

# Ideal Lattices, Class Groups and Parameter Security for Ring-RLWE

Heiko Knospe

TH Köln – University of Applied Sciences

21 September 2026

# Abstract

The Ring Learning with Errors (RLWE) problem is widely believed to be computationally hard and underpins many modern lattice-based cryptographic constructions.

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.

Using these results, we examine standard power-of-two RLWE parameter choices and alternative prime cyclotomic fields.

## Question and Subject of the Study

Power-of-two cyclotomics make RLWE convenient. Do they also make the associated *ideal-lattice* problem algebraically easier?

- 1 The LPR theorem reduces worst-case approximate Ideal-SVP/SIVP to average-case RLWE under specific noise and modulus conditions.
- 2 Cramer–Ducas–Wesolowski (CDW) give a quantum  $\exp(\tilde{O}(\sqrt{n}))$ -approximation algorithm for cyclotomic Ideal-SVP, under stated class-group assumptions. Generalized to arbitrary number fields by Pellet-Mary, Hanrot, and Stehlé (PHS).
- 3 In the CDW approach,  $h^+(K)$  and  $h^-(K)$  matter. Power-of-two cyclotomics are special because  $h^+$  is known or conjectured to be 1.

# Module-LWE Standards

## NIST standards

ML-KEM and ML-DSA use module-LWE over

$$R_q = \mathbb{Z}_q[X]/(X^{256} + 1), \quad n = 256.$$

This is associated with the 512th cyclotomic field, but has module rank  $k > 1$  rather than the RLWE case  $k = 1$ .

| Scheme | modulus       | module dimensions                          |
|--------|---------------|--------------------------------------------|
| ML-KEM | $q = 3329$    | $k \in \{2, 3, 4\}$                        |
| ML-DSA | $q = 8380417$ | $(k, \ell) \in \{(4, 4), (6, 5), (8, 7)\}$ |

## 512th Cyclotomic Field

Advantages of  $\Phi_{512}(X) = X^{256} + 1$ :

- Radix-2 Cooley–Tukey NTT algorithm.
- Simple negacyclic convolution.
- The conversion between the canonical embedding of the dual ring and the coefficient embedding of the primal ring is a scaled isometry.
- Hence spherical canonical error remains spherical up to scaling.
- Mature constant-time implementations.

# RLWE

Let  $K = \mathbb{Q}(\zeta_m)$ ,  $R = \mathcal{O}_K = \mathbb{Z}[\zeta_m]$ ,  $n = \varphi(m)$ , and  $R^\vee = \mathfrak{D}_K^{-1}$  the codifferent ideal (dual lattice under the canonical embedding). Fix a discrete error distribution  $\chi$  on  $R_q^\vee$  (obtained by discretizing a Gaussian on  $K_{\mathbb{R}}$ ). Dual RLWE samples are:

$$a \leftarrow R_q, \quad s \leftarrow R_q^\vee, \quad e \leftarrow \chi, \quad b = as + e \in R_q^\vee.$$

## Definition

The two variants of the RLWE problems are:

- **Search RLWE:** Given polynomially many RLWE samples  $(a_i, b_i) \in R_q \times R_q^\vee$  for an unknown  $s$ , recover  $s$ .
- **Decision RLWE:** Distinguish between RLWE samples (for an unknown, uniformly chosen  $s$ ) and uniformly random pairs  $(a, b) \in R_q \times R_q^\vee$ .

# RLWE Security

## LPR reduction, informally

Let  $K = \mathbb{Q}(\zeta_m)$  have degree  $n = \varphi(m)$ . For a polynomially bounded prime  $q \equiv 1 \pmod{m}$  and error parameter  $\alpha q \geq \omega(\sqrt{\log n})$ , solving average-case search RLWE with spherical error yields a quantum polynomial-time algorithm for  $\gamma$ -Ideal-SVP, where

$$\gamma = \tilde{O}(\sqrt{n}/\alpha).$$

Lyubashevsky, Peikert, Regev, J. ACM 2013 (preliminary version EUROCRYPT 2010).

