In Praise of Twisted Canonical Embedding

Jheyne N. Ortiz[1], Robson R. de Araujo[2], Ricardo Dahab[1], Diego F. Aranha[1], and Sueli I. R. Costa[2]

[1]Institute of Computing, University of Campinas, Brazil
jheyne.ortiz@ic.unicamp.br
[2]Institute of Mathematics, Statistics and Scientific Computing, University of Campinas, Brazil
robson.araujo@ime.unicamp.br

Abstract

In ideal-lattice cryptography, lattices are generated by defining a bijective map between an ideal of a ring of integers and a subset of $\mathbb{C}^n$. This map can be taken to be the coefficient embedding and, along with the Ring-LWE problem, the canonical embedding. However, some lattices cannot be generated using the canonical embedding in a straightforward manner. In this paper, we introduce a new class of problems called α-Ring-LWE, which combines Ring-LWE with the twisted canonical embedding. In this context, α stands to be a number field element that distorts the canonical embedding coordinates. We prove the hardness of α-Ring-LWE by providing a reduction between the Ring-LWE problem to α-Ring-LWE for both search and decision variants. As a result, we obtain a hardness result based on a hard problem over ideal lattices. The addition of a torsion factor enables the construction of a broader class of lattices as rotated lattices. An example is the construction of the integer lattice $\mathbb{Z}^n$ by embedding the ring of integers of the totally real subfield of a cyclotomic number field $\mathbb{Q}(\zeta_p)$ with p being a prime number [BFOV04].

1 Introduction

Shor's algorithm and its variation quantumly solve the integer factorization and discrete logarithm problems in polynomial time [Sho97]. Therefore, the RSA and ECDSA[1] public-key cryptosystems became vulnerable to quantum

[1]Acronym to Elliptic Curve Digital Signature Algorithm.

attacks. Subsequently, cryptographic primitives based on problems that are hard to solve by conventional and quantum computers have been proposed in the literature. The classes of problems that support these primitives are commonly referred as *post-quantum cryptography*. There are constructions whose security relies on problems over supersingular isogenies, lattices, error-correcting codes, multivariate quadratic equations, hash functions, and others.

The urge for viable post-quantum schemes that may ensure future privacy is reflected by NIST's call for proposals of quantum-resistant public-key algorithms to be standardized in the near future [NIS17]. An example of post-quantum public-key scheme is the lattice-based NewHope [ADPS16], which was deployed by Google in a post-quantum TLS experiment simultaneously with current algorithms [Goo16]. Similarly to most cryptosystems based on the Ring-LWE problem[2], NewHope builds upon the power-of-two cyclotomic ring of integers.

Campbell, Groves, and Shepherd have introduced a lattice-based cryptosystem named Soliloquy that, as the homomorphic encryption scheme of Smart and Vercauteren [SV10] and others similar systems, is vulnerable to a key-recovery quantum attack that runs in polynomial time [CGS13]. Soliloquy uses cyclotomic number fields generated by the p-th root of unity, with p being a prime number.

In light of the quantum attack for certain systems based on cyclotomic number fields, the study of lattice-based cryptosystems using number fields besides cyclotomics has been motivated also by a sequence of works that characterizes weak instances of Ring-LWE and Poly-LWE[3] problems [EHL14, ELOS15, CLS15, CIV16b, CIV16a, CLS16]. As a consequence, these works end up exploring vulnerabilities exposed by some field properties, as done by Bernstein et al. in [BCLvV16].

In the Ring-LWE context, the search for alternative instantiations has been put forward by hardness results for all number fields [LPR10, PRSD17a] and a toolkit containing techniques for secure implementation of Ring-LWE primitives over any cyclotomic number field [LPR13]. For example, an alternative instantiation is the adoption of the ring of integers $\mathbb{Z}[x]/\langle x^p - x - 1\rangle$ for p prime, which was proposed in [BCLvV16] for an NTRU-based scheme, and also suggested for the Ring-LWE setting in [PRSD17b].

