3rd *BYMAT Conference* (2020)

# Multiquadratic rings and oblivious linear function evaluation

Alberto Pedrouzo-Ulloa
atlanTTic Research Center
Universidade de Vigo
apedrouzo@gts.uvigo.es

**Abstract:** The Ring Learning with Errors (RLWE) problem has been widely used for the construction of new quantum-resistant cryptographic primitives. Most of the existing RLWE-based schemes make use of power-of-two cyclotomic rings due to their good performance and simplicity. This talk explores the replacement of power-of-two cyclotomic rings by multiquadratics. We show that for polynomials with $n$ coefficients, the cost of the polynomial operations can be reduced from $\mathcal{O}(n \log n)$ multiplications to $\mathcal{O}(n)$ multiplications and $\mathcal{O}(n \log n)$ additions. Finally, we discuss the benefits that these rings can bring about when implementing the OLE (Oblivious Linear Function Evaluation) primitive, which is a basic block used in many Secure Multiparty Computation (MPC) protocols.

**Resumen:** El problema *Ring Learning with Errors* (RLWE) ha sido utilizado ampliamente para la construcción de nuevas primitivas criptográficas resistentes a ataques por parte de un ordenador cuántico. La mayoría de los esquemas existentes basados en RLWE hacen uso de anillos ciclotómicos de orden potencia de dos, debido a su buen comportamiento y sencillez. Esta charla explora el reemplazo de los anillos ciclotómicos potencia de dos por anillos multicuadráticos. Se muestra que, para polinomios con $n$ coeficientes, el coste de las operaciones polinomiales puede ser reducido de $\mathcal{O}(n \log n)$ multiplicaciones a $\mathcal{O}(n)$ multiplicaciones y $\mathcal{O}(n \log n)$ sumas. Finalmente, se discuten los beneficios que estos anillos introducen al implementar la primitiva OLE (*Oblivious Linear Function Evaluation*), que es un bloque básico utilizado en muchos protocolos de *Secure Multiparty Computation* (MPC).

**Keywords:** ring learning with errors, multiquadratic rings, Walsh-Hadamard transform, oblivious linear function evaluation.

**MSC2010:** 11T71, 68P25, 94A60.

**Acknowledgements:** Funded by the Agencia Estatal de Investigación (Spain) and the European Regional Development Fund (ERDF) under project RODIN (PID2019-105717RB-C21). Also funded by the Xunta de Galicia and the European Union (European Regional Development Fund - ERDF) under projects ED431G2019/08 and Grupo de Referencia ED431C2017/53.

**Reference:** Pedrouzo-Ulloa, Alberto. "Multiquadratic rings and oblivious linear function evaluation". In: *TEMat monográficos*, 2 (2021): *Proceedings of the 3rd BYMAT Conference*, pp. 83-86. ISSN: 2660-6003. URL: https://temat.es/monograficos/article/view/vol2-p83.

# 1. Introduction

This extended abstract corresponds to a talk given in the BYMAT 2020 conference, and covers some of the results previously introduced in [3] and [4]. Due to space constraints, our main aim here is to provide a high-level overview of the most important aspects highlighted in the presentation. We refer the reader to [3, 4] for further technical details.

*Notation.* We first introduce the notation used in this work. Vectors and matrices are represented by boldface lowercase and uppercase letters. Polynomials are denoted with regular lowercase letters, omitting the polynomial variable (i.e., $a$ instead of $a(z)$) when there is no ambiguity. We follow a recursive definition for multivariate quotient rings: $R_q[z] = \mathbb{Z}_q[z]/f(z)$ denotes the polynomial quotient ring in the variable $z$ modulo $f(z)$ with coefficients belonging to $\mathbb{Z}_q$. In general, $R_q[x_1, \dots, x_l]$ (resp. $R[x_1, \dots, x_l]$) represents the multivariate quotient polynomial ring with coefficients in $\mathbb{Z}_q$ (resp. $\mathbb{Z}$) and reduced modulo $f_i(x_i)$ for $1 \leq i \leq l$. The polynomial $a$ can also be denoted by a column vector $\boldsymbol{a}$ whose components are the corresponding polynomial coefficients. Finally, the Hadamard (resp. Kronecker) product of two matrices is $\boldsymbol{A} \circ \boldsymbol{B}$ (resp. $\boldsymbol{A} \otimes \boldsymbol{B}$), and $[l]$ denotes the set $\{1, 2, \dots, l\}$. ◂

