

IMPERIAL COLLEGE LONDON

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING

On the Use of Cyclic Algebras in Lattice-based Cryptography

Author:

Andrew Mendelsohn

Submitted in part fulfilment of the requirements for the degree of Doctor of Philosophy in
Electrical and Electronic Engineering of Imperial College London,
September 15, 2023

Abstract

This thesis studies the role of cyclic algebras in lattice-based cryptography. It analyses the security of the mathematical problems underlying a public key encryption (PKE) scheme called CLWE, a variant of Learning with Errors defined over cyclic division algebras (CDAs), obtaining a clearer picture of its security level. This includes relating CLWE to a new module variant of CLWE, and also relating CLWE to ideal lattice problems obtained from one-sided ideals in the natural order of certain CDAs. It then studies three variants of CLWE, corresponding to different parameter choices in the construction of the algebras. These include CDAs which are central over cyclotomic fields of arbitrary conductor, CDAs with fractional non-norm element, and nonassociative CDAs with non-norm element lying in the ring of integers of the maximal subfield of the algebra. This latter (nonassociative) variant is notable for permitting a full search-to-decision reduction for the CLWE problems obtained, for well-chosen moduli. It then turns to a second PKE scheme, based on group rings, called GRLWE, and proposes an attack on the scheme via a transformation which turns samples from the group rings used into samples from structurally-weak cyclic algebras, whose weakness can be cryptographically exploited. A patch is then proposed by replacing the original choice of integral dihedral group rings with integral generalised quaternionic group rings. Finally, it defines a new provably-secure variant of NTRUEncrypt in quaternion algebras, and demonstrates the IND-CPA security of the scheme in algebras of bounded discriminant, via a proof that the distribution of the public keys in the scheme is indistinguishable from uniform, assuming the hardness of CLWE.

Acknowledgements

I would first like to thank Dr Cong Ling for his guidance, wisdom, and patience over the course of my studies, by whom it has been a pleasure to have been supervised, and without whom this thesis could not have been written. I am also deeply appreciative of the ACE-CSR grant which made it possible for me to undertake my PhD studies.

I would also like to thank my family, in particular Mum and Dad, for their unwavering support, constant love, and for the peace of their home. I would like to thank my grandparents, for surrounding me always with books, each in their own peculiar way. I am indebted to Simon Aspray, for the many hours he spent teaching me to see the world with a sense of curiosity and wonder. I would, I suppose, like to thank Benjamin James Claydon for his diuturnal, chronic, and ubiquitous presence in my life these last 20 years; and in particular for the last four, when his companionship and fraternity have so easily replaced cark with cheer. To Chris, Edmund, and Maja, I would like to extend my thanks for all the countless coffee breaks, long lunches, pints, and distractions that were necessary for me to reach this stage; and beyond all, I am thankful for Estera: soție mea minunata și ajutor mea potrivit;

Și era una la părinți
Și mândră-n toate cele,
Cum e Fecioara între sfinți
Și luna între stele.

Dedication

To Ruth Norris; for her model of Christian faithfulness, for her example of scholarly patience and persistence, and for her many, many years of encouragement.

Sola Deo gloria.

Statement of Originality

I declare that all work contained within this thesis is wholly my own, except where references are clearly stated.

Copyright Declaration

‘The copyright of this thesis rests with the author. Unless otherwise indicated, its contents are licensed under a Creative Commons Attribution-Non Commercial 4.0 International Licence (CC BY-NC). Under this licence, you may copy and redistribute the material in any medium or format. You may also create and distribute modified versions of the work. This is on the condition that: you credit the author and do not use it, or any derivative works, for a commercial purpose. When reusing or sharing this work, ensure you make the licence terms clear to others by naming the licence and linking to the licence text. Where a work has been adapted, you should indicate that the work has been changed and describe those changes. Please seek permission from the copyright holder for uses of this work that are not included in this licence or permitted under UK Copyright Law.’

ἔστι δ' οὐ χαλεπὸν ὁποιασοῦν ὑποθέσεις λαμβάνοντας μακροποιεῖν καὶ συνεῖρειν.
— Ἀριστοτέλης, τὰ μετὰ τὰ φυσικά, Ν.ΙΙΙ.

Contents

Abstract	2
Acknowledgements	2
1 Introduction	11
1.1 Motivations	12
1.2 Contributions	18
1.3 Publications	19
2 Background Theory	21
2.1 Lattices	21
2.2 (Discrete) Gaussians	22
2.3 Algebraic Number Theory	24
2.4 Lattice Problems	30
2.5 LWE	31
2.6 Structured LWE	33
2.7 Cyclic Division Algebras	39
2.8 Ideals in Orders of CDAs	42

2.9	CLWE	46
2.10	NTRU	52
3	Clarifying the Security of CLWE	57
3.1	Introduction	57
3.2	Reducing CDA Ideal-SVP to Number Field Ideal-SVP	60
3.3	Consequences	63
3.4	Reducing Module SIVP to CLWE	67
3.5	CLWE with Large Modulus $\geq$ CMLWE	70
3.6	Hardness of CLWE from One-Sided Ideal Lattices	80
3.7	Chapter Summary	85
4	Families of Algebras for CLWE	86
4.1	Introduction	86
4.2	Non-Norm Elements for General Cyclotomic Fields	87
4.3	CLWE with Fractional Non-norm Element	96
4.4	Learning with Errors from Nonassociative Algebras	110
4.5	Chapter Summary	143
5	On the Security of Group Ring LWE	145
5.1	Introduction	145
5.2	Group Rings and GRLWE	148
5.3	Attacking Non-division Cyclic Algebras	152
5.4	An Isomorphism Between Dihedral Group Rings and Cyclic Algebras	156

5.5	Attacking Group Ring LWE	158
5.6	On the Security of Quaternion Group Rings	163
5.7	On Structured MLWE Variants	166
5.8	Chapter Summary	168
6	NTRU in Cyclic Division Algebras	169
6.1	Introduction	169
6.2	Preliminaries	172
6.3	On the Discriminant of the Natural Order	176
6.4	NTRU in CDAs	181
6.5	Results on q -ary Lattices	184
6.6	An NTRU Key Generation Algorithm	189
6.7	A Provably Secure NTRU-based Scheme	195
6.8	Choosing Parameters and Number Fields	199
6.9	Sketched Cryptographic Functionality	200
6.10	Chapter Summary	202
7	Conclusion	203
7.1	Summary of Thesis Achievements	203
7.2	Discussion and Future Work	207
	Bibliography	211
	Appendix	228
A	References for Quotations	228

List of Tables

4.1	The ‘Naive’ Quadratic Case	92
4.2	The ‘Naive’ Case for $d > 2$	93
4.3	The Refined ‘Naive’ Case for $d > 2$	95
4.4	The Cubic Case	95
4.5	The Quartic Case	95
4.6	Even Low-degree Nonassociative Algebras	141
4.7	Cubic-degree Nonassociative Algebras	141
4.8	Nonassociative Algebras Over Maximal Real Subfields	142
4.9	Nonassociative Algebras of Cubic Degree over Prime-power Cyclotomics	142
5.1	Estimating GRLWE	161

Chapter 1

Introduction

Histiaeus, when he was anxious to give Aristagoras orders to revolt, could find but one safe way, as the roads were guarded, of making his wishes known; which was by taking the trustiest of his slaves, shaving all the hair from off his head, and then pricking letters upon the skin, and waiting till the hair grew again. Thus accordingly he did; and as soon as ever the hair was grown, he despatched the man to Miletus, giving him no other message than this - “When thou art come to Miletus, bid Aristagoras shave thy head, and look thereon”. Now the marks on the head, as I have already mentioned, were a command to revolt.

– Herodotus, *Histories*, circa 430 BC

The problem of good cipher design is essentially one of finding difficult problems, subject to certain other conditions. This is a rather unusual situation, since one is ordinarily seeking the simple and easily soluble problems in a field. How can we ever be sure that a system which is not ideal and therefore has a unique solution for sufficiently large N will require a large amount of work to break with every method of analysis? [...] We may construct our cipher in such a way that breaking it is equivalent to [...] the solution of some problem known to be laborious.

– Claude Shannon, *A Mathematical Theory of Cryptography*, 1945 AD

1.1 Motivations

The use of means to hide sensitive information dates at least to the writing of the biblical book of Jeremiah, in which the author enciphers ‘Babylon’ [164] via a cipher replacing the n th letter of an alphabet of size m by the $(m - n)$ th letter¹. Such means of encryption were continued in the form of the Caesar cipher, and more generally simple monoalphabetic substitution and transposition ciphers. However, these ad-hoc, classical methods offer few security guarantees, since decryption simply requires knowledge of the trick used to perform encryption: any enemy of Histiaeus could lie in wait on the road to Miletus, kidnap the travellers entering the city, and shave their heads to see if their scalps contained any interesting information. More sophisticated methods are needed to properly secure information.

In the years since Shannon articulated the principle above [146], a small number of mathematical problems believed to be computationally intractable ascended to the fore of modern public key cryptography. These problems include integer factoring and various kinds of discrete logarithm problems. However, the development of quantum algorithms, such as Shor’s algorithm [147] and Grover’s algorithm [73] in 1994 and 1996 respectively, put the question to this intractability: a sufficiently powerful quantum computer capable of implementing quantum algorithms efficiently could break much then-existing modern cryptography based on the aforementioned underlying mathematical problems, for typical choices of parameters. This has spurred both popular terror (BBC headline: ‘What is the quantum apocalypse and should we be scared?’ [115]) and new lines of cryptographic research.

This research focuses on developing cryptographic schemes no more vulnerable to quantum attack than classical attack, implicitly involving the hunt for underlying mathematical problems with such a property. This subfield of cryptography is known as *post-quantum* cryptography. It mostly comprises work on asymmetric schemes, since it appears the dominant symmetric schemes can resist known quantum attacks with only minor increases in their parameters [30]. This is contrasted by public key schemes like RSA and Diffie-Hellman key exchange, which suffer polynomial-time attacks at the hands of quantum adversaries [26]. Moreover, key encapsulation mechanisms (KEMs), which use asymmetric means to share symmetric keys, are a common

¹An action corresponding to the canonical involution of S_m .

primitive whose reliance on public key cryptography places them also at risk.

The search for quantum-resistant schemes was further galvanized by the commencement of the United States' National Institute for Standards and Technology (NIST) post-quantum cryptographic standardisation process in 2016 [116]. Roughly 70 schemes were admitted to the process, and over the course of six years this list narrowed to seven finalists, with Crystals-Kyber being the selected KEM [117]. Of the finalists, five (including Kyber) were based on a family of mathematical problems known as *lattice problems*. Moreover, in answer to the call for additional digital signature schemes², 40 schemes were admitted, of which seven were based on lattice problems.

A lattice is (in some sense) a ‘regular’ infinite array of points in n -dimensions. Lattices have long been a source of interesting mathematics, having been studied by Minkowski, Voronoi, Davenport, Siegel, and Mordell as part of the study of the ‘geometry of numbers’. However, their relation to cryptography was first developed by Ajtai in [1]. In this work, Ajtai gave a worst-case to average-case reduction for a class of lattice problems; in particular, he showed that finding a short vector in a randomly chosen lattice (within the specified class of lattices) implied a solution to finding a short vector in *any* of those lattices. Later, the first cryptosystem based on such hard lattice problems was given [2].

In the main, the underlying problems directly used in lattice-based cryptography form a triad, with the problems named NTRU, Learning with Errors (LWE), and SIS respectively. Since SIS will not be mentioned at all below, we omit its details. NTRU was introduced in 1996 by Hoffstein, Pipher, and Silverman [77], and the underlying problem has the following general setup: let $\mathcal{R}$ be a discrete ring and $h \in \mathcal{R}$. Given $h \bmod q$, find short $f, g \in \mathcal{R}$ such that $h = g/f \bmod q$. This appears to be a kind of factoring problem, but it can also be seen as a lattice problem: it is equivalent to finding a short vector in the lattice

$$\{(x, y) \in \mathcal{R}^2 : hx - y \equiv 0 \bmod q\}.$$

LWE was introduced by Regev in [102], and is a problem of ‘noisy’ linear algebra. One takes a system of linear equations modulo a positive integer, adds some noise, and asks for a solution

²Round 4 of the standardisation process, which is still underway at the time of writing.

(this is the ‘search’ variant). In a simplified case, such a sample might look like

$$(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e \bmod q) = (\mathbf{a}, a_0 s_0 + a_1 s_1 + \dots + a_n s_n + e \bmod q),$$

where the entries a_i of $\mathbf{a}$ are known coefficients, the entries s_i of $\mathbf{s}$ form the secret, e is the noise (also called the ‘error’), and one is to solve for the s_i . To solve such a problem, it suffices to find either $\mathbf{s}$ or e , and as such is a kind of ‘closest vector problem’ modulo q (see below), in which the target point is $\langle \mathbf{a}, \mathbf{s} \rangle + e$ and one wants to find the closest lattice point, which for certain errors will be $\langle \mathbf{a}, \mathbf{s} \rangle$. Note that when there is only one sample, there may be many possible valid solution pairs $(\mathbf{s}, e)$; with multiple samples for which there is only one valid solution pair, we may properly interpret the problem as CVP. From the knowledge of the lattice point $\langle \mathbf{a}, \mathbf{s} \rangle$, e can then easily be obtained. To batch together multiple samples with the same secret, one considers samples of the form $(A, A\mathbf{s} + \mathbf{e} \bmod q)$, where A is now a matrix and $\mathbf{e}$ is a vector of errors.

In quantifying the hardness of these problems, however, one often needs recourse to other problems, whose hardness is better understood. A central computational challenge on lattices is, given some lattice basis, to compute ‘short’ lattice points, where short is with respect to some specified norm; and computing the shortest vector in a lattice is called the shortest vector problem (SVP). Since the shortest vector could also be understood as the closest vector to the zero-vector, there is also an inhomogeneous version of this problem, the closest vector problem (CVP): given a target vector t in the ambient space containing the lattice, find the closest lattice point to t . A final touchstone lattice problem is the shortest independent vectors problem (SIVP), in which one has to find a number of vectors which are both independent and as short as possible. It is a (contested) virtue that the major problems in lattice-based cryptography have diverse reductions from lattice problems widely considered to be intractable, for specified parameter regimes. In particular, Regev gave a reduction from SVP to LWE^3 and as stated before, NTRU is equivalent to SVP in a certain kind of lattice.

Since their introduction, both LWE and NTRU have found uses in a wide array of applications. These include signature schemes [3], [75], identity-based encryption [59], key exchange [12],

³In fact from a decisional variant of SVP called GapSVP , and from SIVP.

electronic voting [79] and fully homomorphic encryption (FHE) [38], [31] among others.

One can obtain variants of LWE and NTRU by changing the underlying rings from which elements are sampled. In the case of LWE, this ‘structure’ can compensate for two shortcomings: firstly, the large public key size, which in the case of multiple samples above is a $n \times m$ matrix, where n is the number of samples and m the dimension. Cryptographic parameters may take these parameters to be the same order of magnitude as 1000, so in the case when $n = m$, for example, one has to store a great many values to store a LWE public key. There are some techniques to mitigate this issue, such as the use of algorithms during key generation which expand A from a seed, as exemplified in [10]; but these techniques are slow and computationally costly (compared to RLWE below). Another consequence of the high dimension used is that one invariably has to perform matrix multiplication with A , which is not too efficient [11]. To see how adding structure can alleviate these issues, consider the following. Let $\mathcal{R} = \mathbb{Z}[x]/(x^n + 1)$ and $a = a_0 + a_1x + \dots + a_{n-1}x^{n-1} \in \mathcal{R}$. Fixing the standard basis, one can write multiplication by x as a matrix, since it is a linear transformation:

$$m_x = \begin{pmatrix} a_0 & -a_{n-1} & \cdots & -a_1 \\ a_1 & a_0 & \cdots & -a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_0 \end{pmatrix}.$$

Replacing $(A, As + \mathbf{e} \bmod q)$ with $(a, a \cdot s + e \bmod q)$ where a, s , and e are all elements of $\mathcal{R}$, one finds one only needs to store the coefficients of a to possess the public matrix, and moreover polynomial multiplication can be performed efficiently (e.g. [4]). In this manner one obtains *ring* LWE (RLWE) [102], which in particular sets n to be a power of two. Moreover, reductions from SVP on lattices obtained from ideals in those rings were given. An independent work at the same time, with a similar train of thought, introduced what is now referred to as *polynomial* LWE (PLWE) [155], replacing $x^n + 1$ with other irreducible polynomials. In that case one similarly obtains an integral matrix representation from the operation of multiplication on a fixed basis.

There are clearly more algebraic structures in the mathematical world than polynomial rings,

however. The use of modules of finite rank over polynomial rings soon followed [97], resulting in samples of the form $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e \bmod q)$ like in LWE, except that now a, s , and e are taken from a polynomial ring. Not-necessarily-maximal orders in algebraic number fields have been used [27], as well as integral group rings [47]. In another direction, changes to the algebraic operations involved in constructing samples have been proposed, such as using deterministic rounding to create errors [18], using the middle product [140], and alternative multiplications such as in [67].

With regards to NTRU, which already samples elements from polynomial rings, we mention three structured variants. The first, ‘MaTRU’ [52], takes its elements from matrix rings over polynomial rings. ModFalcon [50] and ModNTRU [49] both take elements from modules of finite rank over polynomial rings. There are also many variants replacing the underlying polynomial ring with alternatives, e.g. [161].

While this menagerie of algebraic variants offers various improvements in efficiency and storage, this may come at the cost of security. Consider PLWE. A line of work [62], [45], [44] explores when certain statistical attacks can be mounted to distinguish PLWE samples from uniform. These attacks are possible because of the algebraic structure relied upon (though they are easily countered). Likewise, [150] developed an attack only possible for certain ring-based samples. Other variants of LWE such as multivariate LWE (m-LWE) [123] were shown not to give any security above that of simpler, less structured variants [32]. Moreover, research on attacks of the lattice problems underlying RLWE has made steady incremental progress [56], [23], [24]. Again, algebraic attacks on NTRU variants [84], [7], [48] have led to serious problems for NTRU-based FHE schemes such as YASHE [33] and broke a multilinear map proposal [66]. This illustrates the difficulty involved in structuring cryptographic problems which improve performance with minimal decrease in security.

In [71], a novel algebraic variant of LWE was introduced using a certain maximal order in specific *cyclic division algebras* over cyclotomic fields, named CLWE. These algebras are constructed from a pair of number fields with cyclic Galois group, say L/K with $\text{Gal}(L/K) = \langle \theta \rangle$. Such algebras are parameterised by a so-called ‘non-norm’ element, denoted γ . When $\gamma \in \mathcal{O}_K$, these algebras contain a subring which is also a lattice (that is, an order) called the ‘natural’

order, and if $\gamma \in \mathcal{O}_K^\times$, this order is maximal with respect to inclusion (see [71]). Since elements of the chosen maximal order are integral, like other structured kinds of LWE there is an integral matrix representation obtained by multiplication of elements on a fixed basis, and from this it can be seen that CLWE is structured LWE. These objects include cyclotomic fields, and the form of LWE obtained thus generalises RLWE. Moreover, one sample of CLWE is equivalent to multiple correlated MLWE samples, and so CLWE is structured MLWE. A reduction from ideal lattice problems from ideals in the maximal order to search CLWE was given, and a partial reduction from the search to the decision variants was also derived. This work also gave a public key encryption (PKE) scheme as a cryptographic application.

Moreover, the complexity of multiplication of elements of CDAs is intermediate to that of ring and module elements. As referred to above, multiplication of two polynomials $a \cdot s$ (as in RLWE) can be performed efficiently, with an asymptotic complexity of $O(n \log n)$ for multiplication of degree n polynomials. In the case of rank d modules over such a ring of polynomials, performing the multiplication of a $d \times d$ matrix with a vector $A \cdot \mathbf{s}$ can be performed with complexity $O(nd^2 \log n)$. For CDAs, as is pointed out in [71, Appendix F], one can perform the multiplication of two cyclic algebra elements $a \cdot s$ with complexity $O(nd^2 \log n) + \tilde{O}(nd^\omega)$. This uses fast algorithms for skew polynomials [43]. To evaluate the complexity of computing the LWE instances, fix the underlying LWE dimension to be N in each case; thus for modules, $N = nd$, whereas for CDAs, $N = nd^2$. We then find that the complexity of the module operation is $O(Nd \log N/d)$, whereas for algebra operations we find $O(N \log N/d^2) + \tilde{O}(Nd^{\omega-2})$. Thus, keeping the dimension constant between the problems, we find that, asymptotically in d , CDA multiplication may outperform matrix-vector computations over modules.

Many questions remain, however. Little cryptanalysis was performed, and the precise security level of CLWE, while likely lying somewhere between RLWE and MLWE, is unknown. The effects of changing the specified parameters were unstudied. In addition, there are novel structures in CDAs, which are noncommutative, that were left unexploited for cryptographic purposes. Finally, the question of whether CDAs could have application in other areas of cryptography beyond LWE was left open. In this thesis, we attempt to answer these questions.

1.2 Contributions

We begin in Chapter 3 by studying the security of CLWE in greater detail. The security reduction of [71] reduced ideal SVP to search CLWE, for ideals in the natural order of a K -algebra $\mathcal{A}$, for some number field K , denoted Λ . The structure of maximal such ideals was known due to the work of [119], but more information was lacking. We first classify completely the ideals of Λ lying above primes of $\mathcal{O}_K$ which are unramified in the maximal subfield of $\mathcal{A}$, and use this result to show that the security reduction for CLWE is in fact based on SIVP in ideals of $\mathcal{O}_L$, not Λ . This leaves the security of CLWE somewhat open to question.

We then turn to seeing what else can be said about the security of CLWE. We first reaffirm that CLWE is in some sense a module problem, by showing that a CLWE oracle can be used to solve $q\text{Mod-BDD}$ in a module lattice. We then define a module variant of CLWE, considering modules of finite rank over Λ . We obtain a result in the style of [8], showing that for some change of modulus, CLWE is as hard as its module form. Finally, we reduce ideal lattice problems on lattices obtained from one-sided ideals to CLWE.

In Chapter 4, we then explore three generalisations of CLWE. First, we note that the centers of the algebras considered in [71] had the form $K = \mathbb{Q}(\zeta_n)$ where n is a prime power. We extend the construction of division algebras to *any* cyclotomic, that is to cyclotomics of arbitrary conductor. The results of [71] immediately hold in this general setting, and we propose further parameter sets for CLWE. We then consider algebras parameterised by $\gamma \in K \setminus \mathcal{O}_K$, extending the known constructions of such algebras, developing a method to find unit-magnitude fractional non-norm elements in extensions of cyclotomic fields of any finite degree. We then study security reductions for ideal lattice problems in the algebras obtained from these non-norm elements. Finally, we consider the case $\gamma \in \mathcal{O}_L \setminus \mathcal{O}_K$. Here, the resulting algebras are *nonassociative*. We obtain new results on the ideal theory of Λ in nonassociative algebras, extending the work of [152] and [131], before analysing LWE-style problems defined in such spaces. In particular, we obtain a full search-to-decision reduction for our nonassociative CLWE variant, in contrast to the restricted reduction of [71]. We also give a PKE scheme that holds in the nonassociative setting.

We then turn to look at the use of cyclic algebras elsewhere in post-quantum cryptography. We observe in Chapter 5 that group ring LWE (GRLWE), as defined in [47], mentioned above, can be reinterpreted as LWE in a certain cyclic algebra. We then show that this algebra is not division, and in particular show that a GRLWE sample can be transformed into multiple lower dimensional samples which are theoretically easier to solve, with, for example, any off-the-shelf LWE solver (such as BKZ). A solution to the transformed instances can then be inverted to obtain a solution to the original problem. We also extend this transformation to other group rings proposed in [47]. This attack relies heavily on the choice of group ring, and it was precisely the choice of dihedral groups by the authors that created the insecurity. We propose an alternative choice of group, based on generalised quaternion groups, and show that our attack fails on GRLWE-style samples taken from these group rings.

Finally, we turn to NTRU. In Chapter 6 we define NTRU in the CDAs used in [71] and demonstrate that NTRUEncrypt can be adapted to hold in the noncommutative setting. We call this variant ‘CNTRU’, and compare it to the module NTRU variants [50], [49]. We show that for certain quaternion algebras and scheme parameters, the public keys of CNTRU are statistically close to uniform, following the work of [154], [169], and use this result to prove the IND-CPA security of our scheme. This result holds when the discriminant of the algebra is bounded. We adapt a number of known results on ideal lattices and their geometry to complete the proof.

1.3 Publications

Journal articles

Mendelsohn, A. & Ling, C., "Fractional Non-norm Elements for Division Algebras, and an Application to Cyclic Learning with Errors", accepted by Advances in Mathematics of Communications (extended abstract presented at ALCOCrypt 2023).

Mendelsohn, A. (2022), "A Note On Square-free Commuting Probabilities of Finite Rings", Journal of Algebra and Its Applications, DOI: 10.1142/S0219498824500671.

Grover, C., **Mendelsohn, A.**, Ling, C., & Vehkalahti, R. (2022), "Non-commutative Ring Learning with Errors from Cyclic Algebras", Journal of Cryptology 35, 22, DOI: 10.1007/s00145-022-09430-6.

Conference Papers

Mendelsohn, A. & Ling, C. (2023), "Middle-products of Skew Polynomials and Learning with Errors", accepted for presentation at IMACC 2023

Mendelsohn, A. & Ling, C. (2023), "NTRU in Quaternion Algebras of Bounded Discriminant", PQCrypto 2023.

Porter, C. **Mendelsohn, A.**, & Ling, C. (2022), "Subfield Algorithms for Ideal- and Module-SVP Based on the Decomposition Group", NuTMiC 2021.

Chapter 2

Background Theory

2.1 Lattices

An n -dimensional lattice is a discrete additive subgroup of $\mathbb{R}^n$. One can consider a lattice $\mathcal{L}$ to be the set of integer linear combinations of a set of vectors $B = \{\mathbf{b}_1, \dots, \mathbf{b}_k\}$ that are linearly independent, for some $k \leq n$, written $\mathcal{L}(B) = \left\{ \sum_{i=1}^k z_i \mathbf{b}_i : z_i \in \mathbb{Z} \right\}$. All lattices in this work are assumed to have $k = n$.

The above notion can also be generalised to vector spaces over fields. Let V be a finite-dimensional vector space over a field K and R be a discrete subring of K . An R -lattice in V is a subspace $L \subset V$ such that L is a finitely-generated R -module. Equivalently, L is a finitely-generated torsion-free R -module. L is *full* if it contains a K -basis of V , so $V = K \cdot L$. Taking a basis B of V , the R -linear span of B is a full lattice. We will primarily be interested in the case $V = \mathbb{R}^n$.

Definition 1. Let $\mathcal{L}$ be a lattice, and $\mathbb{R}^n$ be endowed with inner product $\langle \cdot, \cdot \rangle$. Then the set $\mathcal{L}^\vee = \{v \in \mathbb{R}^n : \langle \mathcal{L}, v \rangle \subset \mathbb{Z}\}$ is called the dual lattice of $\mathcal{L}$.

One can use the geometry induced by an inner product to define computationally intractable problems on lattices. Informally, examples of lattice problems are finding the shortest vector in the lattice (SVP), finding the closest vector to a given point (CVP), deciding whether the

shortest vector has size less than one or greater than a parameter β (GapSVP), or outputting n independent sufficiently short vectors (SIVP), when one knows only a certain basis of the lattice. These are believed to be hard and such problems have been used to ground the security of problems that are capable of being used to construct quantum-resistant cryptographic schemes. We will define these problems, and their ‘approximate’ variants, rigorously later on.

Definition 2. Let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice and $\|\cdot\|$ be a norm. Then $\lambda_i(\mathcal{L})$ denotes the i th successive minimum of $\mathcal{L}$ with respect to the norm $\|\cdot\|$, that is the minimum length of a set of i linearly independent vectors in $\mathcal{L}$, where the length of a set of vectors $\{\mathbf{x}_1, \dots, \mathbf{x}_n\}$ is $\max_i (\|\mathbf{x}_i\|)$.

2.2 (Discrete) Gaussians

Let $\mathbb{R}^n$ be equipped with the Euclidean norm $\|\cdot\|_2 = \|\cdot\|$, $\mathbf{a} \in \mathbb{R}^n$, and let $r > 0$. Then the *Gaussian function* is defined $\rho_{r,\mathbf{a}} : \mathbb{R}^n \rightarrow (0, 1]$, $\mathbf{x} \mapsto \exp(-\pi\|\mathbf{x} - \mathbf{a}\|^2/r^2)$. The Gaussian distribution D_r is defined as having probability density function equal to $\frac{1}{r^n}\rho_{r,0}$.

Fix a basis $\mathbf{b}_1, \dots, \mathbf{b}_n$ of $\mathbb{R}^n$ and let $\mathbf{r} = (r_1, \dots, r_n) \in \mathbb{R}^n$. We sample an *elliptical* Gaussian distribution $D_{\mathbf{r}}$ over $\mathbb{R}^n$ by sampling $x_i \leftarrow D_{r_i}$ independently for all $i \neq j$ and outputting $\sum_{i=1}^n x_i \mathbf{b}_i$. If all the r_i are equal we call $D_{\mathbf{r}}$ spherical.

For some lattice $\mathcal{L}$, set $\rho_r(\mathcal{L}) = \sum_{\mathbf{x} \in \mathcal{L}} \rho_r(\mathbf{x})$. Then the *discrete* Gaussian distribution $D_{\mathcal{L},r}$, defined over a lattice $\mathcal{L}$, outputs $\mathbf{x}$ with probability $\frac{\rho_r(\mathbf{x})}{\rho_r(\mathcal{L})}$ for each $\mathbf{x} \in \mathcal{L}$.

The *smoothing parameter*, introduced in [108] and defined below, will be used throughout this thesis:

Definition 3. Let $\mathcal{L}$ be a lattice and $\varepsilon > 0$. Then the *smoothing parameter* $\eta_\varepsilon(\mathcal{L})$ of $\mathcal{L}$ is the smallest $r > 0$ such that $\rho_{1/r}(\mathcal{L}^\vee / \{0\}) \leq \varepsilon$.

We will use the following bounds on the smoothing parameter:

Lemma 2.1. [125, Lemma 3.5] For any full-rank lattice $\mathcal{L} \subseteq \mathbb{R}^n$ and $\epsilon \in (0, 1)$, we have $\eta_\epsilon(\mathcal{L}) \leq \sqrt{\ln(2n(1 + 1/\epsilon))/\pi} \cdot \frac{1}{\lambda_1^\infty(\mathcal{L}^\vee)}$.

Lemma 2.2. [68, Lemma 3.1] For any $\varepsilon > 0$ and n -dimensional lattice Λ with basis $\mathbf{B}$ and corresponding Gram-Schmidt orthogonalisation $\tilde{\mathbf{B}}$,

$$\eta_\varepsilon(\Lambda) \leq \|\tilde{\mathbf{B}}\| \sqrt{\ln(2n(1 + 1/\varepsilon))}/\pi.$$

Lemma 2.3. [68, Lemma 3.2] For any full-rank lattice $\mathcal{L} \subseteq \mathbb{R}^n$ and $\epsilon \in (0, 1)$, we have $\eta_\epsilon(\mathcal{L}) \leq \sqrt{\ln(2n(1 + 1/\epsilon))}/\pi \cdot \lambda_n(\mathcal{L})$.

Lemma 2.4. [17] For any full-rank lattice $\mathcal{L} \subseteq \mathbb{R}^n$, $c \geq 1$, and $\varepsilon = \exp(-c^2 n)$, we have $\eta_\varepsilon(\mathcal{L}) \leq c\sqrt{n}/\lambda_1(\mathcal{L}^\vee)$.

The following lemma gives a criterion to guarantee one can sample from a discrete Gaussian:

Lemma 2.5. [37, Lemma 2.3] There is a probabilistic polynomial-time algorithm that, given a basis $\mathbf{B}$ of an n dimensional lattice $\Lambda = \mathcal{L}(\mathbf{B})$, $\mathbf{c} \in \mathbb{R}^n$ and parameter $r \geq \|\tilde{\mathbf{B}}\| \cdot \sqrt{\ln(2n + 4)}/\pi$ outputs a sample distributed according to $D_{\Lambda+\mathbf{c},r}$.

The *statistical distance* between distributions D, D' over a discrete set S is denoted $\Delta(D, D') = \frac{1}{2} \sum_{x \in S} |D(x) - D'(x)|$. We may denote the uniform distribution over S by $U(S)$. We also need the following statistical lemmas:

Lemma 2.6. [108, Lemma 4.1] For a lattice $\mathcal{L}$ over $\mathbb{R}^n$, $\varepsilon > 0$, $r \geq \eta_\varepsilon(\mathcal{L})$, and $x \in \mathbb{R}^n$, the statistical distance between $(D_r + \mathbf{x}) \bmod \mathcal{L}$ and the uniform distribution modulo $\mathcal{L}$ is bounded above by $\varepsilon/2$. Equivalently, $\rho_r(\mathcal{L} + \mathbf{x}) \in [\frac{1-\varepsilon}{1+\varepsilon}, 1] \cdot \rho_r(\mathcal{L})$

Lemma 2.7. [46, Theorem 1] For any positive definite Σ , vector $\mathbf{c}$, lattice coset $A := \Lambda + \mathbf{a} \subset \mathbf{c} + \text{span}(\Sigma)$, and injective linear transformation $\mathbf{T}$,

$$\mathbf{T}(D_{A, \mathbf{c}, \sqrt{\Sigma}}) = D_{\mathbf{T}A, \mathbf{T}\mathbf{c}, \mathbf{T}\sqrt{\Sigma}}.$$

Lemma 2.8. [108, Lemma 4.4] For any full-rank lattice $\mathcal{L} \subseteq \mathbb{R}^n$, $\mathbf{c} \in \mathbb{R}^n$, $\delta \in (0, 1)$ and $\sigma \geq \eta_\delta(\mathcal{L})$, we have $\Pr_{\mathbf{b} \leftarrow D_{\mathcal{L}, \sigma, \mathbf{c}}}[\|\mathbf{b}\| \geq \sigma\sqrt{n}] \leq \frac{1+\delta}{1-\delta} \cdot 2^{-n}$.

Lemma 2.9. [97, Lemma 2.8] Let $\mathcal{L}$ be an n -dimensional lattice, $\mathbf{u} \in \mathbb{R}^n$, $\mathbf{r} \in (\mathbb{R}^+)^n$, $\sigma > 0$ and $t_i = \sqrt{r_i^2 + \sigma^2}$ for all i . Assume that $\min_i r_i \sigma / t_i \geq \eta_\varepsilon(\mathcal{L})$ for some $\varepsilon \in (0, 1/2)$. Consider the discrete distribution Y on $\mathbb{R}^n$ obtained by sampling from $D_{\mathcal{L}+\mathbf{u}, \mathbf{r}}$ and then adding a vector taken from D_σ . Then we have $\Delta(Y, D_t) \leq 4\varepsilon$.

2.3 Algebraic Number Theory

To create structured lattices, we use structure obtained from abstract-algebraic objects; in particular, structure from fields and, in this thesis, skew-fields containing $\mathbb{Q}$. Here we provide some background on the commutative setting; in particular, that of number fields.

A number field is a field containing $\mathbb{Q}$ of finite dimension as a vector space over $\mathbb{Q}$. Let K be a number field and $\mathcal{O}_K$ denote its ring of integers. A Dedekind domain is an integrally closed, Noetherian domain in which every (non-zero) prime ideal is maximal. In addition, in a Dedekind domain R every fractional ideal has a unique factorization into prime ideals, that is if $\mathcal{I} \subset R$, we have $\mathcal{I} = \prod_{i=1}^m \mathfrak{q}_i^{e_i}$ for some prime ideals $\mathfrak{q}_i$ of R and $e_i \geq 1$, $i = 1, \dots, m$. Recall that $\mathcal{O}_K$ is a Dedekind domain.

We detail the behaviour of primes in extensions of number fields. Let L be a finite extension of K , $\mathfrak{q}$ a prime ideal of $\mathcal{O}_L$, and $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$. We say $\mathfrak{q}$ lies above $\mathfrak{p}$ if $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$. Moreover, $\mathfrak{p}\mathcal{O}_L$ is an ideal of $\mathcal{O}_L$, which is a Dedekind domain, so $\mathfrak{p}\mathcal{O}_L$ has a unique factorization into prime ideals:

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^g \mathfrak{q}_i^{e_i} = \mathfrak{q}_1^{e_1} \dots \mathfrak{q}_g^{e_g}, \quad (2.1)$$

for $\mathfrak{q}_i$ prime in $\mathcal{O}_L$ all lying above $\mathfrak{p}$. We call $e_{\mathfrak{q}_i|\mathfrak{p}} = e_i$ the *ramification index* of $\mathfrak{q}_i$ over $\mathfrak{p}$, and $f_{\mathfrak{q}_i|\mathfrak{p}} = f_i = [\mathcal{O}_L/\mathfrak{q}_i : \mathcal{O}_K/\mathfrak{p}]$ the *inertial degree* of $\mathfrak{p}$ in $\mathfrak{q}_i$. If we want to make the pair of number fields explicit, we may write $f_{L/K}^{\mathfrak{q}}$ for f_i . Now assume the field extension L/K is Galois. Then all the e_i and f_i are equal, and $\text{Gal}(L/K)$ acts transitively on the set of primes lying above any fixed prime of $\mathcal{O}_K$. Note that both $\mathcal{O}_L/\mathfrak{q}_i$ and $\mathcal{O}_K/\mathfrak{p}$ are finite fields.

Proposition 2.1. *The ramification index and inertial degree are multiplicative over towers of number fields; i.e. for $\mathbf{Q}/\mathbf{q}/\mathbf{q}$ in $L/M/K$, $e_{\mathbf{Q}|\mathbf{q}} = e_{\mathbf{Q}|\mathbf{q}} e_{\mathbf{q}|\mathbf{q}}$ and $f_{\mathbf{Q}|\mathbf{q}} = f_{\mathbf{Q}|\mathbf{q}} f_{\mathbf{q}|\mathbf{q}}$.*

Definition 4. An ideal $\mathfrak{p} \subset \mathcal{O}_K$ ramifies in L if $e > 1$, and is unramified if $e = 1$. Alternatively, we say that L/K is unramified at $\mathfrak{p}$. If $e = 1$ and $f = 1$, $\mathfrak{p}$ splits completely. If $f = g = 1$, then $e = [L : K]$ and $\mathfrak{p}$ is totally ramified.

The following maps between fields will be useful:

Definition 5. Let L be a number field of degree n over K . Fix a basis of L/K . Multiplication by an element α of L is a linear map, so has an associated matrix m_α . The norm is defined as the map $N_{L/K} : L \rightarrow K$, given by $\alpha \mapsto \det(m_\alpha)$. When L/K is Galois, we have, equivalently, $N_{L/K}(\alpha) = \prod_{\sigma \in \text{Gal}(L/K)} \sigma(\alpha)$.

The field norm is multiplicative, and is transitive on towers of number fields; that is, if $L/K/F$ is such a tower, then $N_{L/F} = N_{K/F} \circ N_{L/K}$.

Definition 6. Let L be a number field of degree n over K . Fix a basis of L/K . The trace is defined as the map $T_{L/K} : L \rightarrow K$, given by $\alpha \mapsto \text{trace}(m_\alpha)$. When L is Galois, we have, equivalently, $T_{L/K}(x) = \sum_{\sigma \in \text{Gal}(L/K)} \sigma(x)$.

The trace is additive, and like the field norm is transitive on towers of number fields. It is used to define a duality on $\mathcal{O}_K$; if $\mathcal{I}$ is an ideal of $\mathcal{O}_K$, we set

$$\mathcal{I}^\vee := \{x \in K : T_{K/\mathbb{Q}}(x\mathcal{I}) \subset \mathbb{Z}\}.$$

This is an ideal, and satisfies $(\mathcal{I}^\vee)^\vee = \mathcal{I}$. We call $\mathcal{O}_K^\vee$ the codifferent ideal of $\mathcal{O}_K$.

Below, we will need certain bases of $\mathcal{O}_{L_q} := \mathcal{O}_L/q\mathcal{O}_L$ over $\mathcal{O}_{K_q} := \mathcal{O}_K/q\mathcal{O}_K$, where q is completely split:

Lemma 2.10. Let L/K be a finite cyclic Galois extension of number fields of degree d , and $q \geq 2$ a prime completely split in $\mathcal{O}_L$. Suppose $\text{Gal}(L/K) = \langle \theta \rangle$. Then there exists an efficiently computable basis $\{\ell_1, \dots, \ell_d\}$ of $\mathcal{O}_{L_q}$ over $\mathcal{O}_{K_q}$ such that

1. $\ell_i \cdot \ell_j = 1$ if $i = j$, and $\ell_i \cdot \ell_j = 0$ otherwise, and

$$2. \theta(\ell_i) = \ell_{i+1}.$$

Proof. See [71, Appendix F.4]. □

We call these bases ‘cyclic bases’.

Cyclotomic Fields and Primes Therein

A cyclotomic field is a finite extension of $\mathbb{Q}$ obtained by adjoining an n th root of unity to $\mathbb{Q}$. We denote such a root of unity by ζ_n . Such fields are Galois over $\mathbb{Q}$. An n th root of unity is called *primitive* if it has order n , that is, no smaller integer m than n satisfies $\zeta_n^m = 1$. Adjoining one primitive n th root of unity to $\mathbb{Q}$ automatically adjoins all primitive n th roots to $\mathbb{Q}$, since they can be obtained by computing ζ_n^k for any k such that $\gcd(n, k) = 1$. Thus there are $\phi(n)$ primitive n th roots of unity, where ϕ is the Euler totient function, and $[K : \mathbb{Q}] = \phi(n)$. Representing K as the extension of a polynomial ring, one can write $K = \mathbb{Z}[x]/\Phi_n(x)$, where $\Phi_n(x)$ is the minimal polynomial of ζ_n , called the n th cyclotomic polynomial. Note $\Phi_n(x)$ is always a factor of $x^n - 1$ and of degree $\phi(n)$. In the case of power-of-two n , we have $\Phi_n(x) = x^{n/2} + 1$. It is well known that the ring of integers of K is $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$.

Here we consider the ramification of primes p in rings of integers of cyclotomic fields of the form $\mathbb{Q}(\zeta_n)$, for some primitive n th root of unity ζ_n .

Case 1: p does not divide n . Then

Proposition 2.2. [107, Proposition 7.7] *Let $K = \mathbb{Q}(\zeta_n)$. Let p be a rational prime, $\gcd(p, n) = 1$ and f be the lowest integer such that $p^f \equiv 1 \pmod{n}$. Then we have $f = f_{\mathfrak{p}|p}$ for any prime ideal $\mathfrak{p}$ of K lying above p .*

Let $p \in \mathbb{Z}$ be a prime not dividing n . Then p is unramified in $\mathbb{Q}(\zeta_n)$, since the only primes which ramify are those dividing the discriminant, which is a power of n . This is equivalent to saying that $e = 1$. So we have $fg = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, and one can use the above proposition

to find f , and hence g .

Case 2: p divides n . To determine the ramification of such a prime, write $n = p^a \cdot n'$, where $\gcd(p, n') = 1$. Then f is the lowest positive integer such that $p^f \equiv 1 \pmod{n'}$. Also, $e = \phi(p^a)$, and $g = \phi(n')/f$ (see [14] or [170]).

We will need a form of Dirichlet's theorem on arithmetic progressions:

Theorem 2.1. [22]¹ *Let $a, n \in \mathbb{Z}_{\geq 1}$ and $\gcd(a, n) = 1$. Then the natural density of primes p such that $p \equiv a \pmod{n}$ in the set of all primes of $\mathbb{Z}$ is $1/\phi(n)$.*

Examples: 1. Take q such that p^a is the highest power of p that divides $q - 1$. Then $q \equiv 1 \pmod{p^a}$, so by the theorem there are infinitely many such q .

2. Consider the arithmetic progression $1 + 2^a p^b + \sum_{i=0}^m 2^{a+1} p^{b+1}$, for $m = 0, 1, 2, \dots$. Dirichlet's theorem says there are infinitely many primes in this progression. So there are infinitely many primes q such that $2^a p^b \mid q - 1$, and $q \equiv 1 + 2^a p^b \pmod{2^a p^{b+1}}$ and $q \equiv 1 + 2^a p^b \pmod{2^{a+1} p^b}$, i.e. $2^a p^{b+1} \nmid q - 1$ and $2^{a+1} p^b \nmid q - 1$.

Orders in Number Fields

An order $\mathcal{O}$ in a number field K is a subring which is also a lattice. We say an order is *maximal* if it is maximal with respect to inclusion. A maximal order of a number field is unique ('the' maximal order) and coincides with the ring of integers, $\mathcal{O}_K$. The behaviour of ideals in (not necessarily maximal) orders is significantly determined by the *conductor ideal*:

Definition 7. *The conductor of an order $\mathcal{O} \subset \mathcal{O}_K$ is defined*

$$\mathfrak{c} = \mathfrak{c}_{\mathcal{O}} = \{x \in K : x\mathcal{O}_K \subset \mathcal{O}\}.$$

We need the following lemma on the behaviour of ideals in orders:

¹See [58] for a translation into English.

Lemma 2.11. [54] *Let $\mathcal{O}$ be an order in K with conductor $\mathfrak{c}$.*

1. *For each $\mathcal{O}_K$ -ideal $\mathfrak{a}$ coprime to $\mathfrak{c}$, $\mathfrak{a} \cap \mathcal{O}$ is an $\mathcal{O}$ -ideal coprime to $\mathfrak{c}$ and the natural ring homomorphism $\mathcal{O}/(\mathfrak{a} \cap \mathcal{O}) \rightarrow \mathcal{O}_K/\mathfrak{a}$ is an isomorphism.*
2. *For each $\mathcal{O}$ -ideal $\mathfrak{b}$ that is coprime to $\mathfrak{c}$, $\mathfrak{b}\mathcal{O}_K$ is an $\mathcal{O}_K$ -ideal coprime to $\mathfrak{c}$ and the natural ring homomorphism $\mathcal{O}/\mathfrak{b} \rightarrow \mathcal{O}_K/\mathfrak{b}\mathcal{O}_K$ is an isomorphism.*
3. *The nonzero ideals coprime to $\mathfrak{c}$ in $\mathcal{O}_K$ and in $\mathcal{O}$ are in bijection by $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$ and $\mathfrak{b} \mapsto \mathfrak{b}\mathcal{O}_K$ and these maps are multiplicative: $(\mathfrak{a} \cap \mathcal{O})(\mathfrak{a}' \cap \mathcal{O}) = \mathfrak{a}\mathfrak{a}' \cap \mathcal{O}$ and $(\mathfrak{b}\mathcal{O}_K)(\mathfrak{b}'\mathcal{O}_K) = \mathfrak{b}\mathfrak{b}'\mathcal{O}_K$.*

We will later study more general orders in cyclic division algebras.

Local Fields

We will also need some p -adic theory. For more on this, see [144].

Definition 8. *A field is complete if every Cauchy sequence of elements converges. A valuation on a field K is a homomorphism $\nu : K \rightarrow \mathbb{R}$ such that $\nu(xy) = \nu(x) + \nu(y)$, $\nu(x) = \infty$ if and only if $x = 0$, and $\nu(x + y) \geq \min(\nu(x), \nu(y))$. If the image of ν is $\mathbb{Z}$ then ν is said to be discrete. If ring R has field of fractions K , and K is equipped with a discrete valuation such that $R = \{x : x \in K \text{ and } \nu(x) \geq 0\}$, then we call R a discrete valuation ring (DVR).*

DVRs are PIDs and have precisely one proper maximal ideal.

The p -adic valuation: Let $p \in \mathbb{Z}$. Define $\nu_p(x) = r$, for $x = p^r a$ with $a = \frac{b}{c}$ with $\gcd(p, b) = \gcd(p, c) = 1$. Likewise for a Dedekind domain A with field of fractions K and a prime ideal $\mathfrak{p}$, $\nu_{\mathfrak{p}}(x) := r$, for $(x) = \mathfrak{p}^r \mathbf{b} \mathbf{c}^{-1}$ where $\mathbf{b}, \mathbf{c}$ are fractional ideals coprime to $\mathfrak{p}$. This valuation is discrete. The completion of $\mathbb{Q}$ with respect to ν_p is denoted $\mathbb{Q}_p$ and called the rational field of p -adic numbers.

Definition 9. A local field is a field K that is complete with respect to a discrete valuation, and has finite residue field. Denote the ramification index of such a field's unique prime in a finite extension L by $e_{L/K}$.

Thus $\mathbb{Q}_p$ is an example of a local field. We can generate further examples as follows: let K be a number field, and $\mathfrak{q}$ a prime ideal of $\mathcal{O}_K$ lying above q . Denote the completion of K by $\mathfrak{q}$ by $K_{\mathfrak{q}}$. This is also a local field, and is a finite extension of $\mathbb{Q}_q$. The following gives important properties of such fields:

Proposition 2.3. Let K be a local field.

1. $\mathcal{O}_K$ is a discrete valuation ring with a unique proper prime (maximal) ideal.
2. A generator, π , of the maximal ideal, $\mathfrak{m}$, is called a uniformizer. This element is irreducible.
3. The group of units of $\mathcal{O}_K$ is denoted $\mathcal{O}_K^\times = U$. The n th unit group is defined $U^n = \{u \in \mathcal{O}_K^\times : u \equiv 1 \pmod{\mathfrak{m}^n}\}$. We have $U/U^n = (\mathcal{O}_K/\mathfrak{m}^n)^\times$.

Definition 10. We say an extension of local fields L/K is tamely ramified if $\text{char}(\bar{K}) \nmid e_{L/K}$, where $\bar{K} = \mathcal{O}_K/\mathfrak{m}$ is the residue field of K .

The following three results will be used in the proof of Theorem 4.1.

Proposition 2.4. [112, Chapter 2, Proposition 5.3] Let $K_{\mathfrak{q}}$ be as above. Then we have $K_{\mathfrak{q}}^\times \cong \mu_{q-1} \times \langle \pi_{\mathfrak{q}} \rangle \times U_{\mathfrak{q}}^1$, where μ_{q-1} is a cyclic group of order $q-1$, $\pi_{\mathfrak{q}}$ is a uniformizer of $K_{\mathfrak{q}}$, and $U_{\mathfrak{q}}^1$ is the first unit group of $K_{\mathfrak{q}}$.

Theorem 2.2 (Hasse Norm Theorem [74]). Let L/K be a cyclic extension of number fields. A nonzero element of K is a local norm at all primes $\mathfrak{p} \in L$ lying over $p \in K$, for all $p \in K$, if and only if it is a norm of an element in L .

Theorem 2.3 (Local Reciprocity Map [64]). Let $\mathfrak{Q}$ be a prime ideal of $\mathcal{O}_L$ and $\mathfrak{q}$ be a prime ideal of $\mathcal{O}_K$, both lying above q , so $L_{\mathfrak{Q}}/K_{\mathfrak{q}}$ is a finite abelian extension of local fields. Then there is an isomorphism

$$\Theta : K_{\mathfrak{q}}^\times / N_{L_{\mathfrak{Q}}/K_{\mathfrak{q}}}(L_{\mathfrak{Q}}^\times) \rightarrow \text{Gal}(L_{\mathfrak{Q}}/K_{\mathfrak{q}}).$$

2.4 Lattice Problems

Recall $\lambda_i(\mathcal{L})$ denotes the minimum length of a set of i linearly independent vectors in $\mathcal{L}$, where the length of a set $\{\mathbf{x}_1, \dots, \mathbf{x}_n\} \subset \mathbb{R}^n$ is $\max_i (\|\mathbf{x}_i\|)$: the i th successive minimum of $\mathcal{L}$ (in the appropriate norm). The following problems are the computationally intractable lattice problems we use in this thesis to establish the hardness of LWE- and NTRU-based problems.

Definition 11. (*GIVP*) The Generalized Independent Vectors Problem $GIVP_\gamma^\phi$ is: given lattice basis $\mathbf{B}$, find $n = \dim(\mathcal{L}(\mathbf{B}))$ linearly independent vectors $x_1, \dots, x_n \in \mathcal{L}(\mathbf{B})$ such that $\max_i \|x_i\| \leq \gamma \cdot \phi(\mathcal{L}(\mathbf{B}))$.

When $\phi = \lambda_n$, we recover *shortest independent vectors problems*:

Definition 12. (*approx.-SIVP*) Given a lattice $\mathcal{L}$ and an approximation factor $\xi = \xi(n) \geq 1$, the approximate Shortest Independent Vectors Problem, $SIVP_{\mathcal{L}, \xi}$, is to find n linearly independent non-zero vectors $\mathbf{x}_1, \dots, \mathbf{x}_n$ such that $\max_i (\|\mathbf{x}_i\|_2) \leq \xi \cdot \lambda_n(\mathcal{L})$.

Definition 13. (*approx.-SVP*) Given a lattice $\mathcal{L}$ and approximation factor $\xi = \xi(n) \geq 1$ the approximate Shortest Vector Problem, $SVP_{\mathcal{L}, \xi}$, is to find an $a \in \mathcal{L} \setminus \{0\}$ such that $\|a\|_2 \leq \xi \cdot \lambda_1(\mathcal{L})$.

We note here the inhomogeneous variant of SVP, the *closest vector problem* (CVP), in which one is asked for the closest vector to a target point. We will use the following variant of CVP:

Definition 14. (*BDD*) Let $0 < \delta < \lambda_1(\mathcal{L})/2$. Then the bounded distance decoding problem, $BDD_{\mathcal{L}, \delta}$ problem, on input $y = x + e$ for $x \in \mathcal{L}$ and $e \in \mathbb{R}^n$ satisfying $\|e\|_2 \leq \delta$, is to compute x .

Definition 15. (*q-BDD*) Let $q \geq 2$. The q - $BDD_{\mathcal{L}, \delta}$ problem is, given a $BDD_{\mathcal{L}, \delta}$ instance $y = x + e$ with solution $x \in \mathcal{L}$ and error $e \in \mathbb{R}^n$ satisfying $\|e\|_2 \leq \delta$, to output $x \bmod q\mathcal{L}$.

We note here the following reduction from BDD to q -BDD:

Lemma 2.12. [136, Lemma 3.5] For any $q \geq 2$ and lattice $\mathcal{L}$, there is a deterministic polynomial time reduction from $BDD_{\mathcal{L}, \delta}$ to q - $BDD_{\mathcal{L}, \delta}$.

The proof of this lemma is lattice preserving, and so one can reduce BDD on any given lattice to solving q -BDD on that lattice. We will later use this repeatedly in the cases when $\mathcal{L}$ is a one- or two-sided ideal lattice in an order of a cyclic division algebra (definitions postponed).

Definition 16. *We denote by $DGS_{\mathcal{L},\xi}$ the problem of sampling a discrete Gaussian $D_{\mathcal{L},\xi}$, $\xi > 0$, where $\mathcal{L}$ is some n -dimensional lattice.*

2.5 LWE

The lattice problems we have defined so far (SVP, SIVP, etc) have been found to be largely unsuitable to build cryptographic functionality from directly. We instead use problems which we know can be used in cryptography (e.g. to build encryption or signature schemes), and we then reduce intractable lattice problems to these more obviously useful problems. This allows us to obtain cryptographic functionality *and* some kind of security guarantee. In this thesis the major problem considered from which to ‘do cryptography’ on lattices is Learning with Errors (LWE); we also later consider NTRU.

Definition 17. (*LWE Distribution*) *Let $n \in \mathbb{Z}$, $q \geq 2$, and χ be an error distribution over $\mathbb{R}/\mathbb{Z}$. Let $\mathbf{s} \in \mathbb{Z}_q^n$. Define the LWE distribution $A_{\mathbf{s},\chi}$ as the distribution over $\mathbb{Z}_q^n \times \mathbb{R}/\mathbb{Z}$ obtained by sampling $\mathbf{a} \in \mathbb{Z}_q^n$ uniformly at random, $e \leftarrow \chi$, and outputting $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle / q + e \bmod \mathbb{Z})$.*

Cryptographic problems are then defined, using this distribution.

Definition 18. (*Search LWE*) *The search LWE problem $LWE_{\mathbf{s},\chi}$ is, given independently chosen samples from $A_{\mathbf{s},\chi}$ for arbitrary $\mathbf{s}$ and χ , to find $\mathbf{s}$.*

Let Υ be a distribution over possible LWE error distributions.

Definition 19. (*Decision LWE*) *The decision LWE problem $dLWE_{\mathbf{s},\chi}$ is, given samples chosen either independently from $A_{\mathbf{s},\chi}$ with $\mathbf{s} \leftarrow U(\mathbb{Z}_q^n)$ and $\chi \leftarrow \Upsilon$, or from $U(\mathbb{Z}_q^n \times \mathbb{R}/\mathbb{Z})$, to decide which with non-negligible advantage.*

We postpone the definition of NTRU. It will be helpful for the numerous sections below to give a high-level overview of the reduction from SIVP to LWE provided by Regev in [138]. In this setting, the LWE error is sampled from D_α for some $\alpha > 0$.

The reduction begins by observing that SIVP reduces to DGS in polynomial time ([138, Lemma 3.17]), so it suffices to firstly reduce DGS to search LWE, and then, secondly, reduce search LWE to decision LWE. The outline of the first reduction is as follows. It uses the so-called ‘iterative step’ to, given polynomially-many samples from a discrete Gaussian $D_{\mathcal{L},r}$ for very large r , sample from a discrete Gaussian $D_{\mathcal{L},r'}$ where $r' = \frac{r\sqrt{n}}{\alpha q}$ and $\alpha q > 2\sqrt{n}$, so $r' < \frac{r}{2}$. This initial value of r is taken sufficiently large to sample $D_{\mathcal{L},r}$ efficiently by Lemma 2.5. Applying this step polynomially-many times allows one to sample from $D_{\mathcal{L},r''}$ for some pre-specified $r'' \ll r$. Designing the iterative step, then, is the crux of the method. This step has two parts, one classical, one quantum. The first, classical, step, takes in polynomially-many samples from $D_{\mathcal{L},r}$ and a search LWE oracle as input, and solves BDD_δ on the dual lattice $\mathcal{L}^\vee$ with $\delta \leq \frac{\alpha q}{r}$. The second, quantum, step uses this BDD solver to construct a quantum algorithm to sample from $D_{\mathcal{L},r'}$. Combining these two provides the structure of the iterative step.

The quantum step is lattice-preserving, as is the reduction from SIVP to DGS, facts often used to obtain security proofs of structured variants of LWE. In other words, to derive a reduction from structured lattice problems to variants of search LWE, it often suffices to reduce BDD on some (dual) lattice to the structured search LWE instance desired - but more on that later.

As for the search to (worst-case) decision reduction, one begins by simply guessing an entry of the secret vector. If g_i is a guess for s_i and the LWE sample is $(\mathbf{a}, b) = (\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e \bmod q)$, then sampling v uniformly over $\mathbb{Z}_q$ and setting $(\mathbf{a}', b') := (\mathbf{a} + (0, \dots, v, \dots, 0), b + vg_i \bmod q)$, where $(0, \dots, v, \dots, 0)$ has v in the i th position, one finds

$$\begin{aligned} b' &= b + vg_i = \mathbf{a}^t \mathbf{s} + e + vg_i = \mathbf{a}'^t \mathbf{s} - (0, \dots, v, \dots, 0)^t \mathbf{s} + vg_i + e \\ &= \mathbf{a}'^t \mathbf{s} - vs_i + vg_i + e = \mathbf{a}'^t \mathbf{s} - v(s_i - g_i) + e \bmod q, \end{aligned}$$

which is an LWE sample if $g_i = s_i \bmod q$, and is uniform otherwise. Thus the decision oracle can be used to discern when $g_i = s_i \bmod q$, and so via this transform, calling the decision oracle on the outcomes of repeated experiments, provides the whole secret $\mathbf{s}$.

2.6 Structured LWE

We now move to consider algebraically structured forms of LWE, focusing on RLWE, which uses a structure obtained from ideals of rings of integers of cyclotomic fields. Denote such a field by K . To both use the algebraic structure from ideals in $\mathcal{O}_K$ (or some other algebraic object) and also to be able to obtain hardness guarantees from geometric computational problems, we embed ideals into $\mathbb{R}^n$. We do this through the *canonical embedding*.

2.6.1 The Canonical Embedding

Let K be a finite Galois number field over $\mathbb{Q}$ over degree n . Then (by the Primitive Element Theorem) there exists some α such that $K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(m_\alpha(x))$ where $m_\alpha(x)$ is the minimal polynomial of α over $\mathbb{Q}$. Since K is assumed to be Galois, there are n distinct automorphisms of K defined by their action on the roots of $m_\alpha(x)$, and in particular on their action on α , and these automorphisms extend to n distinct embeddings $K \hookrightarrow \mathbb{C}$. Such an embedding σ_i is *real* if $\sigma_i(K) \subset \mathbb{R}$, and is otherwise *complex*. A number field is *totally real* (resp. *totally complex*) if all of its embeddings into $\mathbb{C}$ are in fact embeddings into $\mathbb{R}$ (resp. not into $\mathbb{R}$). It is well known that any Galois extension of $\mathbb{Q}$ is either totally real or totally complex. There are r_1 real embeddings of a number field and r_2 pairs of complex embeddings, such that $r_1 + 2r_2 = n$. Ordering the real embeddings first, and then the complex embeddings such that $\sigma_{r_1+j} = \overline{\sigma_{r_1+r_2+j}}$ for $1 \leq j \leq r_2$, we define

Definition 20. *The canonical embedding is the embedding $\sigma_K : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$ such that*

$$x \mapsto (\sigma_1(x), \dots, \sigma_n(x)),$$

and $\text{im } \sigma_K \subset H := \{(x_1, \dots, x_n) \in \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} : x_{r_1+j} = \overline{x_{r_1+r_2+j}}, 1 \leq j \leq r_2\}$.

We have $H \cong \mathbb{R}^n$ as inner product spaces. We have $\sigma_K(x) + \sigma_K(y) = \sigma_K(x + y)$, so the image of any algebraic lattice in K is a lattice in $\mathbb{R}^n$, and $\sigma_K(xy) = \sigma_K(x) \star \sigma_K(y)$, where $\star$ is the

entry-wise product of vectors.

An alternative way of embedding a Galois number field into $\mathbb{R}^n$ is by writing $K = \mathbb{Q}(\alpha)$ for some element α and writing $x = x_1\alpha + \dots + x_n\alpha^n$ for $x \in K, x_i \in \mathbb{Q}$. The element x can then be mapped to $(x_1, \dots, x_n) \in \mathbb{R}^n$. This is called the *coefficient embedding* of x , denoted $\text{coeff}(x)$.

Ring LWE

In [102] the canonical embedding was used to embed ideals of the ring of integers of a number field K into $\mathbb{R}^n$, and the algebraic structure was used to define an LWE-style problem, Ring Learning with Errors (RLWE) as below. Here, $K_{\mathbb{R}} = K \otimes \mathbb{R}$ and $\mathcal{O}_{K_q} = \mathcal{O}_K/q\mathcal{O}_K$.

Definition 21. (*RLWE Distribution*) Let $n \in \mathbb{Z}$, $q \geq 2$, and χ be an error distribution over $K_{\mathbb{R}}$. Let $s \in \mathcal{O}_{K_q}^{\vee}$. Define the RLWE distribution $A_{s,\chi}$ as the distribution over $\mathcal{O}_{K_q} \times K_{\mathbb{R}}/\mathcal{O}_K^{\vee}$ obtained by sampling $a \in \mathcal{O}_{K_q}$ uniformly at random, $e \leftarrow \chi$, and outputting $(a, as/q + e \bmod \mathcal{O}_K^{\vee})$.

From this distribution we can define search and decision problems, as we did for LWE.

Definition 22. (*Search RLWE*) The search RLWE problem $RLWE_{s,\chi}$ is, given independently chosen samples from $A_{s,\chi}$ for arbitrary $s \in \mathcal{O}_{K_q}^{\vee}$ and χ , to find s .

Again, let Υ be a distribution over possible RLWE error distributions.

Definition 23. (*Decision RLWE*) The decision RLWE problem $dRLWE_{s,\chi}$ is, given samples chosen either independently from $A_{s,\chi}$ for $s \leftarrow U(\mathcal{O}_{K_q}^{\vee})$ and $\chi \leftarrow \Upsilon$, or from $U(\mathcal{O}_{K_q} \times K_{\mathbb{R}}/\mathcal{O}_K^{\vee})$, to decide which (with non-negligible advantage).

Samples from the RLWE distribution give structured LWE instances. To see this, recall that the above rings (in the power-of-two case) look like $R = \mathcal{O}_K = \mathbb{Z}[x]/(x^n + 1)$ where n is a power of two. If we fix the basis $\{1, x, \dots, x^{n-1}\}$ and consider multiplication on any other element, say $s = s_0 + s_1x + \dots + s_{n-1}x^{n-1}$, by some element $a = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$, one can see that

over $\mathbb{Z}$ we obtain

$$\begin{pmatrix} a_0 & -a_{n-1} & \cdots & -a_1 \\ a_1 & a_0 & \cdots & -a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_0 \end{pmatrix} \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix}.$$

If we use these polynomials to form a sample $(a, as + e \bmod q)$, the structure of the matrix representation means one only needs to store the n coefficients of a , rather than an entire matrix.

Security proofs have been given for RLWE in a similar fashion to LWE. These reduce ideal-SVP, that is SVP on the canonical embedding of an ideal of $\mathcal{O}_K$, to search RLWE, since SIVP and SVP are equivalent in a cyclotomic field: note that multiplication by a root of unity preserves the length of a vector, so solving SVP and multiplying the shortest vector by the powers of ζ_n results in n short vectors, as required by SIVP.

The key adaptation of Regev's reduction to search in the RLWE reduction is the 'clearing ideals' lemma:

Lemma 2.13. *[102, Lemma 2.15] Let $\mathcal{I}$ and $\mathcal{J}$ be ideals in R , let $t \in \mathcal{I}$ be such that $t \cdot \mathcal{I}^{-1}$ is coprime with $\mathcal{J}$, and let $\mathcal{M}$ be any fractional ideal in K . Then the function $\theta_t : K \rightarrow K$ defined as $\theta_t(u) = t \cdot u$ induces an isomorphism from $\mathcal{M}/\mathcal{J}\mathcal{M}$ to $\mathcal{I}\mathcal{M}/\mathcal{I}\mathcal{J}\mathcal{M}$, as R -modules. Moreover, this isomorphism may be efficiently inverted given $\mathcal{I}, \mathcal{J}, \mathcal{M}$, and t .*

This is used to prove the q -BDD to search RLWE reduction, where the q -BDD instance $y = x + e \bmod q$ is over the canonical embedding of $\mathcal{I}^\vee$, for some ideal $\mathcal{I} \subset \mathcal{O}_K$, as follows: one samples $z \leftarrow D_{\mathcal{I},r}$ and $e' \leftarrow D_{\alpha/\sqrt{2}}$, and computes $(a, b) \in \mathcal{O}_{K_q} \times K_{\mathbb{R}}/\mathcal{O}_K^\vee$, where

$$a = \theta_t^{-1}(z \bmod q\mathcal{I}) \in \mathcal{O}_{K_q} \quad \text{and} \quad b = (z \cdot y)/q + e' \bmod \mathcal{O}_K^\vee.$$

Then one finds $b = (z \cdot y)/q + e' = zx/q + ze/q + e' = zx/q + e''$. Rewriting $zx = tax \bmod q\mathcal{O}_K^\vee$, setting $s := tx \bmod q\mathcal{O}_K^\vee$, and checking the error is distributed correctly yields a sample negligible statistical distance from an RLWE sample; the assumed search RLWE oracle then recovers s , and thence $x \bmod q$, solving the q -BDD instance as desired.

The reduction from search RLWE to worst-case decision RLWE follows a similar strategy to the plain LWE proof. Using the CRT, one has $\mathcal{O}_K^\vee/q\mathcal{O}_K^\vee \cong \prod_{i=1}^g \mathcal{O}_K^\vee/\mathfrak{q}_i\mathcal{O}_K^\vee$, where $q \in \mathbb{Z}$ is a prime unramified in $\mathcal{O}_K$ such that $q\mathcal{O}_K = \prod_{i=1}^g \mathfrak{q}_i$ and g is bounded. One reduces from search RLWE ‘modulo q ’ to search RLWE ‘modulo $\mathfrak{q}_i$ ’ since transitivity of the Galois group on the ideals above q allows one to find a solution modulo $\mathfrak{q}_i$ and from there obtain the solution modulo the other factors of q , and patch a solution modulo q together by inverting the CRT.

From here one employs a hybrid distribution. We outline this step because of its relevance to CLWE. The hybrid distribution $A_{s,\psi}^i$ over $\mathcal{O}_{K_q} \times K_{\mathbb{R}}/\mathcal{O}_K^\vee$ is defined by sampling $(a, b) \leftarrow A_{s,\psi}$ and outputting $(a, b + h/q)$, where $h \in \mathcal{O}_{K_q}^\vee$ is uniformly random and independent mod $\mathfrak{q}_j\mathcal{O}_K^\vee$ for all $j \leq i$, and 0 mod the remaining $\mathfrak{q}_j\mathcal{O}_K^\vee$.¹ Here ψ is an error distribution over $K_{\mathbb{R}}$. Then worst-case decision RLWE mod $\mathfrak{q}_i$, $\text{WDLWE}_{q,\Psi}^i$, is, given access to $A_{s,\psi}^j$ for arbitrary $s \in \mathcal{O}_{K_q}^\vee$, $\psi \in \Psi$, and $j \in \{i-, i\}$, to find j , for $i \in \mathbb{Z}_g$ and some family of distributions Ψ .

Then, given an RLWE sample (a, b) , one guesses s with g and computes

$$(a', b') = (a + v, b + (h + vg)/q) \in \mathcal{O}_{K_q} \times K_{\mathbb{R}}/\mathcal{O}_K^\vee,$$

where $v \in \mathcal{O}_{K_q}$ is uniformly random mod $\mathfrak{q}_i$ and 0 mod $\mathfrak{q}_j$ for $j \neq i$, and $h \in \mathcal{O}_{K_q}^\vee$ is uniformly random and independent mod $\mathfrak{q}_j\mathcal{O}_K^\vee$ for all $j < i$, and 0 mod the remaining $\mathfrak{q}_j\mathcal{O}_K^\vee$. Observe

$$\begin{aligned} b' &= b + (h + vg)/q = as/q + e + h/q + vg/q \\ &= ((a + v)s + h + v(g - s))/q + e. \end{aligned}$$

If the guess $g = s$, this is $A_{s,\psi}^{i-1}$; else $A_{s,\psi}^i$. Note this crucially requires, when $g \neq s$, for $g - s$ to be invertible modulo $\mathfrak{q}_j\mathcal{O}_K^\vee$, which holds since $\mathcal{O}_K^\vee/\mathfrak{q}_j\mathcal{O}_K^\vee$ is a finite field.

Module LWE

It is straightforward to extend the above definitions to modules of finite rank over $\mathcal{O}_K$. Recall a left module $\mathcal{M}$ over a ring R is an additively closed set equipped with a scalar multiplication

¹Here $A_{s,\psi}^0 := A_{s,\psi}$.

from R satisfying

1. $r(m_1 + m_2) = rm_1 + rm_2$,
2. $(r + s)m = rm + sm$,
3. $r(sm) = (rs)m$, and
4. $1m = m$,

where $r, s \in R$ and $m, m_1, m_2 \in \mathcal{M}$. A right module is defined analogously, and a module is two-sided if it is both a left and right R -module. The set of torsion elements of $\mathcal{M}$ is

$$t(\mathcal{M}) := \{m \in \mathcal{M} : \exists r \in R \setminus \{0\} : rm = 0\}$$

An R -module $\mathcal{M}$ is called free if $\mathcal{M} \cong R^n$, for some n , and *projective* if there exists an R -module $\mathcal{N}$ such that $\mathcal{M} \oplus \mathcal{N} \cong R^n$, for some n . For equivalent definitions of projectivity, see [96]. To define module LWE, we consider two-sided modules of finite rank over $\mathcal{O}_K$, contained in K^m , for some m . It is well known² that given some $\mathcal{O}_K$ -module $\mathcal{M}$, there exist nonzero ideals $\mathcal{I}_k$ of $\mathcal{O}_K$ and linearly independent vectors $(b_k)_k$ of K^m such that $\mathcal{M} = \sum_{k=1}^n \mathcal{I}_k \cdot b_k$, for some $n \leq m$. Then $[(\mathcal{I}_k)_k, (b_k)_k]$ is called a *pseudo-basis* of $\mathcal{M}$. We define a notion of duality on modules using the field trace, and apply it to the pseudo-basis presentation of a module:

Definition 24. $\mathcal{M}^\vee := \{\mathbf{x} \in K^m : \text{Tr}(\langle \mathbf{x}, \bar{\mathbf{y}} \rangle) \in \mathbb{Z} \ \forall \ \mathbf{y} \in \mathcal{M}\}$, where $\langle \cdot, \cdot \rangle$ is the Hermitian form on $\mathbb{C}^m$, $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_i x_i \bar{y}_i$.

If $[(\mathcal{I}_k)_k, (b_k)_k]$ is a pseudo-basis of $\mathcal{M}$, so $\mathcal{M} = \sum_{k=1}^n \mathcal{I}_k \cdot b_k$, we have $\mathcal{M}^\vee = \sum_{k=1}^n \mathcal{I}_k^\vee \cdot b_k^\vee$, where $\langle b_k, b_j^\vee \rangle = 1$ if and only if $k = j$, and 0 otherwise. We now define module LWE.

Definition 25. (*MLWE Distribution*) Let $n \in \mathbb{Z}$, $q \geq 2$, and χ be an error distribution over $K_\mathbb{R}$. Let $\mathbf{s} \in \left(\mathcal{O}_{K_q}^\vee\right)^m$. Define the MLWE distribution $A_{\mathbf{s}, \chi}$ as the distribution over $\mathcal{O}_{K_q}^m \times K_\mathbb{R} / \mathcal{O}_K^\vee$ obtained by sampling $\mathbf{a} \in \mathcal{O}_{K_q}^m$ uniformly at random, $e \leftarrow \chi$, and outputting $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle / q + e \bmod \mathcal{O}_K^\vee)$.

²See, for example, [53, §1.2.23]

From this distribution we can define search and decision problems, as we did for LWE.

Definition 26. (*Search MLWE*) The search MLWE problem $MLWE_{s,\chi}$ is, given independently chosen samples from $A_{s,\chi}$ for arbitrary s and χ , to find s .

Let Υ be a distribution over possible MLWE error distributions.

Definition 27. (*Decision MLWE*) The decision MLWE problem $dMLWE_{s,\chi}$ is, given samples chosen either independently from $A_{s,\chi}$ with $s \leftarrow U\left(\left(\mathcal{O}_{K_q}^\vee\right)^m\right)$ and $\chi \leftarrow \Upsilon$, or from $U\left(\mathcal{O}_{K_q}^m \times K_{\mathbb{R}}/\mathcal{O}_K^\vee\right)$, to decide which (with non-negligible advantage).

Like before, reductions were given, this time from SIVP (which is not equivalent to SVP in module lattices) to MLWE. The iterative step of the reduction from SIVP to search MLWE and the reduction from search to worst-case decision only require mild adaptations to the module lattice setting.

A Smörgåsbord of Algebraic Structures for LWE

In fact, the first variant of LWE using more structured rings was not [102], but [155]. The authors used more general rings than the ring of integers of cyclotomics, and this variant has subsequently been named Polynomial LWE (PLWE). One samples from a domain defined by $\mathbb{Z}_q[x]/(f(x))$ for some irreducible polynomial $f(x)$, and the underlying problems are based on the hardness of lattices obtained under the coefficient embedding. Results relating the hardness of RLWE and PLWE can be found in [141] and [37].

A generalisation of RLWE in another direction concerns *suborders* of $\mathcal{O}_K$. Here one samples from $\mathcal{O} \subsetneq \mathcal{O}_K$. This was defined in [27], and further hardness guarantees were obtained in [28]. There have also been generalisations of MLWE. These include [47], in which the dihedral group rings $\mathbb{Z}[D_{2n}]$ were used to construct structured forms of rank-2 MLWE over cyclotomic rings - and on these, much more later. A prior effort at structuring MLWE is [123], which considered multivariate polynomial rings $\mathbb{Z}_q[x, y]/(f(x), g(y))$, and which was subjected to attack in [32]. A common thread among these variants, as we have seen for RLWE and MLWE, is the presence

of a matrix representation over $\mathbb{Q}$ for multiplication by the elements in the algebraic objects concerned. One can even begin from this perspective, as in some sense middle product LWE [140] does, which replaces the square public matrix A in LWE samples with a structured Toeplitz matrix, which corresponds to the middle product operation on two polynomials³ for which highly efficient algorithms exist. This leads us to the structures we are most concerned with in this thesis.

2.7 Cyclic Division Algebras

Here we define cyclic algebras, give conditions for them to be division algebras, and discuss certain orders they contain.

2.7.1 Algebras

Recall the *center* of a ring R , denoted $\mathcal{Z}(R)$, is the set of elements commuting with all other elements. Let K denote a field. A K -algebra is a ring that is equipped with an injective map $\varphi : K \hookrightarrow \mathcal{Z}(\mathcal{A})$ into the center of $\mathcal{A}$. This makes $\mathcal{A}$ into a vector space over K .

We say $\mathcal{A}$ is *central* if $\mathcal{Z}(\mathcal{A}) = K$. We say $\mathcal{A}$ is *simple* if $\mathcal{A}$ has no nontrivial two-sided ideals. An example of a simple algebra over a field is $M_n(\mathbb{F})$, the $n \times n$ matrix ring over a field $\mathbb{F}$. All algebras in this thesis will be unital, that is, $1 \in \mathcal{A}$.

Here we also define some properties of noncommutative rings that will be referred to below. A (noncommutative) ring R is called *prime* if for all ideals I, J in R , we have $IJ = 0 \Rightarrow I = 0$ or $J = 0$. R is called *hereditary* if every ideal is a projective R -module. Finally, R is called *Dedekind prime* if it is Noetherian, hereditary, and prime.

³Multiply two polynomials, discard the highest and lowest coefficients, then shift the remaining coefficients down such that the lowest remaining coefficient becomes the constant term.

2.7.2 Cyclic Algebras and Non-norm Elements

We define (and construct) *cyclic* algebras as follows: let L/K be a degree $d < \infty$ extension of number fields with cyclic Galois group. Denote a generator of the Galois group by θ . Consider the following direct sum:

$$\mathcal{A} = L \oplus uL \oplus \dots \oplus u^{d-1}L,$$

where u is an auxiliary element satisfying the properties 1) $u^d = \gamma$, where $\gamma \in K$, and 2) for all $x \in L$, we have $xu = u\theta(x)$. $\mathcal{A}$ is a central simple K -algebra, and property 2) gives it a non-commutative multiplication operation. Such an algebra is called a *cyclic algebra*. To ensure every element of $\mathcal{A}$ has a multiplicative inverse, we require that γ is a *non-norm element*:

Definition 28. *An element γ of K is non-norm if there does not exist an element $x \in L$ such that $\gamma^i = N_{L/K}(x)$, for $0 < i < [L : K]$. Equivalently, γ is non-norm if $\gamma \notin N_{L/K}(N^\times)$ for all proper intermediate subfields $K \subset N \subset L$ [118].*

This definition is meaningful, since the answer to the question: for a given extension L/K , is the norm map surjective? is often no; for instance, -1 is not in $N_{\mathbb{Q}(i)/\mathbb{Q}}(\mathbb{Q}(i)^\times)$. The relevance of this is

Proposition 2.5. *[6] A cyclic algebra $\mathcal{A}$ is a division algebra if and only if γ is a non-norm element.*

Then $\mathcal{A}$ is called a *cyclic division algebra* (CDA) with non-norm element γ . The following proposition states that only some powers of an element need be checked to verify that it satisfies the non-norm condition:

Proposition 2.6. *[166, Proposition 3.6] A cyclic algebra $\mathcal{A} = (L/K, \theta, \gamma)$ with $[L : K] = d$ is a division algebra if and only if $\gamma^{d/p}$ is not the norm of any element of $L^\times$, where p is any prime divisor of d or p is equal to d .*

When γ is non-norm, we denote this algebra by $\mathcal{A} = (L/K, \theta, \gamma)$.

