Characterizing Insecure Error Distributions For Various RLWE Problems

A Thesis Presented

by

Alec L. Critten

to

The Honors College

of

The University of Vermont

In Partial Fulfillment of the Requirements
for the Honors Degree of Bachelor of Science
Majoring in Mathematics

May, 2021

Defense Date: April 13, 2021
Thesis Examination Committee:

Christelle Vincent, Ph.D., Advisor
Taylor Dupuy, Ph.D.

Abstract

This thesis studies how a chosen set of parameters for a Ring Learning With Errors (RLWE) cryptographic instance affects its ability to withstand a certain type of attack. We begin with some non-technical motivation on the specific qualities of RLWE that support its candidacy as a post-quantum cryptographic protocol, and why such protocols are necessary due to recent developments in computing. We then discuss some of the context for RLWE, providing some overview on important concepts in algebraic number theory that underpin the mathematical structure of RLWE. We define several variants of RLWE which researchers in this field have analyzed, provide some detail on how these variants relate to each other, and cover some of the types of attacks against these variants. Following this overview, we introduce the experimental phase of this thesis project and cover the functionality of a program used to simulate a RLWE attack. Finally, we analyze some data generated as a result of tests run on our program and briefly discuss how it relates to previous hypotheses on how a RLWE instance's security should be characterized.

In memory of Maria Carmen Rodriguez and David Lee Critten

Acknowledgements

There are several people who I am incredibly appreciative for, and without whom this thesis project would not have been realized. Firstly, I would like to express gratitude to my family for their personal support and for keeping me motivated, especially in light of the tumultuous global events that occurred in the time this thesis was developed. I am thankful for the academic support of the University of Vermont's Honors College. I am also grateful to Professor Taylor Dupuy for being on the thesis committee. Immense thanks are due as well to Sarah Days-Merrill, with whom I worked alongside for this project and who provided essential and very helpful feedback in the process of writing this thesis.

Finally, this thesis would not have been at all possible without the support of my advisor, Dr. Christelle Vincent. This project has been greatly inspiring for me, and I am grateful for what I have learned from her both in terms of mathematics and in navigating the research process. Dr. Vincent has been crucial in helping me discover my passion for mathematics and develop my confidence in my mathematical ability, for which I am deeply indebted. My time at the University of Vermont has been illuminating, and I hope that this project is reflective of the academic and personal development that occurred during my time there.

Table of Contents

List of Figures

Chapter 1

Introduction

This thesis project studies a new computational problem introduced in the last twenty years known as *Ring Learning with Errors* (RLWE). The cryptosystem based on this problem is considered by researchers as a viable candidate for encryption that is both quantum-safe as well as fully-homomorphic.

As the theoretical conceptualization of the quantum computer has become ever-closer to concrete implementations in the last few years, many of the cryptographic protocols used in practice will become insecure once quantum computers are built. Therefore, as intelligence agencies and other entities have announced their intent to abandon these encryption schemes, a secure replacement is needed. Much of the current cryptographic research has been focused on a new class of problems, which includes RLWE, that are computationally hard to solve for classical as well as non-classical computers.

Additionally, RLWE is desirable as a candidate for fully-homomorphic encryption. We say that a hypothetical encryption scheme is *fully-homomorphic* if it respects the properties of a ring homomorphism (a mapping between two rings that preserves the familiar arithmetic operations of addition and multiplication) between data in its unencrypted and encrypted states. The fully-homomorphic property is of practical interest because it allows for one to perform computations and analysis on encrypted data, therefore protecting the data's sensitivity as well as allowing remote computations in cases where it is stored in a database or cloud server.

There are several points of interest in the previous work on this topic that we wish to investigate further. Firstly, we wish to study the bijection between the various types of rings in each variant of RLWE. This will give us a clearer ability to translate security parameters between these variants (specifically, generalizing the conditions set by [Pei16] to ensure invulnerability of dual-RLWE under certain attacks), understand exactly how the RLWE parameters affect an instance's security (particularly the relationship between the norm of the prime modulus and the width of the statistical distribution), and unify the study of the types of attacks on these cryptosystems.

During our research, we worked to apply an attack described in the literature as testable code. Using this newly-developed code, we deployed this attack on these cryptosystems and tested the security of various parameters described in the literature. We compared the results of these tests to the literature and identify any discrepancies between the results. To this end, our goal in this project was to understand if the security parameters in [Pei16] are sufficient or merely necessary in regards to their strictness.

Chapter 2

Background

2.1 Historical Context for RLWE

For decades, cryptosystems based on classically-hard problems have been considered safe from attacks. The well-known RSA cryptosystem, for example, uses the number-theoretical problem of integer factorization and derives its security from the fact that this problem cannot be solved by an attacker using a non-quantum computer in a reasonable amount of time. However, the development of quantum computers in recent years has warranted the need for cryptosystems based on a quantum-hard as well as classically-hard problem. Indeed, in 1995 Shor gave an algorithm to factor integers in quantum polynomial time in [Sho97]. Much of the research presented in the literature on Ring Learning with Errors was conducted and written in the mid-2010s as quantum-safe security became a non-theoretical concern. As such, many of the articles on this subject are in direct response with each other and/or present potential improvements on the general RLWE scheme.

