transforms (NTTs).

2.1 Multivariate RLWE problem

Firstly, we include an informal definition of the multivariate RLWE problem as is stated in [32]. We focus on the most widespread case where the modular functions are cyclotomic polynomials of power-of-two order, i.e., $f_i(z_i)=z_i^{n_i}+1$ with n_i a power-of-two. Additionally, this general definition allows us to also cover the RLWE problem as a particular case when the number of dimensions is one (i.e. $l=1$).

Definition 1 (multivariate RLWE problem [29, 31, 32]). *Given a polynomial ring $R_q[z_1,...,z_l]=\mathbb{Z}_q[z_1,...,z_l]/(z_1^{n_1}+1,...,z_l^{n_l}+1)$ and an error distribution $\chi[z_1,...,z_l]\in R_q[z_1,...,z_l]$ that generates small-norm random polynomials in $R_q[z_1,...,z_l]$, m-RLWE relies upon the computational indistinguishability between samples $(a_i,b_i=a_is+e_i)$ and (a_i,u_i), where $a_i,u_i\leftarrow R_q[z_1,...,z_l]$ are chosen uniformly at random, whereas $s,e_i\leftarrow\chi[z_1,...,z_l]$ are drawn from the error distribution.*

Remark. For cyclotomic modular functions $\{\phi_{m_1}(z_1),...,\phi_{m_l}(z_l)\}$ where $\gcd(m_1,...,m_l)=1$, m-RLWE is isomorphic to RLWE with modular function $\phi_{\prod_i m_i}(z)$ [22]. Unfortunately, this is not the case for the version stated in Definition 1, and the security of m-RLWE is highly dependent on the form of the different modular functions (see Section 2.3).

2.2 An ($m-$)RLWE based Cryptosystem

We instantiate univariate and multivariate versions of the FV cryptosystem [18] as examples for our proposed schemes (see Sections 3 and 4) and our performance comparisons (see Section 5), but the results are generalizable to other cryptosystems such as BGV and CKKS [10, 14]. Due to space constraints, we do not include here a description of all the cryptosystem primitives (we refer to [18] for a detailed description). Instead, we summarize the cryptosystems' properties relevant to our analysis.

The plaintext elements belong to the ring $R_t[z_1,...,z_l]$, and ciphertexts are composed of (at least) two polynomial elements belonging

to $R_q[z_1,\ldots,z_l]$. The security of the scheme relies on the indistinguishability assumption of the m-RLWE problem (see Definition 1), which reduces to RLWE when $l=1$.

2.2.1 Cipher expansion. In FV, we can use the following noise bound (Theorem 1 in [18]) when evaluating an arithmetic circuit of multiplicative depth L

$$4\delta_R^L(\delta_R+1.25)^{L+1}\cdot t^{L-1} < \left\lfloor \frac{q}{B} \right\rfloor, \tag{1}$$

where $\delta_R = \prod_i n_i$ is the ring expansion ratio, q is the modulo of the ciphertext ring R_q, t is the modulo of the plaintext ring R_t, and $||\chi|| < B$, that is, χ is a B-bounded distribution of variance σ^2.

2.2.2 RLWE in secure signal processing. The use of an RLWE-based cryptosystem brings about two main advantages in secure signal processing: (a) its security is highly dependent on the length of the involved polynomials, which directly impacts the cipher expansion if the input data cannot be fully packed; practical signals are usually long sequences, such that they can be encrypted in only one encryption; this helps in increasing the security of the underlying RLWE-based cryptosystem without significantly increasing its expansion; (b) homomorphic properties of the cryptosystem translate into addition and multiplication of plaintext polynomials, which represent signal addition and convolution (filtering), the basic blocks required in any signal processing application.

2.3 Security of multivariate RLWE

The original formulation of multivariate RLWE [29, 32] assumes that the m-RLWE problem (Definition 1) in dimension $n=\prod_{i=1}^{l} n_i$ is as hard as the RLWE problem in dimension n. However, in [9] Bootland *et al.* introduce an attack on m-RLWE; this attack exploits the fact that some of the modular functions enable repeated "low-norm" roots in the multivariate ring. As a result, when common roots exist, this attack is able to factor the m-RLWE samples into RLWE samples of smaller dimension, hence reducing the security of these m-RLWE samples to that of solving a set of independent RLWE samples of the maximum individual degree $\max\{n_i\}_i$.

This attack is specially relevant for m-RLWE samples $(a_i, b_i = a_i s + t e_i)$ chosen as in Definition 1, where all the modular functions introduce common roots.[1]

Next, we exemplify the attack on the bivariate RLWE problem, but it can be recursively applied when attacking higher-dimensional ($l>2$) cases.

2.3.1 An attack to multivariate RLWE. Following Definition 1, consider a bivariate RLWE (2-RLWE) sample $(a, b=as+e) \in R_q^2[x,y]$ and $R_q[x,y] = \mathbb{Z}_q[x,y]/(x^{n_x}+1, y^{n_y}+1)$ with $n_x \geq n_y$ and $k=\frac{n_x}{n_y} \in \mathbb{Z}$ without loss of generality.

Now we define the map

$$\begin{aligned}\tilde{\Theta}: \mathbb{Z}_q[x,y]/(x^{n_x}+1, y^{n_y}+1) &\to \left(\mathbb{Z}_q[x]/(x^{n_x}+1)\right)^{n_y} \\ a(x,y) &\to \left(a(x,x^k), a(x,x^{3k}), \ldots, a(x,x^{(2n_y-1)k})\right).\end{aligned}$$

The map $\tilde{\Theta}$ is a ring homomorphism, and if q is odd it is also invertible (see [9]). This allows to transform the pair $(a,b) \in R_q[x,y]$ into $(\tilde{\Theta}(a), \tilde{\Theta}(b)) \in R_q^{n_y}[x]$. If we denote each of the different components in $\tilde{\Theta}$ by $\tilde{\Theta}_i$, for $i=1,\ldots,n_y$, we have

$$\left(\tilde{\Theta}_i(a), \tilde{\Theta}_i(b) = \tilde{\Theta}_i(a)\tilde{\Theta}_i(s) + \tilde{\Theta}_i(e)\right) \in R_q^2[x], i=1,\ldots n_y. \tag{2}$$

That is, n_y different RLWE samples of dimension n_x, whose noise has a variance n_y times higher than the original 2-RLWE sample (as the result of adding n_y independent noise samples).

The attack then tries to break each of the obtained n_y RLWE samples. Once this is done, if the map is invertible, the original secret key can be reconstructed with the different n_y smaller keys.

This attack can be generalized to an m-RLWE sample (Definition 1) with l dimensions, by recursively applying "versions" of this map a total of $l-1$ times. We assume, without loss of generality, that $n_1 \leq n_2 \leq \ldots \leq n_l$); the attack then converts a sample from m-RLWE into $\frac{n}{n_l}$ RLWE samples with cyclotomic degree n_l and a variance $\frac{n}{n_l}$ times higher.

2.4 Number Theoretic Transforms

Discrete Fourier Transforms (DFTs) are widely used in signal processing due to their frequency physical interpretation and the circular convolution theorem which enables efficient convolutions by means of FFT algorithms (e.g., radix-2 or radix-4). However, DFTs are defined on the complex field, while RLWE-based cryptosystems are naturally defined in finite rings. A direct use of DFTs requires rounding the complex roots of unity, which introduces quantization errors.

Number Theoretic Transforms (NTTs) solve this problem, preserving the properties of a Fourier transform on a finite ring and working entirely with integer arithmetic, but they do not always exist. Consider a ring $\mathbb{Z}_p$ where $p=\prod_{i=1}^{k} p_i^{l_i}$, an NTT of size N can be defined if the following properties hold [26]:

- There exists an N-th root of unity α in $\mathbb{Z}_p$ satisfying $\gcd(\alpha,p) = \gcd(N,p) = 1$.
- N divides $\gcd(p_1-1,\ldots,p_k-1)$.

The expressions for the forward and inverse transforms are

$$\begin{aligned}\tilde{x}[k] &= \sum_{l=0}^{N-1} x[l]\alpha^{lk} \mod p, k=0,\ldots,N-1 \\ x[l] &= N^{-1}\sum_{k=0}^{N-1} \tilde{x}[k]\alpha^{-lk} \mod p, l=0,\ldots,N-1\end{aligned}$$

Analogously, we can see NTT/INTT transforms as matrix multiplications

$$\tilde{\boldsymbol{x}} = \boldsymbol{W}\boldsymbol{x}, \quad \text{and} \quad \boldsymbol{x} = \boldsymbol{W}^{-1}\tilde{\boldsymbol{x}}, \tag{3}$$

where

$$\tilde{\boldsymbol{x}} = (\tilde{x}[0],\ldots,\tilde{x}[N-1])^T, \quad \boldsymbol{x} = (x[0],\ldots,x[N-1])^T,$$

and

$$\boldsymbol{W} = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \alpha & \alpha^2 & \ldots & \alpha^{N-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{N-1} & \alpha^{2(N-1)} & \ldots & \alpha^{(N-1)(N-1)} \end{pmatrix}.$$

As NTTs present a circular convolution property, they can also benefit from fast computation by means of FFT algorithms [20].

[1] As an example, consider the functions $f(x) = x^n + 1$ and $g(y) = y^{2n} + 1$. It is easy to verify that the square of the roots of $g(y)$ are also roots of $f(x)$.