2.7.3 (Maximal) Orders in CDAs

Here we discuss integral structures lying within CDAs. The chief reference is [139]; [92] provides a nice introduction. We denote a general cyclic K -algebra by A , and a CDA by $\mathcal{A}$.

Definition 29. *An $\mathcal{O}_K$ -order in A is a full $\mathcal{O}_K$ -lattice $\mathcal{O}$ in A which is a subring of A . Thus a $\mathbb{Z}$ -order $\mathcal{O}$ in an algebra A is a finitely generated $\mathbb{Z}$ -module that contains a $\mathbb{Q}$ -basis of A , and is also a unital subring of A . If a set is called an order, it is understood to be an $\mathcal{O}_K$ -order. Every order in A contains $\mathcal{O}_K$.*

In any cyclic K -algebra A there always exists a maximal order (with respect to inclusion), and every order is contained within some maximal order.

We will primarily use the following order of $(L/K, \theta, \gamma)$, where $\gamma \in \mathcal{O}_K$, which we will call the *natural order*:

$$\Lambda = \bigoplus_{i=0}^{d-1} u^i \mathcal{O}_L = \mathcal{O}_L \oplus u \mathcal{O}_L \oplus u^2 \mathcal{O}_L \oplus \dots \oplus u^{d-1} \mathcal{O}_L$$

When γ is a unit, it is possible that the natural order is also maximal, i.e. that Λ is not contained in any other non-trivial order. When $K = \mathbb{Q}(\zeta_n)$, L is a certain cyclic Galois extension of K , and $\gamma = \zeta_n$, for n a prime power, Λ was shown to be maximal in [71]. We now outline this construction.

Write $n = p^r$ for some prime p and $r \in \mathbb{N}$. We then select a second prime $\ell > 2$ such that $\ell \equiv 1 \pmod{n}$, and also such that $\ell \not\equiv 1 \pmod{pn}$. Set $M = \mathbb{Q}(\zeta_n, \zeta_\ell) = \mathbb{Q}(\zeta_{n\ell})$. We then fix a degree d subfield of M over K by taking the fixed field of σ^d , where d is a divisor of $\ell - 1$ of desired size such that $\gcd(d, n) > 1$. Since $\gcd(\ell, n) = 1$, M/K is a Galois extension with cyclic Galois group, so we can write $\text{Gal}(M/K) = \langle \sigma \rangle$, and hence the fixed field of σ^d also has cyclic Galois group over K . In [71, Theorem 2] it was proved that the resulting algebra $(L/K, \theta, \zeta_n)$ is division, where $\text{Gal}(L/K) = \langle \theta \rangle$ for some automorphism θ , and in [71, Theorem 3] that the natural order of those CDAs are maximal.

As will be seen in the following section, maximal orders have particularly nice properties.

2.8 Ideals in Orders of CDAs

It will be useful to expand upon the theory of ideals in orders of CDAs. We do this because we will need the theory of both two-sided and one-sided ideals in maximal orders for our reductions later on in this thesis. We begin with two standard results on lattices, before moving on to ideals.

Proposition 2.7. *If $\mathcal{I}, \mathcal{J}$ are full $\mathcal{O}_K$ -lattices in A , $\mathcal{I}\mathcal{J}$ is a full $\mathcal{O}_K$ -lattice, where*

$$\mathcal{I}\mathcal{J} = \left\{ \sum_{i=1}^j x_i y_i : x_i \in \mathcal{I}, y_i \in \mathcal{J}, j \in \mathbb{N} \right\}$$

Definition 30. *Let $\mathcal{L}$ be a full $\mathcal{O}_K$ -lattice in A . The left order of $\mathcal{L}$ is defined*

$$\mathcal{O}_l(\mathcal{L}) = \{a \in A : a\mathcal{L} \subset \mathcal{L}\}.$$

The right order is defined analogously. They are both $\mathcal{O}_K$ -orders in A . If $\mathcal{I}$ and $\mathcal{J}$ are full $\mathcal{O}_K$ -lattices in A , $\mathcal{I}\mathcal{J}$ is a proper product if $\mathcal{O}_r(\mathcal{I}) = \mathcal{O}_l(\mathcal{J})$.

Ideals in Maximal Orders

We will see how the ideal theory of orders changes depending on whether a given order is maximal or not. The theory in the case of maximal orders is much better behaved than for non-maximal orders.

Definition 31. *Let $\mathcal{O}$ be an order in A . A left integral ideal in $\mathcal{O}$ is an additive subgroup $\mathcal{I}$ such that $\mathcal{O}\mathcal{I} \subset \mathcal{I}$. A left fractional ideal is a subset of the form $\lambda\mathcal{I}$, for some left integral ideal $\mathcal{I}$ and $\lambda \in \mathcal{O}_K \setminus \{0\}$. Right ideals are defined analogously, and an ideal which is both left and right is called two-sided. An ideal in $\mathcal{O}$ may be called an $\mathcal{O}$ -ideal.*

Proposition 2.8. *Any full $\mathcal{O}_K$ -lattice $\mathcal{I}$ is a left $\mathcal{O}_l(\mathcal{I})$ -ideal, and $\mathcal{O}_l(\mathcal{I})$ is the largest order for which $\mathcal{I}$ is a left ideal. If $\mathcal{I} \subset \mathcal{O}$, for some order $\mathcal{O}$, then $\mathcal{O} \subset \mathcal{O}_l(\mathcal{I})$.*

Let $\mathcal{I}$ be a left $\mathcal{O}$ -ideal. Then it can be seen that $\mathcal{I}$ is two-sided if and only if $\mathcal{O} \subset \mathcal{O}_r(\mathcal{I})$. When $\mathcal{O}$ is maximal, this is equivalent to $\mathcal{O}_l(\mathcal{I}) = \mathcal{O}_r(\mathcal{I})$. We say an ideal is *full* if it is full as a lattice, and it turns out any ideal in an order of a division algebra is full. Following [92], we denote by $\text{Frac}_l(\mathcal{O})$ the set of full left $\mathcal{O}$ -ideals, and $\text{Frac}_2(\mathcal{O})$ the set of full two-sided $\mathcal{O}$ -ideals.

The Case of Two-sided Ideals

In the following, $\mathcal{I}$ and $\mathcal{J}$ will be full $\mathcal{O}_K$ -lattices. By Proposition 2.7, the product of two left $\mathcal{O}$ -ideals is again a left $\mathcal{O}$ -ideal, and $\mathcal{O}_l(\mathcal{I}\mathcal{J}) \supset \mathcal{O}_l(\mathcal{I})$ and $\mathcal{O}_r(\mathcal{I}\mathcal{J}) \supset \mathcal{O}_r(\mathcal{J})$. This implies closure under multiplication of two-sided ideals.

Definition 32. Define the inverse of $\mathcal{I}$ to be $\mathcal{I}^{-1} = \{\alpha \in A : \mathcal{I}\alpha\mathcal{I} \subset \mathcal{I}\}$.

Proposition 2.9. [139, §22.6, §23.3, §22.7] $\mathcal{I}^{-1}$ is a full $\mathcal{O}_K$ -lattice in A . We have

$$\mathcal{O}_l(\mathcal{I}^{-1}) \supset \mathcal{O}_r(\mathcal{I}), \quad \mathcal{O}_r(\mathcal{I}^{-1}) \supset \mathcal{O}_l(\mathcal{I}), \quad \mathcal{I}\mathcal{I}^{-1} \subset \mathcal{O}_l(\mathcal{I}), \text{ and } \mathcal{I}^{-1}\mathcal{I} \subset \mathcal{O}_r(\mathcal{I}).$$

If $\mathcal{I}$ is a two-sided ideal of a maximal order $\mathcal{O}$, $\mathcal{I}^{-1}$ is also an $\mathcal{O}$ -ideal such that

$$\mathcal{I}\mathcal{I}^{-1} = \mathcal{I}^{-1}\mathcal{I} = \mathcal{O}.$$

Thus in a maximal order the full two-sided ideals have unique inverses, with identity element being the order itself.

As usual, if $\mathcal{I}, \mathcal{J}$ are $\mathcal{O}$ -ideals such that $\mathcal{I} \supset \mathcal{J}$, we say $\mathcal{I}$ *divides* $\mathcal{J}$ and write $\mathcal{I} \mid \mathcal{J}$. If $\mathfrak{P}$ is a two-sided ideal in $\mathcal{O}$, we say $\mathfrak{P}$ is *prime* if $\mathfrak{P} \mid \mathcal{I}\mathcal{J}$ implies $\mathfrak{P} \mid \mathcal{I}$ or $\mathfrak{P} \mid \mathcal{J}$ for any two-sided ideals $\mathcal{I}, \mathcal{J}$. In CDAs the prime ideals perform a similar role as in number fields; we have the following theorem:

Theorem 2.4. [139, Theorem 22.10] Suppose $\mathcal{O}$ is a maximal $\mathcal{O}_K$ -order in A . Then $\text{Frac}_2(\mathcal{O})$ is an abelian group with respect to multiplication, and any proper ideal factors into a product of powers of prime ideals in a unique way.

This theorem does not hold in the non-maximal order case. In addition, the theorem does not hold for one-sided ideals: while the product of two one-sided ideals is again a one-sided ideal, the inverse of a one-sided $\mathcal{O}$ -ideal is not again (in general) an $\mathcal{O}$ -ideal, even if $\mathcal{O}$ is maximal.

We also define a multiplicative norm on two-sided ideals. Let $\mathcal{I}$ be an integral ideal of a maximal order $\mathcal{O}$; then $N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) := |\mathcal{O}/\mathcal{I}|$.

Next, we record an important property of prime ideals of maximal orders:

Proposition 2.10. *[139, Theorem 32.1] The prime ideals of a maximal order coincide with its maximal two-sided ideals. There is a bijective correspondence between the nonzero prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ and the prime ideals $\mathfrak{P} \subset \mathcal{O} : \mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. Moreover, we have $\mathfrak{p}\mathcal{O} = \mathfrak{P}^{e_{\mathfrak{p}}}$ for some integer $e_{\mathfrak{p}}$.*

This result allows us to study prime ideals of Λ (when Λ is maximal) by studying ideals of $\mathcal{O}_K$, which are well understood.

There are two forms of the Chinese Remainder Theorem (CRT) that will be useful. The first is the CRT ‘proper’:

Theorem 2.5. *[139, §22, ex.3] Let $\mathfrak{P}_1, \dots, \mathfrak{P}_n$ be distinct prime ideals of Λ . Let*

$$\mathfrak{B} := \prod_{i=1}^n \mathfrak{P}_i^{e_i}, \quad e_i \in \mathbb{Z}.$$

If each $e_i \geq 0$, then there is a ring isomorphism

$$\Lambda/\mathfrak{B} \cong \prod_{i=1}^n \Lambda/\mathfrak{P}_i^{e_i}.$$

This holds more generally for quotients by products of pairwise coprime ideals. The second form is a CRT-style decomposition of the quotient of Λ by an ideal of the form $\mathcal{I}\Lambda$, for any $\mathcal{I} \in \mathcal{O}_K$:

Theorem 2.6. *[119, Lemma 4] Let Λ be the natural order of a cyclic division algebra $\mathcal{A} = (L/K, \theta, \gamma)$ and $\mathcal{I}$ be an ideal of $\mathcal{O}_K$ which factors into a product of prime ideals as $\mathcal{I} = \mathfrak{q}_1^{e_1} \dots \mathfrak{q}_g^{e_g}$*

as an ideal of $\mathcal{O}_K$. Then, we have the isomorphism

$$\Lambda/\mathcal{I}\Lambda \cong \mathcal{R}_1 \times \dots \times \mathcal{R}_g$$

where $\mathcal{R}_i = \bigoplus_{j=0}^{d-1} u^j (\mathcal{O}_L/\mathfrak{q}_i^{e_i} \mathcal{O}_L)$ is the ring subject to the relations $(\ell + \mathfrak{q}_i^{e_i} \mathcal{O}_L) u = u (\theta(\ell) + \mathfrak{q}_i^{e_i} \mathcal{O}_L)$ and $u^d = \gamma + \mathfrak{q}_i^{e_i}$.

The Case of One-Sided Ideals

We now develop the one-sided ideal theory. In the following, $\mathcal{I}$ will be a full $\mathcal{O}_K$ -lattice. By Proposition 2.7, the product of two left $\mathcal{O}$ -ideals is again a left $\mathcal{O}$ -ideal, and $\mathcal{O}_l(\mathcal{I}\mathcal{J}) \supset \mathcal{O}_l(\mathcal{I})$ and $\mathcal{O}_r(\mathcal{I}\mathcal{J}) \supset \mathcal{O}_r(\mathcal{J})$. So we have closure under multiplication of left (or right) ideals in a fixed order.

Proposition 2.11. *$\mathcal{I}^{-1}$ is a full $\mathcal{O}_K$ lattice in A . We have $\mathcal{O}_l(\mathcal{I}^{-1}) \supset \mathcal{O}_r(\mathcal{I})$, $\mathcal{O}_r(\mathcal{I}^{-1}) \supset \mathcal{O}_l(\mathcal{I})$, $\mathcal{I}\mathcal{I}^{-1} \subset \mathcal{O}_l(\mathcal{I})$, and $\mathcal{I}^{-1}\mathcal{I} \subset \mathcal{O}_r(\mathcal{I})$.*

Definition 33. *Say a lattice $\mathcal{I}$ is left invertible if $\mathcal{I}\mathcal{I}^{-1} \subset \mathcal{O}_l(\mathcal{I})$. Right invertibility is defined similarly, and for one-sided ideals one can replace lattice with ideal in the definition. In general, left and right invertibility are not equivalent.*

Definition 34. *An ideal of a maximal order is called normal. If $\mathcal{I}$ is normal, $\mathcal{I}$ is integral if it is integral for its left order.*

Proposition 2.12. *[139, §21.2, §22.9] Let $\mathcal{I}$ be a full $\mathcal{O}_K$ -lattice in A . Then $\mathcal{O}_l(\mathcal{I})$ is a maximal order if and only if $\mathcal{O}_r(\mathcal{I})$ is. If $\mathcal{I}$ is normal with left order $\mathcal{O}$ and right order $\mathcal{O}'$, then $\mathcal{I}$ is integral as a left $\mathcal{O}$ -ideal if and only if it is integral as a right $\mathcal{O}'$ -ideal, i.e., $\mathcal{I} \subset \mathcal{O}$ if and only if $\mathcal{O} \subset \mathcal{O}'$.*

Lemma 2.14. *[139, Theorem 22.19] Suppose $\mathcal{I}$ and $\mathcal{J}$ are integral normal ideals in A . If $\mathcal{I}\mathcal{J}$ is proper, it is also an integral ideal.*

While there isn't a 'nice' theory of one-sided prime ideals, one can still talk about factorizations

into one-sided maximal integral ideals, where maximal integral ideal means an integral normal ideal, maximal as a left ideal in its left order.

Theorem 2.7. *[139, Theorem 22.8] Let $\mathcal{I}$ be a proper integral ideal. Then $\mathcal{I}$ factors into a proper product of maximal integral ideals, and the number of factors is independent of the factorization.*

Lemma 2.15. *[139, Theorem 22.15] Let $\mathfrak{m}$ be a maximal left ideal of a maximal order $\mathcal{O}$. Then $\mathfrak{P} = \{\alpha \in \mathcal{O} : \alpha\mathcal{O} \subset \mathfrak{m}\}$ is a prime ideal of $\mathcal{O}$. Moreover, $\mathcal{O}/\mathfrak{m}$ is a simple left module finitely generated over $\mathcal{O}/\mathfrak{P}$.*

This lemma means that each maximal integral ideal $\mathfrak{m}$ has an unique associated two-sided ideal $\mathfrak{P}$ (inside a maximal order). While the above results are insufficient to form a group on the set of one-sided ideals, one can describe the *Brandt groupoid*, $BG(A)$, instead, which is the collection of normal ideals of A under multiplication restricted to proper products. We do not expand on the Brandt groupoid here, but do make the following observations for one-sided $\mathcal{I}$ with $\mathcal{O} = \mathcal{O}_l(\mathcal{I})$ and $\mathcal{O}' = \mathcal{O}_r(\mathcal{I})$: if $\mathcal{J}$ is any two-sided $\mathcal{O}$ -ideal, then $\mathcal{J}\mathcal{I}$ is a right $\mathcal{O}'$ -ideal, $\mathcal{I}^{-1}\mathcal{J}$ is a left $\mathcal{O}'$ -ideal, and $\mathcal{I}^{-1}\mathcal{J}\mathcal{I}$ is a two-sided $\mathcal{O}'$ -ideal.

Proposition 2.13. *[139, Theorem 22.21] Let $\mathcal{I}$ be a normal ideal with left order Λ and right order Γ . Let $\mathcal{I}(\Lambda)$ be the set of two-sided ideals of Λ , and similarly for Γ . Then there is an isomorphism $\varphi : \mathcal{I}(\Lambda) \cong \mathcal{I}(\Gamma)$ given by $\varphi(X) = \mathcal{I}^{-1}X\mathcal{I}$, for $X \in \mathcal{I}(\Lambda)$. Conversely, given maximal orders Λ, Γ such that there exists a normal ideal $\mathcal{I}$ with Λ, Γ as its left and right orders, this ideal induces an isomorphism via conjugation that is independent of the chosen ideal.*

2.9 CLWE

Embedding Integral Structures of CDAs into $\mathbb{R}^m$

Consider a CDA $\mathcal{A} = (L/K, \theta, \gamma)$ with $[L : K] = d$. Fixing the L -basis of $\mathcal{A}$, $\{u^i\}_{i \geq 0}$, we can express an element as the linear map $\phi(x)$ given by left multiplication on the u^i . For example,

if $x = \oplus_{i=0}^{d-1} u^i x_i \in \mathcal{A}$,

$$\phi(x) = \begin{pmatrix} x_0 & \gamma\theta(x_{d-1}) & \dots & \gamma\theta^{d-1}(x_1) \\ x_1 & \theta(x_0) & \dots & \gamma\theta^{d-1}(x_2) \\ \dots & \dots & \dots & \dots \\ x_{d-1} & \theta(x_{d-2}) & \dots & \theta^{d-1}(x_0) \end{pmatrix}.$$

If we denote the n embeddings $K \hookrightarrow \mathbb{C}$ by α , we can extend these to embeddings of L (which, in an abuse of notation, we also denote by α). It can be seen that all the nd embeddings of L are obtained from the set $\{\alpha \circ \theta^i\}_{\alpha, i}$. So we may form a vector in $\mathbb{R}^{nd^2}$ from x by concatenating the vectorized images of the $\alpha(\phi(x))$ for all $\alpha \in \text{Emb}(K)$. Then the image of any discrete additive subgroup of $\mathcal{A}$ is mapped to a lattice in $\mathbb{R}^{nd^2}$. Finally, we define two norms on $\mathcal{A}$: we set $\|x\|_p^p = \sum_{\alpha \in \text{Emb}(K)} \sum_{i,j} |\alpha(\phi(x)_{i,j})|^p$, and $\|x\|_\infty = \max_{\alpha, i, j} |\alpha(\phi(x)_{i,j})|$, where $\phi(x)_{i,j}$ denotes the i, j th entry of $\phi(x)$. We may use $\|\cdot\|$ to denote $\|\cdot\|_2$.

Let the trace $\text{Tr}(\cdot)$ of $x \in \mathcal{A}$ be defined $\text{Tr}(x) = T_{K/\mathbb{Q}} \circ \text{trace}(\phi(x))$, where $T_{K/\mathbb{Q}}$ is the field trace. This map is symmetric. The dual of an ideal $\mathcal{I}$ is the set

$$\mathcal{I}^\vee = \{x \in \mathcal{A} : \text{Tr}(x\mathcal{I}) \subset \mathbb{Z}\}.$$

The codifferent ideal of Λ is $\Lambda^\vee$.

Lattice Problems from Ideals of Orders in CDAs

We now define the computationally-hard lattice problems needed for our security reductions.

In our ensuing definitions, $\mathcal{O}$ denotes a maximal order, and $L_{\mathbb{R}} = L \otimes_{\mathbb{Q}} \mathbb{R}$.

Definition 35. Let $\mathcal{A}$ be a CDA, $\mathcal{I} \subset \mathcal{O}$ be an ideal, and $\xi \geq 1$. The approximate Shortest Independent Vectors Problem, SIVP_ξ is to find n linearly independent non-zero vectors $x_1, \dots, x_n$ such that $\max_i (\|x_i\|) \leq \xi \cdot \lambda_n(\mathcal{I})$.

Let $\|e\|_{2,\infty} := \max_j \sqrt{\left(\sum_{i=0}^{d-1} |\sigma_j(e_i)|^2\right)}$, for $e \in \mathcal{A} \otimes_{\mathbb{Q}} \mathbb{R}$.

Definition 36. Let $\mathcal{A}$ be a CDA, $\mathcal{I}$ an ideal of $\mathcal{O}$, and $0 < \delta < \lambda_1(\mathcal{I})/2$. The $\mathcal{A}$ -BDD $_{\mathcal{O},\mathcal{I},\delta}$ problem, given $y = x + e$ for $x \in \mathcal{I}$ and $e \in \bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$ satisfying $\|e\|_{2,\infty} \leq \delta$, is to find x .

Definition 37. For any $q \geq 2$, the $q\mathcal{A}$ -BDD $_{\mathcal{O},\mathcal{I},d}$ problem is, given a $\mathcal{A}$ -BDD $_{\mathcal{O},\mathcal{I},\delta}$ instance $y = x + e$ with solution $x \in \mathcal{I}$ and error $e \in \bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$ satisfying $\|e\|_{2,\infty} \leq \delta$, output $x \bmod q\mathcal{I}$.

Lemma 2.16. For any $q \geq 2$ and order ideal $\mathcal{I}$, there is a deterministic polynomial time reduction from $\mathcal{A}$ -BDD $_{\mathcal{O},\mathcal{I},\delta}$ to $q\mathcal{A}$ -BDD $_{\mathcal{O},\mathcal{I},\delta}$.

Proof. Adapted from [136, Lemma 3.5], which lifts since it is lattice preserving. $\square$

Definition 38. We denote by $\mathcal{A}$ -DGS $_{\xi}$ the problem of sampling a discrete Gaussian $D_{\mathcal{I},\xi}$, $\xi > 0$, where $\mathcal{I}$ is some ideal of $\mathcal{O}$.

We note that $\mathcal{A}$ -SIVP reduces to $\mathcal{A}$ -DGS (see [71]).

The CLWE Problem, and Reductions

In [71], LWE was instantiated using the natural order inside a CDA. We first define the following distribution, where ψ is an arbitrary error distribution:

Definition 39 (The CLWE Distribution). Let L/K be a Galois extension of number fields of dimension $[L : K] = d$, $[K : \mathbb{Q}] = n$ with cyclic Galois group generated by θ . Let $\mathcal{A} := (L/K, \theta, \gamma)$ be a cyclic division algebra with element u such that $u^d = \gamma \in \mathcal{O}_K$. Let Λ be the natural order of $\mathcal{A}$. For an error distribution ψ over $\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$, modulus $q \geq 2$, and a secret $s \in \Lambda_q^{\vee}$, a sample from the CLWE distribution $\Pi_{q,s,\psi}$ is obtained by sampling $a \leftarrow \Lambda_q$ uniformly at random, $e \leftarrow \psi$, and outputting $(a, b) = (a, (a \cdot s)/q + e \bmod \Lambda^{\vee}) \in \Lambda_q \times (\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}) / \Lambda^{\vee}$.

The public element a has a matrix representation $\phi(a)$, and to construct this matrix only the first column need be stored by a user. Let Ψ be a family of error distributions. From the above, search and decision problems can be defined:

Definition 40. Let $\Pi_{q,s,\psi}$ be a CLWE distribution for parameters $q \geq 2, s \in \Lambda_q^{\vee}$, and error distribution $\psi \in \Psi$. The search CLWE problem, denoted $\text{CLWE}_{q,s,\psi}$, is to recover s from a collection of independent samples from $\Pi_{q,s,\psi}$.

Definition 41. Let Υ be a distribution on a family of error distributions over $\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$ and U_{Λ} the uniform distribution on $(\Lambda_q, (\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}) / \Lambda^{\vee})$. The decision CLWE problem, $DCLWE_{q,\Upsilon}$, is given a collection of independent samples from either $\Pi_{q,s,\psi}$ for a random choice of $(s, \psi) \leftarrow U(\Lambda_q^{\vee}) \times \Upsilon$, or from U_{Λ} , to decide which is the case with non-negligible advantage.

Using the following family of error distributions

Definition 42. Let Σ_{α} be the set of Gaussian distributions Σ over $\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$ with Gaussian marginal distributions of parameter $r_{i,j} \leq \alpha$ in the i, j th entry.

a reduction from DGS on ideal lattices to the search CLWE problem was obtained, over CDAs constructed as in Section 2.7.3:

Theorem 2.8. [71, Theorem 6] Let $\mathcal{A}$ be a CDA over a number field L with center K and natural, maximal order Λ with $|\gamma| = 1$. Let $\alpha = \alpha(n) \in (0, 1)$ and $q = q(n) \geq 2$, unramified in L , be parameters such that $\alpha \cdot q \geq \omega(\sqrt{\log nd^2})$. Then, there is a polynomial-time quantum reduction from $\mathcal{A}$ -DGS $_{\xi}$ to search $CLWE_{q,s,\Sigma_{\alpha}}$ for any $\xi = r \cdot \sqrt{d}\omega(\sqrt{\log(d \cdot n)})/\alpha q$, where $r > \sqrt{2}q \cdot \eta_{\varepsilon}(\mathcal{I})$.

This reduction relied upon a ‘clearing ideals’ lemma (see Lemma 4.4 below) and follows the structure of the RLWE reduction closely.

However, the search-to-decision reduction has a technical difference to the RLWE equivalent. The reduction for RLWE relied on the CRT for products of prime ideals of $\mathcal{O}_K$, whereas the CLWE reduction relied on the CRT-*style* decomposition of the quotient of Λ of Theorem 2.6. This gives an isomorphism from $\Lambda/q\Lambda$ to $\prod_{i=1}^g ((\mathcal{O}_L/\mathfrak{q}_i \mathcal{O}_L)/(\mathcal{O}_K/\mathfrak{q}_i), \theta, \gamma)$, where $q\mathcal{O}_K = \prod_{i=1}^g \mathfrak{q}_i$, which for primes unramified in $\mathcal{O}_L$ is a direct product of (generalised) cyclic algebras over $\mathcal{O}_K/\mathfrak{q}_i$, a finite field. The factor of the right hand side induced by $\mathfrak{q}_i$ was labelled R_i . However these algebras are not division algebras, but rather each R_i is isomorphic to a matrix ring over a finite field, rather than simply a finite field (which is what is obtained for the corresponding step for RLWE). Let us work through the consequences.

We define a hybrid distribution $A_{s,\Sigma}^i$ over $\Lambda_q \times (\bigoplus_i u^i L_{\mathbb{R}}) / \Lambda^{\vee}$ by sampling $(a, b) \leftarrow \Pi_{q,s,\Sigma}$ and

outputting $(a, b + h/q)$, where $h \in \Lambda_q^\vee$ is uniformly random and independent modulo R_j for all $j \leq i$, and 0 modulo the remaining R_j . Then worst-case decision CLWE modulo R_i , $\text{WDCLWE}_{q,\Sigma}^i$, is, given access to $A_{s,\Sigma}^j$ for arbitrary $s \in \Lambda_q^\vee$, $\Sigma \in \Sigma_\alpha$, and $j \in \{i-, i\}$, to find j , for $i \in \mathbb{Z}_g$.

To effect the reduction, given an CLWE sample (a, b) , one guesses s with g and computes

$$(a', b') = (a + v, b + (h + vg)/q) \in \Lambda_q \times (\oplus_i u^i L_{\mathbb{R}})/\Lambda^\vee,$$

where $v \in \Lambda_q$ is uniformly random mod R_i and 0 mod R_j for $j \neq i$, and $h \in \Lambda_q^\vee$ is uniformly random and independent mod R_j for all $j < i$, and 0 mod the remaining R_j . Observe

$$b' = b + (h + vg)/q = as/q + e + h/q + vg/q = ((a + v)s + h + v(g - s))/q + e.$$

If the guess $g = s$, this is $A_{s,\Sigma}^{i-1}$. However, if $g \neq s$, we do not find that the resulting distribution is $A_{s,\Sigma}^i$ unless $g - s$ is invertible modulo R_i , that is, invertible in some matrix ring over a finite field. To ensure that this is the case, [71] artificially restricted the secret space for this step of the reduction to a ‘pairwise difference set’ $G \subset \Lambda_q$, which under the CRT-style map is a direct product of sets $G_i \subset R_i$, characterised by the property that the difference of any two elements of G_i inverts. Such a set is of size at most $|G_i| \leq q^d$, when $[L : K] = d$, rather than the full secret space of q^{d^2} . As a consequence, there is currently no unrestricted reduction from computationally hard lattice problems to the decision variant of CLWE.

Several subsequent steps, very similar to the RLWE/MLWE equivalents, established a worst-case to average-case reduction for decision CLWE. The statement of the obtained result is

Theorem 2.9. [71, Theorem 7] *Let Λ be the natural order of a cyclic algebra $\mathcal{A} = (L/K, \theta, \gamma)$, $q = \text{poly}(n)$ and $\alpha q \geq \eta_\varepsilon(\Lambda^\vee)$ for a negligible $\varepsilon = \varepsilon(n)$. Then, there is a probabilistic polynomial time reduction from $\text{CLWE}_{q,\Sigma_\alpha,G}$ for any pairwise different $G \subset \Lambda_q^\vee$ to $\text{DCLWE}_{q,\mathbf{r}_\alpha}$.*

From these CLWE problems, a public key encryption scheme (PKE) was given. We take this moment to fix the syntax of encryption schemes. A *PKE scheme* $\mathcal{E}$ is a tuple of algorithms $\mathcal{E} = (\text{Gen}, \text{Enc}, \text{Dec})$ such that on input a security parameter λ , Gen outputs a key pair (pk, sk) ,

Enc takes as inputs pk and a message m and outputs a ciphertext c , and Dec takes as inputs sk and c and outputs either a message m' or $\perp$, which denotes a decryption failure; and, finally, the latter two algorithms must satisfy for every key pair (pk, sk) and all messages m

$$\text{Dec}_{sk}(\text{Enc}_{pk}(m)) = m.$$

This latter condition may be relaxed to hold only with overwhelming probability; that is, we allow the possibility of decryption failures.

We say a scheme is IND-CPA secure if any probabilistic polynomial time (ppt.) adversary has only negligible advantage in the PubK experiment:

Definition 43. ([91]) Let $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ be a PKE scheme, and $\mathcal{A}$ be an adversary. Say Π is indistinguishable under chosen-plaintext attack if a ppt. adversary in the following experiment $\text{PubK}_{\mathcal{A}, \Pi}(n)$ has negligible advantage:

1. Gen is run to obtain keys (pk, sk) .
2. Adversary $\mathcal{A}$ is given pk , and outputs a pair of equal-length messages m_0, m_1 .
3. A uniform bit $b \in \{0, 1\}$ is chosen, and then a challenge ciphertext $c \leftarrow \text{Enc}_{pk}(m_b)$ is computed and given to $\mathcal{A}$.
4. $\mathcal{A}$ outputs a bit b' . The output of the experiment is 1 if $b' = b$, and 0 otherwise. If $b' = b$ we say that $\mathcal{A}$ succeeds.

That is, $\Pr[\text{PubK}_{\mathcal{A}, \Pi}(n) = 1] \leq \frac{1}{2} + \text{neg}(n)$.

The CLWE scheme has the following form, where letters in bold denote the vector of coefficients of the corresponding algebra element, for any $d \geq 2$ such that $\gcd(n, d) > 1$:

Setup The setup algorithm $\text{Setup}(1^n)$ takes in a security parameter n and outputs a tuple of parameters $\text{params}(n) = ((K = \mathbb{Q}(\zeta_n), L, \ell(n), \theta(n), q(n), \alpha(n)))$, where $\ell(n)$ satisfies $\ell(n) \equiv 1 \pmod{n}$ and $\ell(n) \not\equiv 1 \pmod{pn}$ for any $p \mid n$, L is a degree d extension of K contained in $M = \mathbb{Q}(\zeta_{n\ell(n)})$, $\theta(n)$ generates L/K , $q(n)$ completely splits in L , and $\alpha(n)$ parameterises the

error distribution.

Key Generation The key generation algorithm $\text{Gen}(1^n)$ creates a CDA $\mathcal{A}$ with $\gamma = \zeta_n$ from the output of $\text{Setup}(1^n)$, samples $a \leftarrow U(\Lambda_q)$, $s \leftarrow U(\Lambda_q^\vee)$, and $e \leftarrow \psi$, and creates the public key $pk := (a, as + e)$ according to the CLWE distribution $\Pi_{q,s,\psi}$. The secret key is $sk := s$.

Encryption To encrypt a message $\mathbf{m} \in \{0, 1\}^{nd^2}$, elements $t, e_1, e_2 \leftarrow \psi$ are sampled, and $\text{Enc}_{pk}(m) = c = (c_0, c_1) := (\phi(a)^T \mathbf{t} + \mathbf{e}_1, \phi(b)^T \mathbf{t} + \mathbf{e}_2 + \lceil \frac{q}{2} \rceil \mathbf{m})$ is outputted.

Decryption To decrypt a ciphertext c , $\text{Dec}_{sk}(c) = \lfloor c_1 - \phi(s)^T c_0 \rfloor$.

Correctness of the above scheme holds if $\|\phi(e)^T \mathbf{t} + \mathbf{e}_2 - \phi(s)^T \mathbf{e}_1\|_\infty < \frac{q}{4}$. The scheme is IND-CPA secure under the decision CLWE assumption.

2.10 NTRU

We now turn to the second cryptographic lattice-based problem considered in this thesis, NTRU.

We begin by defining the problem underlying schemes based on NTRU.

The NTRU Assumption

Definition 44. (*NTRU instances*) Let $\mathcal{R}$ be a ring and $q \in \mathbb{Z}_{\geq 2}$ a modulus. An NTRU instance is an element $h \in \mathcal{R}_q$ such that $h \cdot f = g \bmod q\mathcal{R}$ for some pair of non-zero elements $(f, g) \in \mathcal{R}$.

We are interested in the following problem, based off NTRU instances:

Definition 45. (*The NTRU problem*) Let $\mathcal{R}$ and q be as above, and $\epsilon > 0$. Let $\mathcal{D}$ be a distribution over instances of NTRU. The NTRU problem is, given $h \leftarrow \mathcal{D}$, to find non-zero (f, g) such that $h \cdot f = g \bmod q\mathcal{R}$ and $\|f\|, \|g\| \leq \frac{\sqrt{q}}{\epsilon}$.

The hardness of the NTRU problem varies significantly, depending on ϵ . NTRU-based schemes provide one of the most efficient post-quantum cryptographic frameworks. While attacks such as lattice reduction can be used, known attacks are ineffective against NTRU with well-chosen

parameters. This absence of decisive attacks against well-chosen parameters over a long period of time has led NTRU to have a prominent place in the geography of post-quantum cryptography. This is illustrated by two NTRU-based schemes reaching the third round of NIST's post-quantum standardization effort [3], [41]. Moreover, partial security reductions for NTRU have been given in [128], [63], lending further weight to NTRU as a platform for cryptography. The NTRU problem can be formulated as follows: if f and g are 'short' ring elements, and $h := g \cdot f^{-1}$, find (f, g) from $h \bmod q$, for some modulus $q \in \mathbb{Z}$. Typical choices of rings are polynomial rings of the form $\mathbb{Z}[x]/(x^p - 1)$, $\mathbb{Z}[x]/(x^{2^k} + 1)$, and $\mathbb{Z}[x]/(x^p - x - 1)$ [77], [3], [25]. These enjoy fast algorithms for multiplication and low storage requirements. Moreover, a simple public-key encryption scheme can be based on the hardness of the NTRU problem. The history of cryptanalysis of NTRU is lengthy, beginning with lattice reduction attacks [55] and including meet-in-the-middle attacks [82], hybrid attacks [80], attacks based on decryption failures [81], and subfield attacks [7]. These often exploit particular design choices of specific NTRU schemes (such as a choice of ternary secrets, or an 'overstretched' choice of modulus, or the use of rings with many subrings), and hence these weak(er) instances or parameters can be avoided by careful design. As a result, after 25 years of cryptanalysis, the NTRU assumption remains a trusted basis for cryptography.

Connection to Lattices

The solutions over $\mathcal{R}$ to the defining equation $hf \equiv g \bmod q$ form a lattice, denoted

$$\mathcal{L}_{h,q} = \{(x, y) \in \mathcal{R}^2 : hx - y \equiv 0 \bmod q\}.$$

The sum of two solutions to the defining equation is again a solution, and one can also observe that for any $z \in \mathcal{R}$ and $(f, g) \in \mathcal{L}_{h,q}$, (z, zf, zg) satisfies $zhf - zg \equiv z(hf - g) \equiv 0 \bmod q$. Thus $\mathcal{L}_{h,q}$ is a $\mathcal{R}$ -module of rank 2, and the NTRU problem can be rephrased as a shortest vector problem in the NTRU lattice $\mathcal{L}_{h,q}$.

Encryption Scheme

The NTRU encryption scheme, as in [77], runs as follows:

KeyGen: Let $\mathcal{L}_f$, $\mathcal{L}_g$, $\mathcal{L}_\phi$, and $\mathcal{L}_m$ be sets of polynomials in $\mathcal{R} = \mathbb{Z}[x]/(r(x))$ for some degree- N polynomial r . Let $q \gg p \in \mathbb{Z}$ be coprime. Select f from $\mathcal{L}_f$ and g from $\mathcal{L}_g$, such that f inverts modulo both q and p . Compute $h = g \cdot f^{-1} \bmod q$; this polynomial h is the public key, and (f, g) is the private key.

Encryption: Suppose the message is m , taken from $\mathcal{L}_m$. Then to encrypt m , select ϕ from $\mathcal{L}_\phi$ and compute $c = p\phi \cdot h + m \bmod q$. This is the ciphertext.

Decryption: To decrypt c , first compute $a = f \cdot c \bmod q$. Then compute $f^{-1} \cdot a \bmod p$, to recover $m \bmod p$. This decryption holds provided the coefficients of a lie in the correct interval. Otherwise, there is a small chance of *decryption failure*. Parameters can be chosen to eliminate the chance of decryption failure.

Correctness: Observe that

$$a = f \cdot c \bmod q = f \cdot (p\phi \cdot h + m) \bmod q = p\phi \cdot g + f \cdot m \bmod q,$$

so that finally $f^{-1} \cdot a \bmod p = f^{-1} \cdot (p\phi g + f \cdot m) \bmod p = f^{-1} \cdot (fm) \bmod p = m \bmod p$, provided that when we reduce a modulo q (taking the coefficients between $-\frac{q}{2}$ and $\frac{q}{2}$), we obtain simply the polynomial a .

Making NTRU Provably Secure

The above encryption scheme can be implemented efficiently, and is considered secure for well-chosen parameters. However, its security depends on the hardness of the NTRU assumption, rather than well-studied worst-case computational problems. An attempt to remedy this situation was proposed in [154], in which the authors tweaked the scheme to allow them to prove IND-CPA security, assuming the hardness of a variant of RLWE.

The authors achieved this as follows. By amending the key generation algorithm to have both

f and g be invertible modulo q , with $f \equiv 1 \pmod{p}$, and the encryption algorithm to encrypt m be setting $c = hs + pe + m$, it can be proven that an attack breaking the IND-CPA security of this tweaked NTRU scheme implies an attack on an RLWE variant taking samples $(a, as + e) \in R_q^\times \times R_q$, where s, e are sampled from the same distribution.

This line of work was continued by [156], which included analysis of a provably secure NTRU-based digital signature scheme, and [174], [169], which extended the results of [154] to any cyclotomic field, not just cyclotomic fields with power-of-two conductor, as was originally shown. Analysis of the practicality of these provably-secure NTRU schemes was conducted in [42].

Further Discussion of NTRU

There are a variety of parameter choices currently used to instantiate NTRU. In the paper initially proposing the NTRU problem [77], the ring $\mathcal{R} = \mathbb{Z}[x]/(x^N - 1)$ was used, with N prime (and the authors recommended using Sophie Germain primes). Of the two final round NTRU-based schemes in NIST's post-quantum standardization process, NTRU [41] samples f and g from $\mathbb{Z}[x]/(r(x))$ with $r(x) = \Phi_n(x)$, where n is prime and $\Phi_n(x)$ is the n th cyclotomic polynomial. This is contrasted by NTRU Prime [25], which uses $r(x) = x^p - x - 1$ for some prime p (not to be confused with the modulus of the previous section), such that $\mathbb{Z}_q[x]/(x^p - x - 1)$ is a field.

We also note here that f and g are often chosen to be binary or ternary polynomials (i.e. coefficients are in $\{0, 1\}$, $\{-1, 0, 1\}$ respectively), which increases efficiency, but which has been subjected to meet-in-the-middle attacks [80].

We also note the many algebraic variants of NTRU proposed over the years: in CTRU [122], the usual polynomials were replaced with elements from the ring $\mathbb{F}_2[T][X]/(X^n - 1)$; this was later subjected to a polynomial-time attack in [94], which also introduced NTRU over the Gaussian Integers. This idea was expanded by [114] and [161], which introduced NTRU over the Eisenstein integers (ETRU) and the ring of integers of $\mathbb{Q}(\sqrt{-7})$ (KTRU) respectively. More details on ETRU can be found in [113] and [88]. A version of NTRU using ideal lattices can be found in [90], an attempt to secure CTRU can be found in [134], and an attempt to further secure ETRU can be found in [133].

There have also been more exotic attempts to improve NTRU: some of these include non-commutative variants such as [163], [104], [165], [16]; NTRU over group rings in [173]; non-associative schemes in [103] and [162]; and a variant with different invertibility conditions in [19]. A useful comparison of some of these schemes can be found in [148]. An overview of NTRU can be found in [157].

Chapter 3

Clarifying the Security of CLWE

3.1 Introduction

While some cryptanalysis of CLWE was performed (notably a proof that a dimension-reducing attack which applied to another form of structured RLWE [32] cannot be conducted on CLWE) more precise understanding of the security of CLWE has been lacking. In this chapter we take some steps towards clarifying CLWE's security. In particular, we begin by showing that the reduction from lattice problems defined on ideal lattices of maximal natural orders of CDAs only supplies a guarantee from lattice problems on ideal lattices of maximal orders of *number fields*. To do this we extend a result of Oggier and Sethuraman [119] on the ideal structure of such orders in CDAs. This result can also be used to obtain a noncommutative Gentry-Szydlo algorithm in certain CDAs. We then take three steps towards reasserting the hardness of CLWE: firstly, we show that a search CLWE oracle is sufficient to solve the shortest independent vectors problem on certain module lattices; and secondly, we define a module version of CLWE, dubbed CMLWE, and show that for some change in the size of the modulus q , CLWE is at least as hard as CMLWE. This result is in the same vein as that in [8]. And thirdly, we reduce lattice problems on one-sided ideal lattices to CLWE.

In more detail, we consider ideals in natural orders of CDAs of the following form: $\mathcal{A} =$

$(L/K, \theta, \zeta_n)$ with $K = \mathbb{Q}(\zeta_n)$ and L a finite cyclic Galois extension such that $\zeta_n \notin N_{L/K}(L^\times)$.¹ The most complete prior result on the structure of ideals in such orders is the following:

Structure of Unramified Primes. [119, Proposition 4] *Suppose that $\mathfrak{p}$ is a prime in $\mathcal{O}_K$, such that $\mathfrak{p}$ is unramified in L , with $\gamma \not\equiv 0 \pmod{\mathfrak{p}}$. Then the only proper two-sided ideal $\mathcal{I}$ of Λ containing $\mathfrak{p}$ is $\mathfrak{p}\Lambda = \bigoplus_{i=0}^{d-1} u^i \mathfrak{p}\mathcal{O}_L$.*

This characterises the behaviour of prime $\mathcal{O}_K$ -ideals unramified in $\mathcal{O}_L$ lifted to Λ . Our first result is a broad extension of this result. We show that

Ideal Structure Theorem (Theorem 3.1). *Let $\Lambda \subset \mathcal{A} = (L/K, \theta, \gamma)$ denote the natural order. Let $\mathcal{I} \subset \Lambda$ be an integral ideal, and $\overline{\mathcal{I}} = \mathcal{I} \cap K$. Suppose the prime factors of $\overline{\mathcal{I}}$ are unramified in L and $\gamma \not\equiv 0 \pmod{\overline{\mathcal{I}}}$. Then $\mathcal{I} = \overline{\mathcal{I}}\Lambda$.*

In an abuse of language, we will call ideals satisfying the condition of the theorem *unramified*.

This result shows that *all* unramified ideals of Λ have the same structure as in the prime case.

We achieve this result via double induction, one of which is a transfinite induction.

We then detail the consequences of this result. We begin by reducing SIVP in a Λ -ideal to SIVP in an $\mathcal{O}_L$ -ideal. This follows from the canonical embedding of $\mathcal{A}$ into $\mathbb{R}^{nd^2}$ being ‘orthogonal’, Λ containing many roots of unity, and the above ideal structure theorem.

Reduction between SIVP problems (Proposition 3.1). *Let $\mathcal{A} = (L/K, \theta, \zeta_n)$ be a CDA with $K = \mathbb{Q}(\zeta_n)$. Let $\Lambda \subset \mathcal{A}$ be the natural order, and $\mathcal{I} \subset \Lambda$ an unramified ideal. Set $\overline{\mathcal{I}} := \mathcal{I} \cap K$. Then a solution to SIVP in $\overline{\mathcal{I}}\mathcal{O}_L$ yields a solution to SIVP in $\mathcal{I}$. When $d = 2$ and n is a power of 2, a solution to SVP in $\overline{\mathcal{I}}\mathcal{O}_L$ yields a solution to SIVP in $\mathcal{I}$.*

The second consequence is a Gentry-Szydlo algorithm for the Lattice Isomorphism Problem (LIP) for unramified ideals in Λ . When L is a finite totally real extension of a cyclotomic field, $\mathcal{O}_L$ is a CM order (definitions below) and the Gentry-Szydlo algorithm holds in that setting [100]. Using the above-mentioned orthogonality of the embedding of $\mathcal{A}$ and the structure theorem, we show it suffices to solve the LIP for $\mathcal{O}_L$ -ideals in order to solve it for Λ -ideals:

¹We will see later on that the results of the current chapter apply for arbitrary values of n , not just for the prime-power case described above.

Gentry-Szydlo for Natural Orders (Theorem 3.4). *Let $K = \mathbb{Q}(\zeta_n)$, L/K a finite cyclic Galois totally real extension of K , $\mathcal{A} = (L/K, \theta, \gamma)$ a CDA with $\gamma \in \mathcal{O}_K^\times$ and $|\gamma| = 1$, and $\mathcal{I}, \mathcal{J} \subset \Lambda \subset \mathcal{A}$ ideals in the natural order of $\mathcal{A}$. Then there is a deterministic polynomial-time algorithm that decides whether or not $\mathcal{I}, \mathcal{J}$ are isomorphic as Λ -lattices, and if so exhibits such a Λ -isomorphism.*

The ideal structure theorem leaves the precise hardness of CLWE in doubt, since the proof given in [71] to establish its hardness in fact relies on the difficulty of SIVP in some finite extension of a cyclotomic field. However, CLWE is *at least* as hard as this problem. In seeking to clarify the hardness of CLWE, we obtain three results; the first is:

q Mod-BDD reduces to Search CLWE (Theorem 3.5). *Let $\varepsilon(N) = N^{-\omega(1)}$, $\alpha \in (0, 1)$ and $q \geq 2$. Let $\mathcal{M} \subseteq L^2$ be an integral $\mathcal{O}_L$ -module, and $r > \max(\sqrt{2}q \cdot \eta_\varepsilon(\mathcal{M}), q \cdot \eta_\varepsilon(\Lambda))$. Given access to an oracle sampling from the distribution $D_{\mathcal{M}, r}$, there exists a probabilistic reduction from q -Mod-BDD $_{\alpha q \omega(\sqrt{\log nd})/\sqrt{2nd}r}$ to search $\text{CLWE}_{q, s, \Psi_{\leq \alpha}}$ with $d = 2$.*

Composing this with known reductions [97] from module SIVP to q Mod-BDD, we obtain a reduction from module SIVP to search CLWE.

Our second contribution to the study of the hardness of CLWE is a reduction from a module variant of CLWE to CLWE, involving a change of parameters. We define CMLWE, ‘cyclic module learning with errors’, as follows: for an error distribution ψ over $\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$, an integer modulus $q \geq 2$, and a secret $s \in (\Lambda_q^\vee)^m$, a sample from the CMLWE distribution $\Pi_{q, s, m, \psi}$ is obtained by sampling $a \leftarrow \Lambda_q^m$ uniformly at random, $e \leftarrow \psi$, and outputting $(a, b) = (a, \langle a, s \rangle / q + e \bmod \Lambda^\vee) \in \Lambda_q^m \times (\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}) / \Lambda^\vee$.

We prove the hardness of the search problem from this distribution, assuming the hardness of an underlying module lattice problem, in the standard way. This enables us to give a proof of the following result, in the style of [8]:

CMLWE reduces to CLWE (Corollary 3.2). *Let $\Lambda \subset \mathcal{A} = (L/K, \theta, \gamma)$ be the natural order of a CDA with $[L : K] = d$, and let Λ have basis $\mathbf{B}$ in the canonical embedding. Let $\alpha > 0$. Let*

χ be a distribution satisfying

$$\Pr_{s \leftarrow \chi} \left[\max_{i,j} |\sigma_i(s_j)| > B \right] \leq \delta$$

for some B and δ . Then for any $\epsilon \in (0, 1/2)$, any $k \geq 2$ dividing m , and

$$r \geq \frac{1}{q} \left\| \tilde{\mathbf{B}} \right\| \cdot \sqrt{2 \ln(2mnd^2(1 + 1/\epsilon))/\pi},$$

there is an efficient reduction from $\Pi_{q,s,m,\Psi_{\leq \alpha}}$ with $s \leftarrow \chi^m$ to $\Pi_{q,s,m/k,\Sigma_R}$ with $s \leftarrow G \cdot \chi^m$ where $G = \mathbf{I}_{m/k} \otimes (1, q, \dots, q^{k-1}) \in \Lambda^{m/k \times m}$ and $R^2 = (d+1)mr^2B^2 + \alpha^2$ which reduces the advantage by at most $[1 - (1 - \delta)^{dm}] + (4m + 10)\epsilon d$.

The final result of the chapter is a reduction from SIVP on left ideals of Λ to search CLWE. Since number fields are commutative, any one-sided ideal of $\mathcal{O}_K$ is also a two-sided ideal. This situation differs completely from Λ , in which any non-central element may generate a left ideal which is not a right ideal. Our reduction is

Left Ideal SIVP reduces to CLWE (Theorem 3.9). *Let $K = \mathbb{Q}(\zeta_n)$, Λ be the natural order of $\mathcal{A} = (L/K, \theta, \zeta_n)$, and $\alpha \in (0, 1)$ and $q \geq 2$ such that $\alpha q \geq \omega(1)$. Then there is a polynomial-time quantum reduction from $\mathcal{A}\text{-SIVP}_{\xi}^{\text{Left}}$ to search-CLWE $_{q,\Sigma_{\alpha}}$ for any $\sqrt{8Nd} \cdot \xi = (\omega(\sqrt{dn})/\alpha)$.*

3.2 Reducing CDA Ideal-SVP to Number Field Ideal-SVP

In this section we extend a result on ideals in the natural order of certain CDAs, and use this result to reduce ideal SVP in those CDAs to ideal SVP in number fields. In [119], the authors proved

Lemma 3.1. *[119, Proposition 4] Suppose that $\mathfrak{p}$ is a prime in $\mathcal{O}_K$ such that $\mathfrak{p}$ is unramified in L , with $\gamma \not\equiv 0 \pmod{\mathfrak{p}}$. Then the only proper two-sided ideal $\mathcal{I}$ of Λ containing $\mathfrak{p}$ is $\mathfrak{p}\Lambda = \bigoplus_{i=0}^{d-1} u^i \mathfrak{p}\mathcal{O}_L$.*

One can observe that the lemma implies that if $\mathcal{I} \subset \Lambda$ is an ideal such that $\bar{\mathcal{I}} := \mathcal{I} \cap K$ is a prime ideal which is unramified in L and doesn't contain γ , then in fact $\mathcal{I} = \bar{\mathcal{I}}\Lambda$. We extend the above lemma from this perspective to obtain

Theorem 3.1. *Let $\Lambda \subset \mathcal{A} = (L/K, \theta, \gamma)$ denote the natural order. Let $\mathcal{I} \subset \Lambda$ be an integral ideal, and $\bar{\mathcal{I}} = \mathcal{I} \cap K$. Suppose the prime factors of $\bar{\mathcal{I}}$ are unramified in L and $\gamma \not\equiv 0 \pmod{\bar{\mathcal{I}}}$. Then $\mathcal{I} = \bar{\mathcal{I}}\Lambda$.*

Note that in the typical case of constructions of CDAs $\mathcal{A}$ over cyclotomic fields $K = \mathbb{Q}(\zeta_n)$ (as in Section 2.7.3), in which $K \subset L \subset \mathbb{Q}(\zeta_{\ell n})$ for some prime $\ell \equiv 1 \pmod{n}$, the only ideals of $\mathcal{O}_K$ ramified in $\mathcal{O}_L$ are those lying above ℓ ; in particular, there are at most $[L : \mathbb{Q}]$ of these.

We require a corollary of Lemma 3.1:

Corollary 3.1. *Suppose that $\mathfrak{p}$ is a prime in $\mathcal{O}_K$, such that $\mathfrak{p}$ is unramified in L , with $\gamma \not\equiv 0 \pmod{\mathfrak{p}}$. Then the only proper two-sided ideal $\mathcal{I}$ of Λ containing $\mathfrak{p}^{-1}$ is $\mathfrak{p}^{-1}\Lambda = \bigoplus_{i=0}^{d-1} u^i \mathfrak{p}^{-1} \mathcal{O}_L$.*

Proof. Suppose there were a proper ideal strictly containing $\mathfrak{p}^{-1}\Lambda$, say $\mathcal{J}$. But then $\mathfrak{p}^2\mathcal{J}$ is a proper two-sided ideal strictly containing $\mathfrak{p}\Lambda$, which contradicts Lemma 3.1. $\square$

We now prove the theorem.

Proof. Suppose that $\mathcal{I}$ maximally contains a subideal $\mathfrak{J}$ which is unramified in L , that is, $\mathfrak{J}$ is the largest $\mathcal{O}_K$ -ideal contained in $\mathcal{I}$. Suppose $\mathfrak{J} = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \dots \mathfrak{p}_n^{e_n}$, for distinct primes $\mathfrak{p}_i$, and positive integers e_i . We claim that when the largest $\mathcal{O}_K$ -ideal of $\mathcal{I}$ has this form, then $\mathcal{I} = \mathfrak{J}\Lambda$. We want to show that $\mathcal{I} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_n^{e_n} \Lambda$. First, note that $\mathcal{I}$ is contained in a maximal ideal $\mathcal{M}$, which contains some prime ideal $\mathfrak{r}$ of $\mathcal{O}_K$, and so we have $\mathcal{M} = \mathfrak{r}\Lambda$, and $\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_n^{e_n} \Lambda \subset \mathcal{I} \subsetneq \mathfrak{r}\Lambda$. But $\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_n^{e_n} \subset \mathfrak{r}$ implies that $\mathfrak{r} = \mathfrak{p}_i$ for some i ; without loss of generality suppose $\mathfrak{r} = \mathfrak{p}_1$, and we can write $\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_n^{e_n} \Lambda \subset \mathcal{I} \subsetneq \mathfrak{p}_1 \Lambda$.

Proceed by double induction on $n \in \mathbb{N}_{\geq 1}$ and $(e_1, \dots, e_n) \in \mathbb{Z}_{\geq 1} \times \dots \times \mathbb{Z}_{\geq 1}$. We use transfinite induction over the $(e_1, \dots, e_n)$, which requires a well-ordering on $\mathbb{Z}_{\geq 1}^n$. We use the following well-ordering: let $(e_1, \dots, e_n) \in \mathbb{Z}_{\geq 1}^n$. Given n -tuples $(e_1, \dots, e_n), (f_1, \dots, f_n)$, we say $(e_1, \dots, e_n) > (f_1, \dots, f_n) \in \mathbb{Z}_{\geq 1}^n$ if $\prod_1^n p_i^{e_i} > \prod_1^n p_i^{f_i}$, where p_i is the i th prime. Note that (for fixed n) the

smallest element is $(1, \dots, 1)$. This is a total order, and any subset of n -tuples must have a smallest element, so this is a well-ordering of $\mathbb{Z}_{\geq 1}^n$.

We know that the statement is true in the case $n = 1, e_1 = 1$ by Lemma 3.1. We first prove the statement for $n = 1$, and use induction on e_1 . Suppose the statement holds for $e'_1 < e_1$ and suppose $\mathcal{I}$ contains $\mathfrak{p}_1^{e_1}$ and no larger $\mathcal{O}_K$ -ideal. Then we have $\mathfrak{p}_1^{e_1}\Lambda \subset \mathcal{I} \subsetneq \mathfrak{p}_1\Lambda$. Then $\mathfrak{p}_1^{-1}\mathcal{I}$ is integral, and the largest $\mathcal{O}_K$ -ideal it contains is $\mathfrak{p}_1^{e_1-1}$, so $\mathfrak{p}_1^{-1}\mathcal{I} = \mathfrak{p}_1^{e_1-1}\Lambda$ by hypothesis. Hence $\mathcal{I} = \mathfrak{p}_1^{e_1}\Lambda$, as required.

Next, we show the statement for $(1, \dots, 1)$ and any n by inducting on n . Suppose $\mathfrak{J} = \mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_n$, for distinct primes $\mathfrak{p}_i$. Note that $\mathcal{I}$ is contained in a maximal ideal $\mathcal{M}$, which contains some prime ideal $\mathfrak{r}$ of $\mathcal{O}_K$, and so we have $\mathcal{M} = \mathfrak{r}\Lambda$, and $\mathfrak{p}_1\dots\mathfrak{p}_n\Lambda \subset \mathcal{I} \subsetneq \mathfrak{r}\Lambda$. But $\mathfrak{p}_1\dots\mathfrak{p}_n \subset \mathfrak{r}$ implies that $\mathfrak{r} = \mathfrak{p}_i$ for some i ; without loss of generality suppose $\mathfrak{r} = \mathfrak{p}_1$, and write $\mathfrak{p}_1\dots\mathfrak{p}_n\Lambda \subset \mathcal{I} \subsetneq \mathfrak{p}_1\Lambda$. We now claim that if $\mathfrak{p}_1\dots\mathfrak{p}_n$ is the largest $\mathcal{O}_K$ -ideal in $\mathcal{I}$, then $\mathcal{I} = \mathfrak{p}_1\dots\mathfrak{p}_n\Lambda$.

We have seen that the $n = 1$ case is true. Proceeding by induction, suppose the statement is true for $n < k$, and consider an integral ideal $\mathcal{I}$ such that $\mathfrak{p}_1\dots\mathfrak{p}_{k-1}\mathfrak{p}_k$ is the largest $\mathcal{O}_K$ -ideal in $\mathcal{I}$. We have $\mathfrak{p}_1\dots\mathfrak{p}_{k-1}\mathfrak{p}_k\Lambda \subset \mathcal{I} \subsetneq \mathfrak{p}_1\Lambda$. Consider $\mathfrak{p}_1^{-1}\mathcal{I}$; we have $\mathfrak{p}_2\dots\mathfrak{p}_{k-1}\mathfrak{p}_k\Lambda \subset \mathfrak{p}_1^{-1}\mathcal{I} \subsetneq \Lambda$, so $\mathfrak{p}_1^{-1}\mathcal{I}$ is integral. Then observe that the largest $\mathcal{O}_K$ -ideal contained in $\mathfrak{p}_1^{-1}\mathcal{I}$ is $\mathfrak{p}_1\dots\mathfrak{p}_{k-1}$, so by induction we have $\mathfrak{p}_1^{-1}\mathcal{I} = \mathfrak{p}_1\dots\mathfrak{p}_{k-1}\Lambda$, and hence $\mathcal{I} = \mathfrak{p}_1\dots\mathfrak{p}_{k-1}\mathfrak{p}_k\Lambda$, as required.

Now suppose the statement is true for $n < k$ and $(e'_1, \dots, e'_n) = (e_1, \dots, e_n) \in \mathbb{Z}_{\geq 1}^n$, and true for $n = k$ and $(e'_1, \dots, e'_k) < (e_1, \dots, e_k)$, and consider an ideal $\mathcal{I}$ such that $\mathfrak{p}_1^{e_1}\dots\mathfrak{p}_{k-1}^{e_{k-1}}\mathfrak{p}_k^{e_k}$ is the largest $\mathcal{O}_K$ -ideal in $\mathcal{I}$. Like before, $\mathfrak{p}_1^{e_1}\dots\mathfrak{p}_{k-1}^{e_{k-1}}\mathfrak{p}_k^{e_k}\Lambda \subset \mathcal{I} \subsetneq \mathfrak{p}_k\Lambda$ (simply relabel the primes for this to hold). Again, $\mathfrak{p}_k^{-1}\mathcal{I}$ is integral, and observe that the largest $\mathcal{O}_K$ -ideal contained in $\mathfrak{p}_k^{-1}\mathcal{I}$ is $\mathfrak{p}_1^{e_1}\dots\mathfrak{p}_{k-1}^{e_{k-1}}$. We split into two cases: $e_k - 1 = 0$, and $e_k - 1 > 0$.

When $e_k - 1 > 0$, we use induction on $(e'_1, \dots, e'_k)$, and since $(e_1, \dots, e_k - 1) < (e_1, \dots, e_k)$, by hypothesis have $\mathfrak{p}_k^{-1}\mathcal{I} = \mathfrak{p}_1^{e_1}\dots\mathfrak{p}_{k-1}^{e_{k-1}}\Lambda$. Hence $\mathcal{I} = \mathfrak{p}_1^{e_1}\dots\mathfrak{p}_{k-1}^{e_{k-1}}\mathfrak{p}_k^{e_k}\Lambda$, as required.

When $e_k - 1 = 0$, the largest $\mathcal{O}_K$ -ideal contained in $\mathfrak{p}_k^{-1}\mathcal{I}$ is $\mathfrak{p}_1^{e_1}\dots\mathfrak{p}_{k-1}^{e_{k-1}}$. We then induct on n , since $n = k - 1 < k$, to obtain $\mathfrak{p}_k^{-1}\mathcal{I} = \mathfrak{p}_1^{e_1}\dots\mathfrak{p}_{k-1}^{e_{k-1}}\Lambda$ and hence $\mathcal{I} = \mathfrak{p}_1^{e_1}\dots\mathfrak{p}_{k-1}^{e_{k-1}}\mathfrak{p}_k$, as required. $\square$

When γ is a unit, this fully characterises unramified ideals in the natural order of the CDAs we consider.

3.3 Consequences

The result of the previous section has a number of consequences, which we now detail.

3.3.1 Implications for CLWE

In [71], the authors reduced lattice problems on lattices obtained from ideals in maximal orders of certain CDAs to search CLWE, and search CLWE to decision CLWE (subject to a restriction of the secret space). In particular, they obtained

Theorem 3.2. [71, Theorem 6] *Let $\mathcal{A}$ be a cyclic division algebra over a number field L with center K and natural, maximal order Λ with $|\gamma| = 1$. Let $\alpha = \alpha(n) \in (0, 1)$ and $q = q(n) \geq 2$, unramified in L , be parameters such that $\alpha \cdot q \geq \omega(\sqrt{\log N})$. Then, there is a polynomial-time quantum reduction from $\mathcal{A}$ -DGS $_{\xi}$ to search $\text{CLWE}_{q, \Sigma_{\alpha}}$ for any $\xi = r \cdot \sqrt{d} \omega(\sqrt{\log(d \cdot n)}) / \alpha q$, where $r > \sqrt{2} q \cdot \eta_{\varepsilon}(\mathcal{I})$.*

We now explain how Theorem 3.1 affects the guarantee of this result. Let $\mathcal{A} = (L/K, \theta, \gamma)$ be a CDA, with $K = \mathbb{Q}(\zeta_n)$, natural order Λ and γ a primitive root of unity. Recall we embed Λ into $\mathbb{R}^{nd^2}$ via the embeddings of K extended to L , denoted by α_i , $i = 1, \dots, n$; in particular, we embed Λ into $\mathbb{R}^{nd^2}$ by sending $x \in \Lambda$ to $(\text{vec}(\alpha_1(\phi(x))), \dots, \text{vec}(\alpha_n(\phi(x))))^T$.

Note that Λ has at least nd roots of unity: n of these come from $K = \mathbb{Q}(\zeta_n)$, and d come from the powers of u (since γ is a root of unity). This means that if we are given a short vector in an ideal lattice $\mathcal{I}$ of Λ , we can construct nd short vectors in $\mathcal{I}$.

We now observe that the canonical embedding of Λ is orthogonal. To see this, consider the simple case $d = 2$. So $\Lambda = \mathcal{O}_L + u\mathcal{O}_L$. Recall

$$\phi(x) = \begin{pmatrix} x_0 & \gamma\theta(x_1) \\ x_1 & \theta(x_0) \end{pmatrix}.$$

The embedding of $x \in \Lambda$, $\sigma_{\mathcal{A}}(x) = (\text{vec}(\alpha_1(\phi(x))), \dots, \text{vec}(\alpha_n(\phi(x))))^T$ yields

$$\begin{aligned} \sigma_{\mathcal{A}}(x) = & (\alpha_1(x_0), \alpha_1(x_1), \alpha_1(\gamma\theta(x_1)), \alpha_1(\theta(x_0)), \\ & \dots, \alpha_n(x_0), \alpha_n(x_1), \alpha_n(\gamma\theta(x_1)), \alpha_n(\theta(x_0)))^T \in \mathbb{R}^{4n}. \end{aligned}$$

So if $x = x_0 + u \cdot 0$, we obtain

$$\sigma_{\mathcal{A}}(x) = (\alpha_1(x_0), 0, 0, \alpha_1(\theta(x_0)), \dots, \alpha_n(x_0), 0, 0, \alpha_n(\theta(x_0)))^T,$$

and if $x = 0 + ux_1$,

$$\sigma_{\mathcal{A}}(x) = (0, \alpha_1(x_1), \alpha_1(\gamma\theta(x_1)), 0, \dots, 0, \alpha_n(x_1), \alpha_n(\gamma\theta(x_1)), 0)^T.$$

These are clearly orthogonal, and moreover this argument holds for any $d \in \mathbb{N}$.

By Theorem 3.1, $\mathcal{I}$ embeds as the direct sum of embeddings of $\bar{\mathcal{I}}\mathcal{O}_L$. Solving SIVP in $\bar{\mathcal{I}}\mathcal{O}_L$ yields nd short independent vectors $x_1, \dots, x_{nd} \in \bar{\mathcal{I}}\mathcal{O}_L$, and moreover $x_i \cdot (1 + u \cdot 0 + \dots + u^{d-1} \cdot 0) = x_i \cdot 1_{\mathcal{A}}$ is a short vector of $\mathcal{I}$. We can also use the roots of unity in Λ to create more short independent vectors: for example, the set of $u^j x_i$, $0 \leq j < d, 1 \leq i \leq nd$ is a set of nd^2 short independent vectors. Thus to solve SIVP in $\mathcal{I}$, it is sufficient to solve the SIVP instance given by $\mathcal{I} \cap \mathcal{O}_L$.

Moreover in the special case of $d = 2$, $n = 2^r$ for some $r > 0$, we have

$$\#\{\text{Roots of unity in } \Lambda\} = nd = 2n = \frac{n}{2} \cdot 4 = \phi(n)d^2 = [\Lambda : \mathbb{Z}],$$

where ϕ is the Euler totient function, and so the number of roots of unity in Λ is equal to the dimension of Λ over the integers. This means that one only has to solve ideal-SVP in $\bar{\mathcal{I}}\mathcal{O}_L$ to solve SIVP in $\mathcal{I}$, since if $x \in \bar{\mathcal{I}}\mathcal{O}_L$ is a short vector, the set of $u^j \zeta_n^i x$, $0 \leq j < 2, 1 \leq i \leq n$ is a set of $2n$ short independent vectors.

This means that SIVP in ideals of $\Lambda \subset \mathcal{A}$ is equivalent to ideal-SVP in the maximal subfield L of $\mathcal{A}$ when $d = 2$ and n is a power of 2, and equivalent to SIVP in ideals of $\mathcal{O}_L$ otherwise, for the algebras used in CLWE. We note that this doesn't imply that CLWE is only as hard as SIVP in ideals of number fields; rather, it means that at this stage (we begin to address this

question below) we have no proof that CLWE is any harder than SIVP in number fields. We record the conclusion of this section below:

Proposition 3.1. *Let $\mathcal{A} = (L/K, \theta, \zeta_n)$ be a CDA with $K = \mathbb{Q}(\zeta_n)$. Let $\Lambda \subset \mathcal{A}$ be the natural order, $\mathcal{I} \subset \Lambda$ an ideal, and $\bar{\mathcal{I}} := \mathcal{I} \cap K$. Then a solution to SIVP in $\bar{\mathcal{I}}\mathcal{O}_L$ yields a solution to SIVP in $\mathcal{I}$. When $d = 2$ and n is a power of 2, a solution to SVP in $\bar{\mathcal{I}}\mathcal{O}_L$ yields a solution to SIVP in $\mathcal{I}$.*

3.3.2 The Gentry-Szydlo Algorithm for Quaternionic CDAs

In [69], the authors gave a probabilistic algorithm which can be used to determine whether an ideal lattice (in a cyclotomic field) has an orthonormal basis. These techniques were later extended [99], [93], [100] to develop algorithms to determine whether there is an isomorphism between two given ideal lattices, for ideals in commutative orders with complex multiplication. In this section, we use Theorem 3.1 to extend the Gentry-Szydlo algorithm to natural orders of certain quaternion algebras.

The result of relevance to us from the listed works in the previous paragraph is the following:

Theorem 3.3. *[100, Theorem 1.6] There is a deterministic polynomial-time algorithm that, given a CM-order A and invertible A -lattices L and M , decides whether or not L and M are isomorphic as A -lattices, and if so, exhibits such an A -isomorphism.*

Here an order A is commutative, and is *CM* if it has no nonzero nilpotent elements and an automorphism $\bar{\cdot} : A \rightarrow A, x \mapsto \bar{x}$ such that $\psi(\bar{x}) = \overline{\psi(x)}$ for all $x \in A$ and ring homomorphisms $\psi : A \rightarrow \mathbb{C}$. An example of a CM order is the ring of integers $\mathbb{Z}[\zeta_n]$ of a cyclotomic field $\mathbb{Q}(\zeta_n)$, where the map $\bar{\cdot}$ is the automorphism corresponding to complex conjugation. We will most concretely consider the case of $\mathbb{Q}(\zeta_n, \sqrt{\ell})$ for some prime $\ell \equiv 1 \pmod{4}$ coprime to n .

Proposition 3.2. *The ring of integers of a compositum of a totally real finite Galois extension of $\mathbb{Q}$ which is linearly disjoint with $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ with $\mathbb{Q}(\zeta_n)$ is a CM order. The map $\bar{\cdot}$ is the (trivial) extension of the automorphism corresponding to complex conjugation to the compositum.*

Proof. Recall we say a number field is a CM field if it is a totally complex quadratic extension of a totally real field. Then the ring of integers of such a field is a CM order (see e.g. [100]). Let K be a totally real finite Galois extension of $\mathbb{Q}$ linearly disjoint with $\mathbb{Q}(\zeta_n)$. Consider the compositum $\mathbb{Q}(\zeta_n + \zeta_n^{-1})K$; this is a compositum of two totally real fields, so is a totally real field. Moreover $[\mathbb{Q}(\zeta_n)K : \mathbb{Q}(\zeta_n + \zeta_n^{-1})K] = 2$ (by the assumption of linear disjointedness over $\mathbb{Q}$). To see that $\mathbb{Q}(\zeta_n)K$ is totally complex, recall that $\mathbb{Q}(\zeta_n)$ is totally complex, and any finite Galois extension of a totally complex field is totally complex, so therefore $\mathbb{Q}(\zeta_n)K$ is too. $\square$

We now proceed to extend the Gentry-Szydlo algorithm to natural orders of CDAs of the form $\mathcal{A} = (L/K, \theta, \zeta_n)$, where $K = \mathbb{Q}(\zeta_n)$ and L is a totally real finite Galois extension of K , using Theorem 3.1.

Theorem 3.4. *Let $K = \mathbb{Q}(\zeta_n)$, L/K a finite cyclic Galois totally real extension of K , $\mathcal{A} = (L/K, \theta, \gamma)$ a CDA with $\gamma \in \mathcal{O}_K^\times$ and $|\gamma| = 1$, and $\mathcal{I}, \mathcal{J} \subset \Lambda \subset \mathcal{A}$ ideals in the natural order of $\mathcal{A}$. Then there is a deterministic polynomial-time algorithm that decides whether or not $\mathcal{I}, \mathcal{J}$ are isomorphic as Λ -lattices, and if so exhibits such a Λ -isomorphism.*

Proof. Given $\mathcal{I} \subset \Lambda$, by Theorem 3.1 we can write

$$\mathcal{I} = \bigoplus_{i=0}^{d-1} u^i \bar{\mathcal{I}} \mathcal{O}_L,$$

where $\bar{\mathcal{I}} = \mathcal{I} \cap K$. Since $\mathcal{I}$ embeds orthogonally into H^d (cf. the discussion in §3.3.1), we obtain d embedded copies of $\bar{\mathcal{I}}$. To decide whether $\mathcal{I}, \mathcal{J}$ are isomorphic it thus suffices to apply the result of Theorem 3.3 to $\bar{\mathcal{I}} \mathcal{O}_L, \bar{\mathcal{J}} \mathcal{O}_L$, which can be done since $\mathcal{O}_L$ is CM by Proposition 3.2.

If $\bar{\mathcal{I}} \mathcal{O}_L, \bar{\mathcal{J}} \mathcal{O}_L$ are indeed isomorphic, we obtain an isomorphism $\varphi : \bar{\mathcal{I}} \mathcal{O}_L \cong \bar{\mathcal{J}} \mathcal{O}_L$. Linearly extending φ and setting $\varphi(u) = u$ by fiat gives a map $\varphi' : \mathcal{I} \rightarrow \mathcal{J}$. This is a Λ -module isomorphism $\mathcal{I} \rightarrow \mathcal{J}$; we now verify this is an isomorphism of lattices, that is a Λ -module isomorphism that preserves the inner product.

Recall the inner product of $x, y \in \Lambda$ is $\langle x, y \rangle_{\mathcal{A}} = \langle \Sigma_{\mathcal{A}}(x), \overline{\Sigma_{\mathcal{A}}(y)} \rangle_{H^d} = \sum_{i=0}^{d-1} \langle \Sigma_L(x_i), \overline{\Sigma_L(y_i)} \rangle_H =$

$\sum_{i=0}^{d-1} \langle x_i, y_i \rangle_L$. Thus

$$\begin{aligned} \langle \varphi'(x), \varphi'(y) \rangle_{\mathcal{A}} &= \sum_{i=0}^{d-1} \langle \Sigma_L(\varphi(x_i)), \overline{\Sigma_L(\varphi(y_i))} \rangle_H \\ &= \sum_{i=0}^{d-1} \langle \varphi(x_i), \overline{\varphi(y_i)} \rangle_H = \sum_{i=0}^{d-1} \langle x_i, y_i \rangle_L = \langle x, y \rangle_{\mathcal{A}}, \end{aligned}$$

where the third equality uses the fact that φ is a $\mathcal{O}_L$ -lattice isomorphism, and so preserves the inner product $\langle \cdot, \cdot \rangle_H$. $\square$

3.4 Reducing Module SIVP to CLWE

In this section we follow the standard framework for reducing lattice problems to LWE. We will prove that access to a CLWE oracle in dimension d and the ability to sample from a discrete Gaussian over a *module* $\mathcal{M}$, that is from $D_{\mathcal{M},r}$, are sufficient to sample from a discrete Gaussian $D_{\mathcal{M},r'}$ where the parameters satisfy $r' < r$, subject to other standard conditions made explicit below. Combining this with the well-known reduction from module SIVP to DGS [97], we obtain a reduction from module SIVP in rank d to search CLWE in algebras of index d . We first make some comments about modules and pseudobases.

Lemma 3.2. [97, Lemma 2.1] *If $M = \sum_{k=1}^d I_k \mathbf{b}_k$ is a pseudobasis presentation of a module M , then $M^\vee = \sum_{k=1}^d I_k^\vee \mathbf{b}_k^\vee$ where the $\mathbf{b}_\ell^\vee$ satisfy $\langle \mathbf{b}_k, \overline{\mathbf{b}_\ell^\vee} \rangle = 1$ if $k = \ell$ and $\langle \mathbf{b}_k, \overline{\mathbf{b}_\ell^\vee} \rangle = 0$ else.*

Let $t \in I$ such that $t\mathcal{O}_K + qI = I$ (t exists and can be found efficiently given I and the prime ideal factorization of $q\mathcal{O}_K$). The function $\theta_I : K \rightarrow K$ defined $\theta_I(x) = t \cdot x$ induces an isomorphism $R_q \cong I/qI$. This isomorphism has inverse $\theta_I^{-1} : I/qI \rightarrow R_q$, defined $\theta_I^{-1}(y) = t^{-1} \cdot y' \bmod qR$ where $y' = y \bmod qI$ and $y' \in t\mathcal{O}_K$. The function θ_I also induces an isomorphism $I^\vee/qI^\vee \cong R_q^\vee$ with (efficiently computable) inverse $\theta_I^{-1} : R_q^\vee \rightarrow I^\vee/qI^\vee$, $\theta_I^{-1}(y) = t^{-1} \cdot y' \bmod qR$ where $y' = y \bmod qI^\vee$ and $y' \in t\mathcal{O}_K$.

We extend this to modules with a given pseudobasis: if $\mathcal{M} = \sum_{k=1}^d I_k \cdot \mathbf{b}_k$ and $f : I_1/qI_1 \times \dots \times I_d/qI_d \rightarrow \mathcal{M}/q\mathcal{M}$ and $g : \mathcal{M}/q\mathcal{M} \rightarrow I_1/qI_1 \times \dots \times I_d/qI_d$ are maps such that $f(x_1, \dots, x_d) =$

$\sum_{k=1}^d x_k \cdot \mathbf{b}_k$ and $g(\sum_{k=1}^d x_k \cdot \mathbf{b}_k) = (x_1, \dots, x_d)$, then we set $\Theta = f \circ (\theta_{I_1} \times \dots \times \theta_{I_d})$ and $\Theta^{-1} = (\theta_{I_1}^{-1} \times \dots \times \theta_{I_d}^{-1}) \circ g$. Note $\Theta : (R/qR)^d \rightarrow \mathcal{M}/q\mathcal{M}$. There is a corresponding map between the duals which we also write by $\Theta : \mathcal{M}^\vee/q\mathcal{M}^\vee \rightarrow (R^\vee/qR^\vee)^d$.