Provably secure encryption schemes based on lattice problems were first suggested in 1996 by Ajtai in [Ajt96], but it was not until 2005 that the first instance of the more general Learning With Errors problem and its applications to cryptography were formulated by Regev in [Reg05]. In the years following this, the hardness of finding the shortest vector in "ideal lattices" was studied extensively, and ideal lattices were used to give several cryptographic constructions in [LM06, PR06, Mic07].

Other works related to this thesis are [LM18], where the authors present a signature scheme based on the PLWE problem we present here, [PR07], where the authors present a signature scheme based on the RLWE problem, and [LPR10, LPR13], where the authors present a signature scheme based on the dual-RLWE problem.

Even though it is not a focus of this thesis, another reason why RLWE is so studied is that it is an instance of an encryption scheme that can be made to be fully-homomorphic. The idea of a fully-homomorphic encryption scheme was first suggested in 1978 (the same year the RSA cryptosystem was introduced) by Rivest, Adleman and Dertouzos in [RAD78] as they described the first public key encryption scheme. However, the authors were not able to give an actual example of a fully-homomorphic scheme, and they could only talk about what properties it might have and what might be true about it.

Some notable steps towards a fully homomorphic scheme are [SYY99], and [BGN05], who both give semi-homomorphic schemes that each in their own way fall just short of being fully-homomorphic. It was not until 2009 that Gentry in [Gen09] gave the first construction of a fully-homomorphic scheme, using the RLWE problem we present here. More immediately, our research is directly influenced by the articles [CLS17a, CLS17b, EHL14, ELOS15, ELOS16, Pei16, CIV16a, CIV16b], which study closely related questions.

For our research, there are three variants of RLWE cryptography that we will consider - Polynomial Learning with Errors (PLWE), primal-RLWE, and dual-RLWE. We will test the security of instances of PLWE as presented in the literature, as well as consider the bijection between the polynomial rings used in PLWE and the rings of integers of non-dual RLWE. Before detailing the RLWE problem and explaining each of its variants, we recall some relevant concepts from algebraic number theory.

2.2 Algebraic Number Theory

We introduce several key definitions, starting with the most fundamental concepts to our work.

Definition 2.2.1 (Algebraic Number Field)**.** An *algebraic number field* K is a finite extension of the field of rational numbers.

We are particularly interested in a subring of K, known as the *ring of integers*.

Definition 2.2.2 (Ring of Integers)**.** Let K be a number field. The *ring of integers*, typically denoted $\mathcal{O}_K$, is the subring of K that contains all the elements of K whose monic minimal polynomial has coefficients in the integers (as opposed to the elements whose monic minimal polynomial has coefficients in $\mathbb{Q}$).

Note that $\mathbb{Z}$ is always a subset of $\mathcal{O}_K$, and in fact it is the smallest possible ring of integers.

Definition 2.2.3 (Fractional Ideal)**.** Let R be an integral domain and let K be its field of fractions (K is the smallest field R can be embedded in). A *fractional ideal* of R is an R-submodule I of K such that there exists a nonzero $r \in R$ such that $rI \subseteq R$.

This latter concept is important in algebraic number theory; for instance, $\mathcal{O}_K$ is a fractional ideal of K. Now, we define a certain type of embedding and a set that contains it, the latter concept of which is essential to the RLWE computational problem.

Definition 2.2.4 (Minkowski Embedding)**.** Let K be a number field. A *Minkowski embedding* is a nonzero map $f : K \to \mathbb{C}$ that sends elements of an algebraic number field into the field of complex numbers.

Note that embeddings from K into the real numbers are also Minkowski embeddings, since $\mathbb{R} \subset \mathbb{C}$.

Definition 2.2.5 (Canonical Embedding)**.** Let K be a number field, s_1 be the number of real Minkowski embeddings, and s_2 be the number of all its pairs of complex Minkowski embeddings. The oftuple all Minkowski embeddings of an algebraic number field K forms a larger function $M : K \to \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2}$, known as the *canonical embedding*.

The image of $\mathcal{O}_K$ under the map M is the space we are interested in; after applying the canonical embedding, $M(\mathcal{O}_K)$ forms a structure known as a *lattice*.

Definition 2.2.6 (Lattice)**.** A *lattice* L in K is defined as the $\mathbb{Z}$-span of a $\mathbb{Q}$-basis of K.

One important function we will need later is the trace product. We define the *trace product* in terms of the real and complex embeddings of K, where $\alpha \in K$, σ_i are the real embeddings, and τ_i are a choirce of one element from each pair of complex embeddings:

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{s_1} \sigma_i(\alpha) + \sum_{i=1}^{s_2} \left(\tau_i(\alpha) + \overline{\tau_i(\alpha)}\right).$$

Note that $[K : \mathbb{Q}] = n = s_1 + 2s_2$, exactly the dimension of the geometric space in which the lattice points are placed. A generalized formal definition of the trace product follows.

Definition 2.2.7 (Trace Product)**.** Let K be an algebraic number field, L be a lattice in K, and σ_i for $i = 1, \ldots, n$ be the Minkowski embeddings of K. The *trace product* function, denoted $\mathrm{Tr}_{K/\mathbb{Q}}(xy)$ for $x \in K, y \in L$, is defined as:

$$\mathrm{Tr}_{K/\mathbb{Q}}(xy) = \langle M(x), \overline{M(y)} \rangle = \sum_{i=1}^{n} \sigma_i(x)\sigma_i(y)$$

This function behaves similarly to the familiar dot product operation from linear algebra.

