Ring-LWE: Enhanced Foundations and Applications

Chengyu Lin

Submitted in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy
under the Executive Committee
of the Graduate School of Arts and Sciences

COLUMBIA UNIVERSITY

2023

Abstract

Ring-LWE: Enhanced Foundations and Applications

Chengyu Lin

Ring Learning With Errors assumption has become an important building block in many modern cryptographic applications, such as (fully) homomorphic encryption and post-quantum cryptosystems like the recently announced NIST CRYSTALS-Kyber public key encryption scheme. In this thesis, we provide an enhanced security foundation for Ring-LWE based cryptosystems and demonstrate their practical potential in real world applications.

Enhanced Foundation. We extend the known pseudorandomness of Ring-LWE to be based on ideal lattices of non Dedekind domains. In earlier works of Lyubashevsky, Perkert and Regev (EUROCRYPT 2010), and Peikert, Regev and Stephens-Davidowitz (STOC 2017), the hardness of RLWE was established on ideal lattices of ring of integers of number fields, which are known to be Dedekind domains. These works extended Regev's (STOC 2005) quantum polynomial-time reduction for LWE, thus allowing more efficient and more structured cryptosystems. However, the additional algebraic structure of ideals of Dedekind domains leaves open the possibility that such ideal lattices are not as hard as general lattices.

We show that, the Ring-LWE hardness can be based on the polynomial ring, which is potentially be a strict sub-ring of the ring of integers of a number field, and hence not be a Dedekind domain. We present a novel proof technique that builds an algebraic theory for general such rings that also include cyclotomic rings. We also recommend a "twisted" cyclotomic field as an alternative for

the cyclotomic field used in CRYSTALS-Kyber, as it leads to a more efficient implementation and is based on hardness of ideals in a non Dedekind domain.

In Application. We leverages the polynomial nature of Ring-LWE, and introduce XSPIR, a new symmetrically private information retrieval (SPIR) protocol, which provides a stronger security guarantee than existing efficient PIR protocols. Like other PIR protocol, XSPIR allows a client to retrieve a specific entry from a server's database without revealing which entry is retrieved. Moreover, the semi-honest client learns no additional information about the database except for the retrieved entry. We demonstrate through analyses and experiments that XSPIR has only a slight overhead compared to state-of-the-art PIR protocols, and provides a stronger security guarantee while enabling the client to perform more complicated queries than simple retrievals.

Table of Contents

List of Figures

List of Tables

Acknowledgements

I would like to express my deepest gratitude to my advisor, Professor Tal G. Malkin, for her invaluable guidance, support, and inspiration throughout my Ph.D journey. Working with Tal has been a privilege and a pleasure. I am indebted to her for giving me the opportunity to join her research group, learn from her, and collaborate with many other talented people. I would like to thank her for her trust, encouragement, and confidence in my abilities, which have boosted my self-confidence and motivated me to pursue my goals with passion and dedication. I am honored to have Tal as my advisor and will cherish the lessons, memories, and friendships that I have gained under her supervision.

I would like to express my appreciation to my mentor, Charanjit Jutla, who guided me through a fascinating journey in the world of Ring-LWE during my research internship at IBM in 2021. His continuous support, insightful feedback, and patient guidance were instrumental in shaping my research work and completing this thesis. I am grateful for his mentorship and the valuable lessons I learned under his guidance.

I would like to express my gratitude to the members of my thesis committee, Roxana Geambasu, Charanjit Jutla, Eran Tromer, and Moti Yung, for dedicating their valuable time and providing invaluable feedback.

I would like to thank all my collaborators on this and other works, whose invaluable contributions have greatly enriched my research journey. Special thanks go to Alexandr Andoni, Fabrice Benhamouda, Zhihuai Chen, Craig Gentry, Sergey Gorbunov, Siyao Guo, Shai Halevi, Charanjit Jutla, Yuan Kang, Hugo Krawczyk, Qian Li, Zeyu Liu, Tal Malkin, Tal Rabin, Mariana

Raykova, Leonid Reyzin, Ying Sheng, Xiaoming Sun, Ruiqi Zhong, Peilin Zhong for their insightful discussions, and constructive feedback. It has been an honor and pleasure to collaborate with such brilliant and inspiring individuals.

I'm also extremely thankful to all members of the wonderful Columbia crypto group, theory group, ICPC team, as well as the whole CS department. I will never forget the memorable time that we spent together over the past years.

Finally, I really thank my parents Yuantong Lin and Suxia Xu for their unwavering love and support throughout my life. I am forever indebted to them and I will strive to repay their kindness. I also want to extend a special thank you to Jian Ding, for her constant companionship during both good and bad days.

Chapter 1: Introduction

In a ground-breaking work, Regev [Reg05] showed a (quantum) polynomial-time reduction from worst-case lattice problems to a learning problem called *learning with error* (LWE). He also obtained public-key cryptosystems using LWE whose security is then based on worst-case lattice problems such as closest vector problem (CVP), shortest vector problem (SVP) and shortest independent vectors problem (SIVP). The fact that that there are no known efficient quantum algorithms for these hard problems, makes this approach to obtaining encryption schemes even more significant, and has led to numerous applications in cryptography.

As a more efficient variant of LWE, Lyubashevsky, Peikert and Regev [LPR10] introduced the Ring Learning With Errors problem (RLWE) over the ring of integers $\mathcal{O}_{\mathbf{K}}$ of a number field $\mathbf{K}$. The hardness of RLWE is then based on lattice problems restricted to ideal lattices in the ring $\mathcal{O}_{\mathbf{K}}$, instead of general integer lattices. Since addition and multiplication in the ring of integers can be viewed as polynomial addition and multiplication, it allows for more efficient cryptosystems, with almost a quadratic improvement in the security parameter. Additionally, it has allowed for a more sound security setting for many (fully) homomorphic encryption schemes [Gen09], where the ring structure naturally allows for homomorphic evaluation ring-operations [BGV12; Bra12; FV12; GSW13; DM15; Chi+16; Che+17]. For conjectured hardness of RLWE, [LPR10] provide a quantum polynomial-time reduction from the (seemingly) hard Approximate Shortest Independent Vectors Problem (ApproxSIVP) over ideal lattices. While the original [LPR10] reduction, especially for the decisional version of RLWE, was restricted to cyclotomic number fields, in another technical tour-de-force work, Peikert, Regev and Stephens-Davidowitz [PRS17] extend the hardness of decisional-RLWE to arbitrary number fields $\mathbf{K}$, basing the hardness on worst-case lattice problems restricted to ideal lattices in $\mathcal{O}_{\mathbf{K}}$.

Since the ring of integers $\mathcal{O}_{\mathbf{K}}$ of a number field enjoy remarkable algebraic properties, namely

that such rings are Dedekind domains and all ideals in the rings are invertible and have a unique prime ideal factorization, the question naturally arises if the normally hard lattice problems may be at a risk of being weaker due to the additional algebraic structure. In particular, while all ideal lattices are also full-ranked over the integers $\mathbb{Z}$, and of the same rank as the rank of the number field $\mathbf{K}$ as an extension of $\mathbb{Q}$, every ideal of a Dedekind domain can be generated by only two elements of the domain. Moreover, one of the generators can be taken to be just the integer that is the norm of the ideal. In light of this [1], we would like to answer the following question:

Can we establish the hardness of RLWE *on a family of lattices that possess a polynomial algebra but fewer algebraic properties?*

Ideally, one would like to base the hardness of RLWE on worst-case general integer lattices as is the case for LWE. On the other hand, can we leverage the polynomial nature of Ring-LWE in practice to build a more secure and efficient application from Ring-LWE based cryptosystems?

1.1 Enhancing Ring-LWE Hardness

We present a novel approach for basing the hardness of decisional-RLWE on ideal lattice problems in non Dedekind domains. Instead of using the ring of integers $O_{\mathbf{K}}$ of a number field $\mathbf{K} = \mathbb{Q}[X]/(f(X))$ as in previous works, we consider RLWE instances defined in the polynomial ring $\mathcal{R}_{\mathbf{K}} = \mathbb{Z}[X]/(f(X))$. This choice of ring simplifies the cryptosystem applications since the super-ring $O_{\mathbf{K}}$ can contain polynomials with rational coefficients. In particular, we establish that for all q that are not divisible by a small number of *excluded* primes, the q-RLWE instances are as hard as the worst-case lattice problems such as CVP and SIVP, of ideal lattices in this non Dedekind domain. The set of excluded primes is finite and comprises the primes p that divide the index of $\mathcal{R}_{\mathbf{K}}$ in $O_{\mathbf{K}}$, denoted by $[O_{\mathbf{K}} : \mathcal{R}_{\mathbf{K}}]$. We achieve the same security and noise parameters as in [PRS17], and most of our reduction relies on the main technical lemmas from [PRS17]. However, we replace the "ideal clearing lemma" of [LPR10] with a new proof and algorithm that does not rely on properties of Dedekind domains.

[1] We will later discuss in more detail the currently best known attacks (if any) on ideal lattices.

It is worth remarking that for every number field $\mathbf{K}$, there is a finite number m, namely $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}_{\mathbf{K}}]$, such that every ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbf{K}}$ can be scaled by m, so that $m \cdot \mathcal{I}$ is an ideal of $\mathcal{R}_{\mathbf{K}}$. Thus, the ideals (and corresponding lattices) in $\mathcal{R}_{\mathbf{K}}$ include all hard ideal lattices coming from $\mathcal{O}_{\mathbf{K}}$. However, we show later that the reverse is not true.

Earlier works, by Rosca, Stehlé and Wallet [RSW18], as well as Peikert and Pepin [PP19], have also considered setting RLWE in the polynomial ring $\mathcal{R}_{\mathbf{K}}$, but had only shown hardness of polynomial-LWE based on hardness of Dedekind-domain ideal lattices, namely $\mathcal{O}_{\mathbf{K}}$ lattices. In another yet unpublished and independent work [BBS21], Bolboceanu, Brakerski and Sharma have obtained a similar result as ours, but they only give a non-effective version of our result.

Our main technical contribution is the development of a novel theory for non Dedekind domains, which enables us to prove the ideal clearing lemma in a new way. Our contributions can be broken down into three parts. First, we prove that every ideal $\mathcal{I}$ of $\mathcal{R}_{\mathbf{K}}$ is principal when considered modulo $q\mathcal{I}$, where q is relatively prime to $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}_{\mathbf{K}}]$. Second, we introduce an extremely simple randomized algorithm to find a generator of this principal ideal. Notably, the general problem of finding a generator of a principal ideal is only known to have a sub-exponential time classical algorithm [BF14] and a quantum polynomial time algorithm [BS16]. Our randomized algorithm takes a $\mathbb{Z}_q[X]/(f(X))$-linear combination of the columns of a given $\mathbb{Z}$-basis of $\mathcal{I}$. Finally, we prove that it is possible to efficiently "clear the ideal", given only a $\mathbb{Z}$-basis of the ideal $\mathcal{I}$ and a generator of the principal ideal $\mathcal{I}/(q\mathcal{I})$. Our technique and novel randomized algorithm are also applicable to number fields where $\mathcal{O}_{\mathbf{K}}$ is the same as $\mathcal{R}_{\mathbf{K}}$, such as popular cyclotomic number fields, for all q. This leads to an improved (time complexity) reduction for the usual q-RLWE hardness for cyclotomics, compared to [LPR10]. Additionally, our technique does not require q to have a known factorization, unlike [LPR10].

1.2 Application of Ring-LWE: XSPIR

Ring-LWE based cryptography is widely used in practical computationally private information retrieval (PIR) protocols, which allow a client to retrieve a data entry from a server while hiding

which entry was retrieved. Many efficient PIR protocols have been proposed, the most up-to-date of them are SealPIR by Angel et. al. [Ang+18], MulPIR by Ali et. al. [Ali+21], and SHECS-PIR by Park and Tibouchi [PT20]. However, these schemes do not satisfy the stronger version of PIR, known as *Symmetrically Private Information Retrieval* (SPIR), where the client must only learn the retrieved data entry and not any information about other data entries, ensuring privacy for the server's data.

To address this limitation, we present XSPIR, an efficient and practical SPIR scheme. We follows the line of works that started with XPIR [Agu+16] and culminated in SealPIR [Ang+18], MulPIR[Ali+21] and SHECS-PIR[PT20]. Most crucially, our technique leverages the polynomial algebra structure of the underlying Ring-LWE assumption. This is in contrast with general ways to transform PIR schemes to SPIR schemes as proposed in previous works. For example, [Ali+21] discuss in their appendix how data privacy can be added on top of MulPIR, by using oblivious Pseudorandom Function (OPRF), for which the constructions are mainly based on DDH assumption [MRR20; MR19].

Our proposed XSPIR scheme not only provides strong privacy guarantees for both the client and server, but it also achieves practical efficiency, making it an ideal solution for many applications where the data consists of sensitive information.

1.3 Organizations

In Chapter 2, we enhanced the security foundation for Ring-LWE assumption, by basing its hardness on ideals lattice problems in non Dedekind domains.

In Chapter 3, we present how to construct a symmetrically secure private information retrieval protocol upon the polynomial algebra structure of the Ring-LWE assumption. We also demonstrate its performance and compare it with other state-of-the-art PIR scheme.

Chapter 2: Enhanceing Ring-LWE Hardness

2.1 Introduction

In this chapter, we extend the known pseudorandomness of Ring-LWE to be based on ideal lattices of non Dedekind domains. More precisely, we intend to show that the the q-RLWE instances, defined in the polynomial ring $\mathcal{R}_{\mathbf{K}} = \mathbb{Z}[X]/(f(X))$, for all all q such that q and $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}_{\mathbf{K}}]$ are co-prime, are as hard as the worst-case lattice problems such as CVP and SIVP, of ideal lattices in this non Dedekind domain.

Dedekind Index Theorem. Recall, the Dedekind Index Theorem [Cona] gives an easy necessary and sufficient test of when a prime p *does not* divides the index $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}_{\mathbf{K}}]$. The test involves checking the factorization of $f(X)$ modulo p into irreducible polynomials (modulo p) for a specific property. If p does not divide this index, then another theorem of Dedekind shows that the prime ideal factorization of ideal (p) of $\mathcal{O}_{\mathbf{K}}$ can be read off from the factorization of $f(X)$ modulo p. We show that in this case the ideal (p) of $\mathcal{R}_{\mathbf{K}}$ also factors into prime ideals of $\mathcal{R}_{\mathbf{K}}$, i.e. (p) is well-behaved even in $\mathcal{R}_{\mathbf{K}}$. We will refer to these as the good primes, as it will allow us to prove the "ideal-clearing lemma" and also obtain an efficient randomized algorithm for ideal-clearing. However, if some other prime p' fails the test, and hence $p' \mid [\mathcal{O}_{\mathbf{K}} : \mathcal{R}_{\mathbf{K}}]$, then $\mathcal{R}_{\mathbf{K}}$ is a strict sub-ring of $\mathcal{O}_{\mathbf{K}}$, and is then definitely not a Dedekind domain. We will refer to these p' as the bad primes. It is well known that a prime p' can divide $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}_{\mathbf{K}}]$ only if p'^2 divides the discriminant of the field $\mathbf{K}$. Therefore, the number of bad p' is already bounded by the number of factors of the discriminant, and hence is finite and usually few. Thus, the trick is to find a p for which the factorization of (p) is well-behaved and another p' which is bad (so that we are guaranteed a non Dedekind domain). Then the RLWE can be set modulo any q whose prime factors exclude the

small number of bad p'.

Example. Consider the polynomial $f(X) = X^{256} + 2 \cdot 3^2 \cdot 13$. By Eisenstein criterion, $f(X)$ is irreducible over $\mathbb{Q}$, and thus $\mathbf{K} = \mathbb{Q}[X]/(f(X))$ is a number field. Consider the polynomial ring[1] $\mathcal{R} = \mathbb{Z}[X]/(f(X))$. The discriminant of $f(X)$ is just the determinant of the multiplication matrix of $f'(X) = 256 \cdot X^{255}$, and a little calculation shows that only $2, 13$ and 3 can divide the discriminant, and hence are the only possible bad candidates for the Dedekind index test. The factorization of $f(X)$ modulo any of these primes is just X^{256}, and hence has only one irreducible polynomial, i.e. X, as a factor with multiplicity 256. Any factor that has multiplicity more than one is said to ramify (mod that prime), and factors that have multiplicity one are called unramified. Focusing on prime 2, write $f(X)$ as $X^{256} + 2 \cdot t(X)$, and note that $t(X)$ is just the trivial polynomial $3^2 \cdot 13$. The Dedekind index theorem says that a prime, in this case 2, divides $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}]$ *iff* $t(X)$ is divisible by a ramified factor (modulo 2), in this case the factor X. Since, X does not divide $3^2 \cdot 13 \bmod 2$, it implies that 2 does not divide $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}]$, and 2 is a good prime. Hence we can base our RLWE modulo any power of two, and still be assured hardness based on worst case ideal lattices in $\mathcal{R}$. Now, let's check that 3 divides the index, so that $\mathcal{R}$ is a strict sub-ring of $\mathcal{O}_{\mathbf{K}}$. In this case, $t(X) = 2 \cdot 3 \cdot 13$ which is zero mod 3 and hence is trivially divisible by X. Thus, 3 divides $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}]$ and hence $\mathcal{R}$ is not a Dedekind domain. We give more complicated examples in Section 2.8, where we also prove that some non-trivial ideal requires at least three generators. But, the above example was expressly chosen as a potential alternative to CRYSTALS-Kyber [Bos+21] cyclotomic number-field which is defined with $f(X) = X^{256} + 1$. Kyber also sets $q = 3329$ for q-RLWE and more generally module-LWE. Now, it turns out that $-2 \cdot 3^2 \cdot 13$ is a 256-th residue in $\mathbb{Z}_q$, and this leads to a highly efficient implementation. The ramifications are discussed in more detail in Section 2.8.

Known Attacks on Ideal Lattices There are no known efficient classical/quantum algorithms for polynomial-factor approximation of SVP, SIVP etc for ideal lattices of $\mathcal{O}_{\mathbf{K}}$ (or sub-rings such

[1] Since $\mathbf{K}$ will be clear from context, we will drop it from subscript of $\mathcal{R}_{\mathbf{K}}$.

as $\mathcal{R}_{\mathbf{K}}$), even restricted to prime-power cyclotomic fields. However, after a flurry of heuristic claims [Berb ; CGS14], the work [Cra+16] has shown that when restricted to principal ideals, the sub-exponential-approximate SVP problem can be solved in quantum polynomial time. The attack has two parts. First, an arbitrary generator of the principal ideal is computed by index-calculus method by first computing the ideal class group [BF14; BS16]. Second, a short generator is computed by running bounded-distance-decoding on Dirichlet's logunit lattice (i.e. the logarithms of the unit group that form a small ranked lattice) [Cra+16]. For general ideals in $\mathcal{O}_{\mathbf{K}}$, we know that $\mathcal{O}_{\mathbf{K}}$ being a Dedekind domain has the property that every ideal has at most two generators and in fact it is relatively easy to compute some pair of generators for every ideal using prime ideal factorization (see e.g. [FT91; LPR10]). However, now the above second step does not work as logarithm of additive terms is non-linear. We should remark that of the two generators one can always be taken to be a number, e.g. the norm of the ideal, although even this does not help in searching through the logunit lattice. So, more advanced techniques are required *if* there is a potential attack on general ideals of Dedekind domains. As for the polynomial ring $\mathcal{R}_{\mathbf{K}}$, when it is a strict sub-ring of $\mathcal{O}_{\mathbf{K}}$ it is a non Dedekind domain. Since, ideals not co-prime to the conductor ideal may no longer have prime-ideal factorization, the approach of finding generators by prime-ideal factorization does not work (see Table 2.1). One may wonder that since the number of bad primes p', i.e. the ones that divide the index of $\mathcal{R}_{\mathbf{K}}$ in $\mathcal{O}_{\mathbf{K}}$, is small, it maybe the case that only a few ideals are lacking algebraic structure (i.e. of the Dedekind domain kind). While it is true that there are only a few *prime* ideals lacking algebraic structure [Conb, Theorem 8.6], the number of non-prime ideals contained in these prime ideals is unlimited. Another important point to be raised is if one can demonstrate that non-trivial ideals in such non Dedekind domains require more than two generators. We also prove that there are non-trivial ideals, i.e. which do not have a diagonal Hermite normal form, for which at least three generators are required, and which cannot be scaled by a rational number to become an ideal of $\mathcal{O}_{\mathbf{K}}$.

Algebraic Property	$\mathcal{O}_{\mathbf{K}}$	$\mathcal{R}_{\mathbf{K}} \subsetneq \mathcal{O}_{\mathbf{K}}$
Class Group and Unit Group Computation [FT91; BF14]	Yes	Yes*
Irredundant Primary Decomposition of Ideals [AM69, Ch. 4]	Yes	Yes
Jordan-Hölder Filtration of Ideals [Conb; BBS21]	Yes	Yes
Tight bound on Shortest Vector [PR07; LPR10] (Lemma 2.4.5)	Yes	Yes
Every Fractional Ideal is Invertible [Cla84; FT91; Cond]	Yes	No
Every Ideal co-prime to Conductor is Invertible [Cond]	Yes	Yes
Unique Prime Ideal Factorization (PIF) [Cla84; FT91]	Yes	No
PIF of ideals co-prime to Conductor [Cond]	Yes	Yes
Every Ideal has at most two Generators [FT91]	Yes	No
Compute (two or more) generators given $\mathbb{Z}$-basis (e.g. [LPR10])	Yes	?
Ideal $\mathcal{I}$ mod $q\mathcal{I}$ is Principal (for q Dedekind-special) (Secs. 2.5,2.6)	Yes	Yes

Table 2.1: Comparison of algebraic properties that an ideal lattice satisfies in the worst case. If a property is indicated with an affirmative, then it is also known to be efficiently computable (for class group, the claim is only for heuristic sub-exponential complexity[BF14]; moreover (*), for $\mathcal{R}_{\mathbf{K}}$ the class group is only defined limited to the subset of invertible ideals of $\mathcal{R}_{\mathbf{K}}$ (modulo group of *all* principal ideals) [Cond]). The question mark above indicates that it is an open problem.

On Clearing the Ideal. As mentioned earlier, one of the main technical challenges in the hardness reduction, starting from Regev's LWE reduction, is setting up a q-RLWE instance which is somehow not dependent on the worst-case lattice instance, especially given only some basis $\boldsymbol{B}(\mathcal{L})$ of the lattice $\mathcal{L}$. While in the LWE instance, since the multiplication in LWE is just inner product, it is compatible with the lattice and the dual lattice clearing each other out, and the issue of inverting the lattice-basis modulo q does not come up. In the case of RLWE, since it is more "efficient", the multiplication in RLWE is not a trace-product, but rather a polynomial multiplication. Thus, it is not enough that a lattice $\mathcal{L}$ and its dual lattice $\mathcal{L}^\vee$ have the property that $\mathcal{L}^\top \mathcal{L}^\vee = \boldsymbol{I}$. To solve this problem, the ideal clearing lemma of [LPR10] obtains an efficiently invertible (module-) isomorphism between $\mathcal{I}/q\mathcal{I}$ and the whole polynomial ring[2] modulo q, for any ideal $\mathcal{I}$. This isomorphism is not easy to obtain as lattice corresponding to $\mathcal{I}$ may not be invertible modulo q, and in fact (q) as an ideal may have additional factorization into prime ideals. Nevertheless, an efficient isomorphism is obtained by computing prime ideal factorization or effectively inverting the ideal $\mathcal{I}$ itself (instead of inverting its lattice-basis).

[2]More precisely, $\mathcal{O}_{\mathbf{K}}/q\mathcal{O}_{\mathbf{K}}$, for general fields

In our case, i.e. where $\mathcal{R}_{\mathbf{K}}$ is a non Dedekind domain, the ideal $\mathcal{I}$ may not be invertible. However, we prove a more general clearing lemma that suffices for the reduction, and only requires that $\mathcal{I}$ be a principal ideal modulo $q\mathcal{I}$. Note, principal ideals are trivially invertible, as their $\mathbb{Z}$-basis is their (circulant) multiplication matrix. In case of Dedekind domains, it is well known that Dedekind domains modulo any ideal are principal ideal domains. However, $\mathcal{R}_{\mathbf{K}}$ may not be a Dedekind domain. We manage to show that, for any prime p, such that p is good with respect to the Dedekind index theorem, $\mathcal{R}_{\mathbf{K}}/p^r\mathcal{R}_{\mathbf{K}}$ is a principal ideal domain, for any positive integer r. Further, we show that for any ideal $\mathcal{I}$, $\mathcal{I}$ is principal modulo $p^r\mathcal{I}$. Using Chinese Remainder theorem, the result can then be extended to any q that is product of powers of good primes. We also give a highly efficient randomized algorithm to find a generator for the above mentioned principal ideals, which essentially takes a random $\mathcal{R}_{\mathbf{K}}/p\mathcal{R}_{\mathbf{K}}$-linear combination of the columns of the $\mathbb{Z}$-basis of the ideal $\mathcal{I}$.

Related Works. In [Bol+19], a generalization of the RLWE problem is described, wherein the ambient ring is not the ring of integers of a number field, but rather an order (i.e. a full-ranked sub-ring) such as the polynomial ring we consider. In a followup work in [BBS21], they independently[3] show a result similar to our work in that they prove an ideal clearing lemma for arbitrary orders, including the polynomial ring. The relevant isomorphisms in their clearing lemma are not shown to be efficiently computable and they just prove that the relevant ring modules are isomorphic, whereas we give an efficient algorithm to compute and invert these isomorphisms. This is critical in showing an efficient reduction. Their approach to proving the ideal clearing lemma is also different. Instead of showing that for every ideal $\mathcal{I}$, for the good q of the number field, $\mathcal{I}/q\mathcal{I}$ is principal, they take an alternative approach by first showing that $\mathcal{I}$ is always a sub-ideal of an invertible ideal $\mathcal{I}'$, such that $[\mathcal{R} : \mathcal{I}']$ is co-prime to q. The isomorphism is then built using composition of two maps from earlier works, namely [PP19, Theorem 4.1][4] and the original ideal clearing lemma of [LPR10]. The existence of $\mathcal{I}'$ with the relevant property is shown using Jordan-

[3] [BBS21] appeared on the eprint archive about a year before our archiving on eprint.

[4] In Theorem 4.1 of [PP19, Theorem 4.1] it is shown that, given a $\mathbb{Z}$-basis of an ideal $\mathcal{I}$, there is an efficiently computable and invertible isomorphism as long as the ideal $\mathcal{I}$ is co-prime to the ideal (q) of $\mathcal{R}$.

Holder decomposition of ideals in orders of a number field [Conb, Theorem 8.9]. However, it is not shown how $\mathcal{I}'$ can be obtained efficiently given only a $\mathbb{Z}$-basis of the ideal $\mathcal{I}$.

We have surmised that the above mentioned $\mathcal{I}'$ of [BBS21] can be obtained efficiently by a quantum algorithm via the following strategy: first, factor the determinant of the given basis of $\mathcal{I}$, using Shor's quantum algorithm [Sho94]. Next, for each prime p in the factorization that is co-prime to $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}_{\mathbf{K}}]$, one obtains a prime ideal factorization of the ideal (p), using another algorithm of Dedekind and relevant theory of conductor ideals of $\mathcal{R}$ [Cond]. One then searches through powers of each of these prime ideals to get the maximum power that is a factor ideal of $\mathcal{I}$. The product of all such prime ideal powers is the required ideal $\mathcal{I}'$. Since Regev's hardness reduction is anyway quantum, the fact that this algorithm is quantum does not hamper one from obtaining a quantum hardness reduction from ideals of $\mathcal{R}$, although it is desirable to have a classical isomorphism for the clearing lemma such as the one we show. It is worth noting, as we point out in the technical overview (section 2.1.1), that the depth of the quantum circuit for factoring is possibly much deeper than the quantum circuit required for Regev's discrete Gaussian sampling [Reg05]; the former requires computing exponentiation modulo N whereas the latter requires computing the representative of a point modulo the given basic parallelepiped of lattice of ideal $\mathcal{I}$.

In [RSW18], a reduction from decision (resp. search) RLWE in $\mathcal{O}_{\mathbf{K}}$ to decision (resp. search) polynomial-LWE [Ste+09] (i.e. with the ring $\mathcal{R}_{\mathbf{K}}$) is obtained, Since, the hardness of RLWE in $\mathcal{O}_{\mathbf{K}}$ was only known based on hardness of ideals in $\mathcal{O}_{\mathbf{K}}$, this result only ties the hardness of polynomial-LWE to hardness of Dedekind-domain ideal lattices. In [PP19], a more general framework is considered which encompasses Module-LWE [BGV12; LS15] and Order-LWE [Bol+19] and shows reductions from Ring-LWE to these other variants, and with tight reductions, but with the same limitation.

Outline. The rest of this chapter is organized as follows. The remaining part of Introduction contains a technical overview. Section 2.2 covers preliminaries of lattices, smoothing lemma, and hard problems over lattices. Section 2.3 covers basics of ideals and states the Dedekind Index

theorem. Section 2.4 introduces the polynomial ring calculus including dual ideals. Section 2.5 introduces the notion of Dedekind-special primes w.r.t. a separable polynomial which sets up the primes p for each number field for which our reduction works. The section also proves that ideal $\mathcal{I}$ is principal modulo $p^r\mathcal{I}$. Section 2.6 gives a novel randomized algorithm to find a generator for above principal ideal. Section 2.7 proves the pseudo-randomness of q-RLWE using earlier works and the novel formulation of the clearing lemma and its proof using the theory and algorithms developed in earlier sections. We also give and prove our version of the clearing lemma for ring of integers of arbitrary number fields. Section 2.8 considers alternatives to CRYSTALS-Kyber and gives examples of non-bigenic ideals.

2.1.1 Technical Overview

The state-of-the-art decisional Ring-LWE hardness, extended to lattices of ideals (of ring of integers) of all number fields, is the culmination of three works: the original Regev LWE-reduction [Reg05], the decisional Ring-LWE hardness for cyclotomic fields [LPR10], and the extension to all number fields [PRS17].

First, we briefly describe the main components of Regev's hardness reduction from discrete Gaussian sampling (DGS) over worst-case integer lattices to learning-with-error (q-LWE) modulo integer q. While the DGS problem for a lattice $\mathcal{L}$ can be classically solved if the variance σ for the Gaussian sampling is sufficiently large, for instance $\sigma > 2^{2n}\lambda_n(\mathcal{L})$, where n is the dimension of the lattice and λ_n, as usual, is the minimum length of a set of n linearly independent vectors from $\mathcal{L}$. This step is also called the bootstrapping step of DGS. To obtain finer sampling, i.e. for σ approaching a polynomial factor away from $\lambda_n(\mathcal{L})$, Regev employs a recursive strategy involving two reductions:

1. A quantum reduction that allows one to solve finer DGS for $\mathcal{L}$ given a worst-case promise closest-vector-problem (CVP) oracle for the dual lattice $\mathcal{L}^\vee$. A promise CVP oracle $\mathrm{CVP}_{\mathcal{L}^\vee,d}$ solves the closest vector problem as long as the input instance is promised to be within distance d of the lattice $\mathcal{L}^\vee$. The larger the promise under which the CVP oracle works, the finer

is the DGS sampler, upto a limit. It is worth remarking that the main quantum components of this algorithm is a quantum fourier transform, and a computation (over superpositions) that computes a representative of point x modulo a given basic parallelepiped of $\mathcal{L}^\vee$.

2. A classical reduction that uses a q-LWE oracle, along with a fine DGS sampler for $\mathcal{L}$ to solve promise CVP over the dual lattice $\mathcal{L}^\vee$. The finer the DGS sampler, the larger the promise that the CVP solver can handle. One hard problem solved in this step is what maybe referred to as "clearing the lattice". Note that the CVP input instance describes a point x close to some lattice point y of some lattice $\mathcal{L}^\vee$, whereas the q-LWE oracle which is used to solve this problem does not explicitly refer to any lattice. Regev's clever idea is to use the DGS sampler to sample a lattice vector v from $\mathcal{L}$, and take the inner product of v with x to obtain the LWE sample. Since the dual lattice, by definition, is spanned by $\mathcal{L}^{-\top}$, this leads to clearing of the lattice from the LWE instance.

The prior work [LPR10] extended step 2 by utilizing a q-RLWE oracle to solve the CVP problem for ideal lattices of the dual of the *ring of integers* of the underlying number field. However, the reduction to the decisional RLWE problem was only demonstrated for cyclotomic fields. The major challenge that they addressed was that the dual of a lattice, which in this case is a lattice defined by a $\mathbb{Z}$-basis of an ideal $\mathcal{I}$ of the ring, need not be an ideal itself. Fortunately, this issue is well studied in number theory and the appropriate lattice to consider is the one embedded in $\mathbb{C}^n$, the n-dimensional complex domain, via the "canonical embedding". This embedding is similar to a Fourier transform and is essentially the linear transform defined by the Vandermonde matrix of $f(X)$, where $f(X)$ is the irreducible polynomial that defines the number field $\mathbf{K} = \mathbb{Q}[X]/(f(X))$.