In ideal-lattice cryptography, an ideal of a ring of integers relates to a lattice by an injective ring homomorphism. Ring-LWE adopts the canonical embedding, also known as Minkowski embedding, but, for some lattices constructions,

[2]Abbreviation for the Learning With Errors problem over rings. It is not a problem based on lattices but is related by a computational reduction from problems over ideal lattices [LPR10].

[3]Polynomial Learning With Errors, a simplification of the Ring-LWE problem explicitly introduced by Brakerski and Vaikuntanathan in [BV11].

the canonical embedding does not suffice then requiring a torsion in each of its coordinates. The embedding resulting from this torsion is denoted as *twisted canonical embedding*, which is now referred to as *twisted embedding*. In this paper, we introduce α-Ring-LWE, the class of problems Ring-LWE adopting the twisted embedding, and we transitively prove its hardness based on a hard problem over ideal lattices.

2 Preliminaries

In this context, for a vector $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$, when p is a finite number, let the l_p norm be $\|x\|_p = \big(\sum_{i \in [n]} |x_i|^p \big)^{\frac{1}{p}}$. For $p = \infty$, $\|x\|_\infty = \max_{i \in [n]}(|x_i|)$. When not stated otherwise, assume $\|\cdot\|$ denotes the l_2 norm.

2.1 Algebraic Number Theory

Let K be a number field, which is a n-degree extension over $\mathbb{Q}$, $R = \mathcal{O}_K$ its ring of algebraic integers, and $R^\vee$ the corresponding dual of R. For simplicity, we do not adopt the H space as defined in [LPR10] but we point out that H is isomorphic to $\mathbb{R}^n$ as an inner product space. Moreover, let $\sigma_1, \ldots, \sigma_n$ be the n embeddings of K ordered so that $\sigma_1, \ldots, \sigma_{s_1}$ are the real embeddings and the remaining $2s_2 = n - s_1$ complex embeddings are paired in such a way that $\sigma_{s_1+k} = \overline{\sigma_{s_1+s_2+k}}$ for $k \in [s_2]$.

Definition 1 (Ideal lattice). *An ideal lattice is a pair $(\mathcal{I}, q_\alpha)$ where $\mathcal{I}$ is an ideal of $\mathcal{O}_K$ and*

$$q_\alpha : \mathcal{I} \times \mathcal{I} \to \mathbb{Z}, q_\alpha(x, y) = Tr(\alpha x y), \forall x, y \in \mathcal{I},$$

where the trace can be shown to be the sum of the embeddings as $Tr(x) = \sum_{i \in [n]} \sigma_i(x)$, and $\alpha \in K$ is totally positive, i.e. $\sigma_i(\alpha) > 0$ for $i \in [n]$.

Let the *canonical embedding* σ be the map $\sigma : K \to \mathbb{R}^n$ given by

$$\begin{aligned} \sigma(x) = (&\sigma_1(x), \ldots, \sigma_{s_1}(x), \\ &Re(\sigma_{s_1+1}(x)), Im(\sigma_{s_1+1}(x)), \ldots, \\ &Re(\sigma_{s_1+s_2}(x)), Im(\sigma_{s_1+s_2}(x))). \end{aligned}$$

The canonical embedding endows the number field K with a geometrical representation where we can define geometric norms and error distributions over the

tensor product $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$. Also, these embeddings are ring monomorphisms[4] from K to $\mathbb{R}^n$ where addition and multiplication are both component-wise.