2.3 Non-Dual RLWE Definitions

The RLWE cryptography scheme (known as primal-RLWE or non-dual RLWE, described in detail in [CLS17a]) consists of a ring (typically the ring of integers $\mathcal{O}_K$ of an algebraic number field K), a prime modulus q, and an error distribution (either a Gaussian distribution or a discretization of a Gaussian). We consider the ring R modulo qR, henceforth referred to as R_q.

There are two problems that utilize these parameters - a *search* problem and a *de-*

cision problem (much of the following information is taken from Section 2 of [CLS17a] and [ELOS16], and we refer the reader to these sources for a more mathematically-rigorous description of these problems). In both (non-dual) problems, sample pairs (a, b) from $R_q \times R_q$ are constructed. The value of a is independent (sampled from a uniformly-random distribution), and b is dependent on a such that $b = as + e$, where e is a relatively small error added to the value as a security measure and sampled from a Gaussian distribution whose wideness is determined by a parameter $\sigma \in \mathbb{R}_{>0}$, and s is a secret value in R_q. Finally, we give definitions for the two non-dual RLWE problems.

Definition 2.3.1 (The Non-Dual RLWE Search Problem)**.** The objective of the *search problem* is to discover a secret $s \in R_q$ directly given an arbitrary number of samples (a, b) from $R_q \times R_q$ with $b = as + e$.

Definition 2.3.2 (The Non-Dual RLWE Decision Problem)**.** The objective of the *decision problem* is to distinguish samples (a, b) with $b = as + e$ from those in a uniformly random distribution of $R_q \times R_q$.

2.4 RLWE Variants and Cryptographic Reductions

There are two other variants of RLWE that are important to note, as they are discussed together with primal-RLWE (as outlined above) in security considerations. These two variants are known as Polynomial Learning with Errors (PLWE) and dual-RLWE.

2.4.1 RLWE Variants

Polynomial Learning with Errors

Firstly, we give a formal definition of RLWE's polynomial-ring variant, PLWE (the articles [ELOS16] and [EHL14] are recommended for further reading on this subject).

Definition 2.4.1 (Polynomial Learning with Errors)**.** An instance of *Polynomial Learning with Errors* consists of the following:

- A polynomial ring $P_q = \mathbb{F}_q[x]/(f(x))$, where $f(x)$ is a monic irreducible polynomial with $\mathbb{F}_q$-coefficients that splits completely over $\mathbb{F}_q$ and has degree n,
- A prime modulus $q \in \mathbb{Z}$,
- A basis for the polynomial ring,
- A parameter $\sigma \in \mathbb{R}^{>0}$ specifying the width of the spherical discretized Gaussian error distribution.

Like primal-RLWE, PLWE has an analogous search problem (to find $s(x)$ given samples $(a_i(x), b_i(x) = a_i(x)s(x) + e_i(x)) \in P_q \times P_q)$ and decision problem (to distinguish between PLWE samples and uniformly random samples from $P_q \times P_q$).

Dual-RLWE

Dual-RLWE is a variant of primal-RLWE where the secret s and the errors e_i belong to the dual of the ring R parameterizing the instance. In a number field, the dual of a lattice also has a lattice structure. Dual-RLWE is detailed and defined in [Pei16], which we use as a primary point of reference for much of the background work described in this section; much of the algebraic number theory involved in a general non-cryptographic setting is covered in detail in [Con09], from which we use the definition of the dual lattice.

Definition 2.4.2 (Dual Lattice)**.** Let K be a number field and L be a lattice in K. The *dual* of L is

$$L^\vee = \{\alpha \in K : \mathrm{Tr}_{K/\mathbb{Q}}(\alpha \mathcal{L}) \subset \mathbb{Z}\},$$

where $\mathrm{Tr}_{K/\mathbb{Q}}$ is the notation for the trace product function from section 2.2.

In [Con09], it is proven that to check whether an element α of K is in the dual lattice, it suffices to verify that the trace product of α with the basis elements of the lattice is an integer. Because only the basis is required to represent the lattice as a whole, this gives a straightforward way to compute the elements of $L^\vee$. Additionally, note that the dual lattice has the two important properties that $(L^\vee)^\vee = L$ and that $L_1 \subset L_2$ if and only if $L_2^\vee \subset L_1^\vee$.

Although non-intuitive from an elementary perspective, this lattice counterpart is not particularly difficult to compute and express concisely.

2.4.2 Cryptographic Reductions

In this section we discuss how the search and decision problems discussed in 2.3 relate to each other. Of note is the discussion in [CLS17a] on how to convert the search RLWE problem to a decision RLWE problem for Galois number fields. This reduction shows that the search and decision RLWE problems are equivalent in their relative computational hardness under certain assumptions.

Reductions and resultant comparisons of computational hardness exist between the different variants of RLWE beyond the search-decision reduction, as well. For instance, as discussed in Section 5 of [ELOS16], a connection between non-dual RLWE and PLWE is the reduction of the former problem to the latter by considering rings $R_q \cong P_q$ in this case the only distinction is the choice of error distribution (note that the spherical Gaussian in RLWE is not equivalent to the discretized Gaussian in PLWE).

Section 2.3 of [CLS17b] discusses an equivalency between dual and non-dual RLWE in particular under the assumption that the dual ring of $R^\vee$ is principal as a fractional ideal (meaning that $R^\vee$ is generated by a single element). There are numerous other qualitative comparisons based on computational hardness that relate the different variants of the general RLWE problem together, and help conceptually generalize the nature of RLWE attacks.

