Multivariate Ring Learning with Errors

Technical Report UV/TSC/APU/02102014

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

This technical report introduces the expanded proofs for the propositions stated in [1], concerning the conditions of equivalence between RLWE (Ring Learning with Errors) and the introduced m-RLWE (Multivariate Ring Learning with Errors).

Index Terms

Security, Image Encryption, Lattice Cryptography, Homomorphic Processing

I. Introduction

The underlying contribution of the paper [1] is a generalization of Ring Learning With Errors (RLWE) to multivariate polynomial rings (multivariate RLWE, m-RLWE). This generalized problem is specifically applied to 2D-image encryption, through a cryptosystem based on the bivariate version of RLWE. In this technical report, we provide further details for the proofs of Proposition 1 and 2 in [1] about the 2-RLWE and m-RLWE problems, respectively. To this aim, we start with the bivariate RLWE problem and after that we generalize it to m-variate polynomial rings (m-RLWE).

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. We indicate the variable of polynomial rings to avoid confusion between univariate and multivariate 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 $1 \leq i \leq m$. Finally, $\boldsymbol{a} \cdot \boldsymbol{s}$ is the scalar product between the vectors $\boldsymbol{a}, \boldsymbol{s} \in R_q^l[x]$.

Section II of this report briefly recalls come concepts about lattices and RLWE, for the sake of completeness, and Sections III and IV detail the extended problems 2-RLWE and m-RLWE respectively, and the proofs for the conditions of equivalence between them and RLWE.

II. Preliminaries - Ring Learning with Errors

Signal Processing in the Encrypted Domain has traditionally relied on additive homomorphic cryptosystems like Paillier [2] to implement efficient encrypted signal processing. Nevertheless, the family of additively homomorphic cryptosystems is very limited, and it only allows for linear transforms or filtering with known coefficients. Gentry's seminal work on bootstrappable cryptosystems [3], together with lattice-based cryptography, has enabled the design of fully homomorphic cryptosystems that allow to perform both homomorphic additions and multiplications. The state of the art in FHE is based on the Learning with Errors (LWE) and Ring Learning with Errors (RLWE) problems [4], which have proven security reductions to hard lattice problems. Recent advances in RLWE leveled cryptosystems [5], which enable the homomorphic execution of a bounded-degree polynomial function, produce the currently most efficient FHE systems.

In particular, the RLWE problem is an algebraic variant of LWE that uses ideal lattices to improve on the feasibility of implementations. Both have a similar formulation, that Brakerski *et al.* generalize to a common General Learning with Errors (GLWE) problem. These problems are the bases on top of which the paper [1] sets up the m-RLWE problem and the image-focused cryptosystem, so we recall the informal definition of GLWE.

Definition 1 (GLWE problem [5]): 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 $R_q[x]$, the $\text{GLWE}_{l,f,q,\chi}$ problem 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 $n = 1$, the GLWE becomes the standard $\text{LWE}_{l,q,\chi}$ problem, 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), hence achieving a huge reduction on the complexity of the involved operations. As for the generic GLWE (with both $n > 1$ and $l > 1$), Brakerski *et al.* speculate that it is hard for $n \cdot l = \Omega\left(\lambda \log(q/B)\right)$, where B is a bound on the length of the elements output by $\chi[x]$. It must be noted that although RLWE seems a priori easier to attack than LWE, 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.* [5], [6] and Lauter *et al.* [7]. For a formal definition of the GLWE problem and proofs of security reductions for both RLWE and LWE, we refer the reader to [5], [4] and their extended versions.

As a particularity, and despite the possibility of working with any polynomial ring with a generic modular function, we restrict all the developments in [1] and the proofs here only to cyclotomic polynomials with degree power of two, of the form $f(x) = x^{2^k} + 1$, for an integer k. This restriction greatly simplifies the polynomial modular reduction operation, producing more efficient primitives, and it also allows us to graphically derive the proofs detailed below. We can conjecture that all the developments and proofs could be extended to any cyclotomic

polynomial, but this falls out of the scope of [1] and of this technical report.