3 AN ANALYSIS OF PREVIOUS SCHEMES

In this section, we survey the available algorithms to homomorphically evaluate a multidimensional convolution operation with both an RLWE and an m-RLWE based cryptosystem. We give approximations for computational cost, cipher expansion and security with relative expressions between the different algorithms (we refer the reader to Appendices A and B for more details on the derivation of these expressions).

3.1 Our Setup

We set the following parameters to enable a fair comparison:

- The used FV cryptosystem (see Section 2) is based on either RLWE or m-RLWE (see Definition 1) with power-of-two modular functions ($f_i(z_i) = z_i^{n_i} + 1$). The noise distribution of a fresh ciphertext has variance σ^2 and its noise coefficients are upper-bounded by B.
- We use RLWE with $n = n_l$ and m-RLWE with $n = \prod_{i=1}^{l} n_i$. Hence, the ring expansion ratio $\delta_R = n_l$ for RLWE, and $\delta_R = \prod_{i=1}^{l} n_i$ for m-RLWE.
- The computational cost is measured in terms of polynomial coefficient multiplications, without explicitly taking the cost of each coefficient multiplication into account. In Section 5 we introduce this additional factor to have a fair comparison between the analyzed schemes.
- The elemental ring operations are polynomial multiplications and additions in $R[z]$ (RLWE) or $R[z_1,\ldots,z_l]$ (m-RLWE). By means of FFT algorithms, the computational cost of polynomial products is $n_l \log n_l$ for RLWE and $n_1 \ldots n_l \log(n_1 \ldots n_l)$ for m-RLWE.
- Bit security is measured relative to $\texttt{BitSecurity}(\sigma^2, n)$, which represents the bit security of an RLWE instance with error distribution of variance σ^2 and polynomial degree n. In Section 5 we give concrete bit security estimations for the different solutions.

We work with l-dimensional signals and filters whose length per dimension is, respectively, N_i and $F_i \leq N_i$ for $i = 1,\ldots,l$, and consider two main scenarios: (a) a **linear (non-cyclic) convolution** where we reserve enough space inside the ciphertexts to store the result (i.e. $n_i = N_i + F_i - 1$), and (b) a **cyclic convolution**, enabled by means of the pre-/post-processing from [33] on top of the homomorphic negacyclic ring operation (i.e. $n_i = N_i$).

In the next sections, we introduce two RLWE-based approaches for performing a multivariate convolution, and the natural m-RLWE approach, and compare them in terms of computation cost, ciphertext noise and relative bit security, before presenting our proposed scheme.

3.2 Multidimensional convolutions in baseline RLWE

Convolution, correlation and filtering can all be expressed as a linear convolution between two l-dimensional signals $y[u_1,\ldots,u_l] = x[u_1,\ldots,u_l] * h[u_1,\ldots,u_l]$ (where $u_i \in \mathbb{N}$). With a polynomial representation, this reduces to a polynomial product $y(z_1,\ldots,z_l) = x(z_1,\ldots,z_l) \cdot h(z_1,\ldots,z_l)$.

As discussed in [29], implementing a multidimensional convolution with an RLWE-based cryptosystem can be achieved by internally encoding only one of the dimensions (u_l or z_l in this case), and externally evaluating the whole convolution on the remaining $l-1$ dimensions. This means that the two l-dimensional signals are represented with $(l-1)$-dimensional elements $x'[u_1,\ldots,u_{l-1}]$ and $h'[u_1,\ldots,u_{l-1}]$, where each element belongs to $R_q[z_l]$. The resulting operation is $y'[u_1,\ldots,u_{l-1}] = x'[u_1,\ldots,u_{l-1}] * h'[u_1,\ldots,u_{l-1}]$ with $x = 0$ (resp. $h = 0$) for elements outside of the interval $0 \leq u_i < N_i$ (resp. $0 \leq u_i < F_i$).

This external convolution operation can be realized by leveraging the circular convolution property of DFT transforms and using FFT algorithms. However, the implementation of the FFT introduces a multiplicative depth equal to $\log(\prod_{i=1}^{l-1} N_i)$, where N_i is the number of samples in dimension i; the complexity of RLWE-based cryptosystems strongly depends on the number of levels, due to the increase in the size of the ciphertext coefficients (q depends exponentially on the number of levels in Eq. (1)); hence, as noted in [17], it turns out that more basic approaches with a multiplicative depth of one perform better, even if they feature a higher (quadratic) computational cost in terms of coefficient multiplications. Hence, we rule out the "fast" algorithms and we detail the two main direct approaches in the following, to enable a fair comparison of computational complexity with fixed q.

3.2.1 NTT matrix Convolution. Let P be the total number of elements in the convolution signal ($P = \prod_{i=1}^{l-1} N_i$ for the cyclic convolution scenario, and $P = \prod_{i=1}^{l-1} (N_i + F_i - 1)$ for the linear one). The NTT can be implemented by using its matrix formulation, Eq. (3). This results in a total of P^2 multiplications between ciphertexts and cleartext scalar values (and roughly P^2 ciphertext additions). As these operations can be much faster than the P ciphertext multiplications corresponding to the Hadamard product in the NTT domain, we do not take into account the runtime corresponding to the NTT/INTTs matrix computations, but we do consider its effects in the noise of the ciphertext. Table 1(a) shows the computational cost, ciphertext's noise and bit security for this method, particularized for the two scenarios presented in Section 3.1 (linear and cyclic convolution).

3.2.2 Direct Convolution. The second approach is to directly realize the convolution equation in polynomial form, which has a computational cost of roughly the product of the lengths of the involved signals in the convolution. While this solution has a higher computational cost than the previous one, it can be seen that the NTT matrix product incurs in a higher noise than the polynomial version; furthermore, for the case where the length of the filter signal is much smaller than that of the signal (i.e. $\prod_i F_i \ll \prod_i N_i$), the direct convolution approach can be much more efficient than the NTT matrix convolution, due to a smaller cipher expansion (caused by a much more reduced noise increase). Table 1(b) summarizes the computational cost, ciphertext's noise and bit security for this method.

3.3 Multivariate RLWE

RLWE-based cryptosystems lack support for seamlessly encrypting a multidimensional signal in one ciphertext, whereas m-RLWE enables a more compact representation achieving one encryption per signal. By considering the polynomial representation of the signals $y(z_1,\ldots,z_l) = x(z_1,\ldots,z_l) \cdot h(z_1,\ldots,z_l)$, m-RLWE can homomorphically evaluate the multidimensional convolution operation with only one

Table 1: Figures for (a) baseline RLWE with NTT matrix Convolution ($t \approx n_l$), (b) baseline RLWE with Direct Convolution ($t \approx n_l$), (c) multivariate RLWE ($t \approx \max\{n_1,\ldots,n_l\}$) and (d) our packed RLWE ($t \approx \prod_{i=1}^{l} n_i$)

(a) baseline RLWE with NTT matrix Convolution

Computational Cost
$\text{Cost}_{\text{linear}} = L \cdot O(n_l \prod_{i=1}^{l-1}(N_i+F_i-1)\log n_l)$ coeff. mult. $+ L \cdot O(n_l \left(\prod_{i=1}^{l-1}(N_i+F_i-1)\right)^2)$ coeff. add.
$\text{Cost}_{\text{cyclic}} = L \cdot O(n_l \prod_{i=1}^{l-1} N_i \log n_l)$ coeff. mult. $+ L \cdot O(n_l \left(\prod_{i=1}^{l-1} N_i\right)^2)$ coeff. add.
Ciphertext's noise (upper bound on $\frac{\Delta}{2B}$)
(linear) $\frac{\Delta}{2B} \approx 2\left(\prod_{i=1}^{l-1} N_i(N_i+F_i-1)\right)^L t^L (N_l+F_l-1)^{2L+1}$
(cyclic) $\frac{\Delta}{2B} \approx 2\left(\prod_{i=1}^{l-1} N_i^2\right)^L t^L (N_l)^{2L+1}$
Bit Security
(linear) $\texttt{BitSecurity}(\sigma^2, N_l+F_l-1)$
(cyclic) $\texttt{BitSecurity}(\sigma^2, N_l)$

(b) baseline RLWE with Direct Convolution

Computational Cost
$\text{Cost}_{\text{linear}} = L \cdot O(n_l \prod_{i=1}^{l-1}(N_i F_i)\log n_l)$ coeff. mult.
$\text{Cost}_{\text{cyclic}} = L \cdot O(n_l \prod_{i=1}^{l-1}(N_i F_i)\log n_l)$ coeff. mult.
Ciphertext's noise (upper bound on $\frac{\Delta}{2B}$)
(linear) $\frac{\Delta}{2B} \approx 2\left(\prod_{i=1}^{l-1} F_i\right)^L t^L (N_l+F_l-1)^{2L+1}$
(cyclic) $\frac{\Delta}{2B} \approx 2\left(\prod_{i=1}^{l-1} F_i\right)^L t^L (N_l)^{2L+1}$
Bit Security
(linear) $\texttt{BitSecurity}(\sigma^2, N_l+F_l-1)$
(cyclic) $\texttt{BitSecurity}(\sigma^2, N_l)$

(c) multivariate RLWE

Computational Cost
$\text{Cost}_{\text{linear}} = L \cdot O(\prod_{i=1}^{l}(N_i+F_i-1)\log(\prod_{i=1}^{l} N_i+F_i-1))$ coeff. mult.
$\text{Cost}_{\text{cyclic}} = L \cdot O((\prod_{i=1}^{l} N_i)\log(\prod_{i=1}^{l} N_i))$ coeff. mult.
Ciphertext's noise (upper bound on $\frac{\Delta}{2B}$)
(linear) $\frac{\Delta}{2B} \approx 2t^L \left(\prod_{i=1}^{l}(N_i+F_i-1)\right)^{2L+1}$
(cyclic) $\frac{\Delta}{2B} \approx 2t^L \left(\prod_{i=1}^{l} N_i\right)^{2L+1}$
Bit Security
(linear) $\texttt{BitSecurity}(\sigma^2 \prod_{i=1}^{l-1}(N_i+F_i-1), N_l+F_l-1)$
(cyclic) $\texttt{BitSecurity}(\sigma^2 \prod_{i=1}^{l-1} N_i, N_l)$

