ATTACK ON GALOIS RLWE

KRISTIN LAUTER, KATE STANGE, HAO CHEN

ABSTRACT. We describe a new attack on the Ring learning-with-errors (RLWE) problem based on chi-square test, and give examples of Galois number fields vulnerable to our attack. We also analyze the security of cyclotomic extensions under our attack using Fourier analysis on finite fields.

1. INTRODUCTION

The Ring learning with errors (RLWE) problem, proposed in [LPR13], is a variant of the traditional learning with error (LWE) problem, and is an active research area in lattice based cryptography. It has been studied extensively in (a lot of papers).

Central to an RLWE problem instance is a choice of a number field K and a prime q called the *modulus*. The authors of [LPR13] considered the case where K is some cyclotomic field, and proved a reduction from certain hard lattice problems to the dual variant of RLWE. The hardness for the non-dual variant was proved in [DD12]. Also in [LPR13], a search-to-decision reduction was proved for RLWE problems for cyclotomic fields and modulus q which splits completely in the field. This reduction was then generalized to general Galois extensions in [EHL14].

The [ELOS] paper proposed an attack to decision RLWE problem. The attack makes use of ring homomorphisms $\pi : R \to \mathbb{F}_q$, and works when the image of the RLWE error distribution under the map π only takes value in a stricly smaller subset of $\mathbb{F}_q$, with overwhelming probability. The authors of [ELOS] then gave an infinite family of examples vulnerable to the attack. Unfortunately, the vulnerable number fields in [ELOS] are not Galois extensions of $\mathbb{Q}$. Hence, the search-to-decision reduction theorem does not apply, and the attack can not be directly used to solve the search variant of RLWE for those instances.

In our paper, we generalize the attack of [ELOS] to Galois number fields and moduli of higher degree. Also, we analyze the vulnerability of cyclotomic fields to the [ELOS] attack, and show that they are in general safe, except for the case when the modulus p is equal to the index of the cyclotomic field (i.e., $K = \mathbb{Q}(\zeta_p)$).

1.1. **Organization.** In section 2, we recall the canonical embedding of number fields and the central definitions related to the RLWE problems. In section 3, we review prime factorizations in Galois extensions and prove a search-to-decision reduction for Galois extensions K and unramified primes of any degree. In section 4, we introduce an attack to RLWE problems based on the chi-square statistical test, which directly generalizes the attack in [ELOS]. More precisely, the attack aims at two problems: the decision version of RLWE, and an intermediate problem used in the search-to-decision proof of [LPR13], which we denote by SRLWE($\mathcal{R}, \mathfrak{q}$) (see Definition 3.1). The time complexity of our attack for both problems above is $O(\frac{n}{f}q^{2f})$, Here n is the degree of the number field K, and f is the *residue degree* of q in K (see Lemma 3.2). In section 5, we give examples of subfields of cyclotomic fields vulnerable to our new attack, where the moduli q has residue degree two.

In section 6, we show that our attack works on prime cyclotomic fields when the moduli is equal to the unique ramified prime. Finally, in section 7, we show that general cyclotomic extensions with an unramified prime as the modulus q are invulnerable to our attack.

2. BACKGROUND

Let K be a number field of degree n with ring of integers R and let $\sigma_1, \cdots, \sigma_n$ be the embeddings of K into $\mathbb{C}$, the field of complex numbers. The *canonical embedding* of K is

$$\iota : K \to \mathbb{C}^n$$
$$x \mapsto (\sigma_1(x), \cdots, \sigma_n(x)).$$

1

To work with real vector spaces, we define the *adjusted embedding* of K as follows. Let r_1, r_2 denote the number of real embeddings and conjugate pairs of complex embeddings of K. Without loss of generality, assume $\sigma_1, \cdots, \sigma_{r_1}$ are the real embeddings and $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$ for $1 \leq j \leq r_2$. We define

$$\tilde{\iota} : K \to \mathbb{R}^n$$
$$x \mapsto (\sigma_1(x), \cdots, \sigma_{r_1}(x), \mathrm{Re}(\sigma_{r_1+1})(x), \mathrm{Im}(\sigma_{r_1+1})(x), \cdots, \mathrm{Re}(\sigma_{r_1+r_2})(x), \mathrm{Im}(\sigma_{r_1+r_2})(x))$$

It turns out that $\tilde{\iota}(R)$ is a lattice in $\mathbb{R}^n$. Let $w = (w_1, \cdots, w_n)$ be a $\mathbb{Z}$-basis for R.

Definition 2.1. The canonical (resp.adjusted) embedding matrix of w, denoted by A_w (resp. $\tilde{A}_w$), is the n-by-n matrix whose i-th column is $\sigma(w_i)$ (resp. $\tilde{\sigma}(w_i)$).

The two embedding matrices are related in a simple way: let T denote the matrix

$$T = \begin{bmatrix} I_{r_1} & 0 \\ 0 & T_{r_2} \end{bmatrix}, \text{ where } T_s = \frac{1}{\sqrt{2}} \begin{bmatrix} I_{r_2} & I_{r_2} \\ -iI_{r_2} & iI_{r_2} \end{bmatrix},$$

Then we have

$$\tilde{A}_w = TA_w.$$

For $\sigma > 0$, define the Gaussian function $\rho_\sigma : \mathbb{R}^n \to [0,1]$ as $\rho_\sigma(x) = e^{-||x||^2/2\sigma^2}$ (our σ is equal to $r/\sqrt{2\pi}$ for the parameter r in [LPR13]).

Definition 2.2. For a lattiace $\Lambda \subset \mathbb{R}^n$ and $\sigma > 0$, the *discrete Gaussian distribution* on Λ with parameter σ is:

$$D_{\Lambda,\sigma}(x) = \frac{\rho_\sigma(x)}{\sum_{y \in \Lambda} \rho_\sigma(y)}, \forall x \in \Lambda.$$

Equivalently, the probability of sampling any lattice point x is proportional to $\rho_\sigma(x)$.

2.1. Ring LWE problems for general number fields.

Definition 2.3. An *RLWE instance* is a tuple $\mathcal{R} = (K, q, \sigma, s)$, where K is a number field with ring of integers R, q is a prime, $\sigma > 0$, and $s \in R/qR$ is the *secret*.

