2022/2500M-0147

ISSN 1797-3457 (verkkojulkaisu)
ISBN 978-951-25-3371-8

SUMMARY REPORT (TIIVISTELMÄRAPORTTI)

# Analysis and Verification of Post-quantum Cryptography

**Camilla Hollanti (co-PI)**[†], **Chris Brzuska (co-PI)**[†,⋆], **Estuardo Alpirez Bock**[‡], **Rahinatou Yuh Njah Nchiwo**[†], **Kirthivaasan Puniamurthy**[†], and **Pavlo Yatsyna**[†]

[†]Department of Mathematics and Systems Analysis, Aalto University
[⋆]Department of Computer Science, Aalto University
[‡]Xiphera Oy

**Tiivistelmä**

Kvanttitietokoneiden nopeiden edistysaskeleiden odotetaan mahdollistavan tehokkaita tosielämän sovelluksia. Kun kvanttitietokoneet tulevat riittävän toimintakykyisiksi, tärkeimmät kryptografiset julkisen avaimen primitiivimme voivat valitettavasti murtua Shorin algoritmin avulla. Siksi National Institute for Standards and Technology (NIST) on käynnistänyt kilpailun kvanttiturvallisten avainten kapselointimekanismien kehittämiseksi. NIST-kilpailun voittajat on suunniteltu tarjoamaan turvallisuutta mustan laatikon hyökkäyksiä vastaan, mutta niiden turvallinen käyttöönotto edellyttää myös vastustuskykyä sivukanavahyökkäyksille.

Tämän projektin keskiössä on hilapohjaisten kvanttiturvallisten primitiivien entistä parempi kryptanalyysi perustutkimusta ja käytännön arviointia yhdistäen. Pyrimme tunnistamaan taustalla olevien matemaattisten rakenteiden hyödyllisiä ominaisuuksia, jotka tekevät niistä vastustuskykyisiä hyökkäyksille, minkä jälkeen etsimme nämä ehdot täyttäviä potentiaalisia ehdokkaita.

**Abstract**

The current advances in quantum computing are expected to enable powerful real-life applications. Unfortunately, once quantum computers become efficient enough, our most important cryptographic public-key primitives can be broken via Shor's algorithm. Therefore, the National Institute for Standards and Technology (NIST) has started a competition for quantum secure key encapsulation mechanisms. The winners of the NIST competition are tailored to provide black-box security, but their secure deployment also requires resistance against side-channel attacks.

The focus of this project is in improving the cryptanalysis of lattice-based post-quantum primitives, combining foundational research with practical evaluation. In particular, we identify useful features of the underlying mathematical structures that make them resistant against attacks, and then set out to find potential candidates satisfying these properties.

**Postiosoite**
**Postadress**
**Postal Address**
MATINE/Puolustusministeriö
PL 31
FI-00131 Helsinki
Finland

**Käyntiosoite**
**Besöksadress**
**Office**
Eteläinen Makasiinikatu 8 A
00130 Helsinki
Finland

**Puhelin**
**Telefon**
**Telephone**
Vaihde 295 160 01

**s-posti, internet**
**e-post, internet**
**e-mail, internet**
matine@defmin.fi
www.defmin.fi/matine


# 1 Introduction

The backbone of the security of our communication is formed by cryptographic protocols such as TLS, the security protocol behind HTTPS, and EMV, the security protocol for secure payment by credit card. All of these protocols use cryptographic paradigms that are severely threatened by quantum computers, as they rely on computational problems that were presumed to be hard but can be efficiently solved by a quantum computer. Such problems include the factorization of large integers and the discrete logarithm problem. Even though no classical polynomial-time algorithms to solve these problems are known to date, there is a polynomial-time quantum algorithm developed by Shor in 1994 [26]. This means that data that is communicated and stored now utilizing vulnerable classical cryptography is likely to be revealed in the future, once efficient and stable enough quantum computers emerge. Thus, it is important to transition to post-quantum cryptography without delay, even before the development of quantum computers matures.