(d) packed RLWE

Computational Cost
$\text{Cost}_{\text{linear}} = L \cdot O(\prod_{i=1}^{l}(N_i+F_i-1)\log(\prod_{i=1}^{l} N_i+F_i-1))$ coeff. mult.
$\text{Cost}_{\text{cyclic}} = L \cdot O((\prod_{i=1}^{l} N_i)\log(\prod_{i=1}^{l} N_i))$ coeff. mult.
Ciphertext's noise (upper bound on $\frac{\Delta}{2B}$)
(linear) $\frac{\Delta}{2B} \approx 2t^L \left(\prod_{i=1}^{l}(N_i+F_i-1)\right)^{2L+1}$
(cyclic) $\frac{\Delta}{2B} \approx 2t^L \left(\prod_{i=1}^{l} N_i\right)^{2L+1}$
Bit Security
(linear) $\texttt{BitSecurity}(\sigma^2, \prod_{i=1}^{l}(N_i+F_i-1)$
(cyclic) $\texttt{BitSecurity}(\sigma^2, \prod_{i=1}^{l} N_i)$

ciphertext multiplication [29, 32], which can be realized leveraging efficient FFT algorithms with no penalty on the required ciphertext size, which is a clear advantage with respect to baseline RLWE. Nevertheless, due to the recent attack presented in [9], the security of m-RLWE cannot be based on the product dimension of the multidimensional polynomial ($n = \prod_{i=1}^{l} n_i$), but instead on the highest degree of the univariate rings (that is, $\max\{n_i\}$). Table 1(c) summarizes the computational cost, ciphertext's noise and bit security for the m-RLWE multidimensional convolution.

3.4 Comparison between RLWE and m-RLWE

In light of the results shown in Tables 1(a), 1(b), and 1(c), it is clear that m-RLWE is much more efficient than RLWE when implementing multidimensional convolutions, but the increase in ciphertext size is not paired with an analogous increase in the bit security of m-RLWE, in general. Actually, depending on the chosen modular functions, m-RLWE can be isomorphic to RLWE when the modular functions $\{\phi_{m_1}(z_1),\ldots,\phi_{m_l}(z_l)\}$ satisfy $\gcd(m_1,\ldots,m_l) = 1$ (see Section 2.1). Hence, it is possible to preserve some of the advantages of m-RLWE while still keeping the security reduction to a lattice of dimension equal to the product of the degrees of each univariate ring, by resorting to "uneven" non-power-of-two (coprime) univariate modular functions.

As an example, Cheon and Kim [13] initially proposed using m-RLWE with modulo power-of-two cyclotomic polynomials, and updated their application to use "coprime" cyclotomic polynomials [15] after the publication of Bootland *et al.* attack [9].

In the next section we focus on the "worst-case" scenario, where the security of m-RLWE reduces to only the highest of the univariate degrees. Even after this reduction on security, we show that m-RLWE can outperform the use of a simpler RLWE instance, due to two key advantages: (1) working with power-of-two univariate modular functions $1+z^n$ which enable faster algorithms for product and reduction computations, and (2) more flexibility on the choice of the encrypted "lengths".

However, we want to remark that the results presented here can be analogously applied to more general RLWE instances with other cyclotomic polynomial modular functions.

4 PROPOSED SCHEME

This section describes the main contribution of this work. We introduce a new pre-/post-coding block which, when applied before/after RLWE-based encryption/decryption, transforms the polynomial multiplication (1D negacyclic convolution) of RLWE samples with power-of-two modular function ($l = 1$ in Definition 1) into an l-dimensional cyclic convolution operation. This enables the efficient realization of multivariate convolutions under the RLWE problem without a loss in security; i.e., the bit security is that of the whole lattice dimension $n = \prod_{i=1}^{l} n_i$. Therefore, we can encrypt the whole multidimensional signal in just one RLWE encryption with a security based on RLWE and not affected by Bootland's attack, while preserving all the properties of m-RLWE claimed in [29, 32].

We start by defining multivariate NTT/INTTs, as one of the main building blocks of our proposed scheme, and then we present our proposed framework for pre-/post-coding.

4.1 Multivariate Number Theoretic Transforms

Consider a length-N NTT transform over $\mathbb{Z}_p$, as defined in equations (3) by a matrix multiplication with $\boldsymbol{W}$ (and $\boldsymbol{W}^{-1}$ for the INTT).

If $\boldsymbol{x}$ represents a "flattened" vector[2] with the samples of an l-dimensional signal x, we can define an l-dimensional NTT/INTT as the Kronecker product of the NTT matrices for the l dimensions as

[2] A "flattened" $\boldsymbol{x}$ vector is a reshape of the multdimensional signal x into a column vector.

follows:

$$\tilde{\boldsymbol{x}} = \underbrace{\left(\bigotimes_{i=1}^{l} \boldsymbol{W}^{(z_i)}\right)}_{\boldsymbol{V}^{(l)}} \boldsymbol{x}, \quad \boldsymbol{x} = \underbrace{\left(\bigotimes_{i=1}^{l} (\boldsymbol{W}^{(z_i)})^{-1}\right)}_{(\boldsymbol{V}^{(l)})^{-1}} \tilde{\boldsymbol{x}}, \tag{4}$$

where each $\boldsymbol{W}^{(z_i)}$ (resp. $(\boldsymbol{W}^{(z_i)})^{-1}$) is the NTT (resp. INTT) of length N_i for the i-th dimension (z_i) of x. Equivalently in signal representation, the i-th NTT matrix is applied to $x[u_1,\ldots,u_i,\ldots,u_l]$ as a vector of N_i $(l-1)$-dimensional samples indexed by $u_i = 0,\ldots,N_i-1$, for each $i = 1,\ldots,l$. Hence, the matrices $\boldsymbol{V}^{(l)}$ (resp. $(\boldsymbol{V}^{(l)})^{-1}$) represent the l-dimensional NTT (resp. l-dimensional INTT). Additionally, the conditions in Section 2.4 must be satisfied, so for each matrix $\boldsymbol{W}^{(z_i)}$ there must exist an N_i-th root of unity in $\mathbb{Z}_p$.

The l-dimensional NTT/INTT satisfies a multivariate circular convolution property that we exploit in our proposed scheme

$$\boldsymbol{V}^{(l)}\boldsymbol{y} = (\boldsymbol{V}^{(l)}\boldsymbol{x}) \circ (\boldsymbol{V}^{(l)}\boldsymbol{h}), \tag{5}$$

where $\boldsymbol{y},\boldsymbol{x},\boldsymbol{h}$ are the "flattened" vectors corresponding to the signals $y[u_1,\ldots,u_l], x[u_1,\ldots,u_l], h[u_1,\ldots,u_l]$, and $y[u_1,\ldots,u_l]$ is the l-dimensional circular convolution between $x[u_1,\ldots,u_l]$ and $h[u_1,\ldots,u_l]$.

Analogously to their univariate counterparts, multidimensional NTT/INTTs can be efficiently implemented with FFT algorithms.

4.2 "Packed"-RLWE and its underlying Multivariate Structure

Once we have introduced the formulation for multivariate NTTs/INTTs applied to flattened vectors, we can present the pre-/post-processing adapted from [25, 33] which allows to transform the negacyclic convolutions of the rings from Definition 1 into cyclic convolutions.

Consider two length-N signals $x[j]$ and $h[j]$, with polynomial representations $x(z)$,$h(z)$

$$x(z) = \sum_{i=0}^{N-1} x[i]z^i \quad \text{and} \quad h(z) = \sum_{i=0}^{N-1} h[i]z^i.$$

We want to calculate their circular convolution $y(z) = x(z)h(z) \mod 1-z^N$, but the ring operation enabled as a homomorphic product is a polynomial product modulo $1+z^N$ (negacyclic convolutions).

Assume that there exists a $2N$-th root of unity β in $\mathbb{Z}_p$ (that is, $\beta = (-1)^{\frac{1}{N}} \mod p$), the pre-/post-processing [25, 33] consists of the following steps (we term it Murakami pre-/post-processing):

- The input signals are pre-processed with component-wise products

$$x'[j] = x[j](1)^{\frac{-j}{N}}(-1)^{\frac{j}{N}}, \qquad j = 0,\ldots,N-1,$$
$$h'[j] = h[j](1)^{\frac{-j}{N}}(-1)^{\frac{j}{N}}, \qquad j = 0,\ldots,N-1.$$

- Then, $y'(z)$ can be calculated with a negacyclic convolution as $y'(z) = x'(z)h'(z) \mod 1+z^N$.
- The output signal is post-processed with component-wise products

$$y[j] = y'[j]1^{\frac{j}{N}}(-1)^{\frac{-j}{N}}.$$

Equipped with the Murakami pre-/post-processing, we can emulate the operation from a ring with a circular convolution property. The last step is to find a way of transforming the unidimensional circular convolution into a multidimensional one. To this aim, we combine both a unidimensional NTT/INTT (see Section 2.4) and a multidimensional NTT/INTT.