# CDW: A Route to Mildly Short Ideal Vectors

## CDW result, informally

For cyclotomic fields, under the number-theoretic hypotheses used in Cramer–Ducas–Wesolowski, there is a quantum polynomial-time algorithm for Ideal-SVP with approximation factor  $\exp(\tilde{O}(\sqrt{n}))$ .

Given an ideal  $\mathfrak{a}$ , the approach is

$$\boxed{\text{close principal multiple}} \implies \boxed{\text{mildly short generator}}.$$

- 1 Find integral ideals  $\mathfrak{b}, \mathfrak{c}$  with  $\mathfrak{a}\mathfrak{b}\mathfrak{c} = (g)$  principal and controlled norm.
- 2 In the logarithmic unit lattice, use cyclotomic units to replace  $g$  by a mildly short generator  $g/u \in \mathfrak{a}$ .

If  $N(\mathfrak{b}\mathfrak{c}) \leq \exp(\tilde{O}(n^{1+c}))$  for  $c < 1/2$ , the output has the advertised  $\exp(\tilde{O}(\sqrt{n}))$  approximation factor.

## Role of Class Groups in the First Stage

Let  $K^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ . The relevant decomposition is

$$1 \longrightarrow \text{Cl}^-(K) \longrightarrow \text{Cl}(K) \xrightarrow{N_{K/K^+}} \text{Cl}(K^+) \longrightarrow 1, \quad h^- = h/h^+.$$

- 1 Reach the minus part.** Multiply  $\mathfrak{a}$  by short random ideals  $\mathfrak{b}$  until  $[\mathfrak{a}\mathfrak{b}] \in \text{Cl}^-(K)$ . The index to overcome is  $[\text{Cl}(K) : \text{Cl}^-(K)] = h^+(K)$ .
- 2 Kill the minus part.** The projected Stickelberger ideal annihilates  $\text{Cl}^-(K)$ . Find a factor base of short prime ideals whose classes generate  $\text{Cl}^-(K)$ , and via the Stickelberger lattice compute a short integral ideal  $\mathfrak{c}$  such that  $[\mathfrak{a}\mathfrak{b}]^{-1} = [\mathfrak{c}]$ . Then  $\mathfrak{a}\mathfrak{b}\mathfrak{c}$  is principal.

# Class Number Formulas

The analytic class number formula for  $K = \mathbb{Q}(\zeta_m)$  yields formulas for  $h = h(K)$ ,  $h^+(K)$  and  $h^-(K)$ .

$$\frac{2^{r_1}(2\pi)^{r_2} hR}{w\sqrt{|\Delta_K|}} = \prod_{\substack{\chi \in X_m \\ \chi \neq 1}} L(1, \chi),$$

where  $X_m$  is the group of Dirichlet characters modulo  $m$ . However, this formula involves the regulator  $R$ .

# The Real Class Number

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.

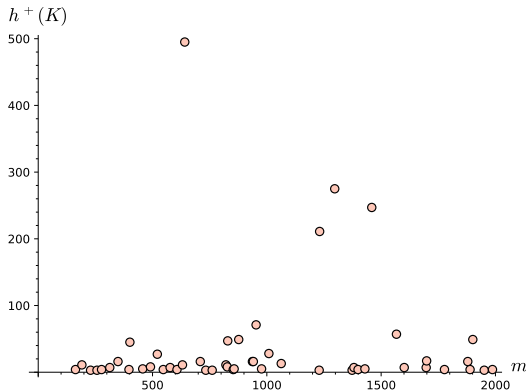
## Theorem (Sinnott)

*Let  $m = p^k$  and let  $C^+$  be the group of cyclotomic units of  $K^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$  with ring of integers  $\mathcal{O}_{K^+}$ . Then  $C^+$  has finite index in  $(\mathcal{O}_{K^+})^\times$  and*

$$h^+(K) = [(\mathcal{O}_{K^+})^\times : C^+].$$

# Computing the Real Class Number

Schoof computed the index  $[(\mathcal{O}_{K^+})^\times : C^+]$  for all primes  $p < 10^5$  up to a factor that is probably 1 (or otherwise at least 80 000). For the computed range, the data show that  $h^+(K)$  is often small.