## 1.1. Preliminaries: Ring Learning with Errros

The security of modern *homomorphic encryption* (HE) schemes [1] relies on the hardness of the *Ring Learning with Errors* (RLWE) problem [6], where power-of-two cyclotomic rings as $R_q = \mathbb{Z}_q[z]/(1 + z^n)$ are usually considered. An informal definition of RLWE is included in Figure 1, where we can see how the hardness relies on the computational indistinguishability between $(a_i, b_i)$ and $(a_i, u_i)$, where $\chi[z]$ generates polynomials in $R_q$, whose coefficients are independent and follow a Gaussian distribution.

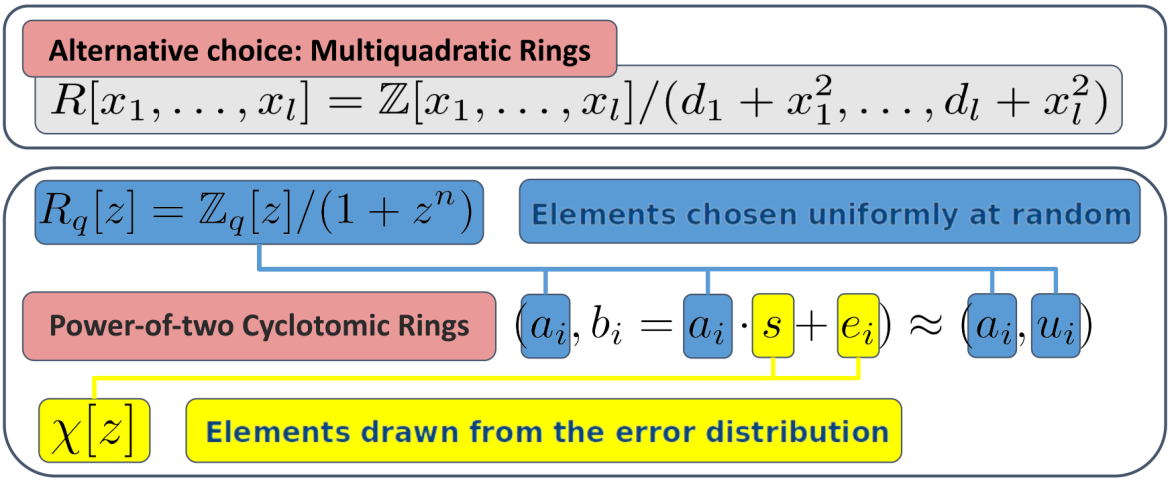


**Figure 1:** Sketch of the RLWE problem.

The use of RLWE provides two important advantages for the construction of encryption schemes:

- RLWE is believed to be difficult to solve by quantum computers.
- Polynomial arithmetic can be done very efficiently with Number Theoretic Transforms (NTTs) [5].

## 1.2. NTT representation

Instead of directly working with the coefficient representation, current HE libraries [1] accelerate computation by making use of a double CRT (Chinese Remainder Theorem) and NTT representation (see Figure 2). In particular, by considering power-of-two cyclotomics, a negacyclic NTT is used which introduces an overhead of $\mathcal{O}(n \log n)$ multiplications. Consequently, motivated by this overhead, in [3, 4] we explored the substitution in RLWE of the conventional power-of-two cyclotomics by multiquadratic rings (see Figure 1).