Once we consider these embedded lattices, it turns out that the usual notion of a dual lattice leads to a lattice that corresponds to a (fractional) ideal of the same ring. This (fractional) ideal is referred to as the dual ideal $\mathcal{I}^\vee$ of the original ideal $\mathcal{I}$. This is crucial in solving the "clearing the lattice" problem in step 2 above, where the problem is more complicated now as the RLWE sample generation uses polynomial (or number field) multiplication, and hence clearing the lattice must also employ polynomial multiplication and not an inner product; the latter sufficed for LWE.

This is one of the main reasons that working with the *dual ideal* is helpful, although it still doesn't immediately solve the problem. To fully tackle the problem [LPR10] formulated and proved an "ideal clearing lemma", which informally showed the following:

(i) an efficient isomorphism ψ that maps the finely sampled v (from the ideal $\mathcal{I}$ or its corresponding lattice $\mathcal{L}$) to the ring modulo q,

(ii) an efficiently invertible isomorphism ϕ that maps y, a lattice point in lattice $\mathcal{L}^\vee$ of dual ideal $\mathcal{I}^\vee$ (or equivalently treating y as an element of ideal $\mathcal{I}^\vee$) to the dual of the ring (again, modulo q),

(iii) such that $\psi(v) * \phi(y) = v * y \pmod{q}$, where '*' is the polynomial multiplication in the number field (*ideal clearing property*).

Note that the image of ϕ and ψ lie in the ring and the dual of the ring respectively, and do not refer to the ideal or the lattice, and hence the name "ideal clearing lemma". More importantly, it is imperative to show that these isomorphisms are efficiently computable (invertible resp.) given only some basis of the ideal (or the corresponding lattice). This, however, is not an easy task and requires algorithms from computational number theory, and in particular the unique prime ideal factorization of ideals of Dedekind domains. [LPR10] show an invertible isomorphism ψ as required above by computing an element t in the ideal $\mathcal{I}^\vee$ such that $t \cdot \mathcal{I}^{-\vee}$ is co-prime to ideal (q). Intuitively, multiplication by t serves as the inverse of isomorphism ψ by noting the following: multiplication by any t in $\mathcal{I}^\vee$ would map the dual of the ring to the ideal $\mathcal{I}^\vee$. However, if the principal ideal (t) shares some prime ideals with factorization of (q), then this would not be a bijection. Thus, by requiring that $t \cdot \mathcal{I}^{-\vee}$ is coprime to (q), the map becomes bijective. But, note that this reasoning only holds in a ring where there is unique prime ideal factorization, and hence this technique only works for rings which have unique prime ideal factorization. It is well-known that the ring of integers $\mathcal{O}_\mathbf{K}$ of a number field $\mathbf{K}$ is a Dedekind domain which is also well-known to have unique prime ideal factorization. Further, all strict sub-rings of ring of integers of a number field are known to be non Dedekind domain, and also *not* have unique prime ideal factorization.

Extension to Polynomial Ring $\mathcal{R}$, a non Dedekind Domain We focus on the polynomial ring $\mathcal{R} = \mathbb{Z}[X]/(f(X))$, which is a subring of the ring of integers $\mathcal{O}_{\mathbf{K}}$ of a number field $\mathbf{K}$. If q divides the index of $\mathcal{R}$ in $\mathcal{O}_{\mathbf{K}}$, then $\mathcal{R}$ is strictly a subring of $\mathcal{O}_{\mathbf{K}}$. We propose an alternate strategy to simplify the "ideal clearing lemma". This strategy can be applied to $\mathcal{R}$ as long as q is coprime to the index of $\mathcal{R}$ in $\mathcal{O}_{\mathbf{K}}$ (denoted as $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}]$). Our approach involves demonstrating that for any ideal $\mathcal{I}$ of $\mathcal{R}$ and any such q, the ideal $\mathcal{I}/q\mathcal{I}$ is a principal ideal of the ring $\mathcal{R}$. We also provide a simple and novel randomized algorithm to find a generator for this principal ideal. Finally, we demonstrate that, with this generator in hand, we can provide the requisite isomorphisms ϕ and ψ described above. These isomorphisms are computationally efficient and invertible, and they satisfy the ideal clearing property.

Since the proof of ideal clearing lemma requires some key lemmas involving the dual ideal, which in turn is defined using the canonical embedding, we begin by giving in section 2.4 a basic introduction to dual ideals, especially tailored for the polynomial ring $\mathcal{R}$. The core of our work is in showing that $\mathcal{I}/q\mathcal{I}$ is a principal ideal of the ring $\mathcal{R}$, and we achieve this goal in a relatively elementary way, without invoking advanced techniques such as localization, Jordan-Holder decomposition, conductor-ideal theory and of course neither the Dedekind domain prime ideal factorization. Surprisingly, we do not even use the Dedekind's index theorem, and we directly work with q which only have prime factors p, such that the factorization of $f(X)$ modulo p passes the Dedekind test.

We briefly summarize the section 2.5 here on how to prove that $\mathcal{I}/q\mathcal{I}$ is a principal ideal of the ring $\mathcal{R}$. For simplicity, assume that $q = p^r$ for some prime p. Let the factorization of $f(X)$ modulo p into irreducible polynomials (modulo p) be

$$f(X) = \prod_i h_i(X)^{e_i} \; + \; p \cdot t(X),$$

and since we stipulate that p satisfies the Dedekind index test, it follows that for any i such that $e_i > 1$ it is the case that $t(X)$ is not in the maximal ideal $(p, h_i(X))$ of $\mathcal{R}$. One can then show that

the principal ideal (p) has the following factorization into maximal (and hence prime) ideals :

$$(p) = \prod_i (p, h_i(X))^{e_i}.$$

This part is actually well-known from another theorem of Dedekind. Next, as a warm up, we first prove the simpler fact that $\mathcal{I}$ modulo q is a principal ideal. In other words $\mathcal{R}/(q)$ is a principal ideal ring. Given the above factorization of (p), using the Chinese remainder theorem (CRT), it suffices to show that for each i, $\mathcal{R}/(p, h_i(X))^{r \cdot e_i}$ is a principal ideal ring. Now, if an ideal $\mathcal{I}$ of $\mathcal{R}$ is not a sub-ideal of the maximal ideal $(p, h_i(X))$ then it is trivially principal modulo $(p, h_i(X))^{r \cdot e_i}$, as it is generated by 1. We next show that if $e_i = 1$, then p is always a generator of an ideal that is a sub-ideal of $(p, h_i(X))$, when considered mod $(p, h_i(X))^{r \cdot e_i}$, and similarly if $e_i > 1$, then $h_i(X)$ is a generator. So, this proves that $\mathcal{I}$ modulo q is a principal ideal. We will later see that these facts about these generators allow us to obtain a randomized algorithm for a generator of $\mathcal{I}/q\mathcal{I}$.

But, before that we need to show that $\mathcal{I}/q\mathcal{I}$ is a principal ideal. We cannot use CRT directly now as we do not have a factorization of $\mathcal{I}$, and in fact in the non Dedekind domain $\mathcal{R}$, such a prime ideal factorization may not exist. Nevertheless, we can show that $\mathcal{I}$ can be written as $\hat{\mathcal{I}} \cdot \prod_i (p, h_i(X))^{t_i}$ where t_i are finite integers, and $\hat{\mathcal{I}}$ is co-prime to all $(p, h_i(X))$. This is the most difficult part of the proof, as it requires showing that t_i is finite for any $\mathcal{I}$. This is proved by showing that if $\mathcal{I}$ is a sub-ideal of every power $(p, h_i(X))^t$ $(t > 0)$, then $\mathcal{I}$ must be the zero ideal, and hence principal. An alternative proof that any non-zero ideal $\mathcal{I}$ of $\mathcal{R}$ must have a largest t such that it is a subset of $(p, h_i(X))^t$ follows by analyzing the determinants of the relevant basis matrices. This uses the property that the determinant of a $\mathbb{Z}$-basis of an ideal $\mathcal{I}$ is exactly the index of the additive subgroup $\mathcal{I}$ of $\mathcal{R}$. However, proving this requires a foray into Smith Normal Form (see e.g. [PZ89, Chapter 3]). Rest of the proof then follows as before using CRT.

As noted, we proved the above claim using CRT, and for most components, we either had zero, one, p or $h_i(X)$ as the principal ideal generator. This allows us to give a simple randomized algorithm for the principal ideal $\mathcal{I}/q\mathcal{I}$, given any $\mathbb{Z}$-basis for the ideal $\mathcal{I}$. Indeed, the simple

algorithm picks n random elements $\rho_k(X)$ ($k \in [n]$) from $\mathbb{Z}_p[X]/(f(X))$. Next, we view each of the n columns of the $\mathbb{Z}$-basis of $\mathcal{I}$ as polynomials, say $\gamma_k(X)$. The algorithm simply outputs $\sum_{k\in[n]} \gamma_k(X) * \rho_k(X)$. We prove that this is a generator of the principal ideal with a decent non-negligible probability. See section 2.6 for details.

2.2 Preliminaries

We'll be working with the polynomial rings modulo a monic polynomial $f(X) \in \mathbb{Z}[X]$ of degree n whose (complex) roots are distinct. Each ring element is a polynomial $g(X) = \sum_{i=0}^{n-1} g_i X^i$ of degree less than n, which can be viewed as a length-n (column) vector of its coefficients $(g_0, \ldots, g_{n-1})$. We will denote this vector by boldface g, i.e. $\mathbf{g}$, and we will use this as a general notational principle.

In particular, we are interested in the following three rings: $\mathcal{R} = \mathbb{Z}[X]/(f(X))$, its modulo q version $\mathcal{R}_q = \mathbb{Z}_q[X]/(f(X))$ for some $q \in \mathbb{Z}$, and the rational version $\mathcal{R}_\mathbb{Q} = \mathbb{Q}[X]/(f(X))$. When $f(X)$ is irreducible, $\mathbf{K} = \mathcal{R}_\mathbb{Q}$ is a number field.

For clarity, we use operator "$*$" for polynomial multiplication, operator "$\times$" for matrix (vector) multiplication and cartesian product.

2.2.1 The Canonical Space $\mathcal{H}$ and Lattices

The ring $\mathcal{R}_\mathbb{Q}$ is definitely a $\mathbb{Q}$-algebra, and a (possibly degenerate) extension of the field $\mathbb{Q}$. Since, $\mathbb{C}$ is the completion of algebraic closure of $\mathbb{Q}$, $\mathcal{R}_\mathbb{Q}$ naturally embeds in $\mathbb{C}$, with $\mathbb{Q} \subseteq \mathcal{R}_\mathbb{Q}$ embedding identically in $\mathbb{C}$. However, there are n such distinct embeddings in $\mathbb{C}$. These n embeddings are automorphic (i.e. automorphisms of the image of $\mathcal{R}_\mathbb{Q}$ in C) if $\mathcal{R}_\mathbb{Q}$ is a Galois field extension. However, in our general case, we will get n embeddings which are not necessarily automorphic. The n embeddings viewed together can be seen as mapping to the following space $\mathcal{H}$, which we will refer to as the *canonical embedding* in the general case, i.e. whether $\mathcal{R}_\mathbb{Q}$ is a Galois extension or not even a field extension.

The canonical space $\mathcal{H}$ is defined as follow where $s_1 + 2s_2 = n$:

$$\mathcal{H} = \left\{ (x_0, \ldots, x_{n-1}) \subseteq \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2} \middle| \forall i \in [s_2] : x_{s_1+i} = \overline{x_{s_1+s_2+i}} \right\} \subseteq \mathbb{C}^n$$

We then describe the canonical embedding from the polynomial ring $\mathcal{R} = \mathbb{Z}[X]/(f(X))$ to this space $\mathcal{H}$ given by a matrix.

Vandermonde Matrix and Discriminant Let the n distinct roots of $f(X)$ be $(z_0, \ldots, z_{n-1})$. Note the complex roots of $f(X)$ come in conjugate pairs, because for integer polynomial, $f(\bar{z}) = \overline{f(z)}$. We can order the roots such that $z_i \in \mathbb{R}$ for $i \in [s_1]$ and $z_{s_1+i} = \overline{z_{s_1+s_2+i}}$ for $i \in [s_2]$, where $s_1 + 2s_2 = n$.

The (square) *Vandermonde matrix* $\boldsymbol{V}$ of the roots of $f(X)$ is given by

$$\boldsymbol{V} = \begin{bmatrix} 1 & z_0 & z_0^2 & \cdots & z_0^{n-1} \\ 1 & z_1 & z_1^2 & \cdots & z_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & z_{n-1} & z_{n-1}^2 & \cdots & z_{n-1}^{n-1} \end{bmatrix}$$

whose determinant is $\det(\boldsymbol{V}) = \prod_{0 \le i < j < n} (z_j - z_i)$. Because all roots are distinct, $\det(\boldsymbol{V}) \neq 0$ and hence $\boldsymbol{V}$ is invertible. We will abuse notation, and call the Vandermonde matrix of z_i's, to be also the Vandermonde matrix of $f(X)$.

The **discriminant** Δ_f of a polynomial is defined to be the square of the determinant of the Vandermonde matrix of $f(X)$. In corollary 2.4.3 we will relate the discriminant to the determinant of the multiplication matrix (in $\mathbb{Q}[X]/(f(X))$) of the derivative of $f(X)$.

Given a polynomial $g(X) \in \mathcal{R}_{\mathbb{Q}}$ and its vector representation $\mathbf{g} \in \mathbb{Q}^n$, we have $(1, z, z^2, \ldots, z^{n-1})^\top \times \mathbf{g} = g(z)$. The product of $\boldsymbol{V}$ and $\mathbf{g}$ is essentially the evaluation of polynomial $g(X)$ at roots of $f(X)$: $(g(z_0), g(z_1), \ldots, g(z_{n-1})) \in \mathcal{H}$. Therefore, the Vandermonde matrix $\boldsymbol{V}$ of $f(X)$ canonically embeds the polynomial in $\mathcal{R}_{\mathbb{Q}}$ into the canonical space $\mathcal{H}$: first view the polynomial as vector of coefficients over $\mathbb{Q}$ ($\subseteq \mathbb{R} \subseteq \mathbb{C}$). The first s_1 rows of $\boldsymbol{V}$ maps this vector into $\mathbb{R}^{s_1}$, and the remaining

rows of $\boldsymbol{V}$ maps this vector into $\mathbb{C}^{2s_2}$, with conjugate pairs. Note that $\boldsymbol{V}(\mathbf{g} * \mathbf{h})$ is same as point-wise product of $\boldsymbol{V}\mathbf{g}$ and $\boldsymbol{V}\mathbf{h}$, for any polynomials $\mathbf{g}$ and $\mathbf{h}$.

Lattice The lattice $\mathcal{L}$ is defined as an additive subgroup of $\mathcal{H}$ given by a set of basis vectors $\{\mathbf{b_0}, \ldots, \mathbf{b_{m-1}}\}$ from $\mathcal{H}$:

$$\mathcal{L} = \left\{ \sum_{i=0}^{m-1} z_i \cdot \mathbf{b_i} \middle| (z_0, \ldots, z_{n-1}) \in \mathbb{Z}^n \right\}.$$

It's dual is defined as $\mathcal{L}^\vee = \left\{ \mathbf{y} \in \mathcal{H} | \, \forall \mathbf{x} \in \mathcal{L} : \langle \mathbf{y}, \mathbf{x} \rangle = \mathbf{y}^H \mathbf{x} \in \mathbb{Z} \right\}$. Here $(\cdot)^H$ denotes the Hermitian (conjugate) transpose. It's easy to verify that $(\mathcal{L}^\vee)^\vee = \mathcal{L}$.

The minimum distance of a lattice is defined as the length of the shortest non-zero lattice vector: $\lambda_1(\mathcal{L}) = \min_{\mathbf{0} \neq \mathbf{x} \in \mathcal{L}} \{\|\mathbf{x}\|\}$.

Gaussians Define $G = \left\{ \mathbf{r} \in \mathbb{R}_+^n \middle| \, \mathbf{r}_{s_1+i} = \mathbf{r}_{s_1+s_2+i}, 0 \leq i < s_1 \right\}$. For any $\mathbf{r} \in G$, the *elliptical Gaussian distribution* $D_{\mathbf{r}}$ over the space $\mathcal{H}$ is defined to have a probability density function propotional to $\rho_{\mathbf{r}}(\mathbf{x}) = \exp\left(- \sum_{i=0}^{n-1} |\mathbf{x}_i / \mathbf{r}_i|^2 \right)$. For real $r > 0$, We also define the spherical Gaussian distribution D_r as $D_{r \cdot \mathbf{1}}$.

Definition 2.2.1 (Smoothing Condition)**.** *For any lattice $\mathcal{L} \subset \mathcal{H}$, a positive real $\epsilon > 0$ and $\mathbf{r} \in G$, we say $\mathbf{r} \geq \eta_\epsilon(\mathcal{L})$ if $\rho_{1/\mathbf{r}}(\mathcal{L}^\vee \setminus \{0\}) \leq \epsilon$ where $1/\mathbf{r} = (1/r_0, 1/r_1, \ldots, 1/r_{n-1})$.*

Lemma 2.2.1 ([MR07; PRS17])**.** (**Smoothing Lemma**) *For any lattice $\mathcal{L} \subset \mathcal{H}$, $\epsilon > 0$ and $\mathbf{r} \geq \eta_\epsilon(\mathcal{L})$. the statistical distance between $(D_{\mathbf{r}} \bmod \mathcal{L})$ and the uniform distribution over $\mathcal{H}/\mathcal{L}$ is at most 2ϵ.*

Lemma 2.2.2 ([MR07])**.** *For any lattice $\mathcal{L} \subset \mathcal{H}$ and $c \geq 1$, we have $c\sqrt{n}/\lambda_1(\mathcal{L}^\vee) \geq \eta_\epsilon(\mathcal{L})$ where $\epsilon = \exp(-c^2 n)$.*

Proposition 2.2.1 ([MR07])**.** *For any lattice $\mathcal{L} \subset \mathcal{H}$ and $\epsilon \in (0, 1)$, we have $\eta_\epsilon(\mathcal{L}) \geq \sqrt{\frac{\log(1/\epsilon)}{\pi}} / \lambda_1(\mathcal{L}^\vee)$.*

For a lattice $\mathcal{L} \subset \mathcal{H}$ and $\mathbf{r} \in G$, the *discrete Gaussian* distribution $D_{\mathcal{L},\mathbf{r}}$ is defined to have support $\mathcal{L}$ and mass function $D_{\mathcal{L},\mathbf{r}}(\mathbf{x}) = \rho_{\mathbf{r}}(\mathbf{x}) / \rho_{\mathbf{r}}(\mathcal{L})$ for $\mathbf{x} \in \mathcal{L}$.

2.2.2 Lattice Problems

We introduce the following (seemingly hard) lattice problems.

Definition 2.2.2 (SVP and SIVP)**.** *On the canonical space $\mathcal{H}$ endowed with some geometric norm (such as the ℓ_2 norm), let $\gamma > 1$, given a lattice $\mathcal{L}$, the* Shortest Vector Problem SVP_γ *asks for an element $\mathbf{x} \in \mathcal{L}$ such that $\|\mathbf{x}\| \leq \gamma \cdot \lambda_1(\mathcal{L})$, and the* Shortest Independent Vectors Problem SIVP_γ *asks for n linearly independent elements in $\mathcal{L}$ whose norms are at most $\gamma \cdot \lambda_n(\mathcal{L})$.*

Definition 2.2.3 (DGS)**.** *Let $\gamma > 0$. The* Discrete Gaussian Sampling problem DGS_γ *is, given a lattice $\mathcal{L} \subseteq \mathcal{H}$ and $r \geq \gamma$, output samples from the distribution $D_{\mathcal{L},r}$.*

More specifically, we consider the above problems restricted to the *ideal lattices*, when lattices are generated by ideals of the polynomial ring $\mathcal{R} = \mathbb{Z}[X]/(f(X))$. See section 2.4.2.

Definition 2.2.4 (GDP)**.** *For a lattice $\mathcal{L} \subseteq \mathcal{H}$, the* Gaussian Decoding Problem $\mathsf{GDP}_{\mathcal{L},r}$ *asks, given a coset $\mathbf{e} + \mathcal{L}$ where $\mathbf{e} \in \mathcal{H}$ is sampled from Gaussian D_r, find $\mathbf{e}$.*

2.3 Ideal Basics

Let R be any commutative ring with unity. An (integral) *ideal* $\mathfrak{a} \subseteq R$ is an additive subgroup that is closed under multiplication by the elements from R. A *fractional ideal* $\mathfrak{a}$ is a subset of R, such that there exists an element $r \in R$ that makes $r \cdot \mathfrak{a}$ an integral ideal of R. An ideal $\mathfrak{a}$ generated by finitely many $g_1, g_2, ...g_k$ is denoted by $(g_1, g_2, ..., g_k)$. Note, $(1) = R$. A **prime ideal** of a ring R is an ideal $\mathfrak{p}$ such that $ab \in \mathfrak{p}$ implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. A **maximal ideal** of a ring R is a non-trivial ideal (i.e. not same as R) that is maximal under the subset relation. Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are called **co-prime** if $\mathfrak{a} + \mathfrak{b} = (1)$. An element $c \in R$ will be called **invertible modulo an ideal** $\mathfrak{a}$ if there exists a $\mu \in R$ and $\lambda \in \mathfrak{a}$ such that $\mu c = 1 + \lambda$. In other words, c is a **unit** of quotient ring $R/\mathfrak{a}$. We now enumerate a list of well-known facts about ideals, which also have elementary proofs (see e.g. [AM69] or [Cla84] for proofs, if not provided).

Lemma 2.3.1. (i) *Every non-trivial ring has at least one maximal ideal.*

(ii) *A maximal ideal is always a prime ideal.*

(iii) *The quotient ring* $R/\mathfrak{a}$ *is a field iff* $\mathfrak{a}$ *is a maximal ideal.*

(iv) *For ideals* $\mathfrak{a}$ *and* $\mathfrak{b}$*, their sum* $\mathfrak{a} + \mathfrak{b}$ *is the set of all* $x + y$ *where* $x \in \mathfrak{a}$ *and* $y \in \mathfrak{b}$*. It is the smallest ideal containing* $\mathfrak{a}$ *and* $\mathfrak{b}$*.*

(v) *Thus, a maximal ideal* $\mathfrak{m}$ *is co-prime to every ideal that is not a subset of* $\mathfrak{m}$*.*

(vi) *If* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are* not *co-prime, then there exists a maximal ideal* $\mathfrak{m}$ *such that* $\mathfrak{a} + \mathfrak{b} \subseteq \mathfrak{m}$*.*

(vii) *If* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are co-prime, then* $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$*.*

(viii) *If a prime ideal* $\mathfrak{p}$ *contains product of two ideal* $\mathfrak{a}\mathfrak{b}$*, then at least one of* $\mathfrak{a}$ *or* $\mathfrak{b}$ *is in* $\mathfrak{p}$*.*

(ix) *If an ideal* $\mathfrak{a}$ *is co-prime to two ideals, say* $\mathfrak{b}$ *and* $\mathfrak{c}$*, then* $\mathfrak{a}$ *is co-prime to* $\mathfrak{b}\mathfrak{c}$*.*

(x) *If ideals* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are co-prime, then for any positive integers* r, s*, their powers* $\mathfrak{a}^r$ *and* $\mathfrak{b}^s$ *are also co-prime.*

(xi) *If a maximal ideal* $\mathfrak{m}$ *contains product of powers of distinct maximal ideals* $\mathfrak{n}_1, ..., \mathfrak{n}_k$*, then* $\mathfrak{m}$ *must be one of* $\mathfrak{n}_1, ..., \mathfrak{n}_k$*.*

Proof. Proof of ((*viii*)). If a prime ideal $\mathfrak{p}$ contains product of two ideal $\mathfrak{a}\mathfrak{b}$, then at least one of $\mathfrak{a}$ or $\mathfrak{b}$ is in $\mathfrak{p}$. If neither of $\mathfrak{a}$ and $\mathfrak{b}$ is contained in $\mathfrak{p}$, then there are elements $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$, that are not in $\mathfrak{p}$. Yet, $a * b$, being in $\mathfrak{a}\mathfrak{b}$ is in $\mathfrak{p}$, contradicting the fact that $\mathfrak{p}$ is prime.

Proof of ((*ix*)). If an ideal $\mathfrak{a}$ is co-prime to two ideals, say $\mathfrak{b}$ and $\mathfrak{c}$, then $\mathfrak{a}$ is co-prime to $\mathfrak{b}\mathfrak{c}$. For if not, then $\mathfrak{a} + \mathfrak{b}\mathfrak{c}$ is contained in a maximal ideal $\mathfrak{m}$, and hence $\mathfrak{b}\mathfrak{c}$ is also contained in $\mathfrak{m}$. By previous item, one of $\mathfrak{b}$ or $\mathfrak{c}$, w.l.o.g. $\mathfrak{b}$, is contained in $\mathfrak{m}$. Since $\mathfrak{a}$ is also contained in $\mathfrak{m}$, this implies that $\mathfrak{a} + \mathfrak{b}$ is contained in $\mathfrak{m}$, contradicting the fact that $\mathfrak{a}$ and $\mathfrak{b}$ are co-prime.

Proof of ((*x*)). If ideals $\mathfrak{a}$ and $\mathfrak{b}$ are co-prime, then for any positive integers r, s, their powers $\mathfrak{a}^r$ and $\mathfrak{b}^s$ are also co-prime: if $\mathfrak{a}^r$ and $\mathfrak{b}^s$ are not co-prime then there is a maximal ideal $\mathfrak{m}$ containing $\mathfrak{a}^r + \mathfrak{b}^s$, and hence also $\mathfrak{a}^r$ and $\mathfrak{b}^s$ individually. Since $\mathfrak{m}$ is also prime, $\mathfrak{m}$ contains both $\mathfrak{a}$ and $\mathfrak{b}$ and hence also their sum, contradicting the fact that $\mathfrak{a}$ and $\mathfrak{b}$ are co-prime.

Proof of ((*xi*)). If a maximal ideal $\mathfrak{m}$ contains product of powers of distinct maximal ideals $\mathfrak{n}_1, ..., \mathfrak{n}_k$, then $\mathfrak{m}$ must be one of $\mathfrak{n}_1, ..., \mathfrak{n}_k$. Say, $\prod_i \mathfrak{n}_i^{r_i}$ is contained in $\mathfrak{m}$. Suppose $\mathfrak{m}$ is not the same as one of $\mathfrak{n}_1, ..., \mathfrak{n}_k$. Then, $\mathfrak{m}$ is co-prime to each of $\mathfrak{n}_i$, and hence also to their powers $\mathfrak{n}_i^{r_i}$, which are also pair-wise co-prime. Thus, one of $\mathfrak{n}_i^{r_i}$ is in $\mathfrak{m}$ (by item (*viii*)), and hence maximal ideal $\mathfrak{n}_i$ is itself in maximal ideal $\mathfrak{m}$, an absurdity. □

Lemma 2.3.2. *For any ring R, and any maximal ideal $\mathfrak{a} = (a_1, a_2)$ of R, let $x \in R$ be such that x is not in $\mathfrak{a}$. Then for any positive integers r, s, x is invertible modulo (a_1^r, a_2^s).*

The lemma can be proved easily in multiple ways, but we prefer an argument used in Prop. 2.5 in [LLL82].

Proof. Clearly, for $r = 1$ and $s = 1$, the claim holds, i.e. x is invertible modulo the maximal ideal $\mathfrak{a}$, as $R/\mathfrak{a}$ is a field. Thus,

$$\mu x = 1 - (\nu_1 a_1 + \nu_2 a_2),$$

for some μ, ν_1, ν_2. If ν_2 is zero, then x is invertible modulo (a_1) and hence also modulo any power of (a_1), and we are done. Similarly, for ν_1 being zero. Else,

$$\mu x + \nu_1 a_1 = 1 - \nu_2 a_2,$$

Multiplying both sides by $1 + \nu_2 a_2 + ... + (\nu_2 a_2)^{s-1}$, we get

$$\mu' x + \nu_1' a_1 = 1 - \nu_2^s a_2^s,$$

for some μ' and ν_1'. Rewriting this as

$$\mu' x + \nu_2^s a_2^s = 1 - \nu_1' a_1,$$

and multiplying both sides by $1 + \nu_1' a_1 + ... + (\nu_1' a_1)^{r-1}$, the claim follows. □

Noetherian Ring

A ring R is called **Noetherian** if every ideal of R is finitely generated. We show that $\mathbb{Z}[X]/(f(X))$ is finitely generated for any polynomial $f(X) \in \mathbb{Z}[X]$, and hence Noetherian.

Lemma 2.3.3. *If a ring R is Noetherian, then for any ideal $\mathfrak{a}$ of R, the ring $R/\mathfrak{a}$ is Noetherian.*

Corollary 2.3.1. *(see [Conc]) The ring $\mathcal{R} = \mathbb{Z}[X]/(f(X))$ is Noetherian for any polynomial $f(X) \in Z[X]$.*

Theorem 2.3.1 (Krull Intersection Theorem)**.** *Let R be a Noetherian ring, and $\mathcal{I}$ an ideal in R. Then*

$$\mathcal{I} * \bigcap_{i=1}^{\infty} \mathcal{I}^i = \bigcap_{i=1}^{\infty} \mathcal{I}^i$$

For an elementary proof see [Kap73, Theorem 74].

We will directly prove the following corollary in lemma 2.5.6 using theorem 2.3.1 for certain requisite maximal ideals in the ring $\mathcal{R} = \mathbb{Z}[X]/(f(X))$, even when $f(X)$ is not irreducible over $\mathbb{Q}$, i.e. when $\mathcal{R}$ is not necessarily an integer domain. However, we state this more general corollary here for high-level discussion.

Corollary 2.3.2 (See e.g. [Eis13])**.** *For any Noetherian ring R that is also an integral domain, for any ideal $\mathcal{I}$ of R,*

$$\bigcap_{i=1}^{\infty} \mathcal{I}^i = 0$$

For a proof of the general form of CRT below, see e.g. [Eis13].

Theorem 2.3.2 (Chinese Remainder Theorem (CRT))**.** *Let $\mathfrak{a}_1, ..., \mathfrak{a}_k$ be a set of pairwise co-prime ideals of a ring R. Then,*

$$R/\mathfrak{a}_1 \cdots \mathfrak{a}_k \equiv \prod_i R/\mathfrak{a}_i$$

Dedekind Domains

A **Dedekind domain** is a non-trivial integral domain in which every non-zero fractional ideal is invertible. An ideal is called proper if it not same as (0) or (1). A major theorem of Dedekind

domain states that every proper ideal of a Dedekind domain can be uniquely (upto re-ordering) factored as a product of proper prime ideals (see e.g. [FT91] or [Cla84]). Further, every proper prime ideal is a maximal ideal.

Let R be a subring of a ring R'. An element $x \in R'$ is said to be **integral** over R if it satisfies a monic polynomial equation, where the polynomial has coefficients in R. The **ring of integers**, denoted $\mathcal{O}_{\mathbf{K}}$ of a number field $\mathbf{K}$ are elements of $\mathbf{K}$ that are integral over $\mathbb{Z}$. It is well-known that the ring of integers $\mathcal{O}_{\mathbf{K}}$ of a number field is a Dedekind domain (see e.g. [FT91]).

For a prime number p, if an ideal $\mathfrak{a}$ of $\mathcal{O}_{\mathbf{K}}$ contains the ideal (p) (of $\mathcal{O}_{\mathbf{K}}$), we say that $\mathfrak{a}$ lies above p. Another well-known property of Dedekind domains is that every prime ideal of $\mathcal{O}_{\mathbf{K}}$ lies above some prime p. An alternative equivalent definition of Dedekind domain is that it is an integrally-closed Noetherian domain in which every nonzero prime ideal is maximal.

