Ideal Lattices, Class Groups and Parameter Security for Ring-LWE

Heiko Knospe[0000−0002−6823−6250]

TH Köln, Institute of Computer and Communication Technology, Campus Deutz, Betzdorfer Str. 2, 50679 Köln, Germany. heiko.knospe@th-koeln.de

Abstract. The Ring Learning with Errors (RLWE) problem is widely believed to be computationally hard and underpins many modern lattice-based cryptographic constructions. Its security rests on a worst-case to average-case reduction from the approximate Shortest Vector Problem (SVP) on ideal lattices to average-case instances of RLWE, established by Lyubashevsky, Peikert, and Regev.
In this work we study the influence of the algebraic structure of cyclotomic fields K on the hardness of Ideal-SVP and hence on the security of RLWE-based schemes. We investigate how the ideal class group of cyclotomic fields, and specifically $h^+(K)$ and $h^-(K)$, influence the efficiency of algorithms that find mildly short vectors in ideal lattices, following the approach of Cramer, Ducas, and Wesolowski.
We provide a detailed analysis of class number growth: the real class numbers $h^+(K)$ exhibit slow polynomial growth, while the relative class numbers $h^-(K)$ grow slightly faster than exponentially.
Using these results, we critically examine standard power-of-two RLWE parameter choices and propose prime cyclotomic fields as alternative parameter rings. Fields with large class groups impose additional computational cost on known class-group-based attacks, potentially strengthening the underlying Ideal-SVP hardness. We present concrete parameter tables and discuss efficiency tradeoffs.

Keywords: Ideal lattices, Class groups, Cyclotomic fields, RLWE parameters

1 Introduction

Lattice-based cryptography currently forms the dominant approach to post-quantum security. Among the central hardness assumptions are the *Learning with Errors* (LWE) problem of Regev [18], its ring variant *Ring-LWE* (RLWE) [16], and its module generalisation *Module-LWE* (MLWE) [14].

The two NIST post-quantum standards ML-KEM (FIPS 203, [11]) and ML-DSA (FIPS 204, [12]) are both based on MLWE over the cyclotomic ring $R = \mathbb{Z}[X]/(X^{256}+1)$. ML-KEM uses modulus $q = 3329$ and a rank-k module with $k \in \{2,3,4\}$ (parameter sets ML-KEM-512/768/1024) [11]. ML-DSA uses the larger modulus $q = 8{,}380{,}417 = 2^{23} - 2^{13} + 1$ and a $k \times \ell$- matrix structure with $(k,\ell) \in \{(4,4), (6,5), (8,7)\}$ (parameter sets ML-DSA-44/65/87) [12].

RLWE is the special case $k = 1$ of MLWE, and forms its algebraic and theoretical foundation. The KEM NewHope [2] is based on RLWE over the cyclotomic ring $R = \mathbb{Z}[X]/(X^n + 1)$, where $n = 512$ or $n = 1024$, and uses the modulus $q = 12289$. RLWE is also heavily used in advanced privacy-enhancing technologies such as Fully Homomorphic Encryption (FHE) [4], Zero Knowledge Proofs (ZKP) [17] and Secure Multi-Party Computation (SMPC) [10].

The hardness of MLWE reduces via the worst-case to average-case reduction of Langlois and Stehlé [14] to the approximate Shortest Vector Problem on *module lattices* (Module-SVP). RLWE, in turn, reduces to SVP on *ideal lattices* (Ideal-SVP) via the reduction of Lyubashevsky, Peikert, and Regev [16]: any efficient quantum attack on RLWE would imply an efficient solution to worst-case Ideal-SVP. Moreover, Albrecht et al. [1] showed that RLWE with modulus q^k is at least as hard as MLWE with modulus q and module rank k. Since the reduction requires a larger modulus and a higher error rate, it is often assumed that there is a hardness gap between module rank-2 lattices and ideal lattices [7].

Multiplications in the quotient ring $R_q = \mathbb{Z}[\zeta_m]/(q)$ can be performed in $O(n \log n)$ time via the Number Theoretic Transform (NTT), if the modulus q is fully split in the cyclotomic ring R. This is a substantial improvement over the matrix multiplications for general LWE [18] which require $O(n^2)$ time.

However, the ideal structure of RLWE lattices also introduces algebraic structure that attackers can potentially exploit. A result of Cramer, Ducas, and Wesolowski [5] showed that, for cyclotomic ideal lattices, a mildly short vector (achieving approximation factor $\exp(\widetilde{O}(\sqrt{n}))$) can be found in quantum polynomial time. This reveals an unexpected hardness gap between Ideal-SVP and general SVP, and raises the following question: *how strongly do parameter choices for RLWE affect the hardness of the underlying Ideal-SVP?*

A crucial algebraic ingredient in the attack [5] is the ideal class group $\mathrm{Cl}(K)$ of the cyclotomic field $K = \mathbb{Q}(\zeta_m)$. The algorithm uses the decomposition of $\mathrm{Cl}(K)$ into a plus part $\mathrm{Cl}(K^+)$ and a minus part $\mathrm{Cl}^-(K)$, and leverages the Stickelberger ideal to annihilate the minus class group. The sizes of $h^+(K) = |\mathrm{Cl}(K^+)|$ and $h^-(K) = |\mathrm{Cl}^-(K)|$ directly govern the computational complexity of key subproblems in the attack.

Contributions. This paper makes the following contributions:

(i) We analyze the hardness of Ideal-SVP through the lens of the Principal Ideal Problem (PIP) and the Close Multiple Problem (CMP), making precise the roles of the plus and minus class groups.
(ii) We provide a detailed numerical and asymptotic analysis of $h^+(K)$ and $h^-(K)$. The plus class groups show slow polynomial growth, while the minus class group grows slightly faster than exponentially and is governed by the analytic class number formula via generalised Bernoulli numbers. We analyze class numbers of cyclotomic fields that are potentially relevant for cryptographic applications.
(iii) We apply Iwasawa theory to characterize the growth of class numbers along cyclotomic $\mathbb{Z}_p$-towers.

(iv) We propose and evaluate *prime cyclotomic fields* as alternative parameter rings for RLWE. Fields with non-trivial $h^+(K)$ or positive $\lambda_p^-(K)$ impose additional cost on known attacks, potentially offering stronger Ideal-SVP hardness. Concrete parameter tables and a tradeoff discussion are provided.

Organisation. Section 2 establishes the theory of lattices and ideal lattices. Section 3 formulates RLWE and presents the worst-case hardness reduction. Section 4 analyses Ideal-SVP via PIP and CMP. Section 5 studies class number growth. Section 6 examines parameter choices for RWLE. Section 7 provides the conclusion.

2 Lattices and Ideal Lattices

In this section, we introduce the fundamentals of ideal lattices in number fields.