Let $\boldsymbol{y}$ be the flattened l-dimensional circular convolution of $\boldsymbol{x}$ and $\boldsymbol{h}$. By the convolution property of the NTTs, we have

$$\left(\boldsymbol{W}^{-1}\boldsymbol{x}'\right) \circledast \left(\boldsymbol{W}^{-1}\boldsymbol{h}'\right) = \boldsymbol{W}^{-1}(\boldsymbol{x}' \circ \boldsymbol{h}'),$$

where $\boldsymbol{x}' = \boldsymbol{V}^{(l)}\boldsymbol{x}$ and $\boldsymbol{h}' = \boldsymbol{V}^{(l)}\boldsymbol{h}$. If we make use of the convolution property of the l-dimensional NTT, Eq (5) with $N = \prod_{i=1}^{l} N_i$, we have

$$\begin{aligned}(\boldsymbol{W}^{-1}\boldsymbol{V}^{(l)}\boldsymbol{x}) \circledast (\boldsymbol{W}^{-1}\boldsymbol{V}^{(l)}\boldsymbol{h}) = \quad & \boldsymbol{W}^{-1}\left((\boldsymbol{V}^{(l)}\boldsymbol{x}) \circ (\boldsymbol{V}^{(l)}\boldsymbol{h})\right) \\ = \quad & \boldsymbol{W}^{-1}\boldsymbol{V}^{(l)}(\boldsymbol{y}).\end{aligned}$$

This represents a chain of matrix transformations that relates the unidimensional circular and l-dimensional circular convolutions.[3]

Hence, the resulting structure of our proposed pre-/post-coding, detailed in Figure 1 is as follows:

- A pre-coding is applied to the input signals

$$\boldsymbol{x}'' = \Upsilon\boldsymbol{W}^{-1}\boldsymbol{V}^{(l)}\boldsymbol{x} \quad \text{and} \quad \boldsymbol{h}'' = \Upsilon\boldsymbol{W}^{-1}\boldsymbol{V}^{(l)}\boldsymbol{h}.$$

- $y''(z)$ is calculated as $x''(z)h''(z) \mod 1+z^N$.
- A post-coding is applied to $y''(z)$

$$\boldsymbol{y} = (\boldsymbol{V}^{(l)})^{-1}\boldsymbol{W}\Upsilon^{-1}\boldsymbol{y}''.$$

The matrices Υ and Υ^{-1} are diagonal matrices containing the elements of the Murakami pre-/post-processing $(1)^{\frac{-j}{N}}(-1)^{\frac{j}{N}}$ and $(1)^{\frac{j}{N}}(-1)^{\frac{-j}{N}}$ for $j = 0,\ldots,N-1$.

Table 1(d) includes a summary with the computational cost, ciphertext's noise and bit security for the execution of a multidimensional convolution with the proposed method. This table includes the cost of the actual convolution without the pre-/post-coding, which would be executed at the client-side in a homomorphic processing scenario, and is evaluated as part of the encryption/decryption in Section 5. In any case, this pre-/post-coding only comprises element-wise multiplications and a chain of two FFT computations on the plaintext ring, so the computational cost of both encryption and decryption with the FV cryptosystem is higher than this processing chain.

5 SECURITY AND PERFORMANCE EVALUATION

This section includes a comparison of RLWE, m-RLWE and the proposed packed-RLWE in terms of security, computational cost and cipher expansion. We start by describing the procedure followed to analyze the security of the different schemes. Afterwards, we analyze and compare the expressions reported in Tables 1(a), 1(b), 1(c) and 1(d), and we highlight the tradeoffs for each scenario. Finally, we include execution runtimes for the case of image and 3D-signal filtering.

5.1 Evaluation for Encrypted Processing of Multidimensional Signals

In [29, 32] we compared several encrypted multidimensional operations implemented with an RLWE or an m-RLWE based scheme. We

[3] While we focus on NTT transforms, similar results could be considered with chains of CRT matrices (see [22]). This would enable the encoding of different multidimensional signals in any instance of RLWE with a general cyclotomic modular function.

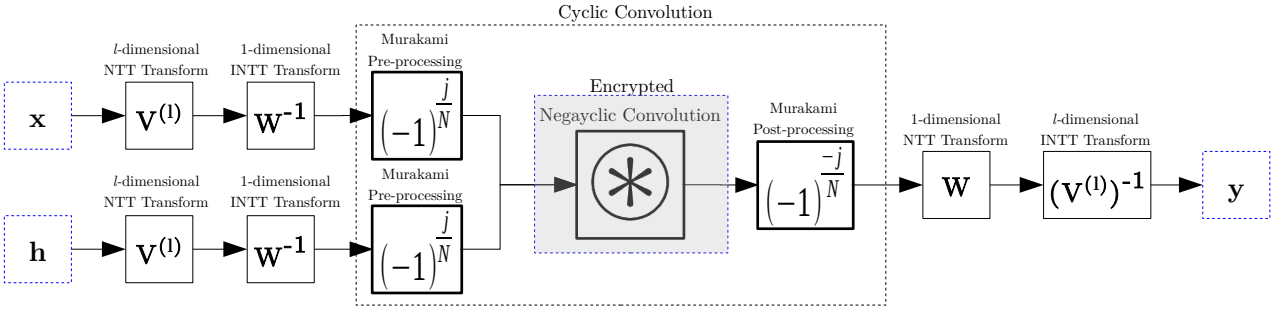


Figure 1: Block diagram of the proposed scheme for "packed"-RLWE

concluded that the m-RLWE implementation enabled a much higher security with faster runtimes.

However, after the attack presented in [9], we know that the security estimations with m-RLWE are no longer valid. Nevertheless, the packed-RLWE solution we have introduced in this work can preserve all the claimed security and efficiency results in [29, 32].

In this work, instead of using a slack variable as in [29, 32], we follow a different approach, and we compare baseline RLWE, m-RLWE (see Section 3) and our packed-RLWE solution (see Section 4) by fixing the minimum level of security in terms of the lattice dimension for baseline RLWE. This dimension is kept constant for each univariate ring of m-RLWE and packed-RLWE, even though the security obtained with the two latter will be higher, and hence, the comparison on efficiency represents a worst-case scenario for m-RLWE and an unfavorable case for our packed-RLWE. We show that even in this pessimistic scenario, both m-RLWE and packed-RLWE can outperform baseline RLWE both in terms of efficiency and security.

For simplicity, we make the following set of assumptions (we refer the reader to Appendices A and B for further details):

- A1 We work with "hyper-cubic" l-dimensional signals with the same length N in each dimension (length-F in case of filters) and we assume n_i to be equal to the value required to store the result of the linear or cyclic convolution.
- A2 We define $F = C \cdot N$ where C is a constant satisfying $0 < C \leq 1$, so that we can express the results in terms of N to compare the behavior of both linear and cyclic convolutions under the same formulation.
- A3 For estimating the cost of each coefficient multiplication in $\mathbb{Z}_q$, we assume the use of Schönhage-Strassen algorithm with a cost of $O(w(\log w)(\log\log w))$, with $w = O(\log_2 q)$. For the asymptotic analysis, we simplify the cost to $O(\log_2 q)$.

5.1.1 Comparison of Computational Cost and Cipher Expansion. A summary with the computational cost and ciphertexts' noise for each of the analyzed approaches, particularized for assumptions A1-A3, is included in Tables 2(a), 2(b) and 2(c). We refer the reader to Appendices A and B for the detailed derivation of the approximate costs and noise bounds. We first compare the asymptotic cost ratios for increasing N between the four approaches, and then move on to a more precise analysis of the effect of each parameter for a given N.

Asymptotic computational cost ratios. By neglecting the effect of some logarithmic factors in the computational cost, we can provide some approximate asymptotic comparisons between the different schemes, in order to highlight the most significant effects. In particular, we consider $N \gg F$, so we approximate $N+F-1 \approx (1+C)N$ and neglect the effect of $(1+C)$ and its powers with respect to powers of N. This allows us to cover both linear and cyclic convolutions with the same computational cost expressions (we refer the reader to Appendices A and B for more details on the simplifications).

If we neglect the effect of additions and consider only products as the operation driving the complexity, we obtain the following ratios

$$\frac{\text{Cost}_{rd}}{\text{Cost}_{rn}} \approx N^l, \quad \frac{\text{Cost}_{mr}}{\text{Cost}_{rn}} \approx l, \quad \frac{\text{Cost}_{pr}}{\text{Cost}_{rn}} \approx l, \quad \frac{\text{Cost}_{pr}}{\text{Cost}_{mr}} \approx \frac{3}{2},$$

where the costs $\{\text{Cost}_{rn}, \text{Cost}_{rd}, \text{Cost}_{mr}, \text{Cost}_{pr}\}$ correspond, respectively, to {Baseline RLWE (NTT matrix comp.), Baseline RLWE (Dir. Conv.), m-RLWE, and packed-RLWE}.

We can see that Cost_{rn} is approximately l times lower than Cost_{mr} and Cost_{pr}, but it has also a lower bit security, which grows with l for packed RLWE.

If we factor in additions by assuming a cost of $O(\log_2 q)$ for each coefficient addition (linear in the size of the coefficients), the asymptotic ratios become

$$\frac{\text{Cost}_{rd}}{\text{Cost}^*_{rn}} \approx \log_2 N, \quad \frac{\text{Cost}_{mr}}{\text{Cost}^*_{rn}} \approx \frac{l\log_2 N}{N^{l-1}}, \quad \frac{\text{Cost}_{pr}}{\text{Cost}^*_{rn}} \approx \frac{l\log_2 N}{N^{l-1}},$$

where Cost^*_{rn} represents the cost of the NTT/INTT matrix computation in baseline RLWE. Consequently, we see that m-RLWE and packed-RLWE are not only more secure, but also asymptotically more efficient than baseline RLWE for a wide set of scenarios.