Definition 2.4. Let $\mathcal{R} = (K, q, \sigma, s)$ be an RLWE instance, and let R be the ring of integers of K. The *error distribution* of $\mathcal{R}$, denote by $D_\mathcal{R}$, is the discrete lattice Gaussian

$$D_\mathcal{R} = D_{\iota(R),\sigma}.$$

Let n denote the degree of K, and let V denote the covolume of the lattice $\tilde{\iota}(R)$. As is pointed out by [ELOS], when analyzing the error distribution, one needs to take into account the sparsity of the lattice $\tilde{\iota}(R)$, which is measured by V. In light of this, we define a relative version of the standard deviation:

$$\sigma_0 = \frac{\sigma}{V^{\frac{1}{n}}}.$$

Definition 2.5 (RLWE distribtuion). Let $\mathcal{R} = (K, q, \sigma, s)$ be an RLWE instance with error distribution $D_\mathcal{R}$, We let R_q denote R/qR, then a sample from the *RLWE distribtuion* of $\mathcal{R}$ is a tuple

$$(a, b = as + e \pmod{qR}) \in (R_q)^2,$$

where the first coordiante a is chosen uniformly at random in R_q, and $e \leftarrow D_\mathcal{R}$. We abbreviate and write $(a, b) \leftarrow \mathcal{R}$.

The RLWE problem has two variants: search and decision.

Definition 2.6 (Search). Let $\mathcal{R}$ be an RLWE intance. The *search Ring-LWE* problem, denoted by SRLWE($\mathcal{R}$), is to discover s given access to arbitrarily many independent samples $(a, b) \leftarrow \mathcal{R}$.

Definition 2.7 (Decision). Let $\mathcal{R}$ be an RLWE intance. The *decision Ring-LWE* problem, denoted by DRLWE($\mathcal{R}$), is to distinguish between the same number of independent samples in two distributions on $R_q \times R_q$. The first is the RLWE distribution of $\mathcal{R}$, and the second consists of uniformly random and independent samples from $R_q \times R_q$.

3. SEARCH-TO-DECISION REDUCTION

We prove the the reduction of SRLWE for Galois extensions to an intermediate problem, denoted by $SRLWE(\mathbb{R}, \mathfrak{q})$ (the same problem is denoted by $\mathfrak{q}_i$-LWE in [LPR13]), of recovering the secret modulo some prime ideal $\mathfrak{q}$ of K lying above q. This result can be viewed as a generalization of [EHL14, Theorem 2] to primes of higher degree. Since our attack in this paper is targeting at $SRLWE(\mathcal{R}, \mathfrak{q})$, we could attack SRLWE for any Galois RLWE instances we found vulnerable.

Definition 3.1. Given an RLWE instance $\mathcal{R} = (K, q, \sigma, s)$ and a prime ideal $\mathfrak{q}$ of K lying above q. The problem SRLWE$(\mathcal{R}, \mathfrak{q})$ is: given access to arbitrarily many independent samples $(a, b) \leftarrow \mathcal{R}$, find $s \pmod{\mathfrak{q}}$. The reduced error distribution with respect to $\mathfrak{q}$ is $D_{\mathcal{R}} \pmod{f q}$, which we denote by $D_{\mathcal{R}, \mathfrak{q}}$.

We prove the reduction from SRLWE$(\mathcal{R})$ to SRLWE$(\mathcal{R}, \mathfrak{q})$ when q is unramified. We recall some algebraic number theoretical facts in the following

Lemma 3.2. *Let $K/\mathbb{Q}$ be a finite Galois extension with ring of integers R, and let q be a prime unramified in K. Then there exists an integer $g \mid n$, and a set of g distinct prime ideals $\mathfrak{q}_1, \cdots, \mathfrak{q}_g$ of R such that*

$$qR = \prod_{i=1}^{g} \mathfrak{q}_i.$$

Let $f = \frac{n}{g}$. Then for each i, the quotient $R/\mathfrak{q}_i$ is a finite field of cardinality q^f, and there is a canonical isomorphism of rings

$$R_q \cong R/\mathfrak{q}_1 \times \cdots \times R/\mathfrak{q}_g.$$

The number f in the above lemma is called the *residue degree* of q in K. The prime q splits completely in K if and only if its residue degree is one.

Now we are ready to state and prove

Theorem 3.3. *Let $\mathcal{R} = (K, q, \sigma, s)$ be an RLWE instance with $K/\mathbb{Q}$ Galois and q unramified in K with residue degree f. Suppose there is an algorithm $\mathscr{A}$ which solves SRLWE$(\mathcal{R}, \mathfrak{q})$ using a list S of samples. Assume that the running time of the algorithm $\mathscr{A}$ is t. Then the problem SRLWE$(\mathcal{R})$ can be solved in time $T = \frac{n}{f} t$ using the samples in S. Here C is some constant depending on K.*

Proof. The Galois group $G = Gal(K/\mathbb{Q})$ acts on the set $\{\mathfrak{q}_1, \cdots, \mathfrak{q}_g\}$ transitively. Hence for each i, we can take $\sigma \in Gal(K/\mathbb{Q})$, such that $\sigma_i(\mathfrak{q}) = \mathfrak{q}_i$, Then we run the algorithm $\mathscr{A}$ on the input $(\sigma_i^{-1}(S), \mathfrak{q}_i)$. The algorithm will output $\sigma_i^{-1}(s) \pmod{\mathfrak{q}}$, which is equal to $s \pmod{\mathfrak{q}_i}$. We then do this for all $1 \leq i \leq g$ and use the last formula of Lemma to recover s. The complexity estimate follows from the fact that we are applying the algorithm g times. $\qquad\square$

In particular, Theorem 3.3 gives a polynomial time reduction from SRLWE$(\mathcal{R})$ to SRLWE$(\mathcal{R}, \mathfrak{q})$.

Remark 3.4. Note that in the complexity computation above we have chosen to neglect the time taken by applying Galois automorphisms to the samples, because the runtime depends hugely on the instance and on the way we represent the samples. For example, for subfields of cyclotomics with normal integral bases, the Galois autormophisms are simply permutations of coordinates, so it could be done very fast.

Remark 3.5. Although the theorem is stated for any unramified prime. From an attacker's perspective, we still take primes of small degree, since the search space for $s \pmod{\mathfrak{q}}$ is of size q^f, and it is bad when f is large.

The search-to-decision reduction will follow from the lemma below.