For any ideal $\mathfrak{a}$ of the Dedekind domain $\mathcal{O}_{\mathbf{K}}$, the (absolute) **norm** of $\mathfrak{a}$, $N(\mathfrak{a})$, is defined to be $[\mathcal{O}_{\mathbf{K}} : \mathfrak{a}]$, i.e. the cardinality of the residue class ring $\mathcal{O}_{\mathbf{K}}/\mathfrak{a}$. We state the following facts as a lemma (see any text on algebraic number theory for proofs, for instance [FT91])

Lemma 2.3.4. (i) *Let $\mathfrak{p}$ denote a non-zero prime ideal of $\mathcal{O}_{\mathbf{K}}$ and let r be a positive integer. Then, we have an isomorphism of additive groups: $\mathcal{O}_{\mathbf{K}}/\mathfrak{p} \cong \mathfrak{p}^r/\mathfrak{p}^{r+1}$ (see II.1.16 of [FT91]).*

(ii) *For a prime ideal $\mathfrak{p}$, $N(\mathfrak{p}^r) = (N(\mathfrak{p}))^r$.*

(iii) *For any two non-zero ideals $\mathfrak{a}, \mathfrak{b}$ of $\mathcal{O}_{\mathbf{K}}$, $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.*

(iv) *If $\mathfrak{a}$ is a prime ideal of $\mathcal{O}_{\mathbf{K}}$ lying above prime p, then $\mathcal{O}_{\mathbf{K}}/\mathfrak{a}$ is a field extension of finite field $\mathbb{Z}_p$ of some finite degree e. Further, $N(\mathfrak{a}) = p^e$. (see (II.1.37) of [FT91]).*

(v) *The norm of a principal ideal (a), $N((a))$, is same as the (absolute value of) field norm of a, i.e. $N_{\mathcal{O}_{\mathbf{K}}/\mathbb{Q}}(a)$. (see (II.1.38) of [FT91], and see section 2.4 for definition of field norm).*

(vi) *The discriminant of any monic irreducible polynomial $f(X)$, Δ_f, divides $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}]^2$, where $\mathbf{K} = \mathbb{Q}[X]/(f(X))$ and $\mathcal{R} = \mathbb{Z}[X]/(f(X))$ (see (II.1.39) of [FT91]).*

(vii) *The norm of an ideal* $\mathfrak{a}$ *of* $\mathcal{O}_{\mathbf{K}}$ *is same as the (absolute value of) determinant of any* $\mathbb{Z}$*-basis of* $\mathfrak{a}$. *(see (II.1.39) of [FT91]).*

Dedekind Index Theorem

Theorem 2.3.3 (Dedekind Index Theorem)**.** *Let* p *be a prime integer. For any monic polynomial* $f(X) \in \mathbb{Z}[X]$ *that is irreducible over* $\mathbb{Q}$*, let* $\mathcal{O}_{\mathbf{K}}$ *be the ring of integers of the number field* $\mathbf{K} = \mathbb{Q}[X]/(f(X))$*. Let the following be the factorization of* $f(X)$ *modulo* p *into powers of* m *irreducible polynomials* $h_i(X) \in \mathbb{Z}_p[X]$ *(*$i \in [m]$*):*

$$f(X) = h_1(X)^{e_1} \ldots h_m(X)^{e_m} \; + \; p \cdot t(X),$$

where e_i *are positive integers, and* $t(X) \in \mathbb{Z}_p[X]$*. Then,* $p \mid [\mathcal{O}_{\mathbf{K}} \; : \; \mathbb{Z}[X]/(f(X))]$ *iff for some* $i \in [m]$*, such that* $e_i \geq 2$*, polynomial* $h_i(X)$ *divides* $t(X)$ *in* $\mathbb{Z}_p[X]$.

For a proof of the celebrated theorem see [Cona] or [Coh93, Theorem 6.1.4]. Recall, for a prime p, $\mathbb{Z}_p[X]$ is a unique factorization domain.

Ring of Integers of Cyclotomic Fields

Now, we restrict ourselves to cyclotomic fields, i.e. where $f(X)$ is a cyclotomic polynomial. Recall, a complex number ζ is a primitive m-th root of unity, if its order is exactly m. The m-th **cyclotomic polynomial** is defined by

$$\Phi_m(X) \; = \; \prod (X - \zeta)$$

where the product runs over the different primitive m-th roots of unity ζ. Since, such primitive roots lie in a splitting extension field E (over $\mathbb{Q}$) of $X^m - 1$, the primitive roots are exactly the generators of the cyclic group of order m; thus degree of $\Phi_m(X)$ is exactly the Euler totient function $\phi(m)$. It is well-known that cyclotomic polynomials are irreducible in $\mathbb{Q}[X]$. The cyclotomic field $\mathbb{Q}[X]/(\Phi_m(X))$ will be denoted by $\mathbb{Q}[m]$.

We have the following well-known identities.

$$\begin{aligned} X^m - 1 &= \prod_{d|m} \Phi_d(X) \\ \Phi_m(X) &= \prod_{d|m} (X^d - 1)^{\mu(m/d)} \\ \Phi_{p^r}(X) &= \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = \sum_{i=0}^{p-1} X^{ip^{r-1}} \end{aligned}$$

where $\mu(\cdot)$ is the mobius function, p is a prime, and $r \geq 1$. It follows that $\Phi_m(X)$ is always a polynomial over the base field $\mathbb{Q}$.

We also have the following lemma, whose proof can be found in any text in algebraic number theory, for instance (VI. 1.14) of [FT91].

Lemma 2.3.5. *If $m = m_1 m_2$ with $(m_1, m_2) = 1$, then $\mathbb{Q}[m]$ is the compositum of arithmetically disjoint fields, i.e.*

$$\mathbb{Q}[m] \cong \mathbb{Q}[m_1] \otimes_{\mathbb{Q}} \mathbb{Q}[m_2]$$

$$O_{\mathbb{Q}[m]} \cong O_{\mathbb{Q}[m_1]} \otimes_{\mathbb{Z}} O_{\mathbb{Q}[m_2]}$$

It is well-known that the ring of integers $O_{\mathbf{K}}$ of a cyclotomic field is same as the polynomial ring $\mathbb{Z}[X]/(\Phi_m(X))$. Below, we give an easy proof of this fact using Dedekind Index Theorem. This polynomial ring will also be referred to as the m-th **cyclotomic ring**. Recall, in section 2.2, we defined the discriminant of a separable polynomial $f(X)$ to be the square of the determinant of the vandermonde matrix of $f(X)$. When $f(X)$ is a cyclotomic polynomial, the discriminant of the polynomial is also called the **discriminant** of the cyclotomic field and denoted $\Delta_{\mathbf{K}}$ (as also the discriminant of the ring of integers, or the cyclotomic ring).

Theorem 2.3.4. *For any m, the ring of integers $O_{\mathbf{K}}$ of the cyclotomic field $\mathbf{K} = \mathbb{Q}[X]/(\Phi_m(X))$ is same as the polynomial ring $\mathcal{R} = \mathbb{Z}[X]/(\Phi_m(X))$. Thus, $\mathcal{R}$ is a Dedekind domain.*

Proof. By lemma 2.3.5, we are reduced to proving the theorem for m that are prime powers, i.e.

$m = q^r$, for some prime q and positive integer r. It is well known[5] that a prime p divides $[\mathcal{O}_\mathbf{K} : \mathcal{R}]$ only if p^2 is a factor of $\Delta_{\Phi_m(X)}$. By corollary 2.4.3 , the discriminant of a monic separable $f(X)$ is same as the determinant of the circulant matrix of $f'(X)$. Further, since the similarity transform given by the vandermonde matrix of $f(X)$, transforms the circulant matrix of any $g(X)$ to a diagonal matrix with entries $g(\zeta_i)$, where ζ_i are the roots of $f(X)$, one can show that $\Delta_{f_1}\Delta_{f_2}$ divides the discriminant of $f_1(X)f_2(X)$. Thus, discriminant of $\Phi_m(X)$ divides the discriminant of $X^m - 1$. For $m = p^r$, the discriminant of $X^m - 1$ is easily seen to be (upto sign) a power of p. Thus, $\Delta_{\Phi_m(X)}$ can only be divisible by prime p. This further implies that only prime p, if any, can divide $[\mathcal{O}_\mathbf{K} : \mathcal{R}]$.

By Dedekind index theorem 2.3.3, for any prime p, p does not divide $[\mathcal{O}_\mathbf{K} : \mathcal{R}]$ iff p is Dedekind-special for $\Phi_m(X)$. Thus, we just need to check that prime p coming from $m = p^r$ is Dedekind-special for $\Phi_m(X)$. Since modulo p, the power-p map is a Frobenius map, we have that $\Phi_{p^r}(X) = \Phi_p(X)^{p^{r-1}} \bmod p$. Next, note that $\Phi_p(X) = (X-1)^{p-1} \bmod p$, by first noting that $X^p - 1 = (X-1)^p \bmod p$. Thus, $\Phi_{p^r}(X) = (X-1)^{\phi(p^r)}$. To test the Dedekind-special property, write $\Phi_{p^r}(X) = (X-1)^{\phi(p^r)} + p * t(X)$. Evaluating both sides at $X = 1$, we note that $\Phi_{p^r}(X)_{|X=1} = p$, and hence $t(1) = 1 \bmod p$. Thus $t(X)$ is not divisible by $(X-1)$ modulo p, and hence p is Dedekind special for $\Phi_{p^r}(X)$. □

2.4 Polynomial Ring Calculus

In this section, we illustrate a simple framework on how to play with polynomial rings.

2.4.1 Circulant Matrices

Definition 2.4.1 (Circulant Matrices modulo $f(X)$)**.** *On polynomial ring modulo $f(X)$, the circulant matrix (modulo $f(X)$) for a ring element $g(X)$ is given by an n-by-n matrix $\boldsymbol{C}_g$ whose i-th column is the coefficients of $g(X) * X^i$ modulo $f(X)$ for $i = 0, 1, \ldots, n-1$.*

We could take the underlying polynomial ring to be any of $\mathcal{R}, \mathcal{R}_\mathbb{Q}$ and $\mathcal{R}_q$. For simplicity,

[5] $\Delta_f = [\mathcal{O}_\mathbf{K} : \mathcal{R}]^2 \cdot \text{disc}(\mathcal{O}_\mathbf{K})$, and $\text{disc}(\mathcal{O}_\mathbf{K})$ is an integer.

in the following part, we abuse the notion of circulant matrix without explicitly mentioning the underlying modulo polynomial $f(X)$.

Proposition 2.4.1. *For any two ring elements $g(X)$ and $h(X)$, $\boldsymbol{C}_g \times \mathbf{h}$ corresponds to the their product $g(X) * h(X)$.*

Proof. Let $h(X) = \sum_{i=0}^{n-1} h_i X^i$. We have that, $\boldsymbol{C}_g \times \mathbf{h} = \sum_{i=0}^{n-1} h_i \cdot (\boldsymbol{C}_g)_i$, which corresponds to the polynomial $\sum_{i=0}^{n-1} h_i \cdot (g(X) * X^i) = g(X) * (\sum_{i=0}^{n-1} h_i X^i) = g(X) * h(X)$. □

Corollary 2.4.1. *For any two ring elements $g(X)$ and $h(X)$, $\boldsymbol{C}_g \times \boldsymbol{C}_h = \boldsymbol{C}_{g*h}$.*

Proof. By Proposition 2.4.1, the i-th column of $\boldsymbol{C}_g \times \boldsymbol{C}_h$ corresponds to the polynomial $g(X) * h(X) * X^i$. Together they form the circulant matrix $\boldsymbol{C}_{g*h}$. □

It's not difficult to see that circulant matrices are closed under addition and multiplication. Moreover, the multiplication commutes.

Corollary 2.4.2. *On polynomial ring modulo $f(X)$, all the circulant matrices form a commutative subring under matrix addition and multiplication.*

Lemma 2.4.1. *On polynomial ring modulo $f(X)$, a circulant matrix $\boldsymbol{C}_g$ has an inverse $\boldsymbol{C}_g^{-1} = \boldsymbol{C}_{g^{-1}}$ iff $g(X)$ is invertible modulo $f(X)$.*

Proof. First for invertible $g(X)$, take its inverse $g^{-1}(X)$. We have $\boldsymbol{C}_g \boldsymbol{C}_{g^{-1}} = \boldsymbol{C}_{g^{-1}} \boldsymbol{C}_g = \boldsymbol{C}_1 = I$.

If $g(X)$ is not invertible. Let $0 \neq h(X)$ be such that $g(X) * h(X) = 0$. Then we have that $\boldsymbol{C}_g \mathbf{h} = \mathbf{0}$ for some $\mathbf{h} \neq \mathbf{0}$, and hence $\boldsymbol{C}_g$ is not invertible. □

For rational polynomial ring $\mathcal{R}_{\mathbb{Q}} = \mathbb{Q}[X]/(f(X))$, the inverse of the circulant matrix can also be given as $\boldsymbol{C}_g^{-1} = \frac{1}{\det(\boldsymbol{C}_g)} \cdot \mathrm{adj}(\boldsymbol{C}_g)$ where $\mathrm{adj}(\boldsymbol{C}_g)$ is the adjugate matrix of $\boldsymbol{C}_g$ with $\mathrm{adj}(\boldsymbol{C}_g)_{i,j} = (-1)^{i+j} \cdot \det(M_{j,i})$. Here, $M_{i,j}$, commonly known as the minor, is obtained by removing the i-th row and j-th column from $\boldsymbol{C}_g$. If $g(X)$ is from $\mathcal{R}$ and $\boldsymbol{C}_g$ is integer, its inverse $\boldsymbol{C}_g^{-1}$ is also integer except for a common (integer) denominator $\det(\boldsymbol{C}_g)$.

Another view of the canonical embedding. Take the Vandermonde matrix $\boldsymbol{V}$ of $f(X)$. It defines an embedding from the polynomial ring $\mathcal{R}$ to its evaluation domain $\mathcal{H}$. Let $\boldsymbol{D}_g$ be the diagonal matrix with its diagonal being the canonical embedding of $g(X)$, i.e. $(\boldsymbol{D}_g)_{i,i} = g(z_i)$. Consider $(\boldsymbol{V} \times \boldsymbol{C}_g)_{i,j} = p_j(z_i)$ where $p_j(X) = g(X) * X^j$. Note that the polynomial multiplication is under the polynomial ring modulo $f(X)$. Because $p_j(X) = g(X)X^j - t_j(X)f(X)$ for some polynomial $t_j(X)$, we have

$$(\boldsymbol{V} \times \boldsymbol{C}_g)_{i,j} = p_j(z_i) = g(z_i) \cdot z_i^j - t_j(z_i) \cdot 0 = g(z_i) \cdot z_i^j = (\boldsymbol{D}_g \times \boldsymbol{V})_{i,j}$$

and hence $\boldsymbol{V}\boldsymbol{C}_g = \boldsymbol{D}_g\boldsymbol{V}$ or $\boldsymbol{V}\boldsymbol{C}_g\boldsymbol{V}^{-1} = \boldsymbol{D}_g$.

In other words, in the polynomial ring modulo $f(X)$, the diagonal matrix of $g(X)$'s evaluations (at roots of $f(X)$) can be obtained by a similarity transformation (given by Vandermonde matrix V of $f(X)$) of the circulant matrix of $g(X)$.

The determinant of the circulant matrix $\boldsymbol{C}_g$ can be then calculated as

$$\det(\boldsymbol{C}_g) = \frac{\det(\boldsymbol{D}_g)}{\det(\boldsymbol{V})\det(\boldsymbol{V}^{-1})} = \det(\boldsymbol{D}_g) = \prod_{i=0}^{n-1} g(z_i) \tag{2.1}$$

where z_i's are the roots of $f(X)$. Note that this is just the product of all the entries in the embedding of $g(X)$. When $f(X)$ is irreducible, and thus $\mathcal{R}_\mathbb{Q}$ is a field, then this quantity, i.e. the determinant $\det(\boldsymbol{C}_g)$ is called the norm of $g(X)$ in the extension field $\mathcal{R}_\mathbb{Q}$ of $\mathbb{Q}$.

2.4.2 Ideal Lattices and Dual Ideals

In this section, we focus on $\mathcal{R}_\mathbb{Q} = \mathbb{Q}[X]/(f(X))$ and its sub-ring, the integer polynomial ring $\mathcal{R} = \mathbb{Z}[X]/(f(X))$. When $f(X)$ is irreducible over $\mathbb{Q}$, $\mathcal{R}_\mathbb{Q}$ is a field, denoted by $\mathbf{K}$. It's ring of integers $\mathcal{O}_\mathbf{K}$ is the integral extension of $\mathcal{R}$, and is quite often not the same as $\mathcal{R}$.

Ideal. As shown in corollary 2.3.1, ideals of $\mathcal{R}$ are finitely generated. Thus, any ideal $\mathcal{I}$ can be given by a finite set of generators, say, $g_0, g_1, \ldots, g_{t-1} \in \mathcal{R}$ as

$$\begin{aligned}\mathcal{I} &= \{a_0 g_0 + a_1 g_1 + \ldots, a_{t-1} g_{t-1} \,|\, a_i \in \mathcal{R}\} \\ &= \left\{ \boldsymbol{C}_{g_0}\mathbf{a_0} + \boldsymbol{C}_{g_1}\mathbf{a_1} + \boldsymbol{C}_{g_{t-1}}\mathbf{a_{t-1}} \middle| \, \mathbf{a_i} \in \mathbb{Z}^n \right\} \\ &= \left\{ \left[\boldsymbol{C}_{g_0} | \boldsymbol{C}_{g_1} | \cdots | \boldsymbol{C}_{g_{t-1}}\right] \times \mathbf{a} \middle| \, \mathbf{a} \in \mathbb{Z}^{t \times n} \right\}\end{aligned}$$

It's not difficult to see that, one can derive an n-by-n integer basis matrix by computing the Hermite normal form of $\left[\boldsymbol{C}_{g_0} | \boldsymbol{C}_{g_1} | \cdots | \boldsymbol{C}_{g_{t-1}}\right]$, or simply by iteratively using the fact that Euclid's algorithm gives a unimodular transformation from $[a \;\; b]$ to $[\gcd(a, b) \;\; 0]$ (for any intgers a, b). We denote by $\boldsymbol{B}(\mathcal{I})$ the basis matrix of $\mathcal{I}$. Note that all basis matrices are close under integer unimodular transformation. Hence, their determinants are the same. Specifically, a *principal ideal* is an ideal generated by only one element g, whose basis matrix could be given as a circulant matrix $\boldsymbol{C}_g$.

If not explicitly mentioned, we focus on *full rank* ideals $\mathcal{I}$ whose basis matrix $\boldsymbol{B}(\mathcal{I})$ is invertible over $\mathbb{Q}$; this is always the case when $f(X)$ is irreducible. For any principal ideal given by $\boldsymbol{C}_g$, it means that $g(X)$ is invertible in $\mathcal{R}_\mathbb{Q}$.

The *(pseudo) inverse* of a full rank ideal $\mathcal{I}$ is defined as the following set:

$$\left\{ g(X) \in \mathcal{R}_\mathbb{Q} \middle| \, \forall h(X) \in \mathcal{I}, g(X) * h(X) \in \mathcal{R} \right\},$$

or equivalently $\{\mathbf{g} \in \mathbb{Q}^n \,|\, \mathcal{I}\mathbf{g} \in \mathbb{Z}^n\} = \left\{ \mathcal{I}^{-1}\mathbf{h} \middle| \, \mathbf{h} \in \mathbb{Z}^n \right\}$. The inverse of the basis matrix $\mathcal{I}^{-1}$ is integer except for a denominator $\det(\mathcal{I})$.

Ideal Lattice. Since an ideal $\mathcal{I}$ of $\mathcal{R}$ has a $\mathbb{Z}$-basis, say $\boldsymbol{B}(\mathcal{I})$, it defines a lattice in $\mathcal{R} \subseteq \mathcal{R}_\mathbb{Q}$. We can also embed this lattice in $\mathcal{H}$, and consider the embedding as a lattice in $\mathcal{H}$. The canonical embedding given by the Vandermonde matrix $\boldsymbol{V}$ of $f(X)$ naturally induces an *ideal lattice* $\mathcal{L}(\mathcal{I})$ in $\mathcal{H}$, given by matrix $\boldsymbol{V}\boldsymbol{B}(\mathcal{I})$.

Ideal Lattice Dual. For an ideal $\mathcal{I}$, the dual of its ideal lattice $\mathcal{L}(\mathcal{I})$ in $\mathcal{H}$ is defined to be

$$\begin{aligned}\mathcal{L}(\mathcal{I})^\vee &= \left\{\mathbf{y} \in \mathcal{H} | \, \forall \mathbf{x} \in \mathcal{L}(\mathcal{I}),\ \mathbf{y}^H \cdot \mathbf{x} \in \mathbb{Z}\right\} \\ &= \left\{\mathbf{y} \in \mathcal{H} | \, \forall \mathbf{z} \in \mathbb{Z}^n,\ \mathbf{y}^H \cdot \boldsymbol{V}\boldsymbol{B}(\mathcal{I})\mathbf{z} \in \mathbb{Z}\right\} \\ &= \left\{\boldsymbol{V}^{-H}\boldsymbol{B}(\mathcal{I})^{-H}\mathbf{z} \middle| \, \mathbf{z} \in \mathbb{Z}^n\right\}.\end{aligned}$$

As mentioned above, the basis $\boldsymbol{B}(\mathcal{I})$ also defines a lattice in $\mathcal{R}_\mathbb{Q}$, and one can define a dual of the ideal itself using *trace pairing*. Recall that we abuse the notation by denoting $\mathbf{a} * \mathbf{b}$ as the coefficients vector of polynomial $a(X) * b(X)$ modulo $f(X)$. The trace pairing of $a(X), b(X) \in \mathcal{R}_\mathbb{Q}$, $\mathrm{Tr}(a(X), b(X))$ is defined to be trace of $\boldsymbol{V} \times (\mathbf{a} * \mathbf{b})$ which is same as $(\boldsymbol{V}\mathbf{a})^\top \times (\boldsymbol{V}\mathbf{b})$. Thus, we can define the dual $\mathcal{I}^\vee$ of ideal $\mathcal{I}$ to be the set

$$\left\{b(X) \in \mathcal{R}_\mathbb{Q} \middle| \, \forall a(X) \in \mathcal{I},\ \mathrm{Tr}(a(X), b(X)) \in \mathbb{Z}\right\}.$$

Note that this is the pre-image in $\mathcal{R}_\mathbb{Q}$ of the complex conjugate of $\mathcal{L}(\mathcal{I})^\vee$. We prove below that this is indeed a (fractional) ideal of $\mathcal{R}$. Hence, we will refer to $\mathcal{I}^\vee$ as the **dual ideal** of $\mathcal{I}$.

Lemma 2.4.2. *For an ideal $\mathcal{I}$ of $\mathcal{R}$ with basis $\boldsymbol{B}(\mathcal{I})$* [6]*,*

i) *the dual $\mathcal{I}^\vee$ is the $\mathbb{Z}$-span of $(\boldsymbol{V}^\top\boldsymbol{V})^{-1}\boldsymbol{B}(\mathcal{I})^{-\top}$,*

ii) *the matrix $\det(\boldsymbol{B}(\mathcal{I})) \cdot \det(\boldsymbol{V}^\top\boldsymbol{V}) \cdot (\boldsymbol{V}^\top\boldsymbol{V})^{-1} \cdot \boldsymbol{B}(\mathcal{I})^{-\top}$ is an integer matrix,*

iii) *the dual $\mathcal{I}^\vee$ is a fractional ideal of $\mathcal{R}$.*

Proof. For part (i), since the dual $\mathcal{I}^\vee$ is the pre-image (under $\boldsymbol{V}$) of the complex conjugate of $\mathcal{L}(\mathcal{I})^\vee$, and the latter has $\mathbb{Z}$-basis $\boldsymbol{V}^{-H}\boldsymbol{B}(\mathcal{I})^{-H}$, the matrix $(\boldsymbol{V}^\top\boldsymbol{V})^{-1}\boldsymbol{B}(\mathcal{I})^{-\top}$ forms a $\mathbb{Z}$-basis for $\mathcal{I}^\vee$.

For part (ii), we only need to show that $(\boldsymbol{V}^\top\boldsymbol{V})$ is integer, since $\boldsymbol{B}(\mathcal{I})$ is always an integer matrix for $\mathcal{I} \subseteq \mathcal{R}$. Consider its entry $(\boldsymbol{V}^\top\boldsymbol{V})_{i,j} = \sum_{k=0}^{n-1} z_k^{i+j}$. We argue that the power sums

[6] This lemma actually holds for any sub-ring of $\mathcal{R}_\mathbb{Q}$, e.g. the ring of integers of a number field with $f(X)$ irreducible over $\mathbb{Q}$.

of roots, $p_t = \sum_{k=0}^{n-1} z_k^t$, is an integer for $0 \leq t \leq 2n$. Note that the coefficients of $f(X) = \prod_{t=0}^{n-1}(X - z_t) = \sum_{t=0}^{n} e_t X^t$ are elementary symmetric polynomials $e_t = e_t(z_0, \ldots, z_{n-1})$ in the roots of $f(X)$. Starting from $p_0 = n$ and $p_1 = e_1 \in \mathbb{Z}$, by Newton's identity, every power sum p_t is an integer linear combination of $\{p_0, \ldots, p_{t-1}\}$ and $\left\{e_0, \ldots, e_{\min(t,n)}\right\}$.

Now we prove (iii). We need to show that for every $\mathbf{g} \in \mathcal{R}$ and $\mathbf{a} \in \mathcal{I}^\vee$, $\mathbf{g} * \mathbf{a}$ is in $\mathcal{I}^\vee$, i.e. for all $\mathbf{b} \in \mathcal{I}$, $\mathrm{Tr}(\mathbf{g} * \mathbf{a} * \mathbf{b})$ is integer. By commutativity of polynomial multiplication, this is same as requiring that $\mathrm{Tr}(\mathbf{a} * \mathbf{g} * \mathbf{b})$ is integer. But $\mathbf{c} = \mathbf{g} * \mathbf{b}$ is in $\mathcal{I}$, as it is an ideal, and hence $\mathrm{Tr}(\mathbf{a} * \mathbf{c})$ is an integer as $\mathbf{a}$ is in $\mathcal{I}^\vee$ and $\mathbf{c}$ is in $\mathcal{I}$. Thus, $\mathcal{I}^\vee$ is closed under multiplication by $\mathcal{R}$. Now, again by commutativity, for every $\mathbf{d} \in \mathcal{R}$, $\mathbf{d}\mathcal{I}^\vee$ is also closed under multiplication by $\mathcal{R}$. Thus (iii) follows from (i) and (ii). □

The Dual (of the) Ring. When the entire ring $\mathcal{R}$ is considered as an ideal, its dual $\mathcal{R}^\vee$, by lemma 2.4.2, is a fractional ideal given by the $\mathbb{Z}$-basis matrix $(\boldsymbol{V}^\top \boldsymbol{V})^{-1}$. and is referred to as the **dual ring**[7] $\mathcal{R}^\vee$.

Let $f(X) = \sum_{i=0}^{n} f_i \cdot X^i$ with $f_n = 1$. Take its derivative $f'(X) = \sum_{i=0}^{n-1}(i+1) \cdot f_{i+1} \cdot X^i$. First, notice that $f'(X)$ is invertible in $\mathcal{R}_\mathbb{Q} = \mathbb{Q}[X]/(f(X))$.

Proposition 2.4.2. *Given $f(X)$ with all distinct roots, its derivative $f'(X)$ shares no common root with $f(X)$.*

Proof. If $f(X)$ and $f'(X)$ share the same root $a \in \mathbb{C}$,

$$f(X) = (X - a)p(X) \text{ and } f'(X) = (X - a)q(X).$$

We take the derivative for the first equation

$$\begin{aligned}(X - a)p'(X) + p(X) &= (X - a)q(X) \\ p(X) &= (X - a)\left(q(X) - p'(X)\right).\end{aligned}$$

[7]This is really a misnomer, as $\mathcal{R}^\vee$ is not closed under multiplication by $\mathcal{R}^\vee$, but only closed under multiplication by $\mathcal{R}$. Hence it is not a ring, but merely a $\mathcal{R}$-module. We will continue to call this the dual ring as in [DD12].

Therefore $p(X)$ has a as a root, and a is (at least) a double root of $f(X)$. It contradicts the assumption that $f(X)$ has distinct roots. □

When $f(X)$ is irreducible over $\mathbb{Q}$, it is known that $f(X)$ has distinct roots over the complex numbers.

We now show that, the dual $\mathcal{R}^\vee$ has the circulant matrix of the inverse of $f'(X)$ as a $\mathbb{Z}$-basis, and since $\mathcal{R}^\vee$ is also a fractional ideal of $\mathcal{R}$, it can also be seen as the fractional ideal [8] generated by the inverse of $f'(X)$. More precisely, the basis matrix $(\boldsymbol{V}^\top \boldsymbol{V})^{-1}$ is same as $\boldsymbol{C}_{f'}^{-1}\boldsymbol{M}$, where $\boldsymbol{M}$ is the following n-by-n unimodular matrix:

$$\boldsymbol{M} = \begin{bmatrix} f_1 & f_2 & \cdots & f_n \\ f_2 & \ddots & f_n & 0 \\ \vdots & f_n & \ddots & \vdots \\ f_n & 0 & \cdots & 0 \end{bmatrix}$$

i.e. where $\boldsymbol{M}_{i,j} = f_{i+j+1}$ if $i + j < n$ and $\boldsymbol{M}_{i,j} = 0$ otherwise.

Lemma 2.4.3. $(\boldsymbol{V}^\top \boldsymbol{V})^{-1} = \boldsymbol{C}_{f'}^{-1}\boldsymbol{M}$.

Proof. It suffices to show that $\boldsymbol{M} \times \boldsymbol{V}^\top \boldsymbol{V} = \boldsymbol{C}_{f'}$. This is equivalent to

$$\boldsymbol{V}\boldsymbol{M}\boldsymbol{V}^\top \boldsymbol{V}\boldsymbol{V}^{-1} = \boldsymbol{V}\boldsymbol{C}_{f'}\boldsymbol{V}^{-1}$$
$$\boldsymbol{V}\boldsymbol{M}\boldsymbol{V}^\top = \boldsymbol{D}_{f'}.$$

Here $\boldsymbol{D}_{f'}$ is a diagonal matrix with $(\boldsymbol{D}_{f'})_{i,i} = f'(z_i)$ where z_i's are (complex) roots of $f(X)$. Next we verify that

$$(\boldsymbol{V}\boldsymbol{M}\boldsymbol{V}^\top)_{i,j} = \sum_{s=0}^{n-1} \sum_{t=0}^{n-s-1} f_{s+t+1} \cdot z_i^s \cdot z_j^t = \sum_{p=0}^{n-1} f_{p+1} \cdot \left(\sum_{s=0}^{p} z_i^s z_j^{p-s} \right)$$

[8] It is well known [Cone] that the dual $\mathcal{O}_K^\vee$ of the ring of integers $\mathcal{O}_K$ of a number field K is *not* always generated by the inverse of $f'(X)$.

