Multivariate Lattices for Encrypted Image Processing

Alberto Pedrouzo-Ulloa, Juan Ramón Troncoso-Pastoriza and Fernando Pérez-González
Signal Theory and Communications Department
University of Vigo
36310 Vigo, Spain
{apedrouzo,troncoso,fperez}@gts.uvigo.es

***Abstract*—Images are inherently sensitive signals that require privacy-preserving solutions when processed in an untrusted environment, but their efficient encrypted processing is particularly challenging due to their structure and size. This work introduces a new cryptographic hard problem called m-RLWE (multivariate Ring Learning with Errors) extending RLWE. It gives support to lattice cryptosystems that allow for encrypted processing of multidimensional signals. We show an example cryptosystem and prove that it outperforms its RLWE counterpart in terms of security against basis-reduction attacks, efficiency and cipher expansion for encrypted image processing.**

***Index Terms*—Security, Image Encryption, Lattice Cryptography, Homomorphic Processing**

I. Introduction

The emerging field of Secure Signal Processing has aimed at efficient privacy-preserving solutions for secure processing of sensitive signals [1]. Among these, images are especially challenging, mainly due to their high size, but there are many image processing scenarios where privacy plays a prominent role: biometric recognition, medical imaging (e.g., Magnetic Resonance Imaging - MRI, Computerized Tomography scans,...), social media sharing or videosurveillance are examples where images hold very sensitive information, and must be protected when processed in untrusted environments (like outsourced scenarios and cloud service providers).

Homomorphic encryption, and especially additive schemes like Paillier's [2], have been extensively used for implementations of encrypted linear transforms and typical signal processing primitives [3]. Following Gentry's breakthrough in Fully Homomorphic Encryption (FHE) [4], some recent works [5] use Somewhat or Fully Homomorphic cryptosystems to enable the simultaneous use of fully encrypted signals and transform coefficients. All these solutions present a high cipher expansion (ratio between cipher size and clear text size) that has been partially mitigated with techniques like packing several clear text inputs into one cipher [6], [7]. These techniques lack flexibility and are not optimized to work with images, still suffering from a high expansion and an overhead for packing and unpacking steps. To the best of our knowledge, there is no prior work that exploits image structure to design a low-expansion and efficient encrypted image processing solution.

This paper proposes a new cryptosystem that exploits the polynomial structure of lattice-based schemes and their relation with images to enable very efficient encrypted image operations with a high security and low cipher expansion. We also propose an extension of Ring Learning with Errors (RLWE), denoted m-RLWE, to design lattice-based image cryptosystems and exemplify some encrypted image processing primitives with our solution. Additionally, the proposed cryptosystem also provides a simple way to perform the above operations for higher-dimensional signals (like 3-D imaging).

Notation and structure: We represent vectors by boldface lowercase letters. Polynomials are denoted with regular lowercase letters, ignoring the polynomial variable (e.g., a instead of $a(x)$) whenever there is no ambiguity. For the sake of clarity, we indicate the variable(s) of polynomial rings, following a recursive definition of multivariate modular rings: $R_q[x] = \mathbb{Z}_q[x]/(f(x))$ denotes the polynomial ring in the variable x modulo $f(x)$ with coefficients belonging to $\mathbb{Z}_q$. Analogously, $R_q[x,y] = (R_q[x])[y]/(f'(y))$ is the bivariate polynomial ring with coefficients belonging to $\mathbb{Z}_q$ reduced modulo $f(x)$ and $f'(y)$. In general, $R_q[x_1,\ldots,x_m]$ represents the corresponding multivariate polynomial ring with coefficients in $\mathbb{Z}_q$ and the m modular functions $f_i(x_i)$ with $1 \leq i \leq m$ (we will assume all modular functions are cyclotomic polynomials of order 2^{k_i}). Finally, $\boldsymbol{a} \cdot \boldsymbol{s}$ is the scalar product between the vectors $\boldsymbol{a}, \boldsymbol{s} \in R_q^l[x]$.

The rest of the paper is organized as follows: Lattices and RLWE are revisited in Section II. Section III introduces the m-RLWE problem and our proposed new cryptosystem. Section IV exemplifies the implementation of several encrypted image processing operations, and Section V evaluates their security and efficiency.