This led the National Institute of Standards and Technology (NIST) [22] to launch a competition in 2016 for proposals for encryption schemes that are quantum secure to replace the present ones. Following this, in the summer of 2023 NIST published a set of new draft standards containing new algorithms for post-quantum public-key cryptography as well as several candidates for signature algorithms. One of these is the FIPS 203 containing the Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM) [21]. These paradigms belong to the area of cryptography referred to as lattice-based cryptography (LBC). The draft standard is still in its infancy and needs to be better understood. In this project, we focus on the CRYSTALS-Kyber (shortly, Kyber), a key encapsulation mechanism included in the ML-KEM draft standard. We study the security of the implementations of Kyber as well as alternative solutions in the foresight of Kyber potentially turning out to be insecure.

# 2 Research objectives and accomplishment plan

The main objective of this project is in developing a better understanding of the security of lattice-based cryptosystems, both, with respect to black-box security and with respect to side-channel attacks. Lattice-based key encapsulation mechanisms usually rely on variants of the so-called learning with errors problem (LWE, more details below), where two important ingredients are the error distribution and the choice of the lattice guaranteeing black-box security. We focus on the latter. To summarize, the main objectives and their subtasks are listed below.

**Objective 1: Systematic cryptanalysis of lattice-based cryptography**

**1.1** Systematically determine properties and invariants of lattices which make them robust against black-box attacks and which allows for implementations that are robust against side-channel attacks.

**1.2** Find lattices which satisfy these properties.

**Objective 2: Practical evaluation**

**2.1** Implement and test our novel attack methods on existing lattice-based NIST draft standard candidate Kyber.

**2.2** Implement and evaluate the side-channel resistance of implementations of our own lattice-based key encapsulation mechanisms.

Alternatives to Kyber. The security of Kyber is based on a mathematical structure called a (Euclidean) lattice. We study properties that might make such structures insecure and which one should hence avoid when choosing the underlying lattice.


A list of properties was already known, on one hand giving *sufficient* conditions for an attack and on the other hand providing desirable properties. In this project, we identify which of these properties are also *necessary* and which ones are the core properties causing weaknesses that we wish to avoid. Some of the desired properties can also be extended to hold in more general structures. More details to follow in the results section.

Implementations. The security of implementations of cryptography has been studied for a long time, but since the algorithms are new and very different from the previous algorithms, we now need to understand which parts can be vulnerable, and a major part of our research falls into this domain. Kyber is built on having smaller ciphertexts at the cost of a slightly more inefficient decryption algorithm. An outcome of this choice is that the decryptions perform more operations on the secret inputs. We show that this is a weakness as performing more operations on the secrets leaks more information.

The learning with errors (LWE) problem proposed by Oded Regev [25] in 2005 is one of the first problems in LBC that is supposedly quantum-safe. At its core lies the notion that even for a seemingly uncomplicated multiplication, an introduction of a minor error term, or "noise," renders the task of uncovering all the products involved in the operation exceedingly challenging. In addition, among many applications of LWE, it plays a great role in homomorphic encryption, which is a method of encrypting plaintext that allows for users to compute directly with the ciphertext without decryption. This has great relevance in cloud computing. Despite its security advantages, LWE is computationally expensive. This limitation motivated the construction of other variants with an extra algebraic structure to handle these lapses. The original implementation of LWE was later updated by Lyubashevsky, Peikert, and Regev [19] to ring learning with errors (RLWE). The key difference here is that instead of using integers, we use elements from certain algebraic structures. The main benefit of this is that we can efficiently implement the algorithm at the cost of the presumed level of security. Therefore, the main issue here is to verify the security aspect of RLWE.

As one may expect, these new additional structures come with a price, yet are efficient for secure encryption even in the post-quantum era. Numerous works are trying to generalize the RLWE, changing various conditions and parameters and scrutinising its effectiveness and security. The influential works of Eisentraeger, Hallgren and Lauter [11] and Elias, Lauter, Ozman, and Stange [12] motivated us to look precisely at the issues and conditions proposed by them (see the list in the next section). The list served as a guideline for the conditions to aspire to in order to ensure security. It also highlighted aspects to be cautious about to prevent vulnerabilities in the system.