Lemma 3.6. *There is a probablistic polynomial time reduction from SRLWE$(\mathcal{R}, \mathfrak{q})$ to DRLWE$(\mathcal{R})$.*

Proof. This is a direct consequence of [LPR13, Lemma 5.9 and Lemma 5.12] and our Theorem 3.3. $\qquad\square$

Corollary 3.7. *Suppose $\mathcal{R}$ is an RLWE instance where K is Galois and q is an unramified prime in K. Then there is a probablistic polynomial-time reduction from SRLWE$(\mathcal{R})$ to DRLWE$(\mathcal{R})$.*

4. The chi-square attack for uniform distribution

4.1. **chi-square test for uniform distribution.** We briefly review the properties and usage of the chi-square test for uniform distributions over a finite set S. We partition S into r subsets

$$S = \bigsqcup_{j=1}^{r} S_i,$$

Suppose there are M samples $y_1, \cdots, y_M \in S$. For each $1 \leq j \leq r$, we compute the expected number of samples that would fall in the j-th subset: $c_j := \frac{|S_j|M}{|S|}$. Then we compute the actual number of samples in S_j, i.e., $t_j := |\{1 \leq i \leq r : y_i \in S_j\}|$. Finally, the χ^2 value is computed as

$$\chi^2(S, y) = \sum_{j=1}^{r} \frac{(t_j - c_j)^2}{c_j}.$$

Suppose the samples are drawn from the uniform distribution on S. Then the χ^2 value follows the chi-square distribution with degree of freedom equal $d = r - 1$. To decide whether the samples are from a uniform distribtuion, we can either look up a table of χ^2 values, or use an approximation rule: when d is large, the χ^2 distribution can be well-approximated by a normal distribution $N(d, 2d)$; for example, if it turns out that $\chi^2 \notin (d - c\sqrt{2d}, d + c\sqrt{2d})$, then the confidence we have that the samples are not taken from a uniform distribution is $2\Phi(c) - 1$.

If P, Q are two probability distributions on S, then their *statistical difference* is defined as

$$d(P, Q) = \frac{1}{2} \sum_{t \in S} |P(t) - Q(t)|.$$

For convenience, we also define the l_2 *distance* between P and Q as $d_2(P, Q) = (\sum_{t \in S} |P(t) - Q(t)|^2)^{\frac{1}{2}}$. We have the inequality $d(P, Q) \leq \frac{\sqrt{|S|}}{2} d_2(P, Q)$.

4.2. **The chi-square attack on** $\mathrm{SRLWE}(\mathcal{R}, \mathfrak{q})$**.** Let $\mathcal{R}$ be an RLWE instance with error distribution $D_{\mathcal{R}}$ and $\mathfrak{q}$ be a prime ideal above q. Our attack relies on the assumption that the distribution $D_{\mathcal{R}} \pmod{\mathfrak{q}}$ is distinguishable from the uniform distribution on the finite field $F = R/\mathfrak{q}$. More precisely, the attack loop through all q^f possitbilities of $\bar{s} = s \pmod{\mathfrak{q}}$. For each guess s', it computes the values $\bar{e}' = \bar{b} - \bar{a}s' \pmod{\mathfrak{q}}$ for every sample $(a, b) \in S$. If the guess is wrong, or if the samples are taken from the uniform distirbution in $(R_q)^2$ instead of an RLWE instance, the values $\bar{e}'$ would be uniformly distributed in F and it is likely to pass the chi-square test. On the other hand, if the guess is correct, then we expect the errors $\bar{e}'$ to fail the test.

Let $N = q^f$ denote the cardinality of F. Note that N is also the number of tests we run in the attack. For the attack to be successful, we need the $(N - 1)$ tests corresponding to wrong guess of $s \pmod{\mathfrak{q}}$ to pass, and the one test corresponding to the correct guess to fail. Therefore, we need to choose the confidence interval of our test so that it is unlikely for a set of samples coming from uniform distribution to fail the test. In practice, we choose the confidence level to be $\alpha = 1 - \frac{1}{10N}$. Let β denote the probability that the sample errors fails the uniform test with probability Then the probability that our algorithm will success is $p = (1 - \frac{1}{10N})^{N-1}\beta$. Note that when N is large, $(1 - \frac{1}{10N})^{N-1}$ is about $e^{-1/10} \approx 0.904$.

Algorithm 1 chi-square attack of $SRLWE(\mathcal{R}, \mathfrak{q})$

Require: $\mathcal{R} = (K, q, \sigma, s)$ – an RLWE instance.
        R – the ring of integers of K.
        $\mathfrak{q}$ – a prime ideal in K above q.
        N – the cardinality of $R/\mathfrak{q}$.
        B – the number of bins $(B < N)$.
        S – a collection of M $(M = \Omega(N))$ RLWE samples $(a, b) \sim \mathcal{R}$.
Ensure: a guess of the value s (mod $\mathfrak{q}$), or **NON-RLWE**, or **INSUFFIICNET-SAMPLES**

1: $\alpha \leftarrow 1 - \frac{1}{10N}$.
2: $\omega \leftarrow \Phi^{-1}((1 + \alpha)/2)$
3: $G \leftarrow \emptyset$
4: **for** s in F **do**
5:     $E \leftarrow \emptyset$.
6:     **for** a, b in S **do**
7:         $\bar{a}, \bar{b} \leftarrow a \pmod{\mathfrak{q}}, b \pmod{\mathfrak{q}}$.
8:         $\bar{e} \leftarrow \bar{b} - \bar{a}s$.
9:         add $\bar{e}$ to E.
10:     **end for**
11:     Run χ^2 test on E and obtain the value $\chi^2(E)$.
12:     **if** $|\chi^2(E) - (N - 1)| > \omega\sqrt{2N - 2}$ **then**
13:         add s to G
14:     **end if**
15: **end for**
16: **if** $G = \emptyset$ **then**
        return **NOT RLWE**
17: **else if** $G = \{g\}$ **then**
        return g
18: **else**
        return **INSUFFIICNET-SAMPLES**
19: **end if**

Note that the time complexity of the attack is $O(q^f)$ since we have q^f possible values for s (mod $\mathfrak{q}$). The number of samples need for the attack is also $O(q^f)$. The correctness of the attack is captured in the following theorem.