2.5 Attacks on RLWE-Family Problems

Now we discuss the attacks on RLWE and its related problems as covered in the literature. The *Chi-square attack* in [CLS17a] is an example of a more general type of attack on the decision version of RLWE which applies a ring homomorphism from the RLWE ring R_q to a finite field $\mathbb{F}_q$. If q is small enough, the attack guesses the image of the secret as an element of $\mathbb{F}_q$ instead of R_q, and then examines the distribution of the samples to see if it relates to the error distribution through a Chi-square statistical test. Note that this type of attack can be modified to attack the search problem. In [CLS17b], the same authors improve on the efficiency of their original Chi-square attack by only considering certain cosets of $\mathbb{F}_q$ instead of the entire finite field.

Another variation on this attack on weak instances of dual-RLWE, as referenced in [Pei16], involves *reduction modulo an ideal divisor of R.* By applying this reduction to R, one can attack a dual-RLWE instance directly if its error distribution is non-uniform or by reducing to error-less LWE which is trivial to solve.

Furthermore, [ELOS16] covers *distinguishing* and *decoding* attacks on (namely, but not exclusively) PLWE instances, both characterized by ring homomorphisms from P_q to smaller rings and reducing the polynomial $p(x)$ to $p(\alpha)$, for small-order roots α of the polynomial modulus of P_q, which is similar to the attacks on the RLWE and dual-RLWE problems.

Chapter 3

Experiment and Results

3.1 Experiment Description and Explanation of Program

For this project, we used a program originally written by Elias, Lauter, Ozman and Stange for the article [ELOS15]. After refactoring this code both to better understand the underlying functionality of the program as well as to adapt it to suit our experimental needs, we proceeded to run several tests. The modified program simulates an RLWE Chi-square attack (as discussed from a theoretical standpoint earlier in 2.5) by taking in the parameters of an RLWE instance, creating RLWE samples, and then attempting to guess the image of the secret in a smaller ring. The parameters which are varied are the polynomial defining the polynomial ring, the modulus, the number of samples to be used in the test, and the number of trials for the program to run.

3.2 Literature Parameters for Security

Much of the discussion contained in the literature centers on the parameters characterizing what the authors can show to be secure or non-secure for RLWE instances. This thesis primarily serves to test these parameters as necessary or merely sufficient in their security. These parameters consist of a number field K with associated prime moduli q and an error-distribution width σ. Our main concern involves the exact cutoffs at which the prime modulus and distribution width affect a RLWE instance's security.

3.3 Experimental Results

Much of the computation done for this project involved finding cases where the attack implemented in the program was successful. We emphasize that a "success" in the context of the program indicates an insecurity, whereas a "failure" indicates the instance's effective defense against the program. In this case we sought a non-zero success rate in 20 randomized trials on the same K, q, and σ parameters. In many number fields, there was a consistent attack success rate of 0 out of 20 trials (or 0 out of 1 trial when done rapidly) for each set of parameters regardless of the choice of q and σ. However, we found seven weak instances on five number fields[1] with non-zero success rates in which we can see how the choice of q and σ directly affect the success/fail ratio of the attack. First, let us consider a composite chart of all seven instances.

[1] Note that the defining polynomial of each number field, along with a comprehensive list of tests, is provided in Appendix I.