Here we aim to reduce Module SIVP to CLWE. To achieve this, it is sufficient to reduce q -Mod-BDD to search CLWE, given access to discrete Gaussian samples. We do this for modules $\mathcal{M}$ satisfying the following property:

Definition 46. We call a module $\mathcal{M} \subset L^m$ with pseudobasis $[(I_k)_k, (b_k)_k]$, $1 \leq k \leq n$, integral if $\mathbf{b}_k \in \mathcal{O}_L^m$ and I_k is an integral ideal, for all $k = 1, \dots, n$.

We will need two lemmas on sampling from algebraic objects:

Lemma 3.3. [97, Lemma 2.13] Let $\mathbf{r} \in (\mathbb{R}^+)^n$ with $r_j = r_{\nu-j}$ for all $j \in \mathbb{Z}_\nu^\times$, $\mathbf{x} \in K^d$ sampled from $D_{\mathbf{s}, \dots, \mathbf{s}}$ and $\mathbf{e} \in K^d$ fixed. Then $\sum_k x_k e_k$ is distributed from $D_{\mathbf{r}'}$ with $r'_j = r_j \cdot \left(\sum_{k \in [d]} |\sigma_j(e_k)|^2 \right)^{1/2}$ for all j .

Lemma 3.4. Let M be a module over K of rank d , $r \geq \sqrt{2}q\eta_\epsilon(M)$, $\epsilon \in (0, 1/2)$, and $\alpha \in (0, 1)$ such that $\frac{r\alpha}{\sqrt{2}\delta} \geq \sqrt{r^2 + (\frac{\alpha}{\sqrt{2}\delta})^2} \cdot \eta_\epsilon(M)$. Let $Z := \langle X, S \rangle + Y$, where $X \sim D_{M,r}$, $S \in M$, $\delta := \|S\|_{2,\infty}$, and $Y \sim D_{\alpha/\sqrt{2}}$. Then $Z \sim D_{\mathbf{r}'}$ with $r_i'^2 = r^2 \cdot \sum_{k=1}^d |\sigma_i(S_k)|^2 + \frac{\alpha^2}{2} \leq r^2 \cdot \|S\|_{2,\infty}^2 + \frac{\alpha^2}{2}$.

Proof. We closely follow the proof of [97, Lemma 4.15]. Observe Y is distributed identically to $\langle e'', S \rangle$ for $e'' \sim D_{\mathbf{s}, \dots, \mathbf{s}}$ with $s_i = \frac{\alpha}{\sqrt{2 \sum_{k=1}^d |\sigma_i(S_k)|^2}}$, by Lemma 3.3. Now write $e'' = e_1'' + e_2''$ with $e_1'' \sim D_{\alpha/2\delta}$ and $e_2'' \sim D_{\mathbf{s}''}$ with $s_i''^2 = s_i^2 - \frac{\alpha^2}{2\delta^2}$. Note $s_i''^2 > 0$ by assumption. We now use Lemma 2.9, to obtain $X + e_1''$ is 4ϵ from D_τ for $\tau = \sqrt{r^2 + (\frac{\alpha}{\sqrt{2}\delta})^2}$, and hence that $X + e_1'' + e_2''$ is 4ϵ from $D_{\mathbf{r}'', \dots, \mathbf{r}''}$ with $r_i''^2 = r^2 + \frac{\alpha^2}{2 \sum_{k=1}^d |\sigma_i(S_k)|^2}$. Another application of Lemma 3.3 gives $\langle X + e_1'' + e_2'', e \rangle \sim D_{\mathbf{r}'}$ with $r_i'^2 = r^2 \cdot \sum_{k=1}^d |\sigma_i(S_k)|^2 + \frac{\alpha^2}{2}$, and hence $r_i'^2 \leq r^2 \cdot \|S\|_{2,\infty}^2 + \frac{\alpha^2}{2}$. $\square$

We prove the following:

Theorem 3.5. Let $\varepsilon = \varepsilon(n) > 0$ be a negligible function of n , $\alpha \in (0, 1)$ and $q \geq 2$. Let $\mathcal{M} \subseteq L^2$ be an integral left $\mathcal{O}_L$ -module, and $r > \sqrt{2}q \cdot \eta_\epsilon(\mathcal{M})$. Given access to an oracle sampling from the distribution $D_{\mathcal{M},r}$, there exists a probabilistic reduction from q -Mod-BDD $_{\alpha q \omega(\sqrt{\log nd})/\sqrt{2ndr}}$ to search CLWE $_{q,s,\Psi_{\leq \alpha}}$ with $d = 2$.

Proof. Let $\mathcal{O}$ be a search $\text{CLWE}_{q,s,\Psi_{\leq \alpha}}$ oracle. Let the q -Mod-BDD instance be $y = x + e$, with $x \in \mathcal{M}^\vee$ and $\|e\|_{2,\infty} \leq \delta = \frac{\alpha q \cdot \omega(\sqrt{\log nd})}{\sqrt{2ndr}}$. Proceed as follows: sample $z \leftarrow D_{\mathcal{M},r}$ and $e', e'' \leftarrow D_{\alpha/\sqrt{2}}$. Write $y = x + e$ and z as

$$y = \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} = \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} + \begin{pmatrix} e_0 \\ e_1 \end{pmatrix} \text{ and } z = \begin{pmatrix} z_0 \\ z_1 \end{pmatrix}.$$

Set $z^0 = \begin{pmatrix} z_0 \\ \gamma\theta(z_1) \end{pmatrix}$ and $z^1 = \begin{pmatrix} z_1 \\ \theta(z_0) \end{pmatrix}$. Note that these are elements of $\mathcal{O}_L^2$. Then set $w^0 = \Theta(z^0 \bmod q\mathcal{O}_L^2)$ and $w^1 = \Theta(z^1 \bmod q\mathcal{O}_L^2)$. Finally, set $b^0 = \frac{1}{q} \langle w^0, y \rangle + e' \bmod \mathcal{O}_L^\vee$ and $b^1 = \frac{1}{q} \langle w^1, y \rangle + e'' \bmod \mathcal{O}_L^\vee$.

Call the oracle $\mathcal{O}$ on $(\phi(a), \mathbf{b}) = (A, (b^0|b^1)^T)$ where $A^T = (z^0|z^1)$. Note $A = \phi(a)$ where $a = z_0 + uz_1$: we have

$$A = \phi(a) = \begin{pmatrix} z_0 & \gamma\theta(z_1) \\ z_1 & \theta(z_0) \end{pmatrix} = \begin{pmatrix} z^0|z^1 \end{pmatrix}^T.$$

Since $r \geq \eta_\epsilon(q\mathcal{M})$, we apply Lemma 2.6 to conclude that $a \bmod q\Lambda$ is distributed at most 4ϵ from the uniform distribution over Λ_q .

If $\mathcal{O}$ succeeds, it returns some $s \in \Lambda_q^\vee$; output $x = \Theta^{-1} \left(\begin{pmatrix} s_0 \\ s_1 \end{pmatrix} \right)$. We now prove correctness.

We show $\mathbf{b}$ is the matrix-vector representation of a CLWE sample $\mathbf{b} = \frac{1}{q}(a \cdot s) + f$, for f distributed according to $D_{r'}$ with $r'_i \leq \alpha$ for all i . We have:

$$b^0 = \frac{1}{q} \langle w^0, y \rangle + e' = \frac{1}{q} \langle w^0, x + e \rangle + e' = \frac{1}{q} \langle w^0, x \rangle + \frac{1}{q} \langle w^0, e \rangle + e' = \frac{1}{q} \langle w^0, x \rangle + e'_0.$$

By definition, $w^0 = \Theta(z^0 \bmod q) = \Theta \left(\begin{pmatrix} z_0 \\ \gamma\theta(z_1) \end{pmatrix} \bmod q \right) = (t_0 \cdot z_0) \cdot b_0 + (t_1 \cdot \gamma\theta(z_1)) \cdot b_1 \bmod q\mathcal{M}$ with $t_k \in I_k$. By Proposition 3.2, we have $\mathcal{M}^\vee = I_0^\vee b_0^\vee + I_1^\vee b_1^\vee$. Write $x = x_0 b_0^\vee + x_1 b_1^\vee \in \mathcal{M}^\vee$. Then $x_k \in I_k^\vee = I_k^{-1} \cdot \mathcal{O}_L^\vee$ for all k . We also have $\langle b_k, b_{k'}^\vee \rangle = 1$ if $k = k'$ and

$\langle b_k, b_{k'}^\vee \rangle = 0$ otherwise. Modulo $q\mathcal{O}_L^\vee$:

$$\begin{aligned} \langle w^0, x \rangle &= \langle (t_0 \cdot z_0) \cdot b_0 + (t_1 \cdot \gamma\theta(z_1)) \cdot b_1, x_0 b_0^\vee + x_1 b_1^\vee \rangle = (t_0 \cdot z_0) \cdot x_0 + (t_1 \cdot \gamma\theta(z_1)) \cdot x_1 \\ &= z_0 \cdot (t_0 \cdot x_0) + \gamma\theta(z_1) \cdot (t_1 \cdot x_1) \bmod q\mathcal{O}_L^\vee. \end{aligned}$$

Because $s = \Theta(x \bmod q\mathcal{M}^\vee) = (t_0 \cdot x_0 \bmod q\mathcal{O}_L^\vee, t_1 \cdot x_1 \bmod q\mathcal{O}_L^\vee)^T$, we have:

$$\langle w^0, x \rangle = z_0 \cdot (t_0 \cdot x_0) + \gamma\theta(z_1) \cdot (t_1 \cdot x_1) = z_0 \cdot s_0 + \gamma\theta(z_1) \cdot s_1 = \langle z^0, s \rangle \bmod q\mathcal{O}_L^\vee.$$

Thus we obtain that $\frac{1}{q}\langle w^0, x \rangle = \frac{1}{q}\langle z^0, s \rangle \bmod \mathcal{O}_L^\vee$. Similarly for w^1, z^1, b^1 . Combining these,

$$\begin{aligned} (A, \mathbf{b}) &= \left(\left(z^0 | z^1 \right)^T, \left(\frac{1}{q}\langle w^0, y \rangle + e' \middle| \frac{1}{q}\langle w^1, y \rangle + e'' \right)^T \right) \\ &= \left(\left(z^0 | z^1 \right)^T, \left(\frac{1}{q}\langle w^0, s \rangle + e'_0 \bmod \mathcal{O}_L^\vee \middle| \frac{1}{q}\langle w^1, s \rangle + e''_1 \bmod \mathcal{O}_L^\vee \right)^T \right), \end{aligned}$$

and this is a valid CLWE sample. The error may be analysed as in [97, Lemma 4.15]: we show that $e'_0 = \frac{1}{q}\langle w^0, e \rangle + e'$ is distributed according to $D_{r'}$ with $r'_i \leq \alpha$ for all i , conditioned on a fixed choice of z^0 . Write $e'_0 = \frac{1}{q}\sum_i w_i^0 e_i + e'$. Since $w^0 \sim D_{\mathcal{M}, r}$, and $\|e\|_{2, \infty} \leq \delta$, $e' \leftarrow D_{\alpha/\sqrt{2}}$, and $r > \sqrt{2}q \cdot \eta_\varepsilon(\mathcal{M})$, we may use Lemma 3.4 and the result follows. $\square$

We note that the above proof holds for any $d \in \mathbb{N}$. The above formalises a sense in which CLWE is a structured MLWE problem.

3.5 CLWE with Large Modulus $\geq$ CMLWE

3.5.1 Pseudobases of Modules over Noncommutative Rings

Recall that for every module $\mathcal{M}$ of finite rank over a commutative Dedekind domain R , there exist ideals I_k of R and $(b_k)_k$ linearly independent vectors of K^d such that $M = \sum_{k=1}^m I_k \cdot b_k$. Then $[(I_k)_k, (b_k)_k]$ is a *pseudo-basis* of $\mathcal{M}$. Below we show this is true for modules over maximal

orders of CDAs. We first need two results on modules over noncommutative rings.

Lemma 3.5. *[61, Theorem 2.1] Let R be an hereditary Noetherian prime ring, and let A be a finitely generated right R -module. Denote the set of torsion elements of A by $t(A)$. Then $A/t(A)$ is projective and $A \cong t(A) \oplus A/t(A)$.*

Lemma 3.6. *[61, Theorem 2.4] If R is a Dedekind prime ring and A is a finitely-generated projective right R -module, then $A \cong R \oplus \cdots \oplus R \oplus I$ for some right R -ideal I .*

It is well known [61] that maximal orders in CDAs over number fields are Dedekind prime. Moreover Dedekind prime rings are hereditary and Noetherian (by definition). For more on these definitions see [70], [106]. We now prove the existence of pseudo-bases of modules over maximal orders:

Theorem 3.6. *Let Λ be a maximal order of a CDA, and $\mathcal{M}$ be a finitely generated torsion-free Λ -module. Then there exist $\omega_1, \dots, \omega_n \in \mathcal{M}$ and fractional ideals of Λ , $I_1, \dots, I_n$ such that*

$$\mathcal{M} = I_1\omega_1 + \dots + I_n\omega_n.$$

Proof. Since $\mathcal{M}$ is torsion-free, $t(\mathcal{M}) = 0$, and hence by Lemma 3.5, $\mathcal{M}$ is projective. By Lemma 3.6, we can write $\mathcal{M} \cong \Lambda^{n-1} \oplus I$ for some right Λ -ideal I . Assume without loss of generality that $1 \in I$. Then let $f : \Lambda^{n-1} \oplus I \rightarrow \mathcal{M}$, and $f(e_i) = \omega_i$. Since f is an isomorphism, $\mathcal{M} = \mathfrak{a}_1\omega_1 + \dots + \mathfrak{a}_{n-1}\omega_{n-1} + \mathfrak{a}_n\omega_n$, with $\mathfrak{a}_n = I$ and $\mathfrak{a}_i = R$, $i = 1, \dots, n-1$. $\square$

If we started with a two-sided Λ -module, the fractional ideals $\mathfrak{a}_i$ must all also be two-sided.

3.5.2 CMLWE

Here we define Cyclic Module Learning with Errors (CMLWE), LWE from a module over Λ . We give a reduction from module lattice problems to the search problem. We introduce this variant so that we can show $\text{CLWE} \geq \text{CMLWE}$ for some change in parameters. This allows us to relate the security of search CLWE on a certain class of module lattices, which then by the search

to decision reduction for CLWE, implies the hardness of decision CLWE (for certain secrets). Below we define the CMLWE distribution and the search and decision CMLWE problems

Definition 47. Let L/K be a Galois extension of number fields of dimension $[L : K] = d$ with cyclic Galois group generated by θ . Let $\mathcal{A} := (L/K, \theta, \gamma)$ be the resulting cyclic algebra with center K and invariant u with $u^d = \gamma \in \mathcal{O}_K$. Let Λ be the natural maximal order of $\mathcal{A}$. For an error distribution ψ over $\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$, an integer modulus $q \geq 2$, and a secret $s \in (\Lambda_q^\vee)^m$, a sample from the CMLWE distribution $\Pi_{q,s,m,\psi}$ is obtained by sampling $a \leftarrow \Lambda_q^m$ uniformly at random, $e \leftarrow \psi$, and outputting $(a, b) = (a, \langle a, s \rangle / q + e \bmod \Lambda^\vee) \in \Lambda_q^m \times (\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}) / \Lambda^\vee$.

Note that when $d = 1$ we recover MLWE.

Definition 48. Let Ψ be a family of error distributions over $\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$. The search CMLWE problem, denoted by $\text{CMLWE}_{q,s,m,\psi}$, is to recover s from a collection of independent samples from $\Pi_{q,s,m,\psi}$ for any $s \in (\Lambda_q^\vee)^m$ and $\psi \in \Psi$.

Definition 49. Let Υ be a distribution on a family of error distributions over $\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$ and $U_{\Lambda,m}$ denote the uniform distribution on $\left(\Lambda_q^m, \left(\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}} \right) / \Lambda^\vee \right)$. The decision CMLWE problem, $\text{DCMLWE}_{q,m,\Upsilon}$, is given a collection of independent samples from either $\Pi_{q,s,m,\psi}$ for random $(s, \psi) \leftarrow U((\Lambda_q^\vee)^m) \times \Upsilon$ or from $U_{\Lambda,m}$, to decide which, with non-negligible advantage.

CMLWE is structured LWE

If we have m samples of CMLWE with the same secret $s \in (\Lambda_q^\vee)^m$, we can write a CMLWE sample in matrix-vector notation: $(A, As + e) \in \Lambda_q^{m \times m} \times ((\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}) / \Lambda^\vee)^m$. Expanding these over a $\mathbb{Z}_q$ -basis gives a LWE sample in dimension $mnd^2 \times mnd^2$. We note here that the modules we consider will only (in general) be left modules.

Lattices from Λ -Modules

Here we show how to embed algebraic lattices in Λ^m as Euclidean lattices in $\mathbb{R}^n$, for some n . Consider a CDA $\mathcal{A} = (L/K, \theta, \gamma)$ with $[L : K] = d$. As before, fix the L -basis of $\mathcal{A}$, $\{u^i\}_{i \geq 0}$, and

express an element as the linear map $\phi(x)$ given by left multiplication on the u^i . As previously shown, if $x = \bigoplus_{i=0}^{d-1} u^i x_i \in \mathcal{A}$, then

$$\phi(x) = \begin{pmatrix} x_0 & \gamma\theta(x_{d-1}) & \dots & \gamma\theta^{d-1}(x_1) \\ x_1 & \theta(x_0) & \dots & \gamma\theta^{d-1}(x_2) \\ \dots & \dots & \dots & \dots \\ x_{d-1} & \theta(x_{d-2}) & \dots & \theta^{d-1}(x_0) \end{pmatrix}.$$

We defined two norms on $\mathcal{A}$; for the first, we set $\|x\|_p^p := \sum_{\alpha \in \text{Emb}(K)} \sum_{i,j} |\alpha(\phi(x)_{i,j})|^p$, and for the second $\|x\|_\infty := \max_{\alpha,i,j} |\alpha(\phi(x)_{i,j})|$, where $\phi(x)_{i,j}$ denotes the i, j th entry of $\phi(x)$. We can extend this to modules over Λ straightforwardly: we apply the canonical embedding to each coordinate of Λ^m . This maps into $\mathbb{R}^{mnd^2}$. We then apply our norms to the vectors obtained in the natural way. We also extend duality with respect to the trace $\text{Tr}(\cdot)$ of $x \in \mathcal{A}$ to module lattices $\mathcal{M} \subset \mathcal{A}^m$ as follows: $\mathcal{M}^\vee$ is the set

$$\mathcal{M}^\vee = \{x \in \mathcal{A}^m : \text{Tr}(\langle x, \overline{\mathcal{M}} \rangle) \subset \mathbb{Z}\},$$

where $\langle \cdot, \cdot \rangle$ is the Hermitian inner product.

3.5.3 Security Proof for Search CMLWE

Here we adapt the security proof of [97] to CMLWE. We prove the following theorem, where $\text{CMod-GIVP}_\gamma^\phi$ is GIVP restricted to modules over Λ :

Theorem 3.7. *Let $\varepsilon(N) = N^{-\omega(1)}$, $\alpha \in (0, 1)$ and $q \geq 2$ such that $\alpha q > 2\sqrt{d}\omega(\sqrt{\log n})$. There is a quantum polynomial time reduction from solving worst-case $\text{CMod-SIVP}_\gamma^{\eta_\varepsilon}$ whp. to solving search $\text{CMLWE}_{q,s,m,\Psi_{\leq \alpha}}$ with non-negligible advantage with $\gamma = \sqrt{8Nm} \cdot \omega(\sqrt{\log n})/\alpha$.*

We proceed by reducing CMod-SIVP to CMod-DGS , and then by reducing CMod-DGS to search CMLWE. This second step requires the so-called ‘iterative step’, which is quantum, and reduces DGS_r to BDD, then BDD to q -BDD, and finally q -BDD to CMLWE and $\text{DGS}_{r'}$ with

$r' \geq r$. Thus if one has a CMLWE oracle and discrete Gaussian samples for very large r' , one repeatedly applies this lemma to sample progressively narrower discrete Gaussians.

The reductions from SIVP to DGS and from DGS to BDD hold for our lattices. Similarly for the reduction from BDD to q -BDD. Thus we are left with reducing q -BDD to CMLWE and DGS. The following lemma achieves this, using the following proposition:

Proposition 3.3. *If $\mathcal{M} = \sum_{k=1}^m I_k b_k$, then $\mathcal{M}^\vee = \sum_{k=1}^m I_k^\vee b_k^\vee$, where the $b_\ell^\vee$ s are defined by $\langle b_k, b_\ell^\vee \rangle = 1$ if $k = \ell$ and $\langle b_k, b_\ell^\vee \rangle = 0$ otherwise.*

Proof. We first show $\sum_{k=1}^m I_k^\vee b_k^\vee \subseteq \mathcal{M}^\vee$. Let $x \in \sum_{k=1}^m I_k^\vee b_k^\vee$. Then for each k there exists $x_k \in I_k^\vee$ such that $x = \sum_{k=1}^m x_k b_k^\vee$. Let $y = \sum_{k=1}^m y_k b_k \in \mathcal{M}$. Then by linearity, we have $\text{Tr}(\langle x, \bar{y} \rangle) = \sum_{k=1}^m \text{Tr}(x_k y_k)$. For all k , we have $x_k \in I_k^\vee$ and $y_k \in I_k$, and thus $\text{Tr}(x_k y_k) \in \mathbb{Z}$. Therefore, we have $\text{Tr}(\langle x, \bar{y} \rangle) \in \mathbb{Z}$ and $x \in \mathcal{M}^\vee$. We now show that $\mathcal{M}^\vee \subseteq \sum_{k=1}^m I_k^\vee b_k^\vee$. Let $x \in \mathcal{M}^\vee \subseteq \mathcal{A}^m$. We can write $x = \sum_{k=1}^m x_k b_k^\vee$, for $x_k \in \mathcal{A}$, $k = 1, \dots, m$. It suffices to show that $x_k \in I_k^\vee$. Let $y_k \in I_k$. By linearity, we have $\text{Tr}(x_k y_k) = \text{Tr}(\langle x, \overline{y_k b_k} \rangle) \in \mathbb{Z}$. Thus $x_k \in I_k^\vee$. $\square$

We need the following bijection between quotients of Λ -ideals $\mathcal{I}/q\mathcal{I}$ and Λ_q :

Proposition 3.4. *[71, Lemma 7] Let q be unramified in L . Let $\mathcal{I} \subset \Lambda$ be an ideal and let $\mathcal{J} = q\Lambda$, where $q \in \mathbb{Z}$ is prime and $q\mathcal{O}_K = \prod_{i=1}^r \mathfrak{q}_i$ is a decomposition into prime ideals. Assume $\gamma \notin \mathfrak{q}_i$ for each i . Then there exists $t \in \mathcal{I} \cap \mathcal{O}_K$ such that the ideal $t\mathcal{I}^{-1} \subset \Lambda$ is coprime to $\mathcal{J}$, and we can compute such a t efficiently given $\mathcal{I}$ and the prime factorization of $\mathcal{J}$. If $\mathcal{P}$ is an arbitrary fractional ideal of Λ then the function $\chi_t : \mathcal{A} \rightarrow \mathcal{A}, x \mapsto t \cdot x$ induces a module isomorphism from $\mathcal{P}/\mathcal{J} \cdot \mathcal{P} \rightarrow \mathcal{I} \cdot \mathcal{P}/\mathcal{I} \cdot \mathcal{J} \cdot \mathcal{P}$, and we can efficiently compute the inverse.*

We now generalise the above to hold for modules of finite rank over Λ :

Proposition 3.5. *Let $\mathcal{M} = \sum_{k=1}^m I_k b_k$, $f : I_1/qI_1 \times \dots \times I_m/qI_m \rightarrow \mathcal{M}/q\mathcal{M}$ be such that $f(x_1, \dots, x_m) = \sum_{k=1}^m x_k b_k$ and $g : \mathcal{M}/q\mathcal{M} \rightarrow I_1/qI_1 \times \dots \times I_m/qI_m$ be such that $g(\sum_{k=1}^m x_k b_k) = (x_1, \dots, x_m)$. Then f and g are ring isomorphisms and $g = f^{-1}$. Let $\chi_{t_1}, \dots, \chi_{t_m}$ be as described above. We define the functions Θ and Θ^{-1} as $\Theta = f \circ (\chi_{I_1} \times \dots \times \chi_{I_m})$ and $\Theta^{-1} = (\chi_{t_1}^{-1} \times \dots \times \chi_{t_m}^{-1}) \circ g$. Then Θ induces an isomorphism $\Lambda_q^m \rightarrow \mathcal{M}/q\mathcal{M}$ with inverse Θ^{-1} .*

Note Θ induces a map between the duals, $\Theta : \mathcal{M}^\vee / q\mathcal{M}^\vee \rightarrow (\Lambda_q^\vee)^m$. We now prove our lemma:

Lemma 3.7. *Let $\varepsilon(N) = N^{-\omega(1)}$, $\alpha \in (0, 1)$ and $q \geq 2$. Let $\mathcal{M} \subseteq \Lambda^m$ be a left Λ -module, and $r > \sqrt{2}q \cdot \eta_\varepsilon(\mathcal{M})$. Given access to an oracle sampling from the distribution $D_{\mathcal{M},r}$, there exists a probabilistic reduction from q -CMod-BDD $_{\alpha q \omega(\sqrt{\log nd})/\sqrt{2}ndr}$ to search CMLWE $_{q,s,m,\Psi_{\leq \sqrt{\frac{m+1}{2}}\alpha}}$.*

Proof. Let $\mathcal{O}$ be a search CMLWE $_{q,s,m,\Psi_{\leq \alpha}}$ oracle. Let the q -CMod-BDD instance be $y = x + e$, with $x \in \mathcal{M}^\vee$ and $\|e\|_{2,\infty} \leq \delta = \frac{\alpha q \omega(\sqrt{\log n})}{\sqrt{2}nr}$. Proceed as follows: for all $\ell \leq m$, sample $z_\ell \leftarrow D_{\mathcal{M},r}$ and $e'_\ell \leftarrow D_{\alpha/\sqrt{2}}$. Set $a_\ell = \Theta^{-1}(z_\ell \bmod q\mathcal{M})$ and $b_\ell = \frac{1}{q} \langle z_\ell, y \rangle + e'_\ell \bmod \Lambda^\vee$. Call the oracle $\mathcal{O}$ on $\{(a_\ell, b_\ell)\}_{\ell \leq m}$. If $\mathcal{O}$ succeeds, it returns some $s \in (\Lambda_q^\vee)^m$. Then output $\Theta^{-1}(s) \in \mathcal{M}^\vee / q\mathcal{M}^\vee$. We now prove correctness.

Let $\varepsilon > 0$ and $s = \Theta(x \bmod q\mathcal{M}^\vee)$. We show there exists $\psi \in \Psi_{\leq \alpha}$ such that the statistical distance between $\Pi_{q,s,m,\psi}$ and the distribution of (a, b) is at most 6ε . We first show that the statistical distance between a and the uniform distribution on Λ_q^m is at most 2ε .

By Proposition 2.6, the statistical distance between the distribution of z and the uniform distribution on $\mathcal{M}_q$ is at most 2ε , because $r \geq q \cdot \eta_\varepsilon(\mathcal{M}) = \eta_\varepsilon(q\mathcal{M})$. Then, since Θ^{-1} induces a bijection from $\mathcal{M}_q$ to Λ_q^m , the statistical distance between the distribution of $a = \Theta^{-1}(z \bmod q\mathcal{M})$ and the uniform distribution on Λ_q^m is at most 2ε .

Now we show $b = \frac{1}{q} \langle a, s \rangle + f$, for f distributed according to $D_{r'}$ with $r'_i \leq \alpha$ for all i . We have:

$$b = \frac{1}{q} \langle z, y \rangle + e' = \frac{1}{q} \langle z, x + e \rangle + e' = \frac{1}{q} \langle z, x \rangle + \left\langle \frac{1}{q} z, e \right\rangle + e'.$$

By definition, $z = \Theta(a) = \sum_{k=1}^m (t_k \cdot a_k) \cdot b_k \bmod q\mathcal{M}$ with $t_k \in I_k$ and $a_k \in \Lambda_q$. By Proposition 3.3, we have $\mathcal{M}^\vee = \sum_{k=1}^m I_k^\vee b_k^\vee$. Let $x = \sum_{k=1}^m x_k b_k^\vee$. Then $x_k \in I_k^\vee = I_k^{-1} \cdot \Lambda^\vee$ for all k . We also have $\langle b_k, b_{k'}^\vee \rangle = 1$ if $k = k'$ and $\langle b_k, b_{k'}^\vee \rangle = 0$ otherwise. Modulo $q\Lambda^\vee$:

$$\langle z, x \rangle = \sum_{k,k'=1}^d (t_k \cdot a_k) \cdot x_{k'} \cdot \langle b_k, b_{k'}^\vee \rangle = \sum_{k=1}^d (t_k \cdot a_k) \cdot x_k = \sum_{k=1}^d a_k \cdot (t_k \cdot x_k).$$

Because $s = \Theta(x \bmod q\mathcal{M}^\vee) = (t_1 \cdot x_1 \bmod q\Lambda^\vee, \dots, t_d \cdot x_d \bmod q\Lambda^\vee)^T$, we have:

$$\langle a, s \rangle = \sum_{k=1}^m a_k \cdot (t_k \cdot x_k) = \langle z, x \rangle \bmod q\Lambda^\vee.$$

Thus we obtain that $\frac{1}{q}\langle z, x \rangle = \frac{1}{q}\langle a, s \rangle \bmod \Lambda^\vee$.

We now show that conditioned on a , $\langle \frac{1}{q}z, e \rangle + e'$ has distribution $D_{r'}$ with $r'_i \leq \alpha$ for all i .

Write $\langle \frac{1}{q}z, e \rangle + e' = \frac{1}{q} \sum_{i=1}^m z_i e_i + e'$ and the coefficient of u^ℓ as

$$\left(\left\langle \frac{1}{q}z, e \right\rangle + e' \right)_\ell = \frac{1}{q} \sum_{j=1}^m \sum_{i=1}^d \tilde{z}_{j,i} \cdot e_{j,i} + e'_\ell,$$

where $\tilde{z}_{j,i}$ is a coefficient of z_j up to multiplication by γ and twisting by θ , and similarly for $e_{j,i}$.

Treating this as the sum of an inner product of elements from a rank dm module and an error, we may analyse the error as in [97, Lemma 4.15], [71, Lemma 10]. We obtain that the statistical distance between the distribution of any u^ℓ coefficient of $\langle \frac{1}{q}z, e \rangle + e'$ and $D_{r'}$ is at most 4ε , where

$$r'_i = \sqrt{\frac{\alpha^2}{2} + \frac{\alpha^2 \sum_{j=1}^m \sum_{k=1}^d |\sigma_i(e_{j,k})|^2}{2\delta^2}} \leq \sqrt{\frac{\alpha^2}{2} + \frac{m\alpha^2 \max_j \sum_{k=1}^d |\sigma_i(e_{j,k})|^2}{2\delta^2}}$$

Since $\delta \geq \max_{i,j} \sqrt{\sum_{k=1}^d |\sigma_i(e_{j,k})|^2}$, we have $r'_i \leq \sqrt{\frac{m+1}{2}}\alpha$, as desired. $\square$

3.5.4 CLWE with Large Modulus $\geq$ CMLWE

Here we adapt the work of [8] to CMLWE. Namely, we give a reduction from CMLWE in rank m and modulus q to CMLWE in rank m/k and modulus q^k , for some k . When $m = k$, this reduces CMLWE in rank k to CLWE (with some change in the modulus). This gives a security guarantee for CLWE relying on the hardness of module lattice problems.

Recall Σ_α denotes the set of Gaussians over $\oplus_{i=0}^{d-1} u^i L_\mathbb{R}$ that have every marginal distribution Gaussian of parameter at most α ; that is, the parameter $r_{ij} \leq \alpha$. We extend this to Gaussians over $(\oplus_{i=0}^{d-1} u^i L_\mathbb{R})^m$ coordinatewise. We write $\mathbb{T}_{\Lambda^\vee}$ for $(\oplus_{i=0}^{d-1} u^i L_\mathbb{R}) / \Lambda^\vee$. Below, we may write Λ for both the object contained in $\mathcal{A}$ and its image under the canonical embedding; we hope context will make which we refer to clear.

Theorem 3.8. *Let Π_{q,s,m,D_α} denote the CMLWE distribution in rank m with modulus q , secret*

$s, \alpha \in (0, 1)$, error chosen from D_α , and $[L : K] = d$. Let $\|s\|_{2,\infty} =: \delta$, $m' \leq m$, and $\epsilon \in (0, 1/2)$. Let $G \in \Lambda^{m' \times m}$ and G_H be the image of G under the canonical embedding. Let $\mathbf{B}_\mathcal{L}$ be a basis of the lattice $\mathcal{L} = \frac{1}{q}G_H^T\Lambda^{m'} + \Lambda^m \in H^{md}$, and $\mathbf{B}_\Lambda$ a basis of $\Lambda \subset H^d$. Suppose

$$r \geq \max \left(\left(\|\tilde{\mathbf{B}}_\mathcal{L}\|, \frac{1}{q}\|\tilde{\mathbf{B}}_\Lambda\| \right) \sqrt{2 \ln(2nmd^2(1 + 1/\epsilon))/\pi} \right)$$

and $\frac{r^2\beta}{\delta} \geq \sqrt{r^2 + \frac{r^2\beta^2}{\delta^2}}\eta_\epsilon(\Lambda)$. Then there is an efficient transformation ϕ such that the statistical distance between $\phi(U(\Lambda_q^m \times \mathbb{T}_{\Lambda^\vee}))$ and $U(\Lambda_{q'}^{m'} \times \mathbb{T}_{\Lambda^\vee})$ is at most 4ϵ , and such that the statistical distance between $\phi(\Pi_{q,s,m,D_\alpha})$ and Π_{q',G_s,m',Σ_R} , with $R^2 = r^2(\|s\|_{2,\infty}^2 + \beta^2) + \alpha^2$ for some β such that $\beta^2 \geq m \cdot \max_{i,j,k} |\sigma_i(s_{jk})|^2$, is at most $(4m + 6)\epsilon$, given by the steps

1. Sample $\mathbf{f} \leftarrow D_{\mathcal{L} - \frac{1}{q}\mathbf{a}_H, r}$.
2. Set $\mathbf{v} = \frac{1}{q}\mathbf{a}_H + \mathbf{f} \bmod \Lambda^m \in \mathcal{L}/\Lambda^m$ and let $\mathbf{x} \in \Lambda_{q'}^{m'}$ be a random solution of $\frac{1}{q}G_H^T\mathbf{x} = \mathbf{v} \bmod \Lambda^m$. Then set $\tilde{\mathbf{a}} \in \Lambda^{m'}$ to be the unique element of $\Lambda^{m'}$ such that $\tilde{\mathbf{a}}_H = \mathbf{x}$.
3. Sample $\tilde{e} \leftarrow D_{r\beta}$ over $\Lambda_\mathbb{R}$, set $\tilde{b} = b + \tilde{e}$, and output $(\tilde{\mathbf{a}}, \tilde{b}) \in \Lambda_{q'}^{m'} \times \mathbb{T}_{\Lambda^\vee}$.

Proof. The proof has three steps; the first two are mostly identical to the corresponding steps of [8, Theorem 1]; the third is slightly tweaked. We include the whole proof for completeness. We first show that uniform samples are mapped to uniform samples; it is immediate that if b is uniformly random, so is $\tilde{b}$. To show that $\tilde{\mathbf{a}}$ is close to uniform, supposing $\mathbf{a} \in \Lambda_q^m$ is uniformly random, we show that $\mathbf{v}$ is close to uniform. Now, $r \geq \eta_\epsilon(\mathcal{L})$, so by Lemma 2.6 for any $\bar{\mathbf{a}} \in \Lambda_q^m$ and $\bar{\mathbf{f}} \in \mathcal{L} - \frac{1}{q}\bar{\mathbf{a}}_H$,

$$\begin{aligned} \Pr[\mathbf{a} = \bar{\mathbf{a}} \text{ and } \mathbf{f} = \bar{\mathbf{f}}] &= q^{-mnd^2} \cdot \frac{\rho_r(\bar{\mathbf{f}})}{\rho_r\left(\mathcal{L} - \frac{1}{q}\bar{\mathbf{a}}_H\right)} \\ &= \frac{q^{-mnd^2}}{\rho_r(\mathcal{L})} \cdot \frac{\rho_r(\mathcal{L})}{\rho_r\left(\mathcal{L} - \frac{1}{q}\bar{\mathbf{a}}_H\right)} \cdot \rho_r(\bar{\mathbf{f}}) \\ &\in C \cdot \left[1, \frac{1+\epsilon}{1-\epsilon}\right] \cdot \rho_r(\bar{\mathbf{f}}) \end{aligned} \tag{3.1}$$

since $|\Lambda_q| = q^{nd^2}$, where $C := q^{-mnd^2}/\rho_r(\mathcal{L})$ is a constant. Recalling that a discrete Gaussian

outputs a value $\mathbf{x}$ with probability $\frac{\rho_r(\mathbf{x})}{\rho_r(\mathcal{L})}$ (where here $\mathcal{L}$ is any lattice), and that $\rho_r(\mathcal{L}) = \sum_{\mathbf{x} \in \mathcal{L}} \rho_r(\mathbf{x})$, by summing over $\bar{\mathbf{a}}$ and $\bar{\mathbf{f}}$ and, since $r \geq \eta_\varepsilon(q^{-1}\Lambda^m)$ by Lemma 2.2, applying Lemma 2.6 again, for any $\bar{\mathbf{v}} \in \mathcal{L}/\Lambda^m$ we find

$$\begin{aligned} \Pr[\mathbf{v} = \bar{\mathbf{v}}] &\in C \cdot \left[1, \frac{1+\varepsilon}{1-\varepsilon}\right] \cdot \rho_r(q^{-1}\Lambda^m + \bar{\mathbf{v}}) \\ &\in C \cdot \left[1, \frac{1+\varepsilon}{1-\varepsilon}\right] \cdot \rho_r(q^{-1}\Lambda^m) \cdot \frac{\rho_r(q^{-1}\Lambda^m + \bar{\mathbf{v}})}{\rho_r(q^{-1}\Lambda^m)} \\ &\in C' \cdot \left[\frac{1-\varepsilon}{1+\varepsilon}, \frac{1+\varepsilon}{1-\varepsilon}\right] \end{aligned}$$

where $C' = C \cdot \rho_r(q^{-1}\Lambda^m)$. Thus $\mathbf{v}$ is distributed statistical distance at most $1 - \left(\frac{1-\varepsilon}{1+\varepsilon}\right)^2 \leq 4\varepsilon$ from uniform, as required.

Next, we consider the distribution of $-\mathbf{f}$ for fixed $\tilde{\mathbf{a}}$. Since choosing $\tilde{\mathbf{a}}$ fixes a value for $\mathbf{v}$, choosing a value for $\mathbf{f}$ fixes $\frac{1}{q}\mathbf{a}_H = \mathbf{v} - \mathbf{f} \bmod \Lambda^m$. It follows by summing over $\bar{\mathbf{f}}$ in Equation 3.1 that $-\mathbf{f}$ for any fixed $\tilde{\mathbf{a}}$ has distribution within statistical distance 2ε of $D_{\frac{1}{q}\Lambda^m - \bar{\mathbf{v}}, r}$, when r is sufficiently large.

Finally, we study the distribution of the error. Assume we begin with a sample from Π_{q,s,m,D_α} , say $(\mathbf{a}, b = \frac{1}{q}\langle \mathbf{a}, \mathbf{s} \rangle + e) \in \Lambda_q^m \times \mathbb{T}_{\Lambda^\vee}$. Recall for such a sample, $e \in \Lambda_\mathbb{R}$ is such that $e \sim D_\alpha$. Conditioning on some fixed $\tilde{\mathbf{a}}$, we set $\tilde{\mathbf{s}} = G\mathbf{s}$ and consider

$$\left(\tilde{b} - \frac{1}{q'} \langle \tilde{\mathbf{a}}, \tilde{\mathbf{s}} \rangle\right) \bmod \Lambda^\vee$$

Denote the vector of the i^{th} block of nd^2 entries of $\mathbf{f} \in \mathbb{R}^{mnd^2}$ by $\mathbf{f}_i \in \mathbb{R}^{nd^2}$ for $i = 1, \dots, m$. Since $\tilde{\mathbf{s}} = G\mathbf{s}$ and $\Lambda^\vee$ is a Λ -ideal, we have

$$\left(\tilde{b} - \frac{1}{q'} \langle \tilde{\mathbf{a}}, \tilde{\mathbf{s}} \rangle\right) = \sum_{i=1}^m \sigma_H^{-1}(-\mathbf{f}_i) \cdot s_i + \tilde{e} + e \bmod \Lambda^\vee.$$

Applying the canonical embedding, the error can be written

$$\sum_i^m -\mathbf{f}_i \cdot \sigma_H(s_i) + \sigma_H(\tilde{e}) + \sigma_H(e),$$

where $-\mathbf{f}_i \sim D_{\frac{1}{q}\Lambda - \bar{\mathbf{v}}_i, r}$, $\tilde{e} \sim D_{r\beta}$, and $e \sim D_\alpha$. We then rewrite $\sigma_H(\tilde{e})$ as $\sigma_H(\tilde{e}) = \sum_i \tilde{e}^i$, where

$\tilde{e}^i \sim D_{\gamma_i}$ such that $\gamma_i \geq r \max_{i,j,k} |\sigma_i(s_{j_k})|$ and $\sum_i \gamma_i^2 = r^2 \beta^2$. We then apply Lemma 3.4 to $\sum_{i=1}^m -\mathbf{f}_i \cdot \sigma_H(s_i) + \tilde{e}^i$, to find that the summands have distribution at most 4ϵ from $\Sigma_{\tilde{R}}$ with

$$\tilde{R}_{i\ell}^2 = r^2 \cdot \sum_{k=1}^d |\sigma_\ell(s_{i_k})|^2 + \gamma_i^2$$

and so the sum is $4m\epsilon$ from $\Sigma_{\alpha''}$ with

$$\alpha''^2 \leq r^2 \cdot \max_\ell \left(\sum_{i,k} |\sigma_\ell(s_{i_k})|^2 + \beta^2 \right).$$

Adding $\sigma_H(e)$ gives a final parameter of $\alpha'^2 \leq r^2 \max_\ell \left(\sum_{i,k} |\sigma_\ell(s_{i_k})|^2 + \beta^2 \right) + \alpha^2$. $\square$

Write $\Psi_{\leq \alpha}$ for the set of Gaussian distributions with diagonal covariance matrix of parameter $\mathbf{r}$ satisfying $r_i \leq \alpha$ for all i . In the corollary below, setting $m = k$ gives a reduction from CMLWE in rank m to CLWE.

Corollary 3.2. *Let $\Lambda \subset \mathcal{A} = (L/K, \theta, \gamma)$ be the natural order of a CDA with $[L : K] = d$, and let Λ have basis $\mathbf{B}$ in the canonical embedding. Let $\alpha > 0$. Let χ be a distribution satisfying*

$$\Pr_{s \leftarrow \chi} \left[\max_{i,j} |\sigma_i(s_j)| > B \right] \leq \delta$$

for some B and δ . Then for any $\epsilon \in (0, 1/2)$, any $k \geq 2$ dividing m , and

$$r \geq \frac{1}{q} \left\| \tilde{\mathbf{B}} \right\| \cdot \sqrt{2 \ln(2mnd^2(1 + 1/\epsilon)) / \pi},$$

there is an efficient reduction from $\Pi_{q,s,m,\Psi_{\leq \alpha}}$ with $s \leftarrow \chi^m$ to $\Pi_{q,s,m/k,\Sigma_R}$ with $s \leftarrow G \cdot \chi^m$ where $G = \mathbf{I}_{m/k} \otimes (1, q, \dots, q^{k-1}) \in \Lambda^{m/k \times m}$ and $R^2 = (d+1)mr^2B^2 + \alpha^2$ which reduces the advantage by at most $[1 - (1 - \delta)^{dm}] + (4m + 10)\epsilon d$.

Proof. Mutatis mutandis, identical to [8, Corollary 1], since our modules are $\mathbb{Z}$ -modules. $\square$

We note that when $d = 1$, CMLWE is simply MLWE, and moreover that in our corollary we obtain the same bound on the parameter as the corresponding result mapping MLWE to RLWE

in [8, Corollary 1].

3.6 Hardness of CLWE from One-Sided Ideal Lattices

In this section, we define lattice problems over one-sided ideals, and show that the hardness of search CLWE can be reduced to solving such lattice problems. Since the reduction from search CLWE to decision CLWE (restricting the secret appropriately) does not rely on any choice of ideal, we obtain the pseudorandomness of CLWE, for properly chosen secrets, from one-sided ideal lattices.

Lattice Problems from One-Sided Ideals

We embed one-sided ideals into $\mathbb{R}^{nd^2}$ exactly as in the two-sided case, and then define problems on these lattices. We make the ‘sidedness’ of the ideals in these problems explicit, although we may suppress this notation when context makes the situation clear. The below definitions are given for left ideals; the problems obtained from right ideals are defined entirely analogously.

Definition 50. Let $\mathcal{A}$ be a CDA and let $\mathcal{I}$ be some left ideal of the natural order Λ . Then, for an approximation factor $\xi = \xi(n) \geq 1$ the (approximate) Left-Ideal Shortest Vector Problem, denoted $\mathcal{A}\text{-SVP}_{\xi}^{\text{Left}}$, is to find a non-zero element $a \in \mathcal{I}$ such that $\|a\| \leq \xi \cdot \lambda_1(\mathcal{I})$, where as usual $\lambda_1(\mathcal{I})$ denotes the minimal length of elements of $\mathcal{I}$ in the appropriate norm.

Definition 51. Let $\mathcal{A}$ be a CDA, $\mathcal{I}$ a left ideal of Λ , and $\xi \geq 1$. Then the approximate Shortest Independent Vectors Problem $\text{SIVP}_{\xi}^{\text{Left}}$ is to find n linearly independent nonzero vectors $\mathbf{x}_1, \dots, \mathbf{x}_n$ such that $\max_i \|\mathbf{x}_i\| \leq \xi \cdot \lambda_n(\mathcal{I})$.

Definition 52. Let $\mathcal{A}$ be a CDA, let $\mathcal{I}$ be some left ideal of Λ , and let $0 < \delta < \lambda_1(\mathcal{I})/2$. Then the $\mathcal{A}\text{-BDD}_{\mathcal{I},\delta}^{\text{Left}}$ problem, on input $y = x + e$ for $x \in \mathcal{I}$ and $e \in \bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$ satisfying $\|e\| \leq \delta$, is to compute x .

Definition 53. Let $q \geq 2$. The $q\mathcal{A}\text{-BDD}_{\mathcal{I},d}^{\text{Left}}$ problem is, given an instance of the $\mathcal{A}\text{-BDD}_{\mathcal{I},\delta}^{\text{Left}}$ problem $y = x + e$ with solution $x \in \mathcal{I}$ and error $e \in \bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$ satisfying $\|e\|_{2,\infty} \leq \delta$, output

$x \bmod q\mathcal{I}$, where $\|e\|_{2,\infty} := \max_j \sqrt{\left(\sum_{i=0}^{d-1} |\sigma_j(e_i)|^2\right)}$.

Lemma 3.8. *For any $q \geq 2$ and one-sided ideal $\mathcal{I}$, there is a deterministic polynomial time reduction from $\mathcal{A}\text{-BDD}_{\mathcal{I},\delta}^{\text{Left}}$ to $q\mathcal{A}\text{-BDD}_{\mathcal{I},\delta}^{\text{Left}}$*

Proof. Lemma 3.5 from [136], which lifts since it is lattice preserving. $\square$

Definition 54. *We denote by $\mathcal{A}\text{-DGS}_{\xi}^{\text{Left}}$ the problem of sampling a discrete Gaussian $D_{\mathcal{I},\xi}$, where $\mathcal{I}$ is some left ideal of the natural order Λ .*

Technical Lemmas

Here we prove one-sided analogues of the ‘clearing out ideals’ lemma required for our proof, using the following lemma, which we restate for convenience:

Lemma 3.9. [71, Lemma 6/7] *Let q be unramified in L , $\mathcal{I}$ be an ideal of Λ , and $\mathcal{J} = q\Lambda$, where $q \in \mathbb{Z}$ is prime and $q\mathcal{O}_K = \prod_{i=1}^r \mathfrak{q}_i$ is a prime decomposition. Assume $\gamma \notin \mathfrak{q}_i$ for each i . Then there exists $t \in \mathcal{I} \cap \mathcal{O}_K$ such that $t\mathcal{I}^{-1}$ is coprime to $\mathcal{J}$, and we can compute such a t efficiently given $\mathcal{I}$ and the prime factorization of $\mathcal{J}$. Moreover if $\mathcal{P}$ is an arbitrary fractional ideal of Λ , the function $\chi_t : \mathcal{A} \rightarrow \mathcal{A}, x \mapsto t \cdot x$ induces a module isomorphism $\mathcal{P}/\mathcal{J}\mathcal{P} \rightarrow \mathcal{I}\mathcal{P}/\mathcal{I}\mathcal{J}\mathcal{P}$. When $\mathcal{J} = \langle q \rangle$ for a prime integer q we can efficiently compute the inverse.*

For a one-sided ideal $\mathcal{I} \subset \Lambda$, the *bound* of $\mathcal{I}$ is the largest two-sided ideal contained in $\mathcal{I}$. Every one-sided ideal of Λ contains such an ideal by Lemma 2.15.

Lemma 3.10 (Clearing Out Right Ideals with Appropriate Bound). *Let $\mathcal{I}$ be a proper integral right ideal of Λ with bound J , where J is coprime to the ideal $q\Lambda$, generated by a prime $q \in \mathbb{Z}$. Suppose q is unramified in $\mathcal{O}_K$. Then, the function $\chi_t : \mathcal{A} \rightarrow \mathcal{A}, x \mapsto t \cdot x$ induces a module isomorphism from $\mathcal{P}/\mathcal{P}q \rightarrow \mathcal{I}\mathcal{P}/\mathcal{I}\mathcal{P}q$, for some efficiently computable $t \in \mathcal{I} \cap \mathcal{O}_K$ and $\mathcal{P}$ any fractional ideal.*

Proof. Consider the following diagram:

$$\begin{array}{ccc}
J\mathcal{P} & \xrightarrow{\varphi_1} & J\mathcal{P}/J\mathcal{P}q \\
\downarrow \iota & & \downarrow f \\
\mathcal{I}\mathcal{P} & \xrightarrow{\varphi_2} & \mathcal{I}\mathcal{P}/\mathcal{I}\mathcal{P}q
\end{array}$$

where f is the map $x + J\mathcal{P}q \mapsto x + \mathcal{I}\mathcal{P}q$. Suppose f is not injective. Then there exists non-zero $x \in J\mathcal{P}/J\mathcal{P}q$ such that $f\varphi_2(x) = 0$. So $x \in J\mathcal{P} \cap \mathcal{I}\mathcal{P}q$. Since J and $q\Lambda$ are coprime, there exists a, b in $J, q\Lambda$ respectively such that $a+b = 1$. Then $x = 1 \cdot x = ax + bx$. Since $ax \in J \cdot \mathcal{I}q\mathcal{P} \subset Jq\mathcal{P}$ as J is two-sided and $\mathcal{I}$ is integral, and $bx \in q\Lambda \cdot J\mathcal{P} \subset qJ\mathcal{P}$, we have $x \in qJ\mathcal{P}$. But then x is zero in $J\mathcal{P}/J\mathcal{P}q$ - a contradiction. So f is injective.

We have the chain of maps $J\mathcal{P}/J\mathcal{P}q \hookrightarrow \mathcal{I}\mathcal{P}/\mathcal{I}\mathcal{P}q \subset \mathcal{P}/\mathcal{P}q$ between finite sets. Since J is two-sided, apply Lemma 4.4 to obtain $\chi_t : \mathcal{P}/\mathcal{P}q \cong J\mathcal{P}/J\mathcal{P}q$. Then we have an injection $f : J\mathcal{P}/J\mathcal{P}q \hookrightarrow \mathcal{I}\mathcal{P}/\mathcal{I}\mathcal{P}q$ between finite sets of equal size, so f must be a bijection. Then $f \circ \chi_t := \chi'_t$ is the required map. $\square$

Note that the above result only requires $\mathcal{P}$ to be a *left* fractional Λ -ideal. We state an analogous result on the right, which is proved nearly identically to Lemma 3.10:

Lemma 3.11. *Let $\mathcal{P}$ be a left Λ -ideal and right Γ -ideal. Let t be an element as above, and $\mathcal{I}$ an ideal with bound J as above. Then the map $\xi_t : \mathcal{P}/q\mathcal{P} \rightarrow \mathcal{P}\mathcal{I}/q\mathcal{P}\mathcal{I}$, induced by right multiplication by t , is a module isomorphism.*

SIVP^{Left}-to-Search CLWE Reduction

Below, we prove our reduction using the error distribution defined in Definition 42:

Lemma 3.12. *Let $\mathcal{I}$ be an integral right ideal with bound J as in Lemma 3.10. Then there is a ppt. algorithm that on input a prime $q \geq 2$, order-ideal $\mathcal{I}^\vee \subset \Lambda$, a $q\mathcal{A}$ -BDD $_{\mathcal{I}, \alpha q \cdot \omega(\sqrt{\log(nd)})/\sqrt{2ndr}}$ instance $y = x + e$ where $x \in \mathcal{I}^\vee$, a parameter $r \geq \sqrt{2}q \cdot \eta(\mathcal{I})$, and samples from the discrete Gaussian $D_{\mathcal{I}, r}$ outputs samples that are within negligible statistical distance of the CLWE distribution $\Pi_{q, s, \Sigma}$ for a secret $s = \chi'_t(x \bmod q\mathcal{I}^\vee) \in \Lambda_q^\vee$, where χ'_t is as in Lemma 3.10 and Σ is an*

error distribution such that when $|\gamma| = 1$, the distribution of the resulting error e'' is Gaussian and has Gaussian marginal distributions in each coordinate with parameters $r_{i,j} \leq \alpha$.

Proof. We follow the proof of [71, Lemma 11], making use of Lemma 3.10 to ensure s is uniform. By Lemma 4.4, compute an element $t \in J \cap \mathcal{O}_K$ to obtain χ'_t . Taking a $z \leftarrow D_{\mathcal{I},r}$ we create a CLWE sample by setting

$$(a, b) := \left(\chi_t'^{-1}(z \bmod q\mathcal{I}), (z \cdot y)/q + e' \bmod \Lambda^\vee \right) \in \left(\Lambda_q \times \left(\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}} \right) / \Lambda^\vee \right)$$

where $e' \leftarrow D_{\alpha/\sqrt{2}}$. For the same reasons given in [71], these samples are within negligible statistical distance of the CLWE distribution and s is uniformly random. First, note that $a \in \Lambda_q$ is statistically close to uniform. Since $r \geq q \cdot \eta(\mathcal{I})$, $z \bmod q\mathcal{I}$ is obtained with probability lying in $\left[\frac{1-\varepsilon}{1+\varepsilon}, 1\right] \cdot \beta$ for some $\beta > 0$. This then implies that the statistical distance between $z \bmod q\mathcal{I}$ and the uniform distribution is bounded by 2ε . Since $\chi_t'^{-1}$ is a bijection we conclude that $a = \chi_t'^{-1}(z \bmod q\mathcal{I})$ is at most statistical distance 2ε from uniform over Λ_q .

It remains to consider b . We show that it has the shape $(a \cdot s)/q + e''$ for an error e'' of the correct distribution, and uniformly random s . Observe that

$$\begin{aligned} b &:= (z \cdot y)/q + e' \bmod \Lambda^\vee \\ &= (z \cdot x)/q + (z \cdot e)/q + e' \bmod \Lambda^\vee. \end{aligned}$$

We now use ξ_t with $\mathcal{P} = \mathcal{I}^\vee$, using the fact ([139, §25, ex. 4]) that for one-sided ideal $\mathcal{I}$ with right order Λ , left order Γ , we have $\mathcal{I}^\vee = \Lambda^\vee \cdot \mathcal{I}^{-1} = \mathcal{I}^{-1} \cdot \Gamma^\vee$, and Lemma 3.11. We obtain $\xi_t : \mathcal{I}^\vee / \mathcal{I}^\vee q \rightarrow \mathcal{I}^\vee \mathcal{I} / \mathcal{I}^\vee \mathcal{I} q = \mathcal{I}^{-1} \Gamma^\vee \mathcal{I} / \mathcal{I}^{-1} \Gamma^\vee \mathcal{I} q \cong \Lambda^\vee / \Lambda^\vee q$, where the last isomorphism comes from Proposition 2.13. Since Λ is maximal, Γ is also maximal. Thus, since $z = t \cdot a \bmod \Lambda_q^\vee$, setting $s = t \cdot x$, if s is uniformly distributed over $\mathcal{I}_q^\vee$, it is uniformly distributed over $\Lambda_q^\vee$.

The distribution of the error can be analysed in the same way as in [71, Lemma 11]. $\square$

Lemma 3.13. *There is an efficient quantum algorithm that given an $N = nd^2$ dimensional lattice $L := \sigma_{\mathcal{A}}(\mathcal{I})$ corresponding to a one-sided ideal $\mathcal{I}$, a real $\delta < \lambda_1(L^\vee)/(2\sqrt{2nd})$, and an oracle that solves $\mathcal{A}\text{-BDD}_{L^\vee, \delta}$ with all but negligible probability, outputs an independent sample*

from $D_{L, \sqrt{d}\omega(\sqrt{\log(nd)})/\sqrt{2}\delta}$.

Proof. Regev's result in [136, Lemma 3.14], is lattice preserving, so it extends to ideal lattices from one-sided ideals. $\square$

We now directly follow the method of [71]: combine Lemmas 3.12 and 3.8 to reduce $\mathcal{A}$ -BDD to Search CLWE; use the reduction and Lemma 4.7 to create the iterative step, which reduces $\mathcal{A}$ -DGS to Search CLWE, and so arrive at the following:

Theorem 3.9. *Let $\mathcal{A}, \Lambda$ be as usual and $\alpha \in (0, 1)$ and $q \geq 2$ such that $\alpha q \geq \omega(1)$. Then there is a polynomial-time quantum reduction from $\mathcal{A}$ -SIVP $_{\xi}^{Left}$ to search-CLWE $_{q, \Sigma_{\alpha}}$ for any $\sqrt{8Nd} \cdot \xi = (\omega(\sqrt{dn})/\alpha)$.*

The search-to-decision reduction of [71] then connects worst-case one-sided ideal lattice problems with decision CLWE.

A One-Sided Ideal with Bound Coprime to $\langle q \rangle$

Suppose $\mathcal{A} = L \oplus uL$ and $[L : K] = 2$, for $K = \mathbb{Q}(\zeta_n)$ and L as usual, with $\gamma = \zeta_n$. Let $\mathfrak{p} \subset \mathcal{O}_L$ be a prime (hence maximal) ideal lying above $p \in \mathbb{Z}$. We will find a one-sided ideal of $\Lambda = \mathcal{O}_L \oplus u\mathcal{O}_L$ with bound coprime to $\langle q \rangle$, where q splits completely in K but its prime factors are inert in L , i.e. $q\mathcal{O}_K = \mathfrak{q}_1 \dots \mathfrak{q}_r$ and $\mathfrak{q}_i\mathcal{O}_L = \mathfrak{q}_i$, for $i = 1, \dots, r$. Set $\mathcal{I} = \mathfrak{p} \oplus u\theta(\mathfrak{p})$. Observe that if $a = a_1 + ua_2 \in \mathcal{I}$ and $b = b_1 + ub_2 \in \Lambda$, then

1. $a \cdot b = (a_1 + ua_2) \cdot (b_1 + ub_2) = a_1b_1 + \gamma\theta(a_2)b_2 + u(a_2b_1 + \theta(a_1)b_2) \in \mathfrak{p} \oplus u\theta(\mathfrak{p})$
2. $b \cdot a = (b_1 + ub_2) \cdot (a_1 + ua_2) = b_1a_1 + \gamma\theta(b_2)a_2 + u(b_2a_1 + \theta(b_1)a_2) \notin \mathfrak{p} \oplus u\theta(\mathfrak{p})$

In 1. we used the fact that $a_2 = \theta(c)$, for some $c \in \mathfrak{p}$, and $\theta^2 = e$, so that $\theta(a_2) = c$ and so lies in $\mathfrak{p}$. Thus $\mathcal{I}$ is a one-sided ideal.

In order for the largest two-sided ideal inside $\mathcal{I}$ to be coprime to $\langle q \rangle$, we proceed as follows: note that $\langle q \rangle = q\Lambda = q\mathcal{O}_L \oplus uq\mathcal{O}_L = \mathfrak{q}_1 \dots \mathfrak{q}_r \oplus u\mathfrak{q}_1 \dots \mathfrak{q}_r$. Thus $q^r \in \langle q \rangle$. If we take $\mathfrak{p}$ as above, such

that it lies above $p \in \mathbb{Z} : p \neq q$, then $p \in \mathcal{I}$. Let $J \subset \mathcal{I}$ be the bound of $\mathcal{I}$. Since $\mathcal{I} \cap \mathcal{O}_L = \mathfrak{p}$, we must have $J \cap \mathcal{O}_L \subset \mathfrak{p}$, and $p^s \in J$ for some s . Since $\gcd(q^r, p^s) = 1$, we must have (by Bezout's theorem) $m, n \in \mathbb{Z} : mq^r + np^s = 1$, and so $\langle q \rangle + J = \Lambda$.

This approach generalises to any dimension d . If $\mathcal{A} = L \oplus uL \oplus \dots \oplus u^{d-1}L$, then setting $\mathcal{I} = \sum_{i=0}^{d-1} u^i \theta^i(\mathfrak{p})$ gives a right ideal inside the natural order.

An alternative method is the following: set $x = a + ub \in \Lambda$ such that $a \in \mathcal{O}_K$, and consider the left ideal generated by x , Λx . This contains $(a - ub)x = a^2 - \gamma\theta(b)b + u(-ba + \theta(a)b) = a^2 - \gamma\theta(b)b + u((\theta(a) - a)b) = a^2 - \gamma\theta(b)b \in \mathcal{O}_K$.² If a and b are chosen such that $\gcd((a^2 - \gamma\theta(b)b)\mathcal{O}_K, q\mathcal{O}_K) = 1$, then since the bound of Λx , say J_x , contains $(a^2 - \gamma\theta(b)b)\mathcal{O}_K$, then J_x is coprime to $q\Lambda$. Indeed, suppose $J_x + q\Lambda \subset \mathcal{M}$ for some maximal left ideal $\mathcal{M}$. Then $\mathcal{M}$ contains $(a^2 - \gamma\theta(b)b)\mathcal{O}_K$ and $q\mathcal{O}_K$, so contains 1 - but this is a contradiction. So for a and b chosen as described, Λx is a one-sided ideal with bound coprime to $q\Lambda$.

3.7 Chapter Summary

We first clarified the existing security proof for CLWE, showing that it only gives as strong a guarantee as SIVP from $\mathcal{O}_L$ -ideals. This was achieved by extending the ideal theory of two-sided Λ -ideals, when γ is a unit. We then showed that a CLWE oracle is sufficient to solve $q\text{Mod-BDD}$, that for a change of modulus CLWE is equivalent to a module form of CLWE, and that CLWE is at least as hard as lattice problems on one-sided ideals, a larger family of problems than those from the two-sided ideals.

One might hope that objects such as one-sided ideals of CDAs, introduced to lattice cryptography here, and which enjoy novel properties compared to two-sided ideals of number fields, might have properties relevant to security or to developing new functionalities from CDAs which are unobtainable in the rank one case; we leave such exploration as a future research topic.

²Note this value is $\det(\phi(x))$.

Chapter 4

Families of Algebras for CLWE

4.1 Introduction

Having re-evaluated and reasserted the security of CLWE in the previous chapter, in this chapter we continue the development of CLWE. In particular, we discuss the construction of CDAs, parameterised by γ , and the resulting structured LWE instances obtained from such CDAs, thus focusing on the creation of *non-norm elements*. The contributions of this chapter in this direction are three-fold:

1. We generalize Theorem 1 from [71] to increase the number of valid CDAs for CLWE, and give concrete examples of such algebras. Namely, we prove that the method used in [71] to construct CDAs over cyclotomic fields of prime-power conductor holds for cyclotomic fields of *any* conductor n . We then discuss obtaining appropriate prime moduli for the CLWE problem. For RLWE, one chooses a prime completely split in a given number field; for CLWE, one has further constraints on the choice of prime, which we often want to split in an extension also. We give methods for finding such primes, and give examples of algebras together with appropriate moduli for CLWE.
2. We then consider CDAs constructed from fractional values of γ , that is, $\gamma \in K \setminus \mathcal{O}_K$. Since we want to preserve the geometry induced by our choice of norm, we study fractional

unit-magnitude non-norm elements in finite extensions of cyclotomic fields, extending the state-of-the-art method for finding such elements to any finite extension L/K . We then study CLWE in such algebras, giving a reduction from SIVP to the search CLWE problem for arbitrary maximal orders.

3. Finally, we consider the scenario $\gamma \in \mathcal{O}_L \setminus \mathcal{O}_K$. In this instance, the resulting algebras $\mathcal{A} = (L/K, \theta, \gamma)$ are nonassociative. These objects were introduced by Waterhouse [171] in the quaternionic case and Steele [152] more generally (or, seen as quotients of skew polynomial rings, descend from [129]). We prove results on the ideal theory of natural orders in such algebras, before defining LWE in such spaces and providing security reductions, and further discussion of nonassociative LWE. This includes the fundamental result that multiplication of ideals in the natural order Λ is not only associative but also commutative, when γ is a unit. It will turn out that constructing CDAs in this setting is quite simple.

4.2 Non-Norm Elements for General Cyclotomic Fields

In [71], the authors used the work of [95] to construct CDAs containing n th roots of unity for prime-power n . Recall the method runs as follows: let $n = p^r$ for some prime p and $r \in \mathbb{N}$, and set $K = \mathbb{Q}(\zeta_n)$. Let $\ell = 1 \bmod n$, $\ell \neq 1 \bmod pn$ be a prime, and set $M = \mathbb{Q}(\zeta_n, \zeta_\ell) = \mathbb{Q}(\zeta_{n\ell})$. One then fixes a subfield of degree d over K inside M by taking the fixed field of σ^d , where d divides n and $\text{Gal}(M/K) = \langle \sigma \rangle$, and the resulting algebra $(L/K, \theta, \zeta_n)$ is division, where $\text{Gal}(L/K) = \langle \theta \rangle$ - that is to say, ζ_n is non-norm. In this section, we extend this method to composite n . The main result of this section is the following theorem:

Theorem 4.1. *Let $n \in \mathbb{N}_{\geq 2}$. Set $K = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n th root of unity. Then there exist infinitely many cyclic Galois extensions L/K of degree n such that ζ_n satisfies the non-norm condition.*

Proof. Write $n = p_1^{e_1} \dots p_k^{e_k}$, for $p_1, \dots, p_k$ pairwise coprime. Pick $\ell \in \mathbb{Z}$ prime such that $p_1^{e_1} \dots p_k^{e_k} \mid \ell - 1$, and such that e_i is the highest power of p_i such that this is true, for all i , so we have

$\ell - 1 = p_1^{e_1} \dots p_k^{e_k} p_{k+1}^{e_{k+1}} \dots p_r^{e_r}$ for some primes $p_{k+1}, \dots, p_r$ distinct from the p_j for $1 \leq j \leq k$, and integers e_i . By Theorem 2.1, there are infinitely many such primes q . Note that $\gcd(n, \ell) = 1$. Now consider $M = K(\zeta_\ell) = \mathbb{Q}(\zeta_n, \zeta_\ell)$. We have $\text{Gal}(M/K) \cong C_{\ell-1}$. Let σ be a generator of $\text{Gal}(M/K)$. Then σ^n fixes an extension, denoted L , of degree n over K . We have $\text{Gal}(L/K) \cong \text{Gal}(M/K) / \text{Gal}(M/L)$, which implies that $\text{Gal}(L/K)$ is also cyclic. We will use Theorem 2.2 to prove the result by localizing at a certain prime ideal. Let the prime ideal $\mathbf{Q}$ lie above $\mathbf{\Omega}$ lie above $\mathbf{q}$ lie above ℓ in the tower of fields $M/L/K/\mathbb{Q}$. Proposition 2.2 implies that the inertial degree $f_{\mathbf{q}|\ell} = 1$. This is equivalent to $[\mathcal{O}_K/\mathbf{q} : \mathbb{F}_\ell] = 1$.

Now, $\ell \mid n\ell$ exactly once, since $\gcd(\ell, n) = 1$. Then $f_{\mathbf{Q}|\ell}$ is the smallest f such that $\ell^f \equiv 1 \pmod{n}$. But $\ell \equiv 1 \pmod{n}$, so $f_{\mathbf{Q}|\ell} = 1$. Since the inertial degree is multiplicative, we have $f_{\mathbf{Q}|\ell} = f_{\mathbf{Q}|\mathbf{q}} f_{\mathbf{q}|\ell}$ and so $f_{\mathbf{Q}|\mathbf{q}} = 1$ also. We have worked out $f_{\mathbf{Q}|\mathbf{q}}$ by considering the tower $M/K/\mathbb{Q}$. We now consider the tower $M/L/K$, which tells us that $f_{\mathbf{Q}|\mathbf{q}} = f_{\mathbf{Q}|\mathbf{\Omega}} f_{\mathbf{\Omega}|\mathbf{q}}$. Multiplicativity of the inertial degree tells us that $f_{\mathbf{Q}|\mathbf{q}} = 1$ implies $f_{\mathbf{\Omega}|\mathbf{q}} = 1$ also.

Denote the completions of the fields L , K , and $\mathbb{Q}$ by the corresponding valuations by $L_{\mathbf{\Omega}}$, $K_{\mathbf{q}}$, and $\mathbb{Q}_\ell$ respectively. Then, since $g = 1$ in extensions of local fields, we combine this with the above discussion on the inertial degrees to conclude that $L_{\mathbf{\Omega}}/K_{\mathbf{q}}$ is totally ramified. Further, since the characteristic of the residue field of $K_{\mathbf{q}}$ is ℓ , but total ramification of $L_{\mathbf{\Omega}}/K_{\mathbf{q}}$ means that the ramification index $e_{L_{\mathbf{\Omega}}/K_{\mathbf{q}}} = [L_{\mathbf{\Omega}} : K_{\mathbf{q}}] = n$, we obtain that $L_{\mathbf{\Omega}}/K_{\mathbf{q}}$ is tamely ramified. Using the local reciprocity map, we obtain $[K_{\mathbf{q}}^\times : N_{L_{\mathbf{\Omega}}/K_{\mathbf{q}}}(L_{\mathbf{\Omega}}^\times)] = |\text{Gal}(L_{\mathbf{\Omega}}/K_{\mathbf{q}})| = [L_{\mathbf{\Omega}} : K_{\mathbf{q}}] = n$. Moreover, a standard result of local fields is that for a totally and tamely ramified finite extension of local number fields, $N_{L_{\mathbf{\Omega}}/K_{\mathbf{q}}}(L_{\mathbf{\Omega}}^\times)$ contains a uniformizer $\pi_{\mathbf{q}}$ of $K_{\mathbf{q}}$, as well as $U_{\mathbf{q}}^1$ (see [64, page 115]). Pulling together the above in conjunction with the local reciprocity map, we obtain the following commutative diagram:

$$\begin{array}{ccc}
 \mu_{\ell-1} & \xrightarrow{f} & \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{e_k}\mathbb{Z} \\
 \downarrow h & \nearrow g & \\
 K_{\mathbf{q}}^\times & &
 \end{array} \tag{4.1}$$

Here g is the homomorphism defined by the local reciprocity map, with kernel $N_{L_{\mathbf{\Omega}}/K_{\mathbf{q}}}(L_{\mathbf{\Omega}}^\times)$ and

image $\text{Gal}(L_{\Omega}/K_{\mathfrak{q}}) \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{e_k}\mathbb{Z}$, h is the inclusion of $\mu_{\ell-1}$ into $K_{\mathfrak{q}}^{\times} \cong \mu_{\ell-1} \times \langle \pi_{\mathfrak{q}} \rangle \times U_{\mathfrak{q}}^1$, and f is the natural surjection from the CRT decomposition of $\mu_{\ell-1} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{e_k}\mathbb{Z} \times \mathbb{Z}/p_{k+1}^{e_{k+1}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_r^{e_r}\mathbb{Z}$ onto $\mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{e_k}\mathbb{Z}$.

We have $f = g \circ h$, where f, g and h are all homomorphisms. Since f maps elements of order dividing n non-trivially, by commutativity of the diagram g also maps such elements non-trivially, so they are not contained in $\ker(g)$. But by the local reciprocity map, $\ker(g) = N_{L_{\Omega}/K_{\mathfrak{q}}}(L_{\Omega}^{\times})$; and so $\zeta_n^i \notin N_{L_{\Omega}/K_{\mathfrak{q}}}(L_{\Omega}^{\times})$, for $0 < i < p_1^{e_1} \dots p_k^{e_k}$, as required. The Hasse norm theorem gives the result. $\square$

Corollary 4.1. *Let $n = p_1^{e_1} \dots p_k^{e_k}$ and $K = \mathbb{Q}(\zeta_{p_1^{e_1} \dots p_k^{e_k}})$, where the p_i are pairwise coprime. There exists a cyclic Galois extension E/K of any index d dividing n , such that ζ_n is non-norm in E/K , i.e. ζ_n is not a norm for $0 < i < d$.*

Proof. Mutatis mutandis, identical to [71]. $\square$

These results allow us to create many new CDAs with roots of unity as non-norm elements.

We give two examples.

Examples

1. Set $n = 3^2 \cdot 2^6 = 576$. Note $\ell = 577$ is prime, and $\ell - 1 = 576$ is divisible by 576, with neither 27 nor 128 dividing $\ell - 1$. So 577 satisfies the conditions of Theorem 4.1. Observe $M := \mathbb{Q}(\zeta_n, \zeta_{\ell}) = \mathbb{Q}(\zeta_{576}, \zeta_{577})$ is an extension of $K := \mathbb{Q}(\zeta_{576})$ of degree 576. Let $\text{Gal}(M/K) = \langle \sigma \rangle$. Then, as in the proof above, $\sigma^n = \sigma^{576} = e$ fixes an extension of degree $n = 576$ over K - in this case the extension is M itself. By the theorem ζ_{576} is a non-norm element in $\mathbb{Q}(\zeta_{576}, \zeta_{577})/\mathbb{Q}(\zeta_{576})$. Apply Corollary 4.1 to fix a degree 2 cyclic Galois extension of K , denoted E , which is possible since 2 divides 576. This extension also has the property that ζ_{576} is a non-norm element over K . Let $\text{Gal}(E/K)$ be generated by θ . Then the cyclic algebra $(E/K, \theta, \zeta_{576})$ has dimension $2^2 \cdot 192 = 768$ over $\mathbb{Q}$, and is division.

2. Set $n = 3^3 \cdot 2^5 = 864$. Note that $\ell = 16,417$ is prime, $16,416 \equiv 0 \pmod{864}$, and neither 81 nor 64 divide $\ell - 1 = 16,416$. So ℓ satisfies the required properties to apply Theorem 4.1. Observe $M := \mathbb{Q}(\zeta_n, \zeta_\ell) = \mathbb{Q}(\zeta_{864}, \zeta_{16,417})$ is a cyclic extension of $K := \mathbb{Q}(\zeta_{864})$, of degree 16,416. Let $\text{Gal}(M/K) = \langle \sigma \rangle$. Then, as in the proof above, $\sigma^n = \sigma^{864}$ fixes an extension of degree $n = 864$ over K , denoted L . The theorem indicates that ζ_{864} is a non-norm element in $L/\mathbb{Q}(\zeta_{864})$. We can then apply Corollary 4.1 to fix a cyclic Galois extension of K of degree 2 over K , since 2 divides 16,416. This extension also has the property that ζ_{864} is a non-norm element over K . Call this extension E and let $\text{Gal}(E/K) = \langle \theta \rangle$. Then the cyclic algebra $(E/K, \theta, \zeta_{864})$ has dimension $2^2 \cdot 288 = 1152$ over $\mathbb{Q}$, and is division.

Maximality of the Natural Order

We note that [71, Theorem 3] states that the natural order in the above prime-power case ($n = p^r$) is maximal. It can be shown with an identical proof that when one takes $n = p_1^{a_1} \dots p_l^{a_l}$, as long as ℓ satisfies $\ell \equiv 1 \pmod{n}$ and $p_i n \nmid \ell - 1$ for $i = 1, \dots, l$, the result still holds: note that the ramification of ideals above ℓ in $\mathcal{O}_K$ in $\mathcal{O}_M$ is the same as before (since the inertial degree depends on $\ell \equiv 1 \pmod{n}$ to equal 1), the ramification index is $\phi(\ell)$, and $g_{M/K} = [M : K]/\phi(\ell) = 1$; this can be summarised by noting that the relevant properties depend on the prime ℓ , and not the degree of K . However, if γ is not a unit, the natural order is not (in general) maximal.

4.2.1 Cryptographic Moduli for CDAs from Composite Cyclotomics

Here we provide methods to find the primes needed to construct CDAs over cyclotomic fields of composite conductor for CLWE, and give concrete examples. To build algebras meeting the requirements of the previous theorem, we need to find a small degree extension L of $K = \mathbb{Q}(\zeta_n)$ and a non-norm element for L/K . As explained above, this is done by taking a large prime ℓ satisfying certain conditions, taking the compositum of K and $\mathbb{Q}(\zeta_\ell)$, and taking an intermediate extension L of K of the desired degree. If chosen well, ζ_n will be a non-norm element.

Recall that ℓ must satisfy two conditions: firstly, that $\ell \equiv 1 \pmod{n}$, and secondly, that $\ell \neq$

$1 \bmod p_i \cdot n$, for $i = 1, \dots, k$, where p_i is a prime in the prime factorization of $n = p_1^{e_1} \dots p_k^{e_k}$. We can find such an ℓ by considering the arithmetic progression $1 + p_1^{e_1} \dots p_k^{e_k} + \sum_{i=0}^m p_1^{e_1+1} \dots p_k^{e_k+1}$, for $m = 0, 1, 2, \dots$. Theorem 2.1 implies there are infinitely many primes in this progression, and for our parameters searching elements in the progression can be done efficiently.

Similarly to RLWE [102]¹, the security proof of CLWE holds for primes q completely split in $\mathcal{O}_K$. Moreover, to enable efficient multiplication, it will be convenient to have q also completely split in L . We can use the fact that if q splits completely in M , it splits completely in all subfields. Thus the most naive approach to find a prime that splits completely in L and K is to find a prime that splits completely in $M = \mathbb{Q}(\zeta_{n\ell})$. This is equivalent to $q \equiv 1 \bmod \ell n$.

This approach is limited, however. Since $\ell \equiv 1 \bmod n$, we have $\ell > n$; since $q \equiv 1 \bmod \ell n$, we have $q > \ell n > n^2$. In general, we want $[K : \mathbb{Q}] = \phi(n)$ to be large, and $[L : K]$ small. As we want q not to be too large, this forces n to be small. Moreover, the larger n gets, the smaller ℓ is required to be. For example, take $n = 100$. Then $[K : \mathbb{Q}] = 40$, and, if we can find an appropriate non-norm element, we could take a degree 5 extension of K for an algebra of degree 1000 over $\mathbb{Q}$. 101 is prime, so we can take $\ell = 101$; then we have $q \geq 100 \cdot 101 + 1 = 10101$. Since 10101 is not prime, the next smallest possible option for q is $2\ell n + 1 = 20203$, which is also not prime. The search continues in this manner, with the size of q rapidly growing.