Following the definition from [Wü02], which slightly differs from [OV04], the *twisted canonical embedding* $\sigma_\alpha : K \to \mathbb{R}^n$ can be defined as

$$\begin{aligned}\sigma_\alpha(x) = (&\sqrt{\sigma_1(\alpha)}\sigma_1(x), \ldots, \sqrt{\sigma_{s_1}(\alpha)}\sigma_{s_1}(x)),\\ &\sqrt{2\sigma_{s_1+1}(\alpha)}Re(\sigma_{s_1+1}(x)), \sqrt{2\sigma_{s_1+1}(\alpha)}Im(\sigma_{s_1+1}(x)), \ldots,\\ &\sqrt{2\sigma_{s_1+s_2}(\alpha)}Re(\sigma_{s_1+s_2}(x)), \sqrt{2\sigma_{s_1+s_2}(\alpha)}Im(\sigma_{s_1+s_2}(x))),\end{aligned}$$

for a totally positive $\alpha \in K$.

The generator matrix of ideal lattices are of the type $M = (\sigma_i(\omega_j))_{i,j\in[n]} \cdot D$, where D is a diagonal matrix and $(\omega_j)_{j\in[n]}$ is a $\mathbb{Z}$-basis of $\mathcal{I}$. When $D = I_n$, the n-by-n identity matrix, the ideal lattice is simply generated by the canonical embedding. Moreover, when D contains in its diagonal the factors $\sqrt{\sigma_i(\alpha)}$ for $i \in [s_1]$ and $\sqrt{2\sigma_{s_1+j}(\alpha)}$ for $j \in [s_2]$, then the ideal lattice is equivalent to $\sigma_\alpha(\mathcal{I})$, with $\mathcal{I}$ being an ideal of the number field.

Also, for the twisted embedding, it is possible to express the diagonal matrix D as a linear transformation $t_\alpha : \mathbb{R}^n \to \mathbb{R}^n$ that can be defined as

$$\begin{aligned}t_\alpha(b_i) = b_i \cdot \big(&\sqrt{\sigma_1(\alpha)}, \ldots, \sqrt{\sigma_{s_1}(\alpha)},\\ &\sqrt{2\sigma_{s_1+1}(\alpha)}, \sqrt{2\sigma_{s_1+1}(\alpha)}, \ldots,\\ &\sqrt{2\sigma_{s_1+s_2}(\alpha)}, \sqrt{2\sigma_{s_1+s_2}(\alpha)}\big),\end{aligned}$$

for each $i \in [n]$, such that $\{b_1, \ldots, b_n\} \in \mathbb{R}^{n\times n}$ is the canonical basis of $\mathbb{R}^n$. Notice that t_α admits inverse as D is a diagonal matrix with non-zero elements in its diagonal. Similarly, the twisted canonical embedding parameterized by $\alpha \in K$ can be defined as the composition

$$\sigma_\alpha \triangleq (t_\alpha \circ \sigma) : K \to \mathbb{R}^n.$$

It can be shown that, if α is such that $Tr(\alpha R) \subset \mathbb{Z}$, then $\sigma_\alpha(\mathcal{I})$ is a lattice over $\mathbb{R}^n$ for any ideal $\mathcal{I}$ of $\mathcal{O}_K$ of rank equal to the extension degree of K.

2.2 The Ring-LWE problem

The Ring-LWE distribution is parameterized by a number field K with ring of integers $R = \mathcal{O}_K$, and an integer modulus $q \geq 2$. Let $\mathcal{I}_q$ denotes the quotient $\mathcal{I}/q\mathcal{I}$ with $\mathcal{I}$ a fractional ideal. The dual of an ideal $\mathcal{I}$ is denoted by $\mathcal{I}^\vee$, and $\mathbb{T}$ is defined as $K_{\mathbb{R}}/R^\vee$.

[4]The monomorphisms, or injective ring homomorphisms, preserves both addition and multiplication in $\mathbb{R}^n$.