Theorem 4.1. *Assume $q \gg 1$. Let Δ denote the statistical distance between the error distribution $D_{\mathcal{R}, \mathfrak{q}} := D_{\mathcal{R}}$ (mod $\mathfrak{q}$) and the uniform distribtuion on $R/\mathfrak{q}$. Then the above attack succeeds with proability at least*

$$p = 0.904(1 - \Phi(\frac{\omega\sqrt{2(N - 1)} - \lambda}{\sqrt{2(N - 1) + 4\lambda}})),$$

where Φ is the cumulative distribution function for the standard Gaussian distribution, $\omega = \Phi^{-1}(1 - \frac{1}{20N})$, and $\lambda = 4M\Delta$.

Proof. The chi-square value for uniformity on samples from $D_{\mathcal{R}, \mathfrak{q}}$ follow a noncentral chi-square distribution with the same degree of freedom and a parameter λ given by

$$\lambda = MNd_2(D_{\mathcal{R}, \mathfrak{q}}, U(R/\mathfrak{q}))^2.$$

(fixme: cite the chisquare paper.) In particular, we have $\lambda \geq 4M\Delta$. We approximate a noncentral chi-square distribution with degree of freedom k and parameter λ with a Gaussian distribution of mean $k + \lambda$ and variance $2k + 4\lambda$. The result now follows from the fact that the argument of Φ is a decreasing function of λ. $\square$

To get a sense of how the constants behave, we give a table containing some p values for various choices of N and Δ. We fix the number of samples to be $M = 5N$. Note that 0.904 is the upper bound of the success rate.

TABLE 4.1. Success rates of chi-square attack

$N(= q^f)$	$d(D_{\mathcal{R},\mathfrak{q}}, U(R/\mathfrak{q}))$	p
257	0.025	0.84
4093	0.005	0.551
67^2	0.005	0.610
12289	0.005	0.903
307^2	0.001	0.27

5. VULNERABLE INSTANCES AMONG SUBFIELDS OF CYCLOTOMIC FIELDS

We restrict our attention to subfields of cyclotomic fields $\mathbb{Q}(\zeta_m)$, where we assume m is *odd and squarefree*. The Galois group $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is canonically isomorphic to $(\mathbb{Z}/m\mathbb{Z})^*$.

Notation: for each subgroup H of $G = (\mathbb{Z}/m\mathbb{Z})^*$, we use $K_{m,H}$ to denote the fixed field

$$K_{m,H} := \mathbb{Q}(\zeta_m)^H.$$

The extension $K_{m,H}/\mathbb{Q}$ is Galois of degree $n = \frac{\varphi(m)}{|H|}$; the degree of a prime q in $K_{m,H}$ is equal to the order of $[q]$ in the quotient group G/H. Moreover, every field of form $K_{m,H}$ has canonical *normal integral basis*, whose embedding matrix is easy to compute. More precisely, let C denote a set of coset representatives of the group G/H. For each $c \in C$, set

$$w_c = \sum_{h \in H} \zeta_m^{hc}.$$

Then $\mathbf{w} := (w_c)_{c \in C}$ is a $\mathbb{Z}$-basis of R. For a proof of this fact, see [Joh11, Proposition 6.1].

We set $\zeta = \exp(2\pi i/m)$. Then the canonical embedding embedding matrix of w is

$$(A_w)_{i,j} = \sum_{h \in H} \zeta^{hij}.$$

Lemma 5.1. *Suppose $\mathcal{R}$ is an RLWE instance such that the underlying field K is a Galois number field, and q is unramified in K. Then error distribution $D(\mathcal{R}, \mathfrak{q})$ is independent of the choice of prime ideal $\mathfrak{q}$ above q.*

Proof. From the proof of [fixme: search-to-decision], we know that the change from a prime $\mathfrak{q}$ to $\mathfrak{q}'$ can be done via applying an element of the galois group $\mathrm{Gal}(K/\mathbb{Q})$ to the RLWE samples from $\mathcal{R}$. The Galois group acts on the embedded lattice $\Lambda := \iota(R)$ by permuting the set of embeddings of K. So we have obtained a group homomorphism

$$\phi : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Aut}(\Lambda).$$

Since permutation matrices are orthogonal, the Galois group action on the lattice Λ is distance-preserving. Hence it preserves discrete Gaussian distributions on Λ. This completes the proof. $\square$

Combining this theorem with Lemma about existence, we see that for fields of form $K_{m,H}$, the error distribution modulo $\mathfrak{q}$ is the same, no matter which prime ideal $\mathfrak{q}$ is used. In the discussion below, we omit our choice of $\mathfrak{q}$.

5.1. **Searching.** The above algorithm allows us to search for vulnerable instances among fields of form $K_{m,H}$. The search is done by generating actual RLWE samples from the instance and run the chi-square attack on these samples. Success of the attack will indicate vulnerability of the instance. Our field search requires sampling efficiently from a discete Gaussian $D_{\Lambda,\sigma}$ for which we choose the method outlined in [**?**].

In the first table, we list some instances for which the attack have succeeded. The columns of Table 5.1 are as follows. The first two columns specify the field $K = K_{m,H}$; the column labled n is the degree of K, q is the modulus of choice, and f is the residue degree of q. Note that we ommited our choice of prime ideal $\mathfrak{q}$, since due to Lemma 5.1 the choice is irrelevant to our attack.

TABLE 5.2. Some Vulnerable sub-cyclotomic RLWE instances

m	generators of H	n	q	f	σ_0	no. samples used	est.runtime (h)	$\hat{p}$
255255	[97943, 83656, 77351, 78541, 129403]	90	463	2	1	21436	1786.41	1.0 (*)
285285	[181156, 210926, 87361]	96	131	2	1	?	?	?

TABLE 5.1. Attacked sub-cyclotomic RLWE instances

m	generators of H	n	q	f	σ_0	no. samples used	running time of attack (in secs)
2805	[1684, 1618]	40	67	2	1	22445	12569.2
90321	[90320, 18514, 43405]	80	67	2	1	26934	17323.4
15015	[12286, 2003, 11936]	60	43	2	1	11094	3813
1468005	[198892, 978671, 431521, 1083139]	144	139	2	1	4000	20593

In the second table, we list some vulnerable instances we found, for which the attack is likely to succeed based on the theorem in chisquare test, but will take a long time to finish. Hence instead of running the actual attack, we first run the chi-square test on the correct error samples, and then run a few chisuqare tests on some random guesses of s (mod $\mathfrak{q}$). We then estimate the success rate using the theorem. More precisely, suppose $\hat{\chi^2}$ is the chi-square value of the sample errors from $D_{\mathcal{R},\mathfrak{q}}$. We replace λ by $\hat{\chi^2}$ in the formula and compute

$$\hat{p} = 0.904 \left(1 - \Phi \left(\frac{\Phi^{-1}(1 - \frac{1}{20N})\sqrt{2(N-1)} - \hat{\chi^2}}{\sqrt{2(N-1) + 4\hat{\chi^2}}} \right) \right).$$

The value $\hat{p}$ is then our estimate of the sucess rate of our attack. In addition, we estimate the runtime based on the average time taken for the tests we've done.