Precise computational cost. While the previous asymptotic analysis is useful to extract the relative behavior of the schemes for very large N, it neglects the effects of some parameters. Now, we calculate the exact costs of the different methods by using the Schönhage-Strassen algorithm for coefficient multiplication, considering $\log_2 q$ for the cost of coefficient additions and without removing any non-significant factors.

We choose two filtering scenarios with 2- and 3-dimensional signals. In all figures we represent the cost (in terms of N) of a convolution between a "hyper-cubic" 2D or 3D signal with length N per dimension and a filter with length $F = \{0.01N, 0.1N, N\}$ per dimension.[4] Figure 2 (resp. Figure 3) represents the cost for a linear

[4]The cost plotted in Figures 2, 3, 4 and 5 considers $n_i \approx N$ or $n_i \approx N+F-1$, but in practice each n_i will be rounded up to a power of two (see Definition 1), so performance will show a step-wise behavior for growing N instead of the smooth figures we show.

Table 2: Cost and noise bounds for (a) baseline RLWE with NTT matrix Convolution ($t \approx n_l$, $N_i = N, F_i = C \cdot N$), (b) baseline RLWE with Direct Convolution ($t \approx n_l$, $N_i = N, F_i = C \cdot N$), (c) m-RLWE ($t \approx \max\{n_1,\ldots,n_l\}$) and packed-RLWE ($t \approx \prod_{i=1}^{l} n_i$, $N_i = N, F_i = C \cdot N$)

(a) baseline RLWE with NTT matrix Convolution

Computational Cost
$\text{Cost}_{\text{linear}} = L \cdot O((1+C)^l N^l \log((1+C)N)) + L \cdot O(((1+C)N)^{2l-1})$ coeff. add. $\text{Cost}_{\text{cyclic}} = L \cdot O(N^l \log N) + L \cdot O(N^{2l-1})$ coeff. add.
Ciphertext's noise (upper bound on $\frac{\Delta}{2B}$)
(linear) $\frac{\Delta}{2B} \approx 2(1+C)^{L(l+2)+1} t^L N^{2L(l+1)+1}$ (cyclic) $\frac{\Delta}{2B} \approx 2t^L N^{2L(l+1)+1}$

(b) baseline RLWE with Direct Convolution

Computational Cost
$\text{Cost}_{\text{linear}} = L \cdot O((1+C)C^{l-1} N^{2l-1} \log((1+C)N))$ $\text{Cost}_{\text{cyclic}} = L \cdot O(C^{l-1} N^{2l-1} \log N)$
Ciphertext's noise (upper bound on $\frac{\Delta}{2B}$)
(linear) $\frac{\Delta}{2B} \approx 2C^{Ll}(1+C)^{2L+1} t^L N^{L(l+2)+1}$ (cyclic) $\frac{\Delta}{2B} \approx 2C^{Ll} t^L N^{L(l+2)+1}$

(c) m-RLWE and packed-RLWE

Computational Cost
$\text{Cost}_{\text{linear}} = L \cdot O(l(1+C)^l N^l \log((1+C)N))$ $\text{Cost}_{\text{cyclic}} = L \cdot O(lN^l \log N)$
Ciphertext's noise (upper bound on $\frac{\Delta}{2B}$)
(linear) $\frac{\Delta}{2B} \approx 2(1+C)^{2Ll+l} t^L N^{2Ll+l}$ (cylic) $\frac{\Delta}{2B} \approx 2t^L N^{2Ll+l}$

(resp. cyclic) convolution of 2D images, while Figure 4 (resp. Figure 5) represents the cost for a linear (resp. cyclic) convolution of 3D signals. All of them plot the relative cost of RLWE with NTT matrix and direct convolution, m-RLWE, and packed-RLWE, as a function of the per-bit elementary operation cost for growing signal size; the ciphertext size q is taken as the minimum value that enables the operation with no decryption errors for a constant noise power; therefore, security is also increased together with N (see Section 5.2). Hence, we are accounting for the raw growth in complexity produced by a change in the signal dimensions.

We can see that changes in the relative filter size C have a higher impact when the dimensionality of the signals increases, and in particular, the expansion in baseline RLWE with direct convolution is strongly influenced by small C values, which explains why it can be better when working with very small filters. In this case, if baseline RLWE gives enough security, it can be the best option, because both m-RLWE/packed-RLWE would require to further increase each of the n_i to store the results. In general, there is a minimum value of C for which packed-RLWE and m-RLWE start outperforming baseline RLWE, and this value decreases when increasing the dimensionality, showing that packed-RLWE and m-RLWE perform better with high-dimensional signals and/or with filters of moderate or big size.

It is worth noting that none of the approaches is universally better than the others, and a combination of all of them may produce the best efficiency/security trade-offs. As an example, if the used filter has one particularly small dimension, it could be worth to encode this dimension as external to the encryption scheme. Conversely, if the security of the largest dimension is enough, the structure of m-RLWE could be preferable, as it can be more easily parallelizable than packed-RLWE and also avoids the pre-/post-coding stage at the client. Nevertheless, packed-RLWE is shown to outperform baseline RLWE and m-RLWE both in efficiency and security in a wide range of parameterizations.

5.2 Security evaluation

Tables 1(a), 1(b), 1(c) and 1(d) express the security of the schemes relative to $\texttt{BitSecurity}(\sigma^2, n)$ (see Sections 3 and 4). This function grows when increasing σ^2 or n (it is much more sensitive to n).

In order to give concrete values for $\texttt{BitSecurity}(\sigma^2, n)$, we make use of the LWE security estimator developed by Albrecht *et al.* [4, 5],[5] by calling the function `estimate_lwe`(n,α,q, secret_ distribution = "normal",reduction_cost_model = BKZ.sieve), where $\sigma = \frac{\alpha q}{\sqrt{2\pi}}$. The results for the analyzed cases are shown in Tables 3 and 4, which are discussed in the next subsection in the context of the achieved security-efficiency tradeoffs.

[5] Available online at `https://bitbucket.org/malb/lwe-estimator`.

5.3 Implementation and execution times

We have implemented the methods from Sections 3 and 4 making use of the RNS variant of the FV cryptosystem [6], in order to have concrete runtimes, instantiating the complexity measures introduced in the previous section. Execution runtimes were measured on an Intel Xeon E5-2667v3 at 3.2 GHz using one core (no parallelization).

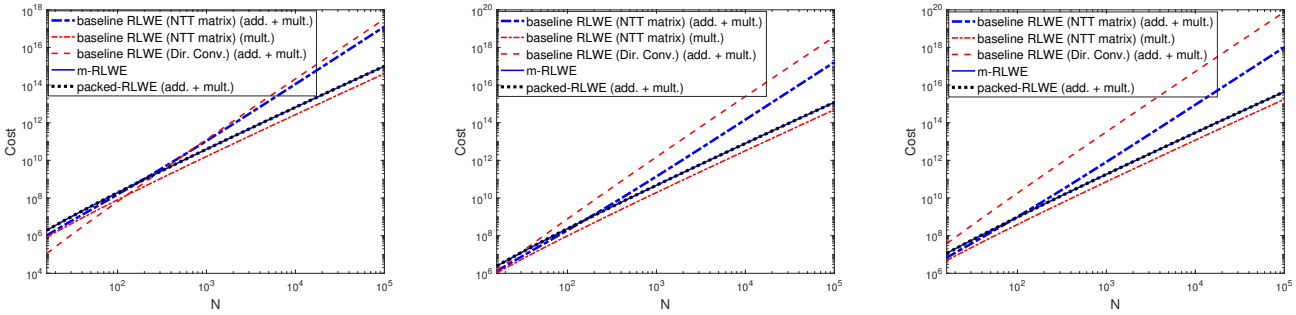
We remark that we have not included results using the Paillier cryptosystem [27] in our performance comparison, but its runtimes and bit security can be easily extrapolated from [29, 32] and [1] respectively. In any case, Paillier cannot address the operations with encrypted signals and filters, and even with clear-text filters it is much slower than any RLWE-based scheme for this type of operations.

Tables 3 and 4 report runtimes for, respectively, encrypted $2D$-image linear filtering and encrypted $3D$-signal cyclic filtering for the same signal length per dimension. We have used $n_i = N_i + F_i - 1$ and $n_i = N_i$ (lattice dimensions equal to the signal dimensions) to show the maximum achievable efficiency for each scheme. In both scenarios, packed-RLWE provides similar runtimes to multivariate RLWE and faster runtimes than both baseline RLWE solutions, while also having a much higher bit security. Actually, with previous approaches we can only guarantee a very reduced security for the chosen polynomial degree, which is clearly below the current recommended bit security estimations (≥ 128 and ≥ 256 for quantum-resistance), and means that their computational complexity for the same acceptable security level as packed-RLWE would be substantially worse.