2.1 Lattices in Euclidean Space

A *lattice* Λ is a discrete subgroup of an n-dimensional Euclidean vector space $V \cong \mathbb{R}^n$. A full-rank lattice is generated as the integer linear span of a basis $v_1, v_2, \ldots, v_n \in V$:

$$\Lambda = \big\{ x_1 v_1 + \cdots + x_n v_n \;\big|\; x_i \in \mathbb{Z} \big\}.$$

Writing B for the matrix whose columns are the basis vectors, this takes the form $\Lambda = \{Bx \mid x \in \mathbb{Z}^n\}$. The space of all n-dimensional lattices is naturally identified with $GL_n(\mathbb{R})/GL_n(\mathbb{Z})$.

A lattice admits infinitely many distinct bases, any two of which are related by a unimodular matrix in $GL_n(\mathbb{Z})$. Lattice reduction algorithms such as LLL [15] and BKZ [20] seek to compute a short, nearly-orthogonal basis from an arbitrary input basis.

Definition 1 (Lattice Volume). *The* fundamental parallelepiped *of a basis* $(v_1, \ldots, v_n)$ *is*

$$P = \big\{ x_1 v_1 + \cdots + x_n v_n \;\big|\; x_i \in [0, 1) \big\}.$$

The lattice volume *(or determinant) is*

$$\det(\Lambda) = |\det(B)| = \sqrt{\det\big((v_i \cdot v_j)_{1 \le i,j \le n}\big)},$$

which is independent of the choice of basis.

Definition 2 (Dual Lattice). *Given a lattice* $\Lambda \subset V$*, the* dual lattice *is*

$$\Lambda^* = \big\{ y \in V \;\big|\; x \cdot y \in \mathbb{Z} \text{ for all } x \in \Lambda \big\}.$$

If Λ *has basis matrix* B*, then* $\Lambda^* = \{(B^T)^{-1} x \mid x \in \mathbb{Z}^n\}$*. The volume of the dual lattice is* $\det(\Lambda^*) = 1/\det(\Lambda)$*.*

2.2 Hard Lattice Problems

The following computational problems on lattices are believed to be intractable even for quantum computers, and form the security foundation of lattice-based cryptography.

Definition 3 (SVP, SIVP, CVP). *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and $\lambda_1(\Lambda)$ the length of its shortest non-zero vector.*

- ***Shortest Vector Problem (SVP):*** *Find a non-zero $v \in \Lambda$ with $\|v\| = \lambda_1(\Lambda)$.*
- ***Shortest Independent Vector Problem (SIVP):*** *Find n linearly independent lattice vectors $v_1, \ldots, v_n \in \Lambda$ minimising $\max_i \|v_i\|$.*
- ***Closest Vector Problem (CVP):*** *Given $w \in \mathbb{R}^n$, find the closest lattice vector $v \in \Lambda$ to w.*

Definition 4 (Approximate SVP$_\gamma$). *Let $\gamma \geq 1$. A vector $w \in \Lambda$ with $\|w\| \leq \gamma \cdot \lambda_1(\Lambda)$ is a solution to* SVP$_\gamma$.

Approximations within polynomial factors $\gamma(n) = \text{poly}(n)$ are believed hard even for quantum polynomial-time algorithms. By contrast, the LLL algorithm [15] achieves approximation within exponential factor $\gamma(n) = 2^{O(n)}$ in polynomial time.

2.3 Ideal Lattices from Cyclotomic Fields

Let $K = \mathbb{Q}(\zeta_m)$ be the *cyclotomic field* of conductor $m > 2$, where ζ_m is a primitive m-th root of unity. Its degree of K over $\mathbb{Q}$ is $n = \varphi(m)$ and its ring of integers is $R = \mathcal{O}_K = \mathbb{Z}[\zeta_m]$. The minimal polynomial of ζ_m is called the cyclotomic polynomial $\Phi_m(X)$.

The *canonical embedding* maps K into $\mathbb{C}^n$ via

$$\sigma : K \to \mathbb{C}^n, \quad x \mapsto (\sigma_1(x), \ldots, \sigma_n(x)),$$

where $\sigma_1, \ldots, \sigma_n$ are the n field embeddings of K into $\mathbb{C}$. For cyclotomic fields, all embeddings are complex and map ζ_m to ζ_m^i, where $i \in (\mathbb{Z}/m\mathbb{Z})^\times$. The image of σ lies in the *real* n-dimensional subspace

$$H = \{x \in \mathbb{C}^n \mid x_{s_2+j} = \overline{x_j},\ 1 \leq j \leq s_2\} \cong K \otimes_{\mathbb{Q}} \mathbb{R} = K_{\mathbb{R}}.$$

The inner product on H induced from $\mathbb{C}^n$ satisfies

$$\langle \sigma(x), \overline{\sigma(y)} \rangle = \text{Tr}(x \cdot y) \quad \text{for } x, y \in K,$$

where $\text{Tr} : K \to \mathbb{Q}$ is the trace map defined by $\text{Tr}(x) = \sigma_1(x) + \cdots + \sigma_n(x)$. This endows K with an ℓ_2-norm via σ. Under σ, every fractional ideal $\mathfrak{a} \subset K$ maps to a full-rank lattice in H. These are called *ideal lattices*. Obviously, ideal lattices have additional structure: for example, they are stable under multiplication with arbitrary ring elements in $\mathcal{O}_K$, and multiplication of a shortest vector with powers of ζ_m yields shortest independent vectors.

2.4 Volumes and Bounds on the Shortest Vector

Proposition 1. *Let Δ_K denote the absolute discriminant of K and set $\delta_K = |\Delta_K|^{1/(2n)}$ (the* root discriminant*). For the ring of integers R, one has* $\mathrm{vol}(R) = \sqrt{|\Delta_K|}$*. For a fractional ideal $\mathfrak{a}$,*

$$\mathrm{vol}(\mathfrak{a}) = \mathrm{N}(\mathfrak{a}) \cdot \sqrt{|\Delta_K|},$$

where $\mathrm{N}(\mathfrak{a})$ denotes the absolute norm of $\mathfrak{a}$. Furthermore, one has $\mathrm{vol}(\mathfrak{a})^{1/n} = \mathrm{N}(\mathfrak{a})^{1/n} \cdot \delta_K$.

Remark 1. The discriminant of K measures the sparsity of the lattice R inside the vector space H via the embedding σ. For the lattice $R = \mathbb{Z}[\zeta_m]$ of rank n, the discriminant is quite large:

$$\Delta_K = (-1)^{n/2} \frac{m^n}{\prod_{p|m} p^{n/(p-1)}}$$

The size of the root discriminant is closer to $\sqrt{m}$ with $\delta_K = \frac{\sqrt{m}}{\prod_{p|m} p^{1/(2(p-1))}}$. For a prime power $m = p^k$, one has $\Delta_K = \pm p^{p^{k-1}(pk-k-1)}$ and $\delta_K = p^{\frac{k}{2} - \frac{1}{2(p-1)}}$, e.g., $\Delta_K = n^n$ and $\delta_K = \sqrt{n}$ for $m = 2^k$ and $n = \varphi(m) = 2^{k-1}$.