II. Preliminaries - Ring Learning with Errors

The advent of fully homomorphic lattice-based cryptosystems allows both homomorphic additions and multiplications, overcoming some limitations of traditional additive homomorphic cryptosystems like Paillier's [2]. The state of the art in FHE is based on the Learning with Errors (LWE) and Ring Learning with Errors (RLWE) problems [8], which have proven security reductions to hard lattice problems. Recent advances in RLWE leveled cryptosystems [9], which enable the homomorphic execution of a bounded-degree polynomial function, produce the currently most efficient FHE systems.

Both RLWE and LWE have a similar formulation, that Brakerski *et al.* generalize to a common General Learning with Errors (GLWE) problem. We recall a slightly adapted informal definition of GLWE, as the basis for our proposals introduced in the next sections:

Definition 1 (GLWE problem [9]): Given a security parameter λ, an integer dimension $l = l(\lambda)$, two univariate polynomial rings $R[x] = \mathbb{Z}[x]/(f(x))$, $R_q[x] = \mathbb{Z}_q[x]/(f(x))$ with $f(x) = x^n + 1$, $q = q(\lambda)$ a prime integer, and $n = n(\lambda)$ a power of two, and an error distribution $\chi[x] \in R_q[x]$ that generates small-norm random univariate polynomials in $R_q[x]$, $\text{GLWE}_{l,f,q,\chi}$ relies upon the computational indistinguishability between pairs of samples $(\boldsymbol{a}_i, b_i = \boldsymbol{a}_i \cdot \boldsymbol{s} + t \cdot e_i)$ and $(\boldsymbol{a}_i, u_i)$, where $\boldsymbol{a}_i \leftarrow R_q^l[x]$, $u_i \leftarrow R_q[x]$ are chosen uniformly at random, $\boldsymbol{s} \leftarrow \chi^l[x]$ and $e_i \leftarrow \chi[x]$ are drawn from the error distribution, and t is an integer relatively prime to q.

When $n = 1$, GLWE becomes the standard $\text{LWE}_{l,q,\chi}$, and when $l = 1$ it boils down to $\text{RLWE}_{q,f,\chi}$. LWE-based cryptosystems are computationally demanding, reason why RLWE was defined as an algebraic version of LWE, trading subspace dimensionality by polynomial ring order (using an ideal ring), achieving huge efficiency improvements. As for the generic GLWE ($n > 1$ and $l > 1$), Brakerski *et al.* [9] speculate that it is hard for $n \cdot l = \Omega(\lambda \log(q/B))$, where B is a bound on the length of the elements output by $\chi[x]$. It must be noted that despite the efficiency improvement, there are no known attacks in RLWE that get a substantial advantage with

respect to attacks to LWE. Consequently, the currently most efficient homomorphic cryptosystems are based on RLWE, especially the ones proposed by Brakerski *et al.* [9], [10] and Lauter *et al.* [11]. For a formal definition of the GLWE problem and proofs of security reductions for RLWE and LWE, we refer the reader to [8], [9], [12].

III. Proposed Scheme

The underlying contribution of this paper is a generalization of RLWE to multivariate polynomial rings, with the specific application to 2D-image encryption using a cryptosystem based on the bivariate version of RLWE. Hence, we start by defining the bivariate RLWE problem as a modification of GLWE, in order to later generalize it to m-variate polynomial rings (m-RLWE), and finally present a modification of Lauter *et al.* cryptosystem [11] based on m-RLWE. We choose Lauter's scheme due to its efficiency, but any other RLWE-based cryptosystem can be extended to the m-RLWE problem by following the introduced procedure.

A. Multivariate RLWE

We begin with the bivariate version of RLWE, which can be achieved by substituting the polynomial ring by a bivariate one $R_q[x,y] = (R_q[x])[y]/(f'(y))$, such that the error distribution $\chi[x,y]$ generates also low-norm bivariate polynomials from $R_q[x,y]$:

Problem 1 (Bivariate RLWE (2-RLWE)): Given a bivariate polynomial ring $R_q[x,y]$ with $f(x) = x^{n_1}+1, f'(y) = y^{n_2}+1$ and an error distribution $\chi[x,y] \in R_q[x,y]$ that generates small-norm random bivariate polynomials in $R_q[x,y]$, 2-RLWE relies upon the computational indistinguishability between samples $(a_i, b_i = a_i \cdot s + t \cdot e_i)$ and (a_i, u_i), where $a_i,\ u_i \leftarrow R_q[x,y]$ are chosen uniformly at random from the ring $R_q[x,y]$, and $s, e_i \leftarrow \chi[x,y]$ are drawn from the error distribution, and t is relatively prime to q.