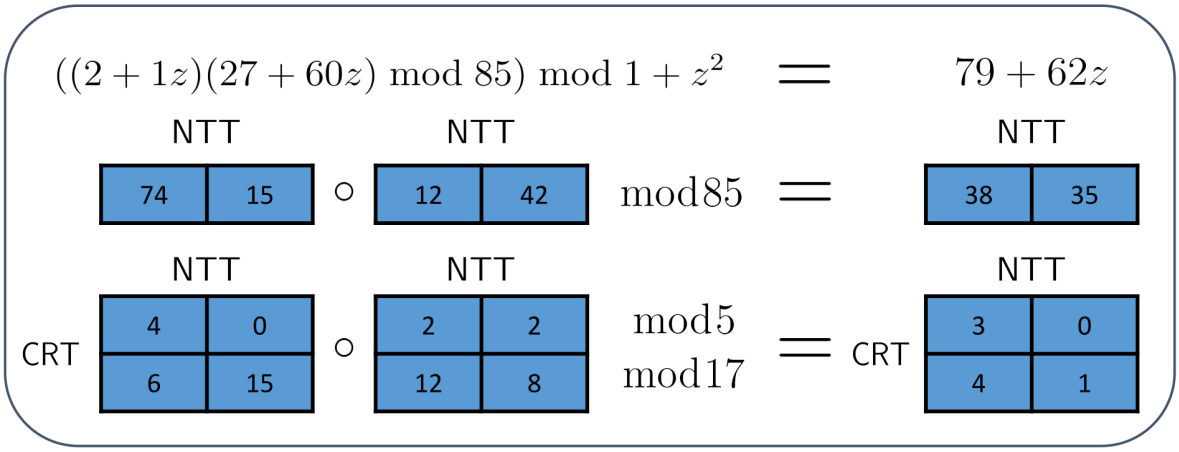


**Figure 2:** Toy example of the CRT-NTT representation.

## 2. Multiquadratic Rings and faster arithmetic

Multiquadratic quotient rings as $R_q[x_1, \dots, x_l] = \mathbb{Z}_q[x_1, \dots, x_l]/(d_1 + x_1^2, \dots, d_l + x_l^2)$ can satisfy a convolution property with a variant of the Walsh-Hadamard transform that we call $\boldsymbol{\alpha}$-generalized WHT in [3, 4]. $\boldsymbol{W}_l$ and $\boldsymbol{W}_l^{-1}$ denote, respectively, the direct and inverse transform matrices associated to $R_q[x_1, \dots, x_l]$.

Figure 3 includes the matrix expressions for both transforms of length $n = 2^l$, where, in order to the ring $R_q$ factors into linear terms [5], $d_j = -\alpha_j^{-1} \bmod q$ and the square-roots of $\alpha_j$ must exist in $R_q$ for all $j$.

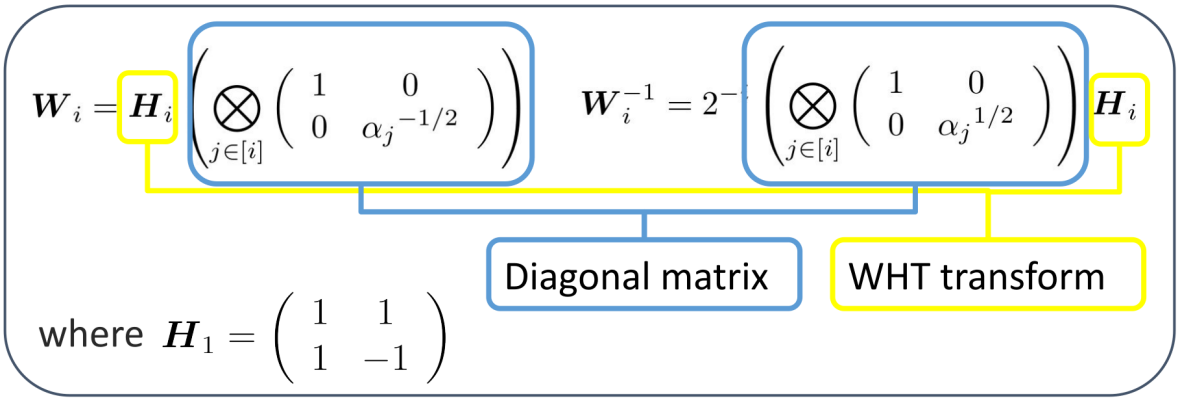


**Figure 3:** Generalized Walsh-Hadamard Transform.

This transform can be very efficiently computed by decomposing it into two different matrices:

- A diagonal matrix which can be computed with a cost of $n$ products.
- A Walsh-Hadamard matrix $\boldsymbol{H}_l$ which can be computed with a cost of only $\mathcal{O}(n \log n)$ additions.