Proposition 2 (Bounds on λ_1). *For a fractional ideal $\mathfrak{a} \subset K$,*

$$\sqrt{n}\ \mathrm{N}(\mathfrak{a})^{1/n} \ \le\ \lambda_1(\mathfrak{a}) \ \le\ \sqrt{n}\ \mathrm{N}(\mathfrak{a})^{1/n}\, \delta_K.$$

Proof. The lower bound follows by applying the AM-GM inequality to the ℓ_2-norm of a shortest vector in the canonical embedding. The upper bound follows from Minkowski's convex body theorem applied to the ideal lattice $\sigma(\mathfrak{a})$.

The *Gaussian heuristic* provides the practical estimate

$$\lambda_1(\mathfrak{a}) \approx \sqrt{n/(2\pi e)}\ \mathrm{vol}(\mathfrak{a})^{1/n},$$

which generally falls between the two bounds.

2.5 Duality of Ideal Lattices

Definition 5. *For a fractional ideal $\mathfrak{a} \subset K$, the* dual ideal *is*

$$\mathfrak{a}^\vee = \big\{ x \in K \ \big|\ \mathrm{Tr}(x \cdot \mathfrak{a}) \subset \mathbb{Z} \big\}.$$

Under the canonical embedding, $\sigma(\mathfrak{a}^\vee) = \overline{\sigma(\mathfrak{a})^*}$. For $R = \mathbb{Z}[\zeta_m]$, the codifferent (dual of R) is

$$R^\vee = \frac{1}{\Phi_m'(\zeta_m)}\, R,$$

where Φ_m is the m-th cyclotomic polynomial. The dual $R^\vee$ is a lattice in the inner product space H, and multiplication by $\Phi_m'(\zeta_m)$ is an isomorphism of H which maps $R^\vee$ to R. However, this map is a scaled isometry only for $m = 2^k$, as the following remark shows.

Remark 2. Let $m = 2^k$. Then $\Phi'_m(\zeta_m) = n\zeta_m^{n-1} = -n\zeta_m^{-1}$ and $R^\vee = \frac{1}{n}R$. Hence the isomorphism is a scaled isometry with respect to the canonical embedding. Furthermore, it is also a scaled isometry with respect to the coefficient embedding of K (see Remark 3 below). However, for prime $m = p$ one has $\Phi'_p(\zeta_p) = \frac{p}{\zeta_p - 1}\zeta_p^{p-1} = \frac{p}{\zeta_p - 1}\zeta_p^{-1}$. The magnitude of that factor depends on the embedding of K into $\mathbb{C}$ since $|1 - \zeta_p^i|$ varies with the position of ζ_p^i on the unit circle. In this case, the scaling factor $\Phi'_p(\zeta_p)$ distorts the geometry. One obtains $R^\vee = \frac{1-\zeta_p}{p}\, R = (1-\zeta_p)^{-(p-2)}\, R$, since $(1-\zeta_p)^{p-1} = (p)$ as ideals in $\mathbb{Z}[\zeta_p]$.

Remark 3. One can also view $K = \mathbb{Q}[X]/(\Phi_m(X))$ as an inner product space via the coefficient embedding, i.e., with respect to the power basis $\{\zeta_m^j\}$. The transformation between the coefficient embedding and the canonical embedding is given by the Vandermonde matrix $V = (\zeta_m^{ij})_{ij}$, where $i \in (\mathbb{Z}/m\mathbb{Z})^\times$ and $j = 0, 1, \ldots, n-1$. For $m = 2^k$ one checks that $VV^* = nI_n$, so that the transformation is a scaled isometry. This shows that the multiplication by $\Phi'_m(\zeta_m) = -n\zeta_m^{-1}$, which maps elements in $R^\vee$ (with respect to the canonical embedding) to R (with respect to the coefficient embedding) is orthogonal up to a scaling factor of $\sqrt{n}$. For other cyclotomic fields, this is still an isomorphism, but the multiplication by $\Phi'_m(\zeta_m)$ and the transformation by the Vandermonde matrix are no longer scaled isometries.

3 The Ring Learning with Errors Problem

3.1 Problem Formulation

Fix $K = \mathbb{Q}(\zeta_m)$, $R = \mathbb{Z}[\zeta_m]$, and a modulus $q \equiv 1 \pmod{m}$ with $q = O(n^k)$ for some $k \geq 1$. Set $R_q = R/(q)$ and $R_q^\vee = R^\vee/(qR^\vee)$.

Definition 6. *For a secret $s \in R_q^\vee$ and error parameter $r = \alpha q > 0$, the RLWE distribution $A_{s,r}$ over $R_q \times K_\mathbb{R}/qR^\vee$ is sampled by drawing $a \in R_q$ uniformly at random, drawing an error $e \in K_\mathbb{R}/qR^\vee$ from a spherical Gaussian distribution with standard deviation σ and parameter $r = \sigma\sqrt{2\pi}$, and outputting $(a,\, b) = (a,\, a \cdot s + e)$.*

Definition 7. *The two variants of the RLWE problems are:*

- ***Search RLWE:*** *Given polynomially many samples $(a_i, b_i) \sim A_{s,r}$ for an unknown s, recover s.*
- ***Decision RLWE:*** *Distinguish between samples from $A_{s,r}$ (for an unknown, uniformly chosen s) and uniformly random pairs $(a, b) \in R_q \times K_\mathbb{R}/qR^\vee$.*

3.2 Dual and Non-Dual Variants

The formulation in Definition 6 uses the dual ring $R^\vee$ and the canonical embedding. In practice, deployed schemes favour a *non-dual* variant with $a, s \in R_q$ and

the coefficient embedding. Multiplying the RLWE equation by $t = \Phi'_m(\zeta_m) \in R$ transforms it into

$$b' = a's + e', \quad a', s \in R_q,$$

where $e' = t \cdot e \in K_{\mathbb{R}}/qR$ is a scaled error. As discussed in Remark 3, one has $t = -n\zeta_m^{-1}$ for $m = 2^k$, so the spherical shape of the error is preserved, even with respect to the coefficient embedding of R.

For prime $m = p$, the algebraic generator $t = \frac{p}{1-\zeta_p}$ introduces an elliptic distortion of the error with respect to the coefficient embedding using the power basis $\{\zeta_m^j,\ j = 0, \ldots, p-2\}$, complicating the direct hardness assumption for non-dual RLWE. A possible approach to this problem is given by Ducas and Durmus [9]: the RLWE equation including the error is multiplied by a factor p which yields $pR^\vee \subset R$ (but not equality). Then sampling is done with respect to the power basis $\{X^j,\ j = 0, \ldots, p-1\}$ of the larger ring $R' = \mathbb{Q}[X]/(X^p - 1)$. The error vector $e' \in R'$ is drawn from a spherical Gaussian distribution, where the standard deviation is $\sqrt{p}$ times smaller than that required in the embedding space. Then e' is projected to an element in the cyclotomic ring $R = \mathbb{Q}[X]/(X^{p-1} + \cdots + X + 1)$. The resulting error vector has the desired spherical Gaussian distribution in the embedding space. The combination of scaling by p and sampling with respect to the power basis of R' increases the standard deviation by a factor of $\sqrt{p}$. We refer to Theorem 2 of the article [9] for a precise statement on the parameters and the hardness of this non-dual variant RLWE.