# 3 Materials and methods

Let us delve into more technical descriptions, though non-experts can safely skip this section. The LWE problem and its variants provide presumably hard problems that form the basis for cryptosystems that are quantum secure. We briefly describe the LWE and RLWE problems in the following. The residue ring of integers modulo $q$ is denoted by $\mathbb{Z}_q$.

**Definition 1.** *[25]: Given the parameter (prime) $q$ and an error distribution $\chi$ over $\mathbb{Z}_q$ the search version of the learning with errors (LWE) is defined as follows:*

- *Let $s \in \mathbb{Z}_q$ be an element (secret) chosen uniformly at random.*
- *Given access to arbitrarily many samples $\{(a_i, a_i s + e_i)\}_{i \geq 1}$ of the LWE distribution where $i \geq 1$, $a_i$ is chosen uniformly at random and $e_i$ is sampled from $\chi$, recover $s$ with non-negligible advantage.*

We can extend the previous definition to RLWE and to polynomial LWE (PLWE):

**Definition 2.** *[19],[27]: Let $K$ be a number field, $\mathcal{O}_K$ its ring of integers and $\mathcal{O} = \mathbb{Z}[x]/(f(x))$ with $f(x)$ monic and irreducible in $\mathbb{Z}[x]$. Let $\chi$ be an error distribution over $\mathcal{O}_K/q\mathcal{O}_K$ (resp. in $\mathcal{O}/q\mathcal{O}$). The RLWE (resp. PLWE) problem for $\chi$ is defined as follows:*

- *Let $s \in \mathcal{O}_K/q\mathcal{O}_K$ (resp. $\mathcal{O}/q\mathcal{O}$) be an element (secret) chosen uniformly at random.*
- *Given access to arbitrary many samples $\{(a_i, a_i s + e_i)\}_{i\geq 1}$ of the RLWE (resp. PLWE) distribution, where for each $i \geq 1$, $a_i$ is chosen uniformly at random and $e_i$ is sampled from $\chi$, recover $s$ with non-negligible advantage.*

The *decision problem* differs in that, instead of finding the secret $s$, one must discern a distinction between genuine samples $(a_i, a_i s + e_i)_{i\geq 1}$ and a randomly generated output, with a non-negligible advantage.

Let us introduce the list from the work of Eisentraeger, Hallgren and Lauter [11]. Again, $K$ will be a number field and $\mathcal{O}_K$ denotes its ring of integers. Finally, we assume that $q$ is a (sufficiently large) prime number.

1. $(q)$ splits completely in $K$, and $q \nmid [\mathcal{O}_K : \mathbb{Z}[\beta]]$.
2. $K$ is Galois over $\mathbb{Q}$.
3. The ring of integers of $K$ is generated over $\mathbb{Z}$ by $\beta$, $\mathcal{O}_K = \mathbb{Z}[\beta] = \mathbb{Z}[x]/(f(x))$ with $f'(\beta) \pmod q$ 'small'.
4. The transformation between the Minkowski embedding of $K$ and the power basis representation of $K$ is given by a scaled orthogonal matrix.
5. Let $f \in \mathbb{Z}[x]$ be the minimal polynomial for $\beta$, such that $f(1) \equiv 0 \pmod q$, where $q$ can be chosen to be sufficiently large.

Items (1) and (2) enable us to demonstrate that the decision RLWE problem is as hard as the search RLWE problem (i.e., there exists a reduction). Moreover, if we can nonrandomly distinguish the samples, an algorithm exists that outputs the secret. These items (1) and (2) are associated with the utilization of the Chinese Remainder Theorem and the "nice behavior" of the error distributions. On the other hand, items (3) and (4) facilitate the reduction of the RLWE average-case decision problem to PLWE. The last item is to be avoided, as it opens an opportunity for an attack.

# 4 Results and discussion

The results are grouped under the related Objective/Task described above.