If $i = j$, we have

$$(\boldsymbol{V}\boldsymbol{M}\boldsymbol{V}^\top)_{i,i} = \sum_{p=0}^{n-1} f_{p+1} \cdot \sum_{s=0}^{p} z_i^p = \sum_{p=0}^{n-1} f_{p+1} \cdot (p+1) \cdot z_i^p = f'(z_i).$$

Otherwise when $i \neq j$, we have

$$\begin{aligned}(\boldsymbol{V}\boldsymbol{M}\boldsymbol{V}^\top)_{i,j} &= \sum_{p=0}^{n-1} f_{p+1} \cdot \left(\sum_{s=0}^{p} z_i^s z_j^{p-s} \right) = \sum_{p=0}^{n-1} f_{p+1} \cdot \left(\frac{z_i^{p+1} - z_j^{p+1}}{z_i - z_j} \right) \\ &= \frac{f(z_i) - f_0 - f(z_j) + f_0}{z_i - z_j} = 0.\end{aligned}$$

□

Corollary 2.4.3. *For monic $f(X)$, $\Delta_f = |\det(\boldsymbol{C}_{f'})|$.*

Moreover, this particular matrix $\boldsymbol{M}$ also has an interesting property, that it symmetricizes every circulant matrices by right multiplication:

Proposition 2.4.3. *For $g(X) \in \mathcal{R}_{\mathbb{Q}}$, $\boldsymbol{C}_g\boldsymbol{M}$ is symmetric.*

Proof. Recall that the circulant matrix $\boldsymbol{C}_g$ is diagonalized by similarity transformation of the Vandermonde matrix $\boldsymbol{V}$ of $f(X)$: $\boldsymbol{D}_g = \boldsymbol{V}\boldsymbol{C}_g\boldsymbol{V}^{-1}$.Thus,

$$\begin{aligned}\boldsymbol{C}_g\boldsymbol{M} &= \boldsymbol{C}_{f'} \times \boldsymbol{C}_{f'}^{-1}\boldsymbol{C}_g\boldsymbol{M} \\ &= \boldsymbol{C}_{f'} \times \boldsymbol{C}_g \times \boldsymbol{C}_{f'}^{-1}\boldsymbol{M} \\ &= \boldsymbol{C}_{f'} \times \boldsymbol{C}_g \times (\boldsymbol{V}^\top\boldsymbol{V})^{-1} \\ &= \boldsymbol{C}_{f'}(\boldsymbol{V}^\top\boldsymbol{V})^{-1} \times \boldsymbol{V}^\top\boldsymbol{V}\boldsymbol{C}_g(\boldsymbol{V}^\top\boldsymbol{V})^{-1} \\ &= \boldsymbol{M} \times \boldsymbol{V}^\top\boldsymbol{D}_g\boldsymbol{V}^{-\top} \\ &= \boldsymbol{M}\boldsymbol{C}_g^\top\end{aligned}$$

We claim that $\boldsymbol{C}_g\boldsymbol{M}$ is symmetric since $\boldsymbol{M}$ is symmetric. □

Lemma 2.4.4. *For an ideal $\mathcal{I}$ of $\mathcal{R}$, for any $\mathbf{a} \in \mathcal{I}$ and any $\mathbf{b} \in \mathcal{I}^\vee$, $\mathbf{a} * \mathbf{b} \in \mathcal{R}^\vee$.*

Proof. Since by lemma 2.4.2, $\mathcal{I}^\vee$ is a (fractional ideal), for any $\mathbf{c} \in \mathcal{R}$, $\mathbf{b} * \mathbf{c}$ is also in $\mathcal{I}^\vee$. Thus, by definition of the dual-ideal (applied to dual of $\mathcal{I}$), $\mathrm{Tr}(\mathbf{a}, \mathbf{b} * \mathbf{c}) \in \mathbb{Z}$. Since this trace is same as trace of $\boldsymbol{V} \times (\mathbf{a} * \mathbf{b} * \mathbf{c})$, this also implies that $\mathrm{Tr}(\mathbf{a} * \mathbf{b}, \mathbf{c}) \in \mathbb{Z}$. Since this holds for all $\mathbf{c} \in \mathcal{R}$, again by definition of dual ideal (applied to dual of $\mathcal{R}$), $\mathbf{a} * \mathbf{b}$ is in dual of $\mathcal{R}$, i.e. $\mathcal{R}^\vee$. □

Proposition 2.4.4. *For $g(X) \in \mathcal{R}_\mathbb{Q}$, we have $\boldsymbol{C}_g(\boldsymbol{V}^\top\boldsymbol{V})^{-1} = (\boldsymbol{V}^\top\boldsymbol{V})^{-1}\boldsymbol{C}_g^\top$, and $(\boldsymbol{V}^\top\boldsymbol{V})\boldsymbol{C}_g = \boldsymbol{C}_g^\top(\boldsymbol{V}^\top\boldsymbol{V})$.*

Proof. Note that the Vandermonde matrix $\boldsymbol{V}$ diagonalizes the circulant matrix $\boldsymbol{V}\boldsymbol{C}_g\boldsymbol{V}^{-1} = \boldsymbol{D}_g$:

$$\boldsymbol{V}^\top\boldsymbol{V}\boldsymbol{C}_g = \boldsymbol{V}^\top\boldsymbol{D}_g\boldsymbol{V} = \boldsymbol{V}^\top\boldsymbol{D}_g^\top\boldsymbol{V} = (\boldsymbol{D}_g\boldsymbol{V})^\top\boldsymbol{V} = (\boldsymbol{V}\boldsymbol{C}_g)^\top\boldsymbol{V} = \boldsymbol{C}_g^\top\boldsymbol{V}^T\boldsymbol{V}.$$

□

Corollary 2.4.4. *For any principal ideal $\mathfrak{a}$ of $\mathcal{R}$, $\mathfrak{a}^\vee = \mathfrak{a}^{-1}\mathcal{R}^\vee$.*

Proof. Let $\mathbf{g}$ be a generator of the principal ideal $\mathfrak{a}$. By lemma 2.4.2, $(\boldsymbol{V}^\top\boldsymbol{V})^{-1}\boldsymbol{C}_g^{-\top}$ is a $\mathbb{Z}$-basis of the dual ideal $\mathfrak{a}^\vee$. By proposition 2.4.4, this is same as $\boldsymbol{C}_g^{-1}(\boldsymbol{V}^\top\boldsymbol{V})^{-1}$. Since $(\boldsymbol{V}^\top\boldsymbol{V})^{-1}$ is a $\mathbb{Z}$-basis for $\mathcal{R}^\vee$, the claim follows. □

This corollary, along with lemma 2.4.4, will be used in proving the ideal clearing lemma.

We also give a counterpart of lemma 2.9 of [LPR10] (which in turn uses [PR07]).

Lemma 2.4.5. *For any ideal $\mathcal{I}$ of $\mathcal{R}_\mathbf{K}$, with $\mathbf{K}$ a degree n extension of $\mathbb{Q}$,*

$$\sqrt{n}det(\mathcal{I})^{1/n} \leq \lambda_1(\mathcal{I}) \leq \sqrt{n}det(\mathcal{I})^{1/n}\sqrt{\Delta_\mathbf{K}^{1/n}}$$

Corollary 2.4.5. *The $\mathbb{Z}$-span of the matrix $\det(\mathcal{I}) \cdot \det(\boldsymbol{V}^\top\boldsymbol{V}) \cdot (\boldsymbol{V}^\top\boldsymbol{V})^{-1} \cdot \mathcal{I}^{-\top}$ is an ideal of $\mathcal{R}$, i.e. $\mathcal{I}^\vee$ is a fractional ideal of $\mathcal{R}$.*

Proof. First of all, by lemma 2.4.2 the $\mathbb{Z}$-span of $\det(\mathcal{I}) \cdot \det(\boldsymbol{V}^\top \boldsymbol{V}) \cdot \mathcal{I}^\vee$ is in $\mathbb{Z}^n$ and hence in $\mathcal{R}$. We need to show that for every $g \in \mathcal{R}$ and $a \in \mathcal{I}^\vee$, $g * a = \boldsymbol{C}_g a$ is in $\mathcal{I}^\vee$, or equivalently the conjugate of $\boldsymbol{V}\boldsymbol{C}_g a$ is in $\mathcal{L}(\mathcal{I})^\vee$. Since, $\mathcal{I}^\vee$ is defined to be the $\mathbb{Z}$-span of $(\boldsymbol{V}^\top \boldsymbol{V})^{-1} \cdot \mathcal{I}^{-\top}$, a can be written as $(\boldsymbol{V}^\top \boldsymbol{V})^{-1} \cdot \mathcal{I}^{-\top} y$, for some $y \in \mathbb{Z}^n$. Then, checking that conjugate of $\boldsymbol{V}\boldsymbol{C}_g a$ is in $\mathcal{L}(\mathcal{I})^\vee$ is, by definition of the lattice dual, same as checking that for all $x \in \mathbb{Z}^n$,

$$y^\top \mathcal{I}^{-1} (\boldsymbol{V}^\top \boldsymbol{V})^{-\top} \boldsymbol{C}_g^\top \boldsymbol{V}^\top \boldsymbol{V} \mathcal{I} x \ \in \mathbb{Z}$$

By proposition 2.4.4, $\boldsymbol{C}_g^\top \boldsymbol{V}^\top \boldsymbol{V}$ is same as $\boldsymbol{V}^\top \boldsymbol{V} \boldsymbol{C}_g$, and since $(\boldsymbol{V}^\top \boldsymbol{V})^\top$ is same as $\boldsymbol{V}^\top \boldsymbol{V}$, the term above simplifies to $y^\top \mathcal{I}^{-1} \boldsymbol{C}_g \mathcal{I} x$. Now, noting that $\mathcal{I}$ is an ideal and hence $\boldsymbol{C}_g \mathcal{I} x = \mathcal{I} x'$ for some $x' \in \mathbb{Z}^n$, the corollary follows. □

2.5 Principal Ideal Ring Theorem for Dedekind-special Modular Polynomials

In this section we will show that for special $f(X)$ and primes p, we can prove that the ring $\mathcal{R}$ modulo p^r, for any positive integer r, is a principal ideal ring (PIR). Moreover, we show that every ideal $\mathfrak{a}$ of $\mathcal{R}$, modulo the ideal $p^r \mathfrak{a}$, is principal. Normally, such a claim holds for Dedekind domains, and the proofs require the unique prime decomposition theorem for Dedekind domains. We show that even if the ring is not a Dedekind domain, for some commonly used Noetherian rings, it can directly be shown that the ring $\mathcal{R}$ modulo p^r is a PIR, and further, every ideal $\mathfrak{a}$ is principal modulo $p^r \mathfrak{a}$.

Let p be a prime such that in the factorization of $f(X)$ modulo p in terms of irreducible polynomials (mod p), i.e.

$$f(X) = \prod_{i=1}^{m} h_i(X)^{e_i} + p * t(X),$$

for all $i \in [m]$, for which e_i is more than one, it is the case that $t(X)$ is invertible modulo the ideal $(p, h_i(X))$ of $\mathbb{Z}[X]$. In other words, for all i such that $h_i(X)$ has multiplicity more than one, it is the case that $t(X)$ is not divisible by $h_i(X)$ modulo p. The *Dedekind index theorem* (theorem 2.3.3) states that for irreducible (over $\mathbb{Q}[X]$) $f(X)$ and such primes p, prime p does not divide $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}]$.

Here, as usual, $O_{\mathbf{K}}$ is the ring of integers[9] of the number field $\mathbf{K} = \mathbb{Q}[X]/(f(X))$, and $\mathcal{R}$, i.e. $\mathbb{Z}[X]/(f(X))$, is a sub-ring of $O_{\mathbf{K}}$.

Consider a polynomial $f(X)$, *not* necessarily irreducible over $Z[X]$. For any prime p such that the factorization of $f(X)$ modulo p has the above property, the pair $(f(X), p)$ will be called a **Dedekind-special modular polynomial**. The polynomial $t(X)$ (more precisely, its representative in $\mathbb{Z}_p[X]$) will be referred to as the **quotient** in the factorization of $f(X)$ modulo p. In this section we will fix the pair $(f(X), p)$ to be a Dedekind-special modular polynomial, and as usual, $\mathcal{R}$ will stand for the ring $\mathbb{Z}[X]/(f(X))$.

For each $i \in [m]$, define the following ideals $\mathfrak{p}_i$ of $\mathcal{R}$: $\mathfrak{p}_i = (h_i(X), p)$. Also, define the following ideals $\mathfrak{s}_i$ of $\mathcal{R}$: $\mathfrak{s}_i = (h_i(X)^{e_i}, p)$.

Lemma 2.5.1. *In the ring $\mathcal{R}$, for $i \in [m]$,*

(i) *the ideal $\mathfrak{p}_i$ is maximal.*

(ii) $\mathfrak{s}_i = \mathfrak{p}_i^{e_i}$.

Proof. (*i*) The proof is straightforward by noting that $h_i(X)$ is irreducible modulo p.

(*ii*) If $e_i = 1$, there is nothing to prove. Otherwise, $\mathfrak{p}_i^{e_i}$ is contained in $\mathfrak{s}_i = (h_i(X)^{e_i}, p)$ follows simply because the only term in $\mathfrak{p}_i^{e_i}$ that is not in (p) is $h_i(X)^{e_i}$. For the other direction, we only need to show that p is contained in $\mathfrak{p}_i^{e_i}$. We show that $p \in (h_i(X)^{e_i}, p * h_i(X)^{e_i-1}, p^{e_i}) \subseteq \mathfrak{p}_i^{e_i}$. Note that ideal $(h_i(X)^{e_i})$ contains $p * t(X)$ by the factorization of $f(X)$, and where $t(X)$ is the quotient in the factorization. Moreover, by the Dedekind-special property of modular polynomial $(f(X), p)$, and given that $e_i \geq 2$, $t(X)$ is not in $(h_i(X), p) = \mathfrak{p}_i$. Thus, since $\mathfrak{p}_i$ is maximal by (i), $t(X)$ is invertible modulo $(h_i(X), p)$. Then, by lemma 2.3.2, $t(X)$ is invertible modulo $(h_i(X)^{e_i-1}, p^{e_i-1})$. Thus, $(t(X), h_i(X)^{e_i-1}, p^{e_i-1}) = (1)$, and further $p * (t(X), h_i(X)^{e_i-1}, p^{e_i-1}) = (p)$, and the claim follows.

□

[9]The ring of integers O_K is potentially an extension of the ring $\mathbb{Z}[X]/(f(X))$, as it contains all elements of $\mathbb{Q}[X]/(f(X))$ that satisfy a polynomial relation with integer coefficients.

The proof of the following two lemmas is similar to that of the proof of lemma 2.5.1(ii).

Lemma 2.5.2. *In the ring $\mathcal{R}$, let $w = \sum_{i=1}^{m} e_i$. If $w \geq 2$, and some $e_i = 1$ (w.l.o.g. $e_m = 1$), then $p^{w-2} * h_m(X)$ is invertible modulo the ideal $(p^{w-1}, \prod_{j=1}^{m-1} h_j(X)^{e_j})$.*

Proof. The case $w = 2$ is implied by the above lemma 2.5.1 and lemma 2.3.2. So, we focus on $w > 2$. Since all $h_i(X)$ are irreducible and distinct, by using the extended Euclidean algorithm in $\mathbb{Z}[X]$, we have

$$\mu(X)p^{w-2}h_m(X) + \lambda(X)\prod_{j=1}^{m-1} h_j(X)^{e_j} = c,$$

for some non-trivial polynomials $\mu(X)$ and $\lambda(X)$ and an integer c. If c is a multiple of the prime p, then $\lambda(X)\prod_{j=1}^{m-1} h_j(X)^{e_j}$ is zero modulo p. Since $\lambda(X)$ is non-trivial this implies that one of $h_j(X)$ is zero modulo p, which is impossible. Thus, $(c, p) = 1$, and hence

$$\mu'(X)p^{w-2}h_m(X) + \lambda'(X)\prod_{j=1}^{m-1} h_j(X)^{e_j} = 1 - \nu p,$$

for some non-trivial polynomials $\mu'(X)$ and $\lambda'(X)$ and an integer ν. Multiplying both sides by $1 + \nu p + ... + (\nu p)^{w-2}$, we have

$$\mu''(X)p^{w-2}h_m(X) + \lambda''(X)\prod_{j=1}^{m-1} h_j(X)^{e_j} = 1 - \nu^{w-1}p^{w-1},$$

for some non-trivial polynomials $\mu''(X)$ and $\lambda''(X)$, and that concludes the proof. □

Lemma 2.5.3. *Let $w = \sum_{i=1}^{m} e_i$. If for all $i \in [m]$, $e_i > 1$, then $t(X)$, the quotient in the factorization of $f(X)$ modulo p, is invertible modulo the ideal $(p^{w-1}, p^{w-2}h_m(X))$.*

Proof. By the Dedekind-special property of $(f(X), p)$, $t(X)$ is not in any $\mathfrak{p}_i$, and hence not in $\mathfrak{p}_m$. Since all $h_1(X)$ is irreducible, an $t(X)$ is not in $(p, h_m(X))$, by using the extended Euclidean algorithm in $\mathbb{Z}[X]$, we have

$$\mu(X)p^{w-2}h_m(X) + \lambda(X)t(X) = c,$$

for some non-trivial polynomials $\mu(X)$ and $\lambda(X)$ and an integer c. If c is a multiple of the prime p, then $\lambda(X)t(X)$ is zero modulo p. Since $\lambda(X)$ is non-trivial this implies that one of $t(X)$ is zero modulo p, which is impossible by the Dedekind-special property. Thus, $(c, p) = 1$, and we conclude using the same argument as in the previous lemma. □

Remark. In the ring of integers $\mathcal{O}_{\mathbf{K}}$ of the number field $\mathbf{K} = \mathbb{Q}[X]/(f(X))$, another theorem of Dedekind gives a similar factorization of the ideal (p) as in the lemma below, when the Dedekind-special property holds for modular polynomial $(f(X), p)$.

The following lemma is proved using lemma 2.5.2 and lemma 2.5.3.

Lemma 2.5.4. *In the ring $\mathcal{R}$, the ideal (p) is same as $\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}...\mathfrak{p}_m^{e_m}$.*

Proof. $\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}...\mathfrak{p}_m^{e_m}$ is subset of (p); this is easy to see since all but one generators in $\prod_{i=1}^{m}(h_i(X)^{e_i}, p)$ are trivially in (p). The last generator $\prod_{i=1}^{m} h_i(X)^{e_i}$ is also in (p), because it is same as $f(X)$ modulo p, which is zero in $\mathcal{R}$ modulo p.

For the other direction, first consider the case where for all $i \in [m]$, $e_i > 1$. We show that the three terms in $\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}...\mathfrak{p}_m^{e_m}$, namely p^w, $p^{w-1}\mathfrak{p}_m$, and $\prod_{i=1}^{m} h_i(X)^{e_i}$ generate p. The last term is same as $p \cdot t(X)$ (by the factorization of $f(X)$ mod p). Thus, taking p as a common factor, the three terms generate $p \cdot 1$ by lemma 2.5.3.

Now, consider the case that there is some i such that $e_i = 1$, w.l.o.g. $e_m = 1$. If $m = 1$ and hence $e_1 = 1$, we have that (p) itself is maximal as every element in $\mathcal{R}$ not in (p) is invertible modulo p. For $m \geq 2$, we show that p is generated by $\prod_{i=1}^{m}(h_i(X), p)^{e_i}$ in $\mathcal{R}$. Let $w = \sum_{i=1}^{m} e_i$. Pick the generators $p^{w-1} * h_m(X)$, $p * \prod_{j=1}^{m-1} h_j(X)^{e_j}(X)$ and p^w from $\prod_{i=1}^{m}(h_i(X), p)^{e_i}$. Taking a common factor p out, we focus on the generators $p^{w-2} * h_m(X)$, $\prod_{j=1}^{m-1} h_j(X)^{e_j}$ and p^{w-1}. An easy application of the lemma 2.5.2 shows these three generators generate 1. □

Theorem 2.5.1. *For any positive integer r,*

$$\mathbb{Z}_{p^r}[X]/(f(X)) \;\cong\; \mathcal{R}/p^r\mathcal{R} \;\cong\; \mathcal{R}/\prod_{i=1}^{m}\mathfrak{p}_i^{r\cdot e_i} \;\cong\; \prod_{i=1}^{m}\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i}$$

Proof. We focus on the second and third congruence, as the first is straight forward. The second congruence follows directly from lemma 2.5.4. Since the powers of co-prime ideals are also co-prime, we apply CRT (of general rings and co-prime ideals) to conclude the proof. □

The rest of the section is devoted to proving that $\mathcal{R}/\mathfrak{p}_i^r$ is a principal ideal ring (PIR) (Theorem 2.5.2 below), and any ideal $\mathfrak{a}$ is principal modulo $p^r\mathfrak{a}$ (Theorem 2.5.3). If $\mathcal{R}$ was a Dedekind domain, the usual proof goes as follows: One first shows that $\mathcal{R}/\mathfrak{p}_i^r$ is isomorphic to $\mathcal{R}_{\mathfrak{p}_i}/\mathfrak{p}_i^r\mathcal{R}_{\mathfrak{p}_i}$, where $\mathcal{R}_{\mathfrak{p}_i}$ is the *localization* of $\mathcal{R}$ at the ideal $\mathfrak{p}_i^r$. If the reader is not familiar with localization, he/she can skip this discussion, as the direct proof we give *does not* use localization. Next, it is shown that the local ring $\mathcal{R}_{\mathfrak{p}_i}$ is a principal ideal domain (PID) by showing that it is a discrete valuation ring (DVR). This step requires the prime ideal decomposition theorem for Dedekind domains. Since the quotient ring of a PID is a PID, the claim follows.

While our ring $\mathcal{R}$ may not be a Dedekind domain, most of the above steps would still go through for our special $f(X)$ and p, except for proving that $\mathcal{R}_{\mathfrak{p}_i}$ is a DVR, which is usually proved using the prime ideal decomposition theorem for Dedekind domains. Luckily, in our special case, we can still prove $\mathcal{R}_{\mathfrak{p}_i}$ is a DVR without the decomposition theorem for Dedekind Domains. As promised, we give a direct proof of Theorem 2.5.2. The proof of Theorem 2.5.3 is slightly more involved and uses the Krull intersection theorem for Noetherian rings.

Theorem 2.5.2. *For all $i \in [m]$, for all positive integers $r > 0$, $\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i}$ is a principal ideal ring.*

Proof. Let $\mathfrak{q}$ be any ideal of $\mathcal{R}/\mathfrak{p}_i^r$. We first show that every ideal $\mathfrak{q}$ of $\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i}$ that is not a sub-ideal of $(h_i(X), p)$ (as an ideal of $\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i}$) is same as ideal (1) of $\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i}$, and hence trivially principal. By lemma 2.5.1, $\mathfrak{p}_i$ is maximal in $\mathcal{R}$. Thus, by lemma 2.3.2 any $a(X) \in \mathcal{R}$ that is not in the maximal ideal $\mathfrak{p}_i = (h_i(X), p)$ is invertible modulo $\mathfrak{p}_i$, and also invertible modulo $\mathfrak{p}_i^{r\cdot e_i}$. If $\mathfrak{q}$ is not a sub-ideal of $(h_i(X), p)\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i}$, then there is an element $a(X)$ in $\mathfrak{q}$ that is not in $(h_i(X), p)\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i}$. Thus $a(X)$ is not in $(h_i(X), p)\mathcal{R}$ and hence is a unit of $\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i}$, making $\mathfrak{q}$ same as (1).

So, now we focus on ideals $\mathfrak{q}$ that are sub-ideals of $(h_i(X), p)$. We first show that the ideal $(h_i(X), p)$ is principal in $\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i}$. There are two cases:

1. $e_i = 1$:

   In this case, we show that $(h_i(X), p)$ is same as ideal (p) in $\mathcal{R}/\mathfrak{p}_i^{r \cdot e_i}$. For this, we show that $h_i(X)$ is generated by p modulo $\mathfrak{p}_i^{r \cdot e_i}$. From the factorization of $f(X)$ modulo p, we know that

   $$h_i(X) * \prod_{j \in [m], j \neq i} h_j(X)^{e_j} = p * t(X),$$

   in $\mathcal{R}$, for some polynomial $t(X)$. Moreover, each of the irreducible polynomials $h_j(X)$, $j \in [m], j \neq i$ is not in $(h_i(X), p)$ because $Z_p[X]$ is a UFD, and hence is invertible modulo $\mathfrak{p}_i^{r \cdot e_i}$ by lemma 2.3.2. Thus $h_i(X)$ is generated by p modulo $\mathfrak{p}_i^{r \cdot e_i}$.

2. $e_i > 1$: In this case, we show that $(h_i(X), p)$ is same as ideal $(h_i(X))$ in $\mathcal{R}/\mathfrak{p}_i^{r \cdot e_i}$. For this, we show that p is generated by $h_i(X)$ modulo $\mathfrak{p}_i^{r \cdot e_i}$. From the factorization of $f(X)$ modulo p, we know that

   $$h_i(X)^{e_i} * \prod_{j \in [m], j \neq i} h_j(X)^{e_j} = p * t(X),$$

   in $\mathcal{R}$, for some polynomial $t(X)$. Moreover, because $(f(X), p)$ is a Dedekind-special modular polynomial, $t(X)$ is invertible modulo $\mathfrak{p}_i = (h_i(X), p)$. But, since $\mathfrak{p}_i$ is maximal, $t(X)$ is also invertible modulo $\mathfrak{p}_i = (h_i(X), p)^{r \cdot e_i}$. Thus, p is generated by $h_i(X)^{e_i}$ modulo $\mathfrak{p}_i^{r \cdot e_i}$, and hence also generated by $h_i(X)$ modulo $\mathfrak{p}_i^{r \cdot e_i}$.

Thus, $(h_i(X), p)$ is a principal ideal of $\mathcal{R}/\mathfrak{p}_i^{r \cdot e_i}$. Let g stand for this single generator of $(h_i(X), p)$, i.e. $g = p$ when $e_i = 1$ and $g = h_i(X)$ when $e_i > 1$. Hence, every ideal $\mathfrak{q}$ that is a sub-ideal of $(h_i(X), p)$, is a sub-ideal of (g). For any non-zero element a in $\mathfrak{q}$, let t_a be the largest integer greater than zero such that $a \in (g)^{t_a}$. Note $t_a < r \cdot e_i$, for otherwise a is zero in $\mathcal{R}/\mathfrak{p}_i^{r \cdot e_i}$. Thus, all elements of $\mathfrak{q}$ are in some ideal $(g)^t$, with $0 < t < r \cdot e_i$. Let t_q be the minimum of these t. Note $1 \leq t_q < r \cdot e_i$. We now show that $\mathfrak{q} = (g)^{t_q}$. Consider an element of a of $\mathfrak{q}$ that is in $(g)^{t_q}$. Then, a can be written as $g^{t_q} * a'$, where a' is not in the maximal ideal $(h(X), p)$ of $\mathcal{R}$. Hence, as before, a' is invertible in $\mathcal{R}/\mathfrak{p}_i^{r \cdot e_i}$, and thus g^{t_q} is in $\mathfrak{q}$. This shows that $\mathfrak{q} = (g)^{t_q}$, which makes it a principal ideal. □

Corollary 2.5.1. *$\mathbb{Z}_{p^r}[X]/(f(X))$ is a principal ideal ring.*

Proof. Follows by theorems 2.5.1 and 2.5.2 as product of principal ideal rings is a principal ideal ring. □

Lemma 2.5.5. *If $f(X)$ is irreducible as a polynomial in $\mathbb{Z}[X]$, then any ideal $\mathfrak{a}$ of $\mathcal{R} = \mathbb{Z}[X]/(f(X))$ can be written as $\hat{\mathfrak{a}} \prod_{i\in[m]} \mathfrak{p}_i^{t_i}$, where t_i are non-negative integers, and $\hat{\mathfrak{a}}$ is an ideal of $\mathcal{R}$ co-prime to every $\mathfrak{p}_i$ $(i \in [m])$.*

Proof. If $\mathfrak{a}$ is co-prime to every $\mathfrak{p}_i$ $(i \in [m])$, then t_i can be taken to be zero, and we are done. Otherwise, let $I \subseteq [m]$ be the non-empty and maximal set of indices i, $i \in [m]$, such that $\mathfrak{a}$ is not co-prime to $\mathfrak{p}_i$. Since each $\mathfrak{p}_i$ is maximal (by lemma 2.5.1), this implies that $\mathfrak{a}$ is a subset of each of $\mathfrak{p}_i$ $(i \in I)$. For each $i \in I$, let $t(i) > 0$ be the largest integer such that $\mathfrak{a}$ is a subset of $\mathfrak{p}_i^{t(i)}$. Such a $t(i)$ is well-defined by corollary to Krull intersection theorem (Corollary 2.3.2), noting that $\mathcal{R}$ is also an integral domain.

We show that there exists an ideal $\hat{\mathfrak{a}}$ such that $\mathfrak{a} = \hat{\mathfrak{a}} * \prod_{i\in I} \mathfrak{p}_i^{t(i)}$.

Let $T = \sum_{i\in I} t(i)$. Define $\hat{\mathfrak{a}}$ to be the *fractional* ideal

$$p^{-T} * \mathfrak{a} * \left(\prod_{i\in I} \prod_{j\in[m], j\neq i} \mathfrak{p}_j^{t(i)} \right).$$

Using lemma 2.5.4, it is straightforward to check that $\hat{\mathfrak{a}} * (\prod_{i\in I} \mathfrak{p}_i^{t(i)}) = \mathfrak{a}$.

We now show that $\hat{\mathfrak{a}}$ is actually an integral ideal, i.e. an ideal of $\mathcal{R}$. We will show that $\mathfrak{a} * \left(\prod_{i\in I} \prod_{j\in[m], j\neq i} \mathfrak{p}_j^{t(i)}\right)$ is in $(p)^T$. Since, for all $i \in I$, $\mathfrak{a}$ is in $\mathfrak{p}_i^{t(i)}$, $\mathfrak{a} \subseteq \cap_{i\in I} \mathfrak{p}_i^{t(i)}$. But, these ideals $\mathfrak{p}_i^{t(i)}$ are all co-prime, and hence $\mathfrak{a} \subseteq \prod_{i\in I} \mathfrak{p}_i^{t(i)}$. We next show that for all $i \in I$, $\mathfrak{p}_i^{t(i)} * \prod_{j\in[m], j\neq i} \mathfrak{p}_j^{t(i)}$ is in $(p)^{t(i)}$. But, this is clear from the factorization of (p) given by lemma 2.5.4.

Claim: Ideal $\hat{\mathfrak{a}}$ is co-prime to every $\mathfrak{p}_i$, $i \in [m]$.

Proof of Claim: If there exists an $i \in [m]$, say i^*, such that $\hat{\mathfrak{a}}$ is not co-prime to $\mathfrak{p}_{i^*}$, then since the latter is maximal, $\hat{\mathfrak{a}}$ is contained in $\mathfrak{p}_{i^*}$. But, since $\mathfrak{a} = \hat{\mathfrak{a}} * \prod_{i\in I} \mathfrak{p}_i^{t(i)}$, this implies that $\mathfrak{a}$ is contained in $\mathfrak{p}_{i^*}^{t(i^*)+1}$, contradicting the maximality of $t(i^*)$. This proves the claim and the lemma. □

Theorem 2.5.3. *If $f(X)$ is irreducible as a polynomial in $\mathbb{Z}[X]$, then for any ideal $\mathfrak{a}$ of $\mathcal{R} = \mathbb{Z}[X]/(f(X))$, $\mathfrak{a}$ is principal modulo $p^r\mathfrak{a}$, i.e. as an ideal of $\mathcal{R}/p^r\mathfrak{a}$.*

This theorem follows by applying lemmas 2.5.5 and 2.5.4.

Proof. First consider the case that $\mathfrak{a}$ is co-prime to all $\mathfrak{p}_i$. Then, by lemma 2.5.4 and lemma 2.3.2 and lemma 2.3.1 (x), we have

$$p^r\mathfrak{a} \;=\; \mathfrak{a}\prod_{i\in[m]}\mathfrak{p}_i^{r\cdot e_i}.$$

Then, by CRT,

$$\mathcal{R}/(p^r\mathfrak{a}) \;\cong\; \mathcal{R}/\mathfrak{a} * \prod_{i=1}^{m}\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i}.$$

So $\mathfrak{a}$ will be principal in $\mathcal{R}/(p^r\mathfrak{a})$, if it is principal in each of the component rings. Theorem 2.5.2, shows that $\mathfrak{a}$ is principal in $\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i}$, and $\mathfrak{a}$ is trivially principal modulo $\mathfrak{a}$, and hence the lemma is proved in this case.

Otherwise, by lemmas 2.5.5 and 2.5.4, for any integer $r \geq 0$, we have, $\mathfrak{a} * (p)^r = \hat{\mathfrak{a}} * \prod_{i\in[m]}\mathfrak{p}_i^{r\cdot e_i+t_i}$, for some non-negative integers t_i. Also, $\hat{\mathfrak{a}}$ is co-prime to each $\mathfrak{p}_i$ and hence to each $\mathfrak{p}_i^{r\cdot e_i}$ (by lemma 2.3.2) . Also, by CRT,

$$\mathcal{R}/(p^r\mathfrak{a}) \;\cong\; \mathcal{R}/\hat{\mathfrak{a}} * \prod_{i=1}^{m}\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i+t_i}.$$

Then, using theorem 2.5.2, $\hat{\mathfrak{a}}$ is principal modulo $\mathfrak{a} * (p)^r$ by employing CRT, just as in the simple case above where $\mathfrak{a}$ was co-prime to all $\mathfrak{p}_i$. By Theorem 2.5.2, each $\mathfrak{p}_i$ is also principal modulo $\mathfrak{p}_j^s$, for any s. So, we just need to show that $\mathfrak{p}_i$ is principal modulo $\hat{\mathfrak{a}}$. Since $\hat{\mathfrak{a}}$ is co-prime to $\mathfrak{p}_i$, there exists elements in $\alpha \in \mathfrak{p}_i$ and $\beta \in \hat{\mathfrak{a}}$, such that $\alpha + \beta = 1$. Thus, $\alpha = 1$ modulo $\hat{\mathfrak{a}}$, and hence $\mathfrak{p}_i$ is same as (1) modulo $\hat{\mathfrak{a}}$. Ideal $\hat{\mathfrak{a}}$ is also co-prime to $\mathfrak{p}_i$, and hence by the same argument as above, $\mathfrak{p}_i$ is same as (1) modulo $\hat{\mathfrak{a}}$. □

We now prove the above lemma 2.5.5 (and hence theorem 2.5.3) without requiring that $\mathcal{R}$ be an integral domain; the requirement of being an integral domain was required to employ the corollary

to Krull intersection theorem (corollary 2.3.2). The proof we give below (lemma 2.5.6) does not use this corollary, and is specific to the maximal ideals $\mathfrak{p}_i$ of the Noetherian ring $\mathcal{R}$.

For each $i \in [m]$, define an ideal $\bar{\mathfrak{p}}_i$ of $\mathcal{R}$ by

$$\bar{\mathfrak{p}}_i = \bigcap_{t=0}^{\infty} \mathfrak{p}_i^t.$$

It is a well-defined ideal of $\mathcal{R}$, because for every element α of $\mathcal{R}$, and every element β of $\bar{\mathfrak{p}}_i \subseteq \mathfrak{p}_i^0 = \mathcal{R}$, $\alpha\beta$ is in every $\mathfrak{p}_i^t$ ($t \geq 0$), as all $\mathfrak{p}_i^t$ are ideals of $\mathcal{R}$.

Lemma 2.5.6. *For all $i \in [m]$, the ideal $\bar{\mathfrak{p}}_i = 0$*

Proof. Since $\mathcal{R}$ is Noetherian, and $\bar{\mathfrak{p}}_i$ is an ideal of $\mathcal{R}$, it is finitely generated, and hence a finite set of k generators, for some $k > 0$, say $g_1, ..., g_k$. Moreover, since $\bar{\mathfrak{p}}_i \subseteq \mathfrak{p}_i$, these generators are also in $\mathfrak{p}_i = (h_i(X), p)$. Let, $\mu_1, ..., \mu_k$ and $\lambda_1, ..., \lambda_k$ be elements of $\mathcal{R}$ such that for each $k \in [k]$, $g_j = \mu_j p + \lambda_j h_i(X)$, where w.l.o.g. μ_j is not a multiple of $h_i(X)$, and otherwise μ_j and λ_j are polynomials of degree less than the degree of monic $f(X)$. This also implies that $g_j = \lambda_j h_i(X)$ mod p. Let J^* be the maximal subset of $[k]$, such that λ_j is non-zero for $j \in J^*$.