The Quadratic Case

We first consider extensions L/K of degree 2, and write L as the compositum of K and a quadratic subfield E of $E' := \mathbb{Q}(\zeta_\ell)$. Since E' is cyclotomic with prime conductor, E is the *unique* quadratic subfield of E' . This can be written explicitly as follows [87, Theorem 9.3]:

$$E = \begin{cases} \mathbb{Q}(\sqrt{\ell}), & \text{if } \ell \equiv 1 \bmod 4 \\ \mathbb{Q}(\sqrt{-\ell}), & \text{if } \ell \equiv 3 \bmod 4. \end{cases}$$

The discriminant of this field, d_E , is also well known, being $d_E = \ell$ if $\ell \equiv 1 \bmod 4$, else $d_E = 4\ell$ if $\ell \equiv 3 \bmod 4$. A final fact is that a prime q splits completely in E if and only if d_E is a quadratic

¹Subsequent works have allayed this restriction on the modulus.

residue modulo q , i.e. there exists $x \in \mathbb{Z}/q\mathbb{Z}$ such that $d_E \equiv x^2 \pmod{q}$ [112, Proposition 8.5].

A prime q splits in L if and only if q splits in both K and E . Thus to find primes that split in both L and K we search for primes q such that $q \equiv 1 \pmod{n}$, with d_E becoming a quadratic residue modulo q . Finally, to ensure we can find non-norm elements, we require that $\gcd(n, 2) \neq 1$ (cf. [71, Theorem 10]).

Here we run through an example. Set $n = 320$. With $d = 2$, we would obtain a degree 512 algebra. Since $1601 \equiv 1 \pmod{320}$ and is prime, we can set $\ell = 1601$. Then $\ell \equiv 1 \pmod{4}$, so $d_E = \ell = 1601$. There are many primes in the required range that are congruent to 1 mod 320 and have d_E as a quadratic residue; for example, 4481 suffices. It is prime, and $4481 = 320 \cdot 14 + 1$. Furthermore, we have $1213^2 \equiv 1601 \pmod{4481}$. Below is a table of results for quadratic extensions of $\mathbb{Q}(\zeta_n)$. Listed are n , $[\mathcal{A} : \mathbb{Q}]$, ℓ , example value(s) of q , and ‘min log rop’. This last quantity is obtained by running the lattice estimator² [9] with similar parameters for the secret, error, and default number of samples as Kyber512, but replacing the lattice dimension and modulus with the corresponding entries of the table. We list the minimum of the base-2 logarithms, over the given values of q in the row. The ‘meaning’ of the rop results is to give a general idea of the number of ring operations required to solve the corresponding LWE instances, and is thus a measure of security.

n	$[\mathcal{A} : \mathbb{Q}]$	ℓ	q	min log rop
320	512	1601	4481, 7681, 9601, 13121	120.6
324	432	1621	3889, 6481, 8101, 10369	104.9
352	640	353	3169, 6337, 11617, 13729	151.2
400	640	401	4001, 4801, 14401	150.5
432	576	433	3889, 8209, 12097, 15121	133.8
448	768	449	4481, 8513, 10753	190.6
484	880	1453	3389, 11617, 13553, 15973	215.9
576	768	577	7489, 10369, 13249, 14401	185.0
640	1024	641	7681, 9601, 12161, 13441	265.3
648	864	7129	3889, 6481, 9721, 10369	220.2
864	1152	2593	3457, 10369	316.4

Table 4.1: The ‘Naive’ Quadratic Case

We note in passing that for quadratic extensions of cyclotomics of the kind considered here,

²Commit 564470e.

$\mathcal{O}_L$ has the form $\mathcal{O}_L = \mathbb{Z}[\zeta_n, \frac{1+\sqrt{\ell}}{2}]$. It was shown in [124] and [45] that PLWE instantiated in such rings, when n is prime, can be insecure if insufficient attention is paid to the choice of error distribution. We note that our above choices do not include any prime n , but we leave the precise analysis of the mentioned papers' methods in our context for future research.

The Naive Method for Higher Values of d

In this section we address extensions L such that $[L : K] > 2$. Unlike in the quadratic case we cannot, in general, write down explicitly what a low-degree subfield of $\mathbb{Q}(\zeta_\ell)$ is. We return to the naive method explained above, finding $q \equiv 1 \pmod{\ell n}$. Though cumbersome, one can still obtain some limited results by this method, although the resulting algebras are slightly small since the largest n that can be taken is 141, if one imposes, say, $q < 20000$. A simple method to find appropriate values of ℓ is to fix prime ℓ and set $n = \ell - 1$. Some results are below:

n	d	$[\mathcal{A} : \mathbb{Q}]$	ℓ	q	min log rop
25	5	500	101	5051	130.5
52	6	864	53	8269	225.2
58	6	1008	59	10267	267.0
60	6	720	61	7321	184.0
66	6	720	67	4423	194.4
78	6	936	79	6163	256.0
82	4	640	83	13613	151.3
82	6	1440	83	13613	414.7
138	4	704	139	19183	162.7

Table 4.2: The 'Naive' Case for $d > 2$

Refined Naive Method

There is, however, a refinement on the above method, by which we relax the condition that $q \equiv 1 \pmod{\ell n}$. Again write L as the compositum of K and a subfield E of $E' = \mathbb{Q}(\zeta_\ell)$. Since $\ell > 2$ is prime, the maximal real subfield $E'^+ = \mathbb{Q}(\zeta_\ell + \zeta_\ell^{-1})$ of E' has degree $\frac{\ell-1}{2}$ over $\mathbb{Q}$, and Galois group isomorphic to $\text{Gal}(E'/\mathbb{Q})/\{\pm 1\}$. The primes that ramify in E'^+ are the primes dividing the discriminant of E' , which is only ℓ . This makes it easy to select unramified primes.

The inertial degree is also well known in the maximal real subfield: it is the smallest integer f such that $q^f \equiv \pm 1 \pmod{\ell}$. So if our extension E is contained in E'^+ , we need to find prime q such that $q \equiv \pm 1 \pmod{\ell}$ and $q \equiv 1 \pmod{n}$.

So which subfields are contained in E'^+ ? Since $\text{Gal}(E'/\mathbb{Q})$ is cyclic and $\text{Gal}(E'/E'^+)$ is one of its subgroups, $\text{Gal}(E'/E'^+)$ is cyclic, so the quotient of the two groups is cyclic and isomorphic to $\text{Gal}(E'^+/\mathbb{Q})$, which has order $\frac{\ell-1}{2}$. The subgroups of a cyclic group $\mathbb{Z}/m\mathbb{Z}$ are the divisors d of m , and there is a single subgroup of order d for each divisor. Thus, in the Galois group of $E'^+/\mathbb{Q}$, there is a subgroup for each divisor of $\frac{\ell-1}{2}$; moreover, by the Galois correspondence, there is a unique Galois subfield of E'^+ with degree over $\mathbb{Q}$ equal to that divisor. Since this is also a subfield of E' , which has cyclic Galois group, this subfield is also the unique subfield of the given degree in E' . Note also that if d is an odd divisor of $\ell - 1$, it is also an odd divisor of $\frac{\ell-1}{2}$. Therefore every odd-degree Galois subfield of a prime cyclotomic field is totally real.

In light of this, our approach is as follows: we look for small values of n , so that we can find small values of ℓ , and hence find a value of q in the appropriate range. We will also look for values of ℓ such that our desired values of $d = [L : K]$ divide $\frac{\ell-1}{2}$, so that E will be totally real and we can apply this ‘refined naive method’ in our hunt for q . A final constraint to note is that we must have $\gcd(n, d) \geq 2$, else we will not have ζ_n be a non-norm element.

Here we run through the previous example again. We have $n = 100$, $[K : \mathbb{Q}] = 40$, and want a degree 5 extension of K to obtain an algebra of degree 1000 over $\mathbb{Q}$. 101 is prime, so we can take $\ell = 101$. This time, instead of requiring $q \equiv 1 \pmod{\ell n}$, we need $q \equiv \pm 1 \pmod{\ell}$ and $q \equiv 1 \pmod{n}$. Note that $5 \mid \frac{101-1}{2} = 50$, so a subfield of degree 5 of the maximal totally real subfield exists. One finds that 10301 satisfies both of these conditions: $10301 = 100 \cdot 103 + 1$, and $10301 = 101 \cdot 102 - 1$. Furthermore, 10301 is of the appropriate size; where the naive method failed, the tweaked version yielded a small prime.

Below is a table, Table 4.3, giving examples of valid primes using this method. Listed are n , the degree $d = [L : K]$, $[\mathcal{A} : \mathbb{Q}]$, and possible values for ℓ and q .

n	d	$[\mathcal{A} : \mathbb{Q}]$	ℓ	q	min log rop
32	5	400	97	18913	91.8
45	5	600	181	16651	138.4
60	6	576	61	7331	144.3
70	5	600	71	9941	145.9
70	7	1176	71	9941	326.3
88	4	640	89	8009	159.9
90	5	600	2791	5581	155.2
100	5	1000	101	10301	264.1
102	3	288	103	10711	72.1
130	5	1200	131	17291	318.7

Table 4.3: The Refined ‘Naive’ Case for $d > 2$

n	$[\mathcal{A} : \mathbb{Q}]$	ℓ	x	q	min log rop	n	ℓ	x	q	min log rop
111	648	4441	2152	12211	155.1	128	2689	275	3329	304.8
171	972	6841	2112	3079	291.8	128	641	147	3457	303.8
183	1080	8053	1422	7321	301.1	128	3457	780	4481	295.7
201	1188	4423	2246	4021	363.9	128	12161	10957	4993	292.3
360	864	2521	461	6121	232.3	128	4481	571	6529	287.8

Table 4.4: The Cubic Case

Table 4.5: The Quartic Case

Completely Splitting Primes in Subfields of Cyclotomics

We now consider primes in subextensions of higher degree. The results in Tables 4.4 and 4.5 are based off the following theorem:

Theorem 4.2. *[105, Theorem 30] Let ℓ be a prime, $E' = \mathbb{Q}(\zeta_\ell)$, and denote its unique subfield of degree d over $\mathbb{Q}$ by E'_d . Let q be a prime coprime to ℓ . Then q splits completely in E'_d if and only if q is a d th power modulo ℓ .*

This allows us to generalize the method of the quadratic case to larger degree subfields of E' . As examples, we list some results for cubic and quartic extensions of K : we list, in addition to the previous values, the value of x for which $q \equiv x^d \pmod{\ell}$. We illustrate the quartic case with extensions of $\mathbb{Q}(\zeta_{128})$, which yields $[\mathcal{A} : \mathbb{Q}] = 1024$. Our results comprise tables 4.4 and 4.5.

4.3 CLWE with Fractional Non-norm Element

We now turn to non-integral values of γ . The main cryptographic contribution of this section is to give a security reduction from SIVP on ideal lattices of maximal orders of CDAs for a much wider class of algebras than was given in [71]. We do this to enable greater design flexibility for CLWE, and to hedge against cryptanalysis of the highly structured algebras currently used for CLWE. We consider algebras of the form $\mathcal{A} = (L/K, \theta, \gamma)$, where K is the n th cyclotomic field, not necessarily of prime power n , and γ is an element in K , with $|\gamma| = 1$ (here $|\cdot|$ is any complex absolute value of K), satisfying the property that γ^i is not in $N_{L/K}(L^*)$, where $N_{L/K}$ is the field norm, for $0 < i < [L : K]$. In particular we prove the following:

Main Result (Corollary 5, informal). *Let $\mathcal{A} = (L/K, \theta, \gamma)$ be a CDA as in the above paragraph, $\mathcal{O} \subset \mathcal{A}$ a maximal order, and q be an unramified prime in L . Then there is a polynomial-time quantum reduction from SIVP on ideal lattices in $\mathcal{O}$ to search CLWE, for certain parameters.*

The constraint that $|\gamma| = 1$ arises to ensure that the geometry of the ideal lattices is tractable to our methods. In order to create useful algebras for CLWE, we adapt methods from coding theory to build such ‘unit-magnitude fractional non-norm elements’ for extensions L/K of cyclotomic fields. These methods were originally developed to create such elements in low-dimensional instances, and we extend them to hold for extensions of L/K for *any* cyclotomic K and an extension L of any degree $[L : K]$. This is the section’s principal mathematical contribution. In particular, the key prior result in this direction is the following, extracted from [121]:

Theorem 4.3. *[121, Appendix] Let $K \in \{\mathbb{Q}(i), \mathbb{Q}(\omega)\}$ and L be a finite cyclic Galois extension of K . If q is a prime which splits into two ideals in K which are inert in L , the ratio of the generating elements of the $\mathcal{O}_K$ -ideals above q satisfies the non-norm condition.*

We obtain the following result, valid not just for cyclotomic fields with ring of integers which are principal ideal domains, but for infinitely many cyclotomics. Below, an ideal is taken to have the form $\mathfrak{q} = (q, \alpha)$ for some element α and $q \in \mathfrak{q} \cap \mathbb{Z}$:

Theorem 4.4. *(Corollary 4, informal) Let K be a cyclotomic field and L/K a degree n Galois extension. If q is a prime such that*

1. q is unramified in $\mathcal{O}_K$,
2. q splits into at least two ideals in $\mathcal{O}_K$, and they are inert in $\mathcal{O}_L$, and
3. the prime ideals above q in $\mathcal{O}_K$ are permuted by the automorphism corresponding to complex conjugation,

then the ratio of a non-integer generating element of any of the $\mathcal{O}_K$ -ideals with its complex conjugate satisfies the non-norm condition for L/K .

Using this result, we can create non-norm elements, and hence CDAs, which are useful for CLWE instantiations. We note here in passing that algorithms to compute maximal orders in CDAs exist, for example [86], [167]. We also observe that much work has been done on creating unit-magnitude integral non-norm elements; see, for example, [166], [78], [20]. Much of this was done to construct space-time block codes, for which noncommutative CDAs were introduced to coding theory in [145]. Regarding fractional non-norm elements, see [121], [65].

4.3.1 Preliminaries

Non-norm Elements

Recall that we call an element of K at which surjectivity of the norm map fails a *non-norm element*; formally,

Definition 55. *An element $x \in K$ is non-norm if there exists no $y \in L$ such that $N_{L/K}(y) = x$. We say x satisfies the non-norm condition if every power x^i for $0 < i < [L : K]$ is non-norm.*

Proposition 4.1. *Let γ be a non-norm element of L/K and $\sigma \in \text{Gal}(L/K)$. Then γ^{-1} and $\sigma(\gamma)$ are also non-norm elements.*

Proof. Suppose γ is a non-norm element and that γ^{-1} is the norm of an element of L , e.g. $\gamma^{-1} = N_{L/K}(x)$ for some $x \in L$. Then $N_{L/K}(x^{-1}) = N_{L/K}(x)^{-1} = (\gamma^{-1})^{-1} = \gamma$, a contradiction. Suppose there exists $x \in L$ such that $N_{L/K}(x) = \prod_{\sigma \in \text{Gal}(L/K)} \sigma(x) = \sigma(\gamma)$. Then since multiplication by σ^{-1} defines a bijection on $\text{Gal}(L/K)$, we would have $N_{L/K}(x) = \gamma$, a contradiction. $\square$

We will also use

Lemma 4.1. [159] *Let L/K be a degree n Galois extension and $\mathfrak{q}$ be a prime ideal in K below the prime ideal $\mathfrak{Q}$ in L . Let $f = f_{\mathfrak{q}}$ be the relative inertial degree of $\mathfrak{Q}$ over $\mathfrak{q}$. If $\gamma \in \mathfrak{q} \setminus \mathfrak{q}^2$, then $\gamma^i \notin N_{L/K}(L^\times)$ for $i = 1, 2, \dots, f-1$.*

If $\mathfrak{q}$ is inert in L , then its inertial degree is equal to $[L : K]$, and an element γ as in the lemma is such that $\gamma^i \notin N_{L/K}(L^\times)$ for $i = 1, 2, \dots, [L : K] - 1$, so we conclude that γ is a non-norm element. Observe that if we pick a pair of generating elements of $\mathfrak{q}$, they will be non-norm elements for powers below their inertial degree. Thus the hunt for non-norm elements reduces to finding pairs of generating elements of inert prime ideals.

Ideal Lattices & Lattice Problems

Let $\mathcal{I}$ be an ideal of any maximal order $\mathcal{O}$ in a CDA $\mathcal{A} = (L/K, \theta, \gamma)$ with $[L : K] = d$ and $\gamma = \frac{a}{b} \in K$ such that $|\gamma| = 1$. We embed such ideals into $\mathbb{R}^{nd^2}$ exactly as before: fixing the L -basis of $\mathcal{A}$, $\{u^i\}_{i \geq 0}$, one can express an element as the linear map $\phi(x)$ given by left multiplication on the u^i . If $x = \bigoplus_{i=0}^{d-1} u^i x_i \in \mathcal{A}$, then

$$\phi(x) = \begin{pmatrix} x_0 & \gamma\theta(x_{d-1}) & \dots & \gamma\theta^{d-1}(x_1) \\ x_1 & \theta(x_0) & \dots & \gamma\theta^{d-1}(x_2) \\ \dots & \dots & \dots & \dots \\ x_{d-1} & \theta(x_{d-2}) & \dots & \theta^{d-1}(x_0) \end{pmatrix}.$$

Denoting the n embeddings $K \hookrightarrow \mathbb{C}$ extended to embeddings of L by α , it can be seen that all the nd embeddings of L are obtained from the set $\{\alpha \circ \theta^i\}_{\alpha, i}$. We form a vector in $\mathbb{R}^{nd^2}$ from x by concatenating the vectorized images of the $\alpha(\phi(x))$ for all $\alpha \in \text{Emb}(K)$. Then the image

of any discrete additive subgroup of $\mathcal{A}$ is mapped to a lattice in $\mathbb{R}^{nd^2}$. As before, we define two norms on $\mathcal{A}$: we set $\|x\|_p^p = \sum_{\alpha \in \text{Emb}(K)} \sum_{i,j} |\alpha(\phi(x)_{i,j})|^p$, and $\|x\|_\infty = \max_{\alpha,i,j} |\alpha(\phi(x)_{i,j})|$, where $\phi(x)_{i,j}$ denotes the i, j th entry of $\phi(x)$. We note that since γ is unit magnitude, factors of γ appearing in $\phi(x)$ vanish under the defined norm maps, and $\|\cdot\|$ is submultiplicative.

We define the trace and dual ideals identically to before.

4.3.2 Extending the Method of Elia et al to Cyclotomic PIDs

The technique of [121] to construct unit-magnitude non-norm elements in a number field $K \in \{\mathbb{Q}(i), \mathbb{Q}(\omega)\}$ is as follows: pick a prime $q \in \mathbb{Z}$ which splits into two prime ideals, $\mathfrak{p}_1$ and $\mathfrak{p}_2$, in $\mathcal{O}_K$. Create an extension L/K such that both prime ideals are inert in L . Since $\mathcal{O}_K$ is a PID, one can then take the ratio of the generators of $\mathfrak{p}_1$ and $\mathfrak{p}_2$ as the non-norm element; the authors establish this last fact in [121, Propositions 2 and 3].

In this section we observe that the crucial properties of their proof are that $\text{Gal}(L/K)$ is cyclic and that the ring of integers of the ground field is a PID. We give a generalised form of the original proof, which only held for two fields. This is contrasted by our statement, which holds for many more fields, and its corollary, which holds for all 46 cyclotomic fields with ring of integers a PID.

Theorem 4.5. *Let L/K be a finite cyclic Galois extension, $\mathcal{O}_K$ be a PID, and q a prime that splits into precisely two ideals in $\mathcal{O}_K$ which are inert in $\mathcal{O}_L$. Then the ratio of the generators of the ideals satisfies the non-norm condition for L/K .*

Proof. The proof follows the latter part of [121, Proposition 2, 3]. Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be prime ideals of $\mathcal{O}_K$ as in the theorem statement. Denote their generators by π_1 and π_2 respectively. Set

$$\gamma = \frac{\pi_1}{\pi_2}.$$

We show that the smallest k such that γ^k is the norm of an element in L is n . Suppose otherwise,

so

$$\gamma^k = N_{L/K}(\ell) = \prod_{l=0}^{n-1} \sigma^l(\ell)$$

for some $\ell \in L$ and $k < n$, with $\text{Gal}(L/K) = \langle \sigma \rangle$. Writing $\ell = \frac{a}{b}$ with $a, b \in \mathcal{O}_L$ and taking ideals, we have

$$(\pi_1)^k \prod_{l=0}^{n-1} (\sigma^l(b)) = (\pi_2)^k \prod_{l=0}^{n-1} (\sigma^l(a)).$$

Since π_1 and π_2 generate comaximal prime ideals, it follows that (π_1) divides $(\sigma(a))$. Thus on the left hand side of the above equation (π_1) occurs with multiplicity $k \bmod n$, whereas on the right hand side (π_1) can only occur with multiplicity divisible by n . Hence assuming $k < n$ leads to a contradiction and we must have $n \mid k$. $\square$

Corollary 4.2. *Let $K = \mathbb{Q}(\zeta_m)$ and define the sets*

$$S := \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 25, 27, 33, 35, 45\},$$

and

$$S' = \{4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 60, 84\}.$$

If $m \in S \cup S'$ or $m \in 2S$, then if L is a degree n cyclic Galois extension of K and q is a prime that splits into precisely two ideals in $\mathcal{O}_K$ which are inert in $\mathcal{O}_L$, then the ratio of the generators of the ideals is non-norm for L/K .

Proof. Combine the previous theorem with [170, Theorem 11.1]. $\square$

We proceed to give examples of fractional non-norm elements of unit magnitude in fields of higher dimension over $\mathbb{Q}$ than $\mathbb{Q}(i)$ and $\mathbb{Q}(\omega)$. We do this by constructing extensions L/K such that certain prime ideals are inert. Moreover, we take primes $q \in \mathbb{Z}$ that only split into two ideals in $\mathcal{O}_K$ such that the action of complex conjugation permutes those prime ideals above q , so the ratio of the generators of the prime ideals has unit magnitude.

Examples

Construction with $\mathbb{Q}(\zeta_{32})$ Set $K = \mathbb{Q}(\zeta_{32})$. Take $n = 6$, and set $L = \mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \zeta_{64})$. Viewing L as a compositum of $\mathbb{Q}(\zeta_{64})$ and $\mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \zeta_{32})$, which are each cyclic over $\mathbb{Q}(\zeta_{32})$ and have coprime degree to one another, one can see that L is also cyclic over K , of degree 6. Consider $q = 773$; $q \equiv 5 \pmod{32}$, which is an element of order 8, so $f_{K|\mathbb{Q}}^q = 8$. Moreover, 773 is unramified in both K and L , since only primes dividing their discriminants are ramified, and those are 2 and 7. We find that $g_{K|\mathbb{Q}}^q = [K : \mathbb{Q}]/f_{K|\mathbb{Q}}^q = 16/8 = 2$. This means 773 splits into two prime ideals in K , denoted $\mathfrak{p}_1$ and $\mathfrak{p}_2$. We show that these ideals are inert in L .

The Galois group of $L/\mathbb{Q}$ is $(\mathbb{Z}/7\mathbb{Z})^\times / \{\pm 1\} \times (\mathbb{Z}/64\mathbb{Z})^\times$ so $f_{L|\mathbb{Q}}^q$ is the smallest power f such that $773^f \equiv \pm 1 \pmod{448}$. Observe that $773 \equiv 325 \pmod{448}$, which is an element of order 48. Furthermore, $773^{24} \not\equiv -1 \pmod{448}$. Thus $f_{L|\mathbb{Q}}^q = 48$. Now, since $[L : K] = 96$, we obtain that $g_{L|\mathbb{Q}}^q = [L : \mathbb{Q}]/f_{L|\mathbb{Q}}^q = 96/48 = 2$. Since 773 splits into 2 ideals in K and L respectively, we must have that $g_{L|K}^q = 1$, so both $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are inert in L . Since $\mathbb{Z}[\zeta_{32}]$ is a PID, we can then take the ratio of the generators of $\mathfrak{p}_1$ and $\mathfrak{p}_2$ for a unit-magnitude non-norm element γ . Having found a non-norm element, we can construct a cyclic division algebra $\mathcal{A} = (L/K, \theta, \gamma)$, where $\text{Gal}(L/K) = \langle \theta \rangle$ and $[\mathcal{A} : \mathbb{Q}] = 6^2 \cdot 16 = 576$.

Construction with $\mathbb{Q}(\zeta_{45})$ Set $K = \mathbb{Q}(\zeta_{45})$. Take $p = 11$ and set $L = \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1}, \zeta_{45})$. For the same reasons as previously, L is cyclic over K and has degree 5. Consider $q = 13$; we have $13 \equiv 2 \pmod{11}$, so 13 has order 10 in $(\mathbb{Z}/11\mathbb{Z})^\times$. Moreover, 13 has order 12 in $(\mathbb{Z}/45\mathbb{Z})^\times$. We then get $g_{K|\mathbb{Q}}^q = [K : \mathbb{Q}]/f_{K|\mathbb{Q}}^q = 24/12 = 2$, so q splits into two prime ideals, $\mathfrak{p}_1$ and $\mathfrak{p}_2$, as required. Note that the Galois group of L is $(\mathbb{Z}/11\mathbb{Z})^\times / \{\pm 1\} \times (\mathbb{Z}/45\mathbb{Z})^\times$, so $f_{L|\mathbb{Q}}^q$ is the lowest f such that $13^f \equiv \pm 1 \pmod{495}$. Since $13^{60} \equiv 1 \pmod{495}$ and $13^{30} \not\equiv 1 \pmod{495}$, we conclude that $f_{L|\mathbb{Q}}^q = 60$. So $g_{L|\mathbb{Q}}^q = [L : \mathbb{Q}]/f_{L|\mathbb{Q}}^q = 120/60 = 2$, so $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are both inert in L . Since $\mathbb{Q}(\zeta_{45})$ is a PID we can then take the ratio of the generators of $\mathfrak{p}_1$ and $\mathfrak{p}_2$ to obtain a non-norm element of unit-magnitude. The resulting algebra $\mathcal{A} = (L/K, \theta, \gamma)$ has degree $5^2 \cdot 24 = 25 \cdot 24 = 600$ over $\mathbb{Q}$.

4.3.3 Non-norm Elements from Non-PIDs

We now extend the result of Theorem 4.5 to hold for a much wider class of fields; in particular we extend it to all cyclotomic fields. In order to achieve this result, we prove a number of results on the set of non-norm elements of a given field extension L/K . We begin with a converse result to Lemma 4.1:

Lemma 4.2. *Let L/K be a degree n Galois extension. Suppose $\gamma \in \mathcal{O}_K \setminus \mathcal{O}_K^\times$ is such that $\gamma^i \notin N_{L/K}(L^\times)$ for $i = 1, 2, \dots, f-1$. Then there exists a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ such that γ is contained in $\mathfrak{p} \setminus \mathfrak{p}^2$, where $\mathfrak{p}$ lies below a prime ideal $\mathfrak{P}$ in L and $f = f_{\mathfrak{P}|\mathfrak{p}}$ is the relative inertial degree of $\mathfrak{P}$ over $\mathfrak{p}$.*

Proof. Every non-unit is contained in some maximal ideal, so γ is contained in a maximal (prime) ideal, say $\mathfrak{p}$. Let $\mathfrak{P}$ be a prime ideal in $\mathcal{O}_L$ lying above $\mathfrak{p}$. Then by definition of the norm map, we have $N_{L/K}(\mathfrak{P}) = \mathfrak{p}^f$, where f is the inertial degree of $\mathfrak{p}$ in $\mathcal{O}_L$. If $\gamma \in \mathfrak{p}^2$, then we have $\gamma^2 \in \mathfrak{p}^3, \dots, \gamma^{f-1} \in \mathfrak{p}^f = N_{L/K}(\mathfrak{P})$, and so we must have $\gamma^{f-1} = N_{L/K}(x)$, for some x in $\mathfrak{P} \subset \mathcal{O}_L$ - but this is a contradiction, by assumption on γ . $\square$

Proposition 4.2. *Let L/K be a degree n Galois extension. Suppose γ_1 and γ_2 in $\mathcal{O}_K$ both satisfy the non-norm condition for L/K . Furthermore, assume $\gamma_i \in \mathfrak{q}_i \setminus \mathfrak{q}_i^2$, for $\mathfrak{q}_i$ a prime ideal of $\mathcal{O}_K$, lying above some fixed prime $q \in \mathbb{Z}$, for $i = 1, 2$. If $\gamma_2 \notin \mathfrak{q}_1$, then $(\gamma_1 \gamma_2^j)^k$ is not a norm, for $0 < k < f_{L|K}^q$ and $0 < j < f_{L|K}^q$.*

Proof. By definition we have $\gamma_1 \notin \mathfrak{q}_1^2$. We also have $\gamma_1 \gamma_2^j \in \mathfrak{q}_1$, since $\mathfrak{q}_1$ is an ideal. Since γ_2 is not in $\mathfrak{q}_1$, $\gamma_2^j \notin \mathfrak{q}_1$ and hence $\gamma_2^j \notin \mathfrak{q}_1^2$. Finally, to show $\gamma_1 \gamma_2^j \notin \mathfrak{q}_1^2$, we use a localization argument.

Write R for the ring of integers of K . Let $R_{\mathfrak{q}_1}$ denote the localization of R at $\mathfrak{q}_1$, i.e. $R_{\mathfrak{q}_1} = \{\frac{a}{b} : a \in R, b \in R \setminus \mathfrak{q}_1\}$. Since R is a Dedekind domain, this is a discrete valuation ring with unique maximal ideal $\mathfrak{q}_1 R_{\mathfrak{q}_1}$. Now suppose $\gamma_1 \gamma_2^j \in \mathfrak{q}_1^2$. We can consider this as an element of $\mathfrak{q}_1^2 R_{\mathfrak{q}_1}$ because there is an injective homomorphism $f : R \rightarrow R_{\mathfrak{q}_1}$ given by $x \mapsto \frac{x}{1}$. Since $\gamma_2^j \notin \mathfrak{q}_1$, γ_2^j is a unit in $R_{\mathfrak{q}_1}$. This means that $\gamma_1 \gamma_2^j \in \mathfrak{q}_1^2 R_{\mathfrak{q}_1}$ if and only if $\gamma_1 \in \mathfrak{q}_1^2 R_{\mathfrak{q}_1}$. Since $\mathfrak{q}_1^2$ is a primary

ideal, we have $\gamma_1 \in \mathfrak{q}_1^2 R_{\mathfrak{q}_1}$ if and only if $\gamma_1 \in \mathfrak{q}_1^2$ - but this is a contradiction. So $\gamma_1 \gamma_2^j$ satisfies the conditions of Lemma 4.1, and we are done. $\square$

When $f_{L/K}^q = [L : K]$, then $\gamma_1 \gamma_2^j$ satisfies the non-norm condition.

Corollary 4.3. *Let L/K be a finite Galois extension. Suppose γ_1 and γ_2 in $\mathcal{O}_K$ both satisfy the non-norm condition for L/K and $\gamma_i \in \mathfrak{q}_i \setminus \mathfrak{q}_i^2$, for $\mathfrak{q}_i$ a prime ideal of $\mathcal{O}_K$, lying above some fixed prime $q \in \mathbb{Z}$, for $i = 1, 2$ and $\gamma_2 \notin \mathfrak{q}_1$. Then $\gamma_1 \gamma_2^{-1}$ is a non-unit non-norm element.*

Proof. Suppose $\gamma_1 \gamma_2^{-1} = N_{L/K}(x)$ for some $x \in L$. We use Proposition 4.2, which says $\gamma_1 \gamma_2^j$ is non-norm. We have $\gamma_1 \gamma_2 = \gamma_2^2 N_{L/K}(x)$. Let p be the smallest prime divisor of d , and $d = pk$. Applying the proposition, we have non-norm element $\gamma_1 \gamma_2^{p-1} = \gamma_2^p N_{L/K}(x)$; but $(\gamma_1 \gamma_2^{p-1})^k = \gamma_2^{pk} N_{L/K}(x)^k = \gamma_2^d N_{L/K}(x)^k = N_{L/K}(\gamma_2 x^k)$, a contradiction. $\square$

We now extend this to show that $\gamma_1 \gamma_2^{-1}$ satisfies the non-norm condition, subject to the above assumptions.

Corollary 4.4. *Let L/K be a finite Galois extension and q be such that $f_{L/K}^q = [L : K]$. Suppose γ_1 and γ_2 satisfy the non-norm condition, Moreover, let γ_i lie in $\mathfrak{q}_i \setminus \mathfrak{q}_i^2$ for some distinct prime ideals $\mathfrak{q}_i \in \mathcal{O}_K$ above a fixed prime q , and $\gamma_2 \notin \mathfrak{q}_1$, $i = 1, 2$. Then $\gamma_1 \gamma_2^{-1}$ satisfies the non-norm condition.*

Proof. By Proposition 4.2, $\gamma_1 \gamma_2^j$ satisfies the non-norm condition, so $(\gamma_1 \gamma_2^j)^i$ is non-norm for $0 < j < d$, $0 < i < d$. By Corollary 4.3, we know that $\gamma_1 \gamma_2^{-1}$ is non-norm. To verify that $\gamma_1 \gamma_2^{-1}$ satisfies the non-norm condition, we check that $(\gamma_1 \gamma_2^{-1})^{d/p_i}$ is not a norm for any prime factor p_i of d (by Proposition 2.6). Suppose $(\gamma_1 \gamma_2^{-1})^{d/p_i} = N_{L/K}(x)$ for some x . This holds if and only if $\gamma_1^{d/p_i} \gamma_2^{-d/p_i} = \gamma_2^d N_{L/K}(x) = N_{L/K}(\gamma_2 x)$. The left hand side can be rewritten $(\gamma_1 \gamma_2^{p_i-1})^{d/p_i}$, which we have shown is not a norm. Thus we obtain a contradiction. $\square$

We are now able to give a construction of unit-magnitude fractional non-norm elements over cyclotomic fields. In what follows, we fix the presentation of a prime ideal $\mathfrak{p}_i$ of $\mathbb{Z}[\zeta_n]$ as

$\mathfrak{p}_i = (p, f_i(\zeta_n))$ for the prime $p \in \mathfrak{p}_i \cap \mathbb{Z}$ and some polynomial $f_i(x)$ such that $f_i(\zeta_n) \notin \mathfrak{p}_i^2$. We note that such a $f_i(x)$ exists:

Lemma 4.3. *Let $K = \mathbb{Q}(\zeta_n)$ be the n th cyclotomic field and $p \in \mathbb{Z}$ be an unramified prime. Write $g_{K|\mathbb{Q}}^p = g$ and $\Phi_n(x) \equiv f_1(x)f_2(x)\dots f_g(x) \pmod{p}$, where $\Phi_n(x)$ is the n th cyclotomic polynomial and the $f_i(x)$ are monic irreducible. Let $\mathfrak{p}_i$ be a prime ideal containing $f_i(\zeta_n)$. Then, for any $i \in \{1, 2, \dots, g\}$, there exists a choice of $f_i(x)$ such that $f_i(\zeta_n) \notin \mathfrak{p}_i^2$.*

Proof. Fix $f_i(x)$ and suppose that both $f_i(\zeta_n)$ and $f_i(\zeta_n) - p$ are elements of $\mathfrak{p}_i^2$. Then $f_i(\zeta_n) - (f_i(\zeta_n) - p) = p$ is an element of $\mathfrak{p}_i^2$, which is false. So at most one of $f_i(\zeta_n)$ and $f_i(\zeta_n) - p$ can lie in $\mathfrak{p}_i^2$. $\square$

Theorem 4.6. *Let K be the n th cyclotomic field and L/K a finite Galois extension. If q is a prime such that $q\mathcal{O}_K = \prod_{i=1}^g \mathfrak{p}_i$ is a factorisation into distinct prime ideals, with the ramification data $e_{L/\mathbb{Q}}^q = 1$, $g = g_{K/\mathbb{Q}}^q > 1$, $g_{L/K}^q = 1$, and the prime ideals $\mathfrak{p}_i$, $i = 1, \dots, g$ above q in $\mathcal{O}_K$ are permuted by the automorphism corresponding to complex conjugation, then writing $\mathfrak{p}_i = (p, f_i(\zeta_n))$ with $f_i(\zeta_n) \notin \mathfrak{p}_i^2$ for $i = 1, \dots, g$, the ratio of the element $f_i(\zeta_n)$ of any of the $\mathfrak{p}_i$ with its complex conjugate $\overline{f_i(\zeta_n)}$ is a non-norm element for L/K .*

Proof. We consider the case where q splits into two ideals in $\mathcal{O}_K$; the general case of arbitrary splitting is demonstrated mutatis mutandis. Write $q\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_i = (q, f_i(\zeta_n))$, $i = 1, 2$, and $f_1(x)$ is such that $f_1(\zeta_n) \notin \mathfrak{p}_1^2$. Then by Lemma 4.1, since $\mathfrak{p}_1$ is inert in L by assumption, $f_1(\zeta_n)$ is a non-norm element for L/K . Consider $\overline{f_1(\zeta_n)}$; since the prime ideals above q are permuted by complex conjugation, we have $\overline{f_1(\zeta_n)} \notin \mathfrak{p}_1$, so $\overline{f_1(\zeta_n)} \in \mathfrak{p}_2$. If $\overline{f_1(\zeta_n)} \in \mathfrak{p}_2^2$, then $f_1(\zeta_n) \in \overline{\mathfrak{p}_2^2} = \mathfrak{p}_2^2 = \mathfrak{p}_1^2$, which is a contradiction. So $\overline{f_1(\zeta_n)} \in \mathfrak{p}_2 \setminus \mathfrak{p}_2^2$ and hence is a non-norm element. Then by Proposition 4.2, $f_1(\zeta_n)\overline{f_1(\zeta_n)}$ is a non-norm element, and by Corollary 4.3, $f_1(\zeta_n)\overline{f_1(\zeta_n)}^{-1}$ is a non-norm element. It is clearly of unit magnitude, and we are done. $\square$

Note that the ideals above q are not fixed by complex conjugation if q splits into a number of prime ideals in $\mathcal{O}_{K^+} = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ which are not inert in $\mathcal{O}_K$. An example of this would be a prime q which completely splits in K .

Corollary 4.5. *Let K be the n th cyclotomic field and L/K a finite Galois extension. If q is a prime such that $q\mathcal{O}_K = \prod_{i=1}^g \mathfrak{p}_i$ is a factorisation into distinct prime ideals, with the ramification data $e_{L/\mathbb{Q}}^q = 1$, $g = g_{K/\mathbb{Q}}^q > 1$, $g_{L/K}^q = 1$, and the prime ideals $\mathfrak{p}_i$, $i = 1, \dots, g$ above q in $\mathcal{O}_K$ are permuted by the automorphism corresponding to complex conjugation, then writing $\mathfrak{p}_i = (p, f_i(\zeta_n))$ with $f_i(\zeta_n) \notin \mathfrak{p}_i^2$ for $i = 1, \dots, g$, the ratio of the element $f_i(\zeta_n)$ of any of the $\mathfrak{p}_i$ with its complex conjugate $\overline{f_i(\zeta_n)}$ satisfies the non-norm condition for L/K .*

Proof. Follows from Theorem 4.6 and Corollary 4.4. □

Example

Let $K = \mathbb{Q}(\zeta_{190})$. Set $p = 11$ and $L = \mathbb{Q}(\zeta_{190}, \zeta_{11} + \zeta_{11}^{-1})$. Note $[L : K] = 5$ and $[K : \mathbb{Q}] = 72$. One can compute that, with $q = 41$, $f_{K|\mathbb{Q}}^q = 18$ and $f_{L|\mathbb{Q}}^q = 90$, so $f_{L|K}^q = 5$, and hence $g_{L|K}^q = [L : K]/f_{L|K}^q = 5/5 = 1$, and the 4 prime ideals in K above q are inert in L . Moreover, one can check that $41^9 \equiv 151 \pmod{190}$ and $41^{18} \equiv 1 \pmod{190}$, so $f_{K^+/\mathbb{Q}}^q = 18$, and hence $g_{K^+/\mathbb{Q}}^q = 2$, so complex conjugation doesn't fix the prime ideals in K above q , and q meets the conditions of Theorem 4.6. Then we can factor the 190th cyclotomic polynomial modulo 41 to

find the generators of the prime ideals; we have

$$\begin{aligned}
\Phi_{190}(x) &\equiv x^{72} + x^{71} - x^{67} - x^{66} + x^{62} + x^{61} - x^{57} - x^{56} - x^{53} + x^{51} + x^{48} \\
&\quad - x^{46} - x^{43} + x^{41} + x^{38} - x^{36} + x^{34} + x^{31} - x^{29} - x^{26} + x^{24} + x^{21} \\
&\quad - x^{19} - x^{16} - x^{15} + x^{11} + x^{10} - x^6 - x^5 + x + 1 \\
&\equiv (x^{18} + 4x^{17} + 16x^{16} + 23x^{15} + 10x^{14} + 40x^{13} + 37x^{12} + 25x^{11} \\
&\quad + 18x^{10} + 31x^9 + x^8 + 4x^7 + 16x^6 + 23x^5 + 10x^4 + 40x^3 + 37x^2 \\
&\quad + 25x + 18) \cdot (x^{18} + 23x^{17} + 37x^{16} + 31x^{15} + 16x^{14} + 40x^{13} + 18x^{12} \\
&\quad + 4x^{11} + 10x^{10} + 25x^9 + x^8 + 23x^7 + 37x^6 + 31x^5 + 16x^4 + 40x^3 \\
&\quad + 18x^2 + 4x + 10) \cdot (x^{18} + 25x^{17} + 10x^{16} + 4x^{15} + 18x^{14} + 40x^{13} \\
&\quad + 16x^{12} + 31x^{11} + 37x^{10} + 23x^9 + x^8 + 25x^7 + 10x^6 + 4x^5 + 18x^4 \\
&\quad + 40x^3 + 16x^2 + 31x + 37) \cdot (x^{18} + 31x^{17} + 18x^{16} + 25x^{15} + 37x^{14} \\
&\quad + 40x^{13} + 10x^{12} + 23x^{11} + 16x^{10} + 4x^9 + x^8 + 31x^7 + 18x^6 + 25x^5 \\
&\quad + 37x^4 + 40x^3 + 10x^2 + 23x + 16) \bmod 41
\end{aligned}$$

Taking a polynomial factor with integer coefficients (up to subtraction by 41), evaluating at ζ_{190} , and dividing by its complex conjugate gives a non-norm element γ and a CDA $\mathcal{A} = (L/K, \theta, \gamma) = (\mathbb{Q}(\zeta_{190}, \zeta_{11} + \zeta_{11}^{-1})/\mathbb{Q}(\zeta_{190}), \theta, \gamma)$, which has $[\mathcal{A} : \mathbb{Q}] = 1800$.

4.3.4 Application to Cryptography

In this section we define LWE over CDAs constructed to have a fractional unit-magnitude non-norm element. After defining a new (more general) form of CLWE than that of [71] which can have γ possibly in $K \setminus \mathcal{O}_K$, we proceed to give a reduction from lattice problems on ideal lattices which are ideals in arbitrary maximal orders to the search CLWE problem, for a certain family of algebras. Unlike in the original form of CLWE, we do not restrict to the natural order, but give definitions and results for any order which is maximal with respect to inclusion. We note that Theorem 3.1 does not necessarily apply to such orders.

CLWE From Arbitrary Maximal Orders

Here we define a revised CLWE distribution, analogously to [71]. In that work, the definition was only given for a specific order in a specific family of algebras, the natural order. In our definition, we define CLWE for arbitrary maximal orders:

Definition 56. Let L/K be a Galois extension of number fields of dimension $[L : K] = d$ with cyclic Galois group generated by θ . Let $\mathcal{A} := (L/K, \theta, \gamma)$ be a cyclic K -algebra and invariant u with $u^d = \gamma \in K$ and $|\gamma| = 1$. Let $\mathcal{O}$ be a maximal order of $\mathcal{A}$. For an error distribution ψ over $\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$, an integer modulus $q \geq 2$, and a secret $s \in \mathcal{O}_q^\vee$, a sample from the CLWE distribution $\Pi_{\mathcal{O}, q, s, \psi}$ is obtained by sampling $a \leftarrow \mathcal{O}_q$ uniformly at random, $e \leftarrow \psi$, and outputting $(a, b) = (a, (a \cdot s)/q + e \bmod \mathcal{O}^\vee) \in \mathcal{O}_q \times (\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}})/\mathcal{O}^\vee$.

Definition 57. Let Ψ be a family of error distributions over $\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$. The search CLWE problem, denoted by $\text{CLWE}_{\mathcal{O}, q, s, \psi}$, is to recover s from a collection of independent samples from $\Pi_{\mathcal{O}, q, s, \psi}$ for any $s \in \mathcal{O}_q^\vee$ and $\psi \in \Psi$.

Definition 58. Let Υ be a distribution on a family of error distributions over $\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$. Let $U_{\mathcal{O}}$ denote the uniform distribution on $\left(\mathcal{O}_q, \left(\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}\right)/\mathcal{O}^\vee\right)$. Then, the decision CLWE problem, $\text{DCLWE}_{\mathcal{O}, q, \Upsilon}$, is given a collection of independent samples from either $\Pi_{q, s, \psi}$ for a random choice of $(s, \psi) \leftarrow U(\mathcal{O}_q^\vee) \times \Upsilon$ or from $U_{\mathcal{O}}$, decide which is the case with non-negligible advantage.

Technical Lemmas

We will require versions of the ‘clearing out ideals’ lemmas:

Lemma 4.4. [71, Lemma 6/7] Let q be unramified in L . Let $\mathcal{I}$ be an ideal of Λ and $\mathcal{J} = q \cdot \Lambda$, where $q \in \mathbb{Z}$ is prime and $q\mathcal{O}_K = \prod_{i=1}^r \mathfrak{q}_i$ is a decomposition into prime ideals in $\mathcal{O}_K$. Assume $\gamma \notin \mathfrak{q}_i$ for each i . Then, there exists $t \in \mathcal{I} \cap \mathcal{O}_K$ such that the ideal $t \cdot \mathcal{I}^{-1} \subset \Lambda$ is coprime to $\mathcal{J}$, and we can compute such a t efficiently given $\mathcal{I}$ and the prime factorization of $\mathcal{J}$. Moreover, let $\mathcal{P}$ denote an arbitrary fractional ideal of Λ . Then, the function $\chi_t : \mathcal{A} \rightarrow \mathcal{A}$ defined as

$\chi_t(x) = t \cdot x$ induces a module isomorphism from $\mathcal{P}/\mathcal{J}\mathcal{P} \rightarrow \mathcal{I}\mathcal{P}/\mathcal{I}\mathcal{J}\mathcal{P}$. Furthermore, in the case $\mathcal{J} = q\Lambda$ for a prime integer q we can efficiently compute the inverse.

For a maximal order $\mathcal{O}$ and ideal $\mathcal{I} \subset \mathcal{O}$, let $\text{ass}(\mathcal{I}) = \{\mathcal{P}_i : \mathcal{I} \subset \mathcal{P}_i\}$ be the set of *associated primes* of $\mathcal{I}$, where the $\mathcal{P}_i$ are prime ideals of $\mathcal{O}$:

Lemma 4.5. *Let $\mathcal{I}$ be an ideal of maximal order $\mathcal{O}$ and let $\mathcal{J}$ be an arbitrary integral ideal of $\mathcal{O}$. Then, there exists an element $t \in \mathcal{I} \cap \mathcal{O}_K$ such that the ideal $t \cdot \mathcal{I}^{-1} \subset \mathcal{O}$ is coprime to $\mathcal{J}$, and we can compute such a t efficiently given $\mathcal{I}$ and the associated primes of $\mathcal{J}$.*

Proof. Let $\{\mathcal{P}_i\}_{i=1,\dots,r} = \text{ass}(\mathcal{J})$ and $t \in (\mathcal{I} \setminus \bigcup_i \mathcal{P}_i \mathcal{I}) \cap \mathcal{O}_K$. Suppose $t \cdot \mathcal{I}^{-1} + \mathcal{J} \neq \mathcal{O}$. So $t \cdot \mathcal{I}^{-1} + \mathcal{J} \subset \mathcal{M}$ for maximal ideal $\mathcal{M} \subset \mathcal{O}$. But maximal ideals are prime, so $t \cdot \mathcal{I}^{-1}$ is contained in an associated prime of $\mathcal{J}$. This implies that $t \in \mathcal{P}_i \mathcal{I}$ for some $\mathcal{P}_i \in \text{ass}(\mathcal{J})$. This is a contradiction. To construct such a t , take an $\mathcal{O}_K$ element in $\mathcal{I} \setminus \mathcal{P}_i \mathcal{I}$ for all i , and compute the preimage under the CRT isomorphism (the CRT holds by [139, §22, ex.3]). $\square$

We can now prove our clearing ideals lemma for arbitrary maximal orders:

Lemma 4.6. *Let $\mathcal{O}$ be a maximal order. Let $\mathcal{I}, \mathcal{J}$ be ideals of $\mathcal{O}$ and $t \in \mathcal{I} \cap \mathcal{O}_K$ be such that $t \cdot \mathcal{I}^{-1}$ and $\mathcal{J}$ are coprime ideals, and let $\mathcal{P}$ be an arbitrary fractional ideal of $\mathcal{O}$. Then, the function $\chi_t : \mathcal{A} \rightarrow \mathcal{A}, x \mapsto t \cdot x$ induces a module isomorphism from $\mathcal{P}/\mathcal{J} \cdot \mathcal{P} \rightarrow \mathcal{I} \cdot \mathcal{P}/\mathcal{I} \cdot \mathcal{J} \cdot \mathcal{P}$. If $\mathcal{J} = q\mathcal{O}$ for an unramified prime $q \in \mathbb{Z}$ we can efficiently compute the inverse.*

Proof. Identical to [71, Lemma 7], since an arbitrary maximal order in a CDA has the same properties as Λ in the algebras considered in that work. Moreover, we can compute the inverse efficiently using the same method as [71, Lemma 7], since an $\mathcal{O}_K$ -order is a $\mathbb{Z}$ -order. $\square$

The Hardness of Search CLWE

We first state an adaptation of [138, Lemma 3.14], similar to [71, Lemma 11], which is the only quantum step of the proof:

Lemma 4.7. *There exists an efficient quantum algorithm that, given any nd^2 dimensional lattice $\mathcal{L} := \sigma_{\mathcal{A}}(\mathcal{I})$ for some ideal $\mathcal{I} \subset \mathcal{O}$, $0 < \delta < \lambda_1(\mathcal{L}^\vee) / (2\sqrt{2nd})$, and an $\mathcal{A}$ -BDD $_{\mathcal{O}, \mathcal{L}^\vee, \delta}$ oracle, outputs an independent sample from $D_{\mathcal{L}, \sqrt{d}\omega(\sqrt{\log(nd)})/\sqrt{2}\delta}$.*

We now show how to transform a $q\mathcal{A}$ -BDD instance into a CLWE instance, given discrete Gaussian samples:

Lemma 4.8. *Let $\mathcal{A} = (L/K, \theta, \gamma)$ be a CDA constructed as above, and $\mathcal{O} \subset \mathcal{A}$ a maximal order. There is a ppt. algorithm that given an unramified prime $q \geq 2$, an invertible fractional $\mathcal{O}$ -ideal $\mathcal{I}^\vee$, a $q\mathcal{A}$ -BDD $_{\mathcal{O}, \mathcal{I}^\vee, \alpha q \cdot \omega(\sqrt{\log(nd)})/\sqrt{2nd} \cdot r}$ instance $y = x + e$, a parameter $r \geq \sqrt{2}q \cdot \eta(\mathcal{I})$, and $D_{\mathcal{I}, r'}$ samples with $r' \geq r$, outputs samples within negligible statistical distance of the CLWE distribution $\Pi_{\mathcal{O}, q, s, \Sigma}$ for $s = \chi_t(x \bmod q\mathcal{I}^\vee) \in \mathcal{O}_q^\vee$, where χ_t is as in Lemma 4.6 and Σ is an error distribution such that if $|\gamma| = 1$ the resulting error e'' is Gaussian and has Gaussian marginal distributions all with parameter $r_{i,j} \leq \alpha$.*

Proof. The proof is similar to the one detailed for one-sided ideals of Λ , in the previous chapter, but included for completeness. First compute $t \in \mathcal{I}$ such that $t \cdot \mathcal{I}^{-1}$ and $q\mathcal{O}$ are coprime using Lemma 4.6. We take $z \leftarrow D_{\mathcal{I}, r'}$ and use it to create a CLWE sample

$$(a, b) = (\chi_t^{-1}(z \bmod q\mathcal{I}), (z \cdot y)/q + e' \bmod \mathcal{O}^\vee) \in \left(\mathcal{O}_q \times \left(\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}} \right) / \mathcal{O}^\vee \right)$$

where $e' \leftarrow D_{\alpha/\sqrt{2}}$. We show that these samples are negligible statistical distance from the true CLWE distribution and that s is uniformly random. Since $r \geq q \cdot \eta(\mathcal{I})$, Lemma 2.6 implies that any $z \bmod q\mathcal{I}$ is obtained with probability in $[\frac{1-\varepsilon}{1+\varepsilon}, 1] \cdot \beta$ for some $\beta > 0$. We can then bound the statistical distance between $z \bmod q\mathcal{I}$ and the uniform distribution by 2ε and conclude that a is close to uniform. Similarly, since χ_t is a bijection, $a = \chi_t^{-1}(z \bmod q\mathcal{I})$ is at most statistical distance 2ε from the uniform distribution over $\mathcal{O}_q$. We next consider b , and show that it has the shape $b = (a \cdot s)/q + e''$, for some error e'' and uniformly random s , conditioned on fixed a . We have

$$\begin{aligned} b &:= (z \cdot y)/q + e' \bmod \mathcal{O}^\vee \\ &= (z \cdot x)/q + (z \cdot e)/q + e' \bmod \mathcal{O}^\vee, \end{aligned}$$

so since $z = t \cdot a \bmod \mathcal{O}_q^\vee$ and $t \in \mathcal{Z}(\mathcal{A})$ we find $(z \cdot x)/q = (a \cdot t \cdot x)/q = (a \cdot s)/q \bmod \mathcal{O}^\vee$ for $s := \chi_t(x \bmod q\mathcal{I}^\vee)$. Hence if x is uniformly random over $\mathcal{I}^\vee$, then s is uniformly random over $\mathcal{O}_q^\vee$, since χ_t is a bijection. The analysis of the error is as before. $\square$

Now suppose we have a search CLWE oracle and an ideal lattice, and we want to obtain samples from a discrete Gaussian with small parameter. We begin by sampling a discrete Gaussian of very large parameter. Combining Lemma 4.8 and Lemma 3.8 gives us an algorithm for $\mathcal{A}$ -BDD. Lemma 4.7 then implies an algorithm to obtain discrete Gaussian samples with the desired parameter. We arrive at

Theorem 4.7. *Given a $\text{CLWE}_{\mathcal{O},q,\Sigma_\alpha}$ -oracle for input $\alpha \in (0,1)$, $q \geq 2$, an ideal $\mathcal{I} \subset \mathcal{O}$, $r \geq \sqrt{2}q \cdot \eta(\mathcal{I})$ satisfying $r' := r \cdot \omega(\sqrt{\log N})/(\alpha q) > \sqrt{2N}/\lambda_1(\mathcal{I}^\vee)$, and polynomially many samples from the discrete Gaussian $D_{\mathcal{I},r}$ there exists an efficient quantum algorithm that outputs an independent sample from $D_{\mathcal{I},r'}$.*

Repeated application of Theorem 4.7 on Gaussian samples of very large parameter allows us to conclude, as in [136, Theorem 3.1], [102, Theorem 4.1], [71, Theorem 6] that there is a polynomial-time reduction from DGS to search CLWE, as each application of Theorem 5 outputs samples with monotonically decreasing parameter $r' < r$; combining this with the reduction from SIVP to DGS, we obtain

Corollary 4.6. *Let $\mathcal{A}, \mathcal{O}, \alpha$ and q be as above. Then there is a polynomial-time quantum reduction from $\mathcal{A}$ -SIVP $_\xi$ to $\text{CLWE}_{\mathcal{O},q,\Sigma_\alpha}$ for any $\sqrt{8Nd} \cdot \xi = (\omega(\sqrt{dn})/\alpha)$.*

4.4 Learning with Errors from Nonassociative Algebras

4.4.1 Introduction

In this section, we generalise CLWE in a different direction to the previous section, and create structured LWE from *nonassociative* CDAs, dubbed nonassociative CLWE (NCLWE). We do this by permitting $\gamma \in \mathcal{O}_L$. We prove a new result on the structure of ideals in the natural

order of certain nonassociative CDAs, give security reductions, and a public key encryption scheme. We motivate developing yet another variant of LWE:

1. As will be seen below, the nonassociative algebras used can reach certain dimensions more flexibly than associative algebras can. This allows for greater freedom in choosing parameters for structured LWE. For example, considering the power of three case, set $K = \mathbb{Q}(\zeta_{243})$. We can create a nonassociative CDA $\mathcal{A}$ with dimension equal to 648 over $\mathbb{Q}$, but it is not known how to achieve this in the associative case. Moreover, for many algebra dimensions constructible in the associative case, there are multiple different ways of realizing nonassociative division algebras with the same dimension.
2. The search to decision reduction of [71] was only valid for a restricted set of secrets, so CLWE lacks a full reduction from hard lattice problems to the decision problem. We will prove below that moving to nonassociative algebras allows one, for certain choices of modulus, to obtain an unrestricted reduction from a search LWE-style problem to the corresponding decision problem. This provides greater confidence in the security of the nonassociative form of CLWE than the associative form.
3. Similarly to [71], the structure of $\phi(a)$ means there is little storage cost associated with NCLWE keys, and multiplication in the matrix representation can be conducted efficiently, compared to MLWE in the same dimension.
4. One might hope that creating RLWE variants which have minimal structure (but retain useful properties) might be more resistant to cryptanalytic techniques than variants with more structure. If true, using a nonassociative ring for ring LWE may offer less attack surface than an associative ring offers.
5. Lastly, this construction may be of mathematical interest, being the first cryptographic construction of lattices with a nonassociative multiplication operation that can be used to construct a form of LWE with a security reduction from basic lattice problems.

In particular, we develop a novel cryptosystem based on the hardness of LWE in nonassociative CDAs, by adapting an existing scheme to account for the nonassociativity of the spaces used.

To do this we prove new results regarding ideals in orders in nonassociative CDAs, and use these results to give a proof that nonassociative LWE is at least as hard as solving lattice problems obtained from ideals in nonassociative CDAs. The main result on nonassociative ideals we obtain is the following:

Properties of Ideals in Orders of Nonassociative CDAs (Theorem 4.11). *Let $\mathcal{A} = (L/K, \theta, \gamma)$ be a nonassociative cyclic division algebra, and $\Lambda \subset \mathcal{A}$ the natural order. Then multiplication of Λ -ideals is commutative and associative.*

We then follow the usual method of reducing DGS to search LWE, and reducing the search LWE problem to the decision problem. Namely, we obtain the following result:

Hardness of Search (Theorem 4.13). *Let $\mathcal{A}$ be a nonassociative cyclic division algebra over a number field L with center K and natural, maximal order Λ with $|\gamma| = 1$. Let $\alpha = \alpha(n) \in (0, 1)$ and $q = q(n) \geq 2$, unramified in L , be parameters such that $\alpha q \geq \omega(1)$. Then there is a polynomial-time quantum reduction from $\mathcal{A}$ -DGS $_{\xi}^{\vee}$ to $SNCLWE_{q,s,\Sigma_{\alpha}}$ for any $\xi = r\sqrt{d}\omega(\sqrt{\log(d \cdot n)})/\alpha q$ and $r > \sqrt{2}q \cdot \eta_{\varepsilon}(\mathcal{I})$.*

Moreover, we prove a result on quotients of the natural order in a nonassociative CDA which permits us to extend the corresponding search-to-decision proof for associative rings to obtain the second part of the following theorem:

Search to Decision (Theorem 4.14). *Let Λ be the natural order of a nonassociative cyclic algebra $\mathcal{A} = (L/K, \theta, \gamma)$, $q \in \text{poly}(n)$ and assume that $\alpha q \geq \eta_{\varepsilon}(\Lambda^{\vee})$ for a negligible $\varepsilon = \varepsilon(n)$. Then there is a ppt. reduction from $SNCLWE_{q,G,\Sigma_{\alpha},G}$ for any pairwise difference set $G \subset \Lambda_q^{\vee}$ to $DNCLWE_{q,\Upsilon_{\alpha}}$.*

When q has prime factors in $\mathcal{O}_K$ inert in $\mathcal{O}_L$, then there is a ppt. reduction from $SNCLWE_{q,s,\Sigma_{\alpha}}$ to $DNCLWE_{q,\Upsilon_{\alpha}}$ in time polynomial in n .

We note, moreover, that the proof of Theorem 4.13 holds with very minor changes when $|\gamma| \neq 1$. These results provide us with confidence that this structured form of LWE has a security level lying somewhere between that of RLWE and MLWE, which, when $\gamma \in \mathcal{O}_L^{\times} \setminus \mathcal{O}_K^{\times}$, is likely greater

than CLWE because of the lower degree of structure involved in the construction. This work provides a generalisation of the framework of CLWE³, since one can consider $\gamma \in \mathcal{O}_L$ which contains the $\gamma \in \mathcal{O}_K$ setting, and this generalisation preserves the ring structure, which may be an advantage over the module setting. In addition to this, as mentioned above we are able to give a collection of different methods to create CDAs, which provide numerous options for creating CDAs for cryptography⁴. We list briefly the different constructions, and emphasize that the options for creating CDAs in the associative case are much more constrained:

1. $\mathcal{A} = (\mathbb{Q}(\zeta_{pn})/\mathbb{Q}(\zeta_n), \theta, \zeta_{pn})$, where $(p, n) = 1$.
2. $\mathcal{A} = (\mathbb{Q}(\zeta_{p^r q^s})/\mathbb{Q}(\zeta_{p^{r-1} q^s}), \theta, \zeta_{p^r q^s})$, where $(p, q) = 1$.
3. $\mathcal{A} = (\mathbb{Q}(\zeta_{p^r q^s})/\mathbb{Q}(\zeta_{p^r q^s})^+, \theta, \zeta_{p^r q^s})$, where $(p, q) = 1$.
4. $\mathcal{A} = (\mathbb{Q}(\zeta_{p \cdot q^r})/\mathbb{Q}(\zeta_{q^r}, \sqrt{-p}), \theta, \zeta_{p \cdot q^r})$, where $(p, q) = 1$ and $p \equiv -1 \pmod{4}$.
5. $\mathcal{A} = (\mathbb{Q}(\zeta_{p^k}, \zeta_q + \zeta_q^{-1})/\mathbb{Q}(\zeta_{p^k}), \theta, \zeta_q + \zeta_q^{-1})$, where $(p, q) = 1$.

Nonassociative CDAs were first defined by Dickson in [57] in the quaternionic case, that of degree 2. Their properties were examined in [171] and [98], and the construction of nonassociative division algebras for degree larger than 2 was given in the work of Steele [151], [152], and further developed in [131].

The use of CDAs for communication was pioneered by coding theorists in works such as [118], [145], and [159]. There is a large literature on such codes, and to that was added a string of papers developing the properties of codes from nonassociative algebras, in [39], [40], [132], [149], and [153]. Noncommutative CDAs were introduced into post-quantum cryptography in [71].

Nonassociative algebras have also been used in symmetric cryptography [60], [142], [85]. We note here that nonassociative spaces have been used in lattice-based cryptography before, namely in [103], a variant of NTRU over the octonions. For the mathematics of general nonassociative algebras, we refer the interested reader to [5], [51], and [143].

³However our proofs do not subsume the corresponding proofs in the associative case, since algebras which are not associative behave very differently to associative algebras. Note below we often state $\gamma \in \mathcal{O}_L \setminus \mathcal{O}_K$, rather than simply $\gamma \in \mathcal{O}_L$.

⁴However, not all of these constructions are covered by the security reductions.

4.4.2 Nonassociative Cyclic Division Algebras

Preliminaries on Nonassociative Cyclic Algebras

We begin by defining nonassociative cyclic algebras. Recall a ring is nonassociative if

$$a(bc) = (ab)c$$

does not always hold, for ring elements a, b, c .

Definition 59. Let K be a number field of degree n and L a cyclic Galois extension of degree d over K . Let θ generate the Galois group of L/K . Let $\gamma \in L \setminus K$. We call

$$\mathcal{A} = L \oplus uL \oplus \dots \oplus u^{d-1}L,$$

where u is an auxiliary element subject firstly to $u^d = \gamma$ and secondly to $xu = u\theta(x)$ for all $x \in L$, a nonassociative cyclic algebra. Fixing the basis $\{1, u, \dots, u^{d-1}\}$, we define multiplication on $u^i x$ and $u^j y$ for $x, y \in L, 0 \leq i, j, < d$ by

$$(u^i x)(u^j y) = \begin{cases} u^{i+j} \theta^j(x)y & \text{if } i+j < d \\ u^{i+j-n} \gamma \theta^j(x)y & \text{if } i+j \geq d \end{cases}$$

and extend this linearly to all of $\mathcal{A}$. As with associative cyclic algebras, we denote this algebra by $\mathcal{A} = (L/K, \theta, \gamma)$.

The above algebra is not associative. For example, $(u \cdot u^{d-1}) \cdot u = u^d \cdot u = \gamma u = u\theta(\gamma)$, but $u \cdot (u^{d-1} \cdot u) = u \cdot u^d = u\gamma$. We measure lack of associativity with

Definition 60. The associator of $\mathcal{A}$ is defined $[x, y, z] = (xy)z - x(yz)$. The left nucleus is defined $\text{Nuc}_l = \{x \in \mathcal{A} : [x, \mathcal{A}, \mathcal{A}] = 0\}$, and the middle and right nuclei are similarly defined. The nucleus of $\mathcal{A}$, $\mathcal{N}(\mathcal{A})$, is the intersection of the left, right, and middle nuclei.

The nuclei are associative subalgebras of $\mathcal{A}$.

Definition 61. *The commutator of $\mathcal{A}$ is $\text{Comm}(\mathcal{A}) = \{x \in \mathcal{A} : xy = yx \text{ for all } y \in \mathcal{A}\}$. The center of the algebra is given by $\mathcal{Z}(\mathcal{A}) = \text{Comm}(\mathcal{A}) \cap \text{Nuc}(\mathcal{A})$. An algebra $\mathcal{A}$ is central if $\mathcal{Z}(\mathcal{A}) = K$.*

Proposition 4.3. *For any nonassociative cyclic algebra $\mathcal{A} = (L/K, \theta, \gamma)$, we have $\mathcal{N}(\mathcal{A}) = L$ and $\text{Comm}(\mathcal{A}) = K$, so $\mathcal{A}$ is a central K -algebra. Moreover, $\mathcal{A}$ is simple.*

Proof. Corollary 3.2.6 and Proposition 3.2.7 from [152]. □

We state a characterisation of the ‘division’ property of algebras:

Definition 62. *A unital algebra over a field is a division algebra if every element has a left and a right inverse.*

Alternatively, one could say an algebra is division if left (and right) multiplication defines a bijective map from the algebra to itself. Thus there are no zero divisors in a division algebra. An algebra element may have distinct left and right inverses.

Proposition 4.4. *Let $\mathcal{A}$ be a nonassociative cyclic algebra of prime degree p . Then $\mathcal{A}$ is a division algebra. If $\mathcal{A}$ has arbitrary degree d and the elements $1, \gamma, \dots, \gamma^{d-1}$ are linearly independent over K , then $\mathcal{A}$ is a division algebra. If γ is not contained in any proper subfield of L , $\mathcal{A}$ is a division algebra.*

Proof. Corollary 3.2.11 and Theorem 3.2.10 of [152]. □

The search for ‘non-norm elements’, i.e. elements of the ground field K which aren’t realisable as the norm of any element of L , is a key part of the construction of associative CDAs. When taken for γ , as we saw above, they ensure the algebra is division. Their importance is paralleled by their rarity, and several, often convoluted, methods have been developed to obtain them. However, as shown in the above theorem, it is much easier in the nonassociative case to guarantee a cyclic algebra is division; indeed, in the degree p case it holds automatically.

Example: Let $K = \mathbb{Q}(\zeta_n)$ and $L = \mathbb{Q}(\zeta_{pn})$ where p and n are coprime. Then $\zeta_p \notin K$, and L/K is cyclic and Galois. Then $(L/K, \theta, \zeta_{pn})$ is a nonassociative cyclic division algebra. Finally, we introduce a mild generalisation of nonassociative cyclic algebras:

Definition 63. Let S/R be a finite extension of commutative rings and $G = \langle \theta \rangle$ be a finite cyclic group of order d acting on S with trivial action on R . Let $\gamma \in S$ and u such that $ux = \theta(x)u$ for all $x \in S$ and $u^d = \gamma$. Then we call

$$\mathcal{A} = (S/R, \theta, \gamma) := \bigoplus_{i=0}^{d-1} u^i S$$

equipped with multiplication as in Definition 59 a generalised cyclic algebra.

Matrix Representation

As explained previously, one can consider RLWE as a structured form of LWE, by fixing a $\mathbb{Z}$ -basis of the chosen ring, and writing $a \cdot s$ as $\phi(a)\mathbf{s}$, where $\phi(a)$ is matrix defined by multiplication by a on the fixed basis, and $\mathbf{s}$ is the coefficient vector of s . This yields a number of correlated LWE samples equal to the dimension of the ring. As we have discussed, MLWE and CLWE can also be considered as structured forms of LWE. In the case of nonassociative algebras, there is also a matrix representation arising from multiplication on a fixed basis in the nonassociative algebra; however, unlike in the associative cases, this defines an embedding into a *vector space* of matrices, rather than a ring, and so does not preserve the multiplicative structure of algebra elements. That is, $\phi(as) \neq \phi(a)\phi(s)$. This limitation of the matrix representation can be intuitively understood as following from the fact that matrix multiplication is associative; thus there could be no *multiplicative* map from a nonassociative space into a space of matrices. The presence of a merely additive map is sufficient for our purposes, and will later enable us to define a reduced trace map, as in the associative case.

This representation is as follows: left multiplication by an element $a = a_0 + ua_1 + \cdots + u^{m-1}a_{m-1}$

on the basis $\{u^i\}$ inside $(L/K, \sigma, \gamma)$ yields the following matrix:

$$\phi(a) = \begin{pmatrix} a_0 & \gamma\sigma(a_{m-1}) & \gamma\sigma^2(a_{m-2}) & \cdots & \gamma\sigma^{m-1}(a_1) \\ a_1 & \sigma(a_0) & \gamma\sigma^2(a_{m-1}) & \cdots & \gamma\sigma^{m-1}(a_2) \\ a_2 & \sigma(a_1) & \sigma^2(a_0) & \cdots & \gamma\sigma^{m-1}(a_3) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m-1} & \sigma(a_{m-2}) & \sigma^2(a_{m-3}) & \cdots & \sigma^{m-1}(a_0) \end{pmatrix}$$

So a sample of nonassociative CLWE generalises MLWE, similarly to the standard form of CLWE, by yielding m correlated MLWE samples from one nonassociative CLWE sample.

Integral Structures in Nonassociative Algebras

In order to define the lattice problems will use in our reduction, we need to define orders and ideals in nonassociative algebras. The primary reference for this section is [131]. Set $\mathcal{A} = (L/K, \theta, \gamma)$ with $\gamma \in L \setminus K$ such that $\mathcal{A}$ is a division algebra. All lattices will be full-rank. As in the associative setting, an order is *maximal* if it is not strictly contained in any larger proper order.

In the following we use the definition in [139] of an $\mathcal{O}_K$ -lattice, namely that an $\mathcal{O}_K$ -lattice is a finitely generated $\mathcal{O}_K$ -torsionfree $\mathcal{O}_K$ -module. An $\mathcal{O}_K$ -lattice is *full* if it contains a K -basis of $\mathcal{A}$. We now formally define (identically to before) the natural order in a nonassociative CDA:

Definition 64. Let $\gamma \in \mathcal{O}_L$. We call $\Lambda = \bigoplus_{i=0}^{d-1} u^i \mathcal{O}_L$ the natural order of $\mathcal{A} = (L/K, \theta, \gamma)$.

Proposition 4.5. If $\gamma \in \mathcal{O}_L$, Λ is an order of $\mathcal{A} = (L/K, \theta, \gamma)$.

Proof. Λ is clearly additively closed. To see multiplicative closure, we demonstrate the case of $d = 2$. Let $a, b \in \Lambda$ and observe

$$a \cdot b = (a_0 + ua_1) \cdot (b_0 + ub_1) = a_0b_0 + u(\theta(a_0)b_1 + a_1b_0) + \gamma a_1b_1,$$

which lies within Λ if $\gamma \in \mathcal{O}_L$. So Λ is a subring, and this holds for all $d \in \mathbb{Z}_{\geq 1}$. Λ is discrete by virtue of $\mathcal{O}_L$ being a lattice inside L . It is an $\mathcal{O}_K$ -module with the standard multiplication. $\square$

Note however that if $\gamma \in L \setminus \mathcal{O}_L$, Λ is not multiplicatively closed.

We proceed to study ideals in Λ , properties of which we redefine for the nonassociative setting.

Definition 65. A two-sided ideal $\mathcal{I} \subset \Lambda$ is defined as an additively closed subset of Λ closed under multiplication from Λ on both sides, i.e. $\Lambda\mathcal{I} \subset \mathcal{I}$ and $\mathcal{I}\Lambda \subset \mathcal{I}$. An ideal is one-sided if closed by multiplication from Λ on one side, e.g. $\mathcal{I}$ is a right ideal if $\mathcal{I}\Lambda \subset \mathcal{I}$.

Definition 66. An ideal is maximal if it is not properly contained in any other proper ideal. An ideal is prime if it is a maximal two-sided ideal.

Definition 67. The sum and product of two ideals $\mathcal{I}, \mathcal{J}$ are defined as usual; $\mathcal{I} + \mathcal{J} = \{i + j : i \in \mathcal{I}, j \in \mathcal{J}\}$ and $\mathcal{I} \cdot \mathcal{J} = \{\sum_{l=1}^m i_l \cdot j_l : i_l \in \mathcal{I}, j_l \in \mathcal{J}, m \in \mathbb{N}\}$. A two-sided ideal $\mathcal{I}$ is fractional if $c\mathcal{I} = \mathcal{J}$ for a two-sided ideal $\mathcal{J}$ and $c \in K$.

The sum of two fractional ideals can clearly be seen to yield another fractional ideal. The product of two ideals in a nonassociative space less clearly yields another ideal, however. In the following pages we develop an ideal theory that will permit us to prove a security reduction for nonassociative CLWE from nonassociative ideal lattices. We recall and extend a number of results from [131].

Let $q \in \mathbb{Z}$ be a prime. Then $q \in \text{Comm}(\mathcal{A})$ and $q\Lambda$ is a two-sided ideal of Λ . Let $\mathcal{I} \subset \mathcal{O}_K$ be an ideal. Then we have the following product

$$\mathcal{I}\Lambda = \left\{ \sum_i a_i l_i \mid a_i \in \mathcal{I}, l_i \in \Lambda \right\} = \left\{ \sum_{i=0}^{d-1} u^i a_i \mid a_i \in \mathcal{I}\mathcal{O}_L \right\},$$

which is a two-sided ideal of Λ .

Proposition 4.6. Let $J \subset \Lambda$ be a two-sided ideal. Then $\mathcal{I} = J \cap \mathcal{O}_L$ is a non-zero ideal of $\mathcal{O}_L$. If $\mathcal{I}$ is an ideal of K , then $\mathcal{I}\Lambda \cap \mathcal{O}_K = \mathcal{I}$.

Proof. Lemma 5.1 and Remark 5.2 of [131]. $\square$

Proposition 4.7. *Let $\mathcal{A} = (L/K, \theta, \gamma)$ be a nonassociative CDA with $\gamma \in \mathcal{O}_L^\times \setminus \mathcal{O}_K^\times$ and natural order Λ . Let $\mathcal{I} \subset \Lambda$ be a two-sided ideal. Then $\theta(\mathcal{I} \cap \mathcal{O}_L) = \mathcal{I} \cap \mathcal{O}_L$.*

Proof. Suppose $\theta(\mathcal{I} \cap \mathcal{O}_L) \neq \mathcal{I} \cap \mathcal{O}_L$. So there exists $x \in \mathcal{I} \cap \mathcal{O}_L$ such that $\theta(x) \notin \mathcal{I} \cap \mathcal{O}_L$. As $\mathcal{I}$ is two-sided, $\mathcal{I}u \subset \mathcal{I}$, so $xu = u\theta(x) \in \mathcal{I}$. Moreover, $u^{d-1}\mathcal{I} \subset \mathcal{I}$, so $u^{d-1}(u\theta(x)) = u^d\theta(x) = \gamma\theta(x) \in \mathcal{I}$. Since γ is a unit, $\gamma^{-1}\mathcal{I} \subset \mathcal{I}$, so $\gamma^{-1}(\gamma\theta(x)) = \theta(x) \in \mathcal{I}$. Finally, $\theta(x) \in \mathcal{O}_L$, so $\theta(x) \in \mathcal{I} \cap \mathcal{O}_L$ - a contradiction. $\square$

This result in fact holds for generalised cyclic algebras when γ is a unit. We recall that if $\mathcal{I} = \mathfrak{q}_1^{s_1} \cdots \mathfrak{q}_t^{s_t}$ is an ideal of $\mathcal{O}_K$, then we have

$$\mathcal{O}_K/\mathcal{I} = \mathcal{O}_K/\mathfrak{q}_1^{s_1} \cdots \mathfrak{q}_t^{s_t} \cong \mathcal{O}_K/\mathfrak{q}_1^{s_1} \times \cdots \times \mathcal{O}_K/\mathfrak{q}_t^{s_t}$$

and

$$\mathcal{O}_L/\mathcal{I}\mathcal{O}_L = \mathcal{O}_L/\mathfrak{q}_1^{s_1} \cdots \mathfrak{q}_t^{s_t}\mathcal{O}_L \cong \mathcal{O}_L/\mathfrak{q}_1^{s_1}\mathcal{O}_L \times \cdots \times \mathcal{O}_L/\mathfrak{q}_t^{s_t}\mathcal{O}_L.$$

Below is a version of the Chinese remainder theorem (CRT) for Λ :

Theorem 4.8. *For $\mathcal{I}$ an ideal of $\mathcal{O}_K$ as above, we have*

$$\begin{aligned} \Lambda/\mathcal{I}\Lambda &\cong ((\mathcal{O}_L/\mathcal{I}\mathcal{O}_L) / (\mathcal{O}_K/\mathcal{I}), \bar{\theta}, \gamma + \mathcal{I}\mathcal{O}_L) = \bigoplus_{i=0}^{d-1} u^i (\mathcal{O}_L/\mathcal{I}\mathcal{O}_L) \\ &\cong ((\mathcal{O}_L/\mathfrak{q}_1^{s_1}\mathcal{O}_L) / (\mathcal{O}_K/\mathfrak{q}_1^{s_1}), \bar{\theta}, \gamma + \mathfrak{q}_1^{s_1}) \times \cdots \\ &\quad \cdots \times ((\mathcal{O}_L/\mathfrak{q}_t^{s_t}\mathcal{O}_L) / (\mathcal{O}_K/\mathfrak{q}_t^{s_t}), \bar{\theta}, \gamma + \mathfrak{q}_t^{s_t}), \end{aligned}$$

where $\bar{\theta}$ is defined by its actions on the ideal quotients, e.g. $\bar{\theta}(x + \mathfrak{q}_i^{s_i}\mathcal{O}_L) = \theta(x) + \mathfrak{q}_i^{s_i}\mathcal{O}_L$.

Proof. [131], Theorem 5.3 and Lemma 5.4. $\square$

In an abuse of notation, we may write θ for $\bar{\theta}$. Below, we study quotients $\Lambda/\mathcal{I}\Lambda$ in greater detail.