Informally, 2-RLWE is to GLWE what RLWE is to LWE, as we are trading (for a second time) subspace dimensionality for a higher polynomial ring degree, therefore increasing the security of regular RLWE and improving on performance with respect to GLWE.

The dimensionality of the noise distribution is now $n = n_1 \cdot n_2$, and we preserve most of the relevant properties of the used ideals by considering the bivariate rings as the tensor product (as R-modules) of the ring of integers of a cyclotomic field. Also, for the coefficient embedding the ideal lattices equivalent to this product ring are generated by block negacyclic matrices of size $n_1 \times n_2$ [13]. We now enunciate the following proposition about the security of the new problem:

Proposition 1: The 2-RLWE problem with $n_x = n$ and $n_y = l$ is equivalent to RLWE with $n_z = l \cdot n$.

We sketch the proof of Prop. 1 (an extended proof can be found in [14]) by using a polyphase decomposition of the involved signals, with the particularity that due to the cryptosystem requirements, which assume polynomials modulo $1 + z^n$, we must work with negacyclic convolutions [13], denoted here by $\circledast$.

Let us consider a typical RLWE sample $(a, b = a \cdot s + e)$, where $a, b \leftarrow R_q[z]$ with $f(z) = z^{ln} + 1$ and $e \leftarrow \chi[z]$. We can write the polynomial $b(z) = \sum_{k=0}^{l-1} z^k b_k(z^l)$ as its decomposition according to its l first polyphase components $b_k(z)$, where

$$b_k(z) = \sum_{m=0}^{n-1} ((a[lm+k] \circledast s[lm+k]) + e[lm+k])z^m. \quad (1)$$

Hence, each RLWE sample can be represented as a set of l equations with $(n-1)$-degree polynomials. Next, we consider a 2-RLWE sample $(a, b = a \cdot s + e)$ with $a, s \leftarrow R_q[x,y]$, $e \leftarrow \chi[x,y]$, $f_x(x) = x^n + 1$ and $f_y(y) = y^l + 1$.

If we denote the coefficients of y^k for each signal as $a_k(x)$, $b_k(x)$, $s_k(x)$, $e_k(x)$, we have the following expression for $0 \le k < l$:

$$b_k(x) = e_k(x) + \sum_{i+j=k} a_i(x)s_j(x) - \sum_{i+j=n+k} a_i(x)s_j(x).$$

Now, if we apply to each $b_k(x)$ the reverse procedure of the polyphase decomposition, we have:

$$b_k(x) = \sum_{m=0}^{n-1} (a'_k[lm] \circledast s'_k[lm])x^m + e_k(x), \quad (2)$$

where the polynomials $a'_k(x)$ and $s'_k(x)$ have as coefficients the different possible concatenations of $a_i(x)$ and $s_j(x)$ respectively; that is, it is a polyphase decomposition in which the coefficients are shuffled in blocks prior to extraction of each phase [14].

Comparing Eqs (1) and (2) as equivalent ways of expressing the RLWE and 2-RLWE distributions respectively, the only difference between both lies in the coefficient ordering of the used s, e and a. Since s and e have a symmetrical distribution and a is uniformly chosen, the distribution of both problems is exactly the same. Therefore, if we solve 2-RLWE, we can also solve RLWE, because both can be expressed equivalently without reducing the entropy of the original problems.

Resorting to the recursive definition of multivariate polynomial rings (cf. Section I), the Bivariate RLWE problem can be seamlessly extended to multivariate polynomials (m-RLWE) with $m > 2$, recursively applying the sketched modification to the general GLWE problem. The formulation is analogous to 2-RLWE with rings $R[x_1, \ldots, x_m]$ and $R_q[x_1, \ldots, x_m]$ and error distribution $\chi[x_1, \ldots, x_m]$, so we do not replicate it again here.

Proposition 2: The m-RLWE problem with n_i and $f(x_i) = 1 + x_i^{n_i}$ for $i = 1, \ldots, m$ is equivalent to RLWE with $n = \prod n_i$.

Whenever the cyclotomic polynomials in each variable x_i have the form $1 + x_i^{n_i}$, the same procedure sketched above for proving Prop. 1 can be applied to prove the equivalence of m-RLWE and the $(m-1)$-RLWE distributions, by "folding" two variables of the former into one variable of the latter. Therefore, Prop. 2 can be proven by induction; the extended version of this proof can be found in [14].