Definition 2 ([LPR10] Ring-LWE distribution). *For $s \in R_q^\vee$, often called the secret, and an error distribution ψ over $K_\mathbb{R}$, a sample from the Ring-LWE distribution $A_{s,\psi}$ over $R_q \times \mathbb{T}$ is generated by choosing $a \leftarrow R_q$ uniformly at random, choosing $e \leftarrow \psi$, and outputting $(a, b = (a \cdot s)/q + e \mod R^\vee)$.*

Definition 3 ([LPR10] Search-Ring-LWE). *Let Ψ be a family of distributions over $K_\mathbb{R}$. The search version of the Ring-LWE problem, denoted search-Ring-LWE$_{q,\Psi}$, is defined as follows: given access to arbitrary many independent samples from $A_{s,\psi}$, the Ring-LWE distribution, for some arbitrary $s \in R_q^\vee$ and $\psi \in \Psi$, find s.*

Definition 4 ([LPR10] Decision-Ring-LWE). *Let Ψ be a family of error distributions, each over $K_\mathbb{R}$. The average-case decision version of the Ring-LWE problem, denoted decision-Ring-LWE$_{q,\Psi}$, is to distinguish with non-negligible advantage between arbitrary many independent samples from $A_{s,\pi}$, for a random choice of $(s, \pi) \leftarrow U(R_q^\vee) \times \Psi$, and the same number of uniformly random and independent samples from $R_q \times \mathbb{T}$.*

3 The class of problems α-Ring-LWE

In this section, we introduce a variation of the Ring-LWE class of problems denoted by α-Ring-LWE. It uses the twisted canonical embedding in order to obtain a geometrical view of K. In the first moment, it leads to the addition of α as a new Ring-LWE parameter, which is an appropriately chosen totally positive element of K. It may allow the construction of integer lattices, replacing the discrete version of Ring-LWE, and providing a more powerful tool for generating other classes of lattices. Moreover, we can provide a hardness proof transitively based on a hard problem over lattices. Considering there is a quantum reduction from the SIVP[5] problem to Ring-LWE for both decision and search versions [LPR10, PRSD17a], it suffices to prove that Ring-LWE is reducible to α-Ring-LWE.

In the following, we redefine some notions that are affected by adding a factor to the canonical embedding, which are basically the geometrical view of the number field and the error distribution. As in [LPR10], we take the error distribution as a spherical Gaussian distribution with parameter r.

[5]Shortest Integer Vectors Problem.

3.1 Gaussian distribution

Let the field trace and norm be defined in terms of the sum and product of the embeddings, respectively, as follows:

$$Tr(x) = \sum_{i \in [n]} \sigma_i(x) \text{ and } N(x) = \prod_{i \in [n]} \sigma_i(x).$$

Additionally, for all $x, y \in K$,

$$Tr(xy) = \sum_{i \in [n]} \sigma_i(x) \cdot \sigma_i(y) = \langle \sigma(x), \overline{\sigma(y)} \rangle.$$

As originally stated in [LPR10], the Gaussian function $\rho_r : \mathbb{R}^n \to (0, 1]$, for $r > 0$, is

$$\rho_r(x) = \exp(-\pi \cdot \|x\|^2 / r^2).$$

Considering that $\|x\| = \|\sigma(x)\|$, for $x \in K$, we can redefine the Gaussian function $\rho_r : \mathbb{R}^n \to (0, 1]$ in terms of the trace of K with respect to the embedding. Combining the facts that $\|x\| = \|\sigma(x)\| = \sqrt{\langle x, x \rangle}$, and $Tr(x\overline{x}) = \langle \sigma(x), \sigma(x) \rangle$, we obtain

$$\rho_r(\sigma(x)) = \exp(-\pi \cdot Tr(x\overline{x}) / r^2),$$

for the canonical embedding. For the twisted embedding, the *Gaussian function* is defined as $\rho_{\tilde{r}}(\sigma_\alpha(x)) = \exp(-\pi \cdot Tr(x\overline{x})/\tilde{r}^2)$, with parameter $\tilde{r} = r/\sqrt{\sigma(\alpha_i)}$, where the square root and the division are taken coefficient-wise.