Claim 1: The set J^* is empty.

Proof of Claim 1: In the ring $\mathcal{R}$, since $f(X)$ is monic, we can assume that g_j is reduced to degree less than degree of $f(X)$. For $j \in J^*$, g_j is a multiple of $h_(X)$ mod p. Since $Z_p[X]$ is a UFD, consider the unique factorization of g_j in $Z_p[X]$, and let the largest power of $h_i(X)$ in this factorization be $h_i(X)^{t_j}$, where $t_j > 0$. Let $g_j(X) = \lambda'_j h_i(X)^{t_j}$ mod p, where λ'_j is non-zero, and is not a multiple of $h_i(X)$ mod p.

Let $t^* = \min \{t_j \mid j \in J^*\}$. Let j^* be an arbitrary index in J^* such that $t_j = t^*$. Since by Krull intersection theorem (theorem 2.3.1), $\bar{\mathfrak{p}}_i \subseteq \mathfrak{p}_i\bar{\mathfrak{p}}_i$, each generator g_j is in $\mathfrak{p}_i\bar{\mathfrak{p}}_i$, which is same as $(h_i(X), p)(g_1, ...g_k)$. Thus,

$$g_{j^*} = h_i(X) * \sum_{j \in J^*} \alpha_j \lambda'_j h_i(X)^{t_j} \text{ mod } (p, f(X)),$$

where α_j is in $\mathcal{R}$, and at least one α_j is non-zero. Substituting, $\lambda'_{j^*} h_i(X)^{t_{j^*}}$ on the left hand side we get

$$\lambda'_{j^*} h_i(X)^{t_{j^*}} = h_i(X) * \sum_{j \in J^*} \alpha_j \lambda'_j h_i(X)^{t_j} \bmod (p, f(X)).$$

This can equivalently be written as

$$\lambda'_{j^*} h_i(X)^{t_{j^*} - t_{j^*}} = h_i(X) * \sum_{j \in J^*} \alpha_j \lambda'_j h_i(X)^{t_j - t_{j^*}} \bmod (p, f(X)),$$

as all $t_j > t_{j^*} > 0$ for $j \in J^*$. But, this is a contradiction of λ'_{j^*} being not a multiple of $h_i(X)$ mod p.

End of Proof of Claim 1

Thus, for all $k \in [k]$, $g_j = \mu_j p$. Again, since by theorem 2.3.1, $\bar{\mathfrak{p}}_i \subseteq \mathfrak{p}_i \bar{\mathfrak{p}}_i$, each generator g_j is in $\mathfrak{p}_i \bar{\mathfrak{p}}_i$, which is same as $(h_i(X), p)(g_1, ...g_k)$. Thus, for any particular $j' \in [k]$,

$$\mu_{j'} p = \sum_{j \in [k]} (\alpha_j p + \beta_j h_i(X)) \mu_j p \bmod (f(X)),$$

where α_j, β_j are in $\mathcal{R}$, and at least one is non-trivial. Since $Z[X]$ is a UFD and $f(X)$ is monic, we can factor[10] out p. And thus,

$$\mu_{j'} = \sum_{j \in [k]} \beta_j h_i(X) \mu_j \bmod (p, f(X)).$$

But, this implies that either $\mu_{j'}$ is zero or $\mu_{j'}$ is a multiple of $h_i(X)$, the latter being a contradiction. Hence, all μ_j are zero for $j \in [k]$. This implies that that $\hat{\mathfrak{p}}_i = 0$. □

Extension to Product of Powers of Primes.

Theorem 2.5.4. *Let $q = \prod_j p_j^{r_j}$ be a product of powers of primes such that for every j, the modular polynomial $(f(X), p_j)$ is Dedekind-special. If $f(X)$ is irreducible as a polynomial in $\mathbb{Z}[X]$, then*

[10] This is where one would usually require that $\mathcal{R}$ is an integer domain.

for any ideal $\mathfrak{a}$ *of* $\mathcal{R} = \mathbb{Z}[X]/(f(X))$, $\mathfrak{a}$ *is principal modulo* $q\mathfrak{a}$*, i.e. as an ideal of* $\mathcal{R}/q\mathfrak{a}$.

The proof of this theorem is similar to the proof of above theorem 2.5.3, by iteratively computing $\hat{\mathfrak{a}}$ (using lemma 2.5.5) that is co-prime to all (p_j) and additionally observing that ideals (p) and (p') are co-prime for distinct primes p and p'.

2.6 Generator Extractor for Principal Ideals

In this section we restrict ourselves to the setting of Section 2.5. Given an ideal $\mathfrak{a}$ described by a set of generators $\{\gamma_i\}_{i\in[n]}$ in $\mathcal{R}$ or a $\mathbb{Z}$-basis $\boldsymbol{B}(\mathfrak{a})$, we wish to compute a generator of the principal ideal $\mathfrak{a}$ modulo $p^r\mathfrak{a}$ (which is principal by theorem 2.5.3).

We show that the following simple and efficient randomized algorithm computes such a generator with non-negligible probability.

Algorithm 1 FindGen

Input: A $\mathbb{Z}$-basis $\boldsymbol{B}$ for an ideal $\mathfrak{a}$ of $\mathcal{R}$.

Output: A single generator $a(X)$ for ideal $\mathfrak{a}$ mod $p^r\mathfrak{a}$.

1: Pick a random n-vector $\boldsymbol{\rho}$ with component polynomials ρ_k ($k \in [n]$) chosen uniformly and independently from $\mathbb{Z}_p[X]/(f(X)) = \mathcal{R}/(p)$.

2: View the n columns of $\boldsymbol{B}$ as n polynomials $\gamma_k \in \mathcal{R}$ ($k \in [n]$).

3: Compute $a(X) = \sum_{k=1}^{m} \rho_k * \gamma_k$ in $\mathcal{R}$.

4: Output $a(X)$

Lemma 2.6.1. *The algorithm* **FindGen** *outputs a generator* $a(X)$ *of* $\mathfrak{a}$ *modulo* $p^r\mathfrak{a}$ *with probability at least* $\prod_{i\in[m]}(1-2/p^{d_i})$*, where* d_i *is the degree of the irreducible (modulo* p*) polynomials* $h_i(X)$ *such that* $f(X) = \prod_{i\in[m]} h_i(X)^{e_i}$ *in* $\mathbb{Z}_p[X]$.

Proof. First, note that each of the n columns of $\boldsymbol{B}$ can be viewed as polynomials $\gamma_k \in \mathcal{R}$ ($k \in [n]$), such that the γ_k collectively form a set of generators (over $\mathcal{R}$) of $\mathfrak{a}$. Recall, $a(X)$ computed in the algorithm is just $\sum_k \rho_k\gamma_k$.

By lemma 2.5.5 and lemma 2.5.4, we have for any integer $r \geq 0$, $\mathfrak{a} \cdot (p)^r = \hat{\mathfrak{a}} \cdot \prod_{i\in[m]} \mathfrak{p}_i^{r\cdot e_i+t_i}$, where $\hat{\mathfrak{a}}$ is co-prime to every $\mathfrak{p}_i$ ($i \in [m]$). Thus, noting that all the $\mathfrak{p}_i$ are prime (lemma 2.5.1), and by employing CRT, we have that the ring $\mathcal{R}/p^r\mathfrak{a}$ is isomorphic to $\mathcal{R}/\hat{\mathfrak{a}} \cdot \prod_{i\in[m]} \mathcal{R}/\mathfrak{p}_i^{r\cdot e_i+t_i}$. Since $\mathfrak{a}$ is zero mod $\hat{\mathfrak{a}}$, $a(X)$ is also zero and hence trivially generates $\mathfrak{a}$ mod $\hat{\mathfrak{a}}$. Thus, we can focus on $\mathfrak{a}$ modulo $\mathfrak{p}_i^{r\cdot e_i+t_i}$, for each $i \in [m]$.

Fix an $i \in [m]$. Denote $\mathfrak{p}_i^{r\cdot e_i+t_i}$ by $\mathfrak{q}_i$. View each of the elements γ_k ($k \in [n]$) also as elements of the quotient ring $\mathcal{R}/\mathfrak{q}_i$, and the randomly chosen elements ρ_k as also elements in $\mathcal{R}/\mathfrak{q}_i$. Denote $\mathfrak{a}$ reduced mod $\mathfrak{q}_i$ by $\mathfrak{a}_i$. By Theorem 2.5.2, $\mathfrak{a}_i$ is principal and is generated by a finite power of g, where g is either p or $h_i(X)$ (depending on whether e_i is one or greater than one resp.). Similarly, each γ_k (the generators of $\mathfrak{a}$) is itself generated by a finite power of g mod $\mathfrak{q}_i$, say the power is $v_{k,i} \geq 0$. Hence, $\mathfrak{a}_i$ is generated by $g^{v_i^*}$, where $v_i^* = \min\{v_{k,i} \ : \ k \in [n]\}$. We need to show that $\sum_k \rho_k\gamma_k$ generates exactly $(g)^{v_i^*}$ mod $\mathfrak{q}_i$.

Note, γ_k can be written as $\alpha_{k,i}g^{v_{k,i}}$ mod $\mathfrak{q}_i$, where $\alpha_{k,i}$ is not in $\mathfrak{p}_i = (h_i(X), p)$. Then, $\sum_k \rho_k\gamma_k$ mod $\mathfrak{q}_i$ can be written as $g^{v_i^*} * \sum_k \rho_k\alpha_{k,i}g^{v_{k,i}-v_i^*}$. Note, at least for one $k \in [n]$, $v_{k,i} - v_i^*$ is zero. So, let I_i be the non-empty set of indices, subset of $[n]$, such that $v_{k,i} - v_i^*$ is zero.

Since by lemma 2.5.1, $\mathfrak{p}_i$ is a maximal ideal of $\mathcal{R}$ and hence every element of $\mathcal{R}$ not in $\mathfrak{p}_i$ is invertible mod $\mathfrak{p}_i$, we need to show that with high probability, over the random choices of $\{\rho_k\}_k$, *for all* $i \in [m]$, $\sum_{k\in I_i} \rho_k\alpha_{k,i}$ is not zero modulo $\mathfrak{p}_i$. Note that for $k \notin I_i$, the quantities $\rho_k\alpha_{k,i}g^{v_{k,i}-v_i^*}$ are in $(g) \subseteq (h_i(X), p)$, so the full sum (over all $k \in [n]$) will be non-zero modulo $(h_i(X), p) = \mathfrak{p}_i$ and hence invertible.

To calculate this probability, we first note that $\mathbb{Z}[X]/(h_i(X), p)$ is a finite field, more precisely GF(p^{d_i}), as $h_i(X)$ is irreducible modulo p, with d_i being the degree of $h_i(X)$. Thus, we can view each of ρ_k and $\alpha_{k,i}$ as element of this field (by reducing mod p). We have already seen that $\alpha_{k,i}$ is non-zero in this field, as it is not in $(h_i(X), p)$. However, a random choice of ρ_k in $\mathbb{Z}_p[X]/(f(X))$ may lead ρ_k to be zero modulo $(h_i(X), p)$, although this probability is small, as we next show.

First, note that $\mathbb{Z}_p[X]/(f(X)) = \mathcal{R}/(p)$. Then, by employing CRT and theorem 2.5.1, ρ_k is uniformly and *independently* distributed in the rings $\mathcal{R}/\mathfrak{p}_i^{e_i}$. Further, by lemma 2.5.1, $\mathfrak{p}_i^{e_i} = \mathfrak{s}_i =$

$(p, h_i(X)^{e_i})$. Thus, $\mathcal{R}/\mathfrak{p}_i^{e_i} = \mathbb{Z}[X]/\ (f(X),\ p,\ h_i(X)^{e_i})$, which is same as $\mathbb{Z}[X]/(p, h_i(X)^{e_i})$.

Hence ρ_k is zero modulo $\mathfrak{p}_i$ only if it is a multiple of $h_i(X)$. Since all (canonically represented) polynomials in $\mathfrak{s}_i$ have degree at most $d_i * e_i - 1$, there are at most $p^{d_i * e_i}$ polynomials. Similarly, all canonical polynomials in $\mathfrak{s}_i$ that are a multiple of $h_i(X)$ are at most $p^{d_i*(e_i-1)}$. This proves that the probability that ρ_k is zero in GF(p^{d_j}) is at most $1/p^{d_i}$. Moreover, conditioned on ρ_k being non-zero, the probability that it is c for some non-zero c in GF(p^{d_i}) is same regardless of c, as number of elements in the coset of c in $\mathfrak{s}_i$ is same for all c. Thus, conditioned on ρ_k being non-zero, ρ_k is uniformly distributed in GF(p^{d_i}).

Thus, probability that $\beta_i = (\sum_{k\in I_i} \rho_k \alpha_{k,i} \bmod\ (h_i(X), p))$ is zero, i.e. zero in GF(p^{d_i}), is at most $1/p^{d_i * |I_i|}$ plus $1/p^{d_i}$, which is at most $2/p^{d_i}$. Since, ρ_k are independently distributed in the various rings $\mathbb{Z}[X]/\mathfrak{s}_i$, the probability that all of these m quantities β_i are non-zero is at least $\prod_{i\in[m]}(1 - 2/p^{d_i})$, which is also a lower bound on the probability that $a(X)$ is a generator of $\mathfrak{a}$ modulo $p^r\mathfrak{a}$. □

Extension to Product of Powers of Primes. Let $q = \prod_j p_j^{r_j}$ be a product of powers of primes such that for every j, the modular polynomial $(f(X), p_j)$ is Dedekind-special. The above algorithm can be correctly extended by choosing ρ_i randomly and independently from $Z_{q'}[X]/(f(X))$ where $q' = \prod_j p_j$. The probability of success in this case is at least $\prod_j \prod_{i\in[m_j]}(1 - 2/p_j^{d_{j,i}})$, where $d_{j,i}$ is the degree of the m_j irreducible polynomials $h_{j,i}(X)$ (modulo p_j) such that $f(X) = \prod_{i\in[m]} h_{j,i}(X)^{e_{j,i}}$ in $\mathbb{Z}_p[X]$.

Extension to Arbitrary q without known-factorization. If the factorization of q is not known, and say $q = \prod_j p_j^{r_j}$ as above, we can still use the above algorithm, but this time by choosing ρ_i randomly and independently modulo $\mathbb{Z}_q[X]/(f(X))$. In the proof of lemma 2.6.1, again using CRT and focusing on individual primes, say p_j, ρ_k is now uniformly and independently distributed in $\mathbb{Z}[X]/\mathfrak{p}_i^{e_i r_j}$. By a similar argument as in the proof of lemma 2.5.1, this ring is isomorphic to $\mathbb{Z}[X]/(p, h_i(X)^{e_i r_j})$. By the probability analysis in the lemma 2.6.1 above, the probability of success remains the same as in the known factorization case above.

Boosting the Probability of Success. One can boost the probability of finding a generator of $\mathfrak{a}$ modulo $q\mathfrak{a}$ by repeating the above algorithm, but to stop the repetition we need an efficient test that $a(X)$ as computed is indeed a generator. But, this is same as checking $(\mathfrak{a}, q\mathfrak{a}) = (a(X), q\mathfrak{a})$, which can be efficiently tested by computing the Hermite normal form of $\boldsymbol{B}$ (the given $\mathbb{Z}$-basis of $\mathfrak{a}$) and the Hermite normal form of $[\boldsymbol{C}_a \mid q\boldsymbol{B}]$, and checking for equality.

2.7 Hardness of Decisional Ring-LWE

In this section, by default, we focus on a degree-n monic polynomial $f(X)$ and an integer $q \geq 2$ where $(f(X), q)$ is *Dedekind-special*. Let $\mathcal{R}_{\mathbb{R}} = \mathbb{R}[X]/(f(X))$.

First we give out the same distribution of error distributions as in [PRS17], which we will use in the following reduction.

Definition 2.7.1 (Error Distribution)**.** *Fix arbitrary $s(n) = \omega(\sqrt{\log(n)})$. For $\alpha > 0$, a distribution sampled from Υ_α is an elliptical Gaussian distribution $D_{\mathbf{r}}$, where $\mathbf{r} \in G$ is sampled as follow: for $i = 0, \ldots, s_1 - 1$, sample $x_i \in D_1$ and set $r_i^2 = \alpha^2(x_i^2 + s^2(n))/2$, for $i = s_1, \ldots, s_1 + s_2 - 1$, sample x_i, y_i from $D_{1/\sqrt{2}}$ and set $r_i^2 = r_{i+s_2}^2 = \alpha^2(x_i^2 + y_i^2 + s^2(n))/2$.*

Definition 2.7.2 (RLWE Distribution)**.** *Let $\boldsymbol{V}$ be the Vandermonde matrix of the modulo polynomial $f(x)$. For $\mathbf{s} \in \mathcal{R}_q^\vee$ and an error distribution ψ over $\mathcal{R}_{\mathbb{R}}$, we define the RLWE distribution $\mathcal{A}_{\mathbf{s},\psi}$ over $\mathcal{R}_q \times \mathcal{R}_{\mathbb{R}}/\mathcal{R}^\vee$ as $\left(\mathbf{a}, \mathbf{b} = \mathbf{a} * \mathbf{s}/q + \boldsymbol{V}^{-1}\mathbf{e} \bmod \mathcal{R}^\vee\right)$ where $\mathbf{e}$ is sampled from ψ, $\mathbf{a}$ is uniform over $\mathcal{R}_q$.*

Definition 2.7.3 ((Average-case) Decisional RLWE Problem)**.** *Let Υ_α be a distribution over family of error distributions, each over $\mathbb{R}[X]/(f(X))$. The* average-case decisional RLWE problem*, $\mathit{RLWE}_{q,\Upsilon_\alpha}$ is to distinguish (with non-negligible advantage) between independent samples from $A_{\mathbf{s},\psi}$ for a random choice of uniform $s \in \mathcal{R}_q^\vee$ and $\psi \in \Upsilon_\alpha$ and the same number of uniformly random and independent samples from $\mathcal{R}_q \times \mathcal{R}_{\mathbb{R}}/\mathcal{R}^\vee$.*

Let $\mathcal{R}$-DGS_γ be the discrete Gaussian sampling problem DGS_γ when restricted to the ideal lattices on the polynomial ring $\mathcal{R} = \mathbb{Z}[X]/(f(X))$.

Theorem 2.7.1. *Let $\alpha = \alpha(n) \in (0,1)$, $q = q(n) \geq 2$ be an integer and $f(x)$ be any degree-n monic polynomial where $(f(X), q)$ is Dedekind-special. Let $\mathcal{R} = \mathbb{Z}[X]/(f(X))$ be a polynomial ring. If $\alpha q \geq 2 \cdot \omega(1)$, for some negligible $\epsilon = \epsilon(n)$, there is a probabilistic polynomial-time quantum reduction from $\mathcal{R}$-DGS_γ to (average case, decisional) $\mathsf{RLWE}_{q,\Upsilon_\alpha}$, where*

$$\gamma = \max\left\{\eta_\epsilon(\mathcal{L}(\mathcal{I})) \cdot (\sqrt{2}/\alpha) \cdot \omega(1), \sqrt{2n}/\lambda_1(\mathcal{L}(\mathcal{I})^\vee)\right\}$$

Note that $\eta_\epsilon(\mathcal{L}) > \omega(\sqrt{\log(n)})/\lambda_1(\mathcal{L}^\vee)$. Using known reduction [Reg06], this immediately implies a polynomial-time quantum reduction from SIVP_γ to (average-case, decision) $\mathsf{RLWE}_{q,\Upsilon_\alpha}$ for any $\gamma \leq \max\left\{\omega(\sqrt{n\log(n)}/\alpha, \sqrt{2n}\right\}$.

In case of spherical error, same as [PRS17, Section 7] we have

Corollary 2.7.1. *With the same notation as Theorem 2.7.1, there's a polynomial time quantum reduction from $\mathcal{R}$-DGS_γ to (average-case, decisional) RLWE_{q,D_ξ} using ℓ samples, where*

$$\gamma = \max\left\{\eta_\epsilon(\mathcal{L}(\mathcal{I})) \cdot (\sqrt{2}/\xi) \cdot \left(\frac{n\ell}{\log(n\ell)}\right)^{\frac{1}{4}} \cdot \omega(\sqrt{\log(n)}), \sqrt{2n}/\lambda_1(\mathcal{L}(\mathcal{I})^\vee)\right\},$$

as long as $\xi q \geq \left(\frac{n\ell}{\log(n\ell)}\right)^{\frac{1}{4}} \cdot \omega(\sqrt{\log(n)})$.

Our proof to theorem 2.7.1 will be exactly the same as [PRS17, Theorem 6.2], that starts with a discrete Gaussian sampler with very large radius, and iteratively applys the following lemma 2.7.1.

Definition 2.7.4. *For $r > 0$, $\zeta > 0$ and $T \geq 1$, define $W_{r,\zeta,T}$ as the set of cardinality $(s_1+s_2)\cdot(T+1)$ containing for each $i = 0, \ldots, s1 + s2 - 1$ and $j = 0, \ldots, T$ the vector $\mathbf{r}_{i,j}$ which is equal to r in all coordinates except in the i-th, and the $(i + s2)$-th if $i \geq s_1$, where it is equal to $r \cdot (1 + \zeta)^j$.*

Lemma 2.7.1. *There's an efficient quantum algorithm that, given an oracle that solves $\mathsf{RLWE}_{q,\Upsilon_\alpha}$, an ideal $\mathcal{I} \subseteq \mathcal{R}$, a number $r \geq \sqrt{2}q \cdot \eta_\epsilon(\mathcal{L}(\mathcal{I}))$ and $r' = r \cdot \omega(1)/(\alpha q) \geq \sqrt{2n}/\lambda_1(\mathcal{L}(\mathcal{I})^\vee)$, polynomially many samples from discrete Gaussian distribution $D_{\mathcal{L}(\mathcal{I}),\mathbf{r}}$ for each $\mathbf{r} \in W_{r,\zeta,T}$ (for some $\zeta = 1/\mathrm{poly}(n)$ and $T = \mathrm{poly}(n)$), and a vector $\mathbf{r}' \geq r'$, outputs an independent sample from $D_{\mathcal{L}(\mathcal{I}),\mathbf{r}'}$.*

As in [PRS17, Lemma 6.5], This iterative step is given by combining the following two parts: a classical one in lemma 2.7.2 that use a discrete Gaussian sampler and a RLWE oracle to solve the Gaussian Decoding Problem (GDP), and a quantum one in lemma 2.7.3 that use this GDP solver to provide discrete Gaussian samples with smaller radius.

Lemma 2.7.2. *There's a probabilistic (classical) polynomial time algorithm that, taking an oracle that solves $\mathsf{RLWE}_{q,\Upsilon_\alpha}$ for $\alpha \in (0,1)$ and integer $q > 2$, an ideal $\mathcal{I} \in \mathcal{R}$, a parameter $r \geq \sqrt{2}q \cdot \eta_\epsilon(\mathcal{L}(\mathcal{I}))$, and polynomially many samples from discrete Gaussian $D_{\mathcal{L}(\mathcal{I}),\mathbf{r}}$ for each $\mathbf{r} \in W_{r,\zeta,T}$ for some $\zeta = 1/\mathrm{poly}(n)$ and $T = \mathrm{poly}(n)$, solves $\mathsf{GDP}_{\mathcal{L}(\mathcal{I})^\vee,g}$ for any $g = o(1) \cdot \alpha q/(2r)$.*

Lemma 2.7.3 ([PRS17, Lemma 6.7])**.** *There is an efficient quantum algorithm that, given any n-dimensional lattice $\mathcal{L}$, a number $g < \frac{\lambda_1(\mathcal{L}^\vee)}{2\sqrt{2n}}$, a vector $\mathbf{r} \geq 1$, and an oracle that solves $\mathsf{GDP}_{\mathcal{L}^\vee,g}$ with all but negligible probability, outputs a sample from $D_{\mathcal{L},\frac{\mathbf{r}}{2g}}$.*

The proof of lemma 2.7.2 follows exactly from [PRS17, Lemma 6.6], except the core reduction from Gaussian Decoding Problem to RLWE in [PRS17, Lemma 6.8] requires the underlying ring to be a dedekind domain, which may not be true in our case. We provide a counterpart in lemma 2.7.4 that works for our non Dedekind domain.

Lemma 2.7.4. *There's an efficient algorithm that, takes as input an integer $q \geq 2$, a dual ideal lattice $\mathcal{L}(\mathcal{I})^\vee$ where $\mathcal{I}$ is an ideal in $\mathcal{R}$, a coset $\mathbf{e} + \mathcal{L}(\mathcal{I})^\vee$ with a bound $d \geq ||\mathbf{e}||_\infty$, a parameter $r \geq \sqrt{2}q \cdot \eta_\epsilon(\mathcal{L}(\mathcal{I}))$ and samples from $D_{\mathcal{L}(\mathcal{I}),\mathbf{r}}$ for some $\mathbf{r} \geq r$. It outputs samples that are within negligible statistical distance from the RLWE distribution $A_{\mathbf{s},\mathbf{r}'}$ for a uniformly random $\mathbf{s} \in \mathcal{R}_q^\vee$, where $(\mathbf{r}'_i)^2 = (\mathbf{r}_i|\mathbf{e}_i|/q)^2 + (rd/q)^2$.*

To prove this lemma 2.7.4, we follow the standard techniques as in [PRS17, Lemma 6.8] which is a slight generalization over [LPR10, Lemma 4.7], elaborated as below.

Proof Sketch. First sample a random $\hat{\mathbf{z}} = \boldsymbol{V}\mathbf{z}$ from the discrete Gaussian $D_{\mathcal{L}(\mathcal{I}),\mathbf{r}}$ where $\mathbf{z} \in \mathcal{I}$. Because $\mathbf{r} \geq \sqrt{2}q \cdot \eta_\epsilon(\mathcal{L}(\mathcal{I}))$, by smoothing lemma 2.2.1, the distribution of ($\mathbf{z} \bmod q\mathcal{I}$) is within

a negligible distance from uniform distribution over $\mathcal{I}/q\mathcal{I}$. Also let $\mathbf{e}'$ be an independent sample from the continuous Gaussian $D_{\alpha/\sqrt{2}}$.

Now, for any element $\boldsymbol{V}\mathbf{y} = \hat{\mathbf{y}} = \mathbf{e} + \hat{\mathbf{x}} \in \mathbf{e} + \mathcal{L}(\mathcal{I})^\vee$, where $\hat{\mathbf{x}} = \boldsymbol{V}\mathbf{x} \in \mathcal{L}(\mathcal{I})^\vee$, we could directly provide a "RLWE sample" from $\mathcal{I}/q\mathcal{I} \times \mathcal{R}_\mathbb{R}/\mathcal{R}^\vee$ as

$$\left(\mathbf{z} \bmod q\mathcal{I}, \mathbf{z} * \mathbf{y}/q + \mathbf{e}' \bmod \mathcal{R}^\vee = \frac{\mathbf{z} * \mathbf{x}}{q} + \frac{1}{q}\boldsymbol{C}_z\boldsymbol{V}^{-1}\mathbf{e} + \mathbf{e}' \bmod \mathcal{R}^\vee\right).$$

for some secret $\mathbf{x} \in \mathcal{I}^\vee/q\mathcal{I}^\vee$. To jump out of the ideal, we use lemma 2.7.5, a counterpart of clearing lemma of [LPR10, Lemma 2.15] for non dedekind domains, that gives (i) an invertible and efficiently computable bijection $\psi : \mathcal{I}/q\mathcal{I} \to \mathcal{R}/q\mathcal{R}$, and (ii) an efficiently invertible and computable bijection $\phi : \mathcal{I}^\vee/q\mathcal{I}^\vee \to \mathcal{R}^\vee/q\mathcal{R}^\vee$, with the additional property that $\mathbf{z}*\mathbf{x} = \psi(\mathbf{z})*\phi(\mathbf{x})$. Therefore the final RLWE distribution would be over $\mathcal{R}_q \times \mathcal{R}_\mathbb{R}/\mathcal{R}^\vee$ as

$$\left(\psi(\mathbf{z} \bmod q\mathcal{I}), \mathbf{z} * \mathbf{y}/q + \mathbf{e}' \bmod \mathcal{R}^\vee = \frac{\psi(\mathbf{z}) * \phi(\mathbf{x})}{q} + \frac{1}{q}\boldsymbol{C}_z\boldsymbol{V}^{-1}\mathbf{e} + \mathbf{e}' \bmod \mathcal{R}^\vee\right)$$

for some secret $\phi(\mathbf{x}) \in \mathcal{R}^\vee/q\mathcal{R}^\vee$. Note that since ψ is invertible, $\psi(\mathbf{z} \bmod q\mathcal{I})$ is almost uniform over $\mathcal{R}/q\mathcal{R} = \mathcal{R}_q$.

Moreover, if we sample $\mathbf{e}$ as in $\mathsf{GDP}_{\mathcal{L}(\mathcal{I})^\vee, g}$ where $g = \alpha q/(\sqrt{2}r)$, the distribution of term $\left(\frac{1}{q}\boldsymbol{C}_z\boldsymbol{V}^{-1}\mathbf{e} + \mathbf{e}'\right)$ will be exactly Υ_α, as in [PRS17, Lemma 6.8]. Then we complete the proof by applying the standard technique to randomize the secret as in [Reg10, Lemma 3.2]

The following lemma is an extension of an important technical lemma from [LPR10, Lemma 2.15], which is informally referred to as the *ideal clearing lemma*, and is the key to extending Regev's LWE-hardness [Reg10] to the Ring-LWE setting. Our proof of the lemma is quite different from the proof in [LPR10] as it extends to some non dedekind domains and hence cannot use the standard prime ideal factorization and ideal invertibility guaranteed for dedekind domains.

Lemma 2.7.5. (**Ideal Clearing Lemma**) *For any integer q that is Dedekind-special for $f(X)$, given a $\mathbb{Z}$-basis $\boldsymbol{B}(\mathcal{I})$ for ideal $\mathcal{I} \subseteq \mathcal{R}$,*

(i) *there is an efficiently computable $\mathcal{R}$-module isomorphism $\psi : \mathcal{I}/q\mathcal{I} \to \mathcal{R}/q\mathcal{R}$,*

(ii) *there is an efficiently invertible $\mathcal{R}$-module isomorphism $\phi : \mathcal{I}^\vee/q\mathcal{I}^\vee \to \mathcal{R}^\vee/q\mathcal{R}^\vee$, such that*

(iii) *for any $\mathbf{z} \in \mathcal{I}/q\mathcal{I}$ and $\mathbf{x} \in \mathcal{I}^\vee/q\mathcal{I}^\vee$, their polynomial product satisfies*

$$\mathbf{z} * \mathbf{x} \equiv \psi(\mathbf{z}) * \phi(\mathbf{x}) \pmod{q\mathcal{R}^\vee}$$

Proof. By Algorithm FindGen (lemma 2.6.1), we can efficiently find a $\mathbf{g}$ that is a generator of $\mathcal{I}$ modulo $q\mathcal{I}$. In other words, as ideals, $\mathcal{I} = (\mathbf{g}) + q\mathcal{I}$. Thus

$$\boldsymbol{B}(\mathcal{I}) = \boldsymbol{C}_g \boldsymbol{U} + q \cdot \boldsymbol{B}(\mathcal{I})\boldsymbol{T} \tag{2.2}$$

for some integer matrix $\boldsymbol{U}$ and $\boldsymbol{T}$. We next show how to efficiently compute $\boldsymbol{U}$ modulo q, which will be used to construct the isomorphisms. Note that the generator $\mathbf{g} \in \mathcal{I}$. Therefore $\mathbf{g} = \boldsymbol{B}(\mathcal{I})\mathbf{d}^{(0)}$ for some integer-vector $\mathbf{d}^{(0)}$. Similarly, the coefficient representation of $g(X) * X^i$ is $\boldsymbol{B}(\mathcal{I})\mathbf{d}^{(i)}$ for some integer vector $\mathbf{d}^{(i)}$. Thus, $\boldsymbol{C}_g = \boldsymbol{B}(\mathcal{I}) \cdot \boldsymbol{D}$, where $\boldsymbol{D}$ is an integer matrix (with columns $\mathbf{d}^{(i)}$). Plugging this into (2.2), we have $\boldsymbol{B}(\mathcal{I}) = \boldsymbol{B}(\mathcal{I})\boldsymbol{D}\boldsymbol{U} + q\boldsymbol{B}(\mathcal{I})\boldsymbol{T}$. Since, $\boldsymbol{B}(\mathcal{I})$ is full ranked and $\boldsymbol{T}$ is an integer matrix, we have $\boldsymbol{D} \cdot \boldsymbol{U} = \boldsymbol{I} \pmod{q}$. Thus we can obtain $\boldsymbol{U}$ (modulo q) as the inverse of $\boldsymbol{D}$ modulo q. This suffices for the following construction.