B. An m-RLWE based Cryptosystem

Any cryptosystem whose security is based on RLWE (e.g., [9], [10], [11]) could be extended to m-RLWE. We choose Lauter *et al.*'s [11], due to its efficiency and security, as a basis to exemplify our semantically secure m-RLWE cryptosystem. Table I summarizes its parameters and primitives.

Ciphertexts are composed by $\gamma \ge 2$ ring elements from $R_q[x_1, \ldots, x_m]$. This size increases with each multiplication (see Table I), and it can be brought back to the size of a fresh cipher by means of a relinearization step, which involves using partial encryptions of the secret key (more details can be found in [9], [11]).

Security and Correctness: The security of the cryptosystem is based on the computational difficulty of reducing the n-dimensional lattice ($n = \prod n_i$) generated by the secret key, and the semantic security guaranteed by the underlying m-RLWE problem (two encryptions of the same or different plaintexts cannot be distinguished). As for correctness, q must be set such that enough space is guaranteed to avoid decryption errors produced by wrap-arounds of the performed homomorphic operations. Due to the analogous (not isomorphic) structure of m-RLWE with $n = \prod n_i$ and degree-n RLWE (cf. Section III-A), bounds for the error norm [11] are preserved when switching from RLWE to m-RLWE, by adjusting the increased

TABLE I
PROPOSED CRYPTOSYSTEM: PARAMETERS AND PRIMITIVES

Parameters		
Let $R_t[x_1,\ldots,x_m]$ be the cleartext ring and $R_q[x_1,\ldots,x_m]$ as ciphertext's. The noise distribution $\chi[x_1,\ldots,x_m]$ in $R_q[x_1,\ldots,x_m]$ takes its coefficients from a spherically-symmetric truncated i.i.d Gaussian $\mathcal{N}(\mathbf{0},\sigma^2\boldsymbol{I})$. q is a prime $q \equiv 1 \mod 2n$ (with $n=\prod n_i$), and $t<q$ is relatively prime to q.		
Cryptographic Primitives		
SH.KeyGen	Process	$s,e \leftarrow \chi[x_1,\ldots,x_m]$, $a_1 \leftarrow R_q[x_1,\ldots,x_m]$ $sk=s$ and $pk=(a_0=-(a_1s+te),a_1)$
SH.Enc	Input	$pk=(a_0,a_1)$ and $m \leftarrow R_t[x_1,\ldots,x_m]$
	Process	$u,f,g \leftarrow \chi[x_1,\ldots,x_m]$ and the fresh ciphertext is $\boldsymbol{c}=(c_0,c_1)=(a_0u+tg+m, a_1u+tf)$
SH.Dec	Input	sk and $\boldsymbol{c}=(c_0,c_1,\ldots,c_{\gamma-1})$
	Process	$m=\left(\left(\sum_{i=0}^{\gamma-1} c_i s^i\right) \mod q\right) \mod t$
SH.Add	Input	$\boldsymbol{c}_0=(c_0,\ldots,c_{\beta-1})$ and $\boldsymbol{c}_1=(c'_0,\ldots,c'_{\gamma-1})$
	Process	$\boldsymbol{c}_{add}=(c_0+c'_0,\ldots,c_{\max(\beta,\gamma)-1}+c'_{\max(\beta,\gamma)-1})$
SH.Mult	Input	$\boldsymbol{c}_0=(c_0,\ldots,c_{\beta-1})$ and $\boldsymbol{c}_1=(c'_0,\ldots,c'_{\gamma-1})$
	Process	Using a symbolic variable v their product is $\left(\sum_{i=0}^{\beta-1} c_i v^i\right)\cdot\left(\sum_{i=0}^{\gamma-1} c'_i v^i\right)=\sum_{i=0}^{\beta+\gamma-2} c''_i v^i$

dimensionality of the ring elements: for D successive products and A sums, the needed q for correct decryption is lower-bounded by

$$q \geq 4(2t\sigma^2\sqrt{n_1n_2\ldots n_m})^{D+1}(2n_1n_2\ldots n_m)^{D/2}\sqrt{A}. \quad (3)$$

IV. ENCRYPTED IMAGE PROCESSING WITH 2-RLWE

Unlike RLWE-based cryptosystems, which lack support for multi-dimensional signals, the proposed cryptosystem introduces a natural way to work with multidimensional linear operations. Additionally, it achieves a more compact representation of the data, as it can effectively cipher one signal value per coefficient of the encryption polynomial. This section exemplifies the implementation of different representative encrypted processing like convolution, correlation or filtering, showing the advantages of the proposed cryptosystem compared to its RLWE-based counterpart. Unless otherwise stated, we will always consider that all the used signals and filters are encrypted, to fully conceal all the involved elements in an untrusted environment.