Then, for a lattice Λ and a point u both in $\mathbb{R}^n$, the *discrete Gaussian distribution* over the coset $\Lambda + u$ parameterized by $\tilde{r} > 0$ is defined by

$$D_{\Lambda+u,\tilde{r}}(x) = \frac{\rho_{\tilde{r}}(x)}{\rho_{\tilde{r}}(\Lambda + u)}, \forall x \in (\Lambda + u).$$

3.2 Hardness of α-Ring-LWE

Considering the new definition of Gaussian distribution, we are able to informally define both variants of the Ring-LWE class of problems using the twisted embedding along with their security proofs.

Definition 5 (α-Ring-LWE distribution). *For $s \in R_q^\vee$, often called the secret, and an error distribution ψ_α over $K_\mathbb{R}$, a sample from the α-Ring-LWE distribution $A_{\alpha,s,\psi}$ over $R_q \times \mathbb{T}$ is generated by choosing $a \leftarrow R_q$ uniformly at random, choosing $e \leftarrow \psi_\alpha$, and outputting $(a, b = (a \cdot s)/q + e \mod R^\vee)$.*

Theorem 1. *For any totally positive $\alpha \in K$, the search-Ring-LWE$_{q,\Psi}$ is re-*

ducible to the search version of α-Ring-LWE, i.e. search-Ring-LWE $\leq$ search-α-Ring-LWE.

Proof. We will show that, given an algorithm that solves the search version of α-Ring-LWE, then the search-Ring-LWE is solvable in polynomial time. Given a set of independent Ring-LWE samples of the form

$$(a_i, b_i = a_i \cdot s + e_i \mod qR^\vee),$$

such that $e_i = \sigma^{-1}(\tilde{e}_i)$ and $\tilde{e}_i \leftarrow \psi$, solving the search-Ring-LWE problem is to find the secret s. Taking the smallest integer positive representative of each coordinate of a_i and b_i in $\mathbb{Z}/q\mathbb{Z}$, it is possible to write the above samples as

$$\left(a_i, b_i = a_i \cdot s + \sigma^{-1}(\tilde{e}_i)\right).$$

Applying the ring homomorphism σ in the set of samples, we take its representatives in $\mathbb{R}^n$, that are

$$(\sigma(a_i), \sigma(a_i) \cdot \sigma(s) + \tilde{e_i}).$$

Using the linear transformation t_α, we expand the samples in $\mathbb{R}^n$ by the factor α, obtaining

$$((t_\alpha \circ \sigma)(a_i), (t_\alpha \circ \sigma)(a_i) \cdot \sigma(s) + t_\alpha(\tilde{e_i})),$$

which can be seen as

$$(\sigma_\alpha(a_i), \sigma_\alpha(a_i) \cdot \sigma(s) + t_\alpha(\tilde{e_i})).$$

Finally, by applying the inverse transformation σ_α^{-1}, we obtain the α-Ring-LWE instance to be solved:

$$\left(a_i,\ a_i \cdot (\sigma_\alpha^{-1} \circ \sigma)(s) + \sigma_\alpha^{-1}(t_\alpha(\tilde{e_i}))\right).$$

Now, using the algorithm that solves α-Ring-LWE we get as an answer the element $\tilde{s} = (\sigma_\alpha^{-1} \circ \sigma)(s)$ corresponding to the set of samples given as input to Ring-LWE. From the value of $\tilde{s}$, we recover the solution to the Ring-LWE instance by computing σ_α and σ^{-1} over $\tilde{s}$ in this sequence, i.e.

$$s = (\sigma^{-1} \circ \sigma_\alpha)(\tilde{s}).$$

□

Similarly to the reduction for the search version of α-Ring-LWE problem, for the decision variant, we make use of the same steps to convert samples from the $A_{s,\psi}$ distribution to $A_{\alpha,s,\psi}$. We assume there exists an algorithm that, given a set of m samples, decides which samples were obtained from $A_{\alpha,s,\psi}$ or uniformly taken from $R_q \times \mathbb{T}$.