III. BIVARIATE RLWE (2-RLWE)

The bivariate version of RLWE 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 [5] 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. Additionally, it can be seen that for the coefficient embedding the ideal lattices equivalent to this product ring are generated by block negacyclic matrices of dimension $n = n_1 \cdot n_2$. We now enunciate the following theorem about the security of the new problem:

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

For the proof of Prop. 1 we use the 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 [8], denoted here by $\circledast$.

a) RLWE sample: Let us consider a typical RLWE sample $(a, b = a \cdot s + e)$, where $a, b \in R_q[z]$ 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 $b_k(z)$ with $k = 0, 1, \ldots, l-1$, where

$$\begin{aligned} b_k(z) &= \sum_{m=0}^{n-1} b[lm+k] z^m \\ &= \sum_{m=0}^{n-1} ((a[lm+k] \circledast s[lm+k]) + e[lm+k]) z^m \end{aligned} \tag{1}$$

Hence, each RLWE sample can be represented as a set of l equations with $(n-1)$-degree polynomials, where for each polyphasic component k the coefficient of z^m satisfies:

$$b_{k,m} = e[lp+k] + [a[lp+k] \circledast s[lp+k]]_{p=m} \tag{2}$$

As the convolutions are negacyclic, each one of the nl coefficients of the RLWE sample is equal to the summation of nl different products of a_i and s_j coefficients, plus a noise sample from e. In those sums of products, the combination of the different $a_i s_j$ present in the expression for each $b_{k,m}$ (2) is unique, so we have for all equations $n^2 l^2$ different combinations of products. Figure 1 graphically shows, in matrix form, the product combinations for each polynomial coefficient.

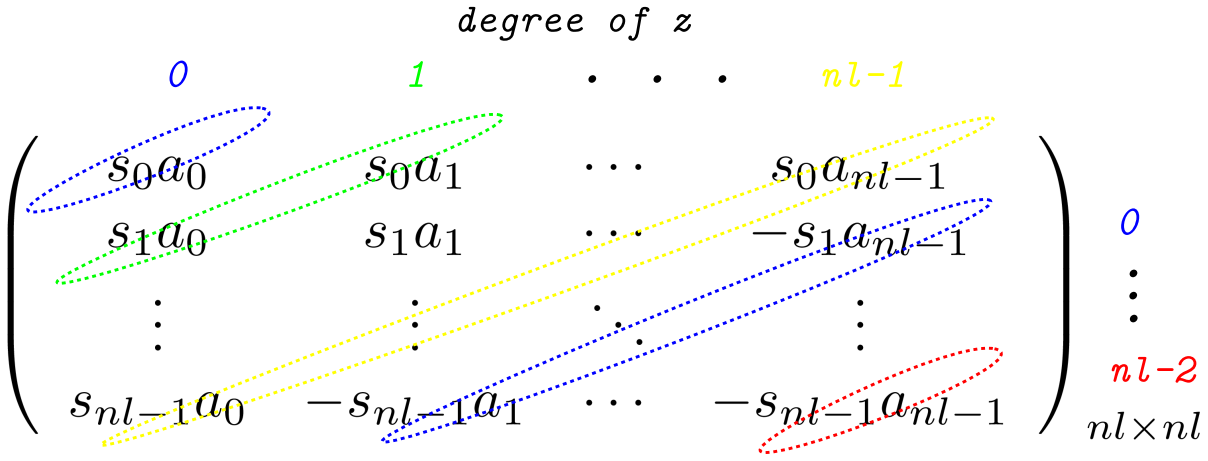

Fig. 1. Product combinations for the coefficients of a RLWE sample.

b) 2-RLWE sample: 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 of each signal with $s_k(x)$, $b_k(x)$, $e_k(x)$, $s_k(x)$ respectively, we have the following expression for $0 \leq k < l$:

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

From this point on, the sample $a_k[m]$ denotes the coefficient of x^m in $a_k(x)$. Now, if we apply to each $b_k(x)$ the reverse procedure of the polyphase decomposition, we have:

$$b_k(x) = \sum_{m=0}^{n-1} (a'_k[lm] \circledast s'_k[lm])x^m + e_k(x), \tag{3}$$

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.