## 4.1 Objective 1.1

In [6] and [5] we look at some of the weak variants of PLWE. It is worth mentioning that these attacks do not threaten the present-day cryptosystems which rely on PLWE, however, give us a list of parameters to avoid if we start considering other options or weakening the present conditions. In [7] we study the equivalence between RLWE and PLWE. In [1] we perform a cryptanalysis of an approach to homomorphic encryption proposed by Leonardi and Ruiz-Lopez in [18]. Next, we will give a brief, high-level description of these projects.


#### 4.1.1 Trace-based cryptanalysis of cyclotomic $R_{q_0} \times R_q$-PLWE for the non-split case [6]

In this paper, we describe a decisional attack against a version of the PLWE problem in which the samples are taken from a certain proper subring of large dimension of the cyclotomic ring $F_q[x]/(\varphi_{p^k}(x))$ with $k > 1$ in the case where $q \equiv 1 \pmod{p}$ but $\varphi_{p^k}(x)$ is not totally split over $F_q$. Our attack uses the fact that the roots of $\varphi_{p^k}(x)$ over suitable extensions of $F_q$ have zero-trace and have overwhelming success probability as a function of the number of input samples.

#### 4.1.2 Cryptanalysis of PLWE based on zero-trace quadratic roots [5]

We extend two of the attacks on the PLWE problem presented in [12] to a ring $R_q = \mathbb{F}_q[x]/(f(x))$ where the irreducible monic polynomial $f(x) \in \mathbb{Z}[x]$ has an irreducible quadratic factor over $\mathbb{F}_q[x]$ of the form $x^2 + \rho$ with $\rho$ of suitable multiplicative order in $\mathbb{F}_q$. Our attack exploits the fact that the trace of the root is zero and has overwhelming success probability as a function of the number of samples taken as input.

#### 4.1.3 On homomorphic encryption using abelian groups: Classical security analysis [1]

Despite the importance of homomorphic encryption, it is worth noting that constructing such an encryption scheme is hard. The closest the community has come in this regard is by using maps based on (variants of) the LWE problem though not fully homomorphic.

In the paper [1], we explore an alternative approach for homomorphic encryption introduced by Leonardi and Ruiz-Lopez in [18]. A big advantage of the Leonardi–Ruiz-Lopez approach over the basic LWE approach is that the noise, which plays the role of the errors in LWE-based homomorphic encryption, does not grow with repeated computation. As such, there is no limitation on the number of additions that can be computed on encrypted data. However, it is not clear if this construction can be extended to multiplicative homomorphic encryption. Choosing parameters for their primitive requires choosing three groups $G, H,$ and $K$. They claim that, when $G, H,$ and $K$ are abelian, then their public-key cryptosystem is not quantum secure. Though in the non-abelian setting, it has some hopes of being quantum secure. In this paper, we study security for finite abelian groups $G, H,$ and $K$ in the classical case. Moreover, we study quantum attacks on instantiations with solvable groups.

#### 4.1.4 Fast polynomial arithmetic in homomorphic encryption with cyclo-multiquadratic fields [7]

RLWE is well-suited for theoretical considerations, while PLWE is preferable for practical applications. Moreover, the complexity of the PLWE problem is rooted in its reduction to a hard lattice problem through the RLWE problem — specifically, solving RLWE implies the existence of a quantum algorithm for the approximate shortest vector problem (SVP) on ideal lattices, which is presumed to be a hard problem (in general, it is worth noting that the approximation factors in reduction proofs often leave quite some gap to the problems that are actually known to be NP-hard). As such, studying the equivalence between PLWE and RLWE becomes of great interest to the cryptography community, especially in LBC. The transformation between these two leads to a noise distortion which is measured by the condition number. We provide refined polynomial upper bounds for the condition number of cyclotomic fields with up to $6$ different primes dividing the conductor.

We further discuss the advantages and limitations of cyclotomic fields to have fast polynomial arithmetic within homomorphic encryption and show how these limi-

tations can be overcome by replacing cyclotomic fields with a family that we refer to as cyclo-multiquadratic fields. This family is of particular interest due to its arithmetic efficiency properties and to the fact that the PLWE and RLWE problems are equivalent for this family.