Unramified Primes: Inert and Split

Recall for fixed prime $\mathfrak{q} \subset \mathcal{O}_K$ we have $[L : K] = e_L f_L g_L$ with g_L the number of primes in the factorization of $\mathfrak{q}\mathcal{O}_L$, e_L the ramification index and f_L the inertial degree. We presently consider cases where $e_L = 1$, so $[L : K] = f_L g_L$. Let $\gamma \in \mathcal{O}_L \setminus \mathcal{O}_K$.

Suppose $g_L = 1$, so $\mathfrak{q}$ is inert in L . Then $f_L = [L : K] = d$ and $\bar{L} := \mathcal{O}_L/\mathfrak{q}\mathcal{O}_L$ is a cyclic Galois extension of $\bar{K} := \mathcal{O}_K/\mathfrak{q}$ of degree d . Then we have the following:

Proposition 4.8. *Let $\mathcal{I} = \mathfrak{q}$ be a prime ideal in $\mathcal{O}_K$ which is inert in $\mathcal{O}_L$, and $\mathfrak{q}\mathcal{O}_L = \mathcal{Q}$, $\mathcal{Q}$ a prime ideal in $\mathcal{O}_L$. Then*

$$\Lambda/\mathcal{I}\Lambda \cong ((\mathcal{O}_L/\mathfrak{q}\mathcal{O}_L)/(\mathcal{O}_K/\mathfrak{q}), \bar{\sigma}, \bar{\gamma}) = (\bar{L}/\bar{K}, \bar{\sigma}, \bar{\gamma})$$

is a nonassociative cyclic algebra of degree d over the finite field $\bar{K}$, where $\bar{\gamma} = \gamma \bmod \mathcal{I}$. If d is prime or if $1, \bar{\gamma}, \dots, \bar{\gamma}^{d-1}$ are linearly independent over $\bar{K}$, then this is a central simple division algebra and hence the only proper two-sided ideal $\mathcal{J}$ of Λ that contains $\mathcal{I} = \mathfrak{q}$ is

$$\mathcal{I}\Lambda = \bigoplus_{j=0}^{d-1} u^j \mathfrak{q}\mathcal{O}_L.$$

Proof. [131, Theorem 6.1]. We give the proof because of its importance for the search-to-decision reduction below. Note $\gamma \notin \mathfrak{q}$, i.e. $\bar{\gamma} \in (\mathcal{O}_K/\mathfrak{q})^\times$, so $\Lambda/\mathcal{I}\Lambda \cong ((\mathcal{O}_L/\mathfrak{q}\mathcal{O}_L)/(\mathcal{O}_K/\mathfrak{q}), \bar{\theta}, \bar{\gamma})$ is a degree d nonassociative cyclic algebra over $\mathcal{O}_K/\mathfrak{q}$. By Proposition 4.4, if d is prime or if $1, \bar{\gamma}, \dots, \bar{\gamma}^{d-1}$ are linearly independent over $\mathcal{O}_K/\mathfrak{q}$, $\Lambda/\mathcal{I}\Lambda$ is a division algebra, so any two-sided ideal is trivial. Hence by the correspondence between ideals of Λ containing $\mathcal{I}\Lambda$ and ideals of $\Lambda/\mathcal{I}\Lambda$ the only proper two-sided ideal $\mathcal{J}$ of Λ containing $\mathcal{I}$ is $\mathcal{I}\Lambda$. $\square$

Now, consider the case when $e_L = 1$ still but $g_L > 1$. This is the split case, in which $\mathcal{I}\mathcal{O}_L = \mathcal{Q}_1 \dots \mathcal{Q}_{g_L}$. As in the associative setting, it was shown in [131, §7.3] that $\Lambda/\mathcal{I}\Lambda \cong ((\bar{L}^{(1)} \times \dots \times \bar{L}^{(g)})/\bar{K}, \bar{\theta}, \bar{\gamma})$, where $\bar{L}^{(i)} = \mathcal{O}_L/\mathcal{Q}_i$. To prove that this quotient is a simple ring, we will have to work harder than in the inert case. We require some definitions.

Definition 68. *Let G be a group. A ring $\mathcal{R}$ is G -graded if there are additive subgroups $\mathcal{R}_g \subset \mathcal{R}$,*

for $g \in G$, such that $\mathcal{R} = \bigoplus_{g \in G} \mathcal{R}_g$ and $\mathcal{R}_g \mathcal{R}_h \subseteq \mathcal{R}_{g+h}$, for $g, h \in G$. If $\mathcal{R}_g \mathcal{R}_h = \mathcal{R}_{g+h}$, for $g, h \in G$, then $\mathcal{R}$ is strongly G -graded.

Consider $\Lambda/\mathcal{I}\Lambda = \bigoplus_{i=0}^{d-1} u^i (\mathcal{O}_L/\mathcal{I}\mathcal{O}_L)$. Setting $G = \mathbb{Z}/d\mathbb{Z}$ and $\mathcal{R}_i = u^i \mathcal{O}_L/\mathcal{I}\mathcal{O}_L$, one can see that the $\mathcal{R}_i$ are additive subgroups, and $\mathcal{R}_i \mathcal{R}_j = (u^i \mathcal{O}_L/\mathcal{I}\mathcal{O}_L)(u^j \mathcal{O}_L/\mathcal{I}\mathcal{O}_L) = u^{i+j} \theta^j (\mathcal{O}_L/\mathcal{I}\mathcal{O}_L) \mathcal{O}_L/\mathcal{I}\mathcal{O}_L = u^{i+j} \mathcal{O}_L/\mathcal{I}\mathcal{O}_L = \mathcal{R}_{i+j}$. So $\Lambda/\mathcal{I}\Lambda$ is a strongly $\mathbb{Z}/d\mathbb{Z}$ -graded ring.

Definition 69. Let G be a group and $\mathcal{J}$ a two-sided ideal of a ring $\mathcal{R}$. Then $\mathcal{J}$ is G -graded if $\mathcal{J} = \bigoplus_{g \in G} (\mathcal{J} \cap \mathcal{R}_g)$. The ring $\mathcal{R}$ is called G -graded simple if the only G -graded ideals of $\mathcal{R}$ are $\{0\}$ and $\mathcal{R}$.

We now show $\Lambda/\mathcal{I}\Lambda$ is $\mathbb{Z}/d\mathbb{Z}$ -graded simple for certain ideals $\mathcal{I}$.

Lemma 4.9. Let $\mathcal{I} \subset \mathcal{O}_K$ be an ideal unramified in $\mathcal{O}_L$. Then $\Lambda/\mathcal{I}\Lambda$ is $\mathbb{Z}/d\mathbb{Z}$ -graded simple.

Proof. Equip $\Lambda/\mathcal{I}\Lambda$ with the $\mathbb{Z}/d\mathbb{Z}$ grading as before. We need to show, for any $\mathbb{Z}/d\mathbb{Z}$ -graded ideal $\mathcal{J}$, that in fact $\mathcal{J} = \bigoplus_{i \in \mathbb{Z}/d\mathbb{Z}} \mathcal{J} \cap u^i \mathcal{O}_L/\mathcal{I}\mathcal{O}_L$ is 0 or $\Lambda/\mathcal{I}\Lambda$. Write $\mathcal{I}\mathcal{O}_L = \prod_i \mathcal{Q}_i$. By the correspondence between ideals of Λ containing $\mathcal{I}\Lambda$ and ideals of $\Lambda/\mathcal{I}\Lambda$ and an abuse of notation, write the ideal as $\mathcal{J}/\mathcal{I}\Lambda$. Then $\mathcal{J}/\mathcal{I}\Lambda \cap \prod_i \mathcal{O}_L/\mathcal{Q}_i$ is an ideal of $\prod_i \mathcal{O}_L/\mathcal{Q}_i$, so has the form $\prod_{i \in S} \mathcal{Q}_i / \prod_{i=1}^g \mathcal{Q}_i$ for some $S \subset [g]$. Moreover, by Lemma 4.7, we must have $\theta(\mathcal{J}/\mathcal{I}\Lambda \cap \prod_i \mathcal{O}_L/\mathcal{Q}_i) = \theta(\prod_{i \in S} \mathcal{Q}_i / \prod_{i=1}^g \mathcal{Q}_i) = \prod_{i \in S} \mathcal{Q}_i / \prod_{i=1}^g \mathcal{Q}_i$. But the Galois action on the primes $\mathcal{Q}_i$ above $\mathfrak{q}$ is transitive, so θ cannot fix any such product except when $S = \{1, \dots, g\}$ or $S = \emptyset$. Thus $\mathcal{J}/\mathcal{I}\Lambda \cap \mathcal{O}_L/\mathcal{I}\mathcal{O}_L = \mathcal{J}/\mathcal{I}\Lambda \cap \mathcal{R}_0$ is 0 or $\mathcal{O}_L/\mathcal{I}\mathcal{O}_L$.

Since $\mathcal{J}/\mathcal{I}\Lambda$ is an ideal and γ is invertible, $u^j \mathcal{J}/\mathcal{I}\Lambda = \mathcal{J}/\mathcal{I}\Lambda$, so

$$\begin{aligned} \mathcal{J}/\mathcal{I}\Lambda \cap \mathcal{R}_i &= u^i \cdot \mathcal{J}/\mathcal{I}\Lambda \cap u^i \cdot \mathcal{R}_0 = u^i (\mathcal{J}/\mathcal{I}\Lambda \cap \mathcal{R}_0) \\ &= \begin{cases} 0 & \text{if } \mathcal{J}/\mathcal{I}\Lambda \cap \mathcal{R}_0 = 0 \\ u^i \mathcal{O}_L/\mathcal{I}\mathcal{O}_L & \text{if } \mathcal{J}/\mathcal{I}\Lambda \cap \mathcal{R}_0 = \mathcal{O}_L/\mathcal{I}\mathcal{O}_L. \end{cases} \end{aligned}$$

So the only possibilities for $\mathcal{J}/\mathcal{I}\Lambda$ are $\bigoplus_{i \in \mathbb{Z}/d\mathbb{Z}} 0 = 0$ or $\bigoplus_{i \in \mathbb{Z}/d\mathbb{Z}} u^i \mathcal{O}_L/\mathcal{I}\mathcal{O}_L = \Lambda/\mathcal{I}\Lambda$. $\square$

A group G is *hypercentral* if every non-trivial factor group of G has a non-trivial center. In particular, any abelian group is hypercentral.

Theorem 4.9. [101, Theorem 4] *If a non-associative unital ring is graded by a hypercentral group, then the ring is simple if and only if it is graded simple and the center of the ring is a field.*

From the above discussion we can conclude

Proposition 4.9. *Let $\mathcal{I} = \mathfrak{q}$ be a prime ideal in $\mathcal{O}_K$ which is unramified in $\mathcal{O}_L$, and $\mathfrak{q}\mathcal{O}_L = \mathcal{Q}_1 \dots \mathcal{Q}_g$, where $\mathcal{Q}_i$ is a prime ideal in $\mathcal{O}_L$ for $i = 1, \dots, g$. Let $\gamma \in \mathcal{O}_L^\times \setminus \mathcal{O}_K^\times$. Then*

$$\Lambda/\mathcal{I}\Lambda \cong ((\bar{L}^{(1)} \times \dots \times \bar{L}^{(g)}) / \bar{K}, \bar{\theta}, \bar{\gamma})$$

is a generalised nonassociative cyclic algebra of degree $d = g$ over $\bar{K}$, where $\bar{L}^{(i)}/\bar{K}$ is cyclic Galois. The only proper two-sided ideal $\mathcal{J}$ of Λ that contains $\mathcal{I} = \mathfrak{q}$ is

$$\mathcal{J} = \mathcal{I}\Lambda = \bigoplus_{j=0}^{d-1} u^j \mathfrak{q}\mathcal{O}_L$$

Proof. The first statement is shown in [131, §7.3]. The second statement follows from the facts that 1. $\mathbb{Z}/d\mathbb{Z}$ is hypercentral, 2. the center of $\Lambda/\mathcal{I}\Lambda$ is a field, and 3. $\Lambda/\mathcal{I}\Lambda$ is $\mathbb{Z}/d\mathbb{Z}$ -graded simple. Then Theorem 4.9 implies $\Lambda/\mathcal{I}\Lambda$ is simple, and hence $\mathcal{I}\Lambda$ is maximal in Λ . $\square$

Although we cannot prove a general result on the factorisation of ideals in maximal nonassociative orders, we can prove the following:

Theorem 4.10. *Let $\Lambda \subset \mathcal{A} = (L/K, \theta, \gamma)$ denote the natural order of a nonassociative CDA, with $\gamma \in \mathcal{O}_L$. Let $\mathcal{I} \subset \Lambda$ be an integral two-sided ideal, and $\bar{\mathcal{I}} = \mathcal{I} \cap K$. Suppose the prime factors of $\bar{\mathcal{I}}$ are unramified in L and $\gamma \not\equiv 0 \pmod{\bar{\mathcal{I}}}$. Then $\mathcal{I} = \bar{\mathcal{I}}\Lambda$.*

Proof. Identical to Theorem 3.1. $\square$

The following result then follows:

Theorem 4.11. *Let $\mathcal{A}$ be an algebra as above. Then ideal multiplication of ideals $\mathcal{I}$ such that $\mathcal{I} \cap \mathcal{O}_K$ is unramified in $\mathcal{O}_L$ yields ideals, and is commutative and associative.*

Proof. Let $\mathcal{I}$ and J be two-sided ideals of Λ . Write $\bar{\mathcal{I}} = \mathcal{I} \cap L$. Then $\mathcal{I} = \bar{\mathcal{I}}\Lambda$ and $J = \bar{J}\Lambda$. Then, using that $L = \mathcal{N}(\mathcal{A})$, we have $\mathcal{I}J = (\bar{\mathcal{I}}\Lambda)(\bar{J}\Lambda) = (\bar{\mathcal{I}}(\Lambda\bar{J}))\Lambda = (\bar{\mathcal{I}})\theta(\bar{J})\Lambda = \bar{\mathcal{I}}\bar{J}\Lambda$. It can be seen by a similar argument that $\bar{\mathcal{I}}\bar{J}\Lambda$ is a two-sided ideal of Λ .

Next note that the product of two ideals whose $\mathcal{O}_K$ -intersections are ideals unramified in $\mathcal{O}_L$ is an ideal which also has $\mathcal{O}_K$ -intersection unramified in $\mathcal{O}_L$, so this set of ideals is closed under taking products.

Moreover, $\mathcal{I}J = (\bar{\mathcal{I}}\Lambda)(\bar{J}\Lambda) = \bar{\mathcal{I}}\bar{J}\Lambda = \bar{J}\bar{\mathcal{I}}\Lambda = (\bar{J}\Lambda)(\bar{\mathcal{I}}\Lambda) = J\mathcal{I}$, so ideal multiplication is commutative.

Finally, let K also be a two-sided Λ -ideal. Then $(\mathcal{I}J)K = (\bar{\mathcal{I}}\bar{J}\Lambda)\bar{K}\Lambda = \bar{\mathcal{I}}\bar{J}\bar{K}\Lambda = \bar{\mathcal{I}}\Lambda(\bar{J}\bar{K}\Lambda) = \mathcal{I}(JK)$. So ideal multiplication is also associative. $\square$

For convenience we will call the two-sided ideals satisfying the condition of the theorem ‘unramified ideals of Λ ’.

Inverse Ideals

Let $\mathcal{A} = (L/K, \theta, \gamma)$ with $\gamma \in \mathcal{O}_L^\times \setminus \mathcal{O}_K^\times$, and let $\mathcal{I} = \bar{\mathcal{I}}\Lambda$ be a two-sided unramified ideal of Λ . Then, writing $J = \bar{\mathcal{I}}^{-1}\Lambda$, we have $\mathcal{I} \cdot J = (\bar{\mathcal{I}}\Lambda)(\bar{\mathcal{I}}^{-1}\Lambda) = (\Lambda\bar{\mathcal{I}})(\bar{\mathcal{I}}^{-1}\Lambda) = \Lambda(\bar{\mathcal{I}}(\bar{\mathcal{I}}^{-1}\Lambda)) = \Lambda((\bar{\mathcal{I}}\bar{\mathcal{I}}^{-1})\Lambda) = \Lambda(\mathcal{O}_L\Lambda) = \Lambda$. Thus all such ideals of Λ are invertible. Write $J = \mathcal{I}^{-1}$. Note that J is additively closed, and closed under multiplication on the right from Λ . Moreover, since $\theta(\bar{\mathcal{I}}) = \bar{\mathcal{I}}$, we have $\bar{\mathcal{I}}\bar{\mathcal{I}}^{-1} = \mathcal{O}_L$ implies $\theta(\bar{\mathcal{I}})\theta(\bar{\mathcal{I}}^{-1}) = \bar{\mathcal{I}}\theta(\bar{\mathcal{I}}^{-1}) = \mathcal{O}_L$, and hence $\mathcal{O}_L\theta(\bar{\mathcal{I}}^{-1}) = \bar{\mathcal{I}}^{-1}\mathcal{O}_L$. Since $\bar{\mathcal{I}}^{-1}$ is an $\mathcal{O}_L$ -ideal, $\theta(\bar{\mathcal{I}}^{-1})$ is also an $\mathcal{O}_L$ -ideal, and we obtain $\theta(\bar{\mathcal{I}}^{-1}) = \bar{\mathcal{I}}^{-1}$. So θ fixes $\bar{\mathcal{I}}^{-1}$. Then $\Lambda J = \Lambda(\bar{\mathcal{I}}^{-1}\Lambda) = \Lambda(\Lambda\theta(\bar{\mathcal{I}}^{-1})) = \Lambda(\Lambda\bar{\mathcal{I}}^{-1}) = (\Lambda\Lambda)\bar{\mathcal{I}}^{-1} = \Lambda\bar{\mathcal{I}}^{-1} = \bar{\mathcal{I}}^{-1}\Lambda = J$, and J is closed under multiplication from the left too. So J is a fractional Λ -ideal.

Clearly this means that $(\mathcal{I}^{-1})^{-1} = \mathcal{I}$, so left and right inverse ideals coincide, and hence each ideal has a unique inverse ideal.

Dual Ideals

When the algebra $\mathcal{A}$ is associative, the *dual lattice* of Λ is usually defined

$$\Lambda^\vee = \{x \in \mathcal{A} : \text{Tr}(x\Lambda) \subset \mathbb{Z}\}$$

where Tr refers to the reduced trace, defined $\text{Tr}(a) := \text{Tr}_{K/\mathbb{Q}}(\text{Trace}(\phi(a)))$. Note this trace is a linear map and non-degenerate, and $\Lambda^\vee$ is additively closed. This is (in that scenario) extended to ideals as follows: the *dual* of an ideal $\mathcal{I}$ in an order Λ is defined

$$\mathcal{I}^\vee = \{x \in \mathcal{A} : \text{Tr}(x\mathcal{I}) \subset \mathbb{Z}\}.$$

However, the $\text{Tr}(\cdot)$ map is not symmetric when $\mathcal{A}$ is nonassociative, which causes many familiar results to fail in the case of nonassociative algebras. That is to say, $\text{Tr}(xy) \neq \text{Tr}(yx)$. This can be seen from the matrix representation: as stated above, $\phi : \mathcal{A} \rightarrow M_d(L)$ is not a homomorphism of rings, but rather of vector spaces. This means $\phi(xy) \neq \phi(x)\phi(y)$, so $\text{Tr}(xy) = T_{K/\mathbb{Q}} \circ \text{Trace}(\phi(xy)) \neq T_{K/\mathbb{Q}} \circ \text{Trace}(\phi(x)\phi(y)) = T_{K/\mathbb{Q}} \circ \text{Trace}(\phi(y)\phi(x)) = \text{Tr}(yx)$, in general. It is hence not clear what the definition of $\mathcal{I}^\vee$ should be for ideals in orders in nonassociative algebras. In the absence of a symmetric trace form, we make the following definition:

Definition 70. Let Λ be the natural order of cyclic division algebra $\mathcal{A} = (L/K, \theta, \gamma)$, with $\gamma \in \mathcal{O}_L^\times$ and $[L : K] = d$. Let $\mathcal{I}$ be an ideal of Λ . Then the dual ideal $\mathcal{I}^\vee$ of $\mathcal{I}$ is defined

$$\mathcal{I}^\vee = \bar{\mathcal{I}}^\vee \Lambda,$$

where $\bar{\mathcal{I}} = \mathcal{I} \cap \mathcal{O}_L$.

Before we prove properties of $\mathcal{I}^\vee$, note that it immediately bears some similarities to the usual notion of the dual ideal of, say, an ideal in the ring of integers in a number field. For integral ideals, we have $\mathcal{I} \subset \Lambda \subset \mathcal{I}^\vee$, and $\mathcal{I}^\vee$ is an $\mathcal{O}_K$ -module. Moreover, $(\mathcal{I}^\vee)^\vee = (\bar{\mathcal{I}}^\vee \Lambda)^\vee = (\bar{\mathcal{I}}^\vee \Lambda \cap L)^\vee \Lambda = (\bar{\mathcal{I}}^\vee)^\vee \Lambda = \bar{\mathcal{I}} \Lambda = \mathcal{I}$. Finally, $\mathcal{I}^\vee = \bar{\mathcal{I}}^\vee \Lambda = (\bar{\mathcal{I}}^{-1} \mathcal{O}_L^\vee) \Lambda = (\bar{\mathcal{I}}^{-1} \Lambda)(\mathcal{O}_L^\vee \Lambda) = \mathcal{I}^{-1} \Lambda^\vee$.

We now show:

Proposition 4.10. *Let $\mathcal{I} \subset \Lambda$ be a two-sided integral unramified ideal. Then $\mathcal{I}^\vee$ is a two-sided fractional ideal of Λ .*

Proof. First, we note that additive closure is immediate since both $\bar{\mathcal{I}}^\vee$ and Λ are additively closed.

Now, observe that $\bar{\mathcal{I}}^\vee \subset L = \mathcal{N}(\mathcal{A})$. This means that if $x \in \Lambda$, then $\mathcal{I}^\vee x = (\bar{\mathcal{I}}^\vee \Lambda)x = \bar{\mathcal{I}}^\vee(\Lambda x) \subset \bar{\mathcal{I}}^\vee \Lambda = \mathcal{I}^\vee$, so $\mathcal{I}^\vee$ is closed under multiplication from Λ on the right.

To see closure from left multiplication: we have $\theta(\mathcal{I}^\vee) = \theta(\bar{\mathcal{I}}^\vee \Lambda) = \theta(\bar{\mathcal{I}}^\vee)\theta(\Lambda) = \theta(\bar{\mathcal{I}}^\vee)\Lambda$, where θ acts on Λ coefficient-wise, and is the identity on u^i for all i . Letting $x \in \Lambda$, consider $x \cdot \mathcal{I}^\vee = x(\bar{\mathcal{I}}^\vee \Lambda) = (x\bar{\mathcal{I}}^\vee)\Lambda$. In moving elements of $\bar{\mathcal{I}}^\vee$ past x , powers of the automorphism θ are applied to $\bar{\mathcal{I}}^\vee$ (corresponding to the power of u being ‘moved past’ by the element of $\bar{\mathcal{I}}^\vee$). So if $\theta(\bar{\mathcal{I}}^\vee) = \bar{\mathcal{I}}^\vee$, we would have: $(x\bar{\mathcal{I}}^\vee)\Lambda = (\bar{\mathcal{I}}^\vee x)\Lambda = \bar{\mathcal{I}}^\vee(x\Lambda) \subset \bar{\mathcal{I}}^\vee \Lambda = \mathcal{I}^\vee$, as required.

We conclude the proof by showing that $\theta(\bar{\mathcal{I}}^\vee) = \bar{\mathcal{I}}^\vee$. Let $\mathfrak{m} \subset \mathcal{O}_L$ be an ideal such that $\theta(\mathfrak{m}) = \mathfrak{m}$, and x be in $\mathfrak{m}^\vee$ and $y \in \mathfrak{m}$. We need $\theta(x) \in \mathfrak{m}^\vee$. Clearly $T_{L/\mathbb{Q}}(xy) \in \mathbb{Z}$. We need $T_{L/\mathbb{Q}}(\theta(x)y) \in \mathbb{Z}$ for any $y \in \mathfrak{m}$. Because $\text{Gal}(L/K)$ is cyclic, we can say $T_{L/\mathbb{Q}}(\theta(x)y) = T_{L/\mathbb{Q}}(x\theta^{-1}(y))$; since $\theta(\mathfrak{m}) = \mathfrak{m}$, $\theta^{-1}(y) \in \mathfrak{m}$, and so $T_{L/\mathbb{Q}}(\theta(x)y) = T_{L/\mathbb{Q}}(x\theta^{-1}(y)) \in \mathbb{Z}$. Thus $\theta(x) \in \mathfrak{m}^\vee$, and so $\theta(\mathfrak{m}^\vee) \subset \bar{\mathfrak{m}}^\vee$. Replacing $\mathfrak{m}$ with $\bar{\mathcal{I}}$, this implies that $\mathcal{I}^\vee$ is a two-sided fractional Λ -ideal. $\square$

Proposition 4.11. *Let $\gamma \in \mathcal{O}_L^\times$. Set $J_{\mathcal{I}} := \{x \in \mathcal{A} : \text{Tr}(xy) \in \mathbb{Z} \text{ for all } y \in \mathcal{I}\}$. Then $\mathcal{I}^\vee = J_{\mathcal{I}}$.*

Proof. We begin by showing $\mathcal{I}^\vee \subset J_{\mathcal{I}}$. We have

$$\begin{aligned} \text{Tr}(\mathcal{I}^\vee \mathcal{I}) &= \text{Tr}((\bar{\mathcal{I}}^\vee \Lambda)(\bar{\mathcal{I}} \Lambda)) = \text{Tr}((\bar{\mathcal{I}}^\vee \Lambda) \bar{\mathcal{I}}) \Lambda \\ &= \text{Tr}((\bar{\mathcal{I}}^\vee (\Lambda \bar{\mathcal{I}})) \Lambda) \\ &= \text{Tr}((\bar{\mathcal{I}}^\vee (\theta(\bar{\mathcal{I}}) \Lambda)) \Lambda) \\ &= \text{Tr}((\bar{\mathcal{I}}^\vee (\bar{\mathcal{I}} \Lambda)) \Lambda) \\ &= \text{Tr}((\bar{\mathcal{I}}^\vee \bar{\mathcal{I}}) \Lambda) \Lambda = \text{Tr}((\bar{\mathcal{I}}^\vee \bar{\mathcal{I}}) \Lambda). \end{aligned}$$

Since $\text{Tr}(u^i z_i) = 0$ if $i \neq 0$, we get $\text{Tr}((\bar{\mathcal{I}}^\vee \bar{\mathcal{I}}) \Lambda) = T_{L/\mathbb{Q}}((\bar{\mathcal{I}}^\vee \bar{\mathcal{I}}) \mathcal{O}_L) = T_{L/\mathbb{Q}}(\bar{\mathcal{I}}^\vee \bar{\mathcal{I}}) \in \mathbb{Z}$, since $\gamma \in \mathcal{O}_L$. So for integral Λ -ideals, $\mathcal{I}^\vee = \bar{\mathcal{I}}^\vee \Lambda$ satisfies $\text{Tr}(\mathcal{I}^\vee \mathcal{I}) \subset \mathbb{Z}$ and (similarly) $\text{Tr}(\mathcal{I} \mathcal{I}^\vee) \subset \mathbb{Z}$,

so $\mathcal{I}^\vee \subset J_{\mathcal{I}}$.

It remains to show that $J_{\mathcal{I}} \subseteq \mathcal{I}^\vee$. Take some $x \in J_{\mathcal{I}}$, and $y \in \mathcal{I}$. Write $x = ab$ with $a \in L$ and $b \in \Lambda$ (this can be done for any algebra element). We want to show that x can be written in the form $a'b'$, where $a' \in \bar{\mathcal{I}}^\vee$ and $b' \in \Lambda$. Thus if we show that $a \in \bar{\mathcal{I}}^\vee$, we will be done.

By definition, $\text{Tr}(x\mathcal{I}) \subset \mathbb{Z}$. This implies that $\text{Tr}(x\bar{\mathcal{I}}) \subset \mathbb{Z}$. Substituting for x , we obtain $\text{Tr}((ab)\bar{\mathcal{I}}) \subset \mathbb{Z}$. We can rearrange to obtain $\text{Tr}((a\bar{\mathcal{I}})b) \subset \mathbb{Z}$. Expanding b into the form $b = \sum_{i=0}^{d-1} u^i b_i$ where the $b_i \in \mathcal{O}_L$ and applying additivity of the trace, we have $\text{Tr}((a\bar{\mathcal{I}})b) = T_{L/\mathbb{Q}}(a\bar{\mathcal{I}}b_0) \subset \mathbb{Z}$. So $ab_0 \in \bar{\mathcal{I}}^\vee$.

Now, note that $u\mathcal{I} \subset \mathcal{I}$. Moreover, up to application by θ and multiplication by γ , we can move any coefficient of $x \in \Lambda$ into the 0th position; if $x = \oplus_{i=0}^{d-1} u^i x_i$, we can place x_j in the 0th position via $xu^{d-j} = \gamma\theta^{d-j}(x_j) + u\gamma\theta^{d-j}(x_{j+1}) + \dots + u^{d-1}\theta^{d-j}(x_{j-1})$. Using this trick, one can obtain $\theta^i(a)b_i \in \bar{\mathcal{I}}^\vee$ as follows: $\mathbb{Z} \supset \text{Tr}(x(u^{d-i}\bar{\mathcal{I}})) = \text{Tr}((ab)(u^{d-i}\bar{\mathcal{I}})) = \text{Tr}(((ab)u^{d-i})\bar{\mathcal{I}}) = \text{Tr}((a(bu^{d-i}))\bar{\mathcal{I}}) = T_{L/\mathbb{Q}}(a\gamma\theta^{d-i}(b_i)\bar{\mathcal{I}})$, so $a\theta^{d-i}(b_i) \in \bar{\mathcal{I}}^\vee$, and hence $\theta^i(a)b_i \in \bar{\mathcal{I}}^\vee$. Now observe that $ab = ab_0 + u\theta(a)b_1 + \dots + u^{d-1}\theta^{d-1}(a)b_{d-1}$, so $ab \in \oplus_{i=0}^{d-1} u^i \bar{\mathcal{I}}^\vee \mathcal{O}_L$. $\square$

4.4.3 Nonassociative Cyclic Learning with Errors

We begin by defining lattices from ideal lattices in nonassociative algebras.

Ideals as Lattices and the Canonical Embedding

Since an ideal of an order is an additive subgroup of a lattice, it is itself a lattice. We can embed order ideals in nonassociative CDAs into $\mathbb{R}^n$ using the canonical embedding, as before, to obtain a lattice in $\mathbb{R}^n$. To do this, we consider the matrix representations of order elements, vectorise the columns to obtain vectors with d^2 entries, and apply the canonical embedding of K , which results in a lattice of dimension nd^2 . We take norms of algebra elements by taking the sum of the squares of the Frobenius norm of their matrix representation under the presence of K -embeddings; that is, for $x \in \mathcal{A}$ we have $\|x\|^2 = \sum_{i=1}^n \|\alpha_i(\phi(x))\|_F^2$, where $\|\cdot\|_F$ denotes the Frobenius norm, and $\alpha_i(\phi(x))$ denotes the application of α_i to the entries of $\phi(x)$. This

norm is submultiplicative, and $|\gamma| = 1$ in our applications (since γ is a root of unity).

Recall the family of error distributions used for CLWE:

Definition 71. Let Σ_α be the set of Gaussian distributions Σ over $\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$ whose $(i, j)^{th}$ coordinate has Gaussian marginal distribution with parameter $r_{i,j} \leq \alpha$.

We use the same distributions (mutatis mutandis) in the nonassociative setting.

Cryptographic Problems: Lattices, LWE

Next, we (re)define the lattice problems used in our reductions for the nonassociative setting. We superscript the names we give to them with ‘ ν ’ to distinguish them from their associative counterparts.

Definition 72. Let $\mathcal{A}$ be a nonassociative cyclic algebra and let $\mathcal{I}$ be a (possibly fractional) ideal of the natural order Λ . Then for an approximation factor $\xi = \xi(n) \geq 1$ the (approximate) Order Ideal Shortest Vector Problem, $\mathcal{A}\text{-SVP}_\xi^\nu$, is to find an element $a \in \mathcal{I} \setminus 0$ such that $\|a\| \leq \xi \cdot \lambda_1(\mathcal{I})$.

Definition 73. Let $\mathcal{A}$ be a nonassociative cyclic algebra and $\mathcal{I}$ a fractional ideal of the natural order Λ . Then the (approximate) Shortest Independent Vectors Problem, $\mathcal{A}\text{-SIVP}_\xi^\nu$, is to find nd^2 linearly independent non-zero vectors $\mathbf{x}_1, \dots, \mathbf{x}_{nd^2}$ over $\mathbb{Z}$ such that $\max_i (\|\mathbf{x}_i\|) \leq \xi \cdot \lambda_{nd^2}(\mathcal{I})$, where $\xi \geq 1$.

Definition 74. Let $\mathcal{A}$ be a nonassociative cyclic algebra, let $\mathcal{I}$ be a (possibly fractional) ideal of the natural order Λ , and let $\delta < \lambda_1(\mathcal{I})/2$. Then the $\mathcal{A}\text{-BDD}_{\mathcal{I},\delta}^\nu$ problem, on input $y = x + e$ for $x \in \mathcal{I}$ and $e \in \bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$ satisfying $\|e\|_{2,\infty} \leq \delta$, is to compute x .

Definition 75. For any $q \geq 2$ the $q\mathcal{A}\text{-BDD}_{\mathcal{I},d}^\nu$ problem is as follows: given an instance of the $\mathcal{A}\text{-BDD}_{\mathcal{I},\delta}^\nu$ problem $y = x + e$ with solution $x \in \mathcal{I}$ and error $e \in \bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$ satisfying $\|e\|_{2,\infty} \leq \delta$, output $x \bmod q\mathcal{I}$.

Definition 76. The Discrete Gaussian Sampling problem, denoted $\mathcal{A}\text{-DGS}_\xi^\nu$, is to sample a discrete Gaussian $D_{\mathcal{I},\xi}$, for some order ideal $\mathcal{I}$ and parameter $\xi > 0$.

The lattices obtained from our algebras can be seen as module lattices (i.e. the lattices are isomorphic to module lattices as $\mathcal{O}_K$ -modules), so there is a reduction from $\mathcal{A}$ -SIVP $_{\xi}^{\nu}$ to $\mathcal{A}$ -DGS $_{\xi}^{\nu}$. We now define the nonassociative CLWE (NCLWE) distribution:

Definition 77. Let L/K be a Galois extension of number fields of dimension $[L : K] = d$, $[K : \mathbb{Q}] = n$ with cyclic Galois group generated by $\theta : L \rightarrow L$. Let $\mathcal{A} := (L/K, \theta, \gamma)$ be the resulting nonassociative cyclic algebra with center K and element u satisfying $u^d = \gamma \in \mathcal{O}_L \setminus \mathcal{O}_K$. Let Λ be the natural order of $\mathcal{A}$. For an error distribution ψ over $\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$, an integer modulus $q \geq 2$, and a secret $s \in \Lambda_q^{\vee}$ a sample from the NCLWE distribution $\Pi_{q,s,\psi}^{\nu}$ is obtained by sampling $a \leftarrow \Lambda_q$ uniformly at random, sampling $e \leftarrow \psi$, and outputting

$$(a, b) = (a, (a \cdot s)/q + e \bmod \Lambda^{\vee}) \in \Lambda_q \times \left(\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}} \right) / \Lambda^{\vee}$$

From this distribution we give search and decision problems:

Definition 78. Let Ψ be a family of error distributions over $\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$. Let $\Pi_{q,s,\psi}^{\nu}$ be a NCLWE distribution for parameters $q \geq 2$, arbitrary $s \in \Lambda_q^{\vee}$, and arbitrary error distribution $\psi \in \Psi$. Then, the search NCLWE problem, denoted $SNCLWE_{q,s,\psi}$, is to recover $s \in \Lambda_q^{\vee}$ from a collection of independent samples from $\Pi_{q,s,\psi}^{\nu}$.

Definition 79. Let Υ be a distribution on a family of error distributions Σ_{α} over $\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$ and U_{Λ} the uniform distribution on $\Lambda_q \times \left(\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}} \right) / \Lambda^{\vee}$. Then the decision NCLWE problem, $DNCLWE_{q,\Upsilon}$, is on input a number of independent samples from either $\Pi_{q,s,\psi}^{\nu}$ for a random choice of $(s, \psi) \leftarrow U(\Lambda_q^{\vee}) \times \Upsilon$, or from U_{Λ} , to decide which with non-negligible advantage.

4.4.4 Hardness of NCLWE

We demonstrate the hardness of NCLWE, using the same strategy as [71]. We will need some lemmas.

Technical Lemmas

The following lemmas are proved for $\mathcal{A} = (L/K, \theta, \gamma)$ with $\gamma \in \mathcal{O}_L^\times \setminus \mathcal{O}_K^\times$, since they implicitly require the above results on products, inverses, and duals of ideals.

Lemma 4.10. *Let $\mathcal{I}$ be an invertible ideal of the natural order Λ , and let $\mathcal{J} = q\Lambda$, where q is a prime integer and $q\mathcal{O}_K = \prod_{i=1}^r \mathfrak{q}_i$ is a decomposition into prime ideals. Furthermore, let the $\mathfrak{q}_i$ be unramified in $\mathcal{O}_L$. Assume $\gamma \notin \mathfrak{q}_i$ for each i . Then, there exists an element $t \in \mathcal{I} \cap \mathcal{O}_K$ such that the ideal $t \cdot \mathcal{I}^{-1} \subset \Lambda$ is coprime to $\mathcal{J}$, and we can compute such a t efficiently given $\mathcal{I}$ and the prime factorization of $\mathcal{J}$.*

Proof. Denote $\mathcal{I} \cap \mathcal{O}_K$ by $\bar{\mathcal{I}}$, which is an $\mathcal{O}_K$ -ideal. We know, by [102], that there exists a $t \in \bar{\mathcal{I}}$ such that $t \cdot \bar{\mathcal{I}}^{-1}$ and $q\Lambda \cap \mathcal{O}_K$ are coprime as $\mathcal{O}_K$ -ideals, with $t \in \bar{\mathcal{I}} \setminus \prod_i \mathfrak{q}_i \bar{\mathcal{I}}$. Suppose $t \cdot \mathcal{I}^{-1} + q\Lambda \neq \Lambda$. Then, since they are both two-sided ideals whose sum is a proper ideal, they must be contained in some maximal ideal. By [131, Theorem 6.1] and Proposition 4.9 above, this maximal ideal must have the form $\mathfrak{q}_i \Lambda$, for some i . Thus $t \cdot \mathcal{I}^{-1} \subset \mathfrak{q}_i \Lambda$ and $t \in \mathfrak{q}_i \mathcal{I} \Lambda \cap \mathcal{O}_K = \mathfrak{q}_i \mathcal{I} \cap \mathcal{O}_K$ (note that the product $\mathfrak{q}_i \mathcal{I} \Lambda$ is well-defined). Since t and $\mathfrak{q}_i$ are central we arrive at a contradiction, and the final equality is a consequence of Proposition 4.6. $\square$

Lemma 4.11. *Let $\mathcal{A}$ and q be given as above. Let $\mathcal{I}$ and $\mathcal{J} = q\Lambda$ be ideals of Λ as above, with $t \in \mathcal{I} \cap \mathcal{O}_K$ such that $t \cdot \mathcal{I}^{-1}$ and $q\Lambda$ are coprime as ideals, and let $\mathcal{P}$ be an arbitrary fractional ideal of Λ . Then the function $\chi_t : \mathcal{A} \rightarrow \mathcal{A}, x \mapsto t \cdot x$ induces an $\mathcal{O}_K$ -module isomorphism from $\mathcal{P}/\mathcal{J} \cdot \mathcal{P} \rightarrow \mathcal{I} \cdot \mathcal{P}/\mathcal{I} \cdot \mathcal{J} \cdot \mathcal{P}$. Furthermore, we can efficiently compute the inverse.*

Proof. Since $t \in \mathcal{O}_K$, multiplication by t induces a module homomorphism. Consider the map $\chi_t : \mathcal{P} \rightarrow \mathcal{I} \cdot \mathcal{P}/\mathcal{I} \cdot \mathcal{J} \cdot \mathcal{P}$. Note that because $\mathcal{J}$ is generated by an element in the center (and hence the nucleus) of $\mathcal{A}$, we have $(\mathcal{I} \cdot \mathcal{J}) \cdot \mathcal{P} = (\mathcal{I} \cdot q\Lambda) \cdot \mathcal{P} = q(\mathcal{I} \cdot \Lambda) \cdot \mathcal{P} = (q\mathcal{I}) \cdot \mathcal{P} = \mathcal{I} \cdot q\mathcal{P} = \mathcal{I} \cdot (q\Lambda \mathcal{P}) = \mathcal{I} \cdot (\mathcal{J} \cdot \mathcal{P})$. Let $j \in \mathcal{J} \cdot \mathcal{P}$. Then $\chi_t(j) = t \cdot j \in \mathcal{I} \cdot (\mathcal{J} \cdot \mathcal{P})$, so it is clear that $\mathcal{J} \cdot \mathcal{P}$ is in the kernel of this map. Conversely, if $\chi_t(x) = 0$ then $t \cdot x \in \mathcal{I} \cdot \mathcal{J} \cdot \mathcal{P}$, from which it follows that $\mathcal{I}^{-1} \cdot t \cdot x \subset \mathcal{J} \cdot \mathcal{P}$ (again making use of q and t being nucleic and central). Since $t \cdot \mathcal{I}^{-1}$ and $q\Lambda$ are coprime, $t \cdot \mathcal{I}^{-1} + \mathcal{J} = \Lambda$, and hence there exist $a \in t \cdot \mathcal{I}^{-1}$ and $b \in \mathcal{J}$ such that

$a + b = 1$. We can then write $x = (a + b) \cdot x = a \cdot x + b \cdot x$, and since both $a \cdot x$ and $b \cdot x \in \mathcal{J} \cdot \mathcal{P}$ it follows that $x \in \mathcal{J} \cdot \mathcal{P}$. We thus obtain injectivity. Efficient invertibility follows as in [71]. $\square$

Hardness of Search NCLWE

We now adapt the security proof of [71] to nonassociative CDAs. It will turn out to be very similar; both our lattices and the lattices of [71] can be seen to be modules over $\mathcal{O}_K$, so they are both module lattices as used in [97]. Thus the results of the latter paper that adapt well for CLWE often adapt for NCLWE. Moreover, nonassociativity will not prove a large obstacle in the proofs - the primary result threatened by lack of associativity is Lemma 4.13, yet we circumnavigate this issue via the centrality of the element t from Lemma 4.11.

Lemma 4.12. *For any $q \geq 2$ there is a deterministic polynomial time reduction from $\mathcal{A}$ - $BDD_{\mathcal{I},d}^\nu$ to $q\mathcal{A}$ - $BDD_{\mathcal{I},d}^\nu$.*

Proof. Proved in Lemma 3.5, [136], for arbitrary lattices. $\square$

Lemma 4.13. *There is a ppt. algorithm that on input prime $q \in \mathbb{Z}$, fractional ideal $\mathcal{I}^\vee \subset \Lambda$, a $q\mathcal{A}$ - $BDD_{L, \alpha q \cdot \omega(\sqrt{\log(nd)})/\sqrt{2ndr}}^\nu$ instance $y = x + e$ where $x \in \mathcal{I}^\vee$, $r \geq \sqrt{2}q\eta(\mathcal{I})$, and samples from $D_{\mathcal{I},r'}$ with $r' \geq r$, outputs samples of negligible statistical distance from the NCLWE distribution $\Pi_{q,s,\Sigma}^\nu$, where the secret $s = \chi_t(x \bmod q\mathcal{I}^\vee) \in \Lambda_q^\vee$ and Σ is an error distribution such that if $|\gamma| = 1$ the resulting error e'' has Gaussian marginal distributions each of which is of parameter bounded by α .*

Proof. The first step of the proof is to compute an element $t \in \mathcal{I}$ such that $\mathcal{I}^{-1} \cdot t$ and $q\Lambda$ are coprime using Lemma 4.10. We then create a sample according to the NCLWE distribution by taking one of the Gaussian samples $z \leftarrow D_{\mathcal{I},r'}$, and setting

$$(a, b) = (\chi_t^{-1}(z \bmod q\mathcal{I}), (z \cdot y)/q + e' \bmod \Lambda^\vee) \in \left(\Lambda_q \times \left(\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}} \right) / \Lambda^\vee \right)$$

where $e' \leftarrow D_{\alpha/\sqrt{2}}$. We now prove these samples are of negligible statistical distance from the NCLWE distribution. Since we have $r \geq q \cdot \eta(\mathcal{I})$, by Lemma 2.6 the probability of obtaining

any given $z \bmod q\mathcal{I}$ lies in $\left[\frac{1-\varepsilon}{1+\varepsilon}, 1\right] \cdot \beta$ for some $\beta > 0$, and hence the statistical distance between $z \bmod q\mathcal{I}$ and the uniform distribution is at most 2ε . Since by Lemma 4.11 χ_t is a bijection, $a = \chi_t^{-1}(z \bmod q\mathcal{I})$ is at most statistical distance 2ε from being uniformly distributed over Λ_q . Finally, we show that b has the shape $(a \cdot s)/q + e''$, for an error e'' and uniformly random s , conditioned on some fixed value of a . We have

$$\begin{aligned} b &:= (z \cdot y)/q + e' \bmod \Lambda^\vee \\ &= (z \cdot x)/q + (z \cdot e)/q + e' \bmod \Lambda^\vee \end{aligned}$$

By construction $z = t \cdot a \bmod \Lambda_q^\vee$, and note t lies in both the center and nucleus of $\mathcal{A}$, so we can write $(z \cdot x)/q = ((a \cdot t) \cdot x)/q = (a \cdot (t \cdot x))/q \bmod \Lambda^\vee$ for $s := \chi_t(x \bmod q\mathcal{I}^\vee)$. If x is uniform over $\mathcal{I}^\vee$, then s is uniformly random over $\Lambda_q^\vee$ (since χ_t is bijective). Finally, the analysis of the error proceeds identically to the corresponding result of [71, Lemma 10]. $\square$

The above two lemmas give us a reduction from BDD to NCLWE. If we combine this with a (quantum) proof that given a BDD oracle, we can output a sample from a discrete Gaussian, we will recover the iterative step as in the standard reduction, and this in turn implies a reduction from DGS to NCLWE. The quantum step is as follows:

Lemma 4.14. *There is an efficient quantum algorithm that given any $N = nd^2$ dimensional lattice $\mathcal{L} := \sigma_{\mathcal{A}}(\mathcal{I})$ for some ideal $\mathcal{I} \subset \Lambda$, real $0 < \delta < \lambda_1(\mathcal{L}^*)/(2\sqrt{2nd})$, and an oracle that solves $\mathcal{A}\text{-BDD}_{\mathcal{L}^*, \delta}'$ with all but negligible probability, outputs an independent sample from $D_{\mathcal{L}, \sqrt{d}\omega(\sqrt{\log(nd)})/\sqrt{2\delta^*}}$.*

Proof. Our lattices are a kind of module lattice (as modules over $\mathcal{O}_K$), so the adaptation of [97] holds in this case too. $\square$

We combine these three results to obtain:

Theorem 4.12. *Given an oracle that solves $\text{SNCLWE}_{q,s,\Sigma_\alpha}$ for input $\alpha \in (0, 1)$, an integer $q \geq 2$, an ideal $\mathcal{I} \subset \Lambda$, a number $r \geq \sqrt{2}q \cdot \eta(\mathcal{I})$ satisfying $r' := r \cdot \omega(\sqrt{\log N})/(\alpha q) > \sqrt{2N}/\lambda_1(\mathcal{I}^\vee)$, and polynomially many samples from the discrete Gaussian $D_{\mathcal{I}, r}$ there exists an efficient quantum algorithm that outputs an independent sample from $D_{\mathcal{I}, r'}$.*

Using this theorem, we can obtain:

Theorem 4.13. *Let $\mathcal{A}$ be a nonassociative CDA over a number field L with center K and natural order Λ with $\gamma \in \mathcal{O}_L^\times \setminus \mathcal{O}_K^\times$ and $|\gamma| = 1$. Let $\alpha = \alpha(n) \in (0, 1)$ and $q \geq 2$ unramified in L be parameters such that $\alpha q \geq \omega(1)$. Then there is a polynomial-time quantum reduction from $\mathcal{A}\text{-DGS}_\xi^\nu$ to $\text{SNCLWE}_{q,s,\Sigma_\alpha}$ for any $\xi = r \cdot \sqrt{d}\omega(\sqrt{\log(d \cdot n)})/\alpha q$, where $r > \sqrt{2}q \cdot \eta_\varepsilon(\mathcal{I})$.*

Proof. We prove the result in the standard iterative manner; for a very large value of r , e.g. $r \geq 2^{2N}\lambda_N(\mathcal{I})$, start by sampling classically from $D_{\mathcal{I},r}$. Then apply the above theorem to obtain a polynomial number of samples from $D_{\mathcal{I},r'}$. Iterating this step gives samples from progressively narrower distributions, until we arrive at the desired Gaussian parameter $s \geq \xi$. $\square$

Search to Decision Reduction

Recall the statement of Theorem 4.8: for $\mathcal{I} = \mathfrak{q}_1^{s_1} \dots \mathfrak{q}_t^{s_t} \subset \mathcal{O}_K$ an ideal, we have

$$\begin{aligned} \Lambda/\mathcal{I}\Lambda &\cong ((\mathcal{O}_L/\mathcal{I}\mathcal{O}_L) / (\mathcal{O}_K/\mathcal{I}), \bar{\theta}, \gamma + \mathcal{I}\mathcal{O}_L) = \bigoplus_{i=0}^{d-1} u^i (\mathcal{O}_L/\mathcal{I}\mathcal{O}_L) \\ &\cong ((\mathcal{O}_L/\mathfrak{q}_1^{s_1}\mathcal{O}_L) / (\mathcal{O}_K/\mathfrak{q}_1^{s_1}), \bar{\theta}, \gamma + \mathfrak{q}_1^{s_1}) \times \dots \times ((\mathcal{O}_L/\mathfrak{q}_t^{s_t}\mathcal{O}_L) / (\mathcal{O}_K/\mathfrak{q}_t^{s_t}), \bar{\theta}, \gamma + \mathfrak{q}_t^{s_t}). \end{aligned} \quad (4.2)$$

In the following proof, we write this as

$$\Lambda/\mathcal{I}\Lambda \cong R_1 \times \dots \times R_t.$$

The $R_i\text{-NCLWE}_{q,s,\Sigma_\alpha}$ problem is to find the value $s \bmod R_i$ given access to the NCLWE distribution $\Pi_{q,s,\Sigma}^\nu$ for some arbitrary $\Sigma \in \Sigma_\alpha$. We begin the reduction with the following lemma:

Lemma 4.15. *Let q and Σ_α be as above. There is a deterministic polynomial time reduction from $\text{SNCLWE}_{q,s,\Sigma_\alpha}$ to $R_i\text{-NCLWE}_{q,s,\Sigma_\alpha}$.*

Proof. Adapted from [71, Lemma 13]. We write $\mathcal{O}_i$ for an $R_i\text{-NCLWE}_{q,\Sigma}$ oracle. We will use $\mathcal{O}_i$ to solve $R_j\text{-NCLWE}_{q,s,\Sigma}$ for each j . Define $\alpha_{j/i}$ to be an extension of the K -automorphism

mapping $\mathbf{q}_j$ to $\mathbf{q}_i$ (since $K/\mathbb{Q}$ is Galois, this exists by transitivity) to an isomorphism from $\mathcal{A}$ to $\mathcal{A}' = (L/K, \theta, \alpha_{j/i}(\gamma))$. Note that $\alpha_{j/i}$ fixes $q\Lambda$, since it merely permutes the prime $\mathcal{O}_K$ -ideals in the factorisation of q . Given $(a, b) \leftarrow \Pi_{q,s,\Sigma}^\nu$, consider the sample $(\alpha_{j/i}(a), \alpha_{j/i}(b))$. Since $\alpha_{j/i}$ fixes Λ_q and $\Lambda_q^\vee$, this pair constitutes a valid NCLWE sample in the algebra $\mathcal{A}' = (L/K, \theta, \alpha_{j/i}(\gamma))$. Thus upon sending such samples to $\mathcal{O}_i$, the oracle outputs a value $t_j \bmod R_i$. We now prove that $\alpha_{j/i}^{-1}(t_j) = s \bmod R_j$. Given a sample (a, b) , applying $\alpha_{j/i}$ maps it to a new NCLWE sample $(\alpha_{j/i}(a), \alpha_{j/i}(a \cdot s/q + e) \bmod \Lambda^\vee)$ in $\mathcal{A}'$. Writing the second entry as $\alpha_{j/i}(a) \cdot \alpha_{j/i}(s)/q + \alpha_{j/i}(e) \bmod \Lambda^\vee$, this is a valid NCLWE instance with secret $\alpha_{j/i}(s)$ and error distribution Σ' ; moreover, since a is uniform so is $\alpha_{j/i}(a)$, and $\alpha_{j/i}$ preserves the error distribution so $\alpha_{j/i}(e)$ is correctly distributed. Thus the value t_j which $\mathcal{O}_i$ outputs satisfies $t_j = \alpha_{j/i}(s) \bmod R_i$, and so $\alpha_{j/i}^{-1}(t_j) = s \bmod R_j$. $\square$

We now define an intermediate distribution as follows: for $s \in \Lambda_q^\vee$, distribution Σ over $\bigoplus_j u^j L_{\mathbb{R}}$, and $i \in [n]$, we define a sample from the distribution $\Pi_{q,s,\Sigma}^{\nu,i}$ over $\Lambda_q \times \left(\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}\right) / \Lambda^\vee$ by taking $(a, b) \leftarrow \Pi_{q,s,\Sigma}^\nu$ and $h \in \Lambda_q^\vee$ which is uniformly random and independent mod $R_j, j \leq i$ and 0 mod $R_j, j > i$, and outputting $(a, b + h/q)$. Set $\Pi_{q,s,\Sigma}^{\nu,0} = \Pi_{q,s,\Sigma}^\nu$.

Using this distribution we define a worst-case decision problem relative to one R_i and reduce it to the search problem R_i -NCLWE.

Definition 80. For some $0 < i \leq n$ and family of error distributions Σ_α , the W -D-NCLWE $_{q,s,\Sigma_\alpha}^i$ problem is the problem of finding j given oracle access to $\Pi_{q,s,\Sigma}^{\nu,j}$ for $j \in \{i-1, i\}$ and valid NCLWE secret and error distribution pair (s, Σ) .

Recall q is a prime which factors in $\mathcal{O}_K$ into a product of prime ideals $\prod_{i=1}^{g_K} \mathbf{q}_i$ such that $\mathbf{q}_i$ is unramified in $\mathcal{O}_L$ for all i . This means $\mathbf{q}_i \mathcal{O}_L = \prod_{i=1}^{g_L} \mathcal{Q}_i$. In the next step of the reduction, when $g_L > 1$ we restrict the secret space, such that the secret is to be chosen from a space G in which the difference of any two elements inverts. These sets were called ‘pairwise difference sets’ in [71], and the decomposition into R_i implies $G \cong G_1 \times \dots \times G_t$ for $G_i \in R_i$, a fact we use in the following. The variant of SNCLWE with secrets restricted to such a G is denoted $\text{SNCLWE}_{q,s,\Sigma_\alpha,G}$ and similarly for the other distributions already defined, and moreover the proof of the above Lemma 4.15 holds when the secret is restricted to such sets G . However,

when $g_L = 1$, $\mathfrak{q}_i$ is inert in $\mathcal{O}_L$, and by the proof of Proposition 4.8, R_i is a division algebra. In this specific instance, there is no need to restrict the size of the secret space, since the difference of two distinct elements in a division algebra inverts by definition. When this is the case, $G_i = R_i$.

Lemma 4.16. *Let $q\mathcal{O}_K = \prod_{i=1}^g \mathfrak{q}_i$ and $\bar{K}^{(i)} := \mathcal{O}_K/\mathfrak{q}_i$. Assuming $s \in G$, there is a ppt. reduction from R_i -NCLWE $_{q,s,\Sigma_\alpha,G}$ to W -D-NCLWE $_{q,s,\Sigma_\alpha}^i$ for any $0 < i \leq n$.*

When the $\mathfrak{q}_i$, $i = 1, \dots, g$, are inert in $\mathcal{O}_L$ and either $d = [L : K]$ is prime or $1, \bar{\gamma}, \dots, \bar{\gamma}^{d-1}$ are linearly independent over $\bar{K}^{(i)}$, then (without any assumption on s) there is a ppt. reduction from R_i -NCLWE $_{q,s,\Sigma_\alpha}$ to W -D-NCLWE $_{q,s,\Sigma_\alpha}^i$ for any $0 < i \leq n$.

Proof. We will guess the secret s with a value g ; we can do this efficiently since there are only $|G_i| \leq q^{d^2} = \text{poly}(n)$ possible values of $s \bmod R_i$, since d is considered to be some small constant. To transform $\Pi_{q,s,\Sigma}^\nu$ into either $\Pi_{q,s,\Sigma}^{\nu, i-1}$ if $g = s \bmod R_i$ or $\Pi_{q,s,\Sigma}^{\nu, i}$ otherwise, for $g \in \Lambda_q^\vee$ we take a sample $(a, b) \leftarrow \Pi_{q,s,\Sigma}^\nu$ and set

$$(a', b') := (a + v, b + (h + vg)/q) \in \Lambda_q \times \left(\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}} \right) / \Lambda^\vee,$$

where $v \in \Lambda_q$ is uniformly random mod R_i and 0 mod R_j for $j \neq i$ and $h \in \Lambda_q^\vee$ is uniformly random and independent mod R_j , $j < i$ and 0 on the other R_j . Note $a' \in \Lambda_q$ is uniformly distributed. We now consider the distribution of b' . Conditioning on a fixed a' , we have

$$\begin{aligned} b' &= b + (h + vg)/q = (as + h + vg)/q + e \\ &= (a's + h + v(g - s))/q + e, \end{aligned}$$

where $e \sim \Sigma$. Now observe: if $g = s \bmod R_i$, then $v(g - s) = 0 \bmod R_i$, so (a', b') is distributed according to $\Pi_{q,s,\Sigma}^{\nu, i-1}$. However, if $g \neq s$, then $v(g - s)$ is uniformly random mod R_i (recall $g - s$ inverts by definition of G) and is 0 modulo the other R_j . We can then set $h' = h + v(g - s)$ and the distribution of (a', b') is exactly $\Pi_{q,s,\Sigma}^{\nu, i}$.

The second statement follows since we may choose $G_i = R_i$. □

We now move to obtain a reduction from a worst-case to average-case problem. This section is

mutatis mutandis identical to the corresponding section of [71] (and is very similar to that of [102]) and is included for completeness.

Definition 81. *The distribution Υ_α on the set of possible error distributions is defined by choosing an error distribution $\Sigma \leftarrow \Sigma_\alpha$ and adding it to D_r , where $r_i = \alpha((nd^2)^{1/4} \cdot \sqrt{y_i})$ for $y_1, \dots, y_{nd^2}$ sampled from $\Gamma(2, 1)$.*

Definition 82. *For $i \in [n]$ and distribution Υ_α over possible error distributions, an algorithm solves the $DNCLWE_{q, \Upsilon_\alpha}^i$ problem if with non-negligible probability over $(s, \Sigma) \leftarrow U(\Lambda_q^\vee) \times \Upsilon_\alpha$ it has a non-negligible difference in acceptance probability on inputs from $\Pi_{q, s, \Sigma}^{\nu, i}$ and $\Pi_{q, s, \Sigma}^{\nu, i-1}$.*

Lemma 4.17. *For any $\alpha > 0$ and $i \in [n]$ there is a randomized polynomial-time reduction from $W\text{-}D\text{-}NCLWE_{q, s, \Sigma_\alpha}^i$ to $DNCLWE_{q, \Upsilon_\alpha}^i$.*

Proof. To sample a distribution from Υ_α we sample from Σ_α and add an elliptical Gaussian; this is as in [102, Lemma 5.12], and so, replacing each instance of $\text{mod } \mathbf{q}_i R^\vee$ with $\text{mod } R_i$, and replacing R_q with Λ_q , since associativity isn't used the proof is the same. $\square$

Lemma 4.18. *Let Υ_α be as above and $s \in \Lambda_q^\vee$. Then given a $DNCLWE_{q, \Upsilon_\alpha}$ oracle $\mathcal{O}$, there exists an efficient algorithm that solves $DNCLWE_{q, \Upsilon_\alpha}^i$ for some $i \in [n]$*

Proof. As in the ring case [102, Lemma 5.14] but for substituting the indexing set $\mathbb{Z}_m^*$ with $[n]$. $\square$

We finally obtain:

Theorem 4.14. *Let Λ be the natural order of a nonassociative CDA $\mathcal{A} = (L/K, \theta, \gamma)$, $d = [L : K]$, $q \geq 2$ such that $q\mathcal{O}_K = \prod_{i=1}^g \mathbf{q}_i$ and $\alpha q \geq \eta_\varepsilon(\Lambda^\vee)$ for negligible $\varepsilon = \varepsilon(n)$. Then there is a ppt. reduction from $SNCLWE_{q, s, \Sigma_\alpha, G}$ for any pairwise difference set $G \subset \Lambda_q^\vee$ to $DNCLWE_{q, \Upsilon_\alpha}$. When the $\mathbf{q}_i$ are inert in $\mathcal{O}_L$ and either d is prime or $1, \bar{\gamma}, \dots, \bar{\gamma}^{d-1}$ are linearly independent over $K^{(i)}$, for each i , then there is a ppt. reduction from $SNCLWE_{q, s, \Sigma_\alpha}$ to $DNCLWE_{q, \Upsilon_\alpha}$.*

What is the Security Level of NCLWE?

This section gave a reduction from ideal SIVP from Λ -ideals to search NCLWE, which extends to a partial reduction to decision NCLWE. However, like in Chapter 1, the structure of ideals in Λ in the nonassociative setting implies that the reduction only guarantees that NCLWE is at least as hard as SIVP from ideal lattices in $\mathcal{O}_L$, so is somewhat limited. However, it does give a minimum guarantee of the hardness of NCLWE (for certain parameters) and as such is a positive result. Moreover, it seems that NCLWE is at least as hard as CLWE, since NCLWE lacks the associativity property, which may be useful for cryptanalysis. In addition, NCLWE has its hardness lower bounded by SIVP in a number field, but may be much harder than this problem - we note, for instance, that the reduction from one-sided ideal lattice problems in Chapter 3 may be adaptable to the nonassociative setting. Finally, we note the existence of a polynomial-time search-decision equivalence in the nonassociative setting for certain primes, which may be indicative of greater security for NCLWE than for CLWE. We conclude that NCLWE is likely at least as computationally intractable as CLWE.

4.4.5 PKE from Nonassociative LWE

Let $\mathcal{A} := (L/K, \theta, \gamma)$, where $\mathcal{A}$ is as above, Σ be an error distribution, and q a prime completely split in $\mathcal{O}_L$. We denote the coefficient vector of $a = a_0 + ua_1 + \dots + u^{d-1}a_{d-1}$ by $\mathbf{a} = (a_0, a_1, \dots, a_{d-1})$. Note that $\mathcal{O}_L/q\mathcal{O}_L$ has a (polynomial size) representation of dimension nd , so in our scheme below we encode a binary message $\mathbf{m} \in \{0, 1\}^{nd^2}$ as an element of Λ_q by sending each block of nd entries of m to a coefficient of the element of Λ . Recall the Regev-style cryptosystem, similar to the ‘LPR’ scheme of [102] given for CLWE, for any prime p :

Setup The setup algorithm $\text{Setup}(1^n)$ takes in a security parameter n and outputs a tuple of parameters $\text{params}(n) = ((K = \mathbb{Q}(\zeta_n), L = \mathbb{Q}(\zeta_{pn}), \theta(n), q(n), \alpha(n))$, where $\theta(n)$ generates L/K , $q(n)$ completely splits in K with factors inert in L , and $\alpha(n)$ parameterises the error distribution.

Key Generation $\text{Gen}(1^n)$ runs $\text{Setup}(1^n)$ and from $\text{params}(n)$ generates a CLWE sample $(a, b := a \cdot s + e)$, where $a \in \Lambda_q$ is uniformly random and $e \leftarrow \Sigma$, and outputs public key

$pk = (\mathbf{a}, \mathbf{b})$. The secret key is $sk = s$.

Encryption To encrypt $\mathbf{m} \in \{0, 1\}^{nd^2}$, sample $t, e_1, e_2 \leftarrow \Sigma$ and output $\mathbf{u} := \phi(a)^T \mathbf{t} + \mathbf{e}_1, \mathbf{v} := \phi(b)^T \mathbf{t} + \mathbf{e}_2 + \lceil \frac{q}{2} \rceil \cdot \mathbf{m}$.

Decryption To decrypt, compute $\mathbf{c} = \mathbf{v} - \phi(s)^T \mathbf{u}$ and recover each coordinate of $\mathbf{m}$ by rounding the corresponding entry of $\mathbf{c}$ to 0 or $\lceil \frac{q}{2} \rceil$ and output 0 or 1 respectively.

This scheme is not directly applicable to our context, for the following reason: the matrix representation of nonassociative algebra elements is not a multiplicative map, i.e. $\phi(a)\phi(s) \neq \phi(as)$. To see this explicitly, consider $d = 2$ and set $a = a_0 + ua_1, s = s_0 + us_1$. Then

$$\phi(a) = \begin{pmatrix} a_0 & \gamma\theta(a_1) \\ a_1 & \theta(a_0) \end{pmatrix} \text{ and } \phi(s) = \begin{pmatrix} s_0 & \gamma\theta(s_1) \\ s_1 & \theta(s_0) \end{pmatrix}.$$

Thus

$$\phi(a)\phi(s) = \begin{pmatrix} a_0s_0 + \gamma\theta(a_1)s_1 & a_0\gamma\theta(s_1) + \gamma\theta(a_1)\theta(s_0) \\ a_1s_0 + \theta(a_0)s_1 & a_1\gamma\theta(s_1) + \theta(a_0)\theta(s_0) \end{pmatrix}.$$

On the other hand, $a \cdot s = a_0s_0 + \gamma\theta(a_1)s_1 + u(a_1s_0 + \theta(a_0)s_1)$, and

$$\phi(as) = \begin{pmatrix} a_0s_0 + \gamma\theta(a_1)s_1 & \gamma\theta(a_1)\theta(s_0) + \gamma a_0\theta(s_1) \\ a_1s_0 + \theta(a_0)s_1 & \theta(a_0)\theta(s_0) + \theta(\gamma)a_1\theta(s_1) \end{pmatrix}.$$

So one can see that

$$\phi(as) - \phi(a)\phi(s) = \begin{pmatrix} 0 & 0 \\ 0 & (\theta(\gamma) - \gamma)a_1\theta(s_1) \end{pmatrix}.$$

Thus when one computes $\mathbf{c} = \mathbf{v} - \phi(s)^T \mathbf{u}$, one is left with

$$\mathbf{c} = \begin{pmatrix} 0 & 0 \\ 0 & (\theta(\gamma) - \gamma)a_1\theta(s_1) \end{pmatrix} \mathbf{t} + \mathbf{e}' + \lceil \frac{q}{2} \rceil \mathbf{m},$$

where $\mathbf{e}'$ is an error term. One could absorb $(\theta(\gamma) - \gamma)a_1\theta(s_1)$ into $\mathbf{e}'$, and if $(\theta(\gamma) - \gamma)a_1\theta(s_1)$ is small proceed as usual; however, $a \in \Lambda_q$ is uniformly random so this has low chance of success.

One could encrypt a message with 0 in the lower entry, i.e. $\mathbf{m} = (m \ 0)^T$, and only run the decryption on the entries of $\mathbf{c}$ for which $\phi(as) - \phi(a)\phi(s) = 0$. However, this restricts the number of bits which can be sent. These observations lead us to the following adapted scheme.

LPR-Style Cryptosystem

This scheme decomposes $\phi(as)$ into the sum of two matrices, as follows:

$$\begin{aligned}\phi(as) &= \begin{pmatrix} a_0s_0 + \gamma\theta(a_1)s_1 & a_0\gamma\theta(s_1) + \gamma\theta(a_1)\theta(s_0) \\ a_1s_0 + \theta(a_0)s_1 & a_1\theta(\gamma)\theta(s_1) + \theta(a_0)\theta(s_0) \end{pmatrix} \\ &= \left(\begin{pmatrix} a_0 & \gamma\theta(a_1) \\ a_1 & \theta(a_0) \end{pmatrix} \begin{pmatrix} s_0 \\ s_1 \end{pmatrix} \middle| \begin{pmatrix} \gamma\theta(a_1) & \gamma a_0 \\ \theta(a_0) & \theta(\gamma)a_1 \end{pmatrix} \begin{pmatrix} \theta(s_0) \\ \theta(s_1) \end{pmatrix} \right) \\ &= \left(\begin{pmatrix} a_0 & \gamma\theta(a_1) \\ a_1 & \theta(a_0) \end{pmatrix} \begin{pmatrix} s_0 \\ s_1 \end{pmatrix} \middle| \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right) + \left(\begin{pmatrix} 0 \\ 0 \end{pmatrix} \middle| \begin{pmatrix} \gamma\theta(a_1) & \gamma a_0 \\ \theta(a_0) & \theta(\gamma)a_1 \end{pmatrix} \begin{pmatrix} \theta(s_0) \\ \theta(s_1) \end{pmatrix} \right),\end{aligned}$$

where $|$ denotes concatenation. Set the second two-by-two matrix to be $\phi(\bar{a})$. Then, more succinctly, $\phi(as) = (\phi(a)\vec{s}|0) + (0|\phi(\bar{a})\vec{\theta}(s))$. Observe that $\phi(a)$ corresponds to algebra element $a = a_0 + ua_1$ and $\phi(\bar{a})$ corresponds to algebra element $\bar{a} = \gamma\theta(a_1) + u\theta(a_0)$. This means that, in terms of the below system, retrieving $\mathbf{t}$ or the errors $\mathbf{e}_1, \mathbf{e}_2$ from $\mathbf{u}_1, \mathbf{u}_2$ respectively is equivalent to solving NCLWE with samples $(a, a \cdot s + e_1), (\bar{a}, \bar{a} \cdot \theta(s) + e_2)$. The scheme runs as follows:

Key Generation: Generate an NCLWE sample $(a, b := a \cdot s + e)$, where $a \in \Lambda_q$ is uniformly random and $e \leftarrow \Sigma$, and output public key $(\mathbf{a}, \mathbf{b})$.

Encryption: To encrypt $\mathbf{m} \in \{0, 1\}^{nd^2}$, sample $t, e_1, e_2, e_3 \leftarrow \Sigma$ and output

$$\mathbf{u}_1 = \begin{pmatrix} \phi(a)^T \\ \mathbf{0} \end{pmatrix} \mathbf{t} + \begin{pmatrix} \mathbf{e}_1 \\ 0 \end{pmatrix}, \mathbf{u}_2 = \begin{pmatrix} \phi(\bar{a})^T \\ \mathbf{0} \end{pmatrix} \mathbf{t} + \begin{pmatrix} \mathbf{e}_2 \\ 0 \end{pmatrix}, \text{ and } \mathbf{v} = \phi(b)^T \mathbf{t} + \mathbf{e}_3 + \left\lceil \frac{q}{2} \right\rceil \cdot \mathbf{m}.$$

Decryption: To decrypt, compute $\mathbf{c} := \mathbf{v} - \begin{pmatrix} s_0 & s_1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \mathbf{u}_1 - \begin{pmatrix} 0 & 0 & 0 \\ \theta(s_0) & \theta(s_1) & 0 \end{pmatrix} \mathbf{u}_2$ and round the entries of $\mathbf{c}$ to 0 or $\left\lceil \frac{q}{2} \right\rceil$ and output 0 or 1 respectively.

This scheme utilizes the full hardness of the NCLWE problem. If $d > 2$ one outputs $d + 1$ vectors $\mathbf{v}, \mathbf{u}_1, \dots, \mathbf{u}_d$, and the matrices involved to calculate these vectors are of size $d \times d$. Thus the number of multiplications required by the scheme grows quickly with d . Finally, the redundant zeroes above are for mathematical convenience, but don't need to be outputted. One can instead set $\mathbf{u}_1 = \phi(a)^T \mathbf{t} + \mathbf{e}_1$ and perform decryption with appropriately modified matrices.

Correctness Let us calculate $\mathbf{c}$. We have

$$\mathbf{c} = \mathbf{v} - \begin{pmatrix} s_0 & s_1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \mathbf{u}_1 - \begin{pmatrix} 0 & 0 & 0 \\ \theta(s_0) & \theta(s_1) & 0 \end{pmatrix} \mathbf{u}_2.$$

Plugging in $\mathbf{u}_1$ and $\mathbf{u}_2$, we obtain

$$\mathbf{c} = \mathbf{v} - \begin{pmatrix} s_0 & s_1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \left(\begin{pmatrix} \Phi(a)^T \\ \mathbf{0} \end{pmatrix} \mathbf{t} + \begin{pmatrix} \mathbf{e}_1 \\ 0 \end{pmatrix} \right) - \begin{pmatrix} 0 & 0 & 0 \\ \theta(s_0) & \theta(s_1) & 0 \end{pmatrix} \left(\begin{pmatrix} \Phi(\bar{a})^T \\ \mathbf{0} \end{pmatrix} \mathbf{t} + \begin{pmatrix} \mathbf{e}_2 \\ 0 \end{pmatrix} \right).$$

Expand out, for

$$\begin{aligned} \mathbf{c} &= \phi(b)^T \mathbf{t} + \mathbf{e}_3 + \left\lceil \frac{q}{2} \right\rceil \cdot \mathbf{m} - \begin{pmatrix} s_0 & s_1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \Phi(a)^T \\ \mathbf{0} \end{pmatrix} \mathbf{t} - \begin{pmatrix} s_0 & s_1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \mathbf{e}_1 \\ 0 \end{pmatrix} \\ &\quad - \begin{pmatrix} 0 & 0 & 0 \\ \theta(s_0) & \theta(s_1) & 0 \end{pmatrix} \begin{pmatrix} \Phi(\bar{a})^T \\ \mathbf{0} \end{pmatrix} \mathbf{t} - \begin{pmatrix} 0 & 0 & 0 \\ \theta(s_0) & \theta(s_1) & 0 \end{pmatrix} \begin{pmatrix} \mathbf{e}_2 \\ 0 \end{pmatrix} \\ &= \left(\phi(as)^T - \begin{pmatrix} s_0 & s_1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \Phi(a)^T \\ \mathbf{0} \end{pmatrix} - \begin{pmatrix} 0 & 0 & 0 \\ \theta(s_0) & \theta(s_1) & 0 \end{pmatrix} \begin{pmatrix} \Phi(\bar{a})^T \\ \mathbf{0} \end{pmatrix} \right) \mathbf{t} + \phi(e)^T \mathbf{t} \\ &\quad + \mathbf{e}_3 + \left\lceil \frac{q}{2} \right\rceil \cdot \mathbf{m} - \begin{pmatrix} s_0 & s_1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \mathbf{e}_1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 & 0 \\ \theta(s_0) & \theta(s_1) & 0 \end{pmatrix} \begin{pmatrix} \mathbf{e}_2 \\ 0 \end{pmatrix}. \end{aligned}$$

We then collect the relevant terms involving $\mathbf{t}$, for

$$\begin{aligned}
\mathbf{c} &= \left(\phi(as)^T - \begin{pmatrix} s_0 & s_1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} a_0 & a_1 \\ \gamma\theta(a_1) & \theta(a_0) \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 & 0 \\ \theta(s_0) & \theta(s_1) & 0 \end{pmatrix} \begin{pmatrix} \gamma\theta(a_1) & \theta(a_0) \\ \gamma a_0 & \theta(\gamma)a_1 \\ 0 & 0 \end{pmatrix} \right) \mathbf{t} \\
&\quad + \phi(e)^T \mathbf{t} + \mathbf{e}_3 + \left\lceil \frac{q}{2} \right\rceil \cdot \mathbf{m} - \begin{pmatrix} s_0(\mathbf{e}_1)_1 + s_1(\mathbf{e}_1)_2 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ \theta(s_0)(\mathbf{e}_2)_1 + \theta(s_1)(\mathbf{e}_2)_2 \end{pmatrix} \\
&= \left(\phi(as)^T - \begin{pmatrix} s_0 a_0 + s_1 \gamma \theta(a_1) & s_0 a_1 + s_1 \theta(a_0) \\ \theta(s_0) \gamma \theta(a_1) + \theta(s_1) \gamma a_0 & \theta(s_0) \theta(a_0) + \theta(s_1) \theta(\gamma) a_1 \end{pmatrix} \right) \mathbf{t} \\
&\quad + \phi(e)^T \mathbf{t} + \mathbf{e}_3 + \left\lceil \frac{q}{2} \right\rceil \cdot \mathbf{m} - \begin{pmatrix} s_0(\mathbf{e}_1)_1 + s_1(\mathbf{e}_1)_2 \\ \theta(s_0)(\mathbf{e}_2)_1 + \theta(s_1)(\mathbf{e}_2)_2 \end{pmatrix},
\end{aligned}$$

where $(\mathbf{e}_i)_j$ is the j th coefficient of e_i . Note that $\phi(as)^T$ will be cancelled by the other matrix in the bracket, so

$$\mathbf{c} = \phi(e)^T \mathbf{t} + \mathbf{e}_3 + \left\lceil \frac{q}{2} \right\rceil \cdot \mathbf{m} - \begin{pmatrix} s_0(\mathbf{e}_1)_1 + s_1(\mathbf{e}_1)_2 \\ \theta(s_0)(\mathbf{e}_2)_1 + \theta(s_1)(\mathbf{e}_2)_2 \end{pmatrix} = e' + \left\lceil \frac{q}{2} \right\rceil \cdot \mathbf{m},$$

and if e' is sufficiently small, we round in the same way as usual to recover $\mathbf{m}$.