6 A DISCUSSION: MULTIDIMENSIONAL STRUCTURES AND THEIR APPLICATIONS

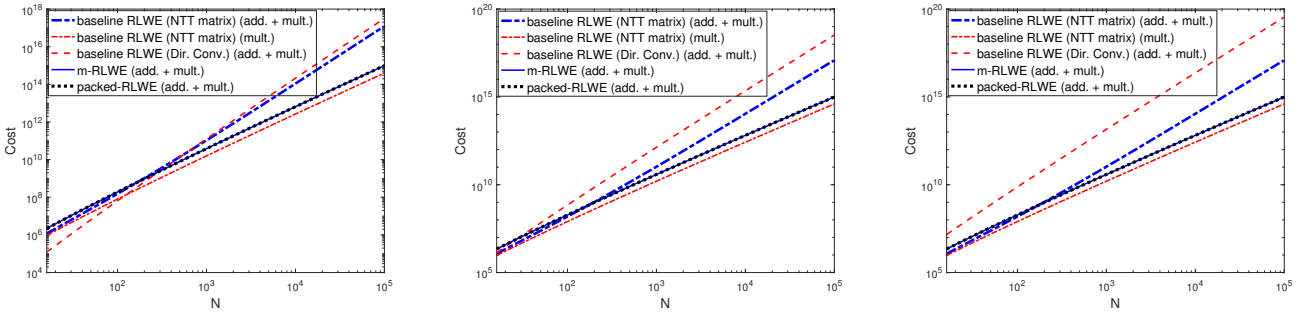
This work introduces a new pre-/post-coding block which enables significant efficiency advantages with respect to regular RLWE when processing multidimensional signals, bringing the benefits of m-RLWE while avoiding the recent attack by Bootland *et al.* [9] by basing the security only on that of RLWE.

While we focus on multidimensional filtering and correlation scenarios with encrypted signals, the proposed multivariate structures can be leveraged in a much wider set of applications. These range from block-processing (where we could apply homomorphic transforms between different block structures), better encrypted packing, multi-scale approaches such as pyramids and wavelet transforms, and even block-DCTs. These solutions could also be combined



(a) $C = 0.01$ (b) $C = 0.1$ (c) $C = 1$

Figure 2: Computational cost of encrypted image linear filtering for different relative filter sizes $C = \{0.01, 0.1, 1\}$



(a) $C = 0.01$ (b) $C = 0.1$ (c) $C = 1$

Figure 3: Computational cost of encrypted image cyclic filtering for different relative filter sizes $C = \{0.01, 0.1, 1\}$

with conventional signal processing approaches such as overlap-save and overlap-add algorithms (see [28]) and used to enhance encrypted matrix operations [15]. Hence, multivariate structures can produce notable efficiency improvements in many applications, when combining the solutions proposed in this work to optimize the security-efficiency trade-offs.

The use of packed-RLWE could also provide clear improvements in more complex applications such as forensic analysis and, in particular, camera attribution in the encrypted domain, where we can already find some works such as [23, 24, 28]. The last two make use of the BGN (Boneh-Goh-Nissim) cryptosystem to implement an homomorphic correlation operation between images. By the use of our proposed method, their runtimes could be greatly improved with no impact (or with an increase) on security.

7 CONCLUSIONS

We have proposed a novel framework for secure outsourced processing of encrypted multidimensional signals. As a fundamental block in our framework, we present a new pre-/post-coding block which enables multivariate structures directly on RLWE-based cryptosystems without compromising the security of the RLWE problem. We have also reevaluated the security of previous solutions based on multivariate RLWE by taking into account a recent attack which exploits the use of modular functions by introducing repeated roots in the ring. We have included an extensive comparison in terms of security and performance between the different approaches, showing the advantages of our scheme with respect to the previous solutions in terms of both faster runtimes and higher security; and also analyzing the possibility of adapting a combination of different methods to the needs of the specific scenario. Consequently, this work opens up a broad set of encrypted processing applications which deal with multidimensional signals and shows the viability of somewhat homomorphic encryption for the privacy-preserving processing of this type of signals.

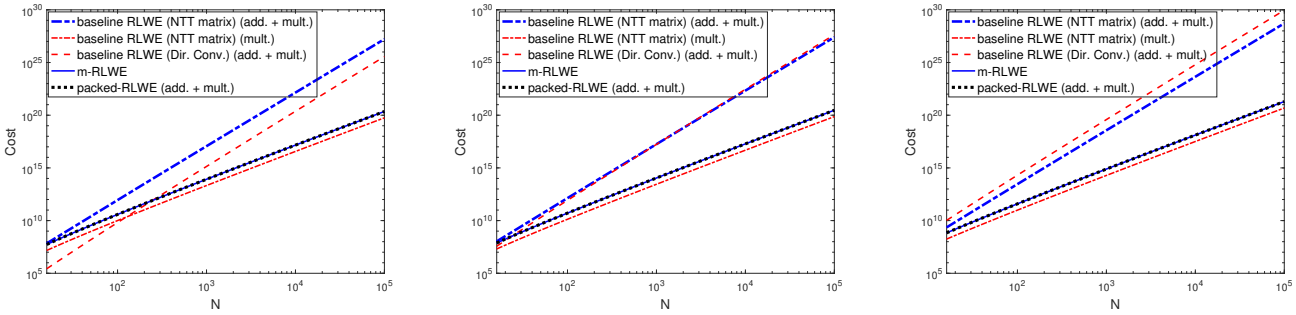
A CIPHER EXPANSION ANALYSIS

In order to calculate the bounds on q (see Section 2) depending on the chosen scheme, we rely on Lemma 3 from [18], which relates noise growth in the FV cryptosystem after each addition and multiplication. We include here a slightly modified version of the lemma:

LEMMA 1 (LEMMA 3 FROM [18]). *Let ct_i for $i = 1,2$ be two ciphertexts with $[ct_i(s)]_q = \Delta \cdot m_i + v_i$ where $\Delta = \lfloor \frac{q}{t} \rfloor$, and $||v_i|| < E < \frac{\Delta}{2}$. Set $ct_{add} = FV.SH.Add(ct_1, ct_2)$ and $ct_{mult} = FV.SH.Mul(ct_1, ct_2, rlk)$ then*

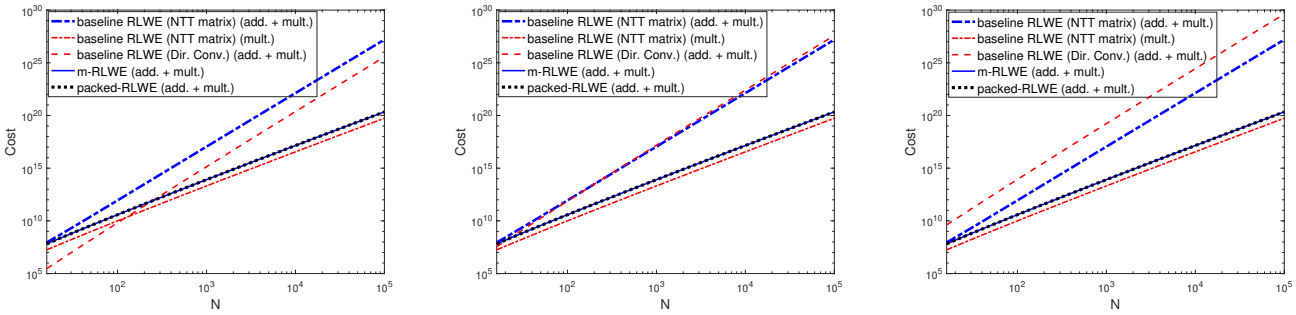
$$[ct_{add}(s)]_q = \Delta \cdot [m_1 + m_2]_t + v_{add},$$
$$[ct_{mul}(s)]_q = \Delta \cdot [m_1 \cdot m_2]_t + v_{mul},$$

with $||v_{add}|| < 2E + t$ and $||v_{mul}|| < Et\delta_R(\delta_R + 1.25) + E_{Relin}$.



(a) $C = 0.01$ (b) $C = 0.1$ (c) $C = 1$

Figure 4: Computational cost of encrypted 3D-signal linear filtering for different relative filter sizes $C = \{0.01, 0.1, 1\}$



(a) $C = 0.01$ (b) $C = 0.1$ (c) $C = 1$

Figure 5: Computational cost of encrypted 3D-signal cyclic filtering for different relative filter sizes $C = \{0.01, 0.1, 1\}$

Taking into account Lemma 1 and the approximation for the noise in a fresh ciphertext, $E = 2\delta_R B$ (see [18]), the noise after L levels of multiplication is approximately $2B\delta_R^{2L+1} t^L$. This expression can be directly used to estimate the size of q (hence the cipher expansion) for both the multivariate and "packed" RLWE schemes.

However, when working with baseline RLWE for a multidimensional convolution, the effect of additions cannot be neglected, as their number is of the order of (or even higher than) δ_R, so we explicitly take them into account in the size of q. After one addition, $||v_{add}|| < 2E + t = 2\delta_R B + t$, where we neglect t because in our scheme $\delta_R B$ dominates the right hand term. Murakami pre-/post-processing (see [25, 33]) needs a t higher than the lattice dimension, so we choose a slightly higher t, that is $t \approx \max\{N_i + F_i - 1\}$ for all schemes but for packed-RLWE, for which $t \approx \prod(N_i + F_i - 1)$.

The effect of these additions into the size of the noise is equivalent to a multiplicative factor A_{add}, yielding a noise of $A_{add}^L \cdot 2B\delta_R^{2L+1} t^L$ after L multiplication levels.