## 4.2 Objectives 1.1-1.2

Let us describe some relevant updates to the list of Eisentraeger, Hallgren and Lauter that we discussed earlier. These updates are largely based on a careful review on recent literature and stitching together various different aspects. This part of our research reaches over both the tasks in Objective 1, and provides us with the desired and to-be-avoided properties of number fields for RLWE variants.

We begin with condition (1), which concerns the choice of the prime number employed in the algorithm. The authors in [17] have demonstrated the feasibility of relaxing the arithmetic requirements for the prime $q$ (using the "modulus-switching" technique) at the price of slight increases in the error term.

Condition (2), on the number field being Galois, can also be relaxed due to the work of Peikert, Regev, and Stephens-Davidowitz [24], where they manage to completely avoid a search-to-decision reduction, which in turn means that we can avoid the restriction on the number field being Galois. In the work, the authors did not find strong evidence for a particular choice of a number field, other than signifying that number fields with dual rings that have a small shortest vector appeared to be less secure.

Condition (3) is regarding the so-called monogenicity condition. Elias, Lauter, Ozman, and Stange in [12] already knew that it was a rather common occurrence. Recently, it was reaffirmed [4] that more than 60% of candidates will satisfy such a condition. Although monogenicity is not rare, the primary challenge was the combination of conditions (2) and (3). Given the possibility of forgoing condition (2), this becomes a more manageable task by e.g. randomly generating short polynomials of a given degree that are irreducible and correspond to monogenic number fields.

Condition (4), which pertains to the transformation from Minkowski embedding to power basis representation, is not vacuous. There are infinitely many instances where, even among the "nice" candidates (i.e., cyclotomics), the transformation does not allow for the equivalence among the problems that we want [10]. Nevertheless, it is an invariant we can easily compute for a given example.

Condition (5) had seen some interesting developments. First of all, the search for the given root can be easily checked. This condition can be further generalized from having $1$ as a root to the existence of a root of a small order. As mentioned above, this condition relates to the existence of attacks on the RLWE. A related question regarding the smearing condition was recently comprehensively addressed in [3]. Furthermore, the family of such attacks was inspected in [23]. Specifically, the invulnerability conditions proposed in the paper are weak enough so that the proper implementation of RLWE in [19] is already provably immune from such attacks.

We have produced a list of possible candidates (i.e., alternatives to the power-of-two cyclotomics). Specifically, these candidate polynomials are irreducible and correspond to monogenic number fields. In the search, we attempted to find those polynomials that have small condition numbers related to (4). All of these alternatives will still have to be tested for attacks related to (5). There is perhaps a more pragmatic approach by restricting the construction to trinomials, i.e., polynomials with only three nonzero coefficients. There is a two-fold benefit here. One is heuristics, given that with fewer coefficients, we may assimilate the good properties of the power of two cyclotomic number fields. The latter, and more important, is that there is a body of work on studying monogenic number fields among trinomials. It could also imply that it is easier to control certain important invariants, like the condition number. The research toward this goal is ongoing.


## 4.3 Objective 2.1

### 4.3.1 Breaking DPA-protected Kyber via the pair-pointwise multiplication [8]

In this paper we study the security of Kyber in light of side-channel analysis attacks. Side-channel attacks consist on observing and analysing the physical parameters generated by a device running a cryptographic algorithm. Such parameters can be the power consumption of the device or the electromagnetic emissions generated during computations. The idea is that these physical parameters are dependent on the secret values processed by these devices (usually the secret key of the cryptographic scheme) and a careful analysis may reveal the value of the secret key.

We present an attack on the decapsulation process of Kyber which helps us extract the value of the long-term secret key of the scheme. This key is used for decryption and it consists of a vector of polynomials represented in number-theoretic transform (NTT) domain. For decryption, these secret polynomials are multiplied with the cipher-text polynomials (also in NTT domain). In Kyber, two polynomials in NTT domain are multiplied in a pair-pointwise fashion: each pair of secret coefficients is multiplied with a pair of ciphertext-coefficients.