Alternatively, one can apply the non-isometric isomorphism between $R^\vee$ and R and transform the spherical Gaussian into an elliptical Gaussian distribution. The base change from the canonical embedding to the coefficient embedding is calculated using a Vandermonde matrix (see Remark 3), respectively its inverse. The result is a $(p-1) \times (p-1)$ covariance matrix. Then the coefficients of the error vector for the non-dual variant of RLWE are sampled from an elliptical Gaussian using this matrix.

3.3 Efficient Arithmetic via the NTT

Since we assumed $q \equiv 1 \pmod{m}$, the modulus q splits completely in R:

$$R_q \cong \prod_{i \in (\mathbb{Z}/m\mathbb{Z})^\times} R/\mathfrak{q}_i \cong \prod_{i \in (\mathbb{Z}/m\mathbb{Z})^\times} \mathbb{Z}_q,$$

where $\mathfrak{q}_i = (q, \zeta_m - \omega_m^i)$ and $\omega_m \in \mathbb{Z}_q$ is a primitive m-th root of unity. In the power basis of R, one substitutes ω_m^i for ζ_m^i to obtain the isomorphism. Thus the Chinese Remainder Theorem decomposition enables multiplication in R_q to be performed in $\mathbb{Z}_q \times \cdots \times \mathbb{Z}_q$. This *Number Theoretic Transform* (NTT) makes RLWE significantly more efficient than plain LWE in both time and memory.

A slight modification is needed when $q \equiv 1$ holds only modulo $m/2$, but not modulo m, as in ML-KEM [11] where $m = 2^9$ and $q = 3329$. Then $\mathbb{Z}_q$ only contains a primitive $\frac{m}{2} = n$-th root of unity ω_n, and reduction modulo $\mathfrak{q}_i = (q, \zeta_m^2 - \omega_n^i)$ gives the quadratic extension $\mathbb{Z}_q[X]/(X^2 - \omega_n^i)$ of $\mathbb{Z}_q$. However, multiplication in a quadratic extension of $\mathbb{Z}_q$ is still very efficient.

3.4 Worst-Case to Average-Case Reduction

The following theorem provides the theoretical security foundation for RLWE-based cryptography.

Theorem 1 (Lyubashevsky–Peikert–Regev [16]). *Let $K = \mathbb{Q}(\zeta_m)$, $n = \varphi(m)$, $q = O(n^k)$, $q \equiv 1 \mod m$, $\alpha \in (0,1)$ and $\alpha q \geq \omega(\sqrt{\log n})$. Suppose the error elements are drawn from a spherical Gaussian distribution with parameter slightly larger than αq (for the non-dual version). There exists a polynomial-time quantum reduction from worst-case SVP_γ on ideal lattices in K, with approximation factor $\gamma = \widetilde{O}(\sqrt{n}/\alpha)$, to the average-case search RLWE problem. An analogous quantum reduction holds for decision RLWE.*

The theorem also holds for the non-dual version which is often preferred in practice. As discussed in Section 3.2, the error distribution then needs to be scaled by a factor of $t = \Phi'_m(\zeta_m) \in R$.

This worst-case to average-case connection is a distinguishing feature of RLWE: breaking RLWE for a uniformly random instance implies an efficient quantum algorithm for the hardest instance of Ideal-SVP. An analogous result for general lattices (plain LWE) was established by Regev [18].

4 Hardness of Ideal-SVP

4.1 The Hardness Gap

While Theorem 1 provides a reduction *from* Ideal-SVP *to* RLWE, the hardness of Ideal-SVP itself is not well understood. Indeed, ideal lattices possess rich algebraic structure that can be exploited:

Theorem 2 (Cramer–Ducas–Wesolowski [5]). *Ideal-SVP in cyclotomic rings $K = \mathbb{Q}(\zeta_m)$ can be solved in quantum polynomial time, achieving approximation factor $\exp(\widetilde{O}(\sqrt{n}))$, under the plausible number-theoretic assumptions that the plus class number satisfies $h^+(K) \leq poly(n)$.*

This contrasts sharply with the best known algorithms for general (unstructured) lattices, which achieve at most $\exp(\Theta(n))$ approximation in polynomial time (via LLL [15]). The resulting hardness gap raises the question of whether the RLWE security reduction via Theorem 1 remains meaningful at the approximation factors relevant for cryptographic parameters, particularly in rings where $h^+(K)$ is small or even 1 (e.g., power-of-2 cyclotomics).

4.2 Finding Mildly Short Vectors

The CDW algorithm decomposes Ideal-SVP into two sequential subproblems. The overall strategy is as follows: given a fractional ideal $\mathfrak{a}$, find short *integral* ideals $\mathfrak{b}$ and $\mathfrak{c}$, which depend on the class group, such that $\mathfrak{abc}$ is principal and

$$\mathrm{N}(\mathfrak{bc}) \leq \exp\big(\widetilde{O}(n^{1+c})\big) \quad \text{for some } c < \tfrac{1}{2}.$$

Because $\mathfrak{b}$ and $\mathfrak{c}$ are integral, $\mathfrak{abc}$ is a sub-ideal of $\mathfrak{a}$. Thus, if a generator g of the principal ideal $\mathfrak{abc}$ satisfying

$$\|g\| \;\le\; \mathrm{N}(\mathfrak{abc})^{1/n}\exp\bigl(\widetilde{O}(\sqrt{n})\bigr) \;=\; \mathrm{N}(\mathfrak{a})^{1/n}\,\mathrm{N}(\mathfrak{bc})^{1/n}\exp\bigl(\widetilde{O}(\sqrt{n})\bigr)$$

can be found, then $g \in \mathfrak{a}$ and g solves SVP in $\mathfrak{a}$ up to a sub-exponential approximation factor. Because $\mathrm{N}(\mathfrak{bc}) \le \exp\bigl(\widetilde{O}(n^{1+c})\bigr)$, the extra factor gets absorbed into the sub-exponential term, maintaining the $\exp\bigl(\widetilde{O}(\sqrt{n})\bigr)$ approximation for $\mathfrak{a}$. This approach separates the task into a *Close Principal Multiple* problem (finding the integral multiplier $\mathfrak{bc}$) and a *Principal Ideal Problem* (finding g).

4.3 The Principal Ideal Problem (PIP)

Definition 8 (PIP). *Given a principal ideal $\mathfrak{a} \subset R$, find a generator $h \in R$ such that*

$$\|h\| \;\le\; \mathrm{N}(\mathfrak{a})^{1/n}\exp\bigl(\widetilde{O}(\sqrt{n})\bigr).$$

The PIP algorithm proceeds in two steps [6]:

1. Find *any* generator g of $\mathfrak{a}$ using a quantum polynomial-time algorithm (e.g., Biasse–Song [3]). Classical methods are insufficient here as they require subexponential time.
2. Apply the *logarithmic embedding* $\mathrm{Log} : K^\times \to \mathbb{R}[G]/(1-\tau)$, where $G = \mathrm{Gal}(K/\mathbb{Q})$ and τ denotes complex conjugation. Let C denote the group of cyclotomic units of R. The cyclotomic units have an explicit definition in terms of the roots of unity ζ_m (see [22]). The lattice $\mathrm{Log}(C)$ has full rank in a codimension-one subspace of $\mathbb{R}[G]/(1-\tau)$ and admits a set of short generators. Solve the CVP in $\mathrm{Log}(C)$: find $u \in C \subset R^\times$ such that $\mathrm{Log}(u)$ is close to $\mathrm{Log}(g)$. Then $\mathrm{Log}(g) - \mathrm{Log}(u) = \mathrm{Log}(gu^{-1})$ is short, so $h = gu^{-1}$ is a mildly short generator of $\mathfrak{a}$.