4.4.6 Concrete Algebras for NCLWE

An example of a method to construct nonassociative CDAs has already been given: let $K = \mathbb{Q}(\zeta_n)$ and $L = \mathbb{Q}(\zeta_{pn})$ where $\gcd(p, n) = 1$. Then $\zeta_{pn} \notin K$, and L/K is cyclic and Galois, so $(L/K, \theta, \zeta_{pn})$ is a nonassociative CDA, since ζ_{pn} does not occur in any proper subfield of L (cf. Proposition 4.4). Clearly $[L : K] = p - 1$, so when $p = 3$ we have an appropriate degree algebra for the stated cryptosystem. Note that we can take ζ_{pn}^k for any k such that $\gcd(pn, k) = 1$ for γ , since that yields a primitive pn th root of unity, and no primitive pn th root of unity is contained in a proper subfield. Moreover, in the case of prime power $n = q^r$, we can create extensions by setting p to be a power of q ; that is, p and n do not need to be coprime, but need to be chosen

such that L/K is cyclic. Below is a table of parameters for possible algebras:

n	p	$[K : \mathbb{Q}]$	$[L : K]$	$[\mathcal{A} : \mathbb{Q}]$
128	5	64	4	1024
256	3,4	128	2	512
256	5	128	4	2048
512	3,4	256	2	1024
243	3,4	162	2	648
243	5	162	4	2592
125	3,4	100	2	400
125	5	100	4	1600
625	3,4	500	2	2000
343	3,4	294	2	1176

Table 4.6: Even Low-degree Nonassociative Algebras

Alternatively, let $L = \mathbb{Q}(\zeta_{pn}) = \mathbb{Q}(\zeta_{3^r \cdot 2^k})$, $K = \mathbb{Q}(\zeta_{3^{r-1} \cdot 2^k})$. Then $[L : \mathbb{Q}] = \phi(3^r \cdot 2^k) = 3^{r-1} \cdot 2^k$, $[K : \mathbb{Q}] = \phi(3^{r-1} \cdot 2^k) = 3^{r-2} \cdot 2^k$, and $[L : K] = 3$. Note L/K is cyclic, so $\mathcal{A} = (L/K, \theta, \zeta_{3^r \cdot 2^k})$ is a nonassociative CDA. Below is a table of parameters for possible algebras:

n	K	p	L	$[K : \mathbb{Q}]$	$[\mathcal{A} : \mathbb{Q}]$
64	$\mathbb{Q}(\zeta_{192})$	9	$\mathbb{Q}(\zeta_{576})$	64	576
64	$\mathbb{Q}(\zeta_{576})$	27	$\mathbb{Q}(\zeta_{1728})$	192	1728
128	$\mathbb{Q}(\zeta_{384})$	9	$\mathbb{Q}(\zeta_{1152})$	128	1152
128	$\mathbb{Q}(\zeta_{1152})$	27	$\mathbb{Q}(\zeta_{3456})$	384	3456
256	$\mathbb{Q}(\zeta_{768})$	9	$\mathbb{Q}(\zeta_{2304})$	256	2304

Table 4.7: Cubic-degree Nonassociative Algebras

Now, consider the case when K is strictly contained within a cyclotomic field. Set $v = 2^k$, $w = 9$, $\mathbb{Q}(\zeta_{vw})^+ = \mathbb{Q}(\zeta_{vw} + \zeta_{vw}^{-1})$. Then $\mathcal{A} = (L/K, \theta, \gamma) = (\mathbb{Q}(\zeta_{vw})/\mathbb{Q}(\zeta_{vw})^+, \theta, \zeta_{vw})$ has

dimension $[L : \mathbb{Q}][L : K] = 2\phi(v)\phi(w) = 2^k \cdot 6 = 2^{k+1}3$. This creates a cyclic division algebra which has degree divisible by only one power of 3. We can also create algebras with degree divisible by higher powers of 3. Below is a table of parameters for possible algebras:

v	w	L	$[L : \mathbb{Q}]$	$[\mathcal{A} : \mathbb{Q}]$
64	27	$\mathbb{Q}(\zeta_{1728})$	576	1152
128	9	$\mathbb{Q}(\zeta_{1152})$	384	768
128	27	$\mathbb{Q}(\zeta_{3456})$	1152	2304
256	9	$\mathbb{Q}(\zeta_{2304})$	768	1536
512	9	$\mathbb{Q}(\zeta_{4608})$	1536	3072

Table 4.8: Nonassociative Algebras Over Maximal Real Subfields

Another way of constructing algebras with similar sizes to those above is as follows. Let $p = 7$ and $n = 2^r$. Setting $L = \mathbb{Q}(\zeta_{7 \cdot 2^r})$ and $K = \mathbb{Q}(\zeta_{2^r}, \sqrt{-7})$, $[L : K]$ is cyclic as $\mathbb{Q}(\sqrt{-7})$ is the unique quadratic subfield of $\mathbb{Q}(\zeta_7)$, and we have $[L : K] = 3$, $[K : \mathbb{Q}] = 2^r$, so $[\mathcal{A} : \mathbb{Q}] = 9 \cdot 2^r$. Finally, we give a construction where $|\gamma| \neq 1$. This leads to some distortion of the error in the proof of Lemma 4.13, but aside from this does not lead to significant complications. Let $K = \mathbb{Q}(\zeta_{p^k})$, where $(p, 7) = 1$, and $L = \mathbb{Q}(\zeta_{p^k}, \zeta_7 + \zeta_7^{-1})$. Then $[L : K] = 3$ and $\mathcal{A} = (L/K, \theta, \zeta_7 + \zeta_7^{-1})$ is a CDA of degree $9(p-1)p^{k-1}$ over $\mathbb{Q}$. In particular, we can construct a degree three extension where $p = 2$, and K has power of two degree. Below is a table of parameters for such algebras.

p^k	$[L : \mathbb{Q}]$	$[\mathcal{A} : \mathbb{Q}]$
128	192	576
256	384	1152
512	768	2304
243	243	729
125	300	900

Table 4.9: Nonassociative Algebras of Cubic Degree over Prime-power Cyclotomics

4.4.7 Operational Complexity

An algorithm was given in [71] to compute the complexity of the multiplication $\phi(a)s$, where a and s are algebra elements in an associative CDA, and q is completely split in K . The complexity of this algorithm was estimated at $O(N \log N/d^2) + \tilde{O}(Nd^{\omega-2})$, where ω is the exponent of matrix multiplication, currently upper-bounded by 2.373 [11]. This is an improvement over that coming from module elements in the same dimension, and we note that the algorithm applies to the nonassociative case also. This is because the complexity of the algorithm relies on the CDAs used for CLWE being quotients of skew polynomial rings, and the algebras used in the current work can also be seen as quotients of skew polynomials (cf. [131]).

4.4.8 Attacking NCLWE

A previous form of structured LWE, called multivariate LWE [123], was attacked in [32]. The basic form of the attack was to find a homomorphism into a subfield of LWE defined over the tensor product of number fields. If the LWE sample is defined over the tensor product $\mathbb{Z}_q[x]/(x^{2^{r_1}} + 1) \otimes \mathbb{Z}_q[x]/(x^{2^{r_2}} + 1)$ with $1 < r_2 \leq r_1$, then one can map a sample of dimension $r_1 r_2$ to r_2 samples of dimension r_1 (see [32] for further detail). We argue here that, in addition to CLWE being immune from this style of attack, so is NCLWE, for an identical reason. Namely, let $\mathcal{A} = (L/K, \theta, \gamma)$ be a nonassociative CDA. Suppose that there is a homomorphism $\chi : \mathcal{A} \rightarrow L$. Then the restriction of χ to L is an automorphism of L . One can see χ must behave as follows: $\chi(u) \cdot \chi(\ell) = \chi(u \cdot \ell) = \chi(\theta(\ell) \cdot u) = \chi(u) \cdot \chi(\theta(\ell))$ for any $\ell \in L$. However, this means that χ is not injective on L , and thus there is no homomorphism to a maximal subfield (or any other subfield). So our construction is immune from this dimension-reducing attack.

4.5 Chapter Summary

In the first part of the chapter we extended the method of construction of CDAs for CLWE to hold for any cyclotomic field K . We used this to compute possible parameter sets for CLWE

instantiations, and showed that in this setting Λ remains a maximal order when γ is a unit.

In the second section we extended the CLWE framework to arbitrary maximal orders in a more general class of CDAs, namely those for which $\gamma \in K$ satisfies the non-norm condition and $|\gamma| = 1$. We also gave examples of computations of such γ . We used this to extend the security proof of the hardness of search CLWE to hold in maximal orders of the CDAs obtained.

The main open problem remaining from that section is to extend the search to decision reduction of CLWE to the larger family of maximal orders considered in this paper. It might also be useful to extend the results to even wider families of algebras.

The focus of the third section was the development of LWE over nonassociative algebras. We developed the ideal theory of nonassociative CDAs, and used this to give a reduction from ideal lattice problems to DNCLWE, which notably included a complete reduction from SNCLWE to DNCLWE, without requiring a restriction of the secret space (for certain primes). We then discussed cryptosystems based on the hardness of the studied problem, and adapted a common scheme to be correct over such CDAs. We discussed the complexity and security of cryptography in nonassociative CDAs, arguing that multiplication can be performed efficiently and that an attack on structured forms of LWE fails to apply to the nonassociative setting. Finally, we gave parameters for the construction of cryptographically useful nonassociative CDAs.

Future work could focus on implementing the above schemes, and developing greater functionality from nonassociative algebras, such as digital signatures, as well as creating new protocols exploiting the novel nonassociative structure.

Chapter 5

On the Security of Group Ring LWE

5.1 Introduction

We now turn from LWE in cyclic algebras to consider a different form of structured MLWE: LWE from group rings.

In [47] LWE was defined for elements taken from the group rings $\mathbb{Z}[D_{2n}]$ where D_{2n} is the dihedral group of cardinality $2n$. If interpreted as a generalisation of MLWE via a matrix representation, one GRLWE sample can be seen to be (loosely) equivalent to two MLWE samples. The authors gave a reduction from lattice problems defined over one-sided group ring ideals to a decision LWE problem, and a PKE scheme.

The main result of this chapter is a dimension-reducing transformation on the GRLWE problem. We show that samples from GRLWE can be invertibly mapped to samples from certain cyclic algebras - though importantly not from CDAs for which the security reductions for CLWE hold. The insecurity of LWE in these algebras allows us to apply a second (invertible) map, which outputs twice the number of samples inputted while halving their dimension. Thus, we can take a GRLWE sample, apply the composition of the two maps, obtain LWE samples in half the original dimension, run lattice attacks on these samples, then invert the mapping to solve the original GRLWE problem.

We then ask whether our method applies to a family of group rings proposed by the authors

of [47], and answer affirmatively (subject to a condition on the choice of basis of a pair of number fields). That is, the dimension-reducing transformation applies to a larger *family* of group rings, not just the specific choice originally proposed.

A natural question to ask following these results might be: to what extent is GRLWE dependent on the choice of group over which we instantiate it? We begin to answer this question by finding a family of groups for which our attack fails (the reason for this failure is explained below). We identify the generalised quaternion groups as a family of groups for which GRLWE appears secure, and prove that our attack cannot be applied in this case. This can be seen as a sort of ‘patch’ to the group ring LWE idea.

We close with a discussion and comparison of existing structured MLWE variants, discussing the attack of [32] on m-RLWE, our attack on GRLWE, and the connection to CLWE.

In more detail, the group rings considered are quotients of group rings of the form

$$\mathbb{Z}[D_{2n}] = \left\{ \sum_{g \in D_{2n}} a_g g : a_g \in \mathbb{Z} \right\}$$

by the ideal $(r^{n/2} + 1)$, where we define the dihedral group

$$D_{2n} = \langle r, s : r^n = e, s^2 = e, srs = r^{-1} \rangle$$

for power-of-two n . In this instance we prove (Lemma 5.2) that

$$R := \mathbb{Z}[D_{2n}] / (r^{n/2} + 1)\mathbb{Z}[D_{2n}]$$

can be considered a maximal order Λ in some cyclic algebra over a number field K , under a map we denote by ϕ .

We then exploit this structure using a lemma of Reiner, which gives a criterion for a cyclic algebra to be isomorphic to a matrix ring (Lemma 5.1) - and this criterion is fulfilled by the image of R under the aforementioned map ϕ to a cyclic algebra. Composing the two maps thus provides an isomorphism from the field of fractions $\varphi \circ \phi : \text{frac}(R) \rightarrow M_2(K)$.

Since the GRLWE samples are defined over $R \bmod qR$, we then consider the induced map $\varphi_q : \Lambda_q \rightarrow M_2(\mathcal{O}_{K_q})$. In particular, while φ is injective, it is not *prima facie* clear that φ_q enjoys nice properties. In this direction, we prove the following:

Theorem 5.1. *(Theorem 5.3, informal) Let q be a prime completely split in the ring of integers of the maximal subfield of $\phi(\text{frac}(R))$. Then $\varphi_q : \Lambda_q \rightarrow M_2(\mathcal{O}_{K_q})$ is a bijection.*

We thus obtain that $\varphi_q \circ \phi : R_q \rightarrow M_2(\mathcal{O}_{K_q})$ is a bijection, and propose the following attack on GRLWE: take a GRLWE sample $(a, b) = (a, as + e) \in R_q \times R_q$. Apply the composition of φ_q and ϕ to (a, b) to obtain a sample $(A, B) \in M_2(\mathcal{O}_{K_q}) \times M_2(\mathcal{O}_{K_q})$. This can be written as $(A, B) = (\varphi_q \circ \phi(a), \varphi_q \circ \phi(b)) = (\varphi_q \circ \phi(a), (\varphi_q \circ \phi(a)) \cdot (\varphi_q \circ \phi(s)) + \varphi_q \circ \phi(e))$. We show that the error is still distributed as an (elliptical) Gaussian, and so (A, B) is a valid LWE sample over K - noting that the transform outputs twice as many samples as we started with, in half the dimension of the original samples. Since the hardness of LWE appears to be superlinear in the dimension, running an off-the-shelf lattice attack on the samples (A, B) has higher likelihood of success than running such attacks on (a, b) . Supposing such an attack outputs $\varphi_q \circ \phi(s)$ (resp. $\varphi_q \circ \phi(e)$), we then invert the map to obtain s (resp. e). We note here that below, in an abuse of notation, we use φ to refer to both the map with domain Λ and the induced map with domain Λ_q .

We also show that this attack holds for a proposed generalisation of the GRLWE problem stated in [47]. The authors pointed out further group rings for which GRLWE could be defined using a group action more generally. However, our methods apply to these scenarios too: we show that we can obtain a map $\text{frac}(R) \rightarrow M_m(K)$ for $m \geq 2$ such that $m \mid \frac{n}{2}$, and prove the following:

Theorem 5.2. *(Theorem 5.5, informal) Let L be a maximal subfield of $\phi(\text{frac}(R))$ and θ an automorphism of L fixing K pointwise, of order m . Suppose $\alpha_1, \dots, \alpha_m$ is a basis of $\mathcal{O}_{L_q}/\mathcal{O}_{K_q}$ such that the matrix*

$$\begin{pmatrix} \alpha_1 & \theta(\alpha_1) & \dots & \theta^{m-1}(\alpha_1) \\ \alpha_2 & \theta(\alpha_2) & \dots & \theta^{m-1}(\alpha_2) \\ \vdots & \vdots & \dots & \vdots \\ \alpha_m & \theta(\alpha_m) & \dots & \theta^{m-1}(\alpha_m) \end{pmatrix}$$

is invertible modulo q . Then the induced map $R_q \rightarrow M_m(\mathcal{O}_{K_q})$ is a bijection.

Using this result, we can extend our attack to this general family of group rings.

We give a table of results using the estimator from [9], demonstrating the approximate loss in security before and after applying our dimension-reducing transformation.

We then proceed to create an integral group ring which appears to be immune to our attack, using the generalized quaternion group, Q_{4n} . We show that certain group rings over Q_{4n} are in fact isomorphic to maximal orders of cyclic *division* algebras (for which CLWE appears hard), and thus our attack fails on them. It is this ‘division’ property which frustrates our attack - in particular, these CDAs do not satisfy the criterion of the lemma of Reiner we used to create the map φ , so our method, applied to these rings, fails at the second step. We prove

Proposition 5.1. (*Proposition 5.3, informal*) *The cyclic algebra*

$$\phi(\text{frac}(\mathbb{Z}[Q_{4n}]/(r^n + 1)\mathbb{Z}[Q_{4n}]))$$

is division.

These group rings, rather than those based on dihedral groups, appear to provide an appropriate platform for the use of GRLWE in cryptography.

5.2 Group Rings and GRLWE

5.2.1 Group Rings

Basic Definitions

Let G be a finite group of cardinality n , and S a commutative ring. Then we define the group ring $S[G]$ as

$$S[G] = \left\{ \sum_{i=1}^n s_i g_i : s_i \in S, g_i \in G \right\}.$$

This becomes a ring by defining addition and multiplication by

$$\sum_{i=1}^n a_i g_i + \sum_{i=1}^n b_i g_i = \sum_{i=1}^n (a_i + b_i) g_i,$$

$$\left(\sum_{i=1}^n a_i g_i \right) \left(\sum_{i=1}^n b_i g_i \right) = \sum_{l=1}^n \left(\sum_{i,j : g_i g_j = g_l} a_i b_j \right) g_l$$

When $S = \mathbb{Z}$ one can embed $\mathbb{Z}[G] \hookrightarrow \mathbb{R}^n$, under which one-sided ideals yield Euclidean lattices. The authors of [47] use the coefficient embedding and $G = D_{2n}$, the n th dihedral group, for n a power of two. For any group ring element $x \in S[G]$, multiplication by x on a fixed basis defines a linear transformation $\Phi(x)$, which is called the regular representation of $S[G]$.

Dihedral Group Rings

The dihedral group of order $2n$, denoted by D_{2n} , has cardinality $2n$ and the presentation

$$D_{2n} = \langle r, s : r^n = e, s^2 = e, srs = r^{-1} \rangle.$$

Commutative groups have only one-dimensional irreducible representations, whereas nonabelian groups may have irreducible representations of larger dimension. The dimension of any irreducible representation of D_{2n} is less than or equal to 2. In the following, n will always be a power of two.

The group ring used in GRLWE [47] is the quotient of a dihedral group ring,

$$R = \mathbb{Z}[D_{2n}] / (r^{n/2} + 1) \mathbb{Z}[D_{2n}].$$

Here we show that GRLWE samples with the above group ring yield structured LWE samples. Let a, t , and $e \in R$. We can write these elements as degree 1 polynomials in s with coefficients being polynomials in r , for example $a = a_0(r) + s \cdot a_1(r)$. If we consider multiplication by a on $\{1, s\}$, we have $a \cdot 1 = a$, $a \cdot s = a_0(r)s + sa_1(r)s = \bar{a}_1(r) + s\bar{a}_0(r)$, where $\bar{\cdot}$ denotes conjugation

by s . Thus we can write $b = a \cdot t + e = A\mathbf{t} + \mathbf{e}$, where

$$A = \begin{pmatrix} a_0(r) & \bar{a}_1(r) \\ a_1(r) & \bar{a}_0(r) \end{pmatrix},$$

and $\mathbf{t}$ and $\mathbf{e}$ are the vectors of coefficients of t and e respectively. These are elements of the polynomial ring $\mathbb{Z}[r]/(r^{n/2} + 1)$, which when n is a power of two is exactly the kind of ring used for RLWE. Thus, expanding the entries of b over the integers as done above, we obtain structured LWE samples. Moreover, one can see from the above matrix A that one GRLWE sample yields structured MLWE samples over a rank 2 module.

5.2.2 Group Ring LWE

Here we define the GRLWE problem(s). As above, let n be a power of two, and

$$R = \mathbb{Z}[D_{2n}] / (r^{n/2} + 1) \mathbb{Z}[D_{2n}].$$

Set

$$R_{\mathbb{R}} = R \otimes_{\mathbb{Z}} \mathbb{R}$$

and let $\mathbb{T} = R_{\mathbb{R}}/R$. Let q be an odd prime. Define

$$R_q = \mathbb{F}_q[D_{2n}] / ((r^{n/2} + 1) \mathbb{F}_q[D_{2n}]).$$

Let Ψ_{α} be the set of Gaussian distributions on $\mathbb{R}^n$ having Gaussian marginal distributions, each with parameter $r_{i,j} \leq \alpha$.

Definition 83. Let R_q be the ring defined above. For an error distribution ψ over $\mathbb{T}$, an integer modulus $q \geq 2$, and a secret $s \in R_q$, a sample from the GRLWE distribution $\Pi_{q,s,\psi}$ is obtained by sampling $a \leftarrow R_q$ uniformly at random, $e \leftarrow \psi$, and outputting $(a, b) = (a, (a \cdot s)/q + e \bmod R) \in R_q \times \mathbb{T}$.

Definition 84. (Search GRLWE). The search GRLWE problem is to find the secret $s \in R_q$,

given a collection of samples $(a_i, b_i) \in R_q \times \mathbb{T}$ taken from $\Pi_{q,s,\psi}$, for arbitrary $s \in R_q$ and $\psi \in \Psi_\alpha$.

Let Υ be a distribution over possible GRLWE error distributions.

Definition 85. (*Decision GRLWE*). The decision GRLWE problem is to distinguish, with non-negligible advantage, whether a collection of independent samples is taken from the GRLWE distribution $\Pi_{q,s,\psi}$ with $s \leftarrow U(R_q)$ and $\psi \leftarrow \Upsilon$, or is taken uniformly at random over $R_q \times \mathbb{T}$.

These problems can also be defined for discretized errors, in which case a sample has the form $(a, as + e) \in R_q \times R_q$. For clarity of exposition we will mostly work with this form of GRLWE.

Public Key Encryption Scheme

The authors then connected these problems to cryptography, giving a PKE scheme, which runs as follows:

Key Generation: Set $sk := (s, e) \in R_q^2$, sampled from the error distribution ψ . Sample $a \leftarrow R_q$ uniformly at random, and set $pk := (a, b) = (a, as/q + e) \in R_q^2$.

Encryption: To encrypt $m \in \{0, 1\}^n$, the authors view the bits of m as coefficients of a polynomial. Then the cipher-text (u, v) is defined

$$(u, v) := (ar/q + e_1, br + e_2 + \lfloor q/2 \rfloor m).$$

where r, e_1, e_2 are sampled from ψ .

Decryption: To decrypt (u, v) , compute $v - su$, to obtain

$$v - su = br + e_2 + \lfloor q/2 \rfloor m - s(ar/q + e_1) = (er - se_1 + e_2) + \lfloor q/2 \rfloor m.$$

If $er - se_1 + e_2$ has small coefficients, one can round to obtain m .

5.3 Attacking Non-division Cyclic Algebras

In this section we explain how cyclic algebras which are not division algebras are open to an attack which converts a larger-dimensional CLWE sample into multiple lower-dimensional CLWE samples, which are easier to solve. Whether a cyclic algebra is division or not depends on the choice of γ : recall from Proposition 2.5 that a cyclic algebra is division if and only if γ is not in the image of the norm. This condition, that γ is a non-norm element of L/K , is required in order to stop parallelizing attacks applying to the CLWE problem. We will later see that the group rings used in GRLWE are isomorphic to cyclic algebras with $\gamma = 1$; a choice of γ which is insecure.

5.3.1 An Isomorphism from Non-division Algebras to ‘Easy’ Algebras

As stated above, to create a division algebra γ is chosen so that γ satisfies the non-norm condition, that is γ^i is not a norm of any element of L for $i = 1, 2, \dots, d-1$. Here, following [72, §5.4], we demonstrate that picking γ that violates this condition leads to vulnerable instances of the CLWE problem. We need the following lemma:

Lemma 5.1. [139, Theorem 30.4] *Let $\mathcal{A} = (L/K, \theta, \gamma)$ be a cyclic algebra with $[L : K] = d$. Let $\gamma, \delta \in K \setminus \{0\}$. Then*

1. $\mathcal{A} \cong \mathcal{A}_i := (L/K, \theta^i, \gamma^i)$ for each i such that $\gcd(i, d) = 1$.
2. If $\gamma = 1$ then $\mathcal{A} \cong M_{d \times d}(K)$.
3. If $\delta = N_{L/K}(\beta)\gamma$ for some non-zero $\beta \in L$ then $\mathcal{A} \cong \mathcal{A}' := (L/K, \theta, \delta)$.

Now, let $\mathcal{A} = (L/K, \theta, \gamma)$ be a cyclic algebra where $\gamma \in \mathcal{O}_K$ is such that $\gamma \in N_{L/K}(L^\times)$. If $(a, a \cdot s + e) \in \Lambda_q \times \Lambda_q$ is a (primal) CLWE instance and a, s are uniform and $e \leftarrow \chi$ is drawn from a Gaussian error distribution, then the isomorphism of part 2. of the above lemma sends $as + e$ to

$$(\mathbf{A}, \mathbf{A} \cdot \mathbf{S} + \mathbf{E})$$

where $\mathbf{A}, \mathbf{S}, \mathbf{E} \in M_{d \times d}(\mathcal{O}_{K_q})$. If this map is smallness preserving, ie. if $e \in \Lambda_q$ is ‘small’ then its image $\mathbf{E}$ has entries in $\mathcal{O}_{K_q}$ which are also ‘small’, then, letting $\mathbf{s}_i, \mathbf{e}_i$ denote the i^{th} columns of $\mathbf{S}, \mathbf{E}$ respectively, $(\mathbf{A}, \mathbf{A}\mathbf{s}_i + \mathbf{e}_i)$ comprises d MLWE samples in dimension n and rank d , for each i . This means one CLWE sample yields d samples of d MLWE instances, where each instance has matrix A , and the i th instance has secret $\mathbf{s}_i$. The difficulty of LWE appears superlinear in the dimension, so solving d MLWE instances in dimension n and rank d should be easier than solving one MLWE instance in dimension nd and rank d . Hence, subject to the assumption that $\mathbf{e}_i$ is small, choosing γ to be a norm of an element of L can be exploited by an attacker.

5.3.2 Analysis of the Error

We now confirm that the isomorphism is smallness preserving, for certain errors, using the analysis of [72, §5.4]. Suppose $\gamma = N_{L/K}(\beta)$. We show that the isomorphism maps a Gaussian distribution on $\mathcal{A}$ to a Gaussian distribution on $\mathcal{A}' = (L/K, \theta, 1)$. Note that the isomorphism mapping $\mathcal{A}$ to $\mathcal{A}'$ fixes L and sends u to $u\beta$, and that the γ which are both roots of unity and in the image of the norm map are norms of a root of unity. We thus find that β is also a root of unity.

The isomorphism mapping $\mathcal{A}'$ to $M_{d \times d}(K)$ is the composition of the following two isomorphisms. The first map, denoted ψ , sends $\mathcal{A}'$ to $\text{Hom}_K(L, L)$, the set of K -linear L -endomorphisms, defined by $x \mapsto f_x(\cdot)$ for $x \in L$, where $f_x(y) = x \cdot y$ for $y \in L$, mapping $u \mapsto \theta$, and extending linearly. The second isomorphism is a map $\text{Hom}_K(L, L) \rightarrow M_{d \times d}(K)$, defined as follows:

1. Fix a K -basis $\{\ell_1, \dots, \ell_d\}$ of L over K .
2. Define $f_j : K \rightarrow L, x \mapsto \ell_j x$.
3. Define $\pi_j : L \rightarrow K, \sum_{i=1}^d x_i \ell_i \mapsto x_j$.
4. Define $\Delta : \text{Hom}_K(L, L) \rightarrow M_{d \times d}(K)$ entrywise via

$$\Delta(\psi)_{i,j} := (\pi_i \circ \psi \circ f_j)(1).$$

Note that the above is constructive. This isomorphism is not unique, since it depends on the choice of K -basis of L . We assumed $e = \sum_{i=0}^{d-1} u^i e_i \in \Lambda_q$ was sampled according to a discrete Gaussian, where the e_i are sampled independently from a discrete Gaussian over $\mathcal{O}_L$. Computing the i, j th entry of $\Delta(e)$ gives

$$\pi_i \left(\sum_{k=0}^{d-1} e_k \theta^k(\ell_j) \right)$$

The j^{th} column of $\Delta(e)$ is then the ℓ_i coordinate of $\sum_{k=0}^{d-1} e_k \theta^k(\ell_j)$.

As mentioned, the distribution of the resulting error depends on the basis $\{\ell_1, \dots, \ell_d\}$. Since the e_k are taken from independent discrete Gaussians over $\mathcal{O}_L$ and the action of θ merely permutes the entries of the canonical embedding, $\sum_{k=0}^{d-1} e_k \theta^k(\ell_j)$ is an elliptical Gaussian with n blocks of d different parameters. Since $\sigma_L(\ell_k)$ is distributed independently of k when $\{\ell_1, \dots, \ell_d\}$ is a cyclic basis, then $\pi_i \left(\sum_{k=0}^{d-1} e_k \theta^k(\ell_j) \right)$ follows an elliptical Gaussian.

We will denote the isomorphism $\mathcal{A} \rightarrow M_d(K)$ by φ in future sections. We give some examples of the image of this isomorphism.

Example 5.1. For any $x = x_0 + ux_1 = a_0 + ia_1 + u(b_0 + ib_1) \in \Lambda \subset \mathcal{A} = (\mathbb{Q}(i)/\mathbb{Q}, \theta, 1)$, the image of x under the isomorphism of Lemma 5.1 with respect to the basis $\{1, i\}$ of $\mathbb{Z}[i]$ over $\mathbb{Z}$ is

$$x \mapsto \begin{pmatrix} a_0 + b_0 & b_1 - a_1 \\ a_1 + b_1 & a_0 - b_0 \end{pmatrix}.$$

Proof. The isomorphism consists of the composition of a mapping from $\mathcal{A}$ to $\text{Hom}_{\mathbb{Q}}(\mathbb{Q}(i), \mathbb{Q}(i))$, sending $x \in \mathbb{Q}(i)$ to the multiplication function $f_x(y) = x \cdot y$ for $y \in \mathbb{Q}(i)$ and sending u to θ , and the isomorphism sending $\text{Hom}_{\mathbb{Q}}(\mathbb{Q}(i), \mathbb{Q}(i))$ to $M_d(\mathbb{Q})$. We have a basis $\{1, i\}$. We find

$$\begin{aligned} \Delta(x)_{j,1} &= (\pi_j \circ x \circ f_1)(1) = (\pi_j \circ x)(1) = \pi_j(x_0 \theta^0(1) + x_1 \theta(1)) = \pi_j(x_0 + x_1) \\ &= \begin{cases} a_0 + b_0 & j = 1 \\ a_1 + b_1 & j = 2 \end{cases} \end{aligned}$$

and

$$\begin{aligned}\Delta(x)_{j,2} &= (\pi_j \circ x \circ f_2)(1) = (\pi_j \circ x)(i) = \pi_j(x_0\theta^0(i) + x_1\theta(i)) = \pi_j(i(x_0 - x_1)) \\ &= \pi_j(b_1 - a_1 + i(a_0 - b_0)) = \begin{cases} b_1 - a_1 & j = 1 \\ a_0 - b_0 & j = 2 \end{cases}.\end{aligned}$$

□

We now show how changing the choice of basis may yield a simpler map φ .

Example 5.2. For any $x = x_0 + ux_1 = a_0 + ia_1 + u(b_0 + ib_1) \in \Lambda \subset \mathcal{A} = (\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+, \theta, 1)$, where $\mathbb{Q}(\zeta_n)^+ := \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, $\theta \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n + \zeta_n^{-1}))$ maps $\zeta_n \mapsto \zeta_n^{-1}$, fixing $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, and $n = 2^r$ for some $r \geq 2$, the image of x under the isomorphism of Lemma 5.1 with respect to the cyclic basis $\{\ell_1, \ell_2\}$ of $\mathbb{Z}[\zeta_n]/q\mathbb{Z}[\zeta_n]$ over $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]/q\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ is

$$\varphi(x) = \begin{pmatrix} a_0 & b_0 \\ b_1 & a_1 \end{pmatrix} \bmod q$$

Proof. We have

$$\begin{aligned}\Delta(x)_{j,1} &= (\pi_j \circ x \circ f_1)(1) = (\pi_j \circ x)(\ell_1) = \pi_j(x_0\theta^0(\ell_1) + x_1\theta(\ell_1)) \\ &= \pi_j(x_0\ell_1 + x_1\ell_2) = \pi_j((a_0\ell_1 + a_1\ell_2)\ell_1 + (b_0\ell_1 + b_1\ell_2)\ell_2) \\ &= \pi_j(a_0\ell_1 + b_1\ell_2) = \begin{cases} a_0, & j = 1 \\ b_1, & j = 2 \end{cases}, \\ \Delta(x)_{j,2} &= (\pi_j \circ x \circ f_2)(1) = (\pi_j \circ x)(\ell_2) = \pi_j(x_0\theta^0(\ell_2) + x_1\theta(\ell_2)) \\ &= \pi_j(x_0\ell_2 + x_1\ell_1) = \pi_j((a_0\ell_1 + a_1\ell_2)\ell_2 + (b_0\ell_1 + b_1\ell_2)\ell_1) \\ &= \pi_j(a_1\ell_2 + b_0\ell_1) = \begin{cases} b_0, & j = 1 \\ a_1, & j = 2 \end{cases}.\end{aligned}$$

□

The upshot of the above discussion is that when γ is in the image of the field norm, from a single CLWE instance one can construct d samples of d rank d MLWE instances over a field of dimension n where the error is well-behaved. The resulting MLWE instances could be attacked with any off-the-shelf MLWE solver, and appear much easier to solve than the original nd -dimensional instance. When γ is not a norm and the algebra is a division algebra, no such attack is possible.

5.4 An Isomorphism Between Dihedral Group Rings and Cyclic Algebras

Any element a of R can be written $a = a_0(r) + sa_1(r)$. This motivates the following map: set $\Lambda = \mathcal{O}_L \oplus u\mathcal{O}_L$ to be the natural order in the degree 2 cyclic algebra $\mathcal{A} = (L/K, \theta, \gamma)$, where $L = \mathbb{Q}(\zeta_n)$ is the n th cyclotomic field, θ is the map on $L = \mathbb{Q}(\zeta_n)$ sending $\zeta_n \mapsto \zeta_n^{-1}$ and extended linearly, K is the subfield of L fixed by this map, $K = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, and $\gamma = 1$. Then define

$$\phi : R \rightarrow \Lambda, \text{ mapping } r \mapsto \zeta_n \text{ and } s \mapsto u,$$

for ζ_n a primitive n th root of unity.

In this section, we show that the map ϕ is a ring isomorphism. We first show that it is a homomorphism, for completeness, before proving bijectivity.

Lemma 5.2. *The map ϕ defined above is an isomorphism of rings from R to Λ .*

Proof. Firstly, we show that ϕ does indeed map into Λ . Clearly $\phi(R)$ lies in $\mathbb{Z}[\zeta_n] \oplus u\mathbb{Z}[\zeta_n]$, so $\phi(R)$ lies in $\mathcal{O}_L \oplus u\mathcal{O}_L$. To see that the structure of Λ is correct: $1 = \phi(s^2) = u^2$, and $\phi(\bar{a}(r)) = \phi(sa(r)s) = ua(\zeta_n)u = \theta(a(\zeta_n))$. Then $s\bar{a}(r) = ssa(r)s = a(r)s$, so $\phi(s\bar{a}(r)) = \phi(s)\phi(\bar{a}(r)) = u\theta(a(\zeta_n))$, and $\phi(s\bar{a}(r)) = \phi(a(r)s) = a(\zeta_n)u$, so $a(\zeta_n)u = u\theta(a(\zeta_n))$. Thus u has the desired properties. Finally, since θ corresponds to $\bar{\cdot}$, and the center of R is the elements $a = a_0(r) + sa_1(r)$ such that $a_1(r) = 0$ and $a_0(r) = \bar{a_0(r)}$, $\phi(Z(R)) = K$, and ϕ really does map elements of R to elements of Λ .

Clearly $\phi(0) = 0$ and $\phi(1) = 1$. Moreover, to show additivity, let $a, b \in R$. Then $\phi(a + b) = \phi(a_0(r) + sa_1(r) + b_0(r) + sb_1(r)) = \phi(a_0(r) + b_0(r) + s(a_1(r) + b_1(r))) = \phi(c_0(r) + sc_1(r)) = c_0(\zeta_n) + uc_1(\zeta_n) = a_0(\zeta_n) + b_0(\zeta_n) + s(a_1(\zeta_n) + b_1(\zeta_n)) = \phi(a) + \phi(b)$.

To show multiplicativity:

$$\begin{aligned}
\phi(ab) &= \phi((a_0(r) + sa_1(r))(b_0(r) + sb_1(r))) \\
&= \phi(a_0(r)b_0(r) + a_0(r)sb_1(r) + sa_1(r)b_0(r) + sa_1(r)sb_1(r)) \\
&= \phi(a_0(r)b_0(r) + \overline{a_1}(r)b_1(r) + s(\overline{a_0}(r)b_1(r) + a_1(r)b_0(r))) \\
&= \phi(a_0(r)b_0(r)) + \phi(\overline{a_1}(r)b_1(r)) + \phi(s\overline{a_0}(r)b_1(r)) + \phi(sa_1(r)b_0(r)) \\
&= a_0(\zeta_n)b_0(\zeta_n) + \overline{a_1}(\zeta_n)b_1(\zeta_n) + u\overline{a_0}(\zeta_n)b_1(\zeta_n) + ua_1(\zeta_n)b_0(\zeta_n).
\end{aligned}$$

By definition, $\overline{a_0}(\zeta_n)$ and $\overline{a_1}(\zeta_n)$ are equal to $\theta(a_0(\zeta_n))$ and $\theta(a_1(\zeta_n))$ in L : for example, $\overline{a_0}(\zeta_n) = \phi(\overline{a_0}(r)) = \phi(a_0(r^{-1})) = a_0(\zeta_n^{-1}) = \theta(a_0(\zeta_n))$. Since $\gamma = 1$, we can write

$$\begin{aligned}
\phi(ab) &= a_0(\zeta_n)b_0(\zeta_n) + \overline{a_1}(\zeta_n)b_1(\zeta_n) + u\overline{a_0}(\zeta_n)b_1(\zeta_n) + ua_1(\zeta_n)b_0(\zeta_n) \\
&= a_0(\zeta_n)b_0(\zeta_n) + \gamma\theta(a_1(\zeta_n))b_1(\zeta_n) + u\theta(a_0(\zeta_n))b_1(\zeta_n) + ua_1(\zeta_n)b_0(\zeta_n) \\
&= (a_0(\zeta_n) + ua_1(\zeta_n))(b_0(\zeta_n) + ub_1(\zeta_n)) \\
&= \phi(a)\phi(b),
\end{aligned}$$

as required. So ϕ is a ring homomorphism.

Finally, we need to show bijectivity. Surjectivity is clear. To prove injectivity, suppose $x \in \ker(\phi)$ is non-zero. Then $\phi(x_0(r)) = x_0(\zeta_n) = 0$ and $\phi(x_1(r)) = x_1(\zeta_n) = 0$. The x_i , $i = 1, 2$, are polynomials in $\mathbb{Z}[X]/(X^{n/2} + 1)$ and since ζ_n is a complex root of $X^{n/2} + 1$ when n is a power of two, $\mathbb{Z}[X]/(X^{n/2} + 1) \cong \mathbb{Z}[\zeta_n]$. So if an integer polynomial evaluated at ζ_n is 0, the polynomial in indeterminate X is 0 mod $X^{n/2} + 1$. Thus $x_0(r)$ and $x_1(r)$ are equal to 0 in $\mathbb{Z}[r]/(r^{n/2} + 1)$, which is a contradiction. So ϕ is a ring isomorphism. $\square$

In summary, there is an isomorphism between $\mathbb{Z}[D_{2n}]/(r^{n/2} + 1)\mathbb{Z}[D_{2n}]$ and $\mathcal{O}_L \oplus u\mathcal{O}_L$ when n is a power of two and L is the n th cyclotomic field, θ is complex conjugation, and $\gamma = 1$.

Thus $\mathbb{Z}[D_{2n}]/(r^{n/2} + 1)\mathbb{Z}[D_{2n}]$ injects into a cyclic algebra with γ which is a norm, and hence GRLWE samples are invertibly mapped to CLWE samples which are vulnerable to the attack stated in the previous section. In the following sections, we explain the attack concretely, and analyse and discuss the consequences.

5.5 Attacking Group Ring LWE

Recall the above notation: let n be a power of two,

$$R = \mathbb{Z}[D_{2n}] / (r^{n/2} + 1) \mathbb{Z}[D_{2n}],$$

For q be an odd prime, set

$$R_q = R/qR = \mathbb{F}_q[D_{2n}] / ((r^{n/2} + 1) \mathbb{F}_q[D_{2n}]).$$

Let $(a, b) = (a, as + e \bmod q) \in R_q \times R_q$ be a primal GRLWE sample. We can write $b = ((a_0(r) + sa_1(r))(s_0(r) + ss_1(r)) + e_0(r) + se_1(r))$. By extending ϕ to R_q by setting $\phi(x + qR) = \phi(x) + q\Lambda$, we have $\phi(R_q) = \Lambda_q$, and denoting the image of element $x \in R$ in Λ by x' , we have that a is mapped to $a' \in \Lambda_q$. Moreover, $\phi(b) = b' = a's' + e' \in \Lambda_q$, with $s', e' \in \Lambda_q$, as above. In addition, it is clear that ϕ preserves the size of the error term e , and the image of the GRLWE sample is distributed correctly, according to a CLWE sample for the above stated parameters. Then, using the isomorphism of Lemma 5.1 for algebras with $\gamma = 1$, transform $(\phi(a), \phi(b)) = (a', b')$ into a sample over $M_2(\mathcal{O}_{K_q}) \times M_2(\mathcal{O}_{K_q})$, denoted $(A, B = AS + E)$, with A, S , and $E \in M_2(\mathcal{O}_{K_q})$.

Solving the two instances of MLWE given by (A, B) is easier than solving the one instance of CLWE given by (a', b') : observe that (A, B) represents two CLWE samples from each of two instances of CLWE (that is, CLWE instances with two different secrets, s_1 and s_2 , which comprise the columns of S), and writing $(A, As_i + e_i)$, $i = 1, 2$, for the two samples from each instance of CLWE, one can see that $(A, As_i + e_i)$ corresponds to two MLWE samples of

dimension $[K : \mathbb{Q}] = n/2$ and module rank 2, whereas (a', b') represents two MLWE samples from one CLWE instance (that is, with only one secret, s), each in dimension $2 \cdot [K : \mathbb{Q}] = n$ and module rank 2.

Now observe that the restriction of φ to Λ , $\varphi|_\Lambda$, gives a map $\Lambda \hookrightarrow M_2(\mathcal{O}_K)$ which is injective but not necessarily surjective. However, the map induced by taking φ modulo q from $\Lambda_q \rightarrow M_2(\mathcal{O}_{K_q})$ is surjective for certain primes:

Theorem 5.3. *Let $K = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, $L = \mathbb{Q}(\zeta_n)$, $\theta = \bar{\cdot}$ denote complex conjugation, and $n = 2^r$, $r \geq 2$. Let $q > 2$ be a prime completely split in $\mathcal{O}_L$. Then the map φ with respect to a cyclic basis, $\varphi : \Lambda_q \rightarrow M_2(\mathcal{O}_{K_q})$, is bijective.*

Proof. Write the factorisations of q as $q\mathcal{O}_K = \prod_{i=1}^{g_K^q} \mathfrak{p}_i$ and $q\mathcal{O}_L = \prod_{j=1}^{g_L^q} \mathcal{P}_j$. Observe that $|\Lambda_q| = |\mathcal{O}_L/q\mathcal{O}_L|^2 = |\mathcal{O}_L/\mathcal{P}_i|^{2g_L^q} = q^{2f_L^q g_L^q} = q^{2[L:\mathbb{Q}]}$. We also have $|M_2(\mathcal{O}_K/q\mathcal{O}_K)| = |M_2(\mathcal{O}_K/\prod_{i=1}^{g_K^q} \mathfrak{q}_i)| = |M_2(\mathcal{O}_K/\mathfrak{q}_i)|^{g_K^q} = (q^{4f_K^q})^{g_K^q} = q^{4f_K^q g_K^q} = q^{4[K:\mathbb{Q}]}$. Since $[L : \mathbb{Q}] = 2[K : \mathbb{Q}]$, the sets have equal cardinality, that is Λ_q and $M_2(\mathcal{O}_{K_q})$ have the same size.

Next, fix the cyclic basis $\{\ell_1, \ell_2\}$ of $\mathcal{O}_{L_q}/\mathcal{O}_{L_q^+}$. As in Example 5.2 we have $\varphi(x) = \begin{pmatrix} a_0 & b_0 \\ b_1 & a_1 \end{pmatrix} \bmod q \in M_2(\mathcal{O}_{K_q})$. This is plainly surjective. Then we have a surjection between sets of equal cardinality, so we have a bijection. $\square$

Thus applying lattice reduction techniques, such as the BKZ algorithm, to the resulting MLWE samples and applying the inverse transformations allows an attacker to recover the secret s in less time than on the original CLWE samples. We demonstrate the approximate loss in security of this procedure to GRLWE in the next section. We conclude the present section with a theorem statement of our main result, considering the GRLWE errors to be sampled from continuous Gaussians. We let $\text{MLWE}_{q,n,s,D_\alpha,d,m}$ denote an MLWE instance with modulus q , ring dimension n , secret s , error distribution D_α in the appropriate dimension, module rank d , and number of samples m . Similarly, we let $\text{GRLWE}_{q,n,s,D_\alpha,m}$ denote a GRLWE instance with modulus q , ring dimension n , secret s , error distribution D_α in the appropriate dimension, and number of samples m .

Theorem 5.4. *Let $q \geq 3$ be an odd prime completely split in $\mathcal{O}_L$, $n \geq 2$ a power of 2, $m \geq 1$, and $\alpha > 0$. Let $L := \mathbb{Q}(\zeta_n)$ be the n th cyclotomic field, $K := L \cap \mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, $R := \mathbb{Z}[D_{2n}]/(r^n + 1)\mathbb{Z}[D_{2n}]$ and $R_q := \mathbb{Z}_q[D_{2n}]/(r^n + 1)\mathbb{Z}[D_{2n}]$. Let $s \in R_q$. Then $\text{GRLWE}_{q,n,s,D_\alpha,m}$ reduces to solving $\text{MLWE}_{q,\frac{n}{2},s_1,D_\alpha,2,2m}$ and $\text{MLWE}_{q,\frac{n}{2},s_2,D_\alpha,2,2m}$, where s_i is the i th column of $\varphi(s) \in \mathcal{O}_{K_q}^{2 \times 2}$.*

Proof. We apply φ to m samples from $\text{GRLWE}_{q,n,s,D_{R,\alpha},m}$, denoted $(a^{(i)}, a^{(i)}s + e^{(i)} \bmod q)$, $i = 1, \dots, m$. Each application yields a sample of the form

$$(\varphi(a^{(i)}), \varphi(a^{(i)}s + e^{(i)}) \bmod q) = (A^{(i)}, A^{(i)}S + E^{(i)} \bmod q),$$

which lies in $\mathcal{O}_{K_q}^{2 \times 2} \times (K_{\mathbb{R}}/q\mathcal{O}_K)^{2 \times 2}$. Denote the columns of S by s_k , $k = 1, 2$. Since the $A^{(i)}$ and $E^{(i)}$ are 2×2 matrices, $(A^{(i)}, A^{(i)}S + E^{(i)})$ can be rewritten

$$(A^{(i)}, A^{(i)}s_k + E_k^{(i)}) \in \mathcal{O}_{K_q}^2 \times (K_{\mathbb{R}}/q\mathcal{O}_K)^2,$$

where $E_k^{(i)}$ denotes the k th column of $E^{(i)}$. This constitutes two samples of $\text{MLWE}_{q,\frac{n}{2},s_k,D_{\alpha_k},2}$ for some α_k , so overall we obtain $2m$ such samples. It only remains to compute α_k .

We note that $\mathcal{A} \otimes \mathbb{R} \cong M_2(K \otimes \mathbb{R})$, and consider our errors to be sampled from the torus $\Lambda \otimes \mathbb{R}/q(\Lambda \otimes \mathbb{Z})$. We then extend φ to $\Lambda \otimes \mathbb{R}/q(\Lambda \otimes \mathbb{Z})$ by setting $\varphi(x) := \begin{pmatrix} a_0 & b_0 \\ b_1 & a_1 \end{pmatrix}$ for any $x \in \Lambda \otimes \mathbb{R}/q(\Lambda \otimes \mathbb{Z}) = \mathcal{O}_{L_q} \otimes \mathbb{R}/q\mathbb{Z} + u(\mathcal{O}_{L_q} \otimes \mathbb{R}/q\mathbb{Z})$, writing the $\mathcal{O}_{L_q}$ -components of the x_i in terms of the cyclic basis $\{\ell_1, \ell_2\}$.

Thus the image of an error e under φ is $\begin{pmatrix} a_0 & b_0 \\ b_1 & a_1 \end{pmatrix} \bmod q$, where we write $e = e_0 + ue_1 = a_0\ell_1 + a_1\ell_2 + u(b_0\ell_1 + b_1\ell_2)$, considering e as an element of $\Lambda_{\mathbb{R}}$. Since we sample a continuous Gaussian over $\Lambda_{\mathbb{R}}$ (respectively $K_{\mathbb{R}}$) $D_{\Lambda_{\mathbb{R}},\alpha}$ (respectively $D_{K_{\mathbb{R}},\alpha}$) by sampling D_α n (respectively $n/4$) times, the a_i, b_i are all sampled independently from $D_{K_{\mathbb{R}},\alpha}$. Thus $E_k^{(i)} \sim D_\alpha$ for $k = 1, 2$, as required. $\square$

Algorithm 1: Dimension-reducing transformation on GRLWE samples

Input: GRLWE sample $(a, b) = (a, as + e) \in R_q \times R_q$, a K -basis of L .

Output: Secret s .

1. $(a', b') := (\phi(a), \phi(b))$.
2. $(A, B) := (\varphi(a'), \varphi(b'))$.
3. Solve (A, B) for $S = \varphi(\phi(s))$.
4. $s = \phi^{-1} \circ \varphi^{-1}(S)$.

5.5.1 Examples

Here we use the Lattice Estimator [9] to estimate the runtime of solving an instance of GRLWE before and after applying the above dimension-reducing transformation. We ran the estimator on GRLWE samples with parameters equivalent to those of the Crystals-Kyber submission to the NIST post-quantum standardisation process, namely with the Kyber512 parameters: ring dimension $n = 512$, module rank $d = 2$, modulus $q = 3329$, and parameter $\sigma = 1.22$. The transformed sample yields plain LWE instances in half the dimension of those yielded by the original samples. The estimator ignores the extra algebraic structure of samples, interpreting the parameters as plain LWE instances. Below is a table summarising the results: β is the block size for the BKZ reduction, δ is the root Hermite factor, d_L is the lattice dimension, and m is the number of samples used.

GRLWE Sample					
$n = 512$	m	β	δ	d_L	Hardness estimate
Primal	-	406	1.003941	985	143.8
Dual	531	423	-	1043	149.6
Transformed Sample					
$n = 256$	m	β	δ	d_L	Hardness estimate
Primal	-	165	1.007055	511	76.4
Dual	293	170	-	549	78.9

Table 5.1: Estimating GRLWE

As can be seen from the table, ignoring the algebraic structure of the samples, the lattices obtained from the transformed samples are significantly less secure than those obtained from the original GRLWE samples. Moreover, since the transform doubles the number of available samples while halving the dimension of each sample, this greater number of samples may be of use to an attacker, compounding the results of the hardness estimation; for instance, a number of attacks on binary LWE need only polynomially many samples in the dimension, e.g. [158]. In order to achieve the initially expected security level in some fixed dimension for GRLWE as constructed in [47], one could double the initial dimension of the samples; however, this is likely to negatively affect the efficiency of schemes based on such parameters.

5.5.2 Extending the Attack to other Groups

The authors of [47] observe that D_{2n} is isomorphic to $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, and comment that their construction can be extended to hold for semidirect products $\mathbb{Z}/n\mathbb{Z} \rtimes H$, where H is a group acting on $\mathbb{Z}/n\mathbb{Z}$. We note that when n is a power of two, and H is a cyclic group acting on $\mathbb{Z}/n\mathbb{Z}$ by exponentiation, one obtains a group ring again isomorphic to a cyclic algebra: if $|H| = m$, $m \mid n/2$ so m is a power of two, and $G = \langle r, s : r^n = e, s^m = e, srs^{-1} = r^k \rangle$, where $\gcd(k, n) = 1$ and $k^m \equiv 1 \pmod{n}$. Then if $G = \mathbb{Z}/n\mathbb{Z} \rtimes H$, $R = \mathbb{Z}[G]/(r^{n/2} + 1)\mathbb{Z}[G]$ is isomorphic to the natural order of $\mathcal{A} = (L/K, \theta, \gamma)$ where $L = \mathbb{Q}(\zeta_n)$, θ is an automorphism of L sending $\zeta_n \mapsto \zeta_n^k$, K is the subfield fixed by θ , and $\gamma = 1$. Note $[L : K] = m$.

We can represent samples from such group rings in matrix-vector form as usual. Suppose our sample is of the form $(a, as + e) \in R_q \times R_q$ for an appropriate modulus q . Then we can rewrite this as $(\Phi(a), \Phi(a)\mathbf{s} + \mathbf{e}) \in M_m(\mathbb{Z}_q[r]/(r^{n/2} + 1)) \times (\mathbb{Z}_q[r]/(r^{n/2} + 1))^m$, where

$$\Phi(a) = \begin{pmatrix} a_0 & s^{-1}a_{m-1}s & \cdots & s^{-(m-1)}a_1s^{(m-1)} \\ a_1 & s^{-1}a_0s & \cdots & s^{-(m-1)}a_2s^{(m-1)} \\ a_2 & s^{-1}a_1s & \cdots & s^{-(m-1)}a_3s^{(m-1)} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m-1} & s^{-1}a_{m-2}s & \cdots & s^{-(m-1)}a_0s^{(m-1)} \end{pmatrix}.$$

This has the form of the matrix representation of a cyclic algebra, where θ corresponds to conjugation by s and $\gamma = 1$. Thus γ is a norm, and again we can apply the attack outlined above. We prove a version of Theorem 5.3 for any m :

Theorem 5.5. *Let $L = \mathbb{Q}(\zeta_n)$, $k > 0$: $(k, n) = 1$ and $k^m \equiv 1 \pmod{n}$, $\theta : \zeta_n \mapsto \zeta_n^k$ of order m , $K \subset L$ the subfield fixed by θ , and $n = 2^r$, $r \geq 2$. Let $q \in \mathbb{Z}$ be a prime unramified in L , and $\alpha_1, \dots, \alpha_m$ a basis of $\mathcal{O}_L/\mathcal{O}_K$ such that the matrix B with i, j th entry $\theta^{j-1}(\alpha_i)$ satisfies $(|\det(B)|, q) = 1$. Then $\varphi : \Lambda_q \rightarrow M_m(\mathcal{O}_{K_q})$ is bijective.*

Proof. Write the factorisations of q as $q\mathcal{O}_K = \prod_{i=1}^{g_K^q} \mathfrak{p}_i$ and $q\mathcal{O}_L = \prod_{i=1}^{g_L^q} \mathcal{P}_i$. We have $|\Lambda_q| = |\mathcal{O}_L/q\mathcal{O}_L|^m = |\mathcal{O}_L/\mathcal{P}_i|^{mg_L^q} = q^{mf_L^q g_L^q} = q^{m[L:\mathbb{Q}]}$. We also have $|M_m(\mathcal{O}_K/q\mathcal{O}_K)| = |M_m(\mathcal{O}_K/\prod_{i=1}^{g_K^q} \mathfrak{q}_i)| = |M_m(\mathcal{O}_K/\mathfrak{q}_i)|^{g_K^q} = (q^{m^2 f_K^q})^{g_K^q} = q^{m^2 f_K^q g_K^q} = q^{m^2 [K:\mathbb{Q}]}$. Since $[L:\mathbb{Q}] = m[K:\mathbb{Q}]$, the sets have equal cardinality, that is Λ_q and $M_m(\mathcal{O}_{K_q})$ have the same size.

If $\varphi : \Lambda_q \rightarrow M_m(\mathcal{O}_{K_q})$ were not injective, there would exist some $x \in \Lambda \setminus q\Lambda$ with coefficients x_i such that $x + q\Lambda \mapsto z \in M_m(q\mathcal{O}_K)$. So $x + q\Lambda \mapsto (qz_{ij})_{i,j}$ with $z_{ij} \in \mathcal{O}_K$. This is equivalent to saying $\pi_i \circ x \circ f_j(1) \in q\mathcal{O}_K$, and therefore $x \circ f_j(1) \in q\mathcal{O}_L$. As above, writing $f_j(1) = \alpha_j$, this is the same as $\sum_{k=0}^{m-1} x_k \theta^k(\alpha_j) \in q\mathcal{O}_L$. Applying this for $j = 1, \dots, m$, we obtain a system of equations each of the form $\sum_{k=0}^{m-1} x_k \theta^k(\alpha_j) = z_{j-1} \in q\mathcal{O}_L$, which we can write in matrix-vector notation as

$$\begin{pmatrix} \alpha_1 & \theta(\alpha_1) & \dots & \theta^{m-1}(\alpha_1) \\ \alpha_2 & \theta(\alpha_2) & \dots & \theta^{m-1}(\alpha_2) \\ \vdots & \vdots & \dots & \vdots \\ \alpha_m & \theta(\alpha_m) & \dots & \theta^{m-1}(\alpha_m) \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{m-1} \end{pmatrix} = \begin{pmatrix} z_0 \\ z_1 \\ \vdots \\ z_{m-1} \end{pmatrix} \in q\mathcal{O}_L^m.$$

If the matrix B with entries $\theta^k(\alpha_j)$ is invertible, the vector of x_i lies in $q\mathcal{O}_L^m$ - and this holds by assumption on $|\det(B)|$. But then we have $x \in q\Lambda$ after all. $\square$

5.6 On the Security of Quaternion Group Rings

We have shown that integral group rings of the form used for GRLWE, that is, dihedral group rings, are subject to a dimension-reducing transformation. In this section we show that if one

changes the group from D_{2m} to Q_{4n} , the generalized quaternion group, one obtains group rings immune to the above attack.

Recall the definition of the generalized quaternion group:

$$Q_{4n} = \langle r, s : r^n = s^2, r^{2n} = 1, s^{-1}rs = r^{-1} \rangle.$$

In [89] is stated the isomorphism problem for integral group rings of finite groups (denoted here by ISO) G and H :

$$\text{Does } \mathbb{Z}[G] \cong \mathbb{Z}[H] \text{ as rings imply } G \cong H? \quad (\text{ISO})$$

Generalized quaternion groups are special cases of dicyclic groups, specifically dicyclic groups of power-of-two order. Dicyclic groups are metacyclic, and therefore metabelian. It has been shown that (ISO) is true for metabelian groups [172]; therefore (ISO) is true for generalized quaternion groups. This means that since $Q_{4n} \not\cong D_{2m}$ for any pair n, m , their integral group rings satisfy $\mathbb{Z}[Q_{4n}] \not\cong \mathbb{Z}[D_{2m}]$ for any pair n, m . Thus, prima facie, the integral quaternionic group ring is a candidate group ring to use to avoid the cryptographic issue identified in this work arising from the use of dihedral group rings.

We proceed to consider $R = \mathbb{Z}[Q_{4n}]/(r^n + 1)\mathbb{Z}[Q_{4n}]$, analogously to the GRLWE construction. One can see that the quotient by $(r^n + 1)$ sets $r^n = -1$, and since $r^n = s^2$, we obtain $s^2 = r^n = -1$. This also means that, in R , $s^3 = -s$.

Consider multiplication of two elements of R : if $a, b \in \mathbb{Z}[Q_{4n}]$, we can write them in the form $a = a_0(r) + sa_1(r) + s^2a_2(r) + s^3a_3(r)$. If we quotient by $r^n + 1$, we also set $s^2 = -1$, and so get $a = a_0(r) - a_2(r) + s(a_1(r) - a_3(r)) \bmod (r^n + 1)$. Rewrite this as $a = a^0(r) + sa^1(r) \bmod (r^n + 1)$, so ab then becomes

$$\begin{aligned} ab &= (a^0(r) + sa^1(r)) (b^0(r) + sb^1(r)) \\ &= a^0(r)b^0(r) - \overline{a^1}(r)b^1(r) + s \left(a^1(r)b^0(r) + \overline{a^0}(r)b^1(r) \right) \bmod (r^n + 1). \end{aligned}$$

This is the same multiplication law as holds for cyclic algebras in $d = 2$ where $\gamma = -1$ and $\bar{\cdot}$ corresponds to the action of θ . One can see, like we showed above for dihedral groups, the following:

Proposition 5.2. *Let $R = \mathbb{Z}[Q_{4n}]/(r^n + 1)\mathbb{Z}[Q_{4n}]$. Let $\Lambda = \mathcal{O}_L \oplus u\mathcal{O}_L$ be the natural order in the degree 2 cyclic algebra $\mathcal{A} = (L/K, \theta, \gamma)$, where $L = \mathbb{Q}(\zeta_n)$, n is a power of 2, θ is the map on $L = \mathbb{Q}(\zeta_n)$ sending $\zeta_n \mapsto \zeta_n^{-1}$ extended linearly, $K = \mathbb{Q}(\zeta_n + \zeta_n^{-1}) = L^+$ is the subfield fixed by this map, and $\gamma = -1$. Define*

$$\phi : R \rightarrow \Lambda, \text{ mapping } r \mapsto \zeta_n \text{ and } s \mapsto u,$$

for ζ_n a primitive n th root of unity. Then ϕ is an isomorphism.

If the above cyclic algebra is division, that is, if -1 is not a norm, there will exist an isomorphism from R to the (maximal) natural order of a cyclic division algebra in the same fashion as before; but the lemma we used to send GRLWE samples to samples over matrix rings will not apply. Recall an algebraic number field of degree n has n embeddings into $\mathbb{C}$. If these map the field into $\mathbb{R}$, they are real embeddings, else complex. If there are r_1 real embeddings and r_2 pairs of complex embeddings, we have $r_1 + 2r_2 = n$. A field with only complex embeddings is called *totally complex*, and a field with only real embeddings is *totally real*. Finally, a field element can be mapped to an r_1 -tuple $\{\pm 1\}^{r_1}$ under the real embeddings of the field, with each entry depending on whether the image of an embedding is positive or negative; if it maps to $\{1\}^{r_1}$, we call it *totally positive*. For more on these definitions, see e.g. [111]. We now show:

Proposition 5.3. *Let $\mathcal{A} = (\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+, \bar{\cdot}, -1)$ be a cyclic algebra. Then $\mathcal{A}$ is a cyclic division algebra.*

Proof. It suffices to prove that -1 is not the norm of any element from $\mathbb{Q}(\zeta_n)$ to $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$. First, note that $\mathbb{Q}(\zeta_n)$ is totally complex and $\mathbb{Q}(\zeta_n)^+$ is totally real. Thus every element of $\mathbb{Q}(\zeta_n)$ is totally positive, which means that the image of the field norm map in $\mathbb{Q}(\zeta_n)^+$ is also totally positive; but -1 is clearly not totally positive in $\mathbb{Q}(\zeta_n)^+$, and is thus not in the image of the norm. $\square$

Thus, if one constructs GRLWE over Q_{4n} as above, the dimension-reducing transformation, and hence attack, do not apply. In terms of the numerical results of section 5.1, this means that a plausible security estimate of GRLWE with fixed dimension n (such as for Kyber512) is given by the output of the Lattice Estimator on lattices of dimension n , rather than $n/2$. We leave the adaptation of the direct-to-decision security proof of GRLWE for generalized quaternion groups as a topic for future research.

5.7 On Structured MLWE Variants

In this section we briefly discuss the relation between the security of the three structured MLWE variants given in the introduction, namely, m-RLWE, GRLWE, and CLWE.

The oldest of the three is m-RLWE, or multivariate LWE, which was given in [123]. It defines LWE over the tensor product of rings (which are maximal orders in algebraic number fields).

The m-RLWE distribution is defined as follows:

Definition 86. For $s \in R_q^\vee$ and an error distribution χ over $K_{(T),\mathbb{R}}$, a sample from the m-RLWE distribution $A_{s,\psi}$ over $R_q \times \mathbb{T}$ is generated by $a \leftarrow R_q$ uniformly at random, $e \leftarrow \psi$, and outputting $(a, b = (a \cdot s)/q + e \bmod R^\vee)$.

Here $K_{(T)} = \bigotimes_{i \in I} K_i$ for K_i cyclotomic, $R = \bigotimes_{i \in I} \mathcal{O}_{K_i}$, I is some indexing set, and $R^\vee$ denotes the dual ideal of R . Finally, set $\mathbb{T} = K_{(T),\mathbb{R}}/R^\vee$. The search and decision problems are defined as usual.

One can understand m-RLWE as follows. For simplicity, suppose the m-RLWE instance consists of the tensor product of two number fields, K_1 and K_2 . Write the tensor product of fields as $K = K_1 \otimes K_2$ where K_1 and K_2 are defined by polynomials $f(x)$ and $g(y)$ respectively. This yields a m-RLWE problem over $R_q = \frac{\mathbb{Z}_q[x,y]}{(f(x),g(y))}$, and corresponds to a structured MLWE instance over $\mathbb{Z}_q[x]/(f(x))$ with dimension $\deg(g)$.

The primary case of interest is that of cyclotomics of power of two degree over $\mathbb{Q}$, defined by the polynomials $x^{k_1} + 1$ and $y^{k_2} + 1$ respectively. This gives an m-RLWE problem over $R_q = \frac{\mathbb{Z}_q[x,y]}{(x^{k_1}+1, y^{k_2}+1)}$, and corresponds to a structured MLWE instance over $\mathbb{Z}_q[x]/(x^{k_1} + 1)$ with

dimension k_2 .

In [32], m-RLWE was subjected to an attack, which runs along the following lines. The authors showed that when k_1 and k_2 are not coprime, there is a field K' containing K_1 such that there is a homomorphism from K into K' , and that the image of y under the homomorphism is well-defined. When this happens, $g(y)$, say, has at least one root in $\mathbb{Z}[x](f(x))$. One can then define a map taking polynomials $h(x, y)$ to the l -tuple of evaluations of $h(x, \cdot)$ at the l such roots of $g(y)$. In this way, the problem can be reduced from one problem in dimension $\deg(f) \cdot \deg(g)$ to multiple lower dimensional problems.

For example, let $f(x) = x^8 + 1$ and $g(y) = y^4 + 1$. Consider the map taking y to x^2 and fixing $K_1 = \mathbb{Z}_q[x]/f(x)$. This is a well defined homomorphism from K to K_1 . Using this map, the authors transform the problem of solving one m-RLWE instance to solving four RLWE instances in dimension 8, rather than one instance in dimension $k_1 \cdot k_2 = 32$. In general, the attack transforms one instance in dimension $k_1 \cdot k_2$ to k_2 RLWE instances of dimension k_1 .

We echo the statement made in [71], that CLWE, as a structured MLWE variant, is immune from this style of attack. Let $\mathcal{A} = (L/K, \theta, \gamma)$ be a cyclic division algebra. Suppose that there is an injective homomorphism $\chi : \mathcal{A} \rightarrow L$. L is Galois over K , so the restriction of χ to L is an injective homomorphism of fields, and is thus an isomorphism from L to L , that is, an automorphism. Observe: $\chi(u) \cdot \chi(\ell) = \chi(u \cdot \ell) = \chi(\theta(\ell) \cdot u) = \chi(u) \cdot \chi(\theta(\ell))$ for any $\ell \in L$. This implies that $\chi(\ell) = \chi(\theta(\ell))$ - but this contradicts χ being injective on L . This contradiction implies that there is no injective homomorphism as above, so one cannot launch the attack of [32] to reduce a CLWE instance to an instance defined over a subfield of $\mathcal{A}$.

Furthermore, addressing the attack on GRLWE, if γ is chosen to make $\mathcal{A}$ division, then the isomorphism given in [139, Theorem 30.4] does not apply to $\mathcal{A}$. So the transformation delineated in this chapter does not apply to a CLWE instance as defined in [71] either.

We conclude from this that the presence of 1. ‘twisting’ field automorphisms, such as θ , and 2. well-chosen γ , secure CLWE from direct adaptations of the family of attacks which map a sample into a subspace, solve in the subspace, and then lift the solution. The automorphisms prevent the existence of a convenient subfield to injectively map into, and ‘nice’ values of γ similarly prevent the LWE instance being reduced to a lower-dimensional matrix instance. In

the case of the first attack, m-RLWE lacks the noncommutativity given by application of θ . In the case of the second attack, GRLWE using the group D_{2n} lacks a value of γ that aids security, and it is not clear how such a value of γ could be introduced (excepting instances where $\gamma = -1$ is not a norm). To conduct such attacks on CLWE, it appears a novel approach is needed.

5.8 Chapter Summary

Thus there is a dimension-reducing transformation which takes GRLWE samples and outputs multiple MLWE samples in half the dimension of the original samples. This map can be seen as the composition of two maps, both of which we proved above to be bijective. This transformation can be converted into an attack on GRLWE by combining the transformation with any method to solve LWE instances. The attack holds for all such group rings as defined in [47], where $G = \mathbb{Z}/n\mathbb{Z} \rtimes H$ as in Section 5.5.2, and leads to a significant loss in security, as can be seen from the results of Section 5.5.1. To counter the attack, one would have to double the initial dimension of the samples to obtain the original desired level of security for the GRLWE problem.

We also gave an example of a group, the generalized quaternion group, for which GRLWE-style group rings are immune from our attack. This is because the corresponding cyclic algebra is a division algebra.

It remains to be seen if other group rings can be constructed for the LWE problem that are proven not to be subject to such an attack. The only groups which have been considered so far are dihedral or quaternionic; perhaps there are other noncommutative groups (not dihedral or quaternionic) that are immune from this strategy. There is certainly no shortage of groups to try. Alternatively, perhaps relaxing assumptions on the group, considering algebraic structures such as monoid rings, could lead to interesting results. Also outstanding is adapting the security proof to hold for quaternion group rings, and thus to instantiate LWE securely over such group rings.

Chapter 6

NTRU in Cyclic Division Algebras

6.1 Introduction

In this chapter we study the NTRU problem in the context of quaternion algebras over number fields. In particular, we define NTRU in CDAs when the ring of scalars (the center) of the algebra is a cyclotomic field with power of two conductor. We call this NTRU variant ‘CNTRU’. The dimension of these algebras over their center is a square, d^2 , and the positive square-root of this dimension, d , is called the index of the algebra. When the index is 1, the CDA is equal to its center, and so in our case is a cyclotomic field; when the index is 2, the CDA is called a quaternion algebra. These quaternion algebras enjoy particularly nice properties (see e.g. [168]) and the proof of our main result on the uniformity of our NTRU public keys appears to fail when $d > 2$.

As mentioned in Chapter 2, the reliability and speed of NTRU has prompted work exploring alternatively structured variants of NTRU [49], [50]. Whereas NTRU uses multiplication of elements in polynomial rings, these constructions use operations in modules over polynomial rings, and aim to instantiate efficient and compact NTRU schemes while enabling greater flexibility with parameter choices. However, neither of [49], [50] give a full proof of security: in [50], it is shown that module NTRU public keys are (asymptotically) close to uniform, if the modulus factors into only two prime ideals in the ring - yet the scheme uses primes which

completely split in the ring; and the authors of [49] give no such proof.

The aim of this chapter is to build a structured form of NTRU with a provable security guarantee that corresponds to the kind of moduli q used in practice; that is, our results hold for completely split q . However, we note that the size of the parameters for which our proof are not practical. Our method follows that of [154] and [169]. In particular, we begin by proving

Theorem 6.1. *Let $\epsilon > 0$, q be completely split in $\mathcal{O}_L$, $p \in \mathcal{Z}(\Lambda_q^\times)$, and $\sigma \geq 4n^{3/2}\sqrt[4]{\ell}\sqrt{2\ln(32nq)}q^{\frac{1}{2}+2\epsilon}$. Let $y_i \in \Lambda_q$ and $z_i = -y_i p^{-1} \bmod q$ for $i = 1, 2$, and $D_{\sigma, z_i}^\times$ denote $D_{\Lambda, \sigma}$ restricted by rejection to $\Lambda_q^\times + z_i$. Then when $d = 2$,*

$$\Delta \left(\frac{y_1 + pD_{\sigma, z_1}^\times}{y_2 + pD_{\sigma, z_2}^\times} \bmod q, U(\Lambda_q^\times) \right) \leq 2^{22n} q^{-8n\epsilon}.$$

To achieve this, we prove a number of new results on q -ary lattices obtained from orders in CDAs (of a particular form). These results can be stated for any $d \geq 1$, but we restrict them to the case of interest, $d = 2$.

The specific algebras the above result holds for are constructed as we have often constructed them in this thesis: let m be a prime power, $K = \mathbb{Q}(\zeta_m)$ is a cyclotomic field of conductor m , and $M = \mathbb{Q}(\zeta_{\ell m})$, for some prime ℓ such that $\ell \equiv 1 \bmod m$ and $\ell \not\equiv 1 \bmod pm$ for any prime divisor p of m . Then M/K is cyclic Galois, with Galois group generated by (say) σ . Let L be the intermediate field fixed by σ^2 ; this can be written explicitly as $L = \mathbb{Q}(\zeta_m, \sqrt{\ell})$ when m is a power of two. Set u to be an element such that $u^2 = \zeta_m$ and $ux = \theta(x)u$ for all $x \in L$, where $\text{Gal}(L/K) = \langle \theta \rangle$. Then $\mathcal{A} = (L/K, \theta^2, \zeta_m) = L + uL$ is a quaternion algebra.

We then proceed to study algorithms to encrypt and decrypt messages based on the NTRU problem in these quaternion algebras. We prove that if there is an efficient indistinguishability-under-chosen-plaintext attack (IND-CPA) algorithm for CNTRU, there is an algorithm with non-negligible advantage for decision CLWE. The uniformity of CNTRU public keys (over invertible elements) forms a crucial part of the proof of this result. This connection is in part a motivation for the particular CDAs we define NTRU over: the existence of a security proof for CLWE in these particular algebras linking SIVP on lattices obtained from ideals of Λ to CLWE allows us to link SIVP and NTRU, too (it should here be recalled that the reduction

from SIVP to CLWE holds for a (slightly) restricted space of secrets). We obtain

Lemma 6.1. *Let $n \geq 8$ be a power of 2, $d = 2$, $\ell \leq Cn$, and $q \geq 8n$ a prime such that $x^n + 1$ splits completely modulo q . Let $\delta > 0$, $p \in \mathcal{Z}(\Lambda_q^\times)$ and $\sigma \geq 2n^{3/2} \sqrt[4]{\ell} \sqrt{\ln(32nq)} q^{\frac{1}{2}+2\epsilon}$ satisfy the conditions of Lemma 6.12 and Theorem 6.5. If there exists an IND-CPA attack algorithm $\mathcal{A}$ against CNTRU, running in time T with advantage δ , then there exists an algorithm to solve decision-CLWE $_{\text{HNF}}^\times$ that runs in time $T' = T + O(\text{poly}(n))$ with success probability $\delta' = \delta - q^{-\Omega(n)}$.*

Note the condition $\ell \leq Cn$ for a constant C : we impose a bound on ℓ in order to allow for a precise statement on the correctness of the decryption algorithm (see Lemma 6.12). This is necessary because of the form of L . Consider the square of field element $1 + \sqrt{\ell}$; this is an element of small ℓ_2 -norm when using $1, \sqrt{\ell}$ as a basis of L/K , but its square, $1 + \ell + 2\sqrt{\ell}$, may potentially be large indeed, if ℓ is large. This constraint amounts to a bound on the discriminant of the quaternion algebra, which has discriminant which we bound by $(n\sqrt{\ell})^{4n}$ (Lemma 6.2); when $\ell \leq Cn$, this becomes a function solely in $n = [K : \mathbb{Q}]$.

In practice, we have not found this imposition difficult to satisfy for small values of C . The interested reader is directed to [71, §3.4] and Section 6.8 of this chapter for further discussion on parameter selection.

We also sketch a KEM and a signature scheme based on NTRU in CDAs, to give examples of greater functionality from CNTRU.

Note that when $d = 1$, $K = L$ and $\mathcal{A} = K$. This is the fact that will enable us to generalise NTRU schemes which sample elements from $\mathbb{Z}[x]/(\Phi_{2^r}(x))$, using algebras of the form $\mathcal{A} = (L/\mathbb{Q}(\zeta_{2^r}), \theta, \zeta_n)$; when $d = 1$, we will recover the familiar families of polynomials in certain spaces, generalising NTRU, ETRU and others. If one uses CDAs over fields K where K is some other popular choice of field for NTRU, one obtains generalisations of those schemes too.

Previous Work

Despite the flood of NTRU variants catalogued in Chapter 2, we note that few of them generalise NTRU, in the sense that they do not offer a broader framework from which the traditional form

of NTRU can emerge; rather, they simply replace the underlying ring, or make other subtle amendments. Two papers [49], [50], mentioned above, do develop general (module) versions of NTRU; these are compared to the construction featured in this chapter below. Finally, we note recent works [34], [128], [63] which provide reductions between various (module) NTRU problems, and also module LWE.

6.2 Preliminaries

Bases of Real Quadratic Extensions of Cyclotomics

We consider an extension L/K , where $K = \mathbb{Q}(\zeta_{2^r})$ and $L = K(\sqrt{\ell}) = \mathbb{Q}(\zeta_{2^r}, \sqrt{\ell})$ and $\gcd(2, \ell) = 1$. With $n = [K : \mathbb{Q}]$ and $m = 2^r$, we define the *powerful basis* of $L/\mathbb{Q}$ as

$$\vec{p} = (1, \zeta_m, \dots, \zeta_m^{n-1}, \sqrt{\ell}, \zeta_m \sqrt{\ell}, \dots, \zeta_m^{n-1} \sqrt{\ell}).$$

We obtain a matrix from this by applying the canonical embedding to each entry:

$$\sigma_L(\vec{p}) = (\sigma_L(1), \sigma_L(\zeta_m), \dots, \sigma_L(\zeta_m^{n-1}), \sigma_L(\sqrt{\ell}), \sigma_L(\zeta_m \sqrt{\ell}), \dots, \sigma_L(\zeta_m^{n-1} \sqrt{\ell})).$$

This is a $2n \times 2n$ matrix. To find the singular values of this matrix, we compute $\sigma_L(\vec{p})^* \sigma_L(\vec{p})$. This is diagonal with two blocks: the top left $n \times n$ diagonal entries are all equal to m , and the bottom right $n \times n$ to $m\ell$. The eigenvalues of a diagonal matrix are its non-zero entries, so the singular values of $\sigma_L(\vec{p})$ are $\sqrt{[L : \mathbb{Q}]}, \sqrt{[L : \mathbb{Q}]\ell}$. Denoting the largest singular value by $s_1(\vec{p})$ and the smallest by $s_{2n}(\vec{p})$, we have $s_1(\vec{p}) = \sqrt{[L : \mathbb{Q}]\ell}$, $s_{2n}(\vec{p}) = \sqrt{[L : \mathbb{Q}]}$. Since

$$\sigma_L(x) = \sigma_L(\vec{p}) \cdot \text{coeff}(x),$$

for $x \in L$, we find $\|\sigma_L(x)\| \leq s_1(\vec{p})\|x\|_{\vec{p}}$, where $\|\cdot\|_{\vec{p}}$ is the norm obtained by writing x in the $\vec{p}$ basis and taking the coefficient embedding. Conversely,

$$\|x\|_{\vec{p}} \leq \frac{1}{s_{2n}(\vec{p})}\|\sigma_L(x)\| = \frac{1}{\sqrt{[L:\mathbb{Q}]}}\|\sigma_L(x)\|.$$

The $s_i(\vec{p})$ can in practice be taken to be polynomial in n , if desired. We will be interested in the above for integral elements $x \in \mathcal{O}_L$, which has powerful basis

$$(1, \zeta_m, \dots, \zeta_m^{n-1}, \frac{1+\sqrt{\ell}}{2}, \zeta_m \frac{1+\sqrt{\ell}}{2}, \dots, \zeta_m^{n-1} \frac{1+\sqrt{\ell}}{2}),$$

when $\ell \equiv 1 \pmod{4}$. Upon computing the singular values of $\sigma(\vec{p})$, we find that

Proposition 6.1. *Let $n = 2^{r-1}$, $\ell \equiv 1 \pmod{2^r}$ a prime, and $L = \mathbb{Q}(\zeta_{2^r}, \sqrt{\ell})$. Then, using the powerful basis of $\mathcal{O}_L$, we have*

$$s_1(\vec{p}) = \frac{\sqrt{n}}{2} \sqrt{\ell + 5 + \sqrt{\ell^2 - 6\ell + 25}} \text{ and } s_{2n}(\vec{p}) = \frac{\sqrt{n}}{2} \sqrt{\ell + 5 - \sqrt{\ell^2 - 6\ell + 25}}.$$

Proof. The symmetric matrix $\sigma(\vec{p})^* \sigma(\vec{p})$ has a block form: the top left block is $[L:\mathbb{Q}] \cdot I_{2^{r-1}}$, where $I_{2^{r-1}}$ is the $2^{r-1} \times 2^{r-1}$ identity matrix, the lower right block is $2^{r-2} \cdot (\ell + 1)$, and the top right and lower left blocks are $2^{r-1} \cdot I_{2^{r-1}}$. The eigenvalues of this matrix are $\lambda_i = 2^{r-2} \cdot \frac{\ell + 5 \pm \sqrt{\ell^2 - 6\ell + 25}}{2}$. So the singular values are

$$s_i(\vec{p}) = \sqrt{2^{r-2} \cdot \frac{\ell + 5 \pm \sqrt{\ell^2 - 6\ell + 25}}{2}} = \frac{\sqrt{n}}{2} \sqrt{\ell + 5 \pm \sqrt{\ell^2 - 6\ell + 25}}$$

□

If $\vec{d}$ is the dual of $\vec{p}$, we obtain $s_1(\vec{d}) = \frac{1}{s_{2n}(\vec{p})}$, $s_{2n}(\vec{d}) = \frac{1}{s_1(\vec{p})}$. We will use bounds in terms of this ‘decoding basis’; in particular, for $x \in \mathcal{O}_L^\vee$,

$$\|x\|_{\vec{d}} \leq \frac{1}{s_{2n}(\vec{d})}\|\sigma_L(x)\| = \frac{\sqrt{n}}{2} \sqrt{\ell + 5 + \sqrt{\ell^2 - 6\ell + 25}} \|\sigma_L(x)\|.$$

When ℓ is bounded by some integer multiple of n , say $\ell \leq Cn$ for $C \geq 2$, we can use the bound

$s_1(\vec{p}) < 2Cn$, when $n \geq 4$.