In our attack, we construct templates of power consumption for possible pairs of secret coefficients and compare those templates with the power consumption of the device under attack. We present different versions of our attack, varying on the number of templates needed for a successful key extraction. We also explain how our attack is successful against implementations of Kyber which actually implement countermeasures against (other) side-channel attacks. We also discuss possible mitigation techniques against our attack and discuss the costs of such techniques

Our paper also studies the state of the art of side-channel attacks on Kyber. Particularly, our result exposes a leakage source on Kyber which had not yet been considered and which is also present in designs implementing side-channel countermeasures. Interestingly, this leakage is strong in Kyber, given that the polynomials in this scheme are multiplied in pair-pointwise fashion [28].

### 4.3.2 Protecting the most significant bits in scalar multiplication algorithms [2]

This paper also deals with side-channel security of cryptographic implementations. Here we focus on elliptic curve-based schemes which make use of scalar multiplication algorithms, such as the Montgomery Ladder [20]. In such schemes, secret keys correspond to randomly generated scalars and they are multiplied with points in an elliptic curve. The multiplication is performed by processing the secret scalar bit by bit, performing a series of arithmetic operations which depend on the value of the bit being processed. Besides its use on elliptic curve cryptographic schemes, the scalar multiplication also plays an important role in isogeny-based schemes.

In our work we show how the most significant bits of the secret scalar can be easily extracted via simple side-channel observations. We exploit leakage which appears during the first iterations of the scalar multiplication algorithm, and show that this leakage is caused by the values used for initialising the input variables of the algorithm. We also explain how knowledge of the most significant bits can be exploited for enabling further physical attacks, including attacks proposed for isogeny-based post-quantum (former) candidates. For mitigating this leakage, we propose software-friendly countermeasures and show their effectiveness via power analysis measurements. We propose two alternative methodologies for implementing these countermeasures and show that they only imply very small performance penalties.

## 4.4 Objective 2.2

The research in Objective 2.2 turned out somewhat obsolete as we expect the possible alternative constructions to exhibit similar kind of vulnerability for side-channel attacks as for e.g. Kyber, relating to the tradeoff between the ciphertext size and decryption efficiency. Namely, the vulnerability only arises if we choose a modulus such that one needs to do an incomplete number-theoretic transform.

## 4.5 Objective 1: Advances in Number Theory

Lastly, we include some more indirectly relevant research that is closely related to lattices.

### 4.5.1 Special journal issue on the theory and applications of Euclidean lattices [13]

In this special issue of the journal Communications in Mathematics and the included editorial survey we outline some of the main aspects of the important research area of lattices at the intersection of theory and applications, including lattice-based cryptography [6].

### 4.5.2 Fundamental research on lattices [9, 14, 15, 16]

The research in [9, 14, 15, 16] focuses on theoretical aspects of lattices and number fields, with the primary goal of saying something abstract about them. However, one of the byproducts is a better understanding of lattices in general, which could be utilized to determine optimal parameters for constructing suitable number fields for RLWE.

# 5 Conclusions

From project inception to the present, Kyber has transitioned from a contender to a key selection in the NIST competition for post-quantum cryptography. Our assessment covered theoretical robustness, practical execution, and potential vulnerabilities. We focused on identifying attacks, especially against Kyber alternatives, and explored immediate threats from side-channel attacks. Criteria for Kyber alternatives were refined and parsed together, presenting a preliminary list for further scrutiny. We looked into the theoretical aspects behind the (R)LWE, but further research toward alternative solutions to Kyber is still needed and this work is ongoing. While providing a foundation for addressing potential flaws in RLWE-based architectures, our theoretical findings thus far are not a direct threat to Kyber's security.

In the near future, we plan to construct explicit candidates for RLWE-based systems and analyze them further. We hope to identify algebraic properties that could serve as a recipe for efficiency and hence make a welcome addition to the aforementioned list of desired properties. The side-channel attacks will also be further studied as well as tested on a laboratory setting in collaboration with our partners.

# 6 Scientific publishing

1. I. Blanco-Chacón, R. Durán-Díaz and **R. Y. Njah Nchiwo** and B. Barbero-Lucas, *Trace-based cryptanalysis of cyclotomic $R_{q,0} \times R_q$ -PLWE for the non-split case*, Communications in mathematics, vol. **31** (2023), 115–135.