Additionally, if we denote the coefficients of $y^k x^m$ with the subscripts k and m, the expression for each coefficient of the 2-RLWE sample satisfies:

$$b_{k,m} = e_{k,m} + \sum_{i+j=k} [a_i[p] \circledast s_j[p]]_{p=m} - \sum_{i+j=n+k} [a_i[p] \circledast s_j[p]]_{p=m} \tag{4}$$

At this point, we can see the parallelism between Eqs. (1), (2) and (3), (4). To show they are fully equivalent

expressions, let us build the 2-RLWE vectors $\boldsymbol{a}$ and $\boldsymbol{s}$ as the following block composition of the a_i and s_j coefficients of the RLWE sample's vectors:

$$\boldsymbol{a} = (a_0, a_1, \ldots, a_{nl-1})_{1\times nl} = (\boldsymbol{a}'_0, \boldsymbol{a}'_1, \ldots, \boldsymbol{a}'_{l-1})_{1\times nl}, \quad \boldsymbol{s} = \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{nl-1} \end{pmatrix}_{nl\times 1} = \begin{pmatrix} \boldsymbol{s}'_0 \\ \boldsymbol{s}'_1 \\ \vdots \\ \boldsymbol{s}'_{l-1} \end{pmatrix}_{nl\times 1}$$

where the involved $\boldsymbol{a}'_i$ and $\boldsymbol{s}'_i$ are respectively row and column vectors of length n. Using these vectors, Figure 2 reflects their product combinations in block matrix form, for the 2-RLWE sample.

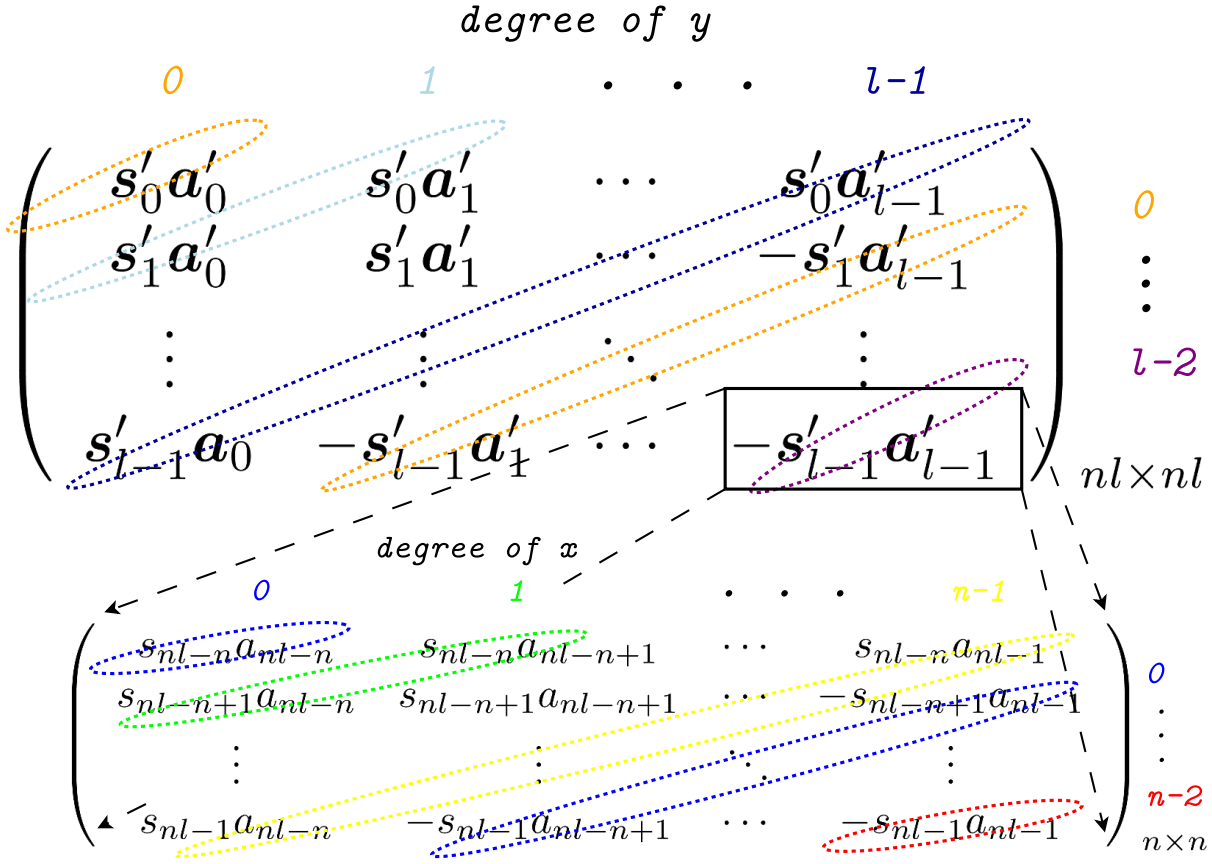

Fig. 2. Product combinations for the coefficients of a 2-RLWE sample.