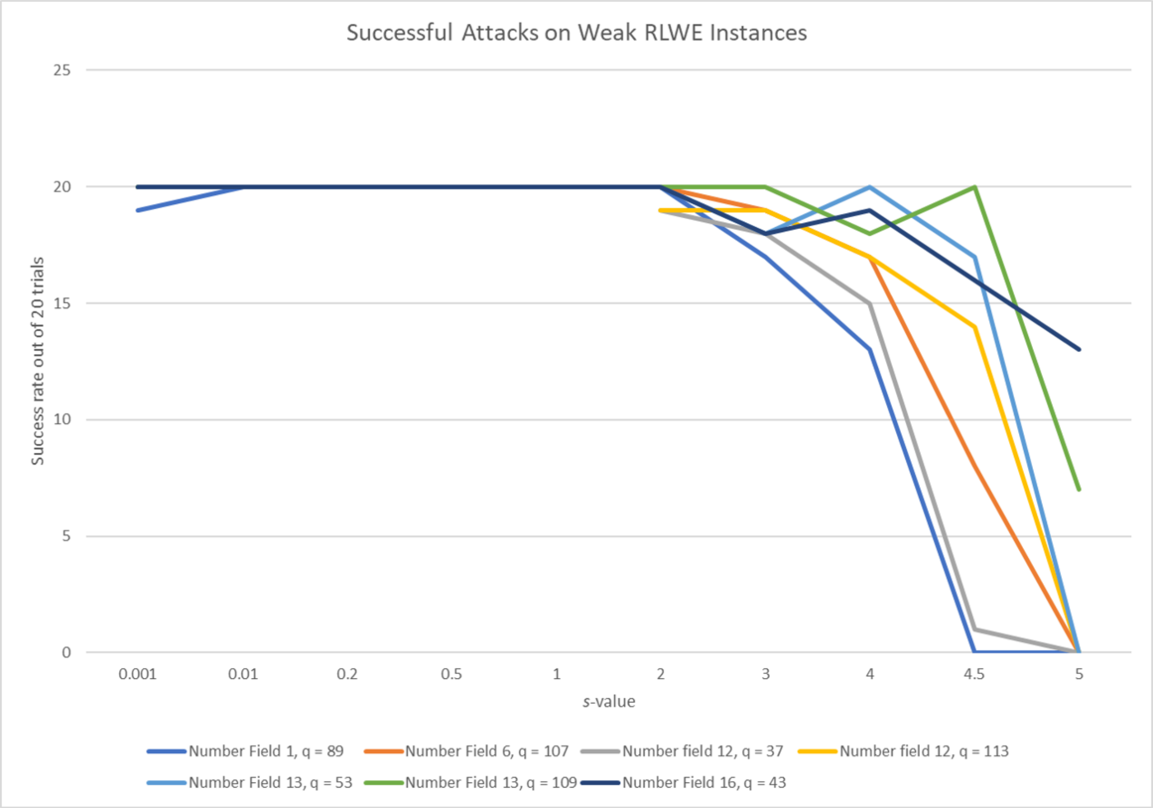

Figure 3.1: The RLWE attack program's success rate on five number field/prime modulus combinations, with varying σ-value, which is denoted by s in this graph.

From this figure, we can see that the width of the error distribution (measured on the x-axis) directly affects the success of the attack simulated in the program. Specifically, we can see that instances with a small distribution (with $\sigma < 2$) is easily susceptible to the attack, whereas those with wider distributions tend to withstand the attack better. Now, we consider the two pairs of instances characterized by the same number field but different prime moduli.

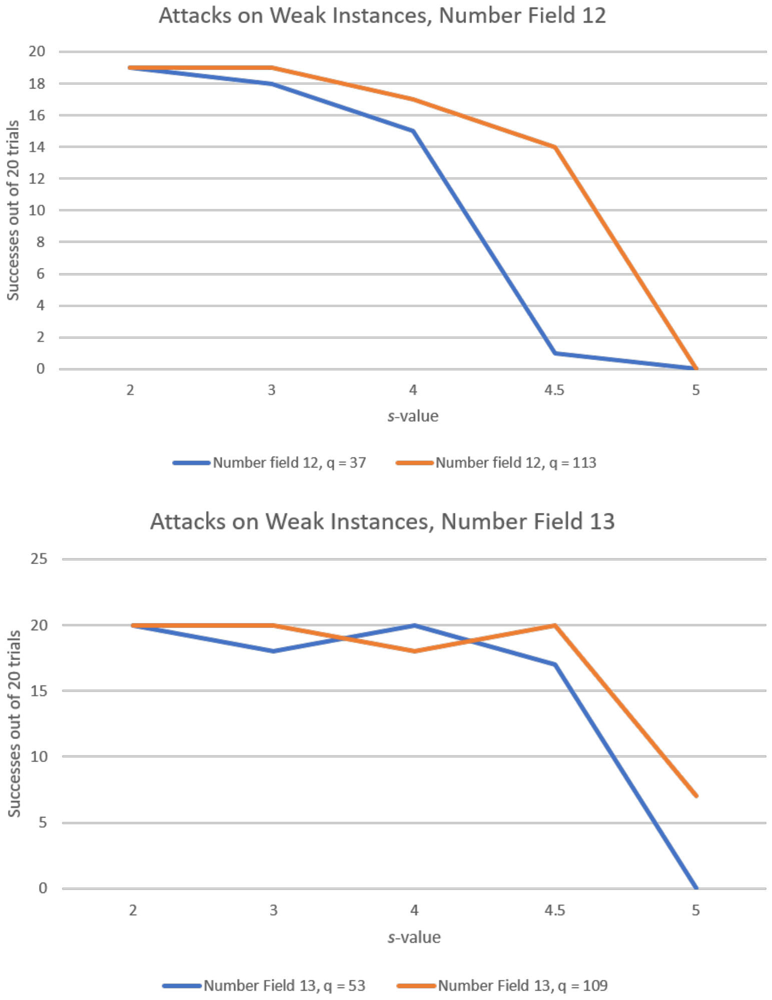

Figure 3.2: The two weak RLWE instances each on number fields 12 and 13.

These four instances, considered separately from those cases with a unique number field, show that the choice of prime modulus also affects the weakness of an RLWE instance. The orange lines in each chart represent the larger of the two prime moduli in each case, and the respective instances are more susceptible to the randomized attacks from our program.

Finally, let us consider the three cases where only one instance from a given number field was found to be insecure.

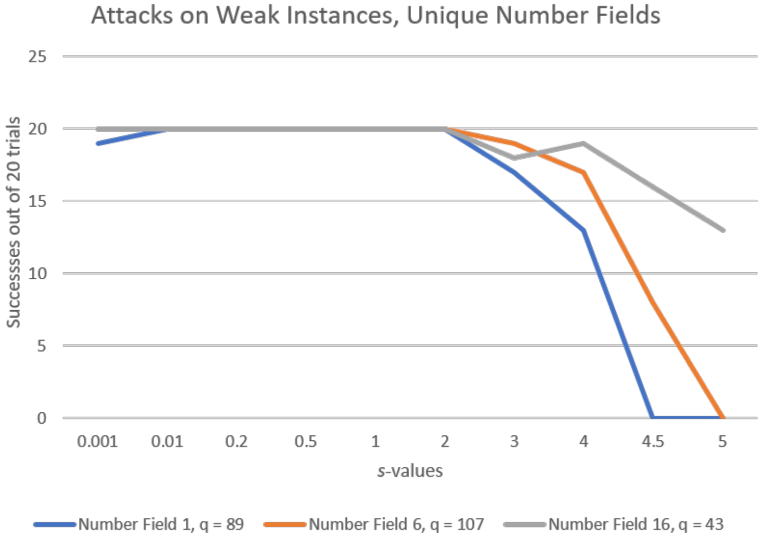

Figure 3.3: The weak RLWE instances with unique number fields.