The expressions for A_{add} for baseline RLWE are

- NTT matrix Convolution:

$$A_{add}^{(linear)} = \prod_{i=1}^{l-1} N_i(N_i + F_i - 1), \quad A_{add}^{(cyclic)} = \prod_{i=1}^{l-1} N_i^2$$

- Direct Convolution:

$$A_{add}^{(linear)} = \prod_{i=1}^{l-1} F_i, \quad A_{add}^{(cyclic)} = \prod_{i=1}^{l-1} F_i$$

If we now assume $N_i = N$ and $F_i = CN_i$ with $0 < C \leq 1$, we have the following noise size approximations after a linear convolution in each scheme

- baseline RLWE (NTT matrix Convolution):

$$\begin{aligned}\frac{\Delta}{2} &\approx 2B(1+C)^{L(l-1)} N^{2L(l-1)} \delta_R^{2L+1} t^L \\ &\approx 2B(1+C)^{Ll+L+1} N^{2Ll+1} t^L.\end{aligned}$$

- baseline RLWE (Direct Convolution):

$$\begin{aligned}\frac{\Delta}{2} &\approx 2BC^{L(l-1)} N^{L(l-1)} \delta_R^{2L+1} t^L \\ &\approx 2BC^{L(l-1)} (1+C)^{2L+1} N^{L(l+1)+1} t^L.\end{aligned}$$

- multivariate and "packed" RLWE:

$$\frac{\Delta}{2} \approx 2B\delta_R^{2L+1} t^L \approx 2B(1+C)^{2Ll+l} N^{2Ll+l} t^L.$$

We know that $0 < 1 + C \leq 2 \ll N$ and its exponent is not higher than the exponent of N, so in the following we will ignore powers of $(1+C)$. This allows us to use the same expression for both linear

Table 3: Runtimes and security for encrypted 2D Linear Filtering ($L=1$, $\sigma=8$, $B=6\sigma$, 2 limbs for q, $F=11$)

$N\times N$	118×118	246×246
baseline RLWE (NTT matrix Convolution)		
n	128	256
Enc. (image + filter) size (bits)	$4.09\cdot10^6$	$16.32\cdot10^6$
Bit security	≈ 31	≈ 33
Encryption time (ms)	2.4	5.8
Decryption time (ms)	1.4	3.7
Convolution time (ms)	43.3	142.4
Baseline RLWE (Direct Convolution		
n	128	256
Enc. (image + filter) size (bits)	$4.09\cdot10^6$	$16.32\cdot10^6$
Bit security	≈ 31	≈ 33
Encryption time (ms)	2.4	5.8
Decryption time (ms)	1.4	3.7
Convolution time (ms)	272.5	812.6
Multivariate RLWE		
n (effective n)	16384 (128)	65536 (256)
Enc. (image + filter) size (bits)	$8.13\cdot10^6$	$32.51\cdot10^6$
Bit security	≈ 32	≈ 33
Encryption time (ms)	1.6	8.6
Decryption time (ms)	1.3	7.8
Convolution time (ms)	28.2	127.5
Packed RLWE		
n	16384	65536
Enc. (image + filter) size (bits)	$8.13\cdot10^6$	$32.51\cdot10^6$
Bit security	> 128	> 128
Encryption time (ms)	3.1	12.6
Decryption time (ms)	2.8	11.8
Convolution time (ms)	28.2	127.5

Table 4: Runtimes and security for encrypted 3D Cyclic Filtering ($L=1$, $\sigma=8$, $B=6\sigma$, 2 limbs for q, $F=5$)

$N\times N\times N$	16×16×16	32×32×32
baseline RLWE (NTT matrix Convolution)		
n	16	32
Enc. (image + filter) size (bits)	$1.12\cdot10^6$	$8.32\cdot10^6$
Bit security	< 30	< 30
Encryption time (ms)	2.9	5.6
Decryption time (ms)	0.3	2.6
Convolution time (ms)	6.0	58.1
Baseline RLWE (Direct Convolution		
n	16	32
Enc. (image + filter) size (bits)	$1.12\cdot10^6$	$8.32\cdot10^6$
Bit security	< 30	< 30
Encryption time (ms)	2.9	5.6
Decryption time (ms)	0.3	2.6
Convolution time (ms)	150.1	1452.8
Multivariate RLWE		
n (effective n)	4096 (16)	32768 (32)
Enc. (image + filter) size (bits)	$2.03\cdot10^6$	$16.25\cdot10^6$
Bit security	< 30	< 30
Encryption time (ms)	0.6	3.7
Decryption time (ms)	0.4	3.0
Convolution time (ms)	6.4	53.3
Packed RLWE		
n	4096	32768
Enc. (image + filter) size ($bits$)	$2.03\cdot10^6$	$16.25\cdot10^6$
Bit security	> 128	> 128
Encryption time (ms)	0.8	6.0
Decryption time (ms)	0.7	5.4
Convolution time (ms)	6.4	53.3

and cyclic convolutions (see Table 5) in the asymptotic cost ratio analysis in Section 5.1.1.

B COMPUTATIONAL COST ANALYSIS

An integer multiplication in $\mathbb{Z}_q$ using a Schönhage-Strassen algorithm has a cost of $O(\log_2 q\cdot(\log_2\log_2 q)\cdot(\log_2\log_2\log_2 q))$. We can compare the computational cost of all the schemes by considering the number of coefficient multiplications and the cost of each coefficient multiplication. For simplicity, we only keep the $\log_2 q$ term in the cost of the Schönhage-Strassen algorithm

- baseline RLWE (NTT matrix Convolution, $t\approx N$):

$$\text{Cost}_{rn}\approx \underbrace{LN^l\log_2 N}_{\text{Num. Coeff. Mult}}\cdot\underbrace{(2Ll+L+1)\log_2 N}_{\approx\log_2 q}$$

- baseline RLWE (Direct Convolution, $t\approx N$):

$$\text{Cost}_{rd}\approx \overbrace{LN^{2l-1}\log_2 N}^{\text{Num. Coeff. Mult}}\cdot\overbrace{((L(l+1)+L+1)\log_2 N+\underbrace{(L(l-1))\log_2 C)}_{\leq 0}}^{\approx\log_2 q}$$

- multivariate RLWE ($t\approx N$):

$$\text{Cost}_{mr}\approx \underbrace{LlN^l\log_2 N}_{\text{Num. Coeff. Mult}}\cdot\underbrace{(2Ll+l+L)\log_2 N}_{\approx\log_2 q}$$

Table 5: Ciphertext noise bounds for all schemes ($N_i=N, F_i=C\cdot N$, ignoring $(1+C)$ factor)

Ciphertext noise (upper bound on $\frac{\Delta}{2}$)
(baseline RLWE, NTT matrix), (linear, cyclic) $\frac{\Delta}{2}\approx 2BN^{2Ll+1}t^L$
(baseline RLWE, Dir. Conv.), (linear, cyclic) $\frac{\Delta}{2}\approx 2BC^{L(l-1)}N^{L(l+1)+1}t^L$
(m-/packed RLWE),(linear, cyclic) $\frac{\Delta}{2}\approx 2BN^{2Ll+l}t^L$

- "packed" RLWE ($t\approx N^l$):

$$\text{Cost}_{pr}\approx \underbrace{LlN^l\log_2 N}_{\text{Num. Coeff. Mult}}\cdot\underbrace{(3Ll+l)\log_2 N}_{\approx\log_2 q}$$

By ignoring the effect of the logarithmic terms and considering that F is not a very small filter, this gives the following approximate ratios:

$$\frac{\text{Cost}_{rd}}{\text{Cost}_{rn}}\approx N^l,\quad \frac{\text{Cost}_{mr}}{\text{Cost}_{rn}}\approx l,\quad \frac{\text{Cost}_{pr}}{\text{Cost}_{rn}}\approx l,\quad \frac{\text{Cost}_{pr}}{\text{Cost}_{mr}}\approx\frac{3}{2}$$

Hence, we can see that the baseline RLWE algorithm still gives a reduction factor in cost linear in the number of dimensions with respect to m-RLWE and packed-RLWE. However, it must be noted that the bit security of both m-RLWE and, especially, packed-RLWE is higher than baseline RLWE; in fact, this security also increases with l (see Tables 1(a), 1(b), 1(c) and 1(d)).

B.1 Some additional considerations

There are some considerations on the effect of the performed approximations in the computed costs Cost_{rn} to Cost_{pr}. Cost_{rd} can be much smaller than the obtained approximation when the filter

is very small (i.e., C very close to zero). As we discuss in Section 5, for a small enough filter, the factor $\log_2 q$ can become so small that it compensates the higher number of coefficient multiplications of baseline RLWE compared to the other methods.

The main difference between Cost_{mr} and Cost_{pr} relies on the need of a higher t with packed-RLWE. This imposes more costly coefficient multiplications due to the higher ciphertext noise. Additionally, the obtained cost measures do not take into account the pre-/post-coding stage introduced by packed-RLWE before/after encryption/decryption, which is not needed in m-RLWE, but this step is negligible when compared to the encryption/decryption complexity.

The cost of the baseline RLWE scheme (Cost_{rn}) can be much higher when coefficient addition is not fast enough, as the previous expressions do not take into account the cost of ciphertext additions required for the NTT/INTT matrix computations. Hence, we introduce now this factor. The number of ciphertext additions required in baseline RLWE (with NTT matrix computation) is roughly 3 times $N^{2(l-1)}$ per level (2 NTTs of $l-1$ dimensions and 1 INTT of $l-1$ dimensions). It has an order higher than the maximum exponent in Cost_{mr} and Cost_{pr}; depending on the cost of ciphertext addition, this dependency can make the baseline algorithm slower than m-RLWE and packed-RLWE. In fact, assuming that the cost of addition per coefficient is roughly $O(\log_2 q)$, we can see that the asymptotic cost of multivariate and "packed" RLWE is smaller, even for a higher security level than that of baseline RLWE. We have

$$\begin{aligned}\text{Cost}^*_{rn} \approx\ & \underbrace{L(1+C)^{2l-1}N^{2l-1}}_{\text{Num. Coeff. Adds.}} \cdot \underbrace{(Ll+L+1)\log_2 N}_{\approx \log_2 q} \\ \approx\ & LN^{2l-1}\cdot(Ll+L+1)\log_2 N,\end{aligned}$$

where Cost^*_{rn} represents the cost that the ciphertext additions in the NTT/INTT transforms incur on for baseline RLWE with NTT matrix computation, that adds up to the previous Cost_{rn} to obtain the total cost.