On the one hand, comparing Eqs (1) and (3) 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 $\boldsymbol{s}$, $\boldsymbol{e}$ and $\boldsymbol{a}$.

On the other hand, the coefficients of the 2-RLWE sample (4) correspond to the summation of the different products of the coefficients of a and s, plus a noise sample. As the signal blocks $a_i[m]$ and $s_i[m]$ don't share any sample with the other blocks $a_j[m]$ and $s_j[m]$ for $j \neq i$ respectively, and all the negacyclic convolutions are performed between different blocks, we can see that all the product combinations are different. Thus, the Eqs (2) and (4) are perfectly analogous up to coefficient ordering and sign, because they have the same number of equations,

both expressions are formed by the summation of different coefficient products of a and s, and finally, they have n^2l^2 different combinations of products in total. This is graphically shown in Figures 1 and 2.

Furthermore, as $\boldsymbol{s}$ and $\boldsymbol{e}$ 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.

IV. Multivariate RLWE (m-RLWE)

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 proposed modification to the general GLWE problem. The formulation is perfectly analogous to the 2-RLWE with rings $R[x_1, \ldots, x_m]$ and $R_q[x_1, \ldots, x_m]$ and error distribution $\chi[x_1, \ldots, x_m]$:

Problem 2 (Multivariate RLWE (m-RLWE)): Given a multivariate polynomial ring $R_q[x_1, \ldots, x_m]$ with $f_i(x) = x_i^{n_i}$ for $i = 1, \ldots, m$ and an error distribution $\chi[x_1, \ldots, x_m] \in R_q[x_1, \ldots, x_m]$ that generates small-norm random multivariate polynomials in $R_q[x_1, \ldots, x_m]$, m-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, $u_i \leftarrow R_q[x_1, \ldots, x_m]$ are chosen uniformly at random from the ring $R_q[x_1, \ldots, x_m]$, and $s, e_i \leftarrow \chi[x_1, \ldots, x_m]$ are drawn from the error distribution, and t is relatively prime to q.

Proposition 2 (Proposition 2 in [1]): 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 degree is a power of two), the same procedure sketched above for proving Prop. 1 can be applied to prove the equivalence of m-RLWE (with $n_1, n_2, \ldots, n_m$) and the $(m-1)$-RLWE distributions (with $n_1, n_2, \ldots, n_{m-2}, n_z$), by "folding" two variables of the former (n_{m-1}, n_m) into one variable of the latter (n_z). Therefore, Prop. 2 can be proven by induction using the following procedure:

- First, we have shown the equivalence between RLWE and 2-RLWE (with $n = l_1 l_2$).
- Then, if we assume the equivalence between $(m-1)$-RLWE and RLWE (with $n = n_1 n_2 \ldots n_{m-2} n_z$), we have to prove the equivalence between $(m-1)$-RLWE (with $n_1, n_2, \ldots, n_{m-2}, n_z$) and m-RLWE (with $n_1, n_2, \ldots, n_{m-2}, n_x, n_y$, where $n_z = n_x n_y$). We only have to account for a recursive application of the previous equations (2) and (4). For it, we simply consider that instead of operating with coefficients belonging to the integers, all the involved coefficients are multivariate polynomials with $m-2$ variables and they also have the same modular functions for both the $(m-1)$-RLWE and m-RLWE sample. Analogously, for a graphical explanation, we can consider that the elements a_i and s_j in Figures 1 and 2 are also multivariate polynomials with $m-2$ variables, or, equivalently, that the matrices for the $a_i s_j$ products in m-RLWE are block matrices that can be recursively decomposed until reaching RLWE.

Thus, if we recursively repeat the equivalence argument between RLWE and 2-RLWE as stated above, we can prove Prop. 2.

REFERENCES

[1] A. Pedrouzo-Ulloa, J. R. Troncoso-Pastoriza, and F. Pérez-González, "Multivariate Lattices for Encrypted Image Processing," in *IEEE International Conference on Acoustics, Speech and Signal Processing (submitted)*, 2015.

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

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

[4] V. Lyubashevsky, C. Peikert, and O. Regev, "On Ideal Lattices and Learning with Errors Over Rings," in *Advances in Cryptology EUROCRYPT 2010*, ser. LNCS. Springer, 2010, vol. 6110, pp. 1–23.

[5] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(Leveled) Fully Homomorphic Encryption without Bootstrapping," in *ITCS'12*. ACM, 2012, pp. 309–325.

[6] 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.

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

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