5.2. **Discussion.** One may notice that in all the vulnerable instances in table, the prime q has degree $f = 2$. We explain why primes of degree higher than one are more likely to vulnerable, and introduce a new test based on it.

The intuition is the following: Assume K is a Galois number field and q is a prime of degree r in K. Suppose we have found a reduced basis $w_1, \cdots, w_n$ of R with respect to the adjusted embedding. Fix a prime ideal $\mathfrak{q}$ above q. Then the image $\bar{w}_1, \cdots \bar{w}_n$ lie in $R/\mathfrak{q}$, a finite field of cardinality q^r. However, if for some index i, the element w_i lies inside some proper subfield K' of K, and if q has degree $r' < r$ in K', then $\bar{w}_i$ will lie in a proper subfield of $R/\mathfrak{q}$. If the above situation happens for a large portion of the w_i's, then we would expect that the error distribution mod $\mathfrak{q}$, which we denoted by $D_{\mathcal{R},\mathfrak{q}}$ in other sections, will take values in a proper subfield of $R/\mathfrak{q}$ more frequently than the uniform distribution.

5.3. **a detailed example.** In order to illustrate the search-to-decision reduction (Theorem **??**), we study an sub-cyclotomic RLWE instance in detail, where we generate RLWE samples, perform the attack, and used search-to-decision reduction to recover the entire secret key s.

Let $m =$ and H be the subgroup of $(\mathbb{Z}/m\mathbb{Z})^*$ generated by .. , and let $K = K_{m,H}$, a Galois number field with degree ?. After a BKZ lattice reduction, we obtained an basis $v_1, \cdots, v_n$ for the ring of integers R, ordered by increasing embedding length. We take the moduli to be $q = ?$, a prime of degree 2. We choose a prime

$\mathfrak{q}$ above q and denote by $\bar{v}$ the image of v in $R/\mathfrak{q}$. We use $\mathbb{F}_q$ to denote the prime subfield of $R/\mathfrak{q}$. It turns out that $\bar{v}_i \in \mathbb{F}_q$ for $1 \leq i \leq ?$.

We then generate ? sample errors $e_j \leftarrow D_{\mathcal{R}}$ and consider their image $\bar{e}_j$ in $R/\mathfrak{q}$. A subfield test (defined in chisquare) gives the p-value .... Since this is smaller than q^2, we could solve SRLWE$(\mathcal{R}, \mathfrak{q})$ with probability.

6. ATTACKING PRIME CYCLOTOMIC FIELDS WHEN THE MODULUS IS THE RAMIFIED PRIME

Let p be an odd prime and $K = \mathbb{Q}(\zeta_p)$. Then K has degree $(p-1)$ and discriminant p^{p-2}. In addition, the prime p is totally ramified in K. Let $\mathfrak{p}$ be the unique prime ideal in R lying above p. The root determinant of the embedded lattice $\tilde{\iota}(R)$ is $p^{\frac{p-2}{2(p-1)}}$.

For the sake of simplicity of our analysis, we choose a different error distribution for our RLWE problem, which is introduced by [DD12]. Consider the elements $v_i = \zeta_p^i$ of R. Note that the first $v_0, \cdots, v_{p-2}$ form a basis for R, and we have the relation $v_{p-1} = -\sum_{i=0}^{p-2}(v_i)$. Sampling from the [DD12] error distribution, which we denote by $DD_{p,\sigma}$, consists of three steps: first, we generate a vector $(g_0, \cdots, g_{p-1})$, where g_i are i.i.d. random variables under the continuous Gaussian distribution $N(0, \sigma^2)$. Then we form the sum $\sum g_i \zeta_p^i$ and use the relation to rewrite it as $\sum_{i=0}^{p-2}(g_i - g_{p-1})\zeta_p^i$. Finally, we take the nearest integer of each coordinates and the error is

$$e = \sum_{i=0}^{p-2}[g_i - g_{p-1}]\zeta_p^i.$$

The authors of [DD12] describe the relation between standard deviation parameters in their sampling and the one in RLWE. Their Lemma roughly says that $DD(p,\sigma)$ is a close approximation to $D_{\bar{\iota}(\mathbb{Z}[\zeta_p]),\sqrt{p}\sigma}$.

Under some mild assumptions, we will show that $e \pmod{\mathfrak{p}}$ takes on a proper subset of $\mathbb{F}_p$. First, let $\{g\} = g - [g]$ denote the distance from a real number g to its nearest integer.

Assumption Suppose $g \leftarrow N(0, \sigma^2)$, we assume that $\{g\}$ is distributed uniformly in $[-1/2, 1/2]$. Note that this assumption is reasonable as long as σ is not too small, e.g., $\sigma > 10$ will do.

Then we prove

Proposition 6.1. *Suppose $\sigma > 10$ and $e \leftarrow DD_{p,\sigma}$. Then for all $w > \sqrt{p\sigma^2 + 4(p-1)/3}$, we have*

$$\mathrm{Prob}(|e \pmod{\mathfrak{p}}| > w) < 2 - 2\Phi^{-1}(w).$$

Proof.

$$e \pmod{\mathfrak{p}} = \sum_{i=0}^{p-2} g_i - (p-1)g_{p-1} - \sum_{i=0}^{p-2}\{g_i - g_{p-1}\}$$
$$= \sum_{i=0}^{p-1} g_i - \sum_{i=0}^{p-2}\{g_i - g_{p-1}\}$$

By definition of the g_i, we have $\sum_{i=0}^{p-1} g_i \sim N(0, p\sigma^2)$. By our assumption, $\{g_i - g_{p-1}\} \sim U(-1/2, 1/2)$ for each index i, with variance $4/3$. By the central limit theorem, when p is large enough the distribution of $\sum_{i=0}^{p-2}\{g_i - g_{p-1}\}$ is approximated by $N(0, 4(p-1)/3)$. It can be checked that these two random variables are independent (fixme: add the proof). Hence $e \pmod{\mathfrak{p}}$ can be well approximated by $N(0, \sigma')$, where $\sigma' = p\sigma^2 + 4(p-1)/3$. The claim now follows. $\square$