2. I. Blanco-Chacón, B. Barbero-Lucas, R. Durán-Díaz and **R. Y. Njah Nchiwo**, *Cryptanalysis of PLWE based on zero-trace quadratic roots*, submitted, 2023.
3. I. Blanco-Chacón, A. Pedrouzo-Ulloa, **R. Y. Njah Nchiwo** and B. Barbero-Lucas, *Fast polynomial arithmetic in homomorphic encryption with cyclo-multiquadratic fields*, arXiv:2304.04619, 2023.
4. E. Agathocleous, V. Anupindi, A. Bachmayr, C. Martindale, **R. Y. Njah Nchiwo** and M. Stanojkovski, *On homomorphic encryption using abelian groups: Classical security analysis*, Springer (to appear), 2023.
5. V. Kala and **P. Yatsyna**, *On Kitaoka's conjecture and lifting problem for universal quadratic forms*, Bull. Lond. Math. Soc. **55** (2023), 854–864.
6. V. Kala, **P. Yatsyna**, B. Żmija, *Real quadratic fields with a universal form of given rank have density zero*, submitted, 2023.
7. G. Cherubini and **P. Yatsyna**, *Degrees of Salem numbers of trace -3*, submitted, 2023.
8. J. Krásenský and **P. Yatsyna**, *On quadratic Waring's problem in totally real number fields*, Proc. Amer. Math. Soc. **151** (2023), 1471–1485.
9. **E. Alpirez Bock**, L. Chmielewski and K. Miteloudi, *Protecting the most significant bits in scalar multiplication algorithms*. In Security, Privacy and Applied Cryptographic Engineering (SPACE) 2022.
10. **E. Alpirez Bock**, G. Banegas, **C. Brzuska**, L. Chmielewski, **K. Puniamurthy** and M. Sorf, *Breaking DPA-protected Kyber via the pair-pointwise multiplication*. IACR eprint archive, 2023.
11. L. Fukshansky and **C. Hollanti** (edt.), *Special issue: Euclidean lattices: theory and applications*, Communications in Mathematics, 31(2), 2023.

## Acknowledgments

The authors would like to thank the Magnus Ehrnrooth Foundation for a doctoral scholarship to Rahinatou Yuh Njah Nchiwo. They also wish to thank all the co-authors of the reported articles and Prof. Russell Lai for fruitful discussions.

## References

[1] E. Agathocleous, V. Anupindi, A. Bachmayr, C. Martindale, R. Y. N. Nchiwo, and M. Stanojkovski. On homomorphic encryption using abelian groups: Classical security analysis. *Springer (to appear)*, 2023. https://eprint.iacr.org/2023/304.

[2] E. Alpirez Bock, L. Chmielewski, and K. Miteloudi. Protecting the most significant bits in scalar multiplication algorithms. In L. Batina, S. Picek, and M. Mondal, editors, *Security, Privacy, and Applied Cryptography Engineering*, Cham, 2022. Springer Nature Switzerland.

[3] L. Babinkostova, A. Chin, A. Kirtland, V. Nazarchuk, and E. Plotnick. The polynomial learning with errors problem and the smearing condition. *Journal of Mathematical Cryptology*, 16(1), 2022.

[4] M. Bhargava, A. Shankar, and X. Wang. Squarefree values of polynomial discriminants I. *Inventiones Mathematicae*, 2022.

[5] I. Blanco-Chacón, B. Barbero-Lucas, R. Durán-Díaz, and R. Y. N. Nchiwo. Cryptanalysis of PLWE based on zero-trace quadratic roots. *submitted*, 2023.

[6] I. Blanco-Chacón, R. Durán-Díaz, R. Y. N. Nchiwo, and B. Barbero-Lucas. Trace-based cryptanalysis of cyclotomic $r_{q_0} \times r_q$ -PLWE for the non-split case. *Communications in Mathematics*, 31, 2023.

[7] I. Blanco-Chacón, A. Pedrouzo-Ulloa, R. Y. N. Nchiwo, and B. Barbero-Lucas. Fast polynomial arithmetic in homomorphic encryption with cyclo-multiquadratic fields. *arXiv:2304.04619*, 2023.