Now, consider following two mappings for claims (i)-(iii). For any $\mathbf{z} \in \mathcal{I}$ and $\mathbf{x} \in \mathcal{I}^\vee$, define

$$\psi(\mathbf{z}) = \boldsymbol{U}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} \pmod{q\mathcal{R}} \tag{2.3}$$

$$\phi(\mathbf{x}) = \mathbf{g} * \mathbf{x} \pmod{q\mathcal{R}^\vee} \tag{2.4}$$

Starting with (i), multiplying (2.2) by $\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z}$ from the right, we get

$$\boldsymbol{C}_g \boldsymbol{U}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} = \mathbf{z} - q\boldsymbol{B}(\mathcal{I})\boldsymbol{T}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z}$$

which is equivalent to $\mathbf{z} \pmod{q\mathcal{I}}$ since $\boldsymbol{T}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z}$ is integer. Letting $\mathbf{a} = \psi(\mathbf{z})$, ψ is invertible as

$\mathbf{g} * \mathbf{a} = \mathbf{z} \pmod{q\mathcal{I}}$. Also, $\psi^{-1}(\mathbf{a}) = \mathbf{g} * \mathbf{a}$ is surjective because $\boldsymbol{C}_g \mathbf{a} \in \mathcal{I}$ for any $\mathbf{a} \in \mathcal{R}$. Thus, ψ^{-1} is easily seen, by commutativity, to be a $\mathcal{R}$-module homomorphism, and ψ is an $\mathcal{R}$-module isomorphism.

For (ii), we first note that by proposition 2.4.4 and using $\boldsymbol{C}_g = \boldsymbol{B}(\mathcal{I}) \cdot \boldsymbol{D}$,

$$\begin{aligned}
\mathbf{g} * \mathbf{x} &= (\boldsymbol{V}^\top \boldsymbol{V})^{-1} \cdot (\boldsymbol{V}^\top \boldsymbol{V}) \cdot \boldsymbol{C}_g \cdot \mathbf{x} \\
&= (\boldsymbol{V}^\top \boldsymbol{V})^{-1} \boldsymbol{C}_g^\top \cdot (\boldsymbol{V}^\top \boldsymbol{V}) \cdot \mathbf{x} \\
&= (\boldsymbol{V}^\top \boldsymbol{V})^{-1} \boldsymbol{D}^\top \boldsymbol{B}(\mathcal{I})^\top (\boldsymbol{V}^\top \boldsymbol{V}) \cdot \mathbf{x} \qquad (2.5)
\end{aligned}$$

Recall by lemma 2.4.2, $(\boldsymbol{V}^\top \boldsymbol{V})^{-1} \boldsymbol{B}(\mathcal{I})^{-\top}$ is a $\mathbb{Z}$-basis of $\mathcal{I}^\vee$, and $(\boldsymbol{V}^\top \boldsymbol{V})^{-1}$ is a $\mathbb{Z}$-basis of $\mathcal{R}^\vee$. Thus using (2.5), we can invert $\phi(\mathbf{x})$ by left multiplcation by $(\boldsymbol{V}^\top \boldsymbol{V})^{-1} \boldsymbol{B}(\mathcal{I})^{-\top} \boldsymbol{U}^\top (\boldsymbol{V}^\top \boldsymbol{V})$ to $\mathbf{x}$ mod $q\mathcal{I}^\vee$. Further, for any $\mathbf{s} \in \mathcal{R}^\vee$, $(\boldsymbol{V}^\top \boldsymbol{V})^{-1} \boldsymbol{B}(\mathcal{I})^{-\top} \boldsymbol{U}^\top (\boldsymbol{V}^\top \boldsymbol{V}) \mathbf{s}$ lies in $\mathcal{I}^\vee$ by the aforementioned basis. Thus, ϕ is an efficiently invertible and surjective $\mathcal{R}$-module homomorphism, thus proving (ii).

Now, we move on to prove (iii). For some $\mathbf{t_0} \in \mathcal{R}$ and $\mathbf{t_1} \in \mathcal{R}^\vee$, we have

$$\begin{aligned}
&\psi(\mathbf{z}) * \phi(\mathbf{x}) \\
&= \left(\boldsymbol{U}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} - q \cdot \mathbf{t_0}\right) * (\mathbf{g} * \mathbf{x} - q \cdot \mathbf{t_1}) \\
&= \boldsymbol{U}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} * \mathbf{g} * \mathbf{x} - q \cdot \mathbf{t_0} * \mathbf{g} * \mathbf{x} - q \cdot \boldsymbol{U}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} * \mathbf{t_1} + q^2 \cdot \mathbf{t_0} * \mathbf{t_1} \\
&\equiv \mathbf{g} * \boldsymbol{U}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} * \mathbf{x} \pmod{q\mathcal{R}^\vee} \qquad (2.6) \\
&\equiv \boldsymbol{C}_g \boldsymbol{U}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} * \mathbf{x} \pmod{q\mathcal{R}^\vee} \\
&\equiv \mathbf{z} * \mathbf{x} - q\boldsymbol{B}(\mathcal{I})\boldsymbol{T}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} * \mathbf{x} \pmod{q\mathcal{R}^\vee} \\
&\equiv \mathbf{z} * \mathbf{x} \pmod{q\mathcal{R}^\vee} \qquad (2.7)
\end{aligned}$$

where (2.6) follows by noting that $\mathbf{t_0} * \mathbf{g} \in \mathcal{I}$ and $\mathbf{x} \in \mathcal{I}^\vee$ and then employing lemma 2.4.4. Similarly, $\boldsymbol{U}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z}$ is in $\mathcal{I} \subseteq \mathcal{R}$, and we can mod out its multiplication by $\mathbf{t_1} \in \mathcal{R}^\vee$. Also, for the last equation (2.7), we use lemma 2.4.4, noting that $\boldsymbol{B}(\mathcal{I})\boldsymbol{T}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z}$ is in $\mathcal{I}$. □

Remark. When comparing with [LPR10], note that they obtain a $t \in \mathcal{I}$ such that $t \cdot \mathcal{I}^{-1}$ is co-prime to ideal (q). In other words, $t \cdot \mathcal{I}^{-1} + (q) = (1)$. Multiplying both sides by the ideal $\mathcal{I}$, we get, $(t) + q\mathcal{I} = \mathcal{I}$, which is same as saying that t is the generator of $\mathcal{I} \bmod q\mathcal{I}$. In other words [LPR10] implicitly shows that $\mathcal{I}$ is principal mod $q\mathcal{I}$, but this is well-known for Dedekind domains. As mentioned earlier, our case is more difficult, yet we manage to prove it.

The above clearing lemma also generalizes to ring of integers of a number field, which is known to be a Dedekind domain. Also, for Dedekind domains $\mathfrak{D}$ it is known that for any ideal $\mathfrak{a}$, $\mathfrak{D}/\mathfrak{a}$ is a principal ideal ring (see e.g. wikipedia entry for "Principal Ideal Rings" for a proof). The lemma stated and proved here is easier to use than the original lemma in [LPR10] because as mentioned in the remark above it just needs an arbitrary generator of the principal ideal $\mathcal{I}/(q\mathcal{I})$. It is an interesting *open problem* to obtain an efficient randomized algorithm for computing such a generator (for all q in the $\mathcal{O}_{\mathbf{K}}$ setting), similar to the one given in section 2.6 for $\mathcal{R}_{\mathbf{K}}$ for Dedekind-special q.

Lemma 2.7.6. (**Ideal Clearing Lemma for Ring of Integers [LPR10]**) *For any positive integer q, given a $\mathbb{Z}$-basis $\boldsymbol{B}(\mathcal{I})$ for ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbf{K}}$, and a generator $\mathbf{g} \in \mathcal{I}$ for the principal ideal $\mathcal{I}/(q\mathcal{I})$,*

(i) *there is an efficiently computable $\mathcal{O}_{\mathbf{K}}$-module isomorphism $\psi : \mathcal{I}/(q\mathcal{I}) \to \mathcal{O}_{\mathbf{K}}/(q\mathcal{O}_{\mathbf{K}})$,*

(ii) *there is an efficiently invertible $\mathcal{O}_{\mathbf{K}}$-module isomorphism $\phi : \mathcal{I}^{\vee}/(q\mathcal{I}^{\vee}) \to \mathcal{O}_{\mathbf{K}}^{\vee}/(q\mathcal{O}_{\mathbf{K}}^{\vee})$,*

(iii) *such that, for any $\mathbf{z} \in \mathcal{I}/(q\mathcal{I})$ and $\mathbf{x} \in \mathcal{I}^{\vee}/(q\mathcal{I}^{\vee})$, their polynomial product satisfies*

$$\mathbf{z} * \mathbf{x} \equiv \psi(\mathbf{z}) * \phi(\mathbf{x}) \pmod{q\mathcal{O}_{\mathbf{K}}^{\vee}}$$

Proof. We will write $\boldsymbol{B}(\mathcal{O}_{\mathbf{K}})$ for a basis of $\mathcal{O}_{\mathbf{K}}$.

We have that $\mathbf{g}$ is a generator of $\mathcal{I}$ modulo $q\mathcal{I}$. In other words, as ideals, $\mathcal{I} = (\mathbf{g}) + q\mathcal{I}$. Thus, $\mathbf{g} \in \mathcal{I}$. Thus,

$$\boldsymbol{C}_g \boldsymbol{B}(\mathcal{O}_{\mathbf{K}}) = \boldsymbol{B}(\mathcal{I}) \cdot \boldsymbol{D}, \tag{2.8}$$

where $\boldsymbol{D}$ is an integer matrix.

We also have that every column of $\boldsymbol{B}(\mathcal{I})$ is generated by $\boldsymbol{C}_g \bmod q\mathcal{I}$, or mod $q\boldsymbol{B}(\mathcal{I})$. Thus,

$$\boldsymbol{B}(\mathcal{I}) = \boldsymbol{C}_g \boldsymbol{B}(\mathcal{O}_{\mathbf{K}})\boldsymbol{U} + q \cdot \boldsymbol{B}(\mathcal{I})\boldsymbol{T} \tag{2.9}$$

for some integer, matrices $\boldsymbol{U}$ and $\boldsymbol{T}$. Equivalently,

$$\boldsymbol{B}(\mathcal{I}) \cdot (I - q\boldsymbol{T}) = \boldsymbol{C}_g \boldsymbol{B}(\mathcal{O}_{\mathbf{K}})\boldsymbol{U}, \tag{2.10}$$

or, since $\boldsymbol{C}_g$ is full-ranked, we have

$$(\boldsymbol{C}_g \boldsymbol{B}(\mathcal{O}_{\mathbf{K}}))^{-1} \boldsymbol{B}(\mathcal{I}) \cdot (I - q\boldsymbol{T}) = \boldsymbol{U} \tag{2.11}$$

We next show that $\boldsymbol{D} \cdot \boldsymbol{U} = I \pmod q$. Note, from (2.8) and observing that $\boldsymbol{B}(\mathcal{I})$ is full-ranked, $\boldsymbol{D} = \boldsymbol{B}(\mathcal{I})^{-1}\boldsymbol{C}_g \boldsymbol{B}(\mathcal{O}_{\mathbf{K}})$. Multiplying the above equation on the left by $\boldsymbol{D}$, we get $(I - q\boldsymbol{T}) = \boldsymbol{D} \cdot \boldsymbol{U}$, and hence

$$\boldsymbol{D} \cdot \boldsymbol{U} = I \pmod q. \tag{2.12}$$

Now, consider the following two mappings for claims (i)-(iii). For any $\mathbf{z} \in \mathcal{I}$ and $\mathbf{x} \in \mathcal{I}^\vee$, define

$$\psi(\mathbf{z}) = \mathbf{a} = \boldsymbol{B}(\mathcal{O}_{\mathbf{K}})\boldsymbol{U}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} \pmod{q\mathcal{O}_{\mathbf{K}}} \tag{2.13}$$

$$\phi(\mathbf{x}) = \mathbf{g} * \mathbf{x} \pmod{q\mathcal{O}_{\mathbf{K}}^\vee} \tag{2.14}$$

For any $\mathbf{z}$ in $\mathcal{I}$, and $\mathbf{a} = \psi(\mathbf{z})$ we have $\boldsymbol{C}_g\mathbf{a} \equiv \boldsymbol{C}_g \boldsymbol{B}(\mathcal{O}_{\mathbf{K}})\boldsymbol{U}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z}$, which by (2.9) is same as $\boldsymbol{B}(\mathcal{I})(I - q\boldsymbol{T})\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} = \mathbf{z} \pmod{q\mathcal{I}}$, So, ψ is an invertible map. It is also surjective since $\boldsymbol{C}_g\mathbf{a}$ is in $\mathcal{I}$ for any $\mathbf{a} \in \mathcal{O}_{\mathbf{K}}$. Since, ψ^{-1} is easily seen to be a $\mathcal{O}_{\mathbf{K}}$-module homomorphism, ψ is an $\mathcal{O}_{\mathbf{K}}$-module isomorphism. Further, we already showed how to compute $\boldsymbol{U}$ efficiently, this proves (i).

For (ii), we first note that by proposition 2.4.4 and using (2.8),

$$\mathbf{g} * \mathbf{x} = (\boldsymbol{V}^\top \boldsymbol{V})^{-1} \cdot (\boldsymbol{V}^\top \boldsymbol{V}) \cdot \boldsymbol{C}_g \cdot \mathbf{x} \tag{2.15}$$

$$= (\boldsymbol{V}^\top \boldsymbol{V})^{-1} \boldsymbol{C}_g^\top \cdot (\boldsymbol{V}^\top \boldsymbol{V}) \cdot \mathbf{x} \tag{2.16}$$

$$= (\boldsymbol{V}^\top \boldsymbol{V})^{-1} \boldsymbol{B}(\mathcal{O}_\mathbf{K})^{-\top} \boldsymbol{D}^\top \boldsymbol{B}(\mathcal{I})^\top (\boldsymbol{V}^\top \boldsymbol{V}) \cdot \mathbf{x} \bmod q\mathcal{O}_\mathbf{K}^\vee, \tag{2.17}$$

where the last equality follows by noting that $(\boldsymbol{V}^\top \boldsymbol{V})^{-1} \boldsymbol{B}(\mathcal{O}_\mathbf{K})^{-\top}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_\mathbf{K}^\vee$ (see footnote to lemma 2.4.2).

Thus, by lemma 2.4.2, $\phi(\mathbf{x})$ is inverted by $(\boldsymbol{V}^\top \boldsymbol{V})^{-1} \boldsymbol{B}(\mathcal{I})^{-\top} \boldsymbol{U}^\top \boldsymbol{B}(\mathcal{O}_\mathbf{K})^\top (\boldsymbol{V}^\top \boldsymbol{V})$ to $\mathbf{x} \bmod q\mathcal{I}^\vee$. Further, for any $\mathbf{s} \in \mathcal{O}_\mathbf{K}^\vee$, $(\boldsymbol{V}^\top \boldsymbol{V})^{-1} \boldsymbol{B}(\mathcal{I})^{-\top} \boldsymbol{U}^\top \boldsymbol{B}(\mathcal{O}_\mathbf{K})^\top (\boldsymbol{V}^\top \boldsymbol{V})\mathbf{s}$ lies in $\mathcal{I}^\vee$ by the aforementioned basis. Thus, ϕ is an invertible and surjective $\mathcal{O}_\mathbf{K}$-module homomorphism, that is also efficiently invertible, thus proving (ii).

Now, we move on to prove (iii). For some $\mathbf{t_0} \in \mathcal{O}_\mathbf{K}$ and $\mathbf{t_1} \in \mathcal{O}_\mathbf{K}^\vee$, we have

$$\begin{aligned}
&\psi(\mathbf{z}) * \phi(\mathbf{x}) \\
&= \left(\boldsymbol{B}(\mathcal{O}_\mathbf{K}) \boldsymbol{U} \boldsymbol{B}(\mathcal{I})^{-1} \mathbf{z} - q \cdot \mathbf{t_0}\right) * \left(\boldsymbol{C}_g \mathbf{x} - q \cdot \mathbf{t_1}\right) \\
&= \boldsymbol{B}(\mathcal{O}_\mathbf{K}) \boldsymbol{U} \boldsymbol{B}(\mathcal{I})^{-1} \mathbf{z} * \boldsymbol{C}_g \mathbf{x} - q \cdot \mathbf{t_0} * \mathbf{g} * \mathbf{x} - q \cdot \boldsymbol{B}(\mathcal{O}_\mathbf{K}) \boldsymbol{U} \boldsymbol{B}(\mathcal{I})^{-1} \mathbf{z} * \mathbf{t_1} + q^2 \cdot \mathbf{t_0} * \mathbf{t_1} \\
&\equiv \boldsymbol{B}(\mathcal{O}_\mathbf{K}) \boldsymbol{U} \boldsymbol{B}(\mathcal{I})^{-1} \mathbf{z} * \boldsymbol{C}_g \mathbf{x} \pmod{q\mathcal{O}_\mathbf{K}^\vee} \qquad (2.18) \\
&\equiv \boldsymbol{C}_g^{-1} \boldsymbol{B}(\mathcal{I})(I - q \cdot \boldsymbol{T}) \boldsymbol{B}(\mathcal{I})^{-1} \mathbf{z} * \boldsymbol{C}_g \mathbf{x} \pmod{q\mathcal{O}_\mathbf{K}^\vee} \\
&\equiv \mathbf{z} * \mathbf{x} - q \cdot \boldsymbol{C}_g^{-1} \boldsymbol{B}(\mathcal{I}) \boldsymbol{T} \boldsymbol{B}(\mathcal{I})^{-1} \mathbf{z} * \boldsymbol{C}_g \mathbf{x} \pmod{q\mathcal{O}_\mathbf{K}^\vee} \\
&\equiv \mathbf{z} * \mathbf{x} - q \cdot \boldsymbol{C}_g \boldsymbol{C}_x \boldsymbol{C}_g^{-1} \boldsymbol{B}(\mathcal{I}) \boldsymbol{T} \boldsymbol{B}(\mathcal{I})^{-1} \mathbf{z} \pmod{q\mathcal{O}_\mathbf{K}^\vee} \\
&\equiv \mathbf{z} * \mathbf{x} - q \cdot \mathbf{x} * \boldsymbol{B}(\mathcal{I}) \boldsymbol{T} \boldsymbol{B}(\mathcal{I})^{-1} \mathbf{z} \pmod{q\mathcal{O}_\mathbf{K}^\vee} \\
&\equiv \mathbf{z} * \mathbf{x} \pmod{q\mathcal{O}_\mathbf{K}^\vee} \qquad (2.19)
\end{aligned}$$

where (2.18) follows by noting that $\mathbf{t_0} * g \in \mathcal{I}$ and $\mathbf{x} \in \mathcal{I}^\vee$ and then employing lemma 2.4.4. Similarly, $\boldsymbol{B}(\mathcal{O}_\mathbf{K}) \boldsymbol{U} \boldsymbol{B}(\mathcal{I})^{-1} \mathbf{z}$ is in $\mathcal{I}$. Also, for the last equation (2.19), we use lemma 2.4.4.

□

2.8 Example Polynomial Rings and non-Bigenic Ideals

In the introduction we considered a slight twist of the cyclotomic polynomial $X^{256}+1$ which is used in the recently announced NIST post-quantum cryptography encryption algorithm CRYSTALS-Kyber [Bos+21]. Cyclotomic polynomials, especially of degree power-of-two, are further preferred as these allow very efficient number-theory transforms (NTT), thus enabling efficient polynomial multiplication. But, it is also well-known that arithmetic modulo "twisted-cyclotomic" irredicible polynomials, say $X^{256}-a$, and modulo q such that a has a 256-th root in $\mathbb{Z}_q$, also enjoy efficient NTT by just pre-multiplying the coefficient vector of a polynomial by the diagonal matrix consisting of powers of $a^{1/256}$. In other words, the Vandermonde matrix of $X^{256}-a$ (modulo q) is the product of Vandermonde matrix of $X^{256}-1$ and the above diagonal matrix.

In the Introduction, we had set $a=-2\cdot 3^2\cdot 13$ for three reasons. First, by Eisenstein criterion, this make $f(X)$ irreducible over $\mathbb{Q}$. Second, using Dedekind index theorem, we showed that $\mathcal{R}$ is strict sub-ring of $\mathcal{O}_{\mathbf{K}}$ in this case. Finally, it can be checked by a computer that $a=-2\cdot 3^2\cdot 13$ is a 256-th residue in the field $\mathbb{Z}_q$ with $q=3329$ as in [Bos+21]. Interestingly, the Kyber proposal chose the prime q to be the smallest prime such that order of q is one modulo 256 and q-RLWE allows for setting up an encryption scheme with non-negligible probability decryption failure. Unfortunately, order of this q is two modulo 512, and hence the 512-th primitive roots of unity only exist in a degree two extension of $\mathbb{Z}_q$. Note, one needs 512-th primitive roots of unity for NTT modulo $X^{256}+1$. This causes a slightly expensive NTT computation depending on whether there is enough parallel processing power available or not. Surprisingly, with $X^{256}-2\cdot 3^2\cdot 13$, after the initial diagonal-matrix transform, we only need 256-th primitive roots, and hence our number field setting potentially allows a more efficient polynomial multiplication modulo q than the cyclotomic number field.

We next turn our attention to the error-distribution implied by the hardness reduction on the RLWE samples, especially in the (polynomial) coefficient setting and not the canonical-embedding

setting, as we want to make sure that the RLWE errors do not overwhelm the payload. However, the error distribution implied for the coefficient setting, while non-spherical, is actually smaller than the spherical-distribution for the cyclotomic setting. This follows from two facts:

1. Theorem 2.7.1 which shows that the error-distribution Υ_α is independent of the number-field, and the hardness-reduction only restricts the scaling α and the variance γ of the underlying hard problem $\mathcal{R}$-DGS_γ in ideal lattice $\mathcal{I}$ by $\gamma \geq \sqrt{2n}/\lambda_1(\mathcal{L}(\mathcal{I})^\vee)$, as long as $\alpha < \sqrt{\log n/n}$,

2. The translation of the error distribution from the canonical embedding back to the ring is composition of two transformations: an isometric transformation following by the inverse of the diagonal transformation. The latter has the j-th diagonal entry $a^{-j/256}$, which is a real number less than and equal to one, with equality only for $j = 0$.

Thus the question boils down to whether $\mathcal{R}$-DGS_γ is easier in $\mathcal{R} = \mathbb{Z}[X]/(X^{256} - a)$ or $\mathcal{R} = \mathbb{Z}[X]/(X^{256} + 1)$. We have focused on showing that the former ring being a non Dedekind domain has less algebraic structure. However, when disregarding the issue of algebraic structure, the ideal lattices in different $\mathbf{K}$ can potentially have different complexity, and this is a well-known open problem to relate ideal lattices of different number fields. We ran some preliminary tests on resistance of ideal-lattice-SVP problem to the LLL algorithm [LLL82], and found no significant difference in the above two rings. However, more rigorous experimentation and analysis is warranted.

2.8.1 Non-bigenic ideals

An ideal will be called *bigenic* if it can be generated by two or less elements of the ring. When $\mathcal{R}$ is a strict subring of $\mathcal{O}_b K$, it is well known that in such a case $\mathcal{R}$ is not a Dedekind domain, and indeed all prime ideals of $\mathcal{R}$ that are not co-prime to the so-called *conductor ideal* of $\mathcal{R}$ are not invertible (see e.g. Theorem 6.1 in [Cond]). Another well-known property of Dedekind domains is that all its ideals are bigenic. However, it is not an easy task to show that some ideal of non Dedekind-domain $\mathcal{R}$ is not bigenic. Although, examples exist of non-bigenic ideals in strict

subrings (of rank n) of $\mathcal{O}_{\mathbf{K}}$ [Cond, Remark 2.3], these subrings are not the polynomial ring $\mathcal{R}$, and moreover these non-bigenic ideals have a diagonal Hermite normal form $\mathbb{Z}$-basis, and in any case these example ideals are as it ideals of the larger ring $\mathcal{O}_{\mathbf{K}}$. We will show below a non-trivial ideal of $\mathcal{R}$ that requires a minimum of three generators.

This example is inspired by [Cone, Example 4.16]. Consider the irreducible (over $\mathbb{Q}$) polynomial $f(X) = X^5 - 2^4 \cdot 3$, and the corresponding number field $\mathbf{K} = \mathbb{Q}[X]/(f(X))$. Consider $\beta = X^4/8$ as an element of $\mathbf{K}$. Its easy to check that $\beta^5 - 2 \cdot 3^4 = 0$, and hence $\beta \in \mathcal{O}_{\mathbf{K}}$. This also shows that $\mathcal{R} = \mathbb{Z}[X]/(f(X))$ is not same as $\mathcal{O}_{\mathbf{K}}$, and hence is not integrally closed and consequently not a Dedekind domain. We now have an easy example of a non-bigenic ideal of $\mathcal{R}$.

Proposition 2.8.1. *The ideal $\mathcal{I} = (8, 2X + 4, X^2 + 4)$ of $\mathcal{R} = \mathbb{Z}[X]/(X^5 - 48)$ has the following properties*

(i) *$\mathcal{I}$ is not bigenic,*

(ii) *no rational scaling of $\mathcal{I}$ is a bigenic ideal of $\mathcal{R}$,*

(iii) *no rational scaling of $\mathcal{I}$ is a fractional ideal of $\mathcal{O}_{\mathbf{K}}$,*

(iv) *the HNF of $\mathbb{Z}$-basis of $\mathcal{I}$ is not diagonal.*

(v) *$\mathcal{I}$ is product of two bigenic ideals, namely $\mathcal{I} = (4, X + 2) \cdot (2, X)$.*

Properties (i) and (v) imply that bigenic ideals of $\mathcal{R}$ above do not form a multiplicative group. This is in contrast to principal ideals that do form a multiplicative group which is the basis of definition of ideal class groups [FT91]. It is worth remarking that $(4, X + 2)$ is not a prime ideal as it is contained in $(2, X + 2)$ and it is well-known that all non-zero prime ideals (of any order of a number field) are maximal [Conb, Sec. 8].

Proof. We focus on proving (i), as the rest will follow easily.

Now, assume to the contrary that this ideal is bigenic and generated by $L0 = (\ell_1, \ell_2)$, and as ideals of $\mathbb{Z}[X]/(X^5 - 48)$, $L0 = \mathcal{I}$. Both ℓ_1 and ℓ_2 must be in the $\mathbb{Z}$-span of $\mathbb{Z}$-basis of the ideal $\mathcal{I}$,

which is depicted below by concatenating the circulant matrices of $8, 2X+4$ and X^2+4. We also compute its Hermite normal form (HNF) [11].

$$\text{HNF}\begin{pmatrix} 4 & 0 & 0 & 48 & 0 & 4 & 0 & 0 & 0 & 96 & 8 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 48 & 2 & 4 & 0 & 0 & 0 & 0 & 8 & 0 & 0 & 0 \\ 1 & 0 & 4 & 0 & 0 & 0 & 2 & 4 & 0 & 0 & 0 & 0 & 8 & 0 & 0 \\ 0 & 1 & 0 & 4 & 0 & 0 & 0 & 2 & 4 & 0 & 0 & 0 & 0 & 8 & 0 \\ 0 & 0 & 1 & 0 & 4 & 0 & 0 & 0 & 2 & 4 & 0 & 0 & 0 & 0 & 8 \end{pmatrix} = \begin{pmatrix} 8 & 4 & 4 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

From the HNF it is clear that ℓ_1 can be written as $a_1X^4 + b_1X^3 + c_1(X^2+4) + d_1(2X+4) + e_1 \cdot 8$ and similarly, ℓ_2 can be written as $a_2X^4 + b_2X^3 + c_2(X^2+4) + d_2(2X+4) + e_2 \cdot 8$, where all of $a_1, ...e_1, a_2, ..., e_2$ are in $\mathbb{Z}$.

Next, note that it suffices to prove that $L1 = (\ell_1, \ell_2, X^5, 48)$ as ideal of $\mathbb{Z}[X]$ does not contain all three of $8, 2X+4$, and X^2+4. We will instead prove something stronger that $L2 = (\ell_1, \ell_2, X^4, 16)$ as ideal of $\mathbb{Z}[X]$ does not contain all three of $8, 2X+4$, and X^2+4.

Further, since we have included X^4 in $L2$, we can now assume w.l.o.g. that a_1 and a_2 are zero. Further, using Euclidean algorithm, w.l.o.g. assume that c_2 is zero. Thus, $\ell_1 = b_1X^3 + c_1(X^2+4) + d_1(2X+4) + e_1 \cdot 8$, and $\ell_2 = b_2X^3 + d_2(2X+4) + e_2 \cdot 8$. Further, since 16 is included in $L2$, e_1 and e_2 can just be restricted to $\{0, 1\}$.

Now, since $L2$ must generate x^2+4, and given that $b_1, ...e_1, b_2, ..., e_2$ are just integers, it is clear that $c_1 = 1 \bmod 16$. Also, it is clear that both e_1 and e_2 cannot be zero, for otherwise 8 cannot be generated. Since c_1 is non-zero, to generate $2x+4$, modulo 16, one can only use ℓ_2 (and not use ℓ_1), and hence $d_2 = 1 \bmod 16$, and $b_2, e_2 = 0 \bmod 16$, which as argued above just means that $e_2 = 0$, and hence $e_1 = 1$. But, this means X^2+4 cannot be generated from $L2$. That completes the proof of (i)

We now go on to prove (ii)-(iv). We have already shown above that the HNF of the ideal $\mathcal{I}$

[11] This has/can been computed by hand, but has also been confirmed by a number theory software.

is not diagonal, so that proves (iv). Since, the ideal $\mathcal{I}$ contains $X^2 + 4$, any rational scaling of $\mathcal{I}$ that keeps it as a subset of $\mathcal{R}$ must be an integer scaling. However, the above proof of non-bigenic nature of $\mathcal{I}$ easily extends to any integer scaling of $\mathcal{I}$.

For (iii), we first show that $\mathcal{I}$ by itself (i.e. without any scaling) is not an ideal of $\mathcal{O}_{\mathbf{K}}$. Recall, $\beta = x^4/8$ is in $\mathcal{O}_{\mathbf{K}}$. We just show that $(2X + 4) \cdot \beta$ is not in $\mathcal{I}$, and hence $\mathcal{I}$ is not closed under multiplication by $\mathcal{O}_{\mathbf{K}}$. To begin with, note that $(X^2 + 4)(X^2 - 4) = (X^4 - 16)$ is in the ideal $\mathcal{I}$. Using this, we have $(2X + 4) \cdot \beta = X^5/4 + X^4/2 = 12 + X^4/2 = 12 + 8$ (modulo $\mathcal{I}$) which is same as 4 modulo 8. Since 4 is not in the ideal $\mathcal{I}$ (of $\mathcal{R}$), this completes the proof.

Next, consider the set $\frac{p}{q} \cdot \mathcal{I}$, for co-prime integers p, q. Again, we just show that $\frac{p}{q}(2X+4) \cdot \beta$ is not in $\frac{p}{q} \cdot \mathcal{I}$. But this is same as checking that $(2X + 4) \cdot \beta$ is not in $\mathcal{I}$, since $\mathcal{R}$ is an integer domain.

To prove (v), note that $(4, X+2) \cdot (2, X) = (8, 2(X+2), 4X, X(X+2))$. This is easily seen to be same as $(8, 2(X+2), 4(X+2), X^2+2(X+2)-4+8)$, and hence is same as $(8, 2(X+2), X^2+4) = \mathcal{I}$. □

Chapter 3: Symmetrically Secure PIR from Ring-LWE

In this chapter, we show how to instantiate a symmetrically secure private information retrieval from the RLWE assumption. We start by providing introduction in Section 3.1. Then we give out necessary definitions in Section 3.2 and present our main construction in Section 3.3. Finally we describe our implementation and evaluate the performance in Section 3.4.

3.1 Introduction

An important application of Ring-LWE based cryptography is to instantiate a practical computationally private information retrieval (PIR) protocol. PIR [Cho+95] allows a client to retrieve a data entry from a server, while hiding which entry was retrieved from the server. It's an important building block which can benefit many privacy preserving applications, including private media steaming [Agu+16; Gup+15], subscription [Che+20a], private group messaging [Che+20b], anonymous communication [Mit+11; AS16; Kwo+16; GKL10], and ad delivery [GLM16]. However, PIR is quite costly. First, it requires the server to process the whole database in order to maintain the privacy of the query. This is inherent, since if certain entries are not processed, the server would know they are not retrieved by the client.

Over the years, there are many PIR protocols in the literature [Agu+16; CMS99; Abu+17; DC14; Kia+15; KO97; LP17; Ste98; GHO19; Döt+19; GR05], including considerable implementation efforts in recent years. There are generally two lines of implementation works. One follows from Gentry and Ramzan [GR05], which has good communication but a high computational cost. The other builds on XPIR by Aguilar-Melchor et. al. [Agu+16]. The later one contains the most efficient implementations to date, who are Ring-LWE based: SealPIR by Angel et. al. [Ang+18], MulPIR by Ali et. al. [Ali+21], and SHECS-PIR by Park and Tibouchi [PT20].