Corollary 6.2. *If p is a sufficiently large prime and $\sigma = o(\sqrt{p})$, then the [ELOS] attack works on the RLWE instance $\mathbb{Q}(\zeta_p)$ with modulus p and the error distribution $DD(p,\sigma)$.*

Proof. The attack in [ELOS] is guaranteed to work provided

$$\frac{p}{|e \pmod{\mathfrak{p}}|} > 2,$$

with overwhelming probability. Assuming $\sigma = o(\sqrt{p})$, then by Proposition 6.1 (take $w = 20$, for example, so that the right hand side is negligibly small), we have $\frac{p}{|e \pmod{\mathfrak{p}}|} \to \infty$ when $p \to \infty$. This completes the proof. $\square$

Example 6.3. Let $p = 1001$. We attack $K = \mathbb{Q}(\zeta_p)$ with modulus p, with $\sigma = 5$. We randomly generate 10 secrets from R_q.

The decision RLWE problem was solved for all 10 instances, the number of samples being used to distinguish is, and the average runtime of the attack is.

Lemma 6.4.
(1) $A_v^t A_v = pI_{p-1} - \mathbf{1}\mathbf{1}^t$.
(2) For all $x \in \mathbb{R}^n$, $||x||_2 \leq ||A_v x||_2 \leq p||x||_2$.
(3) For all $x \in \mathbb{R}^n$, $||y||_2 \leq ||A_v x||_2 \leq p||x||_2$. (3) $A_v^t \cdot \mathbf{1} = \mathbf{1}$.
(4) $(A_v^{-1})^t \cdot \mathbf{1} = \mathbf{1}$.

Proof. Each part is the direct consequence of the previous one. Thus we only need to prove (1), for which we refer to [DD12]. $\square$

Now suppose an error vector e is sampled from the error distribution: $e \leftarrow D_{\Lambda,\sigma}$. Let e' be the coefficent vector of e under the basis v: thus $e' = A_v^{-1}(e)$. Let $\mathbf{1} = (1, 1, \cdots, 1)$ denote the n-dimensional vector of ones. Then

Lemma 6.5.
$$e \pmod{\mathfrak{p}} = -\langle (T^{-1})^t \mathbf{1}, e \rangle.$$

Proof. We have

$$\begin{aligned}
e \pmod{\mathfrak{p}} &= (\mathbf{1}, e') \\
&= (\mathbf{1}, \tilde{A}_v^{-1} e) \\
&= ((\tilde{A}_v^{-1})^t \mathbf{1}, e) \\
&= ((T^{-1})^t (A_v^{-1})^t \mathbf{1}, e). \\
&= -\langle (T^{-1})^t \mathbf{1}, e \rangle.
\end{aligned}$$

$\square$

We quote one lemma on discrete Gaussian distribution on lattices, which is a combination of two lemmas from [LS14]. Lemma 8 and Lemma 2.2 from LPR.

Lemma 6.6. *For any n-dimensional lattice $\Lambda \subseteq \mathbb{R}^n$, $\epsilon \in (0, 1)$, we have*
$$\eta_\epsilon(\Lambda) \leq \sqrt{\ln(n)/\epsilon} \lambda_n(\Lambda).$$

Suppose $t \geq \sqrt{2\pi}$, $u \in \mathbb{R}^n$ and $\sigma \geq \eta_\epsilon(\Lambda)/\sqrt{2\pi}$. Then
$$Prob_{x \leftarrow D_{\Lambda,\sigma}}(|x \cdot u| \geq \sqrt{2\pi}\sigma t) \leq \frac{1 + \epsilon}{1 - \epsilon} t \sqrt{2\pi e} e^{-\pi t^2}.$$

Lemma 6.7. *Let $\Lambda = \tilde{\iota}(\mathbb{Z}[\zeta_p])$. Then $\lambda_n(\Lambda) \leq \sqrt{p-1}$.*

Proof. This follows directly from the fact that $||\iota(\zeta_p^i)||_2 = \sqrt{p-1}$ for all $i \in \mathbb{Z}$ and that the transformation matrix T between ι and $\tilde{\iota}$ is Hermitian. $\square$

We now specialize Lemma 6.6 to

Proposition 6.8. *Let p be a prime and Λ. Then for all $\sigma > \frac{\sqrt{p-1}\ln(2p-2)}{\sqrt{2\pi}}$, we have*

$u = \mathbf{1}$, $\epsilon = 1/2$, $\sigma = \sigma_0 p^{\frac{p-2}{2(p-1)}}$ and $t = 6$. When $\sigma_0 >$, the inequality involving the smoothing parameter is satisfied, and we obtain

Now we are ready to prove the validity of attack.

Theorem 6.9. *Let p be a prime and let $\mathcal{R}$ be the RLWE instance $\mathcal{R} = (\mathbb{Q}(\zeta_p), p, \sigma, s)$. Assume $\sigma = o(\sqrt{p})$. Let $\mathfrak{p}$ denote the unique prime ideal in $\mathbb{Q}(\zeta_p)$ above p. Then there is an $O(p)$ algorithm that solves $SRLWE(\mathcal{R}, \mathfrak{p})$.*

Proof. Using **??**, we may assume that for all $e \to D(\mathcal{R}, \mathfrak{p})$, we have $|e| \leq 6\sqrt{2(p-1)\pi}\sigma$. Using the fact that $\sigma = o(p)$, we see that $|e \pmod{\mathfrak{p}}| = o(p)$. Hence the reduced error distribution only takes value in the subset $|e| \leq 6\sqrt{2(p-1)\pi}\sigma$. When $p \to \infty$, we have $|e \pmod{\mathfrak{p}}| = o(p)$. Hence the attack in [ELOS] works. $\square$

6.1. **Can modulus switching be used?**
Modulus switching, as a technique to reduce absolute noise in homomorphic encryption, has been discussed exetnsively in [BGV12] and [LS14]. Given the previous discusssions, it is a natural question whether modulus switching could be used on RLWE instances for prime cyclotomic fields, to move from a split prime to the ramified prime and perform the attack. However, the naive approach of this combination would not work, as demonstrated by the following argument. We let p denote the modulus we are switching to.