[8] E. A. Bock, G. Banegas, C. Brzuska, Lukasz Chmielewski, K. Puniamurthy, and M. Šorf. Breaking dpa-protected kyber via the pair-pointwise multiplication. Cryptology ePrint Archive, 2023/551, 2023. https://eprint.iacr.org/2023/551.

[9] G. Cherubini and P. Yatsyna. Degrees of Salem numbers of trace $-3$, 2023. arXiv:2301.06536.

[10] A. J. Di Scala, C. Sanna, and E. Signorini. RLWE and PLWE over cyclotomic fields are not equivalent. *Applicable Algebra in Engineering, Communication and Computing*, 2022.

[11] K. Eisenträger, S. Hallgren, and K. Lauter. Weak Instances of PLWE. In A. Joux and A. Youssef, editors, *Selected Areas in Cryptography – SAC 2014*, Cham, 2014. Springer Int. Pub.

[12] Y. Elias, K. E. Lauter, E. Ozman, and K. E. Stange. Provably Weak Instances of Ring-LWE. In R. Gennaro and M. Robshaw, editors, *Advances in Cryptology – CRYPTO 2015*, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.

[13] L. Fukshansky and C. Hollanti, editors. *Special issue: Euclidean lattices: theory and applications*, volume 31(2). Communications in Mathematics, 2023.

[14] V. Kala and P. Yatsyna. On Kitaoka's conjecture and lifting problem for universal quadratic forms. *Bull. Lond. Math. Soc.*, 55(2), 2023.

[15] V. Kala, P. Yatsyna, and B. Żmija. Real quadratic fields with a universal form of given rank have density zero, 2023. arXiv:2302.12080.

[16] J. Krásenský and P. Yatsyna. On quadratic Waring's problem in totally real number fields. *Proc. Amer. Math. Soc.*, 151(4), 2023.

[17] A. Langlois and D. Stehle. Worst-case to average-case reductions for module lattices. Cryptology ePrint Archive, 2012/090, 2012.

[18] C. Leonardi and L. Ruiz-Lopez. Homomorphism learning problems and its applications to public-key cryptography. *Cryptology ePrint Archive*, 2019.

[19] V. Lyubashevsky, C. Peikert, and O. Regev. On Ideal Lattices and Learning with Errors over Rings. *J. ACM*, 60(6), nov 2013.

[20] P. L. Montgomery. Speeding the pollard and elliptic curve methods of factorization. *Mathematics of Computation*, 48(177), 1987.

[21] National Institute of Standards and Technology. Module-lattice-based key-encapsulation mechanism standard. https://csrc.nist.gov/pubs/fips/203/ipd. Accessed: 2023-11-23.

[22] National Institute of Standards and Technology. NIST Announces First Four Quantum-Resistant Cryptographic Algorithms. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms. Accessed: 2023-10-30.

[23] C. Peikert. How (not) to instantiate ring-LWE. In V. Zikas and R. De Prisco, editors, *Security and Cryptography for Networks*, Cham, 2016. Springer Int. Pub.

[24] C. Peikert, O. Regev, and N. Stephens-Davidowitz. Pseudorandomness of ring-LWE for any ring and modulus. Cryptology ePrint Archive, 2017/258, 2017.

[25] O. Regev. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. *J. ACM*, 56(6), sep 2009.

[26] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. *In Proceedings of the 35th Annual Symposium on Foundations of Computer Science,. IEEE Computer Society Press*, 1994.

[27] D. Stehle, R. Steinfeld, K. Tanaka, and K. Xagawa. Efficient public key encryption based on ideal lattices. *In Proc. of ASIACRYPT, Springer*, 31, 2009.

[28] S. Zhou, H. Xue, D. Zhang, K. Wang, X. Lu, B. Li, and J. He. Preprocess-then-ntt technique and its applications to kyber and newhope. In F. Guo, X. Huang, and M. Yung, editors, *Information Security and Cryptology*, Cham, 2019. Springer International Publishing.