Discretisation

We will need the following distribution:

Definition 87. [110] Denote by *Bern* the Bernoulli distribution and let $a \in \mathbb{R}$. The univariate Reduction distribution $\text{Red}(a) = \text{Bern}(\lceil a \rceil - a) - (\lceil a \rceil - a)$ is defined

$$\text{Red}(a) := \begin{cases} 1 + a - \lceil a \rceil, & \text{with probability } \lceil a \rceil - a, \\ a - \lceil a \rceil, & \text{with probability } 1 - (\lceil a \rceil - a). \end{cases}$$

A random variable $\mathbf{R} = (R_1, \dots, R_n)^T \in \mathbb{R}^n$ has a multivariate Reduction distribution $R \sim \text{Red}(\mathbf{a})$ on $\mathbb{R}^n$ for parameter $\mathbf{a} = (a_1, \dots, a_n)^T$ if $R_j \sim \text{Red}(a_j)$ for $j = 1, \dots, n$ are independent univariate Reduction random variables.

Definition 88. Let $\mathcal{L} = \mathcal{L}(B)$ be an n -dimensional lattice under the canonical embedding. For $c \in H$, the coordinatewise randomized rounding (CRR) discretisation $\lfloor X \rfloor_{\mathcal{L}+c}^B$ of random variable X to $\mathcal{L} + c$ is defined by

$$\lfloor X \rfloor_{\mathcal{L}+c}^B = X + B \text{Red}(B^{-1}(c - X)).$$

Extend this to H^d by applying the discretisation in each coordinate. The discretisation variable on H is 0-subgaussian:

Definition 89. For any $\delta \geq 0$, a multivariate random variable $\mathbf{X}$ on $\mathbb{R}^n$ (resp. H) is δ -subgaussian with standard parameter $b \geq 0$ if

$$E(e^{\langle \mathbf{t}, \mathbf{X} \rangle}) \leq e^\delta e^{\frac{1}{2}b^2 \|\mathbf{t}\|^2}, \quad \text{for all } \mathbf{t} \in \mathbb{R}^n \text{ (resp. } \mathbf{t} \in H).$$

Extend this to H^d by saying a multivariate random variable $\mathbf{Z}$ on H^d is δ -subgaussian with standard parameter $b \geq 0$ if $\mathbf{Z}$ is δ -subgaussian with standard parameter $b \geq 0$ in each H -coordinate ($H^d \cong \mathbb{R}^{nd^2}$ as $\mathbb{R}$ -vector spaces). Formally,

Definition 90. A multivariate random variable $\mathbf{Z}$ on H^d is δ -subgaussian with standard parameter $b \geq 0$ if

$$E(e^{\langle \mathbf{t}, \mathbf{Z} \rangle}) \leq e^\delta e^{\frac{1}{2}b^2 \|\mathbf{t}\|^2}, \quad \text{for all } \mathbf{t} \in H^d$$

Definition 91. A random variable $\mathbf{Z}$ on $\mathbb{R}^n$ (or H) is noncentral subgaussian with noncentrality $\|E(\mathbf{Z})\| \geq 0$ and deviation $d \geq 0$ if the centered random variable $\mathbf{Z}_0 = \mathbf{Z} - E(\mathbf{Z})$ is 0-subgaussian with standard parameter d .

We will need the following lemmas:

Lemma 6.2. [109] Suppose that B is a column basis matrix for a lattice in H with largest singular value $s_1(B)$ and $\mathbf{Z}$ is an independent noncentral subgaussian random variable with deviation d_Z . The CRR discretisation of $\mathbf{Z}$ to $\lfloor \mathbf{Z} \rfloor_{\Lambda+c}^B$ is noncentral subgaussian with noncentrality $\|E(\mathbf{Z})\|$ and deviation $\left(d_Z^2 + \left(\frac{1}{2}\right)^2 s_1(B)^2\right)^{\frac{1}{2}}$.

When $L = \mathbb{Q}(\zeta_n, \sqrt{\ell})$ for n a power of two, $\gcd(n, \ell) = 1$, this becomes

Lemma 6.3. Suppose that B is a column basis matrix for a lattice in H^d with largest singular value $s_1(B)$ and $\mathbf{Z}$ is an independent noncentral subgaussian random variable with deviation d_Z . The CRR discretisation of $\mathbf{Z}$ to $\lfloor \mathbf{Z} \rfloor_{\Lambda+c}^B$ is noncentral subgaussian with noncentrality $\|E(\mathbf{Z})\|$ and deviation $\left(d_Z^2 + \frac{1}{2}s_1(B)^2\right)^{\frac{1}{2}}$.

Proof. As in [109, Theorem 2], but with an extra factor of $\sqrt{2}$ from taking the matrix norm of the basis. □

Structured Forms of NTRU

Two papers have proposed structured forms of NTRU using modules [49], [50]. The authors construct NTRU modules of the following form, where $\mathcal{R} = \mathcal{O}_K$ for a number field K :

$$\mathcal{L}_{\mathbf{h},q} = \{(\mathbf{f}, g)^T \in \mathcal{R}^{d+1} : \langle \mathbf{f}, \mathbf{h} \rangle - g \equiv 0 \pmod{q}\}.$$

Here g is a ring element and $\mathbf{f}$ is an d -dimensional vector over $\mathcal{R}$, and embedding the lattice (via either coefficients or ring embeddings) yields lattices in $\mathbb{R}^{(d+1)n}$, where $\dim_{\mathbb{Z}}(\mathcal{R}) = n$. Multiple samples can be taken and written in the following form, where we have chosen d samples to obtain square matrices for convenience of expression (note squareness of the matrices involved is not required):

$$\mathcal{L}_{\mathbf{h},q} = \{(\mathbf{F}, \mathbf{g})^T \in \mathcal{R}^{d \times (d+1)} : \mathbf{F}\mathbf{h} - \mathbf{g} \equiv \mathbf{0} \bmod q\}.$$

These are more general objects than those considered in this work. However, the authors of [50] are able to prove uniformity of their NTRU public keys only for certain prime moduli, those splitting into two prime ideals in $\mathcal{R}$ (those congruent to 3 modulo 8), which are not the primes used in practice. Their recommended parameters are completely splitting primes and a module rank of 2. They prove:

Theorem 6.2 (Theorem A.1, [50]). *Let K be a cyclotomic number field of degree d and maximal order R . Let $n \geq m \geq 1$. Let q be a prime integer which factors as $qR = \mathfrak{p}_1\mathfrak{p}_2$, where the $\mathfrak{p}_i$'s have algebraic norm $q^{d/2}$. For $s \geq 2dq^{m/(n+m)+2/(d(n+m))}$, we have:*

$$\Delta(\mathcal{E}_s, U(R_q^{n \times m})) \leq 2^{-\Omega(d)},$$

where $\mathcal{E}_s$ is the distribution of $\mathbf{F}^{-1}\mathbf{G} \bmod q$, for $\mathbf{F}, \mathbf{G}$ with entries chosen according to discrete Gaussians.

In contrast, restricting ourselves to more structured modules, we obtain a full proof of uniformity of our public keys, for completely split primes in rank 2. Our modules are obtained from *cyclic division algebras*.

6.3 On the Discriminant of the Natural Order

We now recall the construction of CDAs using cyclotomic fields as in [71]. Let m be a prime power, $K = \mathbb{Q}(\zeta_m)$ and $M = \mathbb{Q}(\zeta_{\ell m})$, for a prime ℓ such that $\ell \equiv 1 \bmod m$ and $\ell \not\equiv 1 \bmod pm$ for any prime divisor p of m . Then M/K is cyclic Galois, with Galois group generated by (say)

θ . Let L be the intermediate field fixed by θ^d . It can be verified that ζ_m is not the norm of any element of L , so $(L/K, \theta, \zeta_m)$ is a division algebra. Moreover, Λ is maximal with respect to inclusion in $\mathcal{A}$. Security reductions for LWE in these algebras were given; here we investigate the properties of NTRU implemented in such an algebra.

In the case $d = 2$, L is the compositum of K and the unique quadratic subfield of $\mathbb{Q}(\zeta_\ell)$, which is $\mathbb{Q}(\sqrt{\ell})$. Thus $L = \mathbb{Q}(\zeta_m, \sqrt{\ell})$ and $\Lambda = \mathcal{O}_L + u\mathcal{O}_L$. We now prove an upper bound on the discriminant of Λ :

Definition 92. $\text{disc}(\Lambda/\mathbb{Z}) := \left\{ \det(\text{Tr}(x_i x_j))_{i,j=1}^{nd^2} \mid (x_1, \dots, x_{nd^2}) \in \Lambda^{nd^2} \right\}$.

It was proved in [166, Lemma 2.9] that $\text{disc}(\Lambda/\mathcal{O}_K) = \text{disc}(L/K)^d \gamma^{d(d-1)}$. Since in our case γ is a root of unity, this simplifies to $\text{disc}(\Lambda/\mathcal{O}_K) = \text{disc}(L/K)^d$.

Proposition 6.2. *Let $L = \mathbb{Q}(\zeta_{2^r}, \sqrt{\ell})$, $r \geq 2$, $\ell \equiv 1 \pmod{2^r}$, and $K = \mathbb{Q}(\zeta_{2^r})$. Then*

$$\text{disc}(\Lambda/\mathbb{Z}) \leq (n\sqrt{\ell})^{4n}.$$

Proof. Since $u^i \mathcal{O}_L$ and $u^j \mathcal{O}_L$ are orthogonal with respect to the trace form, except when $i + j \equiv 0 \pmod{2}$, we have

$$\begin{aligned} \det(\text{Tr}(ux_k ux_\ell))_{k,\ell=1}^{2n} &= \det(u^2 \text{Tr}(x_k x_\ell))_{k,\ell=1}^{2n} = \gamma^{nd} \det(\text{Tr}(x_k x_\ell))_{k,\ell=1}^{2n} \\ &= \det(\text{Tr}(x_k x_\ell))_{k,\ell=1}^{2n} = \text{disc}(L/\mathbb{Q}), \end{aligned}$$

for some $x_i \in \mathcal{O}_L$, since $\gamma = \zeta_n$.

It now suffices to prove that $\text{disc}(L/\mathbb{Q}) \leq (n\sqrt{\ell})^{2n}$. Since L is the compositum of $K = \mathbb{Q}(\zeta_{2^r})$ and $\mathbb{Q}(\sqrt{\ell})$, we can apply a general formula on the discriminants of composita (e.g. [105, ex. 23(c)]) to obtain

$$\text{disc}(L/\mathbb{Q}) = \text{disc}(K/\mathbb{Q})^2 \text{disc}(\mathbb{Q}(\sqrt{\ell})/\mathbb{Q})^n.$$

We combine the bound $\text{disc}(K/\mathbb{Q}) \leq n^n$ with $\text{disc}(\mathbb{Q}(\sqrt{\ell})/\mathbb{Q}) = \ell$ for the result. $\square$

Proposition 6.3. [21, Proposition 2.5] *Let Λ be as above and $\mathcal{I} \subset \Lambda$ be an integral ideal. Then*

$$\text{Vol}(\mathcal{I}) = N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) \sqrt{\text{disc}(\Lambda/\mathbb{Z})}.$$

We will use the following bound on the shortest vector of a Λ -ideal lattice under the canonical embedding, with respect to a p -norm, $\lambda_1^p(\mathcal{L})$:

Proposition 6.4. (cf. [127, Lemma 6.1]) *Let $\mathcal{I}$ be an ideal of Λ . Then*

$$\lambda_1^p(\mathcal{I}) \leq (nd^2)^{1/p} N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/nd^2} \text{disc}(\Lambda/\mathbb{Z})^{1/2nd^2}.$$

Proof. Since $\|x\|_p \leq (nd^2)^{\frac{1}{p}} \|x\|_\infty$, we bound $\|x\|_\infty$. Recall $\mathcal{A} \hookrightarrow H^d \subset (\mathbb{R}^{r_1} \times \mathbb{C}^{2r_2})^d$, with $r_1 + 2r_2 = nd$. Set $C = \{x \in H^d : \|x\|_\infty \leq 1\}$ and note $\text{Vol}(C) = 2^{nd^2} \left(\frac{\pi}{2}\right)^{r_2 d}$. Then if $\beta^{nd^2} > \left(\frac{2}{\pi}\right)^{r_2 d} N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) \sqrt{\text{disc}(\Lambda/\mathbb{Z})}$, we have

$$\begin{aligned} \text{Vol}(\beta C) &= \beta^{nd^2} \text{Vol}(C) > \left(\frac{2}{\pi}\right)^{r_2 d} N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) \sqrt{\text{disc}(\Lambda/\mathbb{Z})} 2^{nd^2} \left(\frac{\pi}{2}\right)^{r_2 d} \\ &= N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) \sqrt{\text{disc}(\Lambda/\mathbb{Z})} 2^{nd^2} = \text{Vol}(\mathcal{I}) 2^{nd^2}. \end{aligned}$$

By Minkowski's theorem, βC contains a lattice point from $\mathcal{I}$, so $\lambda_1^\infty(\mathcal{I}) \leq \beta$. □

This implies that in the ℓ_2 -norm, $\lambda_1(\Lambda) \leq (nd^2)^{1/2} (n\sqrt{\ell})^{1/2} = dn\sqrt[4]{\ell}$.

Proposition 6.5. *Let $\Lambda \subset \mathcal{A} = (L/K, \theta, \gamma)$ where $|\gamma| = 1$, $[L : K] = d$ and $[K : \mathbb{Q}] = n$. Then, for $x = \bigoplus_{i=0}^{d-1} u^i x_i \in \Lambda$, $\mathcal{I}$ an ideal of Λ ,*

$$\|x\|_p \geq [\mathcal{A} : \mathbb{Q}]^{1/p} \cdot \left(\prod_{0 \leq i < d} |N_{L/\mathbb{Q}}(x_i)| \right)^{1/[\mathcal{A}:\mathbb{Q}]}.$$

When $\mathcal{I} = \mathfrak{J}\Lambda$ for some $\mathcal{O}_K$ -ideal $\mathfrak{J}$ and $\bar{\mathcal{I}} := \mathcal{I} \cap \mathcal{O}_L$, then

$$\lambda_1^p(\mathcal{I}) \geq [\mathcal{A} : \mathbb{Q}]^{1/p} \cdot |N_{L/\mathbb{Q}}(\bar{\mathcal{I}})|^{d/[\mathcal{A}:\mathbb{Q}]}, \text{ and } \lambda_1^\infty(\mathcal{I}) \geq (N_{L/\mathbb{Q}}(\bar{\mathcal{I}}))^{1/nd}.$$

Proof. We have

$$\begin{aligned}
\|x\|_p^p &= \sum_{\alpha \in \text{Emb}(K)} \sum_{1 \leq i, j < d} |\alpha((\phi(x))_{i,j})|^p \geq d^2 \sum_{\alpha \in \text{Emb}(K)} \left(\prod_{i,j} |\alpha((\phi(x))_{i,j})|^p \right)^{1/d^2} \\
&\geq d^2 [K : \mathbb{Q}] \left(\prod_{\alpha \in \text{Emb}(K)} \left(\prod_{0 \leq i < d} |\alpha(N_{L/K}(x_i))|^p \right)^{1/d^2} \right)^{1/[K:\mathbb{Q}]} \\
&= [\mathcal{A} : \mathbb{Q}] \left(\prod_{0 \leq i < d} |N_{L/\mathbb{Q}}(x_i)| \right)^{p/[\mathcal{A}:\mathbb{Q}]}, \text{ and if } x \in \mathcal{I}, \\
\|x\|_p^p &\geq [\mathcal{A} : \mathbb{Q}] \left(\prod_{0 \leq i < d} |N_{L/\mathbb{Q}}(x_i)| \right)^{p/[\mathcal{A}:\mathbb{Q}]} = [\mathcal{A} : \mathbb{Q}] \left(\left| N_{L/\mathbb{Q}} \left(\prod_{0 \leq i < d} x_i \right) \right| \right)^{p/[\mathcal{A}:\mathbb{Q}]}
\end{aligned}$$

By assumption, the coefficients x_i lie in the ideal $\mathfrak{J}\mathcal{O}_L$. Thus $x_i \in \bar{\mathcal{I}} := \mathcal{I} \cap \mathcal{O}_L$ for $i = 0, \dots, d-1$, and so $\prod_{0 \leq i < d} x_i \in \bar{\mathcal{I}}^d$, and hence $\|x\|_p^p \geq [\mathcal{A} : \mathbb{Q}] \cdot |N_{L/\mathbb{Q}}(\bar{\mathcal{I}})|^{dp/[\mathcal{A}:\mathbb{Q}]}$. Finally, to see $\lambda_1^\infty(\mathcal{I}) \geq (N_{L/\mathbb{Q}}(\bar{\mathcal{I}}))^{1/nd}$, $\|x\|_\infty = \sup_{i,j,\alpha} |\alpha(\phi(x)_{i,j})| \geq \prod_{i,j,\alpha} |\alpha((\phi(x))_{i,j})|^{1/nd^2} = N_{L/\mathbb{Q}}(\prod_{0 \leq i < d} x_i)^{1/nd^2}$. $\square$

Mapping Between Bases of $\mathcal{A}$

We will later need to consider mapping between the coefficient embedding of an element and the canonical embedding of the same element, via a linear transformation. Let $d = 2$; then $\mathcal{A}$ embeds into H^2 under the canonical embedding. Now, since $\Lambda = \mathcal{O}_L + u\mathcal{O}_L$, and $\mathcal{O}_L = \mathbb{Z}[\zeta_{2^r}, \frac{1+\sqrt{\ell}}{2}]$, a matrix acting on a vector to map it to a coefficient embedding representation should act on the first and second coordinates $(\sigma_L(\Lambda))_i$, $i = 1, 2$ in the desired way. Thus the required transformation is $V_\Lambda = \begin{pmatrix} \sigma(\vec{p}) & \mathbf{0} \\ \mathbf{0} & \sigma(\vec{p}) \end{pmatrix}$. Note if $\sigma(\vec{p})$ is invertible, so is V_Λ . We do similarly with respect to $\vec{d}$ and Λ . We can then obtain bounds for norms defined over these bases: for $x \in \Lambda$ with $d = 2$ we obtain

$$\|x\|_{\sigma(\vec{d})} \leq \sqrt{2} s_1(\vec{p}) \|x\|.$$

CLWE and its Security

Below, we link the hardness of NTRU in CDAs to that of CLWE. Here we recall the security reductions which established the hardness of CLWE:

Definition 93. Define the distributions Σ_α as the set of Gaussian distributions Σ over $\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$ with Gaussian marginal distribution in the $(i, j)^{th}$ coordinate with parameter $r_{i,j} \leq \alpha$. The error distribution Υ_α on the family of error distributions is sampled from by choosing $\Sigma \in \Sigma_\alpha$ and adding it to D_r , where each $r_i := \alpha \left((n \cdot d^2)^{1/4} \cdot \sqrt{y_i} \right)$ for $y_1, \dots, y_{n \cdot d^2}$ sampled from $\Gamma(2, 1)$.

Recall the following security reductions for CLWE, from [71]:

Theorem 6.3. Let $\mathcal{A}$ be a cyclic division algebra over a number field L with center K and natural, maximal order Λ with $|\gamma| = 1$. Let $\alpha = \alpha(n) \in (0, 1)$ and $q = q(n) \geq 2$, unramified in L , be parameters such that $\alpha \cdot q \geq \omega(\sqrt{\log(nd^2)})$. Then, there is a polynomial-time quantum reduction from $\mathcal{A}$ -SIVP $_\xi$ to search $CLWE_{q, \Sigma_\alpha}$ for any $\sqrt{8Nd} \cdot \xi = (\omega(\sqrt{dn})/\alpha)$.

Theorem 6.4. Let Λ be the natural order of a cyclic algebra $\mathcal{A} = (L/K, \theta, \gamma)$, $q \in \text{poly}(n)$, and assume that $\alpha \cdot q \geq \eta_\varepsilon(\Lambda^\vee)$ for a negligible $\varepsilon = \varepsilon(n)$. Then, there is a ppt. reduction from search $CLWE_{q, \Sigma_\alpha, G}$ for any pairwise different $G \subset \Lambda_q^\vee$ to decision $CLWE_q, \Upsilon_\alpha$.

These reductions ground the security of decision CLWE on SIVP over ideal lattices in CDAs. Thus if we connect the security of NTRU to that of CLWE, we will have connected the security of NTRU to SIVP. However, we require a particular variant of CLWE to which to reduce NTRU. Here we recall the RLWE variant used in [154]. Let $s \in R_q$ and ψ be a distribution over R_q . Let $A_{s, \psi}^\times$ be the distribution defined by samples $(a, as + e)$ with $(a, e) \leftarrow U(R_q^\times) \times \psi$, where $R_q^\times$ is the set of invertible elements of R_q . When $q = \Omega(n)$, the probability of a uniform element of R_q being invertible is non-negligible, so RLWE is hard even when $A_{s, \psi}$ and $U(R_q \times R_q)$ are replaced by $A_{s, \psi}^\times$ and $U(R_q^\times \times R_q)$ respectively. Denote this variant by $RLWE^\times$.

It is known that s can be chosen from the same distribution as e without losing security [13]. The authors of [154] call the variant of RLWE when the secret and error are both chosen from the error distribution $RLWE_{\text{HNF}}^\times$. To see this, let algorithm $\mathcal{A}$ be able to solve $RLWE_{\text{HNF}}^\times$.

One can transform samples $((a_i, b_i))_i$ into samples $((a_1^{-1}a_i, b_i - a_1^{-1}b_1a_i))_i$, where inversion is performed in $R_q^\times$. This transformation maps $A_{s,\psi}^\times$ to $A_{-e_1,\psi}^\times$, and $U(R_q^\times \times R_q)$ to itself. Note that $b_i - a_1^{-1}b_1a_i = a_is + e_i - a_1^{-1}(a_1s + e_1)a_i = a_is + e_i - a_is - a_1^{-1}e_1a_i = -a_1^{-1}a_ie_1 + e_i$.

We define $\text{CLWE}^\times$ analogously: let $s \in \Lambda_q$, $e \leftarrow \chi$, and $a \leftarrow U(\Lambda_q^\times)$. Output $(a, as + e) \in \Lambda_q^\times \times \bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$, and call the distribution obtained $A_{q,s,\chi}^\times$. We can take s from the same distribution as the error to obtain $\text{CLWE}_{HNF}^\times$; to see the transformation as in the RLWE case, transform $\text{CLWE}^\times$ samples into $\text{CLWE}_{HNF}^\times$ samples via the transformation $(a_i, b_i) \mapsto (a_ia_1^{-1}, b_i - a_ia_1^{-1}b_1)$.

6.4 NTRU in CDAs

In the following, we follow the method outlined in [77] to implement NTRU in CDAs. After demonstrating that the basic form of NTRU adapts easily to our context, we will go on to discuss the tweaks, improvements, and modifications that have arisen in the literature, and how they can be brought into CDAs. We refer to NTRU in a cyclic division algebra as *CNTRU*.

NTRU Instances in CDAs

Definition 94. (*CNTRU instances*) Let $\mathcal{A} = (L/K, \theta, \gamma)$ be an algebra as constructed above, and Λ the natural order. Let $q \in \mathbb{Z}_{\geq 2}$. An instance of *CNTRU* is an element $h \in \Lambda_q$ such that $f \cdot h = g \bmod q\Lambda$ for non-zero pair $(f, g) \in \Lambda$.

We define the NTRU problem for CDAs, based off *CNTRU* instances:

Definition 95. (*The CNTRU problem*) Let Λ and q be as above, and $\epsilon > 0$. Let $\mathcal{D}$ be a distribution over instances of *CNTRU*. The *CNTRU* problem is, given $h \leftarrow \mathcal{D}$, to find non-zero (f, g) such that $f \cdot h = g \bmod q\Lambda$ and $\|f\|, \|g\| \leq \frac{\sqrt{q}}{\epsilon}$.

NTRU Lattices from CDAs

We now consider the lattices generated by *CNTRU* instances. These lattices are a generalization of [50] and [49]’s lattices: take a private key $(f, g) \in \Lambda^2$ and public key $h = f^{-1}g \bmod q\Lambda$.

Observe that the pair (f, g) satisfies

$$fh - g = 0 \bmod q\Lambda, \quad (6.1)$$

so in the same way as NTRU, the set $S = \{(f, g) \in \Lambda^2 : fh - g = 0 \bmod q\Lambda\} \subset \Lambda^2$ is a left Λ -module (i.e. S is additively closed and closed under multiplication from Λ on the left). We note that if we changed our convention and considered

$$\{(f, g) \in \Lambda^2 : hf - g = 0 \bmod q\Lambda\}$$

instead, we could write a generator matrix for this second (right) Λ -module as $\begin{pmatrix} h & 1 \\ q & 0 \end{pmatrix}$ where the columns generate the module over Λ^2 . By fixing a basis $\{u^i\}_i$, we can then rewrite this matrix to obtain one with entries in $\mathcal{O}_L$, $\left(\begin{array}{c|c} H & I_d \\ \hline qI_d & 0 \end{array} \right)$ where

$$H = \begin{pmatrix} h_0 & \gamma\theta(h_{d-1}) & \gamma\theta^2(h_{d-2}) & \dots & \gamma\theta^{d-1}(h_1) \\ h_1 & \theta(h_0) & \gamma\theta^2(h_{d-1}) & \dots & \gamma\theta^{d-1}(h_2) \\ \dots & \dots & \dots & \dots & \dots \\ h_{d-1} & \theta(h_{d-2}) & \theta^2(h_{d-3}) & \dots & \theta^{d-1}(h_0) \end{pmatrix}.$$

Note that in the module NTRU examples referenced above, the element h defines a vector over a field, so appears in just one column of the corresponding matrix, whereas one sample of CNTRU for $[L : K] = d$ results in $h \bmod q$ defining an NTRU-style matrix with d columns determined by h , as can be seen. This is (loosely) equivalent to d samples of module NTRU.

To make the comparison explicit, recall that module forms of NTRU rely on lattices of the form

$$\mathcal{L}_{\mathbf{h},q} = \{(\mathbf{F}, \mathbf{g}) \in \mathcal{R}^{d \times (d+1)} : \mathbf{F}\mathbf{h} - \mathbf{g} \equiv \mathbf{0} \bmod q\}.$$

In this case, one can see that these $\mathcal{R}$ -modules have a similar form to the CNTRU modules defined above as

$$\mathcal{L}_{h,q} = \{(f, g)^T \in \Lambda^2 : fh - g \equiv 0 \pmod{q}\},$$

when ring multiplication is written in matrix-vector form using the regular representation of Λ :

$$\mathcal{L}_{h,q} = \{(\mathbf{f}, \mathbf{g})^T \in \mathcal{O}_L^{2d \times 1} : \phi(f)\mathbf{h} - \mathbf{g} \equiv 0 \pmod{q}\}.$$

Thus we expect the hardness of NTRU problems in CDAs to lie between that of NTRU over rings and NTRU over modules. Moreover, because of the ring structure of Λ , one could use algorithms such as [43] to follow the analysis of [71] and gain (asymptotic) efficiency over standard forms of module NTRU. Finally, we note that the storage required for a CNTRU private key is much less than the module case (for multiple samples), because of the structure of $\phi(f)$ as compared with that of F , using the above notation. In particular, one only has to store the first column of $\phi(f)$, as opposed to the entire matrix.

NTRU-based PKE

To develop encryption based on the CNTRU problem, we proceed as in [77]. Take the following setup: let $\mathcal{A} = (L/K, \theta, \gamma)$ be a CDA, and $\Lambda \subset \mathcal{A}$ the natural order, assumed to be maximal. Let $K = \mathbb{Q}(\zeta_{2^r})$, $[K : \mathbb{Q}] = n$, and $[L : K] = d$. Then $\Lambda = \mathcal{O}_L \oplus u\mathcal{O}_L \oplus \dots \oplus u^{d-1}\mathcal{O}_L$. Denote by $\mathcal{L}_f$, $\mathcal{L}_g$, $\mathcal{L}_\phi$, and $\mathcal{L}_m$ sets of elements of Λ . Select $p, q \in \mathbb{Z}$ such that $\gcd(p, q) = 1$ and $p \ll q$.

Key Generation: Select f from $\mathcal{L}_f$, and g from $\mathcal{L}_g$. Furthermore, ensure that f has inverses in Λ_q and in Λ_p . Set $(pk, sk) := (h, (f, g))$ where

$$h := f^{-1} \cdot g \pmod{q\Lambda}.$$

Encryption: To encrypt $m \in \mathcal{L}_m$, take ϕ from $\mathcal{L}_\phi$ and use the public key, h , to form

$$c := ph \cdot \phi + m \bmod q\Lambda.$$

Decryption: To decrypt c , compute $a := f \cdot c \bmod q\Lambda$, then $f^{-1} \cdot a \bmod p\Lambda$.

Correctness

Note that

$$\begin{aligned} a &= f \cdot c \bmod q = f \cdot (ph \cdot \phi + m) \bmod q = fph \cdot \phi + f \cdot m \bmod q \\ &= pf \cdot (f^{-1} \cdot g) \cdot \phi + f \cdot m \bmod q = pg\phi + f \cdot m \bmod q, \end{aligned}$$

since $f \cdot f^{-1} \equiv 1 \bmod q$. Then

$$\begin{aligned} f^{-1} \cdot a \bmod p &= f^{-1}(pg \cdot \phi) + f^{-1}(f \cdot m) = p(f^{-1}g\phi) + (f^{-1} \cdot f) \cdot m \bmod p \\ &= (f^{-1} \cdot f) \cdot m \bmod p = m \bmod p. \end{aligned}$$

Remark: This is basically the same as NTRU, but we have to be careful about the order we multiply elements, because of noncommutativity.

Observe that when $d = 1$, we are in the usual set up for NTRU. We could choose the sets $\mathcal{L}_f$, $\mathcal{L}_g$ etc. to be analogous to the ring case, if for example we wanted f and g to be ternary.

Note that the original NTRU scheme doesn't meet the IND-CPA security condition (though [128] gives partial reductions for search and decision NTRU problems). Below we will state an adaptation to the above scheme, and mirror the security guarantee of [154].

6.5 Results on q -ary Lattices

In this section we prove a regularity lemma on q -ary lattices obtained from the natural order of our family of CDAs.

Uniformity of the NTRU Public Key Distribution

We ultimately aim to demonstrate near-uniformity of the CNTRU public key distribution, focusing on the case $d = 2$. Almost all of the argument below holds for arbitrary d , but one step restricts us to $d = 2$; we leave the removal of this restriction as a topic of future research. We prove our result for completely split primes, but note that the proof can be adapted for any prime which is unramified in L .

Let Λ be the natural order of a CDA as above, where $[K : \mathbb{Q}] = n$ and $[L : K] = d$. Let $q \in \mathbb{Z}$ be prime, such that q is unramified in $\mathcal{O}_L$. Then:

Lemma 6.4. *[119, Proposition 4] Suppose that $\mathcal{I} = \mathfrak{q}$ is a prime in $\mathcal{O}_K$, such that $\mathfrak{q}\mathcal{O}_L = \mathfrak{Q}_1\mathfrak{Q}_2 \cdots \mathfrak{Q}_g$ in L , with $\gamma \neq 0 \pmod{\mathfrak{q}}$. Then the only proper two-sided ideal of Λ containing $\mathcal{I}$ is $\mathcal{I}\Lambda = \bigoplus_{j=0}^{d-1} u^j \mathfrak{q}\mathcal{O}_L$.*

Since in our case Λ is a maximal order, ideals uniquely factorize into products of prime ideals and prime ideals are maximal. By the above lemma all unramified two-sided ideals of Λ factor into a product of ideals of the form $\mathfrak{q}\Lambda$, where $\mathfrak{q}$ lies in K . Thus any two-sided unramified ideal can be expressed as $\mathcal{I} = \prod_{i \in S} \mathfrak{q}_i \Lambda$, for some indexing set S . In the following, we will consider the ideals lying above $q\Lambda$, where q splits completely L : these have the form $\mathcal{I} = \prod_{i \in S} \mathfrak{q}_i \Lambda$ where $q\mathcal{O}_K = \prod_i^n \mathfrak{q}_i$ and $S \subset \{1, \dots, n\}$. We now define the following module lattices:

Definition 96. *Let $q \geq 2$ be a prime completely split in $\mathcal{O}_L$. Let $\mathcal{I}$ be an ideal of Λ of the form $\mathcal{I} = \prod_{i \in S} \mathfrak{q}_i \Lambda$ containing $q\Lambda$, and $\mathcal{I}_S$ be an ideal of Λ_q of the form $\mathcal{I}_S = \prod_{i \in S} \mathfrak{q}_i \Lambda / q\Lambda$ for some $S \subset \{1, \dots, n\}$. Let $m \geq 2$ and $\mathbf{a} = (a_1, \dots, a_m) \in \Lambda_q^m$.*

$$\mathbf{a}^\perp(\mathcal{I}_S) := \{(t_1, \dots, t_m) \in \mathcal{I}^m : \sum_i t_i a_i \equiv 0 \pmod{q}\}, \text{ and}$$

$$L(\mathbf{a}, \mathcal{I}_S) := \{(t_1, \dots, t_m) \in (\Lambda^\vee)^m : t_i \equiv a_i s \pmod{q\mathcal{I}^\vee} \text{ for some } s \in \Lambda^\vee, \forall i\}.$$

Lemma 6.5. $\mathbf{a}^\perp(\mathcal{I}_S) = q(L(\mathbf{a}, \mathcal{I}_S))^\vee$, and $L(\mathbf{a}, \mathcal{I}_S) = q(\mathbf{a}^\perp(\mathcal{I}_S))^\vee$.

Proof. To show $\mathbf{a}^\perp(\mathcal{I}_S) \subset q(L(\mathbf{a}, \mathcal{I}_S))^\vee$, we show that any $\mathbf{t} = (t_1, \dots, t_m) \in \mathbf{a}^\perp(\mathcal{I}_S)$ has $\text{Tr}(\mathbf{t} \cdot \mathbf{z}) \equiv 0 \pmod{q}$ for any $\mathbf{z} \in L(\mathbf{a}, \mathcal{I}_S)^\vee$. Write $z_i = a_i s + qz'_i$, for $s \in \Lambda^\vee$ and $z'_i \in \mathcal{I}^\vee$. Then

$Tr(\mathbf{t} \cdot \mathbf{z}) = Tr(\sum_i t_i z_i) = \sum_i Tr(t_i z_i) = \sum_i Tr(t_i a_i s) + Tr(q \cdot t_i z'_i) = Tr(\sum_i (t_i a_i) s) + q Tr(t_i z'_i) \in q\mathbb{Z}$.

To show the reverse containment, let $x \in L(\mathbf{a}, \mathcal{I}_S)^\vee$. We show that $\sum_i q x_i a_i \equiv 0 \pmod{q}$ and $q x_i \in \mathcal{I}$. Note $q \cdot (\mathcal{I}^\vee)^m \in L(\mathbf{a}, \mathcal{I}_S)^\vee$. Set v_i to be an element of $L(\mathbf{a}, \mathcal{I}_S)^\vee$ with zeroes everywhere except for the i th entry, which is $q s'$ for $s' \in \mathcal{I}^\vee$. Then $Tr(x \cdot v_i) = Tr(q \cdot x_i s') \in \mathbb{Z}$, so $q x_i \in \mathcal{I}$. Moreover, for all $\mathbf{t} \in L(\mathbf{a}, \mathcal{I}_S)$, we have $Tr(\mathbf{x} \cdot \mathbf{t}) \in \mathbb{Z}$. Writing $t_i = a_i s + q t'_i$ where $t'_i \in \mathcal{I}^\vee$, we obtain $Tr(\mathbf{x} \cdot \mathbf{t}) = \sum_i Tr(x_i a_i s + q x_i t'_i) = Tr((\sum_i x_i a_i) s) + \sum_i Tr(q x_i t'_i) \in \mathbb{Z}$, and hence we have $Tr((\sum_i x_i a_i) s) \in \mathbb{Z}$. So $\sum_i x_i a_i \in \Lambda$, as required. $\square$

We now lower bound the shortest vector in $L(\mathbf{a}, \mathcal{I}_S)$ probabilistically. Recall $K = \mathbb{Q}(\zeta_{2^r})$ with $[K : \mathbb{Q}] = n$, $M = \mathbb{Q}(\zeta_{2^r \ell})$ for a prime $\ell \equiv 1 \pmod{2^r}$, and L is intermediate of degree 2 over K .

Lemma 6.6. *Let $S \subset \{1, \dots, n\}$, $m \geq 2$, $d = 2$, and $\epsilon > 0$. Then $\lambda_1^\infty(L(\mathbf{a}, \mathcal{I}_S)) \geq B := q^\beta / (n\sqrt{\ell})$, where $\beta = (1 - \frac{|S|}{n})(\frac{3}{4} - \frac{1}{m}) - \epsilon$, except with probability at most $2^{(1+10m)n} q^{-4m\epsilon}$, where $\mathbf{a} \leftarrow U(\Lambda_q^\times)^m$.*

Proof. Set $P = Pr_{\mathbf{a} \leftarrow U((\Lambda_q^\times)^m)} [L(\mathbf{a}, \mathcal{I}_S) \text{ contains } \mathbf{t} \neq \mathbf{0} : \|\mathbf{t}\|_\infty < q^\beta / nd]$. To bound this, consider $P(\mathbf{t}, s) := Pr_{\mathbf{a} \leftarrow U((\Lambda_q^\times)^m)} [t_i \equiv a_i s \pmod{q\mathcal{I}^\vee}, \forall i]$. This, because $\mathbf{t} \in (\Lambda^\vee)^m$ lies in $L(\mathbf{a}, \mathcal{I}_S)$ if and only if $t_i \equiv a_i s \pmod{q\mathcal{I}^\vee}$ for some $s \in \Lambda^\vee$. Since the a_i are sampled independently, we can rewrite this as $P(\mathbf{t}, s) = \prod_i^m P_i(t_i, s)$, where $P_i(t_i, s) := Pr_{a_i \leftarrow U(\Lambda_q^\times)} [t_i \equiv a_i s \pmod{q\mathcal{I}^\vee}]$. So we obtain

$$P \leq \sum_{\mathbf{t} \in (\mathcal{I}^\vee)^m :} \sum_{s \in \Lambda^\vee / q\mathcal{I}^\vee} \prod_i^m P_i(t_i, s).$$

$$0 < \|t_i\|_\infty < B \quad \forall i$$

Now, since $\mathcal{I} = \prod_{i \in S} \mathfrak{q}_i \Lambda$, we have $\mathcal{I}^{-1} = \prod_{i \in S} \mathfrak{q}_i^{-1} \Lambda$, and

$$q\mathcal{I}^\vee = q\mathcal{I}^{-1} \Lambda^\vee = \left(\prod_{i=1}^n \mathfrak{q}_i \Lambda \right) \left(\prod_{i \in S} \mathfrak{q}_i^{-1} \Lambda \right) \Lambda^\vee = \prod_{i \in S'} \mathfrak{q}_i \Lambda^\vee,$$

where $S' = \{1, \dots, n\} \setminus S$. By the CRT $\mathcal{I}^\vee / q\mathcal{I}^\vee \cong \mathcal{I}^\vee / \mathfrak{q}_{i_1} \Lambda^\vee \times \dots \times \mathcal{I}^\vee / \mathfrak{q}_{i_{|S'|}} \Lambda^\vee$, for a subsequence $i_j \in S'$, $j = 1, \dots, |S'|$.

We claim that if $P_i(t_i, s) \neq 0$ there exists a subset $S'' \subset S'$ such that t_i and $s \in \prod_{i \in S''} \mathfrak{q}_i \Lambda^\vee$

and $t_i, s \notin \mathfrak{q}_j \Lambda^\vee$ for any $j \in S' \setminus S''$. If this weren't the case, there would exist $j \in S'$ such that $s \equiv 0 \pmod{\mathfrak{q}_j \Lambda^\vee}$ and $t \not\equiv 0 \pmod{\mathfrak{q}_j \Lambda^\vee}$, or vice versa. But in either scenario $P_i(t_i, s) = 0$, because $a_i \in \Lambda_q^\times$. So such a S'' exists.

If $j \in S''$, $t_i \equiv a_i s \equiv 0 \pmod{\mathfrak{q}_j \Lambda^\vee}$ for all $a_i \in \Lambda_q^\times$. Alternatively, if $j \in S' \setminus S''$, $t_i \equiv a_i s \not\equiv 0 \pmod{\mathfrak{q}_j \Lambda^\vee}$, so there is a unique such $a_i \in \Lambda_q^\times$ satisfying the equation. Finally, for $j \in S$, there is no constraint on the a_i . So for a fixed set size $|S''| = d'$, the number of possible $a_i \in \Lambda_q^\times$ satisfying $t_i \equiv a_i s \pmod{q\mathcal{I}^\vee}$ is

$$\left(\prod_{i=0}^{d-1} (q^d - q^i) \right)^{n-(|S'| - |S''|)} = \left(\prod_{i=0}^{d-1} (q^d - q^i) \right)^{n+d' - |S'|},$$

and so

$$P_i(t_i, s) = \left(\prod_{i=0}^{d-1} (q^d - q^i) \right)^{n+d' - |S'|} / \left(\prod_{i=0}^{d-1} (q^d - q^i) \right)^n = \left(\prod_{i=0}^{d-1} (q^d - q^i) \right)^{d' - |S'|},$$

since $\Lambda/\mathfrak{q}_i \Lambda \cong M_d(\mathbb{F}_q)$, so $\Lambda_q \cong \prod_{i=1}^n M_d(\mathbb{F}_q)$ and $|\Lambda_q^\times| = \prod_{i=1}^n |Gl_d(\mathbb{F}_q)|$.

We can now rewrite P as follows, where $\mathfrak{h} = \prod_{i \in S''} \mathfrak{q}_i \Lambda^\vee$:

$$P \leq \sum_{0 \leq d' \leq |S'|} \sum_{S'' \subset S'} \sum_{\mathbf{t} \in (\mathcal{I}^\vee)^m : t_i \in \mathfrak{h}} \sum_{s \in \Lambda^\vee / q\mathcal{I}^\vee \cap \mathfrak{h}} \prod_i^m \left(\prod_{i=0}^{d-1} (q^d - q^i) \right)^{d' - |S'|}.$$

$$|S''| = d' \quad 0 < \|t_i\|_\infty < B \quad \forall i$$

The rest of the analysis divides into two cases, depending on the size of d' . In the first case, we consider $d' \geq \beta n$. Define $N(B, d') := \#\{t \in \mathcal{I}^\vee : \|t\|_\infty < B \text{ and } t \in \mathfrak{h}\}$. Observe that $\|t\|_\infty = \max_{\alpha, i, j} |\alpha((\phi(t))_{i,j})| \geq \lambda_1^\infty(\mathfrak{h}) \geq N_{L/\mathbb{Q}}(\bar{\mathfrak{h}})^{1/nd}$, because $t \in \mathfrak{h}$, where $\bar{\mathfrak{h}} = \mathfrak{h} \cap L$. Observe that $\bar{\mathfrak{h}} = \prod_{i \in S''} \mathfrak{q}_i \Lambda^\vee \cap L = \prod_{i \in S''} \mathfrak{q}_i \mathcal{O}_L^\vee$, so

$$\begin{aligned} N_{L/\mathbb{Q}}(\bar{\mathfrak{h}})^{1/nd} &= N_{L/\mathbb{Q}}\left(\prod_{i \in S''} \mathfrak{q}_i \mathcal{O}_L^\vee\right)^{1/nd} = N_{L/\mathbb{Q}}\left(\prod_{i \in S''} \mathfrak{q}_i \mathcal{O}_L\right)^{1/nd} N_{L/\mathbb{Q}}(\mathcal{O}_L^\vee)^{1/nd} \\ &\geq \frac{q^{\frac{dd'}{nd}}}{n\sqrt{\ell}} = \frac{q^{\frac{d'}{n}}}{n\sqrt{\ell}} \geq \frac{q^\beta}{n\sqrt{\ell}} = B, \end{aligned}$$

where we used $N_{L/\mathbb{Q}}(\mathcal{O}_L^\vee) = \text{disc}(L)^{-1}$, and the bound $\text{disc}(L) \leq (n^2 \ell)^n$ (this bound holds for

$d = 2$). Thus $N(B, d') = 0$ if $d' \geq \beta n$.

The second case is $d' < \beta n$. Set $\mathfrak{B}(l, \mathbf{c}) = \{\mathbf{x} \in H^d : \|\mathbf{x} - \mathbf{c}\|_\infty < l\}$. One can interpret $N(B, d')$ as the number of points of $\sigma_{\mathcal{A}}(\mathbf{h})$ in $\mathfrak{B}(B, \mathbf{0})$. Set $\lambda := \lambda_1^\infty(\mathbf{h})/2$, so $\mathfrak{B}(\lambda, \mathbf{v}_1) \cap \mathfrak{B}(\lambda, \mathbf{v}_2) = \emptyset$ for any distinct $\mathbf{v}_1, \mathbf{v}_2 \in \mathfrak{h}$. Moreover, if $\mathbf{v} \in \mathfrak{B}(B, \mathbf{0})$, it holds that $\mathfrak{B}(\lambda, \mathbf{v}) \subseteq \mathfrak{B}(B + \lambda, \mathbf{0})$. We can then say that

$$\begin{aligned} N(B, d') &\leq \frac{\text{Vol}(\mathfrak{B}(B + \lambda, \mathbf{0}))}{\text{Vol}(\mathfrak{B}(B, \lambda, \mathbf{0}))} = \frac{(2(\lambda + B))^{nd^2}}{2\lambda^{nd^2}} = \left(\frac{B}{\lambda} + 1\right)^{nd^2} \\ &\leq \left(\left(\frac{q^\beta}{n\sqrt{\ell}}\right) / \left(\frac{\lambda_1^\infty(\mathbf{h})}{2}\right) + 1\right)^{nd^2} \leq (2q^{\beta - \frac{d'}{n}} + 1)^{nd^2} \leq 2^{2nd^2} q^{nd^2\beta - d'd^2}. \end{aligned}$$

As $\mathfrak{h}/q\mathcal{I}^\vee = \prod_{i \in S''} \mathfrak{q}_i \Lambda^\vee / \prod_{i \in S'} \mathfrak{q}_i \Lambda^\vee \cong \prod_{i \in S''} \mathfrak{q}_i \Lambda / \prod_{i \in S'} \mathfrak{q}_i \Lambda \cong \Lambda / \prod_{i \in S' \setminus S''} \mathfrak{q}_i \Lambda$, then $|\mathfrak{h}/q\mathcal{I}^\vee| = |\Lambda / \prod_{i \in S' \setminus S''} \mathfrak{q}_i \Lambda| = \prod_{i=1}^{|S' \setminus S''|} |M_d(\mathbb{F}_q)| = q^{d^2(|S'| - d')}$. Then

$$\begin{aligned} P &\leq \sum_{0 \leq d' \leq \beta n} \sum_{S'' \subset S'} \sum_{\mathbf{t} \in (\mathcal{I}^\vee)^m : t_i \in \mathfrak{h}} \sum_{s \in \Lambda^\vee / q\mathcal{I}^\vee \cap \mathfrak{h}} \prod_i^m \left(\prod_{i=0}^{d-1} (q^d - q^i) \right)^{d' - |S'|} \\ &\quad |S''| = d' \quad 0 < \|t_i\|_\infty < B \quad \forall i \\ &\leq \max_{d' < \beta n} \frac{q^{d^2(|S'| - d')} N(B, d')^m 2^{|S'|}}{(\prod_{i=0}^{d-1} (q^d - q^i))^{m(|S'| - d')}} \leq 2^{n(1+dm+2d^2m)} q^{-d^2nm\epsilon}, \end{aligned}$$

for $\epsilon = (1 - \frac{|S|}{n})(\frac{d+1}{2d} - \frac{1}{m}) - \beta$, using $|Gl_d(\mathbb{F}_q)| > q^{\frac{d(d+1)}{2}}/2^d$. $\square$

In the above proof we used $\text{disc}(L) \leq (n\sqrt{\ell})^{2n}$. This only holds for our construction of L when $d = 2$. The above result can be proven for more values of d , but because of the restriction in place on a theorem below, we specialise to $d = 2$. We now prove a regularity result.

Lemma 6.7. *Let q be completely split in L , $d = 2$, $m \geq 2$, $\delta \in (0, 1/2)$, $\epsilon > 0$, $S \subset \{1, \dots, n\}$, $\mathbf{c} \in \Lambda^m$, and $\mathbf{t} \leftarrow D_{\Lambda^m, \sigma, \mathbf{c}}$ for $\sigma \geq \frac{n\sqrt{\ell}}{\sqrt{\pi}} \sqrt{\ln(8mn(1 + 1/\delta))} q^{-\beta}$, where $\epsilon = (1 - \frac{|S|}{n})(\frac{3}{4} - \frac{1}{m}) - \beta$. For all but a fraction less than $2^{n(1+10m)} q^{-4nm\epsilon}$ of $\mathbf{a} \in (\Lambda_q^\times)^m$,*

$$\Delta(\mathbf{t} \bmod \mathbf{a}^\perp(\mathcal{I}_S), U(\Lambda^m / \mathbf{a}^\perp(\mathcal{I}_S))) \leq 2\delta.$$

Proof. A direct combination of Lemmas 2.1, 2.6, 6.5, and 6.6. $\square$

6.6 An NTRU Key Generation Algorithm

In [154] and [156], the authors published work improving the hardness guarantees of NTRU. They tweak the original version of NTRU, adding an error term that allows them to demonstrate IND-CPA security, assuming the hardness of a variant of RLWE. Here we adapt their work to our setting, following [169].

The Revised CNTRU Scheme

Recall D_σ samples over $L_{\mathbb{R}}^2$ to enable us to sample elements of Λ_q , and $p \in \Lambda_q^\times$. We will sample the elements s, e from the same distribution, $\chi = \lfloor D_{\xi q} \rfloor_{\Lambda^\vee}$, where $\lfloor \cdot \rfloor_{\Lambda^\vee}$ is the CRR discretisation, $\xi = \alpha \left(\frac{2nk}{\log(4nk)} \right)^{\frac{1}{4}}$, $\alpha q \geq \omega(\sqrt{\log 4n})$, and $k = O(1)$.

Setup The setup algorithm $\text{Setup}(1^n)$ takes in a security parameter n and outputs a tuple of parameters $\text{params}(n) = ((K = \mathbb{Q}(\zeta_n), L, \ell(n), \theta(n), q(n), \sigma(n), \alpha(n), \xi(n)))$, where $\ell(n)$ satisfies $\ell(n) \equiv 1 \pmod n$ and $\ell(n) \not\equiv 1 \pmod{pn}$ for any $p \mid n$, L is a degree d extension of K contained in $M = \mathbb{Q}(\zeta_{n\ell(n)})$, $\theta(n)$ generates L/K , $q(n)$ completely splits in L , $\sigma(n)$ parameterises the distribution of (f', g) , and $\alpha(n), \xi(n)$ parameterise the error distribution as above.

Key Generation: $\text{Gen}(1^n)$ runs $\text{Setup}(1^n)$ for $\text{params}(n)$. Sample $f' \leftarrow D_{\Lambda, \sigma}$ and let $f = p \cdot f' + 1$; if $f \bmod q \notin \Lambda_q^\times$, resample. Sample $g \leftarrow D_{\Lambda, \sigma}$; if $g \bmod q \notin \Lambda_q^\times$, resample.

Return secret key $sk = (f, g)$ and public key $pk = h = f^{-1}pg \in \Lambda_q^\times$.

Encryption: Given $m \in \Lambda_p^\vee$, sample $s, e \leftarrow \chi$ and return $c = hs + pe + m \in \Lambda_q^\vee$.

Decryption: Given ciphertext c and secret key f , compute $c' = f \cdot c \in \Lambda_q^\vee$ and return $c' \bmod p$.

Correctness: $c' = fc = f(hs + pe + m) = fhs + fpe + fm = pgs + fpe + fm$.

If the coefficients of $pgs + fpe + fm$ are small enough, reduction modulo q leaves the coefficients unchanged, and $c' \bmod p = m \bmod p$.

We want to prove that if there is an IND-CPA attack on CNTRU, then a variant of CLWE can be broken. The following holds for the algebras used in CLWE, namely when $K = \mathbb{Q}(\zeta_{2^r})$,

$n = [K : \mathbb{Q}]$ and L is a finite cyclic extension of K of degree 2. We now show there is a high probability of selecting an appropriate value f for the public key.

Lemma 6.8. [71, Lemma 17] *For a fixed d , the proportion of invertible elements of $M_d(\mathbb{F}_q)$ is at least $(1 - \frac{1}{q})^d$.*

Lemma 6.9. *Let $d = 2$, $0 < \epsilon < \frac{1}{2}$, $r \geq 2n\sqrt[4]{l}\sqrt{\frac{\ln 8n(1+1/\epsilon)}{\pi}} \cdot q^{\frac{1}{n}}$, $p \in \Lambda_q^\times$, $D_{\Lambda,r}$ a discrete Gaussian sampling Λ and $q \in \mathbb{Z}$ a prime that splits completely in K , i.e. $q\mathcal{O}_K = \prod_{i=1}^{[K:\mathbb{Q}]} \mathfrak{p}_i$. Then $\Pr_{f' \leftarrow D_r}[(pf' + 1 \bmod q\Lambda) \notin \Lambda_q^\times] \leq n \left(\frac{2}{q} - \frac{1}{q^2} + 2\epsilon \right)$.*

Proof. We bound $\Pr_{f' \leftarrow D_r}[(pf' + 1 \bmod \mathfrak{p}_i\Lambda) \notin \Lambda/\mathfrak{p}_i\Lambda^\times]$. Since r is sufficiently large, $pf' + 1 \bmod \mathfrak{p}_i\Lambda$ is statistically close to the uniform distribution. Thus the probability that $pf' + 1$ is not invertible in $\Lambda/\mathfrak{p}_i\Lambda$ is 1 minus the proportion of invertible elements in $\Lambda/\mathfrak{p}_i\Lambda \cong M_d(\mathbb{F}_q)$ plus 2ϵ . Note $M_d(\mathbb{F}_q)$ has size $|M_d(\mathbb{F}_q)| = q^{d^2}$ and the set of invertible elements in R_i size $|GL_d(q)| = \prod_{i=0}^{d-1} (q^d - q^i)$. By Lemma 6.8 this proportion is at least $(1 - \frac{1}{q})^d$, so with $d = 2$ we lower bound the probability with $1 - (1 - \frac{1}{q})^2$. The CRT and a union bound implies the result. Regarding r , since when $d = 2$ and K is a cyclotomic field with power of 2 conductor the number of roots of unity in Λ equals $[\mathcal{A} : \mathbb{Q}]$ and since $\mathfrak{p}_i\Lambda$ is a Λ -ideal, $\lambda_{nd^2}(\mathfrak{p}_i\Lambda) = \lambda_1(\mathfrak{p}_i\Lambda)$. We then apply Lemma 2.3 and compute $\eta_\epsilon(\mathfrak{p}_i\Lambda) \leq \sqrt{\ln(2nd^2(1+1/\epsilon))/\pi} \cdot \lambda_{nd^2}(\mathfrak{p}_i\Lambda) = \sqrt{\ln(2nd^2(1+1/\epsilon))/\pi} \cdot \lambda_1(\mathfrak{p}_i\Lambda) \leq \sqrt{\ln(2nd^2(1+1/\epsilon))/\pi} \cdot 2n\sqrt[4]{l}q^{1/n} = \sqrt{\ln(8n(1+1/\epsilon))/\pi} \cdot 2n\sqrt[4]{l}q^{1/n}$. $\square$

If $q \geq n + 1$, then $(1 - \frac{1}{q})^{nd} \geq ((1 - \frac{1}{n+1})^n)^d \geq e^{-d}$ and the proportion of invertible elements in Λ_q is non-negligible. We now show that with high likelihood the elements f and g used to construct the public key will not be too large.

Lemma 6.10. *Let $n \geq 8$ be a power of 2 such that $x^n + 1$ splits completely modulo $q \geq 8n$. Let $\mathcal{A} = (L/K, \theta, \gamma)$ with $K = \mathbb{Q}(\zeta_n)$, $[L : K] = 2$, $\delta > 0$, and $\sigma \geq 2n\sqrt[4]{l}\sqrt{\frac{2\ln(24n)}{\pi}} \cdot q^{1/n}$. The secret polynomials f, g returned by the CNTRU algorithm satisfy, with probability $\geq 1 - 2^{4-4n}$,*

$$\|f\| \leq \sqrt{2}(1 + \sigma\|p\|_\infty\sqrt{2n}) \text{ and } \|g\| \leq 2\sigma\sqrt{n}.$$

Proof. When $d = 2$, $\lambda_{nd^2}(\Lambda) = \lambda_1(\Lambda) \leq d\sqrt{n} \cdot (\text{disc}(\Lambda))^{\frac{1}{2nd^2}} \leq 2n\sqrt[4]{l}$. If we set $\delta = \frac{1}{3n-1}$, then Lemma 2.3 implies $\eta_\delta(\Lambda) \leq \sqrt{\frac{2\ln(24n)}{\pi}} \cdot 2n\sqrt[4]{l}$. We can then use Lemma 2.8 to obtain

$\Pr_{x \leftarrow D_{\Lambda, \sigma}}(\|x\| \geq d\sqrt{n}\sigma) \leq \frac{3n}{3n-2}2^{-nd^2}$. Then

$$\begin{aligned} \Pr_{g \leftarrow D_{\Lambda, \sigma}}(\|g\| \geq d\sqrt{n}\sigma \mid g \in \Lambda_q^\times) &= \frac{\Pr_{g \leftarrow D_{\Lambda, \sigma}}(\|g\| \geq d\sqrt{n}\sigma \text{ and } g \in \Lambda_q^\times)}{\Pr_{g \leftarrow D_{\Lambda, \sigma}}(g \in \Lambda_q^\times)} \\ &\leq \frac{\Pr_{g \leftarrow D_{\Lambda, \sigma}}(\|g\| \geq d\sqrt{n}\sigma)}{\Pr_{g \leftarrow D_{\Lambda, \sigma}}(g \in \Lambda_q^\times)} \\ &\leq \frac{3n}{3n-2} \cdot 2^{-4n} \cdot \left(1/1 - n \left(\frac{2}{q} - \frac{1}{q^2} + 2\epsilon\right)\right) \\ &\leq 2^{-4n} \cdot 16 \leq 2^{4-4n}. \end{aligned}$$

This applies to both f' and g , so we have $\|f'\|, \|g\| \leq 2\sqrt{n}\sigma$ with probability at least $1 - 2^{4-4n}$. Finally, observe $\|f\| = \|pf' + 1\| \leq \|pf'\| + \|1\| \leq \|p\|_\infty \|f'\| + \sqrt{2} \leq \|p\|_\infty \sigma 2\sqrt{n} + \sqrt{2} = \sqrt{2}(1 + \sigma\|p\|_\infty\sqrt{2n})$ with probability $\geq 1 - 2^{4-4n}$. $\square$

We now show near-uniformity of the required distribution, to ensure our NTRU public keys are statistically close to the uniform distribution over $\Lambda_q^\times$.

Theorem 6.5. *Let $\epsilon > 0$, q be completely split, $p \in \mathcal{Z}(\Lambda_q^\times)$, and $\sigma \geq 4n^{3/2}\sqrt[4]{\ell}\sqrt{2\ln(32nq)}q^{\frac{1}{2}+2\epsilon}$. Let $y_i \in \Lambda_q$ and $z_i = -y_i p^{-1} \bmod q$ for $i = 1, 2$, and $D_{\sigma, z_i}^\times$ denote $D_{\Lambda, \sigma}$ restricted by rejection to $\Lambda_q^\times + z_i$. Then when $d = 2$,*

$$\Delta\left(\frac{y_1 + pD_{\sigma, z_1}^\times}{y_2 + pD_{\sigma, z_2}^\times} \bmod q, U(\Lambda_q^\times)\right) \leq 2^{22n}q^{-8n\epsilon}.$$

Proof. Let $P_a := \Pr_{f_i \leftarrow D_{\sigma, z_i}^\times, i=1,2}[(y_1 + pf_1) \cdot (y_2 + pf_2)^{-1} = a]$, with $a \in \Lambda_q^\times$. We aim to show that $|P_a - \frac{1}{|\Lambda_q^\times|}| < \epsilon'$, for some $\epsilon' > 0$, except for an exponentially small fraction of the $a \in \Lambda_q^\times$. Let $\mathbf{a} = (a_1, a_2) \leftarrow U((\Lambda_q^\times)^2)$. When $z_i = -p^{-1}y_i \bmod q$, $(y_1 + pf_1) \cdot (y_2 + pf_2)^{-1} = -a_1^{-1}a_2 \bmod q$ is equivalent to $a_1f_1 + a_2f_2 = p^{-1}(-a_1y_1 - a_2y_2) \bmod q$, and so to $a_1f_1 + a_2f_2 = a_1z_1 + a_2z_2 \bmod q$. Since $-a_1^{-1}a_2 \in \Lambda_q^\times$ is uniform,

$$P_{-a_1^{-1}a_2} = P_{\mathbf{a}} := \Pr_{f_i \leftarrow D_{\sigma, z_i}^\times, i=1,2}[a_1f_1 + a_2f_2 = a_1z_1 + a_2z_2 \bmod q],$$

if $\mathbf{a} \in (\Lambda_q^\times)^2$. One can see that the set of solutions to $a_1f_1 + a_2f_2 = a_1z_1 + a_2z_2 \bmod q$ in Λ , taken from $D_{\sigma, z_i}^\times$, $i = 1, 2$, is $\mathbf{z} + \mathbf{a}^{\perp \times}$, where $\mathbf{a}^{\perp \times} = \mathbf{a}^\perp \cap (\Lambda_q^\times \cap q\Lambda)^2$, and $\mathbf{a}^\perp = \mathbf{a}^\perp(\Lambda_q)$. We

can then write

$$P_{\mathbf{a}} = \frac{D_{\Lambda^2, \sigma}(\mathbf{z} + \mathbf{a}^{\perp \times})}{D_{\Lambda, \sigma}(z_1 + \Lambda_q^\times + q\Lambda) \cdot D_{\Lambda, \sigma}(z_2 + \Lambda_q^\times + q\Lambda)}.$$

Now, let $\mathbf{t} \in \mathbf{a}^\perp$. Then $t_1 a_1 + t_2 + a_2 \equiv 0 \pmod{q}$ implies that $t_2 = -t_1 \frac{a_1}{a_2}$ and the t_i lie in a shared ideal of Λ_q . Denote this ideal by $\mathcal{I}_S$. Then

$$\mathbf{a}^{\perp \times} = \mathbf{a}^\perp \setminus \cup_{S \subset \{1, \dots, n\}} \mathbf{a}^\perp(\mathcal{I}_S) \text{ and } \Lambda_q^\times + q\Lambda = \Lambda \setminus \cup_{S \subset \{1, \dots, n\} \setminus \emptyset} (\mathcal{I}_S + q\Lambda).$$

Applying an inclusion-exclusion argument, we get two expressions to analyse:

$$D_{\Lambda^2, \sigma}(\mathbf{z} + \mathbf{a}^{\perp \times}) = \sum_{S \subset \{1, \dots, n\}} (-1)^{|S|} D_{\Lambda^2, \sigma}(\mathbf{z} + \mathbf{a}^\perp(\mathcal{I}_S)), \text{ and} \quad (6.2)$$

$$D_{\Lambda, \sigma}(z_i + \Lambda_q^\times + q\Lambda) = \sum_{S \subset \{1, \dots, n\}} (-1)^{|S|} D_{\Lambda, \sigma}(z_i + \mathcal{I}_S + q\Lambda). \quad (6.3)$$

We deal with (6.2) first, with two cases. If $|S| \leq \epsilon n$, use Lemma 6.7 with $m = 2$ and $\delta = q^{-nd^2 - \lfloor \epsilon n \rfloor d^2}$. Note that $q\Lambda^2 \subset \mathbf{a}^\perp(\mathcal{I}_S) \subset \Lambda^2$, so $|\Lambda^2 / \mathbf{a}^\perp(\mathcal{I}_S)| = q^{d^2(n - |S|)}$. Then for all except a fraction less than $2^{n(1+4d^2+2d)} q^{-2d^2 n \epsilon}$ of $\mathbf{a} \in (\Lambda_q^\times)^2$,

$$\left| D_{\Lambda^2, \sigma}(\mathbf{z} + \mathbf{a}^\perp(\mathcal{I}_S)) - \frac{q^{d^2(n - |S|)}}{q^{2nd^2}} \right| = \left| D_{\Lambda^2, \sigma}(\mathbf{z} + \mathbf{a}^\perp(\mathcal{I}_S)) - q^{-nd^2 - d^2|S|} \right| \leq 2\delta.$$

In the second case, when $|S| > \epsilon n$, one can choose a subset $S'' \subset S'$ such that $|S''| = \lfloor \epsilon n \rfloor$. Then $\mathbf{a}^\perp(\mathcal{I}_S) \subset \mathbf{a}^\perp(\mathcal{I}_{S'})$, so $D_{\Lambda^2, \sigma}(\mathbf{z} + \mathbf{a}^\perp(\mathcal{I}_S)) \leq D_{\Lambda^2, \sigma}(\mathbf{z} + \mathbf{a}^\perp(\mathcal{I}_{S'}))$, so $D_{\Lambda^2, \sigma}(\mathbf{z} + \mathbf{a}^\perp(\mathcal{I}_S)) \leq$

$2\delta + q^{-nd^2-d^2\lfloor \epsilon n \rfloor}$. We can now say that

$$\begin{aligned}
& \left| D_{\Lambda^2, \sigma}(\mathbf{z} + \mathbf{a}^{\perp \times}) - 2^{n(d-1)} \frac{|\Lambda_q^\times|}{|\Lambda_q|^2} \right| \\
& \leq \left| \sum_{S \subset \{1, \dots, n\}} (-1)^{|S|} D_{\Lambda^2, \sigma}(\mathbf{z} + \mathbf{a}^\perp(\mathcal{I}_S)) - 2^{n(d-1)} \left(2^{-n(d-1)} \frac{(q^{d^2} - 1)^n}{q^{2nd^2}} \right) \right| \\
& \leq \left| \sum_{S \subset \{1, \dots, n\}} (-1)^{|S|} D_{\Lambda^2, \sigma}(\mathbf{z} + \mathbf{a}^\perp(\mathcal{I}_S)) - \frac{(q^{d^2} - 1)^n}{q^{2nd^2}} \right| \\
& \leq \left| \sum_{S \subset \{1, \dots, n\}} (-1)^{|S|} D_{\Lambda^2, \sigma}(\mathbf{z} + \mathbf{a}^\perp(\mathcal{I}_S)) - \sum_{k=0}^n (-1)^k \binom{n}{k} q^{d^2(-n-k)} \right| \\
& \leq \left| \sum_{S \subset \{1, \dots, n\}} (-1)^{|S|} D_{\Lambda^2, \sigma}(\mathbf{z} + \mathbf{a}^\perp(\mathcal{I}_S)) - \sum_{S \subset \{1, \dots, n\}} (-1)^{|S|} q^{-d^2(n+|S|)} \right| \\
& \leq \left| \sum_{S \subset \{1, \dots, n\}} (-1)^{|S|} \left(D_{\Lambda^2, \sigma}(\mathbf{z} + \mathbf{a}^\perp(\mathcal{I}_S)) - q^{-d^2(n+|S|)} \right) \right| \\
& \leq 2^n (2\delta + 2q^{-d^2(n+\lfloor \epsilon n \rfloor)}) \leq 2^{n+1} (\delta + q^{-d^2(n+\lfloor \epsilon n \rfloor)}),
\end{aligned}$$

except for a fraction of $\mathbf{a} \in (\Lambda_q^\times)^2$ less than $2^{n(2+2d+4d^2)} q^{-2d^2 n \epsilon}$. Writing $D_{\Lambda^2, \sigma}(\mathbf{z} + \mathbf{a}^{\perp \times}) = (1 + \delta_0) 2^{n(d-1)} \frac{|\Lambda_q^\times|}{|\Lambda_q|^2}$, we find that

$$\begin{aligned}
|\delta_0| & \leq \frac{|\Lambda_q|^2}{|\Lambda_q^\times|} 2^{-n(d-1)} 2^{n+1} (\delta + q^{-d^2(n+\lfloor \epsilon n \rfloor)}) \\
& \leq 2^{nd} q^{nd^2} 2^{-n(d-1)} 2^{n+1} (\delta + q^{-d^2(n+\lfloor \epsilon n \rfloor)}) \\
& = 2^{2n+2} q^{-d^2 \lfloor \epsilon n \rfloor}
\end{aligned}$$

Moving on to (6.3), begin by observing that $\det(\mathcal{I}_S + q\Lambda) = N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) \sqrt{\text{disc}(\Lambda)} = q^{|S|} \sqrt{\text{disc}(\Lambda)}$. Moreover, $\lambda_{nd}(\mathcal{I}_S + q\Lambda) = \lambda_1(\mathcal{I}_S + q\Lambda) \leq d\sqrt{n} \cdot \det(\mathcal{I}_S + q\Lambda)^{1/nd^2} = d\sqrt{n} \cdot q^{|S|/nd^2} \text{disc}(\Lambda)^{1/2nd^2}$. When $d = 2$ and n is a power of two, we in fact have $\lambda_{nd^2}(\mathcal{I}_S + q\Lambda) \leq d\sqrt{n} \cdot q^{|S|/nd^2} \text{disc}(\Lambda)^{1/2nd^2}$. Since $\text{disc}(\Lambda/\mathbb{Z}) \leq (n\sqrt{\ell})^{4n}$, we obtain $\lambda_{nd^2}(\mathcal{I}_S + q\Lambda) \leq d\sqrt{n} \cdot q^{|S|/nd^2} \sqrt{n} \sqrt[4]{\ell} = nd \sqrt[4]{\ell} q^{|S|/nd^2}$. Then Lemma 2.3 implies that

$$\eta_\delta(\mathcal{I}_S + q\Lambda) \leq \sqrt{\ln(2nd^2(1 + 1/\delta))/\pi} \cdot \lambda_{nd^2}(\mathcal{I}_S + q\Lambda) \leq \sqrt{\ln(2nd^2(1 + 1/\delta))/\pi} \cdot nd \sqrt[4]{\ell} q^{|S|/nd^2}$$

Since σ is larger than this quantity for $|S| \leq n/2$ and $\delta = q^{-nd^2/2}$, we can apply Lemma 2.6 to obtain $|D_{\Lambda,\sigma}(z_i + \mathcal{I}_S + q\Lambda) - \frac{1}{|\Lambda/\mathcal{I}|}| = |D_{\Lambda,\sigma}(z_i + \mathcal{I}_S + q\Lambda) - \frac{1}{q^{d^2|S|}}| \leq 2\delta$. If $|S| > n/2$, we can pick a subset $S' \subset S$ such that $|S'| \leq n/2$, and then $D_{\Lambda,\sigma}(z_i + \mathcal{I}_S + q\Lambda) \leq D_{\Lambda,\sigma}(z_i + \mathcal{I}_{S'} + q\Lambda) \leq 2\delta + q^{-nd^2/2}$. We now justify a claim, before proceeding with the rest of the proof:

Claim: For $d \geq 2$ and $q \geq 5$, we have $\prod_{i=1}^d (q^i - 1) \geq (q^{\frac{d(d+1)}{2}} - 1)/2^{\frac{d-1}{2}}$.

To see this, induct on d . When $d = 2$, the claim simplifies to the statement $(q - 1)(q^2 - 1) > (q^3 - 1)/\sqrt{2}$, which is true iff the polynomial $(\sqrt{2} - 1)q^3 - \sqrt{2}q^2 - \sqrt{2}q + (1 + \sqrt{2}) > 0$, which is true when $q \geq 5$. Suppose the claim is true for $d = k - 1 \geq 2$, and consider $\prod_{i=1}^k (q^i - 1)$. By induction, $\prod_{i=1}^{k-1} (q^i - 1) \geq (q^{\frac{k(k-1)}{2}} - 1)/2^{\frac{k-2}{2}}$, and we can write

$$\prod_{i=1}^k (q^i - 1) \geq (q^{\frac{k(k-1)}{2}} - 1)(q^k - 1)/2^{\frac{k-2}{2}} = (q^{\frac{k(k+1)}{2}} - q^{\frac{k(k-1)}{2}} - q^k + 1)/2^{\frac{k-2}{2}}.$$

Then the claim is true if

$$(q^{\frac{k(k+1)}{2}} - q^{\frac{k(k-1)}{2}} - q^k + 1)/2^{\frac{k-2}{2}} > (q^{\frac{k(k+1)}{2}} - 1)/2^{\frac{k-1}{2}},$$

i.e. $(\sqrt{2} - 1)q^{\frac{k(k+1)}{2}} - \sqrt{2}q^{\frac{k(k-1)}{2}} - \sqrt{2}q^k + \sqrt{2} + 1 > 0$, which holds if $q \geq 5$, $k \geq 2$.

The claim implies that $2^{\frac{n(d-1)}{2}}|\Lambda_q^\times|/(q^{d^2} - 1)^n > 1$, for appropriate d and q , which we will use below. Resuming the proof, we have

$$\begin{aligned} & \left| D_{\Lambda,\sigma}(z_i + \Lambda_q^\times + q\Lambda) - 2^{\frac{n(d-1)}{2}} \frac{|\Lambda_q^\times|}{|\Lambda_q|} \right| \\ & \leq \left| \sum_{S \subset \{1, \dots, n\}} (-1)^{|S|} D_{\Lambda,\sigma}(z_i + \mathcal{I}_S + q\Lambda) - \frac{(q^{d^2} - 1)^n}{q^{nd^2}} \right| \\ & = \left| \sum_{S \subset \{1, \dots, n\}} (-1)^{|S|} D_{\Lambda,\sigma}(z_i + \mathcal{I}_S + q\Lambda) - \sum_{k=0}^n (-1)^k \binom{n}{k} q^{-d^2 k} \right| \\ & = \left| \sum_{S \subset \{1, \dots, n\}} (-1)^{|S|} D_{\Lambda,\sigma}(z_i + \mathcal{I}_S + q\Lambda) - \sum_{S \subset \{1, \dots, n\}} (-1)^{|S|} q^{-d^2 |S|} \right| \\ & = \left| \sum_{S \subset \{1, \dots, n\}} (-1)^{|S|} \left(D_{\Lambda,\sigma}(z_i + \mathcal{I}_S + q\Lambda) - q^{-d^2 |S|} \right) \right| \\ & \leq 2^n (2\delta + 2q^{-nd^2/2}) = 2^{n+1} (\delta + q^{-nd^2/2}); \end{aligned}$$

writing $D_{\Lambda,\sigma}(z_i + \Lambda_q^\times + q\Lambda) = (1 + \delta_i)2^{\frac{n(d-1)}{2}} \frac{|\Lambda_q^\times|}{|\Lambda_q|}$, for $\epsilon < \frac{1}{2}$ we get the required bounds on the δ_i since $|\delta_i| \leq 2^{\frac{-n(d-1)}{2}} \frac{|\Lambda_q|}{|\Lambda_q^\times|} 2^{n+1}(\delta + q^{-nd^2/2}) \leq 2^{\frac{n(d+3)}{2}+2} q^{-nd^2/2}$.

Finally, we obtain that since $P_{\mathbf{a}} = \frac{D_{\Lambda^2,\sigma}(\mathbf{z} + \mathbf{a}^{\perp \times})}{D_{\Lambda,\sigma}(z_1 + \Lambda_q^\times + q\Lambda) \cdot D_{\Lambda,\sigma}(z_2 + \Lambda_q^\times + q\Lambda)}$,

$$\begin{aligned} \left| P_{\mathbf{a}} - \frac{1}{|\Lambda_q^\times|} \right| &= \left| \frac{D_{\Lambda^2,\sigma}(\mathbf{z} + \mathbf{a}^{\perp \times})}{D_{\Lambda,\sigma}(z_1 + \Lambda_q^\times + q\Lambda) \cdot D_{\Lambda,\sigma}(z_2 + \Lambda_q^\times + q\Lambda)} - \frac{1}{|\Lambda_q^\times|} \right| \\ &= \left| \frac{(1 + \delta_0)2^{n(d-1)} \frac{|\Lambda_q^\times|}{|\Lambda_q|^2}}{(1 + \delta_1)2^{\frac{n(d-1)}{2}} \frac{|\Lambda_q^\times|}{|\Lambda_q|} (1 + \delta_2)2^{\frac{n(d-1)}{2}} \frac{|\Lambda_q^\times|}{|\Lambda_q|}} - \frac{1}{|\Lambda_q^\times|} \right| \\ &= \left| \frac{(1 + \delta_0)}{(1 + \delta_1)(1 + \delta_2)|\Lambda_q^\times|} - \frac{1}{|\Lambda_q^\times|} \right|, \end{aligned}$$

and since the δ_i tend to 0, we obtain the result. $\square$

6.7 A Provably Secure NTRU-based Scheme

In this section we provide a proof of IND-CPA security, subject to the hardness of LWE in CDAs, for the revised CNTRU scheme.

Security of the Revised Scheme

For convenience, we restate the variant CNTRU scheme:

Key Generation: Sample $f' \leftarrow D_{\Lambda,\sigma}$. Set $f = pf' + 1$; if $f \bmod q \notin \Lambda_q^\times$, resample. Sample $g \leftarrow D_{\Lambda,\sigma}$; if $g \bmod q \notin \Lambda_q^\times$, resample. Set $sk = (f, g)$, $pk = h = f^{-1}pg \in \Lambda_q^\times$.

Encryption: Given $m \in \Lambda_p^\vee$, sample $s, e \leftarrow \chi$ and return $c = hs + pe + m \in \Lambda_q^\vee$.

Decryption: Given c and f , compute $c' = f \cdot c \in \Lambda_q$ and return $c' \bmod p$.