A stronger version of PIR is *Symmetrically Private Information Retrieval (SPIR)* [Ger+00], where we additionally require privacy for the server's data. Specifically, the requirement is that the client should only learn the retrieved data entry, but not any information about any other data entries. This can be useful in many applications where the data consists of sensitive information (e.g., a medical database).

Currently, all these implemented PIR schemes do not satisfy such a security guarantee. For the homomorphic encryption based protocols (the line we will follow), the reason is the following. To improve efficiency, these protocols take advantage of compressing more data into a single ciphertext, allowing the client to retrieve a large chunk of data from each ciphertext (usually more than one entry). Simply reducing the amount of data packed in each ciphertext would cause a large overhead in efficiency. Moreover, even with only one entry packed in one ciphertext, these schemes leak information about the data beyond a single entry. One can apply standard techniques to add data privacy (which is indeed discussed in some of the above works, but not implemented), but this may result in further decrease in efficiency, as well as other disadvantages, discussed below.

Alternatively, we present XSPIR, a practically efficient SPIR scheme. We follow the line of works that started with XPIR and culminated in SealPIR, MulPIR, SHECS-PIR [Agu+16; Ang+18; Ali+21; PT20], and add data privacy against a semi-honest client. Crucially, we use techniques that are directly integrated with the underlying *BFV Leveled Homomorphic Encryption scheme* [Bra12; FV12] (based on the RLWE assumption). This is in contrast with general ways to transform PIR schemes to SPIR schemes as proposed in previous works. For example, [Ali+21] discuss in their appendix how data privacy can be added on top of MulPIR, by using oblivious Pseudorandom Function (OPRF), for which the constructions are mainly based on DDH assumption [MRR20; MR19]. Our technical approach enjoys the following advantages.

- Better security with low overhead: we add data privacy against a semi-honest client (namely, the client cannot learn any information beyond the retrieved entry), while paying only a small price in efficiency. Specifically, compared to the state-of-the-art PIR protocols (which leak information on data), we are about 30-40% slower in computation but 20% better in

communication.

- Extended functionality: since our scheme directly builds on BFV without dependency on extra primitives, we can manipulate the BFV ciphertexts to allow retrieval of more complex functions of data entries (rather than just retrieving an individual entry). For example, if the client wants to query the summation of the cube of two entries (i.e., $x_i^3 + x_j^3$ for entries i and j), we can easily modify our scheme to achieve this functionality (relying on straightforward properties of the BFV scheme). The revelation of the circuit evaluation result will not leak any extra information about the two entries or the rest of the data.

- No new assumption: as an added benefit, our SPIR scheme does not need to rely on any additional assumption beyond the one that is used for PIR (namely RLWE, that is needed for the BFV encryption scheme).

3.1.1 Related Works

PIR Private information retrieval (PIR) was introduced by Chor et al. [Cho+95], and inspired two lines of work: *information theoretic PIR* (IT-PIR) and *computational PIR* (cPIR) (we will use "PIR" to refer to cPIR by default). IT-PIR requires the database to be stored in several non-colluding servers. The client sends a query to each server and gets the result by combining the responses. IT-PIR has relative computational efficiency for each server and is information theoretic secure. However, it cannot be achieved with a single server, and the privacy relies on non-collusion of the servers, which can be problematic in practice [Bei+02; Cho+95; DHS14; DGH12; Gol07]. In contrast, cPIR requires only computational security, and can be achieved with a single server. As previously discussed, there's a long line of works achieving cPIR. The computational cost for the server in all these works is quite high, which is a bottleneck for practical employment. Some of this is inherent: indeed, the server must perform at least linear (in the size of the database) amount of computation per query, or else some information will be leaked (e.g., if an entry is not touched during its computation, the server knows this is not the entry that the client is trying

to retrieve). However, the existing results involve a very heavy computation beyond the size of the data (there is an additional multiplicative overhead depending on the security parameter and underlying cryptographic primitives, which is quite high). Significant progress have been made towards improving efficiency, although it remains a bottleneck.

SPIR Symmetrically private information retrieval (SPIR) was introduced by Gertner et. al. [Ger+00], who showed how transform any PIR scheme to a SPIR scheme, in the information theoretic setting. Modern cPIR schemes can also be transformed to SPIR schemes in generic ways, e.g., using an OPRF, as discussed above. However, to the best of our knowledge, the only existing implementations of SPIR proper are from over 15 years ago, and in Java [Bon+; SJ05]. There are some implementation of related primitives, as we discuss next.

Related Primitives There are several works implementing database access systems with more complex queries, which include some privacy for both the client and the server (cf.,[Jar+13; Pap+14; Fis+15]); However, these schemes do not have full privacy, and allow some leakage of information about the queries.

A closely related primitive is *1-out-of-N Oblivious Transfer (OT)*. This is in fact equivalent to SPIR, but usually used in a different context where N is small, since it typically has a communication cost linear in N (while for PIR/SPIR a major goal is sublinear communication). Indeed, existing OT protocols mainly focus on constant size (say 1-out-of-2) OT, and on extending OT, namely implementing a large number of OT invocations efficiently [MRR21; Rin]. The most efficient 1-out-of-N OT to date (but without implementation) is [MRR20], where the authors construct random OT (retrieving a random location from a random database). In turn, random 1-out-of-N OT can be used at an offline stage to allow for a very efficient (but still linear) online 1-out-of-N OT.

Another relevant primitive is *Private Set Intersection (PSI)* [Mea86; HFH99; CLR17a; Che+18; Con+21]. PSI has two parties, a sender and a receiver, each holding a set of elements, who would like to privately compute the intersection of their sets. We note that most of the homomorphic en-

cryption based PSI [CLR17a; Che+18; Con+21] rely on OPRF. Recently, Li, Lu, and Wu [LLW21] used PSI for *password checkup* based on homomorphic encryption. They use a masking method by multiplying the result with a random vector to mask the redundant data entries. This approach bears some similarity with ours, but there are three problems trying to apply it to SPIR: first, it requires one extra multiplicative level, resulting in an additional overhead in both communication and computation, while our "oblivious masking" technique does not; second, this technique does not directly apply to SPIR because SPIR requires the server to send back an entry with meaningful data, so we cannot directly multiply our result by a random vector of numbers, (while in their case, they just need to send zero back as an indication); third, it doesn't prevent the server from leaking the information about its database-dependent computation due to BFV ciphertext noise, while we solve this problem by "ciphertext sanitization".

3.1.2 Technical Overview

We start with a brief description of how prior PIR protocols that we build on work at a high level. We first *fold the database* as a hypercube (for example, a 2-dimensional matrix), and recursively process the query for each dimension (say rows and then columns) [KO97; Ste98]. Based on the BFV leveled homomorphic encryption scheme [Bra12; FV12], each query is represented as a ciphertext, which would later be *obliviously expanded* to an encrypted 0/1 indicator vector [Ang+18; Ali+21]. The server then homomorphically performs the inner product between those 0/1 indicator vectors and the database, and returns the result. Note that BFV homomorphic encryption scheme allows *packing* multiple plaintexts inside one ciphertext, enabling "single instruction, multiple data" (SIMD) style homomorphic operations [GHS12; SV11; BGH13; Che+19]. The database can be reshaped to pack more than one data entry together for better performance.

Prior PIR constructions, following the above outline, do not achieve data privacy. We identify two main causes of information leakage, and propose new techniques (directly integrated with the BFV encryption scheme) in order to overcome them efficiently.

- With *ciphertext packing* optimization, the client will get more than one data entry from the

server's response ciphertext. A simple solution is to give up on full-capacity ciphertext packing to achieve data privacy. But its price is a great reduction in efficiency, because we can no longer fully utilize the "SIMD"-style operations provided by the underlying BFV scheme. This results more expensive homomorphic operations required during the server's computation. To overcome this problem, we introduce an *"oblivious masking"* procedure, which maintains the ciphertext packing feature, but can efficiently remove the undesired data entries from the packed ciphertext, without letting the server know which data entries are kept. In addition, we integrate the oblivious masking with the PIR query procedure, so it does not introduce any extra communication cost.

- At high level, the PIR protocol works as follow: the client sends some ciphertexts to the server, the server perform some database dependent computation on the received ciphertexts and returns the result to the client. The security of the underlying homomorphic encryption scheme is protecting the information encrypted inside the original ciphertexts. But the server's result could leak information about the computation, and hence give extra information about the database other than the queried entry. We use *ciphertext sanitization* [Gen09; DS16] to make sure that, even with the secret key, the client cannot learn extra information about a ciphertext other than the decrypted message.

3.2 Preliminaries

3.2.1 (Symmetrically) Private Information Retrieval

We focus only on single round cPIR, where the client sends a single query message and the server sends a single response message. Our protocol adheres to this form, as do other recent efficient PIR protocols.

A PIR scheme is parameterized by the database size N,[1] and consists of 3 PPT algorithms:

- $\mathsf{pp} \leftarrow \mathsf{PIR.Setup}(\lambda)$: Instantiate the protocol with security parameter λ.

[1] we leave the size of each element implicit as it does not affect the definition.

- $\mathsf{q} \leftarrow \mathsf{PIR.Query}(i)$: Given an input $i \in [N]$, the client generates a query q to the server.
- $\mathsf{r} \leftarrow \mathsf{PIR.Response}(\mathsf{q}, \mathsf{DB})$: the server takes the client's query q and a database $\mathsf{DB} = (\mathsf{DB}_0, \ldots, \mathsf{DB}_{N-1})$ of N entries, and replies to the client with r.
- $z \leftarrow \mathsf{PIR.Extract}(\mathsf{r})$: the client extracts the information from the server's reply r.

Correctness requires that, for all $i \in [N]$, for any output of the query function $\mathsf{q} \leftarrow \mathsf{PIR.Query}(i)$, for all database DB and reply $\mathsf{r} \leftarrow \mathsf{PIR.Response}(\mathsf{q}, \mathsf{DB})$ generated by the server, it has $\mathsf{PIR.Extract}(\mathsf{r}) = \mathsf{DB}_i$.

Definition 3.2.1 (Query Privacy)**.** *We say a PIR scheme is (computationally) query private if and only if for any two queries i and i', the two distributions $\mathsf{q} \leftarrow \mathsf{PIR.Query}(i)$ and $\mathsf{q} \leftarrow \mathsf{PIR.Query}(i')$ are computationally indistinguishable.*

Definition 3.2.2 (Data Privacy for Semi-Honest Client)**.** *We say a PIR scheme is (computationally) data private if and only if, for all $i \in [N]$, given query $\mathsf{q} \leftarrow \mathsf{PIR.Query}(i)$, for any two databases DB and DB' where $\mathsf{DB}_i = \mathsf{DB}'_i$, the two distributions $\mathsf{r} \leftarrow \mathsf{PIR.Response}(q, \mathsf{DB})$ and $\mathsf{r}' \leftarrow \mathsf{PIR.Response}(q, \mathsf{DB}')$ are computationally indistinguishable.*

In the following part, we use PIR to refer to a PIR scheme with query privacy only, and SPIR (or symmetric PIR) to refer to PIR with both query privacy and with data privacy for semi-honest client. In both cases, we mean computational schemes (with a single server) and one-round of communication as defined above.

We care about 2 types of complexity measures:

- Computational complexity: in particular, the server's running time for $\mathsf{PIR.Response}$ (as well as the client's running time for $\mathsf{PIR.Query}$ and $\mathsf{PIR.Extract}$, but this is typically much smaller, which typically takes only milliseconds and independent of database size).
- Communication complexity: the *upload* cost is measured by $|\mathsf{q}|$ and the *download* cost is measured by $|\mathsf{r}|$.

3.2.2 Homomorphic Encryption

We use homomorphic encryption scheme as a public key encryption scheme that can homomorphically evaluate arithmetic operations on messages inside ciphertexts. We can formulate it as the following 4 PPT algorithms:

- $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{HE.Setup}(1^\lambda)$: Takes security parameter λ as input and outputs public key pk, secret key sk.
- $\mathsf{ct} \leftarrow \mathsf{HE.Enc}(\mathsf{pk}, m)$: Takes pk and a plaintext m as inputs, and outputs a ciphertext ct.
- $\mathsf{ct}' \leftarrow \mathsf{HE.Eval}(\mathsf{pk}, C, (\mathsf{ct}_1, \ldots, \mathsf{ct}_t))$: Takes pk, a circuit C and multiple input ciphertexts $(\mathsf{ct}_1, \ldots, \mathsf{ct}_t)$ and outputs a ciphertext ct'.
- $m' \leftarrow \mathsf{HE.Dec}(\mathsf{sk}, \mathsf{ct})$: Takes sk and a ciphertext ct as input and outputs a plaintext m'.

For correctness, we require that $\mathsf{HE.Dec}(\mathsf{sk}, \mathsf{HE.Enc}(\mathsf{pk}, m)) = m$ for $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{HE.Setup}(1^\lambda)$ and require $\mathsf{HE.Eval}$ to homomorphically apply the circuit C to the plaintext encrypted inside the input ciphertexts.

Definition 3.2.3 (Semantic Security)**.** *We say a homomorphic encryption scheme is semantically secure if and only if for any two messages m and m', the two distributions* $\mathsf{ct} \leftarrow \mathsf{HE.Enc}(\mathsf{pk}, m)$ *and* $\mathsf{ct}' \leftarrow \mathsf{HE.Enc}(\mathsf{pk}, m')$ *are computationally indistinguishable given the public key* pk.

Ciphertext Sanitization Most homomorphic encryption scheme only cares about hiding the encrypted messages. However, the result ciphertext of the homomorphic evaluation could leak some information about the evaluated circuit C, which might be harmful in some applications. One could employ a randomized sanitization proposed by Ducas and Stehlé [DS16] $\mathsf{HE.Sanitize}(\mathsf{pk}, \mathsf{ct})$ to achieve circuit privacy, satisfying the following:

- [Correctness] For any ciphertext ct, $\mathsf{HE.Dec}(\mathsf{sk}, \mathsf{HE.Sanitize}(\mathsf{pk}, \mathsf{ct})) = \mathsf{HE.Dec}(\mathsf{sk}, \mathsf{ct})$;

- [(Statistical) Sanitization] For any two ciphertext $\mathsf{ct}, \mathsf{ct}'$ such that $\mathsf{HE.Dec}(\mathsf{sk}, \mathsf{ct}) = \mathsf{HE.Dec}(\mathsf{sk}, \mathsf{ct}')$, the two distributions after sanitizations $\mathsf{HE.Sanitize}(\mathsf{pk}, \mathsf{ct})$ and $\mathsf{HE.Sanitize}(\mathsf{pk}, \mathsf{ct}')$ are (statistically) indistinguishable given keys pk and sk.

Brakerski/Fan-Vercauteran Scheme We use the Brakerski/Fan-Vercauteran homomorphic encryption scheme [Bra12; FV12], which we refer to as the BFV scheme. Given a polynomial from the cyclotomic ring $R_t = \mathbb{Z}_t[X]/(X^D + 1)$, the BFV scheme encrypts it into a ciphertext consisting of two polynomials, where each polynomial is from a larger cyclotomic ring $R_q = \mathbb{Z}_q[X]/(X^D + 1)$ where $q > t$. We refer to t, q and D as the plaintext modulus, the ciphertext modulus, and the ring size, respectively. We require the ring dimension D to be a power of 2.

In addition to standard homomorphic operations, like addition and multiplication between a ciphertext and another ciphertext/plaintext, BFV scheme also supports *substitution* [Ang+18]. Given an odd integer k and a ciphertext ct encrypting a polynomial $p(x)$, the substitution operation $\mathsf{SUB}(\mathsf{ct}, k)$ returns a ciphertext encrypting the polynomial $p(x^k)$. For example, taking $k = 3$, an encrypted polynomial $3 + x + 5x^3$ can be substituted to be a ciphertext encrypting $3 + x^3 + 5x^9$.

With Enhanced Ring-LWE By Chapter 2, we can also instantiate the BFV scheme on polynomial rings that are non Dedekind domains, by picking an irreducible non cyclotomic modular polynomial. All the homomorphic operations, including the substitution, naturally extend to this case.

The efficient implementation of homomorphic operations, particularly those that involve polynomial multiplications, is crucial for the practicality of homomorphic encryption schemes. These implementations typically rely on fast discrete Fourier transforms or fast number theoretic transforms. However, such implementations require that the modular polynomial, with a degree of D, has D primitive roots over $\mathbb{Z}_q$, where q is the ciphertext modulus. This requirement also holds for cyclotomic rings.

To achieve a more robust security foundation without sacrificing efficiency, we recommend selecting a modular polynomial that is a "twisted cyclotomic" polynomial of the form $X^D - a$,

where a has a D-th root over $\mathbb{Z}_q$. In this case, the primitive roots of $a^{1/D}$ over $\mathbb{Z}_q$ are the primitive roots of $X^D - 1$ over $\mathbb{Z}_q$, scaled by $a^{1/D}$. By selecting a “twisted cyclotomic" polynomial, one can achieve the necessary primitive roots while also ensuring that the polynomial algebraic structure is not easily exploited by potential attackers.

3.3 Constructing XSPIR

In Section 3.3.1, we provide a PIR protocol without data privacy, based on state-of-the-art PIR [Ang+18; Ali+21], which we will use as our starting point. Then in Section 3.3.2, we present our new techniques, and how they can be integrated with the PIR protocol to efficiently provide the data privacy.

3.3.1 PIR from Homomorphic Encryption

Baseline PIR We start from the basis for most state-of-the-art practical PIR protocols. The scheme relies on homomorphic encryption, and its simplest version is the following. Given a database $(\mathsf{DB}_0, \ldots, \mathsf{DB}_{N-1})$ of N entries, the client initiates the query by sending N ciphertexts c_i, where the ciphertext for the desired entry encrypts 1, and all other ciphertexts encrypt 0 (that is, the ciphertexts encrypt an indicator vector). For each ciphertext, the server homomorphically multiplies it by the corresponding entry DB_i from the database, and returns the homomorphic sum of the results $\sum_{i=1}^{N} \mathsf{DB}_i \cdot c_i$, which is the encryption of the desired entry.

To achieve sublinear communication, Kushilevitz, Ostrovsky [KO97] and later Stern [Ste98] proposed applying this scheme recursively: parameterized by the recursion level d, instead of viewing the database as a one-dimensional vector of length N, one can arrange it into a d-dimensional hypercube. Now each entry in the database will be indexed by a length-d vector $(i_0, \ldots, i_{d-1})$ where each index ranges from 0 to $N^{1/d}$. The retrieval process is then handled recursively, where the client sends $N^{1/d}$ ciphertexts for each level (encrypting an appropriate indicator vector), for a total of $d \cdot N^{1/d}$ ciphertexts. The server sends back one ciphertext (resulting from homomorphic operations of addition and multiplication by plaintexts).

Compressing Queries In the above protocol, each ciphertext sent by the client encrypts a single bit, blowing up communication. To reduce communication, SealPIR [Ang+18] and MulPIR [Ali+21] instantiate the underlying homomorphic encryption scheme with the BFV scheme. Recall that in BFV, each ciphertext encrypts an element from cyclotomic ring $\mathbb{Z}_t[X]/(X^D + 1)$ where D is a power of 2, which is a degree-D polynomial with integer coefficient ranging from 0 to $t - 1$ for some large prime t. Now, instead of encrypting a single bit, a BFV ciphertext encrypts a vector consisting of the coefficients of the polynomial (i.e., D elements in $\mathbb{Z}_t$).

Specifically, to represent a query of index i, instead of sending an indicating vector of ciphertexts, SealPIR [Ang+18] first sends an encrypted monomial x^i (which can be viewed as a polynomial with coefficients being the indicating vector for i). The server then runs a procedure called *oblivious expansion* that allows it to obtain the encrypted coefficients and get the 0/1 indicator vector. Later MulPIR [Ali+21] observed that such technique works not only on a monomial x^i, but also for general polynomials, and took advantage of this for polynomials with more than one non-zero coefficients. Details of *oblivious expansion* is shown in Algorithm 3.1.

Figure 3.1 Oblivious Expansion based on [Ang+18; Ali+21].
Given an input ciphertext q encrypting a polynomial $p(x)$ of degree n, return a list of n ciphertexts, encrypting the coefficients of $p(x)$.
Recall the homomorphic substituion operation: given a ciphertext ct encrypting $p(x)$ and an odd integer k, the substitution $\mathsf{SUB}(\mathsf{ct}, k)$ returns a ciphertext encrypting polynomial $p(x^k)$. We know that x^D is equal to -1 on cyclotomic ring $\mathbb{Z}_t[X]/(X^D+1)$. For polynomial $p(x) = \sum_{i=0}^{D-1} d_i \cdot x^i$, substituting it with $k = D+1$ gives $p(x^{D+1}) = \sum_{i=0}^{D-1} d_i \cdot x^{i \cdot D+i} = \sum_{i=0}^{D-1} d_i \cdot (-1)^i \cdot x^i$. Adding it back to $p(x)$ would zero out every coefficient for x_i where i is odd, and double every other coefficients. Repeatedly using similar steps for $k = D/2^j + 1$ on $p(x)$ would zero out every coefficient of x_i where i is not 0, and multiply d_0 by some power of 2. Then with some "shifting" (multiplying with some monomial x^{-2^j}), and dividing by the appropriate power of 2, given a encrypted polynomial $p(x) = \sum_{i=0}^{n-1} d_i \cdot x^i$, one can extract a vector of ciphertexts where the i^{th} ciphertext encrypts d^i.

procedure EXPAND(q, n, D) ▷ D is the ring size for the underlying BFV HE scheme

Find $m = 2^\ell$ such that $m \geq n$

$\mathsf{clist} \leftarrow [\mathsf{q}]$

for $j = 0$ to $\ell - 1$ **do**

for $k = 0$ to $2^\ell - 1$ **do**

$c_0 \leftarrow \mathsf{clist}[k]$

$c_1 \leftarrow x^{-2^j} \cdot c_0$ ▷ scalar multiplication

$c'_k \leftarrow \mathsf{SUB}(c_0, D/2^j + 1) + c_0$

▷ SUB is the substitution in BFV HE scheme

$c'_{k+2^j} \leftarrow \mathsf{SUB}(c_1, D/2^j + 1) + c_1$

end for

$\mathsf{clist} \leftarrow [c'_0, ..., c'_{2^{j+1}-1}]$

end for

$inverse \leftarrow m^{-1} \pmod t$ ▷ t is the plaintext modulus

for k = 0 to $n - 1$ **do**

$r_k \leftarrow \mathsf{clist}[k] \cdot inverse$

end for

return $(r_0, ..., r_{n-1})$

end procedure

Packing More Information As discussed above, the ciphertext encrypts an integer polynomial with degree D and coefficients from $\mathbb{Z}_t$. One could pack at most $D \cdot \lfloor \log t \rfloor$ bits of data inside a single ciphertext. For better efficiency, we should reshape the database so that each entry is of size $D \cdot \lfloor \log t \rfloor$ bits. For a typical choice of parameters for BFV scheme, say $D = 8192$ and $t \approx 2^{20}$ (t being a prime slightly larger than 2^{20}), that's about 20KB data per ciphertext.

Combining all these techniques, we show our PIR construction in Algorithm 3.2. The overall algorithm is the same as the MulPIR algorithm in [Ali+21]. We tuned the parameters in order to increase efficiency in some settings, and to allow us to add data privacy without changing to less efficient BFV parameters, as we do in the next section. Detailed performance comparisons are in section 3.4.

Figure 3.2 A baseline PIR Scheme (following [Ali+21])

procedure PIR.Setup(λ)
  $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{HE.Setup}(1^\lambda)$
  return $(\mathsf{pk}, \mathsf{sk})$
end procedure
procedure PIR.Query($N, d, \mathsf{pk}, i = (i_0, ..., i_{d-1})$)
  Initialize polynomial $p = 0$
  for $j = 0$ to $d - 1$ **do**
    $p \leftarrow p + x^{j \cdot N^{1/d} + i_j}$
  end for
  $\mathsf{q} \leftarrow \mathsf{HE.Enc}(\mathsf{pk}, p)$
  return (q)
end procedure
procedure PIR.Response($\mathsf{DB}, N, d, \mathsf{pk}, \mathsf{q}$)
  $n \leftarrow N^{1/d}$
  $idx \leftarrow$EXPAND$(q, d \cdot n, D)$ ▷ Oblivious expansion in 3.1
  for $k = 0$ to $d - 1$ **do**
    $\mathsf{q}_k \leftarrow [idx[k \cdot n + 0], \ldots, idx[k \cdot n + n - 1]]$
  end for
  $\mathsf{rlist} \leftarrow [\mathsf{DB}_0, \ldots, \mathsf{DB}_{N-1}]$
  $\ell \leftarrow N/n$
  for $k = 0$ to $d - 1$ **do**
    for $i = 0$ to $\ell - 1$ **do**
      $\mathsf{r}_i \leftarrow \langle \mathsf{q}_k, [\mathsf{rlist}[0 \cdot \ell + i], \ldots, \mathsf{rlist}[(n-1) \cdot \ell + i]] \rangle$
    end for
    $\mathsf{rlist} \leftarrow [\mathsf{r}_0, \ldots, \mathsf{r}_{\ell-1}]$
    $\ell \leftarrow \ell/n$
  end for
  $\mathsf{r} \leftarrow \mathsf{rlist}[0]$
  return r
end procedure

3.3.2 XSPIR: Adding Data Privacy

So far, we described efficient standard PIR. However, this protocol (like the ones it was based on) leaks information about the data, even to an honest client. To achieve data privacy, we need to address the following two problems:

- As previously discussed, to better utilize the plaintext space of the BFV scheme and improve efficiency, we reshaped the database so that each entry now fits in a degree-D polynomial with coefficients from $\mathbb{Z}_t$, which packs $D \cdot \lfloor \log t \rfloor$ bits of information. If the client is only allowed to learn, say, a single element from $\mathbb{Z}_t$, a simple solution would be to pack only one coefficient inside each ciphertext. However, this solution is very costly. Is it possible to pack many values (say D) inside one ciphertext for better efficiency, while the client cannot learn extra information except for only one of them?

- The server computes a *deterministic* $\mathsf{PIR.Response}$ procedure that depends on every part of the database. The output naturally leaks information about the server's computation and hence other parts of the database. Consider the following simple example: the client is fetching 0-th entry from a database $\mathsf{DB} = (\mathsf{DB}_0, \mathsf{DB}_1)$ with 2 entries. After learning DB_0, the client can learn DB_1 by iterating over all possible values and simulating the server's computation. Is there a way to make the server's output ciphertext irrelevant for any part of the database other than the retrieved entry?

Instead of taking a generic approach as suggested by [Ali+21], we show how to efficiently achieve the data privacy by directly taking advantage of the underlying BFV homomorphic encryption scheme.

Oblivious Masking In the previous PIR construction, one ciphertext encrypts a polynomial $p(x) = \sum_{i=0}^{D-1} d_i \cdot x^i$, where each d_i is a part of the reshaped data entry that lies in $\mathbb{Z}_t$. To address the first problem above, if the client is only allowed to learn d_k for some $k \in [D]$, we need an efficient way to obliviously remove unnecessary information (the other coefficients).

Let us start with a first attempt. To keep only the k-th part d_k of the polynomial $p(x)$, the client could send another ciphertext encrypting x^{-k}, and the server can multiply them together to get $p'(x) = x^{-k} \cdot p(x) = \sum_{i=0}^{D-1} d_i \cdot x^{i-k}$. In this case, the constant coefficient is what we are looking for. We could use a similar procedure to oblivious expansion in Algorithm 3.1 to extract it out.

This method brings an additional overhead as the client needs to send an additional ciphertext encrypting x^{-k}. To save this communication overhead, we observe that the client is not fully utilizing the plaintext space $\mathbb{Z}_t[X]/(X^D + 1)$, as the query ciphertexts sent by the client are polynomials with $0/1$ coefficients. We could embed the information k in those coefficients without introducing a new monomial, with an alternative packing technique.

First, instead of sending a new ciphertext encrypting x^{-k}, we put k into the first query ciphertext sent by the client. For example, instead of sending x^i for some index i, we send $(k+1) \cdot x^i$. After the oblivious expansion, the server can sum up the results to obtain a ciphertext encrypting a constant polynomial $(k + 1)$. It requires $t > D$, which is almost always the case.

Second, instead of packing data entires $(d_0, \ldots, d_{D-1})$ into the coefficients of a polynomial, we would find a polynomial $p(x)$ such that $p(\omega_i) = d_i$ using number-theoretic transformation, where ω_i is the i-th root of unity in $\mathbb{Z}_t$, similar to the technique shown in [SV11]. Our goal is then to keep only the information on $p(\omega_k) = d_k$. To achieve this, we could add a random polynomial with $r(\omega_k) = 0$ to it. We first find a polynomial $q(x)$ with $q(\omega_i) = -(i+1)$. Adding to it a constant polynomial $(k + 1)$ results in a new polynomial $q'(\omega_i) = k - i$. Finally, multiplying it by a random polynomial gives us what we want.

Such technique also works when the client is retrieving more than one consecutive elements in $\mathbb{Z}_t$. For example, if every data entry fits in 2 elements of $\mathbb{Z}_t$, we could find the polynomial $q(x)$ with $q(\omega_i) = \lfloor -(i/2 + 1) \rfloor$ instead of $-(i + 1)$. And the rest of the computation would be the same.

Ciphertext Sanitization To address the second problem and make sure that the result doesn't contain information about other parts of the database, one way is to use the ciphertext sanitization procedure proposed by Ducas and Stehlé [DS16]. For efficiency, we use a simpler way of re-

randomization, which is noise flooding [Gen09; DS16]. Specifically, before sending back the result, the server adds an encryption of zero to it with certain amount of noise, so that the result will be statistically close to a freshly encrypted ciphertext. To achieve statistical distance of 2^{-s}, a standard smudging lemma [Ash+12] shows that it suffices to add to it an encryption of 0 with noise level $s + \log_2 D$ bits higher than the original ciphertext.

We apply all these techniques to our PIR scheme to make it into a SPIR scheme, which we call XSPIR. See Algorithm 3.3 for the detailed scheme.

Figure 3.3 XSPIR: Our SPIR Scheme
Blue lines are differences from the previous PIR protocol 3.2

procedure PIR.Setup(λ)
  $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{HE.Setup}(1^\lambda)$
  return $(\mathsf{pk}, \mathsf{sk})$
end procedure
procedure PIR.Query($N, d, \mathsf{pk}, i = (i_0, ..., i_{d-1}, k)$)
  Initialize polynomial $p = 0$
  for $j = 0$ to $d - 1$ **do**
    $p \leftarrow p + (k + 1) \cdot x^{j \cdot N^{1/d} + i_j}$
  end for
  $\mathsf{q} \leftarrow \mathsf{HE.Enc}(\mathsf{pk}, p)$
  return (q)
end procedure
procedure PIR.Response($\mathsf{DB}, N, d, \mathsf{pk}, \mathsf{q}$)
  $n \leftarrow N^{1/d}$
  $idx \leftarrow$EXPAND$(q, d \cdot n, D)$
  for $k = 0$ to $d - 1$ **do**
    $\mathsf{q}_k \leftarrow [idx[k \cdot n + 0], \ldots, idx[k \cdot n + n - 1]]$
  end for
  $\mathsf{rlist} \leftarrow [\mathsf{DB}_0, \ldots, \mathsf{DB}_{N-1}]$
  $\ell \leftarrow N/n$
  for $k = 0$ to $d - 1$ **do**
    for $i = 0$ to $\ell - 1$ **do**
      $\mathsf{r}_i \leftarrow \langle \mathsf{q}_k, [\mathsf{rlist}[0 \cdot \ell + i], \ldots, \mathsf{rlist}[(n - 1) \cdot \ell + i]] \rangle$
    end for
    $\mathsf{rlist} \leftarrow [\mathsf{r}_0, \ldots, \mathsf{r}_{\ell-1}]$
    $\ell \leftarrow \ell/n$
  end for
  $\mathsf{r} \leftarrow \mathsf{rlist}[0]$
  $\mathsf{pt} \leftarrow (-1, \ldots, -D)$ ▷ Making a plaintext polynomial, where $\mathsf{pt}(\omega_i) = -(i + 1)$

3.3.3 Security

The query privacy (see definition 3.2.1) follows directly from the semantic security of the underlying BFV homomorphic encryption scheme [Bra12; FV12]. As the client is sending encrypted indices, and the semantic security (see definition 3.2.3) guarantees that the server cannot learn any information from the ciphertext.

Data privacy against semi-honest clients (see definition 3.2.2) is more complex. For all $k \in [N]$, given client's query $\mathsf{q} \leftarrow \mathsf{PIR.Query}(k)$, for any two databases DB and DB' where $\mathsf{DB}_k = \mathsf{DB}'_k$, consider the following two distributions $\mathsf{r} \leftarrow \mathsf{PIR.Response}(q, \mathsf{DB})$ and $\mathsf{r}' \leftarrow \mathsf{PIR.Response}(q, \mathsf{DB}')$.