Convolution, correlation and filtering can all be expressed as a linear convolution between two m-dimensional signals $\boldsymbol{X}$ and $\boldsymbol{H}$, namely $\boldsymbol{Y}[n_1,\ldots,n_m]=\boldsymbol{X}[n_1,\ldots,n_m]*\boldsymbol{H}[n_1,\ldots,n_m]$, which is equivalent to the ring product of the signals represented as multivariate polynomials $y(z_1,\ldots,z_m)=x(z_1,\ldots,z_m)\cdot h(z_1,\ldots,z_m)$.

Using the original RLWE-based scheme, an encrypted convolution would comprise encoding each dimension separately as elements of the univariate polynomial ring $R_t[z]$, resulting in two $(m-1)$-dimensional elements $\boldsymbol{X}_{n_1,\ldots,n_{m-1}}(z)$ and $\boldsymbol{H}_{n_1,\ldots,n_{m-1}}(z)$ of $R_t^{m-1}[z]$. If $N_{n_i,y}$ is the number of samples in dimension n_i for the signal y, the number of involved polynomial products is $\prod_{i=1}^{m-1} N_{n_i,x}N_{n_i,h}$ (i.e., $N^{2(m-1)}$ products if $N_{n_i,x}=N_{n_i,h}=N$).

Contrarily, with our proposed cryptosystem the convolution can be done through a single polynomial product of the encryptions, homomorphic to the polynomial product of the clear text. Particularly, an encrypted image convolution with the proposed cryptosystem would translate into the product of two bivariate polynomial encryptions.

Complex signals: Complex numbers are usually encrypted by separating real and imaginary parts in two independent ciphers, and performing complex products as four real products. But m-RLWE can naturally incorporate one extra variable for the polynomial ring $\mathbb{Z}_t[w]/(w^2+1)$, isomorphic to the complex integers ring, where the variable w plays the role of the imaginary unit. While the computational cost of complex operations would not be affected, this is a more compact and integrated representation of encrypted complex signals, and it effectively doubles the size of the secret key accordingly, therefore increasing the security of the scheme.

V. SECURITY AND PERFORMANCE EVALUATION

In terms of security, we address the distinguishing attack [15] aimed at breaking the indistinguishability assumption through basis reduction algorithms, and we follow the procedure of [11]. Decoding attacks (aimed at getting the secret key s) are not included due to space limitations, but values for $n=\prod n_i$ similar to those used in [11] can achieve protection against decoding attacks as described in [16]; we will therefore adhere to these minimum values for n.

We take the root Hermite factor δ for the underlying lattice as a measure of security, as it is directly related to the running time needed for a basis-reduction algorithm to succeed. We briefly comment on the relation between the cryptosystem parameters and δ, and then compare it with its RLWE counterpart [11] in terms of root Hermite factor and computational load for encrypted image filtering.

A. Security as a function of the root Hermite factor δ

The best attacks against lattice-based cryptosystems are grounded on basis reduction, which tries to obtain a nearly orthogonal basis with small vectors from an arbitrary basis. BKZ [17] is currently one of the most efficient algorithms, which uses blocks of size ranging from 2 to the dimension of the lattice; increasing block sizes produce better bases at the cost of a higher computational load. The root Hermite factor $\delta > 1$ drives the complexity of reduction attacks on the lattice, such that the run time of an attack is approximately proportional to $e^{k/\log\delta}$ for a constant k: lower δ means higher security. For the optimal distinguishing attack using BKZ, the runtime yields the following expression in terms of δ [11]

$$\log_2(\delta)=(\log_2(c\cdot q/s))^2/(4n\log_2(q)), \quad (4)$$

where n is the rank of the lattice, $c\approx\sqrt{\ln(\frac{1}{\epsilon})/\pi}$, ϵ is the attacker advantage (taken as $\epsilon=2^{-32}$), and s is a scale parameter of the error distribution (for an n-dimensional Gaussian, $s=\sigma\sqrt{2\pi}$).