After the modulus switching, we have

$$\begin{aligned}
e' &= b' - a's \\
&= \alpha(b - as) - b'' + a''s. \\
&= \alpha e + \lambda p - b'' + a''s.
\end{aligned}$$

Now suppose $\mathfrak{q}$ is a prime in K above q.

It is thus an interesting problem to combine modulus switching with our attack.

7. INVULNERABILITY OF GENERAL CYCLOTOMIC EXTENSIONS FOR UNRAMIFIED PRIMES

7.1. **Introduction.** Let $m \geq 1$ be any integer and let $K = \mathbb{Q}(\zeta_m)$. Let q be a prime and assume that q is unramified in K, and let $\mathfrak{q}$ be a prime ideal above q. We show that under some simplifying assumptions, the image of a reduced RLWE error distribution $D_{\mathcal{R},\mathfrak{q}}$ will be indistinguishable from the uniform distribution $U(\mathbb{F}_q)$. The tool we use is Fourier analysis on finite fields.

First, we introduce a class of distributions indexed by even integers $k \geq 2$, aiming at approximating discrete Gaussians over $\mathbb{Z}$.

Definition 7.1. For any even integer $k \geq 2$, let $\mathcal{V}_k$ denote the distribution over $\mathbb{Z}$ such that

$$\text{Prob}(\mathcal{V}_k = m) = \begin{cases} \frac{\binom{k}{m+\frac{k}{2}}}{2^k} & \text{if } |m| \leq \frac{k}{2} \\ 0 & \text{otherwise} \end{cases}$$

The integer k in the definition plays the role of the standard deviation σ for discrete Gaussians. When $q > k$, we abuse notations and also use $\mathcal{V}_k : \mathbb{F}_q \to \mathbb{R}$ denote the probability density function of the distribution $\mathcal{V}_k \pmod{q}$ over $\mathbb{F}_q$ defined by the same formula.
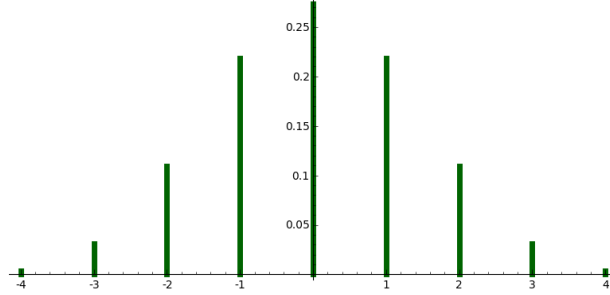

FIGURE 7.1. Probability density function of $\mathcal{V}_8$

Definition 7.2 (Modified error distribtuion $MD_{\mathcal{R}}$). Let $k \geq 2$ be an even integer. Then a sample from the modified error distribtuion $MD_{m,q,k}$ is

$$e = \sum_{i=0}^{n-1} e_i \zeta_m^i \pmod{qR},$$

where the coefficients e_i are sampled independently from $\mathcal{V}_k$.

Assumption Keeping the above notations, set

$$\sigma = \frac{k}{\sqrt{2\pi}},$$

and let $\mathcal{R} = (K, q, \sigma, s)$. We assume that the distribtutions $MD_{m,q,k}$ are $D_{\mathcal{R}}$ are "close modulo $\mathfrak{q}$", in the sense that the two distributions $MD_{m,q,k} \pmod{\mathfrak{q}}$ and $D_{\mathcal{R},\mathfrak{q}}$ are indistinguishable, for every choice of $\mathfrak{q}$.

Granting the above assumption, we will analyze the distance between $MD_{m,q,k} \pmod{\mathfrak{q}}$ and the uniform distribution over $R/\mathfrak{q}$.

7.2. **Fourier analysis.** We recall the definition and key properties of Fourier transform over finite fields. Suppose f is a real-valued function on $\mathbb{F}_q$. The *Fourier transform* of f is defined as

$$\hat{f}(y) = \sum_{a \in \mathbb{F}_q} f(a) \bar{\chi}_y(a),$$

where

$$\chi_y(a) := e^{2\pi i a y/q}.$$

Let u denote the probability density function of the uniform distribution over $\mathbb{F}_q$: $u(a) = \frac{1}{q}$ for all $a \in \mathbb{F}_q$, and let δ denote the characteristic function of the one-point set $\{0\} \subseteq \mathbb{F}_q$. Recall that the convolution of two functions f, g is

$$f * g(a) = \sum_{b \in \mathbb{F}_q} f(a - b)g(b)$$

Fact 7.3 (Properties of Fourier transform)**.**

(1) $\hat{\delta} = qu$.

(2) $\hat{u} = \delta$.

(3) $\widehat{f * g} = \hat{f} \cdot \hat{g}$.

(4) *the inversion formula:*

$$f(a) = \frac{1}{q} \sum_{y \in \mathbb{F}_q} \hat{f}(y)\chi_y(a).$$

Now suppose f, g are the probability density functions of two random variables F, G with value in $\mathbb{F}_q$.

Lemma 7.4. *Let h denote the density function of the sum $H = F + G$. Suppose the random variables F, G are independent, then*

$$h = f * g.$$

In general, suppose $F_1, \cdots, F_n$ are mutually independent random variables in $\mathbb{F}_q$, with density functions $f_1, \cdots, f_n$. Let f denote the density function of the sum $F = \sum F_i$, then

$$f = f_1 * \cdots * f_n.$$

Proof. We prove the two-variable case. For any $a \in \mathbb{F}_q$,

$$Prob(F + G = a) = \sum_{b \in \mathbb{F}_q} Prob(F = a - b, G = b)$$

$$= \sum_{b \in \mathbb{F}_q} Prob(F = a - b)Prob(G = b). \qquad \text{(since } F, G \text{ are independent)}$$

$$= (f * g)(a).$$

The general case follows by an induction on n. $\qquad\qquad\square$

Lemma 7.5. *For all even integers $k \geq 2$, $\hat{\mathcal{V}}_k(y) = \cos\left(\frac{\pi y}{q}\right)^k$.*