Ciphertext sanitization (see 3.2.2 and [DS16]) guarantees that, for any ciphertext ct encrypting some polynomial p, the distribution $\mathsf{HE.Sanitize}(\mathsf{pk}, \mathsf{ct})$ is indistinguishable from a freshly encrypted ciphertext $\mathsf{HE.Enc}(\mathsf{pk}, p)$. Therefore both r and r' are indistinguishable from the fresh encryption of their underlying messages, respectively. We further show that r and r' encrypt messages from the same distribution. WLOG, assume that the whole database can be packed into one ciphertext and $D = N$. It is not hard to extend the argument to the general case of $N > D$. The ciphertext r is encrypting a polynomial p whose coefficients are in $\mathbb{Z}_t$ such that $p(\omega_i) = (k+1) \cdot \mathsf{DB}_i + (k-i) \cdot r_i$ where r_i is uniformly distributed over $\mathbb{Z}_t$. If $i = k$, we have $p(\omega_k) = (k+1) \cdot \mathsf{DB}_k$. Otherwise $p(\omega_i)$ is distributed uniformly at random over $\mathbb{Z}_t$ for $k \neq i \in [D]$. Similar argument works for r': r' is encrypting a polynomial p' such that $p'(\omega_i)$ is a uniform random element from $\mathbb{Z}_t$ for $i \neq k$ and $p'(\omega_k) = (k+1) \cdot \mathsf{DB}'_k = (k+1) \cdot \mathsf{DB}_k = p(\omega_k)$.

3.4 Implementation and Evaluation

In this section, we describe our implementation, evaluate its performance, and compare it with previous implementations. One thing to note is that, since there are no public modern SPIR implementations, we could only compare our XSPIR protocol with the state-of-the-art PIR protocols (which is not data private). We show that our performance is comparable to state-of-the-art PIR protocols while providing a stronger security guarantee.

Implementation and Experimental Setup Our scheme is implemented on top of the SEAL homomorphic encryption library version 3.5.6 [Seaa], with C++. We use the EXPAND algorithm from SealPIR. For SealPIR, we use the publicly available source code [Seab], and run under the same environment, integrating it with our testing framework.

All experiments are running on a CPU 8th Gen Intel® Core™ i7-8550U quad-core processor, 4.2GHz Max Turbo and 16 GB RAM, and with operating system Ubuntu 16.04. The numbers are averages of 100 trials, where the standard deviations are less than 10% of the reported means. The SealPIR code is running with the parameters suggested by their paper and code. We implement the MulPIR on our code base with their suggested parameters. We cannot compare with SHECS-PIR [PT20], as their code is not publicly available. However, according to our analysis based the data provided by [PT20], our XSPIR performance would be comparable to theirs as well (with some variations depending on the entry size).

3.4.1 Parameter Choices

We have two security parameters, a computational security parameter for the underlying BFV scheme, and a statistical security parameter to apply noise flooding (necessary for ciphertext sanitization towards data privacy). We set our statistical security parameter to $s = 40$, as suggested by standard practice, and widely used in many other works [CLR17b; OOS17; Kol+16]. According to the smudging lemma in [Ash+12], an additional noise of $s + \log D$ bits is applied to guarantee a statistical distance of $\leq 2^{-s}$. We set our computational security parameter to $\lambda = 128$ as suggested by [Alb+18]. We set our ring size to be $D = 8192$ and therefore according to [Alb+18], we have a noise budget of 218 bits with $D = 8192, \lambda = 128$. For statistical secure parameter $s = 40$, we would then need $40 + \log_2(8192) = 53$ bits of extra noise, which gives our 165 bits of noise budget left for our entire computation. To accommodate 2.5 bytes per slot of a ciphertext, we need a prime plaintext modulus t of 21 bits, so for each level of multiplicative depth, we consume roughly 20-30 bits of noise budget. This is sufficient for a recursion level of $d = 2$, which is the most efficient choice. As for $d > 2$, the depth of homomorphic multiplication increases, and therefore results in

Size of database	18M	72M	288M	1.125GB
XSPIR (Server Time, ms)	1735	4921	14531	41853
SealPIR (Server Time, ms)	591	1571	6052	21675
MulPIR (Server Time, ms)	1322	3853	10785	30217
XSPIR (Upload, KB)	123	123	123	123
SealPIR (Upload, KB)	61.2	61.2	61.2	61.2
MulPIR (Upload, KB)	122	122	122	122
XSPIR (Download, KB)	73	73	73	73
SealPIR (Download, KB)	307	307	307	307
MulPIR (Download, KB)	119	119	119	119
XSPIR (Communication, KB)	196	196	196	196
SealPIR (Communication, KB)	368.2	368.2	368.2	368.2
MulPIR (Communication, KB)	241	241	241	241

Table 3.1: Entry size = 288 bytes and ring dimensions are set to 4096. In blue color is XSPIR from Algorithm 3.3. Although there is only one ciphertext involved in both upload and download communication. Its size varies because of the modulus switching. Other entries are PIR schemes without data privacy: SealPIR [Ang+18], MulPIR [Ali+21].

more computational cost. Therefore, for best performance, we set $D = 8192, d = 2$ for security requirement $\lambda = 128, s = 40$.

To maximize the efficiency, we pack totally 8192×2.5bytes = 20 KB into one ciphertext. In our experiments, we select entry size = 288 bytes (this does not influence the performance, we but we select the same entry size as in previous works for better comparison). Given this entry size, we can pack at most 71 entries into one single ciphertext.

3.4.2 Experimental Comparisons

To evaluate how our scheme works, we run a series of microbenchmarks to measure: (1) computational cost on the server's side, (2) upload communication cost, and (3) download communication cost. The total communication cost is measured by the sum of upload cost and download cost. Our detailed comparisons and data are recorded in Table 3.1.

As shown in the table, for all database sizes tested, our communication cost is about 25% better than MulPIR and around 50% better than SealPIR, while our performance is about 40-50% worse

than MulPIR and about 2-3 times worse than SealPIR. Recall that the goal in MulPIR was to obtain better communication (compared to SealPIR), at the price of worse computation. Our scheme can be viewed as going even further in that direction, but more importantly, adding a better security guarantee, for the database as well.

3.4.3 Comparison to 1-out-of-n OT

As mentioned in Section 3.1.1, SPIR is technically equivalent to 1-out-of-N OT, although the later one is typically used in different contexts. Accordingly, the existing open-source codes [Rin] for OT's focus on OT extensions, running multiple OT's at the same time. We thus can't run their library for executing a single (or a small number of) retrievals with the relatively huge database size we run experiments with, as in our XSPIR.

We next try to compare our XSPIR scheme to the state of the art 1-out-of-N OT by McQuoid et. al. [MRR20]. Since this is not impelemented, we only compare the asymptotics. In our scheme, the communication is $O(N^{1/d})$, and the server's computation is $O(N + d \cdot N^{1/d})$ homomorphic operations. In [MRR20], they construct *random* OT, where both the query and the database are selected at random (this is typical in settings where this is used for an initial offline computation phase).

Typically, the purpose of using a 1-out-of-N random OT is to move most of the computation to an offline stage, where the random OT protocol is performed. Then, in the online stage when the client receives the actual query, it sends the difference between that and the random query used to the server. The server rotates the random data by that shift, and uses it to mask the actual database. It then sends the whole masked database to the client. The client can unmask the desired entry using the value obtained in the random OT phase. Using the random OT scheme of [MRR20] in this way, we obtain a 1-out-of-N random OT with server time of $O(N)$ exponentiations, upload cost of $O(1)$, and download cost of $O(N)$. This gives worse communication (which is no longer sublinear!) but better computational cost than our protocol asymptotically.

References

[Reg05] Oded Regev. "On lattices, learning with errors, random linear codes, and cryptography". In: *37th Annual ACM Symposium on Theory of Computing*. Ed. by Harold N. Gabow and Ronald Fagin. Baltimore, MA, USA: ACM Press, 2005, pp. 84–93.

[LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. "On Ideal Lattices and Learning with Errors over Rings". In: *Advances in Cryptology – EUROCRYPT 2010*. Ed. by Henri Gilbert. Vol. 6110. Lecture Notes in Computer Science. French Riviera: Springer, Heidelberg, Germany, 2010, pp. 1–23.

[Gen09] Craig Gentry. "Fully homomorphic encryption using ideal lattices". In: *41st Annual ACM Symposium on Theory of Computing*. Ed. by Michael Mitzenmacher. Bethesda, MD, USA: ACM Press, 2009, pp. 169–178.

[BGV12] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. "(Leveled) fully homomorphic encryption without bootstrapping". In: *ITCS 2012: 3rd Innovations in Theoretical Computer Science*. Ed. by Shafi Goldwasser. Cambridge, MA, USA: Association for Computing Machinery, 2012, pp. 309–325.

[Bra12] Zvika Brakerski. "Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP". In: *Advances in Cryptology – CRYPTO 2012*. Ed. by Reihaneh Safavi-Naini and Ran Canetti. Vol. 7417. Lecture Notes in Computer Science. Santa Barbara, CA, USA: Springer, Heidelberg, Germany, 2012, pp. 868–886.

[FV12] Junfeng Fan and Frederik Vercauteren. *Somewhat Practical Fully Homomorphic Encryption*. Cryptology ePrint Archive, Report 2012/144. `https://eprint.iacr.org/2012/144`. 2012.

[GSW13] Craig Gentry, Amit Sahai, and Brent Waters. "Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based". In: *Advances in Cryptology – CRYPTO 2013, Part I*. Ed. by Ran Canetti and Juan A. Garay. Vol. 8042. Lecture Notes in Computer Science. Santa Barbara, CA, USA: Springer, Heidelberg, Germany, 2013, pp. 75–92.

[DM15] Léo Ducas and Daniele Micciancio. "FHEW: Bootstrapping Homomorphic Encryption in Less Than a Second". In: *Advances in Cryptology – EUROCRYPT 2015, Part I*. Ed. by Elisabeth Oswald and Marc Fischlin. Vol. 9056. Lecture Notes in Computer Science. Sofia, Bulgaria: Springer, Heidelberg, Germany, 2015, pp. 617–640.

[Chi+16] Ilaria Chillotti et al. "Faster Fully Homomorphic Encryption: Bootstrapping in Less Than 0.1 Seconds". In: *Advances in Cryptology – ASIACRYPT 2016, Part I*. Ed. by

Jung Hee Cheon and Tsuyoshi Takagi. Vol. 10031. Lecture Notes in Computer Science. Hanoi, Vietnam: Springer, Heidelberg, Germany, 2016, pp. 3–33.

[Che+17] Jung Hee Cheon et al. "Homomorphic Encryption for Arithmetic of Approximate Numbers". In: *Advances in Cryptology – ASIACRYPT 2017, Part I*. Ed. by Tsuyoshi Takagi and Thomas Peyrin. Vol. 10624. Lecture Notes in Computer Science. Hong Kong, China: Springer, Heidelberg, Germany, 2017, pp. 409–437.

[PRS17] Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz. "Pseudorandomness of ring-LWE for any ring and modulus". In: *49th Annual ACM Symposium on Theory of Computing*. Ed. by Hamed Hatami, Pierre McKenzie, and Valerie King. Montreal, QC, Canada: ACM Press, 2017, pp. 461–473.

[RSW18] Miruna Rosca, Damien Stehlé, and Alexandre Wallet. "On the Ring-LWE and Polynomial-LWE Problems". In: *Advances in Cryptology – EUROCRYPT 2018, Part I*. Ed. by Jesper Buus Nielsen and Vincent Rijmen. Vol. 10820. Lecture Notes in Computer Science. Tel Aviv, Israel: Springer, Heidelberg, Germany, 2018, pp. 146–173.

[PP19] Chris Peikert and Zachary Pepin. "Algebraically Structured LWE, Revisited". In: *TCC 2019: 17th Theory of Cryptography Conference, Part I*. Ed. by Dennis Hofheinz and Alon Rosen. Vol. 11891. Lecture Notes in Computer Science. Nuremberg, Germany: Springer, Heidelberg, Germany, 2019, pp. 1–23.

[BBS21] M. Bolboceanu, Z. Brakerski, and D. Sharma. *On Algebraic Embedding for Unstructures Lattices*. `https://eprint.iacr.org/2021/053.pdf`. 2021.

[BF14] J.-F. Biasse and C. Fieker. "Subexponential class group and unit group computation in large degree number fields". In: *LMS J. Comput. Math.* 17 (suppl. A) (2014), pp. 385–403.

[BS16] J.-F. Biasse and F. Song. "A polynomial time quantum algorithm for computing class groups and solving the principal ideal problem in arbitrary degree number fields". In: *Proc. SODA* (2016).

[Ang+18] Sebastian Angel et al. "PIR with Compressed Queries and Amortized Query Processing". In: *2018 IEEE Symposium on Security and Privacy*. San Francisco, CA, USA: IEEE Computer Society Press, 2018, pp. 962–979.

[Ali+21] Asra Ali et al. "Communication–Computation Trade-offs in PIR". In: *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Aug. 2021. ISBN: 978-1-939133-24-3.

[PT20] Jeongeun Park and Mehdi Tibouchi. "SHECS-PIR: Somewhat Homomorphic Encryption-Based Compact and Scalable Private Information Retrieval". In: *Computer Security*

– *ESORICS 2020*. Ed. by Liqun Chen et al. Cham: Springer International Publishing, 2020, pp. 86–106. ISBN: 978-3-030-59013-0.

[Agu+16] Carlos Aguilar Melchor et al. "XPIR: Private Information Retrieval for Everyone". In: *Proceedings on Privacy Enhancing Technologies* 2016.2 (Apr. 2016), pp. 155–174.

[MRR20] Ian McQuoid, Mike Rosulek, and Lawrence Roy. *Minimal Symmetric PAKE and 1-out-of-N OT from Programmable-Once Public Functions*. Cryptology ePrint Archive, Report 2020/1043. `https://eprint.iacr.org/2020/1043`. 2020.

[MR19] Daniel Mansy and Peter Rindal. "Endemic Oblivious Transfer". In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. CCS '19. Association for Computing Machinery, 2019. ISBN: 9781450367479.

[Cona] Keith Conrad. *DEDEKIND'S INDEX THEOREM*. Expository papers/Lecture notes. Available at: `https://kconrad.math.uconn.edu/blurbs/gradnumthy/dedekind-index-thm.pdf`.

[Bos+21] Joppe W. Bos et al. "CRYSTALS - Kyber, NIST PQC 3rd Round Submission". In: `https://pq-crystals.org/kyber/data/kyber-specification-round3-20210804.pdf`. 2021.

[Berb] D. Berstein. "A subfield-logarithm attack against ideal lattices". In: (Feb 2014).

[CGS14] P. Campbell, M. Groves, and D. Shepherd. "Soliloquy: A cautionary tale". In: *ETSI 2nd Quantum-Safe Crypto Workshop* (2014).

[Cra+16] Ronald Cramer et al. "Recovering Short Generators of Principal Ideals in Cyclotomic Rings". In: *Advances in Cryptology – EUROCRYPT 2016, Part II*. Ed. by Marc Fischlin and Jean-Sébastien Coron. Vol. 9666. Lecture Notes in Computer Science. Vienna, Austria: Springer, Heidelberg, Germany, 2016, pp. 559–585.

[FT91] A. Fröhlich and M. J. Taylor. *Algebraic Number Theory*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1991.

[Conb] Keith Conrad. *Ideal Factorization*. Expository paper. url: `https://kconrad.math.uconn.edu/blurbs/gradnumthy/idealfactor.pdf`.

[AM69] Michael Francis Atiyah and I. G. MacDonald. *Introduction to commutative algebra.* Addison-Wesley-Longman, 1969, pp. I–IX, 1–128. ISBN: 978-0-201-40751-8.

[PR07] Chris Peikert and Alon Rosen. "Lattices that admit logarithmic worst-case to average-case connection factors". In: *39th Annual ACM Symposium on Theory of Computing*.

Ed. by David S. Johnson and Uriel Feige. San Diego, CA, USA: ACM Press, 2007, pp. 478–487.

[Cla84] A. Clark. *Elements of Abstract Algebra*. Dover Books on Mathematics Series. Dover Publications, 1984. ISBN: 9780486647258.

[Cond] Keith Conrad. *The conductor ideal of an order*. Expository paper. url: https://kconrad.math.uconn.edu/blurbs/gradnumthy/conductor.pdf.

[Bol+19] Madalina Bolboceanu et al. "Order-LWE and the Hardness of Ring-LWE with Entropic Secrets". In: *Advances in Cryptology – ASIACRYPT 2019, Part II*. Ed. by Steven D. Galbraith and Shiho Moriai. Vol. 11922. Lecture Notes in Computer Science. Kobe, Japan: Springer, Heidelberg, Germany, 2019, pp. 91–120.

[Sho94] Peter W. Shor. "Algorithms for Quantum Computation: Discrete Logarithms and Factoring". In: *35th Annual Symposium on Foundations of Computer Science*. Santa Fe, NM, USA: IEEE Computer Society Press, 1994, pp. 124–134.

[Ste+09] Damien Stehlé et al. "Efficient Public Key Encryption Based on Ideal Lattices". In: *Advances in Cryptology – ASIACRYPT 2009*. Ed. by Mitsuru Matsui. Vol. 5912. Lecture Notes in Computer Science. Tokyo, Japan: Springer, Heidelberg, Germany, 2009, pp. 617–635.

[LS15] Adeline Langlois and Damien Stehlé. "Worst-case to average-case reductions for module lattices". In: *Des. Codes Cryptogr.* 75.3 (2015), pp. 565–599.

[PZ89] M. Pohst and H. Zassenhaus. *Algorithmic algebraic number theory*. Cambridge univ. Press, 1989.

[MR07] Daniele Micciancio and Oded Regev. "Worst-case to average-case reductions based on Gaussian measures". In: *SIAM Journal on Computing* 37.1 (2007), pp. 267–302.

[LLL82] Arjen Lenstra, Hendrik Lenstra, and Laszlo Lovasz. "Factoring Polynomials with Rational Coefficients". In: *Mathematische Annalen* 261 (1982), pp. 515–534.

[Conc] Keith Conrad. *NOETHERIAN RINGS*. Expository paper. url: https://kconrad.math.uconn.edu/blurbs/ringtheory/noetherian-ring.pdf.

[Kap73] Irving Kaplansky. "Commutative rings". In: *Conference on Commutative Algebra*. Springer. 1973, pp. 153–166.

[Eis13] David Eisenbud. *Commutative algebra: with a view toward algebraic geometry*. Vol. 150. Springer Science & Business Media, 2013.

[Coh93] Henri Cohen. *A course in computational algebraic number theory*. Vol. 8. Springer-Verlag Berlin, 1993.

[DD12] Léo Ducas and Alain Durmus. "Ring-LWE in Polynomial Rings". In: *PKC 2012: 15th International Conference on Theory and Practice of Public Key Cryptography*. Ed. by Marc Fischlin, Johannes Buchmann, and Mark Manulis. Vol. 7293. Lecture Notes in Computer Science. Darmstadt, Germany: Springer, Heidelberg, Germany, 2012, pp. 34–51.

[Cone] Keith Conrad. *The different ideal*. Expository papers/Lecture notes. Available at: `https://kconrad.math.uconn.edu/blurbs/gradnumthy/different.pdf`.

[Reg06] Oded Regev. "Lattice-Based Cryptography (Invited Talk)". In: *Advances in Cryptology – CRYPTO 2006*. Ed. by Cynthia Dwork. Vol. 4117. Lecture Notes in Computer Science. Santa Barbara, CA, USA: Springer, Heidelberg, Germany, 2006, pp. 131–141.

[Reg10] Oded Regev. "The Learning with Errors Problem (Invited Survey)". In: *2010 IEEE 25th Annual Conference on Computational Complexity*. 2010, pp. 191–204.

[Cho+95] Benny Chor et al. "Private Information Retrieval". In: *36th Annual Symposium on Foundations of Computer Science*. Milwaukee, Wisconsin: IEEE Computer Society Press, 1995, pp. 41–50.

[Gup+15] Trinabh Gupta et al. *Scalable and private media consumption with Popcorn*. Cryptology ePrint Archive, Report 2015/489. `https://eprint.iacr.org/2015/489`. 2015.

[Che+20a] Raymond Cheng et al. *Talek: a Private Publish-Subscribe Protocol*. In Submission. `https://raymondcheng.net/download/papers/talek-tr.pdf`. 2020.

[Che+20b] Raymond Cheng et al. *Talek: Private Group Messaging with Hidden Access Patterns*. Cryptology ePrint Archive, Report 2020/066. `https://eprint.iacr.org/2020/066`. 2020.

[Mit+11] Prateek Mittal et al. "PIR-Tor: Scalable Anonymous Communication Using Private Information Retrieval". In: *USENIX Security 2011: 20th USENIX Security Symposium*. San Francisco, CA, USA: USENIX Association, 2011.

[AS16] Sebastian Angel and Srinath Setty. "Unobservable Communication over Fully Untrusted Infrastructure". In: *USENIX Security 2016: 25th USENIX Security Symposium*. Ed. by Thorsten Holz and Stefan Savage. USENIX Association, 2016.

[Kwo+16] Albert Kwon et al. “Riffle: An Efficient Communication System With Strong Anonymity”. In: *Proceedings on Privacy Enhancing Technologies* 2016.2 (Apr. 2016), pp. 115–134.

[GKL10] Jens Groth, Aggelos Kiayias, and Helger Lipmaa. “Multi-query Computationally-Private Information Retrieval with Constant Communication Rate”. In: *PKC 2010: 13th International Conference on Theory and Practice of Public Key Cryptography*. Ed. by Phong Q. Nguyen and David Pointcheval. Vol. 6056. Lecture Notes in Computer Science. Paris, France: Springer, Heidelberg, Germany, 2010, pp. 107–123.

[GLM16] Matthew Green, Watson Ladd, and Ian Miers. “A Protocol for Privately Reporting Ad Impressions at Scale”. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. CCS ’16. Association for Computing Machinery, 2016. ISBN: 9781450341394.

[CMS99] Christian Cachin, Silvio Micali, and Markus Stadler. “Computationally Private Information Retrieval with Polylogarithmic Communication”. In: *Advances in Cryptology – EUROCRYPT’99*. Ed. by Jacques Stern. Vol. 1592. Lecture Notes in Computer Science. Prague, Czech Republic: Springer, Heidelberg, Germany, 1999, pp. 402–414.

[Abu+17] Hamza Abusalah et al. “Beyond Hellman’s Time-Memory Trade-Offs with Applications to Proofs of Space”. In: *Advances in Cryptology – ASIACRYPT 2017, Part II*. Ed. by Tsuyoshi Takagi and Thomas Peyrin. Vol. 10625. Lecture Notes in Computer Science. Hong Kong, China: Springer, Heidelberg, Germany, 2017, pp. 357–379.

[DC14] Changyu Dong and Liqun Chen. “A Fast Single Server Private Information Retrieval Protocol with Low Communication Cost”. In: *ESORICS 2014: 19th European Symposium on Research in Computer Security, Part I*. Ed. by Miroslaw Kutylowski and Jaideep Vaidya. Vol. 8712. Lecture Notes in Computer Science. Wroclaw, Poland: Springer, Heidelberg, Germany, 2014, pp. 380–399.

[Kia+15] Aggelos Kiayias et al. “Optimal Rate Private Information Retrieval from Homomorphic Encryption”. In: *Proceedings on Privacy Enhancing Technologies* 2015.2 (Apr. 2015), pp. 222–243.

[KO97] Eyal Kushilevitz and Rafail Ostrovsky. “Replication is NOT Needed: SINGLE Database, Computationally-Private Information Retrieval”. In: *38th Annual Symposium on Foundations of Computer Science*. Miami Beach, Florida: IEEE Computer Society Press, 1997, pp. 364–373.

[LP17] Helger Lipmaa and Kateryna Pavlyk. “A Simpler Rate-Optimal CPIR Protocol”. In: *FC 2017: 21st International Conference on Financial Cryptography and Data Security*. Ed. by Aggelos Kiayias. Vol. 10322. Lecture Notes in Computer Science. Sliema, Malta: Springer, Heidelberg, Germany, 2017, pp. 621–638.

[Ste98] Julien P. Stern. "A New Efficient All-Or-Nothing Disclosure of Secrets Protocol". In: *Advances in Cryptology – ASIACRYPT'98*. Ed. by Kazuo Ohta and Dingyi Pei. Vol. 1514. Lecture Notes in Computer Science. Beijing, China: Springer, Heidelberg, Germany, 1998, pp. 357–371.

[GHO19] Sanjam Garg, Mohammad Hajiabadi, and Rafail Ostrovsky. *Efficient Range-Trapdoor Functions and Applications: Rate-1 OT and More*. Cryptology ePrint Archive, Report 2019/990. `https://eprint.iacr.org/2019/990`. 2019.

[Döt+19] Nico Döttling et al. "Trapdoor Hash Functions and Their Applications". In: *Advances in Cryptology – CRYPTO 2019, Part III*. Ed. by Alexandra Boldyreva and Daniele Micciancio. Vol. 11694. Lecture Notes in Computer Science. Santa Barbara, CA, USA: Springer, Heidelberg, Germany, 2019, pp. 3–32.

[GR05] Craig Gentry and Zulfikar Ramzan. "Single-Database Private Information Retrieval with Constant Communication Rate". In: *ICALP 2005: 32nd International Colloquium on Automata, Languages and Programming*. Ed. by Luís Caires et al. Vol. 3580. Lecture Notes in Computer Science. Lisbon, Portugal: Springer, Heidelberg, Germany, 2005, pp. 803–815.

[Ger+00] Yael Gertner et al. "Protecting Data Privacy in Private Information Retrieval Schemes". In: *J. Comput. Syst. Sci.* 60.3 (June 2000).

[Bei+02] Amos Beimel et al. "Breaking the $O(n^{1/(2k-1)})$ Barrier for Information-Theoretic Private Information Retrieval". In: *43rd Annual Symposium on Foundations of Computer Science*. Vancouver, BC, Canada: IEEE Computer Society Press, 2002, pp. 261–270.

[DHS14] Daniel Demmler, Amir Herzberg, and Thomas Schneider. "RAID-PIR: Practical multi-server PIR". In: vol. 2014. Nov. 2014.

[DGH12] Casey Devet, Ian Goldberg, and Nadia Heninger. "Optimally Robust Private Information Retrieval". In: *USENIX Security 2012: 21st USENIX Security Symposium*. Ed. by Tadayoshi Kohno. Bellevue, WA, USA: USENIX Association, 2012, pp. 269–283.

[Gol07] Ian Goldberg. "Improving the Robustness of Private Information Retrieval". In: *2007 IEEE Symposium on Security and Privacy*. Oakland, CA, USA: IEEE Computer Society Press, 2007, pp. 131–148.

[Bon+] Dan Boneh et al. *Private Information Retrieval*. `https://crypto.stanford.edu/pir-library/`.

[SJ05] Felipe Saint-Jean. *Java implementation of a single-database computationally symmetric private information retrieval (cSPIR) protocol*. Tech. rep. YALE UNIV NEW HAVEN CT DEPT OF COMPUTER SCIENCE, 2005.

[Jar+13] Stanislaw Jarecki et al. “Outsourced symmetric private information retrieval”. In: Proceedings of the ACM Conference on Computer and Communications Security, 2013.

[Pap+14] Vasilis Pappas et al. “Blind Seer: A Scalable Private DBMS”. In: *2014 IEEE Symposium on Security and Privacy*. Berkeley, CA, USA: IEEE Computer Society Press, 2014, pp. 359–374.

[Fis+15] Ben A. Fisch et al. “Malicious-Client Security in Blind Seer: A Scalable Private DBMS”. In: *2015 IEEE Symposium on Security and Privacy*. San Jose, CA, USA: IEEE Computer Society Press, 2015, pp. 395–410.

[MRR21] Ian McQuoid, Mike Rosulek, and Lawrence Roy. *Batching Base Oblivious Transfers*. Cryptology ePrint Archive, Report 2021/682. `https://eprint.iacr.org/2021/682`. 2021.

[Rin] Peter Rindal. *libOTe: an efficient, portable, and easy to use Oblivious Transfer Library*. `https://github.com/osu-crypto/libOTe`.

[Mea86] Catherine Meadows. “A More Efficient Cryptographic Matchmaking Protocol for Use in the Absence of a Continuously Available Third Party”. In: *1986 IEEE Symposium on Security and Privacy*. 1986, pp. 134–134.

[HFH99] Bernardo A. Huberman, Matt Franklin, and Tad Hogg. “Enhancing Privacy and Trust in Electronic Communities”. In: *Proceedings of the 1st ACM Conference on Electronic Commerce*. EC ’99. Association for Computing Machinery, 1999. ISBN: 1581131763.

[CLR17a] Hao Chen, Kim Laine, and Peter Rindal. “Fast Private Set Intersection from Homomorphic Encryption”. In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. CCS ’17. Association for Computing Machinery, 2017. ISBN: 9781450349468.

[Che+18] Hao Chen et al. “Labeled PSI from Fully Homomorphic Encryption with Malicious Security”. In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. CCS ’18. Association for Computing Machinery, 2018. ISBN: 9781450356930.

[Con+21] Kelong Cong et al. “Labeled PSI from Homomorphic Encryption with Reduced Computation and Communication”. In: *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. CCS ’21. Association for Computing Machinery, 2021. ISBN: 9781450384544.

[LLW21] Jie Li, Yamin Liu, and Shuang Wu. “Pipa: Privacy-preserving Password Checkup via Homomorphic Encryption”. In: *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security* (2021).

[GHS12] Craig Gentry, Shai Halevi, and Nigel P. Smart. “Fully Homomorphic Encryption with Polylog Overhead”. In: *Advances in Cryptology – EUROCRYPT 2012*. Ed. by David Pointcheval and Thomas Johansson. Vol. 7237. Lecture Notes in Computer Science. Cambridge, UK: Springer, Heidelberg, Germany, 2012, pp. 465–482.

[SV11] N.P. Smart and F. Vercauteren. *Fully Homomorphic SIMD Operations*. Cryptology ePrint Archive, Report 2011/133. `https://eprint.iacr.org/2011/133`. 2011.

[BGH13] Zvika Brakerski, Craig Gentry, and Shai Halevi. “Packed Ciphertexts in LWE-Based Homomorphic Encryption”. In: *PKC 2013: 16th International Conference on Theory and Practice of Public Key Cryptography*. Ed. by Kaoru Kurosawa and Goichiro Hanaoka. Vol. 7778. Lecture Notes in Computer Science. Nara, Japan: Springer, Heidelberg, Germany, 2013, pp. 1–13.

[Che+19] Hao Chen et al. “Efficient Multi-Key Homomorphic Encryption with Packed Ciphertexts with Application to Oblivious Neural Network Inference”. In: *ACM CCS 2019: 26th Conference on Computer and Communications Security*. Ed. by Lorenzo Cavallaro et al. ACM Press, 2019, pp. 395–412.

[DS16] Léo Ducas and Damien Stehlé. “Sanitization of FHE Ciphertexts”. In: *Advances in Cryptology – EUROCRYPT 2016, Part I*. Ed. by Marc Fischlin and Jean-Sébastien Coron. Vol. 9665. Lecture Notes in Computer Science. Vienna, Austria: Springer, Heidelberg, Germany, 2016, pp. 294–310.

[Ash+12] Gilad Asharov et al. “Multiparty Computation with Low Communication, Computation and Interaction via Threshold FHE”. In: *Advances in Cryptology – EUROCRYPT 2012*. Ed. by David Pointcheval and Thomas Johansson. Vol. 7237. Lecture Notes in Computer Science. Cambridge, UK: Springer, Heidelberg, Germany, 2012, pp. 483–501.

[Seaa] *Microsoft SEAL (release 3.5)*. `https://github.com/Microsoft/SEAL`. Microsoft Research, Redmond, WA. Apr. 2020.

[Seab] *Microsoft SealPIR*. `https://github.com/microsoft/SealPIR`.

[CLR17b] Hao Chen, Kim Laine, and Peter Rindal. “Fast Private Set Intersection from Homomorphic Encryption”. In: *ACM CCS 2017: 24th Conference on Computer and Communications Security*. Ed. by Bhavani M. Thuraisingham et al. Dallas, TX, USA: ACM Press, 2017, pp. 1243–1255.

[OOS17] Michele Orrù, Emmanuela Orsini, and Peter Scholl. “Actively Secure 1-out-of-N OT Extension with Application to Private Set Intersection”. In: *Topics in Cryptology – CT-RSA 2017*. Ed. by Helena Handschuh. Vol. 10159. Lecture Notes in Computer

Science. San Francisco, CA, USA: Springer, Heidelberg, Germany, 2017, pp. 381–396.

[Kol+16] Vladimir Kolesnikov et al. “Efficient Batched Oblivious PRF with Applications to Private Set Intersection”. In: *ACM CCS 2016: 23rd Conference on Computer and Communications Security*. Ed. by Edgar R. Weippl et al. Vienna, Austria: ACM Press, 2016, pp. 818–829.

[Alb+18] Martin Albrecht et al. *Homomorphic Encryption Security Standard*. Tech. rep. HomomorphicEncryption.org, 2018.