A lower δ is achieved with a lower s (producing shorter lattice vectors), due to the evolution of the ratio q/s. With the bound for q given by (3), and ignoring all the factors independent from s, it can be shown that asymptotically $\frac{q}{s}\propto\frac{s^{2D+2}}{s}=s^{2D+1}$. Therefore, in (4) both δ and q increase when s grows, producing an additional tradeoff for s, that should be small to better resist reduction attacks, but large enough to give enough randomness to avoid birthday attacks.

B. Evaluation for Encrypted Image Processing

We consider two privacy-preserving scenarios: the encrypted correlation of two encrypted images of size $N\times N$, and the encrypted filtering of an image of size $N\times N$ by a filter of size $F\times F$, with $F<N$, and we compare security and complexity for our 2-RLWE cryptosystem versus the RLWE counterpart [11]. Therefore, we fix $s=2\sqrt{n}$, $t=256$ and $D=1$ (each cipher undergoes one encrypted product), and a maximum value for δ, i.e., a minimum security level against reduction attacks. Hence, we use a slack variable h as the ratio between the polynomial degree n in [11] needed to achieve the maximum δ, and the length of the result in the ciphered dimension.

1) Encrypted correlation of two images: Given the image size $N\times N$, the polynomial degree to accommodate the encrypted result is $n_i\geq 2N$ (and $n\geq 2N$ for [11]), but we have to account for the needed δ given by h. We can estimate the relation between δ and the computational cost of both cryptosystems using (4) and the fact that the cost (in terms of coefficient products) is quadratic in N^2:

$$\delta_{2-RLWE}^{\frac{2N-1}{h}}\approx\delta_{Lauter}, \quad \text{cost}_{2-RLWE}\approx\frac{4}{h^2}\text{cost}_{Lauter}.$$

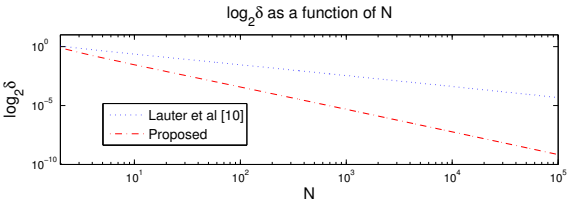

Fig. 1. Security $log_2\delta$ for encrypted correlation (equal cost, $h = 2$).

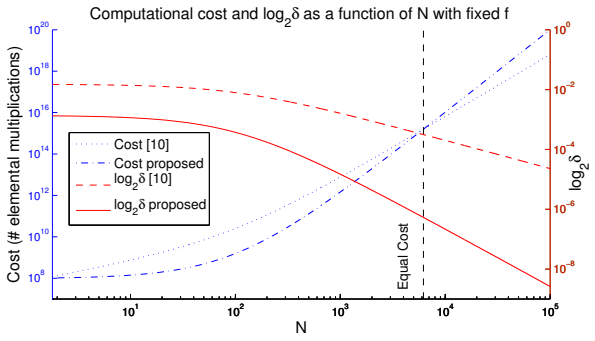

Fig. 2. Cost and $log_2\delta$ for encrypted image filtering ($F = 100, h = 8$).

When $h = 1$, Lauter encryptions would be roughly 4 times faster than ours, but 2-RLWE has a much higher security. For $h = 2$, both have a similar cost, and ours has a much higher security (Fig. 1). For $h > 2$, the proposed scheme is both more efficient and secure. Therefore, unless the security with $h = 1$ is enough for the application, the proposed scheme is more efficient and much more secure. In fact, a reasonable security level can only be achieved currently for lattices with $n \geq 4096$. Hence, for small images (e.g., size 512×512) our cryptosystem can adapt to the optimum polynomial degree keeping a very high level of security, while [11] will suffer a big cipher expansion with a much lower security level.

2) Encrypted image filtering: We can approximate the relation between cost and δ for this scenario, assuming $F \ll N$, as:

$$\delta_{2-RLWE}^{\frac{N+F-1}{h}} \approx \delta_{Lauter}, \quad \text{cost}_{2-RLWE} \approx \frac{N}{h^2 F}\text{cost}_{Lauter}.$$

Our scheme's δ_{2-RLWE} decreases exponentially with the size of the image and the filter with respect to δ_{Lauter}. As for the cost, the proposed cryptosystem is more efficient for low-size images and/or large filters, yielding a much higher security in the whole size range.