The cyclotomic unit group C is well-understood via the theorem of Sinnott [21] and provides a rich enough structure for an efficient CVP solution.

4.4 The Close Principal Multiple Problem (CPM)

Definition 9 (CPM). *Given a fractional ideal $\mathfrak{a}$, find short* integral *ideals $\mathfrak{b}, \mathfrak{c}$ such that $\mathfrak{abc}$ is principal, with $\mathrm{N}(\mathfrak{bc})$ as small as possible.*

The ideal class group $\mathrm{Cl}(K) = \mathcal{I}(K)/P(K)$ plays a central role. Complex conjugation τ on K induces the norm map $N_{K/K^+} : \mathrm{Cl}(K) \to \mathrm{Cl}(K^+)$ where $K^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ is the maximal real subfield. We define $\mathrm{Cl}^-(K)$ via the exact sequence

$$1 \longrightarrow \mathrm{Cl}^-(K) \longrightarrow \mathrm{Cl}(K) \xrightarrow{N_{K/K^+}} \mathrm{Cl}(K^+) \longrightarrow 1,$$

and write $h(K) = |\mathrm{Cl}(K)|$, $h^+(K) = |\mathrm{Cl}(K^+)|$, and $h^-(K) = h(K)/h^+(K)$.

The CPM algorithm proceeds in two stages:

1. **Reaching** $\mathrm{Cl}^-(K)$**.** Multiply $\mathfrak{a}$ by random short prime ideals $\mathfrak{b}$ until the class $[\mathfrak{ab}]$ lies in $\mathrm{Cl}^-(K)$. The expected number of steps depends on the index $[\mathrm{Cl}(K) : \mathrm{Cl}^-(K)] = h^+(K)$.
2. **Killing the class via the Stickelberger ideal.** The Stickelberger ideal $\mathcal{S} \subset \mathbb{Z}[G]$ annihilates $\mathrm{Cl}(K)$ [22]. Let $R_G = \mathbb{Z}[G]/(1+\tau)$ and $\pi : \mathbb{Z}[G] \to R_G$ be the projection. The projected Stickelberger ideal $\pi(\mathcal{S})$ annihilates $\mathrm{Cl}^-(K)$, has short generators, and additionally is a *full rank* $\mathbb{Z}$-sublattice of rank $\frac{\varphi(m)}{2} = \frac{n}{2}$ within the Euclidean space associated to R_G. One assumes that a factor base of short $\mathbb{Z}[G]$-generators of $\mathrm{Cl}^-(K)$ can be found efficiently. Using a quantum algorithm for the class group discrete logarithm one expresses the *inverse* class $[\mathfrak{ab}]^{-1} \in \mathrm{Cl}^-(K)$ in terms of this factor base. Reducing the exponent vector via the Stickelberger lattice yields a short integral ideal $\mathfrak{c}$ such that $[\mathfrak{c}] = [\mathfrak{ab}]^{-1}$. Thus, $\mathfrak{abc}$ is principal. The difficulty of this step depends on the size and the group structure of $\mathrm{Cl}^-(K)$.

The success and efficiency of CPM depend critically on both $h^+(K)$ and $h^-(K)$: a larger $h^+(K)$ increases the cost of step (1), while a larger $h^-(K)$ increases the factor-base complexity and the discrete logarithm $\mathrm{Cl}^-(K)$ in step (2). We analyse these quantities in the next section.

5 Class Numbers and Iwasawa Theory

5.1 The Real Class Number $h^+(K)$

The exact computation of $h^+(K)$ for cyclotomic fields $K = \mathbb{Q}(\zeta_m)$ is notoriously difficult and few plus class numbers have been determined exactly [19]. The following theorem of Sinnott connects $h^+(K)$ to the index of cyclotomic units.

Theorem 3 (Sinnott [21]). *Let C^+ be the group of cyclotomic units of $K^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$. Then C^+ has finite index in $(R^+)^\times$ and*

$$2^b\, h^+(K) = [(R^+)^\times : C^+],$$

where $b = 0$ if $m = p^k$, and otherwise $b = 2^{g-2} + 1 - g$, where $g \geq 2$ is the number of distinct prime factors of m.

Schoof [19] computed the index $[(R^+)^\times : C^+]$ for all primes $p < 10^5$ up to factor that is probably 1 (or otherwise at least 80000). The numerical data (see Figure 1) strongly suggests that $h^+(K)$ grows at most polynomially in m (and in many cases equals 1). Some notable large real class numbers are $h^+(\mathbb{Q}(\zeta_{641})) = 495$, $h^+(\mathbb{Q}(\zeta_{1231})) = 211$, $h^+(\mathbb{Q}(\zeta_{1297})) = 275$, and $h^+(\mathbb{Q}(\zeta_{1459})) = 247$.

Practical RLWE instantiations predominantly rely on power-of-two cyclotomic fields, In this case, it is known that the real class numbers are odd and $h^+(\mathbb{Q}(\zeta_{2^k})) = 1$ for $k \leq 9$ (see [19], for $k = 9$ under the generalized Riemann hypothesis). It is conjectured (*Weber's class number problem*) that $h^+(\mathbb{Q}(\zeta_{2^k})) = 1$ for all $k \in \mathbb{N}$.

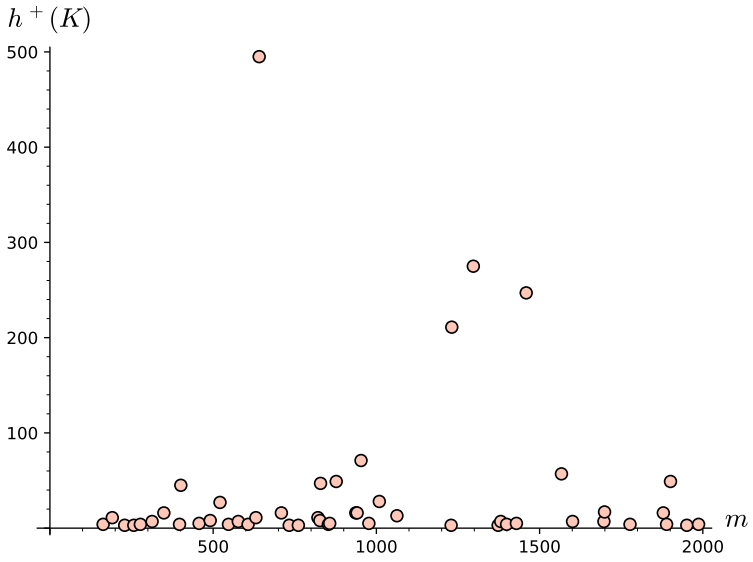

Fig. 1. Probable class numbers $h^+(K)$ of the maximal real subfield of prime cyclotomic fields $K = \mathbb{Q}(\zeta_m)$ [19].