We first obtain a bound on the infinity norm of a discretised Gaussian sample under the canonical embedding with the following lemma:

Lemma 6.11. Assume that $\xi = \alpha \left(\frac{ndk}{\log(nd^2k)} \right)^{\frac{1}{4}}$, $\chi = \lfloor D_{\xi \cdot q} \rfloor_{\Lambda^\vee}$, $\alpha q \geq \omega(\sqrt{\log nd^2})$ and $k = O(1)$. Set $\delta = \omega \left(\sqrt{nd \log nd^2} \cdot \alpha^2 \cdot q^2 \right)$ and B the decoding basis of $\Lambda^\vee$, then for any $\mathbf{t} \in H^d$,

$$\Pr_{\mathbf{x} \leftarrow \chi} (|\langle \mathbf{t}, \mathbf{x} \rangle| > \delta \|\mathbf{t}\|^2) \leq (nd^2)^{-\omega(\sqrt{nd \log nd^2}) \|\mathbf{t}\|^2}.$$

Proof. A Gaussian random variable $\mathbf{x} \leftarrow D_{q\xi}$ of mean $\mathbf{0}$ and standard deviation $\frac{q\xi}{\sqrt{2\pi}}$ has a noncentral subgaussian discretisation $\lfloor \mathbf{x} \rfloor$ with noncentrality 0 and deviation $\left(\frac{q^2\xi^2}{2\pi} + \frac{1}{2}s_1(B)^2\right)^{\frac{1}{2}}$ by Lemma 6.3. The definition of subgaussian gives

$$E(e^{\langle \mathbf{t}, \lfloor \mathbf{x} \rfloor \rangle}) \leq e^{\frac{1}{2} \left(\frac{q^2\xi^2}{2\pi} + \frac{1}{2}s_1(B)^2 \right) \|\mathbf{t}\|^2},$$

for any $\mathbf{t} \in H^d$. A Chernoff bound then implies

$$\begin{aligned} \Pr(|\langle \mathbf{t}, \lfloor \mathbf{x} \rfloor \rangle| > \delta \|\mathbf{t}\|^2) &= \Pr\left(e^{|\langle \mathbf{t}, \lfloor \mathbf{x} \rfloor \rangle|} > e^{\delta \|\mathbf{t}\|^2}\right) \\ &\leq 2e^{\frac{1}{2} \left(\frac{q^2\xi^2}{2\pi} + \frac{1}{2}s_1(B)^2 \right) \|\mathbf{t}\|^2 - \delta \|\mathbf{t}\|^2}. \end{aligned}$$

$s_1(B) \leq 1$, so $\frac{1}{2} \left(\frac{q^2\xi^2}{2\pi} + \frac{1}{2}s_1(B)^2 \right) \|\mathbf{t}\|^2 = \Omega\left(\alpha^2 \cdot q^2 \sqrt{nd \log(nd^2)}^{-\frac{1}{2}} \cdot \|\mathbf{t}\|^2\right)$. Thus

$$\Pr(|\langle \mathbf{t}, \lfloor \mathbf{x} \rfloor \rangle| > \delta \|\mathbf{t}\|^2) \leq (nd^2)^{-\omega(\sqrt{nd \log nd^2}) \|\mathbf{t}\|^2}.$$

□

The above lemma gives an estimate for $\|\mathbf{x}\|_\infty$ with $\mathbf{x} \leftarrow \chi = \lfloor D_{q\xi} \rfloor$:

$$\Pr_{e \leftarrow \lceil \chi \rceil} (\|e\|_\infty > \delta) \leq (nd^2)^{-\delta}, \quad (6.4)$$

where $\delta = \omega(\sqrt{nd \log nd^2} \alpha^2 q^2)$ and $\alpha q \geq \omega(\sqrt{\log nd^2})$. In the following, we make our assumption that $\ell \leq Cn$ for some constant $C \geq 2$; in this case, when C_1 and C_2 are bounds such that $\|\cdot\|^c \leq C_1 \|\cdot\|$ and $\|\cdot\| \leq C_2 \|\cdot\|^c$, we have $C_1 = \sqrt{2}s_1(\vec{p}) < 2\sqrt{2}Cn$, so $C_1 = O(n)$, and $C_2 = \sqrt{2}s_1(\vec{d}) < 1$.

Lemma 6.12. *Let $n \geq 8$ be a power of 2, $q \geq 8n$ split completely in L , $\ell \leq Cn$, $\sigma \geq 2n\sqrt[4]{l}\sqrt{\frac{2\ln(24n)}{\pi}}q^{1/n}$. The decryption algorithm outputs m with probability $1 - (4n)^{-\omega(\sqrt{2n \log 4n})}$ over s, e, f, g if $\omega(2\sqrt{2}n^2\sqrt{\log 4n}\alpha^2 q^2) \sigma \|p\|_\infty^2 \leq q/2$.*

Proof. Notice that $f \cdot h \cdot s = p \cdot g \cdot s \bmod q\Lambda^\vee$, we have $fc = pgs + pfe + fm \bmod q\Lambda^\vee \in \Lambda^\vee$. If $\|pgs + pfe + fm\|_\infty^c < \frac{q}{2}$, then we have fc has the representation of the form $pgs + pfe + fm$ in $\Lambda_q^\vee$. Hence, we have $m = (fc \bmod q\Lambda^\vee) \bmod p\Lambda^\vee$. It thus suffices to upper bound the probability that $\|pgs + pfe + fm\|_\infty^c \geq \frac{q}{2}$.

Note that $\|fc\|_\infty^c \leq \|fc\|^c \leq C_1 \|fc\| = C_1 (\|pgs\| + \|pfe\| + \|fm\|)$. By the choice of σ and Lemma 6.10, with probability larger than $1 - 2^{4-nd^2}$, $\|f\| \leq \sqrt{d}(1 + \sigma\|p\|_\infty\sqrt{nd})$ and $\|g\| \leq \sqrt{nd}\sigma$. Combining with (6.4),

$$\begin{aligned} \|pfe\| + \|pgs\| &\leq \sqrt{d}(1 + \sigma\|p\|_\infty\sqrt{nd})\|p\|_\infty\|e\|_\infty + \sqrt{nd}\sigma\|p\|_\infty\|s\|_\infty \\ &\leq 2\sigma\sqrt{nd}\|p\|_\infty^2\|e\|_\infty + \sqrt{nd}\sigma\|p\|_\infty\|s\|_\infty \leq \omega(nd^{3/2}\sqrt{\log nd^2}\alpha^2q^2)\sigma\|p\|_\infty^2 \end{aligned}$$

with probability $1 - (nd^2)^{-\omega(\sqrt{nd\log nd^2})}$. Since $m \in \Lambda^\vee/p\Lambda^\vee$, by reducing modulo the $p\sigma(\vec{d})_i$, write $m = \sum_{i=1}^{nd^2} \varepsilon_i p\sigma(\vec{d})_i$ with $\varepsilon_i \in (-\frac{1}{2}, \frac{1}{2}]$. We have

$$\|m\| = \left\| \sum_{i=1}^{nd^2} \varepsilon_i p\sigma(\vec{d})_i \right\| \leq \|p\|_\infty \left\| \sum_{i=1}^{nd^2} \varepsilon_i \sigma(\vec{d})_i \right\| \leq \|p\|_\infty \frac{\sqrt{nd}}{2} C_2,$$

so $\|fm\| \leq \|f\|\|m\| \leq \sqrt{d}(1 + \sigma\|p\|_\infty\sqrt{nd}) \cdot \|p\|_\infty \frac{\sqrt{nd}}{2} C_2 \leq 2\sigma\sqrt{nd}\|p\|_\infty \cdot \|p\|_\infty \frac{\sqrt{nd}}{2} C_2 \leq nd^2\sigma\|p\|_\infty^2 C_2$ with probability $\geq 1 - 2^{4-n}$. All together, we have

$$\begin{aligned} \|fc\|_\infty^c &\leq C_1 \left(\omega(nd^{3/2}\sqrt{\log nd^2}\alpha^2q^2)\sigma\|p\|_\infty^2 + nd^2\sigma\|p\|_\infty^2 C_2 \right) \\ &\leq \omega \left(n^2 d^{3/2} \sqrt{\log nd^2} \cdot \alpha^2 q^2 \right) \sigma\|p\|_\infty^2 \end{aligned}$$

with probability $1 - (nd^2)^{-\omega(\sqrt{nd\log nd^2})}$, since $C_2 \leq 1$ and $C_1 = O(n)$. $\square$

We now attempt a proof of IND-CPA security. Recall the CLWE variant we will use: let $s, e \leftarrow \chi$, and $a \leftarrow U(\Lambda_q^\times)$. Here χ is the CRR discretisation of the usual CLWE distribution to $\Lambda_q^\vee$; [71] gave a reduction from CLWE to this variant. Output $(a, as + e) \in \Lambda_q^\times \times \Lambda_q^\vee$, and call this distribution $A_{q,s,\chi}^\times$. Define the usual search and decision problems over this distribution to obtain $\text{CLWE}_{HNF}^\times$.

Lemma 6.13. *Let $n \geq 8$ be a power of 2, $d = 2$, $\ell \leq Cn$, and $q \geq 8n$ a prime such that*

$x^n + 1$ splits completely modulo q . Let $\delta > 0$, $p \in \mathcal{Z}(\Lambda_q^\times)$ and $\sigma \geq 2n^{3/2}\sqrt[4]{\ell}\sqrt{\ln(32nq)}q^{\frac{1}{2}+2\epsilon}$ satisfy the conditions of Lemma 6.12 and Theorem 6.5. If there exists an IND-CPA attack algorithm $\mathcal{A}$ against CNTRU, running in time T with advantage δ , then there exists an algorithm to solve decision-CLWE $_{\text{HNF}}^\times$ that runs in time $T' = T + O(\text{poly}(n))$ with success probability $\delta' = \delta - q^{-\Omega(n)}$.

Note that if $p \in \mathbb{Z}_q^\times$, the algorithm runs in time $T' = T + O(n)$.

Proof. The proof runs similarly to [154, Lemma 13], [169, Lemma 16]. We use the attack algorithm against CNTRU to construct an algorithm $\mathcal{B}$ with non-negligible advantage against CLWE $_{\text{HNF}}^\times$. Write $\mathcal{O}$ for an oracle that samples from one of $U(\Lambda_q^\times \times \Lambda_q^\vee)$ and $A_{s,\chi}^\times$ for some previously chosen $s \leftarrow \chi$. $\mathcal{B}$ begins by obtaining a sample $(h', c') \in \Lambda_q^\times \times \Lambda_q^\vee$ via $\mathcal{O}$. The idea is that $\mathcal{B}$ uses $\mathcal{A}$ with public key $h = p \cdot h' \in \Lambda_q$ to guess the bit b in the IND-CPA experiment. As part of the IND-CPA experiment, $\mathcal{A}$ outputs messages $m_0, m_1 \in \Lambda_p^\vee$. $\mathcal{B}$ then samples $b \leftarrow U(\{0, 1\})$, computes ciphertext $c = p \cdot c' + m_b$, and sends c to $\mathcal{A}$. Finally, $\mathcal{A}$ submits a value b' for b , and if $b' = b$, $\mathcal{B}$ outputs 1. Else, $\mathcal{B}$ outputs 0.

Since h' is uniformly random in $\Lambda_q^\times$ and p is invertible mod q , so is h , and so the public key given to $\mathcal{A}$ is of statistical distance at most $q^{-\Omega(n)}$ from the correct distribution for the attack algorithm, by Theorem 6.5. Additionally, since $c' = h \cdot s + e$ with $s, e \leftarrow \chi$, c has the desired distribution for the IND-CPA attack algorithm. In conclusion, if $\mathcal{O}$ outputs samples from $A_{s,\chi}^\times$, then $\mathcal{A}$, and hence $\mathcal{B}$, returns 1 with probability $\geq 1/2 + \delta - q^{-\Omega(n)}$. If $\mathcal{O}$ outputs uniform samples from $U(\Lambda_q^\times \times \Lambda_q^\vee)$, then c is uniformly random in $\Lambda_q^\vee$ since $p \in \Lambda_q^\times$, and is independent of b . Thus $\mathcal{B}$ outputs 1 with probability $1/2$, as desired. $\square$

If $K = \mathbb{Q}(\zeta_{2^r})$, $2^{r-1} = n \geq 8$, $L = \mathbb{Q}(\zeta_{2^r}, \sqrt{\ell})$ for prime $\ell : \ell \equiv 1 \pmod{2^r}$, $\ell \leq Cn$ for some $C \geq 2$, $q \geq 8n$ a prime q split completely in L , $\alpha \in (0, 1)$: $\alpha q \geq \omega(\sqrt{\log 4n})$, $\xi = \alpha \left(\frac{2nk}{\log(4nk)} \right)^{\frac{1}{4}}$ with $k = O(1)$, $\epsilon \in (0, \frac{1}{2})$, $p \in \Lambda_q^\times$, $\sigma \geq 2n^{3/2}\sqrt[4]{\ell}\sqrt{\ln(32nq)}q^{\frac{1}{2}+2\epsilon}$ and $\omega(2\sqrt{2}n^2\sqrt{\log 4n}\alpha^2q^2)\sigma\|p\|_\infty^2 \leq q/2$, the security reduction to CLWE from ideal lattice problems holds, and CNTRU connects with SIVP (note that the CLWE reduction is valid for a restricted secret space).

6.8 Choosing Parameters and Number Fields

In this section, we give a brief overview of some parameters choices for NTRU, focusing on n and q , before giving possible parameters for CDAs.

Parameters for NTRU in Previous Works

NTRU [77] uses convolution rings $\mathbb{Z}[x]/(x^N - 1)$ with N prime, which are not ring of integers of algebraic number fields. This is the same as in [76], [83]; since CDAs are constructed from fields, the parameters used here do not adapt straightforwardly to our setting. This situation is mirrored in the NTRU finalist in NIST's post-quantum standardisation process, [41]. The authors use the rings $\mathbb{Q}(x)/(x - 1)\Phi_n(x)$ with prime n , which are not fields. In this case, the polynomials ' $\Phi_n(x)$ ' are cyclotomic, hence $x^n - 1 = (x - 1)\Phi_n(x)$; and $(x - 1)\Phi_n(x)$ is plainly not irreducible.

However, the authors of [154], [156] replace $x^n - 1$ by $x^n + 1$, for power-of-two n . These are the $2n$ th cyclotomic polynomials, which are amenable to generalisation by CDAs. Since n is a power of two, natural choices are $n = 512$ or $n = 1024$. They also recommend $p = 3$ or $p = 2$. As for q , if $\alpha q > n^{0.75}$, the decryption algorithm recovers m with probability $1 - n^{\omega(1)}$. For the security proof to hold, one needs $q \equiv 1 \pmod{2n}$. So in the context of CDAs, one could choose $n = 256$, $q = 7681$, or $n = 512$, $q = 12289$, if working with the same framework as [156].

Falcon [3] uses $n = 512$ for NIST Level I, and $n = 1024$ for NIST Level V, where n is the degree of the cyclotomic ring. They use $q = 12289$. ModFalcon [50] uses a rank two module over a power of two cyclotomic of degree 512, and also sets $q = 12289$. In contrast, ModNTRU [49] uses a rank three module over a power of two cyclotomic of degree 512, but uses $q = 2^{19}$, instead of prime q .

Parameters for NTRU in CDAs

We follow the module NTRU instances in using power of two cyclotomics. Although there has been some concern raised over the large number of subfields and automorphisms attached

to these objects [160], there has not yet been an efficient attack against the NTRU problem exploiting these features (for non-‘overstretched’ parameters). We recommend using algebras of dimension approximately 1000 over $\mathbb{Q}$. Following the construction detailed above: $\mathcal{A} = (L/\mathbb{Q}(\zeta_n), \theta, \zeta_n)$ with $K \subset L \subset M = \mathbb{Q}(\zeta_{\ell n})$ for $\ell \equiv 1 \pmod{n}$, $\ell \not\equiv 1 \pmod{pn}$ for any prime $p \mid n$. Take q to be a prime completely split in L , not too large to avoid attacks exploiting ‘overstretched’ parameters. Example parameters might be $n = 1024$, $d = 2$, $\ell = 12289$, and $q = 13313$.

As for choosing the sets $\mathcal{L}_f$ and so on, one can take these to be binary or ternary with set weights for efficiency, as some other NTRU schemes do, if desired. We leave the precise analysis of choices of such sets as future work.

6.9 Sketched Cryptographic Functionality

KEM

Here we outline an CNTRU-based KEM. We follow the structure of the KEM in [41] closely. Denote the CNTRU key generation, encryption, and decryption algorithms by KeyGen, Encrypt, and Decrypt respectively.

KeyGen _{KEM}
1. $(pk', sk') = (h, (f, g, h)) \leftarrow \text{KeyGen}(\text{seed})$
2. $s \leftarrow_{\$} \{0, 1\}^{nd^2}$
3. return $(pk, sk) = (pk', (sk', s)) = (h, (f, g, h, s))$

Below, $H_1(\cdot)$ and $H_2(\cdot)$ are hash functions. Correctness is straightforward.

Encapsulate(h)	Decapsulate($(f, g, h, s), c$)
1. $(r, m) \leftarrow \mathcal{L}_r \times \mathcal{L}_m$	1. $(r, m) \leftarrow \text{Decrypt}(sk, c)$
2. $c \leftarrow \text{Encrypt}(h, (r, m))$	2. $k_1 \leftarrow H_1(r, m)$, $k_2 \leftarrow H_2(s, c)$
3. $k_1 \leftarrow H_1(r, m)$	3. if $(r, m) \neq \perp$ return k_1
4. return (c, k_1)	4. else return k_2

Signatures

We now give a signature scheme for CNTRU, based on pqNTRUSign [75]. Below are the key generation, signing, and verification algorithms. As usual, we fix coprime integers p and q with $q \gg p$. In [75], ternary polynomials are used, though we note this is not essential for the correctness of the scheme. Let $\mathcal{T}$ denote elements of Λ with ternary coefficients, i.e. $\mathcal{T} = \{f = \oplus_{i=0}^{d-1} u^i f_i \in \Lambda : f_i \text{ is ternary}\}$. Moreover, let $\mathcal{R} = \{h = \oplus_{i=0}^{d-1} u^i h_i : \|h_i\|_\infty \leq q/2, i = 0, \dots, d-1\}$ and $\mathcal{S} = \{g = \oplus_{i=0}^{d-1} u^i g_i \in \Lambda : \|g_i\|_\infty \leq p/2, i = 0, \dots, d-1\}$.

KeyGen _{Sign}
1. $F \leftarrow \mathcal{T}$ and set $f = pF$.
2. If $f \notin \Lambda_q^\times$, resample F .
3. $g \leftarrow \mathcal{S}$.
4. If $g \notin \Lambda_q^\times$, resample g .
5. $h := f^{-1}g \bmod q$.
6. $(pk, sk) = (h, (f, g))$.

Like pqNTRUSign, we require a function H which takes a public key h and a message μ to be signed, and outputs a pair of elements with bounded norm, that is $H : \mathcal{R} \times \{0, 1\}^* \rightarrow \mathcal{S} \times \mathcal{S}$. The values B_s and B_t are bounds that can be changed to vary the security level and efficiency of the protocol.

Sign(μ): input $(pk, sk, \mu) = (h, (f, g), \mu)$
1. $(s_p, t_p) = H(h, \mu)$.
2. $r \leftarrow \Lambda : \ r\ _\infty \leq \left\lfloor \frac{q}{2p} + \frac{1}{2} \right\rfloor, i = 0, \dots, d-1$.
3. $(s_0, t_0) := (s_p + pr, s_0 h \bmod q)$.
4. $a := (t_p - t_0)g^{-1} \bmod p$.
5. If $\ af\ _\infty > B_s$ or $\ ag\ _\infty > B_t$ or $\ s\ _\infty > \frac{q}{2} - B_s$ or $\ t\ _\infty > \frac{q}{2} - B_t$, restart.
6. $(s, t) := (s_0, t_0) + (af, ag)$.
7. Output $\sigma = (s, t, \mu)$.

The signing algorithm is nearly identical to that of pqNTRUSign. We do, however, have to be careful about how we multiply a and f, g . For correctness to hold, we use the pair (af, ag) in our algorithm, whereas in [75] one can use (fa, ga) or (af, ag) . This is because the NTRU lattice is an $\mathcal{O}_L$ -bimodule in the commutative case, whereas CNTRU lattices are only left Λ -modules.

Verify(σ): input $(h, \sigma) = (h, (s, t, \mu))$
1. $(s_p, t_p) \leftarrow H(h, \mu)$. 2. Check $(s_p, t_p) \equiv (s, t) \pmod{p}$. 3. Check $t \equiv sh \pmod{q}$. 4. Check $\ s\ _\infty \leq \frac{q}{2} - B_s$ and $\ t\ _\infty \leq \frac{q}{2} - B_t$. 5. If all checks succeed, output <i>Valid</i>.

It is straightforward to show correctness for this scheme, for well chosen B_s, B_t .

We do not analyse the above schemes in detail; we include them to demonstrate that such functionality is obtainable from NTRU in noncommutative rings.

6.10 Chapter Summary

In this chapter we have defined a general form of NTRU, and shown that for certain parameters the NTRU instances obtained are indistinguishable from samples chosen uniformly at random. We have given the cryptographic application of a public-key encryption scheme, and shown that an IND-CPA attack on the PKE scheme implies an efficient attack on decision CLWE. Along the way we have proved new results on q -ary lattices obtained from natural orders of CDAs.

Future work includes selecting parameters for the signature scheme and the KEM and implementing these schemes. Further cryptanalysis is required to better understand the security of CNTRU. It would also be desirable to see if one could lift the constraint ‘ $d = 2$ ’, and obtain results for higher degrees.

Chapter 7

Conclusion

εἰ δὲ ὁ οὐ βλέπομεν ἐλπίζομεν, δι' ὑπομονῆς ἀπεκδεχόμεθα.
—Παῦλος, ἡ πρὸς Ρωμαίους ἐπιστολή, [55,57] AD.

7.1 Summary of Thesis Achievements

This thesis was concerned with the CLWE problem, its variants, GRLWE, and NTRU in CDAs.

7.1.1 Clarifying the Security of CLWE

We began in Chapter Three by studying the security reduction of [71]. We showed that the guarantee given by the security proof in that work did not give the claimed security level (that is, hardness from problems strictly harder than ideal lattice problems in number fields). We did this by proving a new structure result on the ideals of the natural order Λ in $\mathcal{A} = (L/K, \theta, \gamma)$ where $K = \mathbb{Q}(\zeta_n)$ and $\gamma = \zeta_n$, for any n . This was combined with properties of the canonical embedding to reduce ideal SIVP in ideals of Λ to ideal SIVP in ideals of $\mathcal{O}_L$. This result completely classified ideals in Λ which have intersection with K which is unramified in $\mathcal{O}_L$, and extended the work of [119]. In addition to its implication for CLWE, it also implied a Gentry-Szydlo style result for the Ideal Lattice Isomorphism Problem in Λ .

Chapter Three then turned to positive results. We first showed that SIVP on module lattices in rank two can be reduced to search CLWE. This formalised the sense in which CLWE is a structured form of MLWE. We then introduced CMLWE, a module variant of CLWE in which modules of finite rank over Λ are considered as the sample space for LWE-style samples. This generalised both CLWE and MLWE. The end to which this variant was introduced was to obtain a result like that of [8], in which it is shown that after a trade-off in parameters, the security of RLWE (with modulus q^k) is the same as MLWE (with modulus q). We demonstrated a similar result for CLWE and CMLWE. To achieve this, we proved lemmas on pseudobases of modules over certain noncommutative rings, demonstrated the hardness of the search variant of CMLWE, and analysed the statistical distance of certain combinations of algebra elements sampled from discrete and continuous Gaussians. Finally, we introduced one-sided ideals and defined lattice problems on them under the canonical embedding. We then adapted the security proof of [71] to hold for these ideal lattices, which required proving new ‘clearing out ideals’ lemmas for one-sided ideals, and adapting the reduction from $q\mathcal{A}$ -BDD to search CLWE using a theorem of [139] on conjugations by one-sided ideals. We then gave two constructions of one-sided ideals.

7.1.2 Extending CLWE to Other Algebras

Chapter Four addressed algebraic constructions of CDAs, parameterised by the choice of γ , and their application to LWE-based cryptography. CLWE took $\gamma \in \mathcal{O}_K$, and in particular $\gamma = \zeta_n$ for prime-power n . The first result of Chapter Four was an extension of the proof (from [95]) that for $\mathcal{A} = (L/K, \theta, \gamma)$ where $K = \mathbb{Q}(\zeta_n)$, ζ_n is non-norm, to hold for composite n , not only for prime-power n . The later proofs of [71] immediately hold for these non-norm elements, since they do not rely on n being a prime-power. We then gave possible parameter sets for CDAs and moduli for CLWE that satisfy the conditions of the theorem, for a range of algebra indices. We next considered algebras of the form $\mathcal{A} = (L/K, \theta, \gamma)$ where $K = \mathbb{Q}(\zeta_n)$ and $\gamma \in K \setminus \mathcal{O}_K$ of unit-magnitude. Previous methods to find such fractional non-norm elements had been developed for low-degree cyclotomics in [121]. We extended the results of that work to hold for

any cyclotomic with ring of integers a PID. We then studied the more general case, where $\mathcal{O}_K$ is a Dedekind domain. We proved new results on non-norm elements in this setting, developing a method to find such elements. We then studied LWE defined over maximal orders in the CDAs obtained, and gave a reduction from ideal SIVP to a search CLWE-style problem.

Finally, we considered taking γ in the maximal subfield of $\mathcal{A}$, that is $\gamma \in \mathcal{O}_L \setminus \mathcal{O}_K$. These algebras are nonassociative, studied in [171], [152] and the ideal theory of natural orders in such algebras less developed than in the associative case, the state of the art being [131]. We first developed the ideal theory in such natural orders. We classified the form of all maximal ideals in Λ lying above ideals in K unramified in $\mathcal{O}_L$, and used this to extend the ideal structure theorem of Chapter Three to the nonassociative setting, when γ is a unit. This then implied fundamental results on the ideal arithmetic of Λ : unramified ideals have unique factorisation into primes, and multiply commutatively and associatively. We then defined lattice problems in these ideals, and reduced ideal SIVP to decision LWE defined in these nonassociative spaces. This reduction was striking for its lack of restriction on the secret space, a constraint which remains a limitation of CLWE. We then analysed PKE schemes, compensating for the lack of a multiplicative matrix representation with a small additive step in the decryption algorithm, and suggested some parameters.

7.1.3 Attacking and Repairing GRLWE

In Chapter Five we turned to GRLWE, another structured form of MLWE, based off structures in integral group rings over dihedral groups [47]. The group ring structure employed was shown to have the properties of an order in a central simple algebra, and in fact that of a cyclic algebra. In the case of $G = D_{2n}$, this cyclic algebra had $\gamma = 1$, and by a result of [139] was isomorphic to a matrix ring over the center K . We then analysed the impact of the map from the group ring to the matrix ring on the errors of GRLWE samples, and showed that the restriction of the isomorphism to the integral elements was a bijection, when the modulus q was chosen appropriately (and in fact, as is typically chosen in practice). The matrix samples in the image of this map were doubled in number and halved in dimension, and therefore susceptible

to attack from any LWE solver if the initial dimension was sufficiently low. The matrix secret obtained could then be inverted under the map to obtain a solution to the original group ring problem. We attempted to quantify this attack with the lattice estimator [9], and extended it to the more general group rings suggested by the authors of the original paper. We then proposed generalised quaternion group rings Q_{4n} as a structure not susceptible to our attack. When one maps the group ring to an order in a cyclic algebra, one finds in the case of $G = Q_{4n}$ that $\gamma = -1$, which is not a norm for the number fields L/K that construct the algebra. Thus there is no such isomorphism to a matrix ring, and our attack failed.

7.1.4 Introducing CNTRU

Finally, in Chapter Six we studied NTRU in CDAs. We introduced ‘CNTRU’, a PKE scheme based off NTRUEncrypt which relies on the hardness of NTRU-style instances in the natural order Λ of quaternion algebras of the form $\mathcal{A} = (L/K, \theta, \gamma)$ where $K = \mathbb{Q}(\zeta_n)$, $L = K(\sqrt{\ell})$, and $\gamma = \zeta_n$. We followed the general outline of [156], developing results on q -ary lattices, in this case coming from Λ , which were used to prove the indistinguishability of the distribution of CNTRU public keys from uniform. This is proved for a scheme tweaked in the sense of [169], where elements are mapped under the canonical embedding and then discretised. Moreover, the result, using current methods, appears to fail for higher index algebras: when the index is larger than two, the unit group of Λ appears to not be dense enough in Λ for the asymptotic statement of the theorem to hold. We then demonstrate IND-CPA security of CNTRU, assuming the hardness of a variant of CLWE in which the public element a is invertible and s is chosen from the same distribution as the error, in $\Lambda_q^\vee$. This links CNTRU with ideal SIVP, albeit through the restricted search-to-decision reduction of CLWE. The structure of our algebras is somewhat nonstandard for NTRU, and the presence of $\sqrt{\ell}$ appears in invariants of the algebra such as the discriminant; to ensure reasonable parameters for CNTRU, we stipulate that ℓ should be a bounded multiple of n , a constraint which appears (from our tests) to be easily satisfiable in practice.

7.2 Discussion and Future Work

7.2.1 Problems Remaining from [71]

We first list the major problems left open from [71] which we were either unable to close, or which we did not attempt to resolve. The most pressing of these is the status of the search-to-decision proof for CLWE. While for certain primes we were able to obtain a full reduction for our nonassociative variant of CLWE, it is still unclear if such a reduction can be obtained in the associative setting; that is, whether the restriction imposed on the secret space is an artifact of proof technique, or necessary because of deeper structural reasons. As noted in [72], one might hope to obtain a direct-to-decision reduction in the style of [126], but it is not clear how to adapt the OHCP problem defined therein to the setting of CLWE, and indeed, the current author also struggled to adapt the results of that work to cyclic algebras.

A second major open line of research is to implement CLWE. This would benchmark the performance of CLWE against popular LWE-based schemes such as Kyber [135] and Frodo [10]. We also note here that while not a problem arising from the work of [71], a similarly useful project would be to implement CNTRU, to compare its performance to ModNTRU and ModFalcon.

7.2.2 Further Constructions

In Chapter 3 we reduced ideal lattice problems from one-sided ideals in Λ to search CLWE. We gave two constructions of such ideals: the first is an existence proof, and the constructed ideal offers no more security than the reduction from two-sided ideals, since solving SIVP in the intersection of that one-sided ideal with $\mathcal{O}_L$ allows one to solve SIVP in the one-sided ideal. The second construction does not suffer from this drawback, but instead does not have a closed form which is amenable to computation. It would be worthwhile to study one-sided ideals of maximal orders to better understand the security guarantee provided by our proof.

Two algebraic problems arose in Chapter 4. First, we devised a method to find unit-magnitude

fractional non-norm elements for finite extensions of cyclotomic fields. We used this to create a generalised form of CLWE, and reduced lattice problems to the search problem of this CLWE variant. However, we were unable to give a search-to-decision reduction for this variant. Such a result would help clarify the cryptographic behaviour of CLWE in a more general setting.

Secondly, similarly to the question posed by the restricted search-to-decision reduction of CLWE, NCLWE only has a full reduction for primes q which split into unramified primes of $\mathcal{O}_K$ which are inert in $\mathcal{O}_L$. It would be desirable to discover whether this can be extended to more general choices of prime q .

A further algebraic issue arose in the proof of the indistinguishability of public keys of CN-TRU. This proof could only be made to work for quaternion algebras, CDAs with $d = 2$. It is unknown whether a better strategy of proof would extend the result to algebras with $d > 2$, which could be a valuable result.

There are a number of algebraic avenues still untrod with regards to CLWE. Firstly, we note that one can interpret CLWE as a *skew polynomial* problem, similarly to how RLWE is a polynomial ring problem. One can consider the skew polynomial ring $\mathcal{O}_L[u, \theta]$, that is, polynomials in the variable u subject to $ux = \theta(x)u$ for all $x \in \mathcal{O}_L$, and show that $\Lambda \subset \mathcal{A} = (L/K, \theta, \gamma)$ is isomorphic to $\mathcal{O}_L[u, \theta]/(u^d - \gamma)$, and so inherits a number of properties from skew polynomial rings. One could define a skew polynomial variant in which the quotient by $(u^d - \gamma)$ is replaced by other irreducible skew polynomials. This may be an interesting avenue to explore for both constructions and cryptanalysis, and may open up connections to coding theory, in which skew polynomials are used extensively, e.g. [15]. Indeed the author has a manuscript under submission exploring this connection and its relation to the middle product for skew polynomials and to CLWE. A skew polynomial variant of NTRU is also plausible.

We also observe that [29] defined a LWE/LPN-style variant over function fields and demonstrated that a search-to-decision reduction is possible. Since one can define cyclic algebras over function fields [130, Chapter 19], we wonder whether exploring the use of these objects could yield fruitful cryptographic results.

One may also wish to adapt Learning with Rounding to the cyclic algebra setting, replacing the sampled error with a deterministically-generated error term.

7.2.3 Greater Functionality

Aside from algebraic constructions, cryptographic functionality is a high priority for future work on CLWE. The development of advanced primitives such as fully homomorphic encryption (FHE) from CLWE, in the style of say [35], or from CNTRU in the style of [31], could give interesting results. Likewise, as suggested in [72], more uncertain projects such as building multilinear maps from CLWE could (not totally implausibly) be possible, even if such ideas are optimistic.

The two most promising novel properties of the move from commutative to noncommutative algebras appear to be the presence of only one-sided ideals, and the existence of (nontrivial) commutator maps. We made use of one-sided ideals in Chapter 3, but not constructively. Perhaps the peculiar properties of one-sided ideals, such as their factorisation theory, could be used to obtain cryptographic functionality. Likewise, the ring commutator $[a, b] := ab - ba$ is always equal to 0 in a number field, but, fixing either a or b , gives an additive homomorphism from $\mathcal{A}$ to the elements of trace zero. The presence of such maps seems promising for an algebraist hoping to build novel cryptographic primitives with cyclic algebras. Moreover, these maps (when an input is fixed) are bilinear maps - perhaps, again optimistically, one might hope that these could be cryptographic bilinear maps, a highly useful object [120].

Of course, less exotic primitives could be studied than FHE or new commutator-based schemes. Signature schemes, KEMs, or key exchange from CLWE and CNTRU could be practical uses of these problems. We also note that the PKE scheme of NCLWE is less efficient than that of CLWE, since one is forced to compensate for the loss of associativity by some additive step in decrypting. The development of a PKE scheme without this extra step would be an improvement to NCLWE.

7.2.4 Cryptanalysis

Finally, cryptanalysis of CLWE, NCLWE, and CNTRU would be welcome. These are all still new problems, and their security has not been comprehensively or practically tested.

A promising avenue for this could be exploiting the lack of a full search-to-decision reduction

for CLWE. If these problems are not equivalent, conceivably one of them could be substantially easier than the other, at least for some large portion of the possible secrets.

We note that the hard problems underlying CLWE and NCLWE have also not been well-studied, but are rather algebraic variants of well-studied problems. Solutions to SVP in certain lattices are implied by solutions to the Hidden Subgroup Problem (HSP) for certain nonabelian groups. For instance, solving the Dihedral HSP would imply a quantum polynomial time algorithm for SVP [137]. Moreover these problems are directly linked to the security of LWE [36]. While we do not know the unit group of an arbitrary maximal order in a CDA, we do know the unit groups of certain quaternionic orders [168], and exploring algorithms for HSPs for these groups may lead to results relevant to CLWE.

Finally, adapting existing cryptanalytic attacks on RLWE or MLWE to the specific algebraic structure present in CLWE may lead to efficient attacks on CLWE. While the structure of CLWE is not obviously any more vulnerable to existing attacks than that of RLWE, it is possible that vulnerabilities exist. Tweaking existing attacks to take this structure into account seems the most likely way to develop attacks on CLWE-style problems.

7.2.5 Concluding Remarks

Lattices, and the computational problems they offer, are still relatively fresh to cryptography. They have realised cryptographic functionality few other platforms can provide, yet incremental and steady cryptanalytic progress has been and will continue to be made. In response to this progress, cryptographers must adapt, as they always have. Beyond the commutative structures commonly used by cryptographers for lattice-based cryptography lies a vast amount of noncommutative and exotic algebraic structures which remain cryptographically untapped. It is the hope of the author that this thesis suggests to the reader that connecting such abstract algebraic objects with provably secure cryptography is a profitable and stimulating endeavour.

Bibliography

- [1] M. Ajtai. “Generating Hard Instances of Lattice Problems”. In: *Electron. Colloquium Comput. Complex.* TR96 (1996). DOI: 10.1145/237814.237838.
- [2] M. Ajtai and C. Dwork. “A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence”. In: *STOC 97*. Association for Computing Machinery, 1997, 284–293. ISBN: 0897918886. DOI: 10.1145/258533.258604.
- [3] P-A. Fouque et. al. *Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU*. <https://falcon-sign.info/falcon.pdf>.
- [4] A. Al Badawi, B. Veeravalli, and K. M. M. Aung. “Efficient Polynomial Multiplication via Modified Discrete Galois Transform and Negacyclic Convolution”. In: *FICC 2018*. Ed. by K. Arai, S. Kapoor, and R. Bhatia. Vol. 886. AICC. Springer International Publishing, 2019, pp. 666–682. ISBN: 978-3-030-03402-3.
- [5] A. A. Albert. “On Nonassociative Division Algebras”. In: *Transactions of the American Mathematical Society* 72.2 (1952), pp. 296–309. URL: <http://www.jstor.org/stable/1990756>.
- [6] A.A. Albert. *Structure of Algebras*. AMS colloquium publications v. 24. American Mathematical Society, 1939. ISBN: 9780821810248.
- [7] M. Albrecht, S. Bai, and L. Ducas. “A Subfield Lattice Attack on Overstretched NTRU Assumptions”. In: *CRYPTO 2016*. Vol. 9814. LNCS. Springer Berlin Heidelberg, 2016, pp. 153–178.

- [8] M. Albrecht and A. Deo. “Large Modulus Ring-LWE $\geq$ Module-LWE”. In: *ASIACRYPT 2017*. Ed. by T. Takagi and T. Peyrin. Vol. 10624. LNCS. Springer International Publishing, 2017, pp. 267–296. ISBN: 9783319706948.
- [9] M. Albrecht, R. Player, and S. Scott. “On the concrete hardness of Learning with Errors”. In: *Journal of Mathematical Cryptology* 9.3 (2015), pp. 169–203. DOI: doi:10.1515/jmc-2015-0016.
- [10] E. Alkim, J. W. Bos, L. Ducas, P. Longa, I. Mironov, M. Naehrig, V. Nikolaenko, C. Peikert, A. Raghunathan, and D. Stebila. *FrodoKEM, Round 3 Specification*. 2021. URL: <https://frodokem.org/files/FrodoKEM-specification-20210604.pdf>.
- [11] J. Alman and V. V. Williams. “A Refined Laser Method and Faster Matrix Multiplication”. In: *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pp. 522–539. DOI: 10.1137/1.9781611976465.32.
- [12] D. Apon, D. Dachman-Soled, H. Gong, and J. Katz. “Constant-Round Group Key Exchange from the Ring-LWE Assumption”. In: *PQCrypto 2019*. Ed. by J. Ding and R. Steinwandt. Vol. 11505. LNCS. Springer International Publishing, 2019, pp. 189–205. ISBN: 978-3-030-25510-7.
- [13] B. Applebaum, D. Cash, C. Peikert, and A. Sahai. “Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems”. In: *CRYPTO 2009*. Ed. by S. Halevi. Vol. 5677. LNCS. Springer Berlin Heidelberg, 2009, pp. 595–618. ISBN: 9783642033568. DOI: 10.1007/978-3-642-03356-8_35.
- [14] R. B. Ash. *A Course In Algebraic Number Theory*. 2003. URL: <https://faculty.math.illinois.edu/~r-ash/Ant/AntChapter8.pdf>.
- [15] D. Augot, P. Loidreau, and G. Robert. “Generalized Gabidulin Codes over Fields of Any Characteristic”. In: *Des. Codes Cryptography* 86.8 (2018), 1807–1848. DOI: 10.1007/s10623-017-0425-6.
- [16] K. Bagheri, M-R. Sadeghi, and D. Panario. “A Non-Commutative Cryptosystem Based on Quaternion Algebras”. In: *Designs, Codes and Cryptography* 86.10 (2018), 2345–2377. DOI: 10.1007/s10623-017-0451-4.

- [17] W. Banaszczyk. “New bounds in some transference theorems in the geometry of numbers”. In: *Mathematische Annalen* 296 (1993), pp. 625–635.
- [18] A. Banerjee, C. Peikert, and A. Rosen. “Pseudorandom Functions and Lattices”. In: *EUROCRYPT 2012*. Ed. by D. Pointcheval and T. Johansson. Vol. 7237. LNCS. Springer Berlin Heidelberg, 2012, pp. 719–737.
- [19] W. Banks and I. Shparlinski. “A Variant of NTRU with Non-invertible Polynomials”. In: *INDOCRYPT 2002*. Vol. 2551. LNCS. Nov. 2002. DOI: 10.1007/3-540-36231-2_6.
- [20] A. Barreal, C. Corrales, and C. Hollanti. “Natural orders for asymmetric space–time coding: minimizing the discriminant”. In: *AAECC* 29 (Nov. 2018). DOI: 10.1007/s00200-017-0348-5.
- [21] E. Bayer-Fluckiger, J.-P. Cerri, and J. Chaubert. “Euclidean Minima and Central Division Algebras”. In: *International Journal of Number Theory* 05.07 (2009), pp. 1155–1168. DOI: 10.1142/S1793042109002614.
- [22] Deutsche Akademie der Wissenschaften zu Berlin. *Abhandlungen der Königlichen Akademie der Wissenschaften in Berlin*. Abhandlungen der Königlich Preussischen Akademie der Wissenschaften. Realschul-Buchhandlung, 1839.
- [23] O. Bernard, A. Lesavourey, T.-H. Nguyen, and A. Roux-Langlois. “Log- $\mathcal{S}$ -unit Lattices Using Explicit Stickelberger Generators to Solve Approx Ideal-SVP”. In: *ASIACRYPT 2022*. Ed. by S. Agrawal and D. Lin. Vol. 13793. LNCS. Springer Nature Switzerland, 2022, pp. 677–708. ISBN: 978-3-031-22969-5.
- [24] O. Bernard and A. Roux-Langlois. “Twisted-PHS: Using the Product Formula to Solve Approx-SVP in Ideal Lattices”. In: *ASIACRYPT 2020*. Ed. by S. Moriai and H. Wang. Vol. 12492. LNCS. Springer International Publishing, 2020, pp. 349–380. ISBN: 978-3-030-64834-3.
- [25] D. Bernstein, C. Chuengsatiansup, T. Lange, and C. van Vredendaal. “NTRU Prime: Reducing Attack Surface at Low Cost”. In: *SAC 2017*. Ed. by C. Adams and J. Camenisch. Vol. 10719. LNCS. Springer International, pp. 235–260. ISBN: 9783319725659.

- [26] D. J. Bernstein, N. Heninger, P. Lou, and L. Valenta. “Post-quantum RSA”. In: *PQCrypto 2017*. Ed. by T. Lange and T. Takagi. Vol. 10346. LNCS. Springer International Publishing, 2017, pp. 311–329. ISBN: 978-3-319-59879-6.
- [27] M. Bolboceanu, Z. Brakerski, R. Perlman, and D. Sharma. “Order-LWE and the Hardness of Ring-LWE with Entropic Secrets”. In: *ASIACRYPT 2019*. Ed. by S. Galbraith and S. Moriai. Vol. 11922. LNCS. Springer International Publishing, 2019, pp. 91–120.
- [28] M. Bolboceanu, Z. Brakerski, and D. Sharma. *On Algebraic Embedding for Unstructured Lattices*. Cryptology ePrint Archive, Report 2021/053. <https://eprint.iacr.org/2021/053>. 2021.
- [29] M. Bombar, A. Couvreur, and T. Debris-Alazard. “On Codes and Learning with Errors over Function Fields”. In: *CRYPTO 2022*. Ed. by Y. Dodis and T. Shrimpton. Vol. 13508. LNCS. Springer Nature Switzerland, 2022, pp. 513–540. ISBN: 978-3-031-15979-4.
- [30] X. Bonnetain, M. Naya-Plasencia, and A. Schrottenloher. “Quantum Security Analysis of AES”. In: *IACR Transactions on Symmetric Cryptology 2019.2* (2019), 55–93. DOI: 10.13154/tosc.v2019.i2.55-93.
- [31] C. Bonte, I. Iliashenko, J. Park, H. V. L. Pereira, and N. P. Smart. “FINAL: Faster FHE Instantiated with NTRU and LWE”. In: *ASIACRYPT 2022*. Ed. by S. Agrawal and D. Lin. Vol. 13792. LNCS. Springer Nature Switzerland, 2022, pp. 188–215. ISBN: 978-3-031-22966-4.
- [32] C. Bootland, W. Castryck, and F. Vercauteren. “On the security of the multivariate ring learning with errors problem”. In: *ANTS-XIV, Fourteenth Algorithmic Number Theory Symposium, Proceedings*. Auckland, New Zealand: MSP, 2020.
- [33] J. W. Bos, K. Lauter, J. Loftus, and M. Naehrig. “Improved Security for a Ring-Based Fully Homomorphic Encryption Scheme”. In: *IMACC 2013*. Ed. by M. Stam. Vol. 8308. LNCS. Springer Berlin Heidelberg, 2013, pp. 45–64. ISBN: 978-3-642-45239-0.
- [34] K. Boudgoust, C. Jeudy, A. Roux-Langlois, and A. Wen. “Entropic Hardness of Module-LWE from Module-NTRU”. In: *INDOCRYPT 2022*. Ed. by T. Isobe and S. Sarkar. Vol. 13774. LNCS. Springer International Publishing, 2022, pp. 78–99. ISBN: 9783031229121.

- [35] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. “(Leveled) Fully Homomorphic Encryption without Bootstrapping”. In: *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*. ITCS '12. Association for Computing Machinery, 2012, 309–325. ISBN: 9781450311151. DOI: 10.1145/2090236.2090262.
- [36] Z. Brakerski, E. Kirshanova, D. Stehlé, and W. Wen. “Learning with Errors and Extrapolated Dihedral Cosets”. In: *PKC 2018*. Ed. by M. Abdalla and R. Dahab. Vol. 10770. LNCS. Springer International Publishing, 2018, pp. 702–727. ISBN: 978-3-319-76581-5.
- [37] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehlé. “Classical Hardness of Learning with Errors”. In: *Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing*. STOC '13. Association for Computing Machinery, 2013, 575–584. ISBN: 9781450320290. DOI: 10.1145/2488608.2488680.
- [38] Z. Brakerski and V. Vaikuntanathan. “Efficient Fully Homomorphic Encryption from (Standard) LWE”. In: *FOCS 2011*. 2011, pp. 97–106. DOI: 10.1109/FOCS.2011.12.
- [39] C. Brown and S. Pumplün. “How a nonassociative algebra reflects the properties of a skew polynomial”. In: *Glasgow Mathematical Journal* 63.1 (2021), 6–26. DOI: 10.1017/S0017089519000478.
- [40] C. Brown and S. Pumplün. “Nonassociative cyclic extensions of fields and central simple algebras”. In: *Journal of Pure and Applied Algebra* 223.6 (2019), pp. 2401–2412. ISSN: 0022-4049. DOI: <https://doi.org/10.1016/j.jpaa.2018.08.018>.
- [41] J. Hoffstein A. Hülsing J. Rijneveld J. M. Schanck P. Schwabe W. Whyte Z. Zhang C. Chen O. Danba. *NTRU: Algorithm Specifications And Supporting Documentation*. <https://ntru.org/f/ntru-20190330.pdf>. 2019.
- [42] D. Cabarcas, P. Weiden, and J. Buchmann. “On the Efficiency of Provably Secure NTRU”. In: *Post-Quantum Cryptography*. Ed. by M. Mosca. Springer International Publishing, 2014, pp. 22–39. ISBN: 9783319116594.
- [43] X. Caruso and J. Le Borgne. “Fast Multiplication for Skew Polynomials”. In: *ISSAC '17*. Association for Computing Machinery, 2017, 77–84. ISBN: 9781450350648. DOI: 10.1145/3087604.3087617.

- [44] H. Chen, K. Lauter, and K. E. Stange. “Attacks on the Search RLWE Problem with Small Errors”. In: *SIAM Journal on Applied Algebra and Geometry* 1.1 (2017), pp. 665–682. DOI: 10.1137/16M1096566.
- [45] H. Chen, K. Lauter, and K. E. Stange. “Security Considerations for Galois Non-dual RLWE Families”. In: *SAC 2016*. Ed. by H. Avanzi R. & Heys. Vol. 10532. LNCS. Springer International Publishing, 2017, pp. 443–462. ISBN: 9783319694535.
- [46] Y. Chen, N. Genise, and P. Mukherjee. “Approximate Trapdoors for Lattices and Smaller Hash-and-Sign Signatures”. In: *ASIACRYPT 2019*. Ed. by S. D. Galbraith and S. Moriai. Vol. 11923. LNCS. Springer International Publishing, 2019, pp. 3–32. ISBN: 978-3-030-34618-8.
- [47] Q. Cheng, J. Zhang, and J. Zhuang. “LWE from non-commutative group rings”. In: *Designs, Codes and Cryptography* 90.1 (2022), pp. 239–263. DOI: 10.1007/s10623-021-00973-6.
- [48] J. H. Cheon, J. Jeong, and C. Lee. “An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without a low-level encoding of zero”. In: *LMS Journal of Computation and Mathematics* 19.A (2016), 255–266. DOI: 10.1112/S1461157016000371.
- [49] J. H. Cheon, D. Kim, T. Kim, and Y. Son. *A New Trapdoor over Module-NTRU Lattice and its Application to ID-based Encryption*. Cryptology ePrint Archive, Report 2019/1468. <https://eprint.iacr.org/2019/1468>. 2019.
- [50] C. Chuengsatiansup, T. Prest, D. Stehlé, A. Wallet, and K. Xagawa. “ModFalcon: Compact Signatures Based On Module-NTRU Lattices”. In: *ASIA CCS ’20*. Assoc. for Computing Machinery, 853–866. ISBN: 9781450367509. DOI: 10.1145/3320269.3384758.
- [51] P. Clark. *Introduction to Nonassociative Algebras*. URL: <http://math.uga.edu/~pete/nonassociativealgebra.pdf>.
- [52] M. Coglianese and B.-M. Goi. “MaTRU: A New NTRU-Based Cryptosystem”. In: *INDOCRYPT 2005*. Ed. by S. Maitra, C. E. Veni Madhavan, and R. Venkatesan. Vol. 3797. LNCS. Springer Berlin Heidelberg, 2005, pp. 232–243. ISBN: 978-3-540-32278-8.

- [53] H. Cohen. *Advanced Topics in Computational Number Theory*. Graduate Texts in Mathematics. Springer New York, 1999. ISBN: 9780387987279.
- [54] K. Conrad. *The Conductor Ideal of an Order*. 2018. URL: <https://kconrad.math.uconn.edu/blurbs/gradnumthy/conductor.pdf>.
- [55] D. Coppersmith and A. Shamir. “Lattice Attacks on NTRU”. In: *EUROCRYPT ’97*. Vol. 1233. LNCS. Springer Berlin Heidelberg, 1997, pp. 52–61.
- [56] R. Cramer, L. Ducas, and B. Wesolowski. “Short Stickelberger Class Relations and Application to Ideal-SVP”. In: *EUROCRYPT 2017*. Ed. by J.-S. Coron and J. B. Nielsen. Vol. 10210. LNCS. Springer International Publishing, 2017, pp. 324–348. ISBN: 978-3-319-56620-7.
- [57] L. E. Dickson. “Linear algebras with associativity not assumed”. In: *Duke Mathematical Journal* 1.2 (1935), pp. 113–125. DOI: 10.1215/S0012-7094-35-00112-0.
- [58] P. G. L. Dirichlet. *There are infinitely many prime numbers in all arithmetic progressions with first term and difference coprime*. 2014. URL: <https://arxiv.org/abs/0808.1408>.
- [59] L. Ducas, V. Lyubashevsky, and T. Prest. “Efficient Identity-Based Encryption over NTRU Lattices”. In: *ASIACRYPT 2014*. Ed. by P. Sarkar and T. Iwata. Vol. 8874. LNCS. Springer Berlin Heidelberg, 2014, pp. 22–41. ISBN: 978-3-662-45608-8.
- [60] J.-G. Dumas and J.-B. Orfila. “Generating S-Boxes from Semi-fields Pseudo-extensions”. In: *CoRR* abs/1411.2503 (2014). URL: <http://arxiv.org/abs/1411.2503>.
- [61] D. Eisenbud and J.C Robson. “Modules over Dedekind prime rings”. In: *Journal of Algebra* 16.1 (1970), pp. 67–85. ISSN: 0021-8693. DOI: 10.1016/0021-8693(70)90041-4.
- [62] Y. Elias, K. E. Lauter, E. Ozman, and K. E. Stange. “Provably Weak Instances of Ring-LWE”. In: *CRYPTO 2015*. Ed. by R. Gennaro and M. Robshaw. Vol. 9215. LNCS. Springer Berlin Heidelberg, 2015, pp. 63–92. ISBN: 978-3-662-47989-6.
- [63] J. Felderhoff, A. Pellet-Mary, and D. Stehlé. “On Module Unique-SVP and NTRU”. In: *ASIACRYPT 2022*. Ed. by S. Agrawal and D. Lin. Vol. 13793. LNCS. Springer Nature Switzerland, 2022, pp. 709–740. ISBN: 9783031229695.

- [64] I.B. Fesenko and S.V. Vostokov. *Local Fields and Their Extensions*. Translations of Mathematical Monographs. American Mathematical Society, 2002. ISBN: 978-0821832592.
- [65] C. Frei, D. Loughran, and R. Newton. “Number fields with prescribed norms”. In: *Commentarii Mathematici Helvetici* 97 (Apr. 2022), pp. 133–181. DOI: 10.4171/CMH/528.
- [66] S. Garg, C. Gentry, and S. Halevi. “Candidate Multilinear Maps from Ideal Lattices”. In: *EUROCRYPT 2013*. Ed. by T. Johansson and P.Q. Nguyen. Vol. 7881. LNCS. 2012. DOI: 10.1007/978-3-642-38348-9_1.
- [67] G. Gavin and S. Bonnevey. “Fractional LWE: A Nonlinear Variant of LWE”. In: *CANS 2019*. Vol. 11829. LNCS. Springer International Publishing, 2019, pp. 360–371.
- [68] C. Gentry, C. Peikert, and V. Vaikuntanathan. “Trapdoors for Hard Lattices and New Cryptographic Constructions”. In: *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*. STOC ’08. Association for Computing Machinery, 2008, 197–206. ISBN: 9781605580470. DOI: 10.1145/1374376.1374407.
- [69] C. Gentry and M. Szydło. “Cryptanalysis of the Revised NTRU Signature Scheme”. In: *EUROCRYPT 2002*. Ed. by L. R. Knudsen. Vol. 2332. LNCS. Springer Berlin Heidelberg, 2002, pp. 299–320. ISBN: 978-3-540-46035-0.
- [70] K. R. Goodearl and R. B. Warfield Jr. *An Introduction to Noncommutative Noetherian Rings*. 2nd ed. London Mathematical Society Student Texts. Cambridge University Press, 2004. DOI: 10.1017/CB09780511841699.
- [71] C. Grover, A. Mendelsohn, C. Ling, and R. Vehkalahti. “Non-commutative Ring Learning with Errors from Cyclic Algebras”. In: *Journal of Cryptology* 35.3 (2022), p. 22. DOI: 10.1007/s00145-022-09430-6.
- [72] Charles Grover. “LWE over cyclic algebras: a novel structure for lattice cryptography”. PhD thesis. Imperial College London, 2019. URL: <https://spiral.imperial.ac.uk/handle/10044/1/97982>.
- [73] L. K. Grover. “A Fast Quantum Mechanical Algorithm for Database Search”. In: *STOC 96*. Association for Computing Machinery, 1996, 212–219. ISBN: 0897917855. DOI: 10.1145/237814.237866.

- [74] H. Hasse. *Beweis eines Satzes und Widerlegung einer Vermutung über das allgemeine Normenrestsymbol*. German. 1931, pp. 64–69. URL: https://www.digizeitschriften.de/id/252457811_1931|log1.
- [75] J. Hoffstein, J. Pipher, J. M. Schanck, J. H. Silverman, and W. Whyte. “Transcript Secure Signatures Based on Modular Lattices”. In: *PQCRYPTO 2014*. Ed. by M. Mosca. Vol. 8772. LNCS. Springer International Publishing, 2014, pp. 142–159. ISBN: 978-3-319-11659-4.
- [76] J. Hoffstein, J. Pipher, J. M. Schanck, J. H. Silverman, W. Whyte, and Z. Zhang. “Choosing Parameters for NTRUEncrypt”. In: *CT-RSA '17*. Ed. by H. Handschuh. Vol. 10159. LNCS. Springer International Publishing, 2017, pp. 3–18. ISBN: 9783319521534.
- [77] J. Hoffstein, J. Pipher, and J. Silverman. “NTRU: A Ring-Based Public Key Cryptosystem”. In: *ANTS III*. Vol. 1423. LNCS. Springer-Verlag, 1998, 267–288. ISBN: 3540646574.
- [78] C. Hollanti, J. Lahtonen, and H.-F. Lu. “Maximal Orders in the Design of Dense Space-Time Lattice Codes”. In: *IEEE Transactions on Information Theory* 54.10 (2008), pp. 4493–4510. DOI: 10.1109/TIT.2008.928998.
- [79] P. Hough, C. Sandsbråten, and T. Silde. *Concrete NTRU Security and Advances in Practical Lattice-Based Electronic Voting*. Cryptology ePrint Archive, Paper 2023/933. 2023. URL: <https://eprint.iacr.org/2023/933>.
- [80] N. Howgrave-Graham. “A Hybrid Lattice-Reduction and Meet-in-the-Middle Attack Against NTRU”. In: *CRYPTO 2007*. Ed. by A. Menezes. Vol. 4622. LNCS. Springer Berlin Heidelberg, pp. 150–169. ISBN: 9783540741435.
- [81] N. Howgrave-Graham, P. Q. Nguyen, D. Pointcheval, J. Proos, J. H. Silverman, A. Singer, and W. Whyte. “The Impact of Decryption Failures on the Security of NTRU Encryption”. In: *CRYPTO 2003*. Ed. by D. Boneh. Vol. 2729. LNCS. Springer Heidelberg, pp. 226–246. ISBN: 9783540451464.
- [82] N. Howgrave-Graham, J. Silverman, and W. Whyte. *A Meet-In-The-Middle Attack on an NTRU Private Key*. NTRU Cryptosystems, July 2003.

- [83] N. Howgrave-Graham, J. H. Silverman, and W. Whyte. “Choosing Parameter Sets for NTRUEncrypt with NAEP and SVES-3”. In: *CT-RSA 2005*. Ed. by A. Menezes. Springer Heidelberg, pp. 118–135. ISBN: 9783540305743.
- [84] Y. Hu and H. Jia. “Cryptanalysis of GGH Map”. In: *EUROCRYPT 2016*. Vol. 9665. LNCS. Springer Berlin Heidelberg, 2016, pp. 537–565.
- [85] I. Hussain, A. Anees, and T. Almaadeed. “A novel encryption algorithm using multiple semifield S-boxes based on permutation of symmetric group”. In: *Computational and Applied Mathematics* 42 (Feb. 2023). DOI: 10.1007/s40314-023-02208-x.
- [86] G. Ivanyos and L. Rónyai. “Finding Maximal Orders in Semisimple Algebras over $\mathbb{Q}$ ”. In: *Comput. Complex.* 3.3 (1993), 245–261. ISSN: 1016-3328. DOI: 10.1007/BF01271370.
- [87] G. Janusz. *Algebraic Number Fields*. American Mathematical Soc., 1995. ISBN: 9780821872437. URL: https://books.google.co.uk/books?id=RT5R_29X69wC.
- [88] K. Jarvis. “NTRU over the Eisenstein Integers”. MA thesis. U. of Ottawa, 2011.
- [89] E. Jespers. “Structure of group rings and the group of units of integral group rings: an invitation”. In: *Indian Journal of Pure and Applied Mathematics* (Sept. 2021). DOI: 10.1007/s13226-021-00179-5.
- [90] A. H. Karbasi and R. Atani. “ILTRU: An NTRU-Like Public Key Cryptosystem Over Ideal Lattices”. In: *Cryptol. ePrint Arch.* (2015), p. 549.
- [91] J. Katz and Y. Lindell. *Introduction to Modern Cryptography, Second Edition*. Chapman & Hall/CRC Cryptography and Network Security Series. Taylor & Francis, 2014. ISBN: 9781466570269. URL: <https://books.google.co.uk/books?id=0WZYBQAAQBAJ>.
- [92] M. Kimball. *Quaternion Algebras in Number Theory*. 2017. URL: <http://www2.math.ou.edu/~kmartin/quaint/>.
- [93] P. Kirchner. “Algorithms on Ideal over Complex Multiplication order”. In: *CoRR* (Feb. 2016). URL: <http://arxiv.org/abs/1602.09037>.
- [94] R. Kouzmenko. “Generalizations of the NTRU cryptosystem”. PhD thesis. 2005.

- [95] J. Lahtonen, N. Markin, and G. McGuire. “Construction of Multiblock Space–Time Codes From Division Algebras With Roots of Unity as Nonnorm Elements”. In: *IEEE Transactions on Information Theory* 54.11 (2008), pp. 5231–5235.
- [96] T.Y. Lam. *Lectures on Modules and Rings*. Graduate Texts in Mathematics. Springer New York, 1999. ISBN: 9780387984285.
- [97] A. Langlois and D. Stehlé. “Worst-case to average-case reductions for module lattices”. In: *Designs, Codes and Cryptography* 75.3 (2015), pp. 565–599. ISSN: 1573-7586. DOI: 10.1007/s10623-014-9938-4.
- [98] H. J. Lee and W. C. Waterhouse. “Maximal orders in nonassociative quaternion algebras”. In: *Journal of Algebra* 146.2 (1992), pp. 441–453. ISSN: 0021-8693. DOI: 10.1016/0021-8693(92)90077-Y.
- [99] H. W. Lenstra and A. Silverberg. “Revisiting the Gentry-Szydlo Algorithm”. In: *CRYPTO 2014*. Vol. 8616. LNCS. Aug. 2014. ISBN: 9783662443705. DOI: 10.1007/978-3-662-44371-2_16.
- [100] H. W. Lenstra and A. Silverberg. “Testing Isomorphism of Lattices over CM-Orders”. In: *SIAM Journal on Computing* 48.4 (2019), pp. 1300–1334. DOI: 10.1137/17M115390X.
- [101] P. Lundström and J. Öinert. “Simple Graded Rings, Non-Associative Crossed Products and Cayley-Dickson Doublings”. In: *Journal of Algebra and Its Applications* 19 (Oct. 2016). DOI: 10.1142/S021949882050231X.
- [102] V. Lyubashevsky, C. Peikert, and O. Regev. “On Ideal Lattices and Learning with Errors over Rings”. In: *EUROCRYPT 2010*. Ed. by H. Gilbert. Vol. 6110. LNCS. Springer Berlin Heidelberg, 2010, pp. 1–23. DOI: 10.1007/978-3-642-13190-5_1.
- [103] E. Malekian and A. Zakerolhosseini. “A non-associative lattice-based public key cryptosystem”. In: *Security and Communication Networks* 5.2 (2012), pp. 145–163. DOI: <https://doi.org/10.1002/sec.297>.
- [104] E. Malekian, A. Zakerolhosseini, and A. Mashatan. “QTRU: quaternionic version of the NTRU public-key cryptosystems”. In: *The ISC International Journal of Information Security* 3.1 (2011), pp. 29–42. DOI: 10.22042/isecure.2015.3.1.3.

- [105] D. Marcus. *Number Fields*. Universitext. Springer-Verlag, 1977. ISBN: 9783319902326.
- [106] J.C. McConnell, J.C. Robson, and L.W. Small. *Noncommutative Noetherian Rings*. Graduate studies in mathematics. American Mathematical Society, 2001. ISBN: 9780821821695.
- [107] A. B. Meli. *Cyclotomic Extensions and Quadratic Reciprocity*. 2013. URL: <http://math.uchicago.edu/~may/REU2013/REUPapers/Meli.pdf>.
- [108] D. Micciancio and O. Regev. “Worst-case to average-case reductions based on Gaussian measures”. In: *45th Annual IEEE Symposium on Foundations of Computer Science*. 2004, pp. 372–381. DOI: 10.1109/FOCS.2004.72.
- [109] S. Murphy and R. Player. “ δ -subgaussian Random Variables in Cryptography”. In: *ACISP 2019*. Ed. by J. Jang-Jaccard and F. Guo. Vol. 11547. LNCS. Springer International Publishing, 2019, pp. 251–268. ISBN: 9783030215484.
- [110] S. Murphy and R. Player. “Discretisation and Product Distributions in Ring-LWE”. In: *J. of Mathematical Cryptology* 15.1 (2021), pp. 45–59. DOI: doi:10.1515/jmc-2020-0073.
- [111] W. Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers*. Springer Monographs in Mathematics. Springer Berlin Heidelberg, 2004. ISBN: 9783540219026.
- [112] J. Neukirch. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2010. ISBN: 9783642084737.
- [113] M. Nevins and K. Jarvis. “ETRU: NTRU over the Eisenstein Integers”. In: *Designs, Codes and Cryptography* 74 (2013), 219–242. DOI: 10.1007/s10623-013-9850-3.
- [114] M. Nevins, C. Karimianpour, and A. Miri. “NTRU in Rings Beyond $\mathbb{Z}$ ”. In: *Designs, Codes and Cryptography* 56 (2009), 65–78. DOI: 10.1007/s10623-009-9342-7.
- [115] BBC News. *What is the quantum apocalypse and should we be scared?* Accessed July 4th, 2023. <https://www.bbc.co.uk/news/technology-60144498>. 2022.
- [116] NIST. *Post-Quantum Cryptography: Call for Proposals*. Accessed July 4th, 2023. <https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/Call-for-Proposals>. 2017.

- [117] NIST. *Post-Quantum Cryptography: Round 3 Submissions*. <https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions>. 2021.
- [118] F. Oggier and G. Berhuy. *An Introduction to Central Simple Algebras and Their Applications to Wireless Communication*. AMS Mathematical Surveys and Monographs. AMS, 2013. ISBN: 978-0-8218-4937-8.
- [119] F. Oggier and B. A. Sethuraman. “Quotients of orders in cyclic algebras and space-time codes”. In: *Advances in Mathematics of Communications* 7.4 (2013), pp. 441–461.
- [120] T. Okamoto. “Cryptography Based on Bilinear Maps”. In: *AAECC 06*. Ed. by M. P. C. Fossorier, H. Imai, S. Lin, and A. Poli. Vol. 3857. LNCS. Springer Berlin Heidelberg, 2006, pp. 35–50. ISBN: 978-3-540-31424-0.
- [121] B. A. Sethuraman P. Elia and P. Vijay Kumar. “Perfect Space-Time Codes for Any Number of Antennas”. In: *IEEE Transactions of Information Theory* 53 (2007), pp. 3853–3868.
- [122] J. Ohler P. Gaborit and P. Solé. *CTRU, a polynomial analogue of NTRU*. Nov. 2002. URL: <https://hal.inria.fr/inria-00071964>.
- [123] A. Pedrouzo-Ulloa, J. R. Troncoso-Pastoriza, and F. Pérez-González. “On Ideal Lattices over the Tensor Product of Number Fields and Ring Learning with Errors over Multivariate Rings”. In: *CoRR* abs/1607.05244 (2016). URL: <http://arxiv.org/abs/1607.05244>.
- [124] C. Peikert. “How Not to Instantiate Ring-LWE”. In: *SCN 2016*. Vol. 9841. LNCS. Springer-Verlag, 2016, 411–430. DOI: 10.1007/978-3-319-44618-9_22.
- [125] C. Peikert. “Limits on the Hardness of Lattice Problems in ℓ_p Norms”. In: *CCC 07*. 2007, pp. 333–346. DOI: 10.1109/CCC.2007.12.
- [126] C. Peikert, O. Regev, and N. Stephens-Davidowitz. “Pseudorandomness of Ring-LWE for Any Ring and Modulus”. In: *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*. STOC 2017. Association for Computing Machinery, 2017, 461–473. ISBN: 9781450345286. DOI: 10.1145/3055399.3055489.

- [127] C. Peikert and A. Rosen. “Lattices That Admit Logarithmic Worst-Case to Average-Case Connection Factors”. In: *STOC '07*. Association for Computing Machinery, 2007, 478–487. ISBN: 9781595936318. DOI: 10.1145/1250790.1250860.
- [128] A. Pellet-Mary and D. Stehlé. “On the Hardness of the NTRU Problem”. In: *ASIACRYPT 2021*. Ed. by M. Tibouchi and H. Wang. Vol. 13090. LNCS. Springer, pp. 3–35. ISBN: 9783030920623.
- [129] J.-C. Petit. “Sur certains quasi-corps généralisant un type d’anneau-quotient”. In: *Séminaire Dubreil. Algèbre et théorie des nombres* 20.2 (1967), pp. 1–18. URL: http://www.numdam.org/item/SD_1966-1967__20_2_A2_0.
- [130] R. S. Pierce. *Associative Algebras*. Graduate Texts in Mathematics. Springer, 1982. ISBN: 978-1-4757-0165-4.
- [131] S. Pumplün. “Quotients of orders in algebras obtained from skew polynomials with applications to coding theory”. In: *Communications in Algebra* 46.11 (2018), pp. 5053–5072. DOI: 10.1080/00927872.2018.1461882.
- [132] S. Pumplün and T. Unger. “Space-time block codes from nonassociative division algebras”. In: *Advances in Mathematics of Communications* 5.3 (2011), pp. 449–471. ISSN: 1930-5346. DOI: 10.3934/amc.2011.5.449.
- [133] A. Karbasi R. Atani S. Atani. “A Provably Secure Variant of ETRU Based on Extended Ideal Lattices Over Direct Product of Dedekind Domains”. In: *JCS* 5 (2018), pp. 13–34. DOI: 10.22108/jcs.2018.106856.0.
- [134] A. Karbasi R. Atani S. Atani. “NETRU: A Noncommutative and Secure Variant of CTRU Cryptosystem”. In: *ISC Int. J. Inf. Sec.* 10 (2018), pp. 45–53.
- [135] L. Ducas E. Kiltz T. Lepoint V. Lyubashevsky J. M. Schanck P. Schwabe G. Seiler R. Avanzi J. Bos and D. Stehlé. *CRYSTALS-Kyber*. CRYSTALS Cryptographic Suite for Algebraic Lattices. <https://pq-crystals.org/kyber/data/kyber-specification-round3-20210804.pdf>. 2021.
- [136] O. Regev. “On lattices, learning with errors, random linear codes, and cryptography”. In: *Journal of the ACM* 56 (2009). DOI: 10.1145/1568318.

- [137] O. Regev. “Quantum Computation and Lattice Problems”. In: *SIAM Journal on Computing* 33.3 (2004), pp. 738–760. DOI: 10.1137/S0097539703440678.
- [138] Oded Regev. “On Lattices, Learning with Errors, Random Linear Codes, and Cryptography”. In: *J. ACM* 56.6 (Sept. 2009). DOI: 10.1145/1568318.1568324.
- [139] I. Reiner. *Maximal Orders*. London Mathematical Society Monographs. Oxford University Press, 2003. ISBN: 9780198526735.
- [140] M. Roşca, A. Sakzad, D. Stehlé, and R. Steinfeld. “Middle-Product Learning with Errors”. In: *CRYPTO 2017*. Ed. by J. Katz and H. Shacham. Vol. 10403. LNCS. Springer International Publishing, 2017, pp. 283–297.
- [141] M. Rosca, D. Stehlé, and A. Wallet. “On the Ring-LWE and Polynomial-LWE Problems”. In: *EUROCRYPT 2018*. Vol. 10820. LNCS. Springer International Publishing, 2018, pp. 146–173.
- [142] I. F. Rúa and E. F. Combarro. “Cryptographic Uncertainty: Some Experiments on Finite Semifield Based Substitution Boxes”. In: *The Mathematics of the Uncertain: A Tribute to Pedro Gil*. Ed. by E. Gil, E. Gil, J. Gil, and M. Á. Gil. Springer International Publishing, 2018, pp. 485–492. ISBN: 9783319738482. DOI: 10.1007/978-3-319-73848-2_45.
- [143] R. Schafer. *An Introduction to Nonassociative Algebras*. Benediction Classics, 2010. ISBN: 1849025908. URL: <https://archive.org/details/anintroductionto25156gut>.
- [144] J.P. Serre. *Local Fields*. Trans. by M.J. Greenberg. Graduate Texts in Mathematics. Springer New York, 2013. ISBN: 9781475756739.
- [145] B.A. Sethuraman, B.S. Rajan, and V. Shashidhar. “Full-diversity, high-rate space-time block codes from division algebras”. In: *IEEE Trans. Inf. Theory* 49.10 (2003), pp. 2596–2616. DOI: 10.1109/TIT.2003.817831.
- [146] C. Shannon. *A Mathematical Theory of Cryptography*. Bell Laboratories, Sept. 1945.
- [147] P. W. Shor. “Algorithms for quantum computation: discrete logarithms and factoring”. In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, pp. 124–134.

- [148] S. Singh and S. Padhye. “Generalisations of NTRU cryptosystem”. In: *SCN* 9.18 (2016), pp. 6315–6334. DOI: <https://doi.org/10.1002/sec.1693>.
- [149] K. P. Srinath and B. S. Rajan. “Fast-Decodable MIDO Codes With Large Coding Gain”. In: *IEEE Transactions on Information Theory* 60.2 (2014), pp. 992–1007. DOI: 10.1109/TIT.2013.2292513.
- [150] K. E. Stange. “Algebraic Aspects of Solving Ring-LWE, Including Ring-Based Improvements in the Blum–Kalai–Wasserman Algorithm”. In: *SIAM Journal on Applied Algebra and Geometry* 5.2 (2021), pp. 366–387. DOI: 10.1137/19M1280442.
- [151] A. Steele. “Nonassociative cyclic algebras”. In: *Israel Journal of Mathematics* 200 (June 2014). DOI: 10.1007/s11856-014-0021-7.
- [152] A. Steele. “Some new classes of division algebras and potential applications to space-time block coding”. (unpublished). PhD thesis. Univeristy of Nottingham, 2014.
- [153] A. Steele, S. Pumplün, and F. Oggier. “MIDO space-time codes from associative and nonassociative cyclic algebras”. In: *2012 IEEE Information Theory Workshop, ITW 2012* (Sept. 2012), pp. 192–196. DOI: 10.1109/ITW.2012.6404655.
- [154] D. Stehlé and R. Steinfeld. “Making NTRU as Secure as Worst-Case Problems over Ideal Lattices”. In: *EUROCRYPT 2011*. Ed. by K. G. Paterson. Vol. 6632. LNCS.
- [155] D. Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa. “Efficient Public Key Encryption Based on Ideal Lattices”. In: *ASIACRYPT 2009*. Ed. by M. Matsui. Springer Berlin Heidelberg, 2009, pp. 617–635. ISBN: 9783642103667.
- [156] D. Stehlé and R. Steinfeld. *Making NTRUEncrypt and NTRUSign as Secure as Standard Worst-Case Problems over Ideal Lattices*. Cryptology ePrint Archive. <https://eprint.iacr.org/2013/004>. 2013.
- [157] R. Steinfeld. “NTRU cryptosystem: Recent developments and emerging mathematical problems in finite polynomial rings”. In: *Algebraic Curves and Finite Fields*. Ed. by H. Niederreiter, A. Ostafe, D. Panario, and A. Winterhof. De Gruyter, 2014, pp. 179–212. DOI: doi:10.1515/9783110317916.179.

- [158] C. Sun, M. Tibouchi, and M. Abe. “Revisiting the Hardness of Binary Error LWE”. In: *ACISP 2020*. Ed. by J. K. Liu and H. Cui. Vol. 12248. LNCS. Springer International Publishing, 2020, pp. 425–444. ISBN: 9783030553043.
- [159] Kiran T. and B. Sundar Rajan. “STBC-Schemes with Nonvanishing Determinant for Certain Number of Transmit Antennas”. In: *IEEE Transactions on Information Theory* 51 (2005), pp. 2984–2992.
- [160] NTRU Prime Risk-Management Team. *Risks of lattice KEMs*. 2021. URL: <https://ntruprime.cr.yp.to/warnings.html>.
- [161] K. Thakur and B. Tripathi. “KTRU: NTRU over the Kleinian Integers”. In: *J. of International Academy of Physical Sciences* (2016), pp. 177–183.
- [162] K. Thakur and B. P. Tripathi. “STRU: A Non Alternative and Multidimensional Public Key Cryptosystem”. In: *GJPAM* 13 (2017), 1447–1464. URL: <http://www.ripublication.com/Volume/gjpamv13n5.htm>.
- [163] K. Truman. “Analysis and Extension of Non-Commutative NTRU”. A file of the relevant material can be found here: <https://drum.lib.umd.edu/bitstream/handle/1903/7344/umi-umd-4753.pdf?sequence=1&isAllowed=y>. PhD thesis. Aug. 2007.
- [164] D.R. Vance, G. Athas, Y. Avrahami, and J.G. Kline, eds. *BHS Standard Version Hebrew Bible*. Biblia Hebraica Stuttgartensia. Hendrickson Publishers Marketing, LLC, 2006. ISBN: 9781598561609.
- [165] N. Vats. “NNRU, a noncommutative analogue of NTRU”. In: *CoRR* abs/0902.1891 (2009). URL: <http://arxiv.org/abs/0902.1891>.
- [166] R. Vehkalahti, C. Hollanti, J. Lahtonen, and K. Ranto. “On the Densest MIMO Lattices From Cyclic Division Algebras”. In: *IEEE Trans. Inf. Theory* 55.8 (2009), pp. 3751–3780. DOI: 10.1109/TIT.2009.2023713.
- [167] J. Voight. “Quadratic forms and quaternion algebras: Algorithms and arithmetic”. PhD thesis. 2005, p. 156. ISBN: 978-0-542-29154-8. URL: <https://www.proquest.com/docview/305032530>.

- [168] J. Voight. *Quaternion Algebras*. Graduate Texts in Mathematics. Springer International Publishing, 2021. ISBN: 9783030566944.
- [169] Y. Wang and M. Wang. “Provably Secure NTRUEncrypt over Any Cyclotomic Field”. In: *SAC 2018*. Ed. by C. Cid and M. J. Jacobson Jr. LNCS 11349. Springer, pp. 391–417. ISBN: 9783030109707.
- [170] L. C. Washington. *Introduction to Cyclotomic Fields*. Graduate Texts in Mathematics. Springer New York, 2012. ISBN: 9781461219347.
- [171] W. C. Waterhouse. “Nonassociative quaternion algebras”. In: *Algebras, Groups, Geometries* 4.3 (1987), pp. 365–378.
- [172] A. Whitcomb. “The Group Ring Problem”. PhD thesis. University of Chicago, 1968. URL: <https://www.proquest.com/docview/302361327>.
- [173] T. Yasuda, H. Anada, and K. Sakurai. “Application of NTRU Using Group Rings to Partial Decryption Technique”. In: *INTRUST 2015*. Ed. by M. Yung, J. Zhang, and Z. Yang. Vol. 9565. LNCS. Springer, 2016, pp. 203–213. ISBN: 9783319315508.
- [174] Y. Yu, G. Xu, and X. Wang. “Provably Secure NTRU Instances over Prime Cyclotomic Rings”. In: *PKC 2017*. Ed. by S. Fehr. LNCS 10174. Springer Berlin Heidelberg, pp. 409–434. ISBN: 9783662543658.

A References for Quotations

Page 3: M. Eminescu, *Luceafărul*. In: *România Jună*, Almanachul Societății Academice Socială-Literare (1883).

Page 6: Aristotle, *The Metaphysics*. Loeb Classical Library Volume II (no. 287). Translated by H. Tredennick and G. C. Armstrong. Harvard University Press (1935).

Page 11: Herodotus, *Histories*. Volume III. Translated by G. Rawlinson. John Murray (1862).

Page 11: C. Shannon, *A Mathematical Theory of Cryptography*. Bell Laboratories (1945).

Page 203: Paul, *The Epistle to the Romans*. In: *The Greek New Testament*. Edited by D. Jongkind, P.J. Williams, P.M. Head, and J. Patrick. Crossway (2017).