Note that Number Field 1 has degree 10, Number Field 6 has degree 12, and Number Field 16 has degree 20. Thus, the instance in Figure 3.3 with the largest-degree number field remains the weakest of the three depicted. This suggests that the size of the number field degree may also impact a RLWE instance's security.

While these instances provide insight into how the values of the error-distribution width and prime modulus affect a RLWE instance's weakness, it is currently unknown how the choice of number field definitively affects an instance's security. This would be an interesting point for further research, in addition to further granularizing the σ-value points of success/failure of the attack on weak instances.

Overall, though, our results showing the relationship between a RLWE instance's security and σ are consistent with the hypotheses in [Pei16]. However, we note that Peikert's conditions are sufficient but not necessary due to many instances found where there are no attack successes regardless of the choice of σ (see Appendix I for a comprehensive list). This suggests that the requisite conditions for a RLWE instance's security can be more precisely characterized upon further inquiry.

Bibliography

[Ajt96] M. Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proceedings of the Twenty-eighth Annual ACM Symposium on the Theory of Computing (Philadelphia, PA, 1996)*, pages 99–108. ACM, New York, 1996.

[BGN05] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. Evaluating 2-DNF formulas on ciphertexts. In *Theory of cryptography*, volume 3378 of *Lecture Notes in Comput. Sci.*, pages 325–341. Springer, Berlin, 2005.

[CIV16a] Wouter Castryck, Ilia Iliashenko, and Frederik Vercauteren. On error distributions in ring-based LWE. *LMS J. Comput. Math.*, 19(suppl. A):130–145, 2016.

[CIV16b] Wouter Castryck, Ilia Iliashenko, and Frederik Vercauteren. Provably weak instances of ring-LWE revisited. In *Advances in cryptology—EUROCRYPT 2016. Part I*, volume 9665 of *Lecture Notes in Comput. Sci.*, pages 147–167. Springer, Berlin, 2016.

[CLS17a] Hao Chen, Kristin Lauter, and Katherine E. Stange. Attacks on the search RLWE problem with small errors. *SIAM J. Appl. Algebra Geom.*, 1(1):665–

682, 2017.

[CLS17b] Hao Chen, Kristin Lauter, and Katherine E. Stange. Security considerations for Galois non-dual RLWE families. In Roberto Avanzi and Howard Heys, editors, *Selected Areas in Cryptography – SAC 2016*, pages 443–462, Cham, 2017. Springer International Publishing.

[Con09] Keith Conrad. The different ideal. https://kconrad.math.uconn.edu/blurbs/gradnumthy/different.pdf, 2009.

[EHL14] Kirsten Eisenträger, Sean Hallgren, and Kristin Lauter. Weak Instances of PLWE. In Antoine Joux and Amr Youssef, editors, *Selected Areas in Cryptography – SAC 2014*, volume 8781, pages 183–194. Springer International Publishing, Cham, 2014. Series Title: Lecture Notes in Computer Science.

[ELOS15] Yara Elias, Kristin E. Lauter, Ekin Ozman, and Katherine E. Stange. Provably weak instances of ring-LWE. In *Advances in cryptology—CRYPTO 2015. Part I*, volume 9215 of *Lecture Notes in Comput. Sci.*, pages 63–92. Springer, Heidelberg, 2015.

[ELOS16] Yara Elias, Kristin E. Lauter, Ekin Ozman, and Katherine E. Stange. Ring-LWE cryptography for the number theorist. In *Directions in number theory*, volume 3 of *Assoc. Women Math. Ser.*, pages 271–290. Springer, [Cham], 2016.

[Gen09] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *STOC'09—Proceedings of the 2009 ACM International Symposium on Theory of Computing*, pages 169–178. ACM, New York, 2009.

[LM06] Vadim Lyubashevsky and Daniele Micciancio. Generalized compact knapsacks are collision resistant. In *Automata, languages and programming. Part II*, volume 4052 of *Lecture Notes in Comput. Sci.*, pages 144–155. Springer, Berlin, 2006.

[LM18] Vadim Lyubashevsky and Daniele Micciancio. Asymptotically efficient lattice-based digital signatures. *J. Cryptology*, 31(3):774–797, 2018.

[LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In *Advances in cryptology—EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Comput. Sci.*, pages 1–23. Springer, Berlin, 2010.

[LPR13] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. A toolkit for ring-LWE cryptography. In *Advances in cryptology—EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Comput. Sci.*, pages 35–54. Springer, Heidelberg, 2013.

[Mic07] Daniele Micciancio. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. *Comput. Complexity*, 16(4):365–411, 2007.

[Pei16] Chris Peikert. How (not) to instantiate ring-LWE. In *Security and cryptography for networks*, volume 9841 of *Lecture Notes in Comput. Sci.*, pages 411–430. Springer, [Cham], 2016.