Again, taking the most significant factors into account, and considering that F is not a very small filter, we obtain the following approximate ratios

$$\frac{\text{Cost}_{rd}}{\text{Cost}^*_{rn}} \approx \log_2 N, \quad \frac{\text{Cost}_{mr}}{\text{Cost}^*_{rn}} \approx \frac{l\log_2 N}{N^{l-1}}, \quad \frac{\text{Cost}_{pr}}{\text{Cost}^*_{rn}} \approx \frac{l\log_2 N}{N^{l-1}}.$$

REFERENCES

[1] January 2016. Recommendation for Key Management, Part 1: General. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf.

[2] Carlos Aguilar-Melchor, Joris Barrier, Laurent Fousse, and Marc-Olivier Killijian. 2016. XPIR : Private Information Retrieval for Everyone. *PoPETs* 2016, 2 (2016), 155–174.

[3] Carlos Aguilar-Melchor, Marc-Olivier Killijian, Cédric Lefebvre, and Thomas Ricosset. 2018. A Comparison of the Homomorphic Encryption Libraries HElib, SEAL and FV-NFLlib. In *SecITC 2018*. 425–442.

[4] Martin R. Albrecht, Benjamin R. Curtis, Amit Deo, Alex Davidson, Rachel Player, Eamonn W. Postlethwaite, Fernando Virdia, and Thomas Wunderer. 2018. Estimate All the {LWE, NTRU} Schemes!. In *SCN*. 351–367.

[5] Martin R. Albrecht, Rachel Player, and Sam Scott. 2015. On the concrete hardness of Learning with Errors. *J. Mathematical Cryptology* 9, 3 (2015), 169–203.

[6] Jean-Claude Bajard, Julien Eynard, M. Anwar Hasan, and Vincent Zucca. 2016. A Full RNS Variant of FV Like Somewhat Homomorphic Encryption Schemes. In *SAC 2016*. 423–442.

[7] T. Bianchi, A. Piva, and M. Barni. 2009. On the Implementation of the Discrete Fourier Transform in the Encrypted Domain. *IEEE Trans. on Information Forensics and Security* 4, 1 (March 2009), 86–97.

[8] T. Bianchi, A. Piva, and M. Barni. 2010. Composite Signal Representation for Fast and Storage-Efficient Processing of Encrypted Signals. *IEEE Trans. on Inf. Forensics & Sec.* 5, 1 (March 2010), 180–187.

[9] Carl Bootland, Wouter Castryck, and Frederik Vercauteren. 2018. On the Security of the Multivariate Ring Learning with Errors Problem. *IACR Cryptology ePrint Archive* 2018 (2018), 966.

[10] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. 2014. (Leveled) Fully Homomorphic Encryption without Bootstrapping. *ACM Trans. Comput. Theory* 6, 3, Article 13 (July 2014), 13:1–13:36 pages.

[11] Hao Chen and Kyoohyung Han. 2018. Homomorphic Lower Digits Removal and Improved FHE Bootstrapping. In *EUROCRYPT 2018*. 315–337.

[12] Jung Hee Cheon, Kyoohyung Han, Andrey Kim, Miran Kim, and Yongsoo Song. 2018. Bootstrapping for Approximate Homomorphic Encryption. In *EUROCRYPT 2018*. 360–384.

[13] Jung Hee Cheon and Andrey Kim. 2018. Homomorphic Encryption for Approximate Matrix Arithmetic. Cryptology ePrint Archive, Report 2018/565. https://eprint.iacr.org/2018/565.

[14] Jung Hee Cheon, Andrey Kim, Miran Kim, and Yong Soo Song. 2017. Homomorphic Encryption for Arithmetic of Approximate Numbers. In *ASIACRYPT 2017*. 409–437.

[15] Jung Hee Cheon, Andrey Kim, and Donggeon Yhee. 2018. Multi-dimensional Packing for HEAAN for Approximate Matrix Arithmetics. *IACR Cryptology ePrint Archive* 2018 (2018), 1245.

[16] Jung Hee Cheon, Duhyeong Kim, Yongdai Kim, and Yongsoo Song. 2018. Ensemble Method for Privacy-Preserving Logistic Regression Based on Homomorphic Encryption. *IEEE Access* 6 (2018), 46938–46948.

[17] Yarkin Doröz, Gizem S. Çetin, and Berk Sunar. 2016. On-the-fly Homomorphic Batching/Unbatching. In *Financial Cryptography and Data Security*. 288–301.

[18] J. Fan and F. Vercauteren. 2012. Somewhat Practical Fully Homomorphic Encryption. Crypt. ePrint Archive, Report 2012/144.

[19] Ran Gilad-Bachrach, Nathan Dowlin, Kim Laine, Kristin E. Lauter, Michael Naehrig, and John Wernsing. 2016. CryptoNets: Applying Neural Networks to Encrypted Data with High Throughput and Accuracy. In *ICML*. 201–210.

[20] David Harvey. 2014. Faster arithmetic for number-theoretic transforms. *J. Symb. Comput.* 60 (2014), 113–119.

[21] R. L. Lagendijk, Z. Erkin, and M. Barni. 2013. Encrypted Signal Processing for Privacy Protection. *IEEE SP Mag.* 30, 1 (2013), 82–105.

[22] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. 2013. A Toolkit for Ring-LWE Cryptography. In *Advances in Cryptology - EUROCRYPT*. 35–54.

[23] Manoranjan Mohanty, Ming Zhang, Muhammad Rizwan Asghar, and Giovanni Russello. 2018. PANDORA: Preserving Privacy in PRNU-Based Source Camera Attribution. In *IEEE TrustCom/BigDataSE*. 1202–1207.

[24] M. Mohanty, M. Zhang, M. R. Asghar, and G. Russello. 2019. e-PRNU: Encrypted Domain PRNU-Based Camera Attribution for Preserving Privacy. *IEEE Transactions on Dependable and Secure Computing* (2019), 1–1.

[25] H. Murakami. 2000. Generalization of the cyclic convolution system and its applications. In *IEEE ICASSP'00*, Vol. 6. 3351–3353.

[26] H.J. Nussbaumer. 1982. *Fast Fourier Transform and Convolution Algorithms*. Springer.

[27] P. Paillier. 1999. Public-key Cryptosystems Based on Composite Degree Residuosity Classes. In *EUROCRYPT'99*. Springer, 223–238.

[28] Alberto Pedrouzo-Ulloa, Miguel Masciopinto, Juan Ramón Troncoso-Pastoriza, and Fernando Pérez-González. 2018. Camera Attribution Forensic Analyzer in the Encrypted Domain. In *IEEE WIFS*. 1–7.

[29] A. Pedrouzo-Ulloa, J. R. Troncoso-Pastoriza, and F. Pérez-González. 2015. Multivariate Lattices for Encrypted Image Processing. In *IEEE ICASSP 2015*. 1707–1711.

[30] A. Pedrouzo-Ulloa, J. R. Troncoso-Pastoriza, and F. Pérez-González. 2016. Image Denoising in the Encrypted Domain. In *IEEE WIFS 2016*. 1–6.

[31] Alberto Pedrouzo-Ulloa, Juan Ramón Troncoso-Pastoriza, and Fernando Pérez-González. 2016. On Ring Learning with Errors over the Tensor Product of Number Fields. *CoRR* abs/1607.05244 (2016). arXiv:1607.05244 http://arxiv.org/abs/1607.05244

[32] Alberto Pedrouzo-Ulloa, Juan Ramón Troncoso-Pastoriza, and Fernando Pérez-González. 2017. Multivariate Cryptosystems for Secure Processing of Multidimensional Signals. *CoRR* abs/1712.00848 (2017). arXiv:1712.00848 http://arxiv.org/abs/1712.00848

[33] A. Pedrouzo-Ulloa, J. R. Troncoso-Pastoriza, and F. Pérez-González. 2017. Number Theoretic Transforms for Secure Signal Processing. *IEEE Transactions on Information Forensics and Security* 12, 5 (May 2017), 1125–1140.

[34] J.R. Troncoso-Pastoriza, D. Gonzalez-Jimenez, and F. Perez-Gonzalez. 2013. Fully Private Noninteractive Face Verification. *IEEE Trans. on Information Forensics and Security* 8, 7 (July 2013), 1101–1114.

[35] J.R. Troncoso-Pastoriza, S. Katzenbeisser, M. Celik, and A. Lemma. 2007. A Secure Multidimensional Point Inclusion Protocol. In *9th ACM Workshop on Multimedia & Security*. 109–120.

[36] J.R. Troncoso-Pastoriza and F. Perez-Gonzalez. 2011. Secure Adaptive Filtering. *IEEE Transactions on Information Forensics and Security* 6, 2 (June 2011), 469–485.

[37] Peijia Zheng and Jiwu Huang. 2018. Efficient Encrypted Images Filtering and Transform Coding With Walsh-Hadamard Transform and Parallelization. *IEEE Trans. Image Processing* 27, 5 (2018), 2541–2556.