Figure 2 plots both δ and cost as a function of N using a 100-tap encrypted filter and $h = 8$. Our scheme achieves higher efficiency and lower δ for images with $N < 6200$; hence, it is more efficient and secure for a typical size range of images in practical applications.

For completeness, we also compared the cost of both schemes with a varying ratio F/N. With $h = 8$, $N+F-1 = 256$, $n_{Lauter} = 2048$ and $n_{2-RLWE} = 65536$, our scheme is more efficient for filters with more than 4 taps per dimension, as our cost, encryption size and δ_{2-RLWE} are constant for any $F < N$, while for [11], cost and q increase with F and $\sqrt{F}$ respectively, therefore increasing δ_{Lauter}.

C. Implementation and execution times

We have implemented both Lauter RLWE-based cryptosystem and our 2-RLWE extension in C using the GMP 6.0.0 [18] and FLINT 2.4.3 [19] libraries. We implemented bivariate polynomial products as a recursive embedding of polynomial coefficients in each variable, and Karatsuba multiplication algorithm for large numbers [20]. Table II compares the encrypted image filtering performance ($F = 11$) with a) our 2-RLWE cryptosystem, b) its RLWE counterpart [11] with $h = 8$, and c) the traditional Paillier (with a clear text filter), on a Core i5-4670 computer with 20 GB of RAM running Linux.

TABLE II
ENCRYPTED FILTERING PERFORMANCE ($D = 1, t = 256, s = \sqrt{2\pi}$)

N	118	246	502	1014
Proposed cryptosystem				
n	16384	65536	262144	1048576
$\lceil \log_2(q) \rceil$	43	46	49	52
Enc. image size (bits)	$1.4{\cdot}10^6$	$6.03{\cdot}10^6$	$2.57{\cdot}10^7$	$1.09{\cdot}10^8$
δ	1.00045	1.00012	1.000032	1.0000085
Encrypt. time (s)	0.031	0.144	0.673	4.127
Decrypt. time (s)	0.029	0.137	0.649	4.038
Conv. time (s)	0.058	0.275	1.299	8.047
Lauter cryptosystem ($h = 8$)				
n	1024	2048	4096	8192
$\lceil \log_2(q) \rceil$	37	39	40	42
Enc. image size (bits)	$8.94{\cdot}10^6$	$3.93{\cdot}10^7$	$1.64{\cdot}10^8$	$6.98{\cdot}10^8$
δ	1.0062	1.0037	1.0017	1.00087
Encrypt. time (s)	0.062	0.258	1.248	7.122
Decrypt. time (s)	0.038	0.214	1.053	6.200
Conv. time (s)	0.737	4.342	22.206	134.719
Paillier cryptosystem (with 2048 bit modulus)				
Enc. image size (*bits*)	$5.7 \cdot 10^7$	$2.48 \cdot 10^8$	$1.03 \cdot 10^9$	$4.21 \cdot 10^9$
Encrypt. time (s)	174	756	3150	12852
Decrypt. time (s)	205	819	3277	13107
Conv. time (s)	111	483	2011	8205

The reported encryption times comprise the encryption of all involved signals (except for Paillier, for which the filter is not encrypted), and for the lattice cryptosystems we do not include a relinearization step after each multiplication, but take into account the (more demanding) decryption of the extended encryptions instead. We can see that both lattice-based cryptosystems are far more efficient than Paillier, also having a much lower cipher expansion. Moreover, our scheme yields smaller encrypted images, by keeping a compact cipher structure that adapts to both image dimensions increasing the lattice dimensionality and, hence, the security. For typical image sizes, it is more secure and efficient than Lauter's for encryption, decryption and, especially, for the whole encrypted convolution.

VI. CONCLUSIONS

This work introduces a new hard problem called m-RLWE, generalizing RLWE, aimed at processing encrypted multidimensional signals, while improving on cipher expansion, security and efficiency. Any RLWE based cryptosystem could be extended to m-RLWE.

We provide an example cryptosystem based on m-RLWE by extending Lauter *et al*'s scheme. We show its application (in general, any scheme based on 2-RLWE) for encrypted image filtering, suggesting a compact representation for complex coefficients, supported by the cryptosystem itself. We also show the advantages of our scheme with respect to its RLWE counterpart and a clear-text filter Paillier-based implementation, in terms of security, efficiency and cipher expansion. This work opens up a broad set of encrypted image processing applications and shows the viability of somewhat homomorphic encryption for efficient privacy-preserving image processing.