This renders the first stage of the CPM algorithm, i.e, reaching $\mathrm{Cl}^-(K)$, entirely vacuous, thereby streamlining the attack. This potential weakness in power-of-two cyclotomics serves as a motivation for exploring alternative cyclotomic fields with larger $h^+(K)$.

5.2 The Relative Class Number $h^-(K)$

In stark contrast to the plus part, the relative class numbers are growing faster than exponentially, and $h^-(\mathbb{Q}(\zeta_m)) = 1$ holds only for a finite set of small integers m. Furthermore, the relative class number is well-understood via the analytic class number formula.

Theorem 4 (Analytic Class Number Formula). *For $K = \mathbb{Q}(\zeta_m)$,*

$$h^-(K) = Q\, w \prod_{\substack{\chi \bmod m \\ \chi \text{ odd}}} \left(-\tfrac{1}{2} B_{1,\chi}\right),$$

where the product is over all odd Dirichlet characters χ of $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$, $B_{1,\chi}$ are the first generalised Bernoulli numbers, and

$$Q = \begin{cases} 1 & m = p^k, \\ 2 & \text{otherwise,} \end{cases} \qquad w = \begin{cases} 2m & m \text{ odd,} \\ m & \text{otherwise.} \end{cases}$$

Numerically, $\log h^-(K) \sim \frac{1}{4}\varphi(m)\log(m)$ as $m \to \infty$ (see [22] Theorem 4.20). However, this asymptotic formula overestimates $\log h^-(K)$ for the cyclotomic fields used in cryptographic schemes, i.e. $m = 256, \ldots, 4096$, where the factor in front of $\varphi(m)\log(m)$ is closer to 0.1 than to 0.25. We computed $h^-(K)$ using Theorem 4 and depict the result in Figure 2. Our numerical data shows that the size of $h^-(K)$ for power-of-2 cyclotomic fields $K = \mathbb{Q}(\zeta_m)$, where $m = 256, 512, 1024, 2048$, is at the upper end of the range of class numbers for fields of comparable degree.

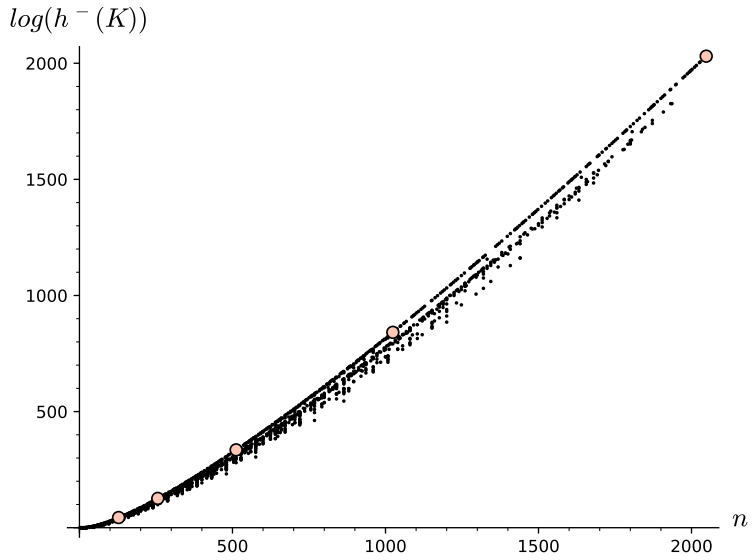

Fig. 2. Relative class numbers $h^-(\mathbb{Q}(\zeta_m))$ against $n = \varphi(m)$, with markers for $m = 2^k$, $k = 8, \ldots, 12$.

What can be said about the growth of class numbers in extensions of cyclotomic fields?

Proposition 3. *Suppose that $m_1 \mid m_2$, $K = \mathbb{Q}(\zeta_{m_1})$ and $L = \mathbb{Q}(\zeta_{m_2})$. Then the Norm map $N : \mathrm{Cl}(L) \to \mathrm{Cl}(K)$ is surjective, and hence $h(K) \mid h(L)$.*

Proof. This follows from class field theory, using the fact that the cyclotomic extension L/K has no unramified subextensions (see [22] Theorem 10.1).

Therefore, the prime factorisation of class numbers is extended to include additional factors in extensions of cyclotomic fields.

Apart from formulas about the estimated size and the divisibility established in Proposition 3 there is no general growth formula for class numbers. However, when a prime number p is fixed *Iwasawa theory* provides a growth formula for the p-part of the class groups in $\mathbb{Z}_p$-extensions, and in particular for the cyclotomic $\mathbb{Z}_p$-extension.

Table 1. Class numbers of Power-of-two cyclotomic fields (see [22] for $\varphi(m) \leq 256$)

m	$\varphi(m)$	$h^-(K)$
32	16	1
64	32	17
128	64	$359057 = 17 \cdot 21121$
256	128	$10449592865393414737 = 17 \cdot 21121 \cdot 29102880226241$
512	256	$626250398449093235874572148252892284197821938997560532 9 =$ $17 \cdot 21121 \cdot 76532353 \cdot 29102880226241 \cdot 78307539695534689379886170 89$
1024	512	$381797475160219002830149856048779360790504342984157709791781101116579665300$ $254736866232114592210948040568062585468034135855299377845573557102439 21 =$ $17 \cdot 21121 \cdot 76532353 \cdot 550807805953 \cdot 29102880226241 \cdot 78307539695534689379886170 89 \cdot$ $610147178334345804752381117726771 3 \cdot 18140545534249343384065004284771254601912038 41$
2048	1024	$17 \cdot 21121 \cdot 76532353 \cdot 249361921 \cdot 6436466177 \cdot 550807805953 \cdot 29102880226241 \cdot \ldots$ *
4096	2048	$17 \cdot 21121 \cdot 83969 \cdot 7891969 \cdot 76532353 \cdot 249361921 \cdot 6436466177 \cdot 550807805953 \cdot$ $29102880226241 \cdot 130705364014081 \cdot \ldots$ *

*: Larger prime factors omitted.

5.3 Growth of Class Numbers via Iwasawa Theory

Iwasawa theory provides a precise asymptotic for class numbers in infinite cyclotomic towers (and in general $\mathbb{Z}_p$-extensions). Let p be a prime and $d \in \mathbb{N}$ such that $p \nmid d$. Let $K = \mathbb{Q}(\zeta_{dp})$, and set $K_r = \mathbb{Q}(\zeta_{dp^{r+1}})$. For $p = 2$, we set $K = \mathbb{Q}(\zeta_{4d})$ and $K_r = \mathbb{Q}(\zeta_{d2^{r+2}})$. The *cyclotomic $\mathbb{Z}_p$-tower* $K = K_0 \subset K_1 \subset K_2 \subset \cdots$ is the fundamental object of Iwasawa theory.