[PR06] Chris Peikert and Alon Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In *Theory of cryptography*, volume 3876 of *Lecture Notes in Comput. Sci.*, pages 145–166. Springer, Berlin, 2006.

[PR07] Chris Peikert and Alon Rosen. Lattices that admit logarithmic worst-case to average-case connection factors. In *STOC'07—Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, pages 478–487. ACM, New York, 2007.

[RAD78] Ronald L. Rivest, Len Adleman, and Michael L. Dertouzos. On data banks and privacy homomorphisms. In *Foundations of secure computation (Workshop, Georgia Inst. Tech., Atlanta, Ga., 1977)*, pages 169–179. 1978.

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *STOC'05: Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, pages 84–93. ACM, New York, 2005.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484â1509, October 1997.

[SYY99] Tomas Sander, Adam Young, and Moti Yung. Non-interactive cryptocomputing for NC^1. In *40th Annual Symposium on Foundations of Computer Science (New York, 1999)*, pages 554–566. IEEE Computer Soc., Los Alamitos, CA, 1999.

Appendix I: Defining Polynomials and Test Results

Below is a table comprising the defining polynomial of each number field that was tested for this project. It is followed by a comprehensive list of every test run, listing the respective number field, prime modulus, σ-value, and success ratio.

Defining Polynomials	
Number Field	Defining Polynomial
Number Field 1	$y^{10} + 9y^8 + 28y^6 + 35y^4 + 15y^2 + 1$
Number Field 2	$y^{12} - y^{11} - 25y^{10} + 25y^9 + 235y^8 - 235y^7 - 1013y^6 + 1013y^5 + 1899y^4 - 1899y^3 - 1013y^2 + 1013y - 181$
Number Field 3	$y^{12} + 11y^{10} + 45y^8 + 84y^6 + 70y^4 + 21y^2 + 1$
Number Field 4	$y^{12} + 13y^{10} + 64y^8 + 146y^6 + 148y^4 + 48y^2 + 1$
Number Field 5	$y^{12} + 12y^{10} + 53y^8 + 104y^6 + 86y^4 + 24y^2 + 1$
Number Field 6	$y^{12} + 12y^{10} + 54y^8 + 112y^6 + 105y^4 + 36y^2 + 1$
Number Field 7	$y^{16} + 16y^{14} + 104y^{12} + 352y^{10} + 660y^8 + 672y^6 + 336y^4 + 64y^2 + 2$

Number Field 8	$y^{16} + 16y^{14} + 105y^{12} + 364y^{10} + 714y^8 + 784y^6 + 440y^4 + 96y^2 + 1$
Number Field 9	$y^{16} + 16y^{14} + 104y^{12} + 352y^{10} + 659y^8 + 664y^6 + 316y^4 + 48y^2 + 1$
Number Field 10	$y^{16}+15y^{14}+91y^{12}+286y^{10}+495y^8+462y^6+210y^4 + 36y^2 + 1$
Number Field 11	$y^{16} + 16y^{14} + 104y^{12} + 352y^{10} + 660y^8 + 672y^6 + 336y^4 + 64y^2 + 2$
Number Field 12	$y^{18} + 17y^{16} + 120y^{14} + 455y^{12} + 1001y^{10} + 1287y^8 + 924y^6 + 330y^4 + 45y^2 + 1$
Number Field 13	$y^{18} + 18y^{16} + 135y^{14} + 546y^{12} + 1287y^{10} + 1782y^8 + 1386y^6 + 540y^4 + 81y^2 + 1$
Number Field 14	$y^{20} + 21y^{18} + 188y^{16} + 934y^{14} + 2806y^{12} + 5202y^{10}+5809y^8+3629y^6+1090y^4+120y^2+1$
Number Field 15	$y^{20} + 20y^{18} + 170y^{16} + 800y^{14} + 2275y^{12} + 4003y^{10}+4280y^8+2605y^6+775y^4+75y^2+1$
Number Field 16	$y^{20} + 20y^{18} + 169y^{16} + 784y^{14} + 2172y^{12} + 3664y^{10}+3683y^8+2072y^6+575y^4+60y^2+1$

Number Field 1		
Prime Modulus	σ-value	Success Ratio
89	0.001	successes: 19/20
89	0.01	successes: 20/20
89	0.2	successes: 20/20
89	0.5	successes: 20/20
89	0.5	successes: 19/20
89	1	successes: 20/20
89	2	successes: 20/20
89	3	successes: 17/20
89	4	successes: 13/20
89	4.5	successes: 0/20
89	5	successes: 0/20
109	0.001	successes: 0/20
109	0.01	successes: 0/20
109	0.2	successes: 0/20
109	0.5	successes: 0/20
109	0.75	successes: 0/20
109	2	successes: 0/20
109	3	successes: 0/20
109	4	successes: 0/20
109	5	successes: 0/20
197	0.5	successes: 0/20

197	2	successes: 0/20
197	3	successes: 0/20
197	4	successes: 0/20
197	5	successes: 0/20
241	0.5	successes: 0/20
241	2	successes: 0/20
241	3	successes: 0/20
617	0.001	successes: 0/20
617	0.01	successes: 0/20
617	0.2	successes: 0/20
661	0.001	successes: 0/1
661	0.01	successes: 0/1
661	0.2	successes: 0/1
661	0.5	successes: 0/1
661	0.75	successes: 0/1