ACKNOWLEDGMENTS

This work was partially funded by the Spanish Government and the European Regional Development Fund (ERDF) under projects TACTICA and COMPASS (TEC2013-47020-C2-1-R), and by the Galician Regional Government and ERDF under projects "Consolidation of Research Units" (GRC2013/009), REdTEIC (R2014/037) and AtlantTIC.

REFERENCES

[1] R. Lagendijk, Z. Erkin, and M. Barni, "Encrypted Signal Processing for Privacy Protection: Conveying the utility of homomorphic encryption and multiparty computation," *IEEE Signal Processing Magazine*, vol. 30, no. 1, pp. 82–105, Jan 2013.

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

[3] T. Bianchi, A. Piva, and M. Barni, "On the Implementation of the Discrete Fourier Transform in the Encrypted Domain," *IEEE Trans. on Information Forensics and Security*, vol. 4, no. 1, pp. 86–97, March 2009.

[4] C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," in *Proceedings of ACM STOC'09*. ACM, 2009, pp. 169–178.

[5] J. R. Troncoso-Pastoriza, D. Gonzalez-Jimenez, and F. Perez-Gonzalez, "Fully Private Noninteractive Face Verification," *IEEE Trans. on Information Forensics and Security*, vol. 8, no. 7, pp. 1101–1114, July 2013.

[6] J. R. Troncoso-Pastoriza, S. Katzenbeisser, M. Celik, and A. Lemma, "A Secure Multidimensional Point Inclusion Protocol," in *Proceedings of the 9th Workshop on Multimedia & Security*, ser. MM&Sec '07. New York, NY, USA: ACM, 2007, pp. 109–120.

[7] T. Bianchi, A. Piva, and M. Barni, "Composite Signal Representation for Fast and Storage-Efficient Processing of Encrypted Signals," *IEEE Trans. on Information Forensics and Security*, vol. 5, no. 1, pp. 180–187, March 2010.

[8] V. Lyubashevsky, C. Peikert, and O. Regev, "On Ideal Lattices and Learning with Errors over Rings," *J. ACM*, vol. 60, no. 6, pp. 43:1–43:35, Nov. 2013.

[9] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(Leveled) Fully Homomorphic Encryption without Bootstrapping," *ACM Trans. Comput. Theory*, vol. 6, no. 3, pp. 13:1–13:36, Jul. 2014.

[10] Z. Brakerski and V. Vaikuntanathan, "Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages," in *Advances in Cryptology CRYPTO 2011*, ser. LNCS, 2011, vol. 6841.

[11] K. Lauter, M. Naehrig, and V. Vaikuntanathan, "Can Homomorphic Encryption be Practical?" Cryptology ePrint Archive, Report 2011/405, 2011, http://eprint.iacr.org/.

[12] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehlé, "Classical Hardness of Learning with Errors," in *Proceedings of the ACM STOC'13*. ACM, 2013, pp. 575–584.

[13] P. J.Davis, *Circulant Matrices*. Providence, Rhode Island: American Mathematical Society, 1994.

[14] A. Pedrouzo-Ulloa, J. R. Troncoso-Pastoriza, and F. Pérez-González, "Multivariate Ring Learning with Errors," University of Vigo, Tech. Rep., September 2014, http://webs.uvigo.es/gpscuvigo/sites/default/files/publications/TRMLWE2014.pdf.

[15] D. Micciancio and O. Regev, "Lattice-based Cryptography," in *Post-Quantum Cryptography*. Springer, 2009, pp. 147–191.

[16] R. Lindner and C. Peikert, "Better Key Sizes (and Attacks) for LWE-based Encryption," in *CT-RSA'11*. Springer, 2011, pp. 319–339.

[17] Y. Chen and P. Nguyen, "BKZ 2.0: Better Lattice Security Estimates," in *Advances in Cryptology ASIACRYPT 2011*, ser. LNCS. Springer, 2011, vol. 7073, pp. 1–20.

[18] "GNU Multipe Precision Arithmetic Library," www.gmplib.org.

[19] "Fast Library for Number Theory," www.flintlib.org.

[20] D. J. Bernstein, "Fast multiplication and its applications," in *Algorithmic Number Theory*, J. P. Buhler and P. Stevenhagen, Eds. Cambridge: Cambridge University Press, 2008, vol. 44, pp. 325–384.