## Computing the Minus Class Number

From the analytic class number formula, one obtains an explicit formula for  $h^-$  (without regulator):

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

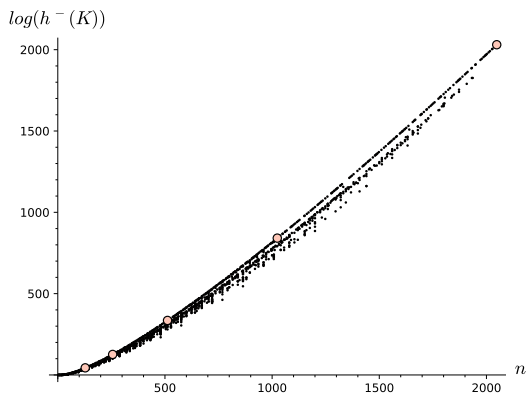
where  $B_{1,\chi}$  are first generalized Bernoulli numbers, and

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

Numerically,  $\ln h^-(K) \sim \frac{1}{4} n \ln(m)$ , where  $n = \varphi(m)$ , as  $m \rightarrow \infty$ . However, this asymptotic formula overestimates  $\ln h^-(K)$  for cryptographic dimensions, where the factor in front of  $n \ln(m)$  is closer to 0.1 than to 0.25.

# Computing the Minus Class Number

Numerical evaluations show that the size of  $h^-(K)$  for power-of-2 cyclotomic fields  $K = \mathbb{Q}(\zeta_m)$  ( $m = 256, 512, 1024, 2048$ ) is at the upper end of the range of relative class numbers for fields of comparable degree.



## Candidate Fields for RLWE using Prime Cyclotomics

| $p$  | $n = p - 1$ | $h^+$ | $\log_2 h^-$ | $\lambda_p^-$ | example $q \equiv 1 \pmod{p}$ |
|------|-------------|-------|--------------|---------------|-------------------------------|
| 257  | 256         | 3     | 126.04       | 1             | 1543; 9767; 328961            |
| 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                  |

$h^-$  values: computed via Bernoulli numbers; prime  $h^+$  values: Schoof's calculations.

| $m$  | $n = \frac{m}{2}$ | $h^+$ | $\log_2 h^-$ | $\lambda_2^-$ | example $q \equiv 1 \pmod{m}$ |
|------|-------------------|-------|--------------|---------------|-------------------------------|
| 512  | 256               | 1*    | 126.17       | 0             | 3329**; 7681; 8380417         |
| 1024 | 512               | 1***  | 335.21       | 0             | 12289; 13313                  |
| 2048 | 1024              | 1***  | 841.34       | 0             | 12289; 18433                  |
| 4096 | 2048              | 1***  | 2030.45      | 0             | 12289; 40961                  |

\* under GRH; \*\*  $q \equiv 1 \pmod{\frac{m}{2}}$ ; \*\*\* conditional on Weber's conjecture.

# Main Obstacle: Prime Conductors Change Error Geometry

The transparent dual/non-dual correspondence is special to  $m = 2^k$ .

## Power of two

$$\Phi'_{2^k}(\zeta_{2^k}) = -n\zeta_{2^k}^{-1}.$$

Multiplication by a generator of the different is a scaled isometry in the canonical embedding. Spherical dual error remains spherical up to scale.

## Prime conductor

$$\Phi'_p(\zeta_p) = \frac{p\zeta_p^{-1}}{\zeta_p - 1}.$$

Its magnitude varies across embeddings. Mapping dual RLWE to  $R$  produces an *elliptical* distribution in a power basis.