Number Field 2		
Prime Modulus	σ-value	Success Ratio
53	0.001	successes: 0/1
53	0.01	successes: 0/1
53	0.2	successes: 0/1
53	0.5	successes: 0/1
53	0.75	successes: 0/1
79	0.001	successes: 0/1

79	0.01	successes: 0/1
79	0.2	successes: 0/1
79	0.5	successes: 0/1
79	0.75	successes: 0/1

Number Field 3		
Prime Modulus	σ-value	Success Ratio
53	0.5	successes: 0/20
53	2	successes: 0/20
53	3	successes: 0/20
53	4	successes: 0/20
53	5	successes: 0/20
157	0.5	successes: 0/20
157	2	successes: 0/20
157	3	successes: 0/20
157	4	successes: 0/20
157	5	successes: 0/20

Number Field 4		
Prime Modulus	σ-value	Success Ratio
41	0.5	successes: 0/20
41	2	successes: 0/20
41	3	successes: 0/20
41	4	successes: 0/20

41	5	successes: 0/20
293	0.5	successes: 0/20
293	2	successes: 0/20
293	3	successes: 0/20
293	4	successes: 0/20
293	5	successes: 0/20

Number Field 5		
Prime Modulus	σ-value	Success Ratio
83	0.001	successes: 0/1
83	0.01	successes: 0/1
83	0.2	successes: 0/1
83	0.5	successes: 0/1
83	0.75	successes: 0/1
113	0.001	successes: 0/1
113	0.01	successes: 0/1
113	0.2	successes: 0/1
113	0.5	successes: 0/1
113	0.75	successes: 0/1
449	0.001	successes: 0/1
449	0.01	successes: 0/1
449	0.2	successes: 0/1
449	0.5	successes: 0/1
449	0.75	successes: 0/1

587	0.001	successes: 0/1

Number Field 6		
Prime Modulus	σ-value	Success Ratio
73	0.5	successes: 0/20
73	2	successes: 0/20
73	3	successes: 0/20
73	4	successes: 0/20
73	5	successes: 0/20
107	0.001	successes: 20/20
107	0.01	successes: 20/20
107	0.2	successes: 20/20
107	0.5	successes: 20/20
107	1	successes: 20/20
107	2	successes: 20/20
107	3	successes: 19/20
107	4	successes: 17/20
107	4.5	successes: 8/20
107	5	successes: 0/20

Number Field 7		
Prime Modulus	σ-value	Success Ratio
31	1	successes: 0/1
193	1	successes: 0/1

Number Field 8		
Prime Modulus	σ-value	Success Ratio
59	1	successes: 0/1
179	1	successes: 0/1

Number Field 9		
Prime Modulus	σ-value	Success Ratio
199	0.001	successes: 0/1
199	0.01	successes: 0/1
199	0.2	successes: 0/1
199	0.5	successes: 0/1
199	0.75	successes: 0/1
241	0.001	successes: 0/1
241	0.01	successes: 0/1
241	0.2	successes: 0/1

Number Field 10		
Prime Modulus	σ-value	Success Ratio
101	1	successes: 0/1
137	1	successes: 0/1

Number Field 11		
Prime Modulus	σ-value	Success Ratio
31	0.5	successes: 0/20

31	2	successes: 0/20
31	3	successes: 0/20
31	4	successes: 0/20
31	5	successes: 0/20
47	1	successes: 0/1
97	1	successes: 0/1
193	0.5	successes: 0/20

Number Field 12		
Prime Modulus	σ-value	Success Ratio
37	2	successes: 19/20
37	3	successes: 18/20
37	4	successes: 15/20
37	4.5	successes: 1/20
37	5	successes: 0/20
113	2	successes: 19/20
113	3	successes: 19/20
113	4	successes: 17/20
113	4.5	successes: 14/20
113	5	successes: 0/20

Number Field 13		
Prime Modulus	σ-value	Success Ratio
53	0.001	successes: 20/20

53	0.01	successes: 20/20
53	0.2	successes: 20/20
53	0.5	successes: 20/20
53	1	successes: 20/20
53	2	successes: 20/20
53	3	successes: 18/20
53	4	successes: 20/20
53	4.5	successes: 17/20
53	5	successes: 0/20
109	0.001	successes: 20/20
109	0.01	successes: 20/20
109	0.2	successes: 20/20
109	0.5	successes: 20/20
109	1	successes: 20/20
109	2	successes: 20/20
109	3	successes: 20/20
109	4	successes: 18/20
109	4.5	successes: 20/20
109	5	successes: 7/20
269	0.01	successes: 0/1
269	1	successes: 0/1
269	2	successes: 0/1
269	5	successes: 0/1
433	0.01	successes: 0/1

433	1	successes: 0/1

Number Field 14		
Prime Modulus	σ-value	Success Ratio
197	1	successes: 0/1
397	1	successes: 0/1

Number Field 15		
Prime Modulus	σ-value	Success Ratio
101	1	successes: 0/1
149	1	successes: 0/1

Number Field 16		
Prime Modulus	σ-value	Success Ratio
43	0.001	successes: 20/20
43	0.01	successes: 20/20
43	0.2	successes: 20/20
43	0.5	successes: 20/20
43	1	successes: 20/20
43	2	successes: 20/20
43	3	successes: 18/20
43	4	successes: 19/20
43	4.5	successes: 16/20
43	5	successes: 13/20

89	1	successes: 0/1
89	2	successes: 0/1
89	5	successes: 0/1