Theorem 2. *For any totally positive $\alpha \in K$, the decision-Ring-LWE$_{q,\Psi}$ is reducible to the decision version of α-Ring-LWE, i.e. decision-Ring-LWE $\leq$ decision-α-Ring-LWE.*

Proof. Given a set of m elements of $R_q \times \mathbb{T}$ as input to the decision-Ring-LWE problem, we apply the sequence of transformations σ, t_α, and σ_α^{-1} in each element. If the sample was obtained from $A_{s,\psi}$, it has the form $\big(a_i,\ a_i \cdot (\sigma_\alpha^{-1} \circ \sigma)(s) + \sigma_\alpha^{-1}(t_\alpha(\tilde{e_i}))\big)$. Otherwise, it is simply (a_i, b_i). Then, the algorithm that solves the decision version of α-Ring-LWE problem outputs a set of $m/2$ elements distinct from the uniform distribution. By applying σ_α and σ^{-1}, in this sequence, we find the samples originally obtained from the Ring-LWE distribution, which are the output of the algorithm that solves the decision-Ring-LWE problem. □

4 A construction of Integer Lattice

Using the twisted embedding, an ideal lattice is $\Lambda = \sigma_\alpha(\mathcal{I})$ for an ideal $\mathcal{I}$. Once the canonical embedding is a specialization of its twisted form, adding a distortion enables the construction of rotated lattices. An example in the construction of the $\mathbb{Z}^n$-lattice described in [BFOV04]. This construction is on the maximal real subfield of a cyclotomic field.

Let $p \geq 5$ be a prime number such that $n = (p-1)/2$ and $\zeta = \zeta_p = \exp(-2\pi i/p)$, the p-th root of unity. The rotated $\mathbb{Z}^n$-lattices are built via the ring of integers of the maximal real subfield $K = \mathbb{Q}(\zeta + \zeta^{-1})$ with $\alpha \in K$ defined as $\alpha = (1-\zeta)(1-\zeta^{-1})$.

By taking $p = 27$, we compute the irreducible polynomial corresponding to K using the SageMath system with the source code depict in the following.

```
p = 27
CC = CyclotomicField(p)
CC.maximal_totally_real_subfield()
```

The resulting minimal polynomial is

$$f(x) = x^{14} + x^{13} - 13x^{12} - 12x^{11} + 66x^{10} + 55x^9 - 165x^8 - 120x^7 + 210x^6 + 126x^5 - 126x^4 - 56x^3 + 28x^2 + 7x - 1.$$

In experimental results, when using $q = 224{,}737$ and $\sigma = 2.0$, an implementation of the Ring-LWE encryption scheme, which is based on the description of Clercq et al. in [dCRVV15], was able to successfully encrypt and decrypt a large number of arbitrary 256-bit messages.

5 Future Work

Although the process of building lattices using the twisted embedding is already clear, some questions remain uncertain in the cryptographic context and when characterizing the generated lattice. For example, finding a suitable number field element α may be a challenging task since it influences in the embedding coordinates and then in the norm of the lattice vectors. Moreover, rethinking the lattice generation process opens to the opportunity of embedding $\mathbb{Z}$-modules instead of ideals in order to construct lattices. Then, our hardness results require a careful analysis since not every module is an ideal as well. Finally, we still need to define which lattice and number field properties are desirable for ideal-lattice cryptography, i.e. being a Galois field, lattice density, others. In this sense, our future work consists in trying out for number field instantiations in order to find secure system parameters or even lattices constructions that may overcome the well studied cyclotomic number field in terms of lattice capabilities, security, and suitability to efficient implementations.

References

[ADPS16] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange—a new hope. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 327–343, Austin, TX, 2016. USENIX Association.

[BCLvV16] Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal. NTRU Prime: reducing attack surface at low cost. Cryptology ePrint Archive, Report 2016/461, 2016. `http://eprint.iacr.org/2016/461`.