# Error Geometry: The Ducas–Durmus Framework

## Choices for non-dual sampling

- **Direct transformation** via the different gives an elliptical, basis-distorted distribution.
- **Ducas–Durmus approach:** Scale by  $p$  and sample a polynomial  $e'(X) \in \mathbb{Q}[X]/(X^p - 1)$  with spherical (i.i.d.) Gaussian coefficients, and reduce modulo  $\Phi_p(X)$ :

$$e(X) = e'(X) \bmod \Phi_p(X) \in \mathbb{Q}[X]/(\Phi_p(X)) \cong \mathbb{Q}(\zeta_p).$$

Because  $X^{p-1} \equiv -(1 + X + \dots + X^{p-2})$ , the resulting coefficients  $e_i = e'_i - e'_{p-1}$  are correlated, but embed spherically into the canonical geometry.

Yu–Xu–Wang (PKC 2017) constructed an IND-CPA secure NTRU variant over  $\mathbb{Z}[X]/(\Phi_p(X))$  using the Ducas–Durmus setting.

## Arithmetic: NTT for Prime Cyclotomics

If  $q \equiv 1 \pmod{p}$ , then  $\Phi_p(X)$  splits completely into linear factors:

$$R_q \cong \prod_{i \in (\mathbb{Z}/p\mathbb{Z})^\times} \mathbb{Z}_q.$$

- **Naive evaluation:** Direct matrix multiplication costs  $O(p^2)$  operations.
- **Rader's algorithm:** Maps the nontrivial  $(p-1)$ -point evaluation to a cyclic convolution of length  $p-1$  via a multiplicative generator  $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ .
- **Smooth  $p-1$ :** If  $p-1$  is smooth and  $(p-1) \mid (q-1)$ , this convolution runs via standard small-radix NTT in  $O(p \log p)$ .

## Arithmetic: NTT for Prime Cyclotomics

### Example

For  $p = 257$ , the convolution length is  $p - 1 = 256 = 2^8$  (radix-2). Choosing  $q = 328961 = 1 + 5 \cdot (257 \cdot 256)$  guarantees both  $257 \mid (q - 1)$  and  $256 \mid (q - 1)$ , enabling pure radix-2 NTT convolution over  $\mathbb{F}_q$ .

## Conclusion

- Power-of-two cyclotomics remain superb engineering choices. Their small real class groups are, however, especially favourable to the currently known class-group-based approach for mildly approximating Ideal-SVP.
- Prime fields such as  $p = 257, 401, 641, 1297$  offer nontrivial  $h^+$  at plausible dimensions and are natural candidates for systematic study.
- Their cost is relevant: less convenient transform structure and nontrivial error geometry in a practical coefficient embedding.
- The conclusion is not “prime cyclotomics are more secure.” They provide an experimental family in which ideal-class-group structure, Ideal-SVP algorithms, and concrete RLWE cryptanalysis can be tested.

# Backup: Minus Class Numbers for Power-of-Two Cyclotomics

**Table:** *Class numbers of power-of-two cyclotomic fields (see Washington 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          | $6262503984490932358745721482528922841978219389975605329 =$<br>$17 \cdot 21121 \cdot 76532353 \cdot 29102880226241 \cdot 7830753969553468937988617089$ |
| 1024 | 512          | $381797475160219002830149856048779360790504342984157709791781101116579665300 \dots$                                                                    |
| 2048 | 1024         | $17 \cdot 21121 \cdot 76532353 \cdot 249361921 \cdot 6436466177 \cdot 550807805953 \cdot 29102880226241 \cdot \dots^*$                                 |
| 4096 | 2048         | $17 \cdot 21121 \cdot 83969 \cdot 7891969 \cdot 76532353 \cdot 249361921 \cdot 6436466177 \cdot \dots^*$                                               |

\*: Larger prime factors omitted.