Theorem 5 (Iwasawa, Ferrero-Washington). *The p-part of $h(K_r)$ satisfies*

$$v_p\big(h(K_r)\big) = \lambda_p\, r + c$$

for all sufficiently large r, where $\lambda_p = \lambda_p(K) \geq 0$ is the Iwasawa λ-invariant *of the tower and c is a constant. Analogously one defines $\lambda_p^+(K)$ and $\lambda_p^-(K)$.*

Greenberg conjectured that $\lambda_p^+(K) = 0$, so that the growth of the p-part of class numbers is concentrated in the relative class number. This aligns with general expectation supported by the existing numerical data that the plus class number is relatively small. Note that Iwasawa theory only deals with the *p-part* of the class groups.

A case of particular interest is the base field $K = \mathbb{Q}(\zeta_p)$. A prime p is called *regular* if $p \nmid h^-(\mathbb{Q}(\zeta_p))$, equivalently $\lambda_p^-(\mathbb{Q}(\zeta_p)) = 0$. One can also show that $p \mid h^+(\mathbb{Q}(\zeta_p))$ implies $p \mid h^-(\mathbb{Q}(\zeta_p))$, and the Kummer-Vandiver conjecture states that $p \nmid h^+(\mathbb{Q}(\zeta_p))$. Regular primes play a key role in the proof of Fermat's Last Theorem, and it is predicted that approximately $e^{-1/2} \approx 60.65\%$ of all primes are regular [22].

Kim has recently given a more specific formula for prime cyclotomic fields:

Theorem 6 ([13]). *Let $K = \mathbb{Q}(\zeta_p)$ and let $i(p)$ be the index of irregularity, i.e., the number of Bernoulli numbers B_j, $j = 2, 4, \ldots, p-3$ which are divisible by p. Suppose that the Kummer-Vandiver conjecture holds. Then $\lambda_p(K) = i(p)$ and for all $r \geq 0$:*

$$v_p\big(h(K_r)\big) = i(p)\, r + v_p(h(K)).$$

Lambda-invariants and Dirichlet characters. For $K = \mathbb{Q}(\zeta_{dp})$ with $p \nmid d$, the invariant $\lambda_p^-(K)$ decomposes as $\lambda_p^-(K) = \sum_{\chi \text{ odd}} \lambda_p(\chi)$, where the sum is over odd characters χ of $\mathrm{Gal}(K/\mathbb{Q})$ and $\lambda_p(\chi)$ is determined by the p-adic L-function attached to χ. In the special case of $d = 1$, Kim's theorem shows that $\lambda_p(\chi) \leq 1$, but in general λ_p can be larger. It is now possible to compute $\lambda_p(\chi)$ efficiently for arbitrary Dirichlet characters, and the distribution of these invariants was studied in [8]. Delbourgo and K. conjectured that the proportion of primes p for which $\lambda_p(\chi\omega^i) > 0$ for at least one Teichmüller twist ω^i (i.e., p is χ-irregular, where p does not divide the conductor of χ) equals $(1 - e^{-1/2})/\varphi(\mathrm{ord}(\chi))$. This conjecture generalises the classical prediction for regular primes and is supported by extensive numerical evidence across a large range of characters and primes [8].

Stability of ℓ-parts ($\ell \neq p$). Washington ([22] Theorem 16.12) proved that for any prime $\ell \neq p$, the ℓ-part of $\mathrm{Cl}(K_r)$ remains bounded as $r \to \infty$. Therefore, the growth of the p-part of the class number in a cyclotomic $\mathbb{Z}_p$-extension is governed by the λ_p-invariant, whereas the ℓ-part remains bounded. The exponential growth of the class numbers is therefore achieved by picking up larger and larger prime factors.

6 Parameter Analysis for Ring-LWE

6.1 Power-of-Two Cyclotomic Parameters

The vast majority of deployed RLWE-based schemes use power-of-two cyclotomic rings $K = \mathbb{Q}(\zeta_{2^k})$ because of the following favourable properties:

- The ring dimension $n = 2^{k-1}$ is a power of two, enabling a highly efficient radix-2 NTT (see section 3.3).
- The different ideal is generated by $t = 2^{k-1} \in \mathbb{Z}$, so scaling from dual to non-dual RLWE preserves the spherical shape of the error distribution (see section 3.2).
- Small NTT-friendly primes q satisfying $q \equiv 1 \bmod m$ or mod $\frac{m}{2}$ exist (e.g., $q = 3329$ used in ML-KEM [12]).

However, there are also some potential disadvantages:

- For all computed cases, $h^+(K) = 1$ and Weber's conjecture predicts that $h^+(K) = 1$ for all power-of-two cyclotomic fields. The trivial plus class number means that the CMP algorithm reaches $\mathrm{Cl}^-(K)$ with no extra cost (step 1 is immediate).

Table 2. Power-of-two cyclotomic fields in standard RLWE parameter sets.

m	$\varphi(m)$	$h^+(K)$	$\log_2 h^-(K)$	prime q with $q \equiv 1 \pmod m$
256	128	1	43.79	3329; 7681
512	256	1*	126.17	3329†; 8 380 417
1024	512	1**	335.21	12289; 40961; $2^{60} - 2^{14} + 1$
2048	1024	1**	841.34	12289; 18433; 40961
4096	2048	1**	2030.45	12289; 40961; 61441

†: Satisfies $q \equiv 1 \pmod{m/2}$ only. *: Under GRH **: Under Weber's conjecture.

- The cyclotomic Iwasawa λ_2-invariant of the base field $\mathbb{Q}(i)$ is zero and $h^+(K)$ is odd, implying that the class group of K has odd order.
- K has a tower of subfields $\mathbb{Q}(\zeta_{2^j})$, $j < k$, which might be exploited in future attacks. Furthermore, the surjective Norm maps $\mathrm{Cl}(K) \to \mathrm{Cl}(\mathbb{Q}(\zeta_{2^j}))$ yield known quotients of $\mathrm{Cl}(K)$.

6.2 Alternative Prime Cyclotomic Parameters

Prime cyclotomic fields $K = \mathbb{Q}(\zeta_p)$ offer additional parameter choices with comparable or stronger Ideal-SVP hardness for the following reasons:

- A non-trivial real class number $h^+(K)$ means that step (1) of CMP requires multiplying $\mathfrak{a}$ by $\Theta(h^+(K))$ random short prime ideals before reaching $\mathrm{Cl}^-(K)$.
- The size of relative class numbers $h^-(K)$ is roughly the same and mainly depends on the degree of K. However, depending on the factorisation of $p - 1$, prime cyclotomic fields can have fewer subfields than power-of-two cyclotomic fields.
- Fields where $\lambda_p^-(K) > 0$ exhibit richer p-class group structure, making the Stickelberger reduction harder.

Table 3. Prime cyclotomic fields as candidate alternative RLWE parameters.