[BFOV04] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo. New algebraic constructions of rotated zn-lattice constellations for the rayleigh fading channel. *IEEE Transactions on Information Theory*, 50(4):702–714, April 2004.

[BV11] Zvika Brakerski and Vinod Vaikuntanathan. Fully Homomorphic Encryption from ring-LWE and Security for Key Dependent Messages. In *Proceedings of the 31st Annual Conference on Advances in Cryptology*, CRYPTO'11, pages 505–524, Berlin, Heidelberg, 2011. Springer-Verlag.

[CGS13] Peter Campbell, Michael Groves, and Dan Shepherd. SOLILOQUY: A Cautionary Tale. *Docbox.Etsi.Org*, pages 1–9, 2013.

[CIV16a] Wouter Castryck, Ilia Iliashenko, and Frederik Vercauteren. On error distributions in ring-based LWE. *LMS Journal of Computation and Mathematics*, 19(A):130–145, 2016.

[CIV16b] Wouter Castryck, Ilia Iliashenko, and Frederik Vercauteren. Provably Weak Instances of Ring-LWE Revisited. In *Proceedings of the 35th Annual International Conference on Advances in Cryptology — EUROCRYPT 2016 - Volume 9665*, pages 147–167, New York, NY, USA, 2016. Springer-Verlag New York, Inc.

[CLS15] Hao Chen, Kristin E. Lauter, and Katherine E. Stange. Attacks on the Search-RLWE problem with small error. Cryptology ePrint Archive, Report 2015/971, 2015. `https://eprint.iacr.org/2015/971`.

[CLS16] Hao Chen, Kristin Lauter, and Katherine E. Stange. Security considerations for Galois non-dual RLWE families. Cryptology ePrint Archive, Report 2016/193, 2016. `https://eprint.iacr.org/2016/193`.

[dCRVV15] R. de Clercq, S. S. Roy, F. Vercauteren, and I. Verbauwhede. Efficient software implementation of ring-lwe encryption. In *2015 Design, Automation Test in Europe Conference Exhibition (DATE)*, pages 339–344, March 2015.

[EHL14] Kirsten Eisenträger, Sean Hallgren, and Kristin Lauter. *Weak Instances of PLWE*, pages 183–194. Springer International Publishing, Cham, 2014.

[ELOS15] Yara Elias, Kristin E. Lauter, Ekin Ozman, and Katherine E. Stange. *Provably Weak Instances of Ring-LWE*, pages 63–92. Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[Goo16] Google. Experimenting with Post-Quantum Cryptography, 2016. `https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html`.

[LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. *On Ideal Lattices and Learning with Errors over Rings*, pages 1–23. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[LPR13] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. A Toolkit for Ring-LWE Cryptography. Cryptology ePrint Archive, Report 2013/293, 2013. `http://eprint.iacr.org/2013/293`.

[NIS17] National Institute of Standards and Technology - NIST. Post-Quantum Crypto Standardization, 2017. `http://csrc.nist.gov/groups/ST/post-quantum-crypto/cfp-announce-dec2016.html`.

[OV04] Frédérique Oggier and Emanuele Viterbo. Algebraic Number Theory and Code Design for Rayleigh Fading Channels. *Commun. Inf. Theory*, 1(3):333–416, December 2004.

[PRSD17a] Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz. Pseudorandomness of Ring-LWE for Any Ring and Modulus. Cryptology ePrint Archive, Report 2017/258, 2017. `http://eprint.iacr.org/2017/258`.

[PRSD17b] Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz. Pseudorandomness of Ring-LWE for Any Ring and Modulus (Slides), 2017. `https://web.eecs.umich.edu/~cpeikert/pubs/slides-anyring.pdf`.

[Sho97] Peter W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.*, 26(5):1484–1509, October 1997.

[SV10] N. P. Smart and F. Vercauteren. *Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes*, pages 420–443. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[Wü02] Gisbert Wüstholz, editor. *A Panorama of Number Theory or The View from Baker's Garden*. Cambridge University Press, 2002.