Hence, comparing to the more conventional negacyclic NTT used in the RLWE problem, the use of multiquadratic rings reduces the multiplicative cost of polynomial multiplications by a factor of $\log_2 n$.

## 3. OLE applications

The OLE (Oblivious Linear function Evaluation) primitive is a very important building block in many MPC (Secure Multiparty Computation) protocols [2], and consequently, any achieved improvement on its efficiency brings about important benefits on a wide variety of applications.

An informal description of the OLE primitive can be seen in Figure 4 (we refer to [2, 4] for a formal definition). It considers a set $\mathcal{P} = \{\mathcal{P}_R, \mathcal{P}_S\}$ with two different parties:

- The receiver $\mathcal{P}_R$, which holds an input $x$ and learns the output $f(x) = ax + b$, but nothing more about $a$ and $b$ than can be inferred from both $x$ and $f(x)$.
- The sender $\mathcal{P}_S$, which holds inputs $a$ and $b$, and learns nothing regarding $x$.

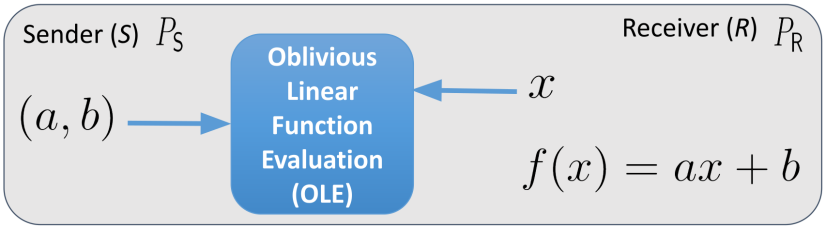


**Figure 4:** OLE primitive.

## 3.1. AHE-based OLE

The OLE primitive from Figure 4 can be implemented with additively homomorphic encryption (AHE):

- $\mathcal{P}_R$ sends $\mathsf{E}(x)$ to $\mathcal{P}_S$. Note that $\mathsf{E}(\cdot)$ represents the encryption functionality.
- $\mathcal{P}_S$ homomorphically calculates $a \cdot \mathsf{E}(x) + b = \mathsf{E}(ax + b)$.
- $\mathcal{P}_R$ receives $\mathsf{E}(ax + b)$ and decrypts it to obtain $f(x)$.

We instantiated in [4] an AHE scheme based on the RLWE problem with both multiquadratic and power-of-two cyclotomic rings. A very brief summary of the obtained results with 128 bits of security is:

- Multiquadratic-based OLE is at least two times faster than its power-of-two cyclotomic counterpart.
- Multiquadratic-based OLE has higher storage needs (requires around 1.7 times more bits).

# References

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

[2] Baum, Carsten; Escudero, Daniel; Pedrouzo-Ulloa, Alberto; Scholl, Peter, and Troncoso-Pastoriza, Juan Ramón. "Efficient Protocols for Oblivious Linear Function Evaluation from Ring-LWE". In: *SCN 2020*. Vol. 12238. LNCS. Springer, 2020, pp. 130–149.

[3] Pedrouzo-Ulloa, Alberto; Troncoso-Pastoriza, Juan Ramón; Gama, Nicolas; Georgieva, Mariya, and Pérez-González, Fernando. "Revisiting Multivariate Ring Learning with Errors and its Applications on Lattice-based Cryptography". In: *IACR Cryptol. ePrint Arch.* 2019 (2019), paper 1109.

[4] Pedrouzo-Ulloa, Alberto; Troncoso-Pastoriza, Juan Ramón; Gama, Nicolas; Georgieva, Mariya, and Pérez-González, Fernando. "Multiquadratic Rings and Walsh-Hadamard Transforms for Oblivious Linear Function Evaluation". In: *IEEE WIFS*. 2020.

[5] Pedrouzo-Ulloa, Alberto; Troncoso-Pastoriza, Juan Ramón, and Pérez-González, Fernando. "Number Theoretic Transforms for Secure Signal Processing". In: *IEEE Transactions on Information Forensics and Security* 12.5 (2017), pp. 1125–1140.

[6] Peikert, Chris; Regev, Oded, and Stephens-Davidowitz, Noah. "Pseudorandomness of ring-LWE for Any Ring and Modulus". In: *ACM STOC*. 2017, pp. 461–473.