$m = p$	$\varphi(m)$	$h^+(K)$	$\log_2 h^-(K)$	$\lambda_p^-(K)$	prime q with $q \equiv 1 \pmod m$
257	256	3	126.04	1	1543; 9767
401	400	45	238.64	1	3209; 4813
587	586	1	402.30	2	8219; 10567
641	640	495	453.42	0	3847; 12821
1297	1296	275	1139.16	2	5189; 20753
3547	3546	16777	3996.52	0	21283; 99317

Comparing Table 3 with Table 2, prime cyclotomic fields of similar dimension $n = \varphi(m)$ can have larger real class numbers $h^+(K)$, with values ranging from 1 to 16 777. On the other hand, the relative class numbers are similar in size. Note that $p = 587$ is the only safe prime in Table 3. The corresponding cyclotomic field K has exactly two proper non-trivial subfields. However, it follows from the Jordan-Hölder filtrations in [19] that it is hard to find safe primes with non-trivial real class groups.

Efficiency tradeoffs. The use of prime cyclotomic rings involves the following tradeoffs:

- Since $q \equiv 1 \pmod{p}$ ensures complete splitting, the NTT still applies. However, $n = p - 1$ is generally not a power of two, requiring a more general (mixed-radix) NTT variant at a modest efficiency cost.
- For prime p, the non-dual RLWE variant inherits an elliptic Gaussian error distribution.

7 Conclusion

We have examined the relationship between the algebraic structure of ideal class groups in cyclotomic fields and the hardness of the Ideal-SVP problem that underlies RLWE security. Recent work [5] has established a hardness gap in the Ideal-SVP problem. However, it is not known whether this can be exploited in attacks against RLWE or MLWE.

A core part of the algorithm in [5] uses class group computations for cyclotomic fields. We investigated the class number and the relative class numbers which influence the efficiency of the attack. The real class number is usually small, while the relative class number $h^-(K)$ grows slightly faster than exponentially with primary dependence on the degree of the cyclotomic field.

Power-of-two cyclotomic fields are currently the dominant choice in cryptographic schemes. In this work, we propose alternative parameters that could offer similar or stronger hardness of the Ideal-SVP problem. Fields $K = \mathbb{Q}(\zeta_p)$ with large $h^+(K)$ and non-zero Iwasawa invariant $\lambda_p^-(K)$ are candidates for RLWE parameter rings offering harder Ideal-SVP. However, NTT variants come with a slight loss of efficiency. Furthermore, the dual and non-dual RLWE formulations are equivalent for power-of-two cyclotomics but diverge for prime cyclotomics due to elliptic error distortion.

Disclosure of Interests. The author has no competing interests to declare that are relevant to the content of this article.

References

1. Albrecht, M.R., Göpfert, F., Virdia, F.: Large modulus Ring-LWE ≥ Module-LWE. IACR Cryptol. ePrint Arch. 2016/770 (2017).

2. Alkim, E., Avanzi, R., Bos, J., Ducas, L., de la Piedra, A., Pöppelmann, T., Schwabe, P., Stebila, D.: NewHope: Algorithm specifications and supporting documentation. Second Round Submission to the NIST Post-Quantum Cryptography Standardization Project (2019). https://newhopecrypto.org/data/NewHope_2019_07_10.pdf
3. Biasse, J.F., Song, F.: A polynomial time quantum algorithm for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In: Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2016), pp. 893–902. SIAM, Philadelphia (2016).
4. Brakerski, Z., Vaikuntanathan, V.: Fully homomorphic encryption from ring-LWE and security for key dependent messages. In: Rogaway, P. (ed.) Advances in Cryptology – CRYPTO 2011, LNCS, vol. 6841, pp. 505–524. Springer, Heidelberg (2011).
5. Cramer, R., Ducas, L., Wesolowski, B.: Mildly short vectors in cyclotomic ideal lattices in quantum polynomial time. J. ACM 68 (2), 1–26 (2021).
6. Cramer, R., Ducas, L., Peikert, C., Regev, O.: Recovering short generators of principal ideals in cyclotomic rings. In: Fischlin, M., Coron, J.S. (eds.) Advances in Cryptology – EUROCRYPT 2016, LNCS, vol. 9666, pp. 559–585. Springer, Heidelberg (2016).
7. de Boer, K., van Woerden, W.: Lattice-based Cryptography: A survey on the security of the lattice-based NIST finalists. IACR Cryptol. ePrint Arch. 2025/304 (2025).
8. Delbourgo, D., Knospe, H.: On Iwasawa lambda-invariants for abelian number fields and random matrix heuristics. Math. Comp. 92, 1817–1836 (2023).
9. Ducas, L., Durmus, A.: Ring-LWE in polynomial rings. In: Safavi-Naini, R., Canetti, R. (eds.) Public-Key Cryptography – PKC 2012, LNCS, vol. 7293, pp. 34–51. Springer, Heidelberg (2012).
10. Damgård, I., Pastro, V., Smart, N.P., Zakarias, S.: Multiparty computation from somewhat homomorphic encryption. In: Safavi-Naini, R., Canetti, R. (eds.) Advances in Cryptology – CRYPTO 2012, LNCS, vol. 7417, pp. 643–662. Springer, Heidelberg (2012).
11. National Institute of Standards and Technology: Module-Lattice-Based Key-Encapsulation Mechanism Standard. Federal Information Processing Standards Publication (FIPS) 203. U.S. Department of Commerce, Washington, D.C. (2024). https://doi.org/10.6028/NIST.FIPS.203
12. National Institute of Standards and Technology: Module-Lattice-Based Digital Signature Standard. Federal Information Processing Standards Publication (FIPS) 204. U.S. Department of Commerce, Washington, D.C. (2024). https://doi.org/10.6028/NIST.FIPS.204
13. Kim, S.Y.: On the Iwasawa invariants of prime cyclotomic fields. Res. Number Theory 9(2), 29 (2023).
14. Langlois, A., Stehlé, D.: Worst-case to average-case reductions for module lattices. Des. Codes Cryptogr. 75(3), 565–599 (2015).
15. Lenstra, A.K., Lenstra, H.W. Jr., Lovász, L.: Factoring polynomials with rational coefficients. Math. Ann. 261(4), 515–534 (1982).
16. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. J. ACM 60(6), Art. 43 (2013).
17. Lyubashevsky, V., Nguyen, N.K., Plançon, M.: Lattice-based zero-knowledge proofs and applications: shorter, simpler, and more general. In: Malkin, T., Peikert, C. (eds.) Advances in Cryptology – CRYPTO 2022, LNCS, vol. 13507, pp. 71–101. Springer, Cham (2022).
18. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. J. ACM 56(6), Art. 34 (2009).

19. Schoof, R.: Class numbers of real cyclotomic fields of prime conductor. Math. Comp. 72(242), 913–937 (2003).
20. Schnorr, C.P., Euchner, M.: Lattice basis reduction: improved practical algorithms and solving subset sum problems. Math. Program. 66(1–3), 181–199 (1994).
21. Sinnott, W.: On the Stickelberger ideal and the circular units of an abelian field. Invent. Math. 62(2), 181–234 (1980).
22. Washington, L.C.: Introduction to Cyclotomic Fields, 2nd edn. Graduate Texts in Mathematics, vol. 83. Springer, New York (1997).