Proof. The proof is simply unwinding all the definitions. We have

$$2^k \cdot \hat{\mathcal{V}}_k(y) = \sum_{m=-\frac{k}{2}}^{\frac{k}{2}} \binom{k}{m + \frac{k}{2}} e^{2\pi i y m/q}$$

$$= e^{-\pi i y k/q} \sum_{m=-\frac{k}{2}}^{\frac{k}{2}} \binom{k}{m + \frac{k}{2}} e^{2\pi i y (m+k/2)/q}$$

$$= e^{-\pi i y k/q} \sum_{m'=0}^{k} \binom{k}{m'} e^{2\pi i y m'/q}$$

$$= e^{-\pi i y k/q} (1 + e^{2\pi i y/q})^k$$

$$= (e^{-\pi i y/q} + e^{\pi i y/q})^k$$

$$= (2 \cos(\pi y/q))^k.$$

Dividing both sides by 2^k gives the result. $\qquad\qquad\square$

Now we come back to the error distribution $MD(m, q, k) \pmod{\mathfrak{q}}$. There is a one-to-one correspondence between primitive m-th roots of unity in $\mathbb{F}_q$ and the prime ideals above q in $\mathbb{Q}(\zeta_m)$. Let α be the root corresponding to our choice of $\mathfrak{q}$. Then sample from $MD(m, q, k) \pmod{\mathfrak{q}}$ is $E = \sum_{i=0}^{n-1} \alpha^i E_i \pmod{q}$,

where the E_i are independent variables under the distribution $\mathcal{V}_k$. Let e denote its probability density function. The following lemma is crucial to our analysis:

Lemma 7.6.

$$\widehat{e}(y) = \prod_{i=1}^{n} \cos\left(\frac{\alpha^i \pi y}{q}\right)^k.$$

Proof. This follows directly from Lemma 7.5 and Lemma 7.3. ☐

Now we are able to bound the difference $e(a) - 1/q$ using the Fourier inversion formula.

Theorem 7.7. *For all $a \in \mathbb{F}_q$,*

(7.1)
$$|e(a) - 1/q| \leq \frac{1}{q} \sum_{y \in \mathbb{F}_q, y \neq 0} |\hat{e}(y)|.$$

Proof.

$$e(a) - 1/q = e(a) - u(a)$$
$$= \frac{1}{q} \sum_{y \in \mathbb{F}_q} (\hat{e}(y) - \hat{u}(y))\chi_y(a)$$
$$= \frac{1}{q} \sum_{y \in \mathbb{F}_q} (\hat{e}(y) - \delta(y))\chi_y(a)$$
$$= \frac{1}{q} \sum_{y \in \mathbb{F}_q, y \neq 0} \hat{e}(y)\chi_y(a). \qquad (\text{since } \hat{e}(0) = 1)$$

Now the theorem follows by taking from that $|\chi_y(a)| \leq 1$ for all a, y. ☐

Corollary 7.8. *The statistical distance between e and u satisfies*

$$d(e, u) \leq \frac{1}{2} \sum_{y \in \mathbb{F}_q, y \neq 0} |\hat{e}(y)|.$$

Let $\epsilon(m, q, k, \alpha)$ denote the right hand side of (7.1), i.e.,

$$\epsilon(m, q, k, \alpha) = \frac{1}{q} \sum_{y \in \mathbb{F}_q, y \neq 0} \prod_{i=0}^{n-1} \cos\left(\frac{\alpha^i \pi y}{q}\right)^k.$$

We let α run through all primitive m-th root of unities in $\mathbb{F}_q$ and define

$$\epsilon(m, q, k) := \max\{\epsilon(m, q, k, \alpha) : \alpha \text{ has order } m \text{ in } \mathbb{F}_q\}.$$

The punchline of our argument is: the value $\epsilon(m, q, k)$ is usually negligibly small. As a result, the distribution $MD(m, q, k) \pmod{\mathfrak{q}}$ is computationally indistinguishable from the uniform distribution for all $\mathfrak{q}$. The following is a table of data to illustrate this phenomenon.

TABLE 7.1. Values of $\epsilon(m, q, k)$

m	q	$-\lceil \log_2(\epsilon(m, q, 2)) \rceil$
244	1709	230
101	1213	177
256	3329	194
256	14081	208
55	10891	44
197	3547	337
96	4513	35
160	20641	61
145	19163	176
512	10753	431
512	19457	414

Remark 7.9. It is possible to generalize this cryptoanalysis to higher degree primes, where the Fourier analysis is performed in extension fields $\mathbb{F}_{q^f}$. The only change in the definition would be $\chi_y(a) = e^{\frac{2\pi i Tr(a_i y)}{q}}$, and we will have

$$\widehat{e}(y) = \prod_{i=1}^{n} \cos\left(\frac{\pi Tr(\alpha^i y)}{q}\right)^k.$$

Then a similar analysis goes through. We have made a table for primes of degree two.

TABLE 7.2. Values of $\epsilon(m, q, 2)$ for primes of degree 2

m	q	$-[\log_2(\epsilon(m, q, 2))]$
53	211	61
55	109	48
63	881	33
64	383	31
512	257	263

Remark 7.10. There is a heuristic argument on why one expects $\epsilon(m, q, k, \alpha)$ to be small. Each term in the summand is a product of cosines of form $\prod_{i=0}^{n-1} \cos\left(\frac{\alpha^i \pi y}{q}\right)^k$. For each $0 \neq y \in \mathbb{F}_q$, Since the elements α^i are distinct and usually spaced-out in $\mathbb{F}_q$, it is very likely that $\alpha^i y$ is close $q/2$ for some values of i, making the corresponding cosine value small.

8. CONCLUSION AND OPEN PROBLEMS

REFERENCES

[BGV12] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan, *(leveled) fully homomorphic encryption without boot-strapping*, Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, ACM, 2012, pp. 309–325.

[DD12] Léo Ducas and Alain Durmus, *Ring-lwe in polynomial rings*, Public Key Cryptography–PKC 2012, Springer, 2012, pp. 34–51.

[EHL14] Kirsten Eisenträger, Sean Hallgren, and Kristin Lauter, *Weak instances of plwe*, Selected Areas in Cryptography–SAC 2014, Springer, 2014, pp. 183–194.

[Joh11] HENRI Johnston, *Notes on galois modules*, Notes accompanying the course Galois Modules given in Cambridge in (2011).

[LPR13] Vadim Lyubashevsky, Chris Peikert, and Oded Regev, *On ideal lattices and learning with errors over rings*, Journal of the ACM (JACM) **60** (2013), no. 6, 43.

[LS14] Adeline Langlois and Damien Stehlé, *Worst-case to average-case reductions for module lattices*, Designs, Codes and Cryptography **75** (2014), no. 3, 565–599.