

ATTACKS ON SEARCH-RLWE

HAO CHEN, KRISTIN LAUTER, KATHERINE E. STANGE

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

1. INTRODUCTION

The Ring learning with errors (RLWE) problem, proposed in [LPR13a], 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 [LPR13a] 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 [LPR13a], 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 $\pi : R \rightarrow \mathbb{F}_q$, and works when the image of the RLWE error distribution under the map π only takes value in a strictly 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 [LPR13a], which we denote by $\text{SRLWE}(\mathcal{R}, q)$ (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 *residual 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 residual 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 $\sigma_1, \dots, \sigma_n$ be the embeddings of K into \mathbb{C} , the field of complex numbers. The *canonical embedding* of K is

$$\begin{aligned} \iota : K &\rightarrow \mathbb{C}^n \\ x &\mapsto (\sigma_1(x), \dots, \sigma_n(x)). \end{aligned}$$

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 $\sigma_1, \dots, \sigma_{r_1}$ 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

$$\begin{aligned} \tilde{\iota} : K &\rightarrow \mathbb{R}^n \\ x &\mapsto (\sigma_1(x), \dots, \sigma_{r_1}(x), \operatorname{Re}(\sigma_{r_1+1}(x)), \operatorname{Im}(\sigma_{r_1+1}(x)), \dots, \operatorname{Re}(\sigma_{r_1+r_2}(x)), \operatorname{Im}(\sigma_{r_1+r_2}(x))) \end{aligned}$$

It turns out that $\tilde{\iota}(R)$ is a lattice in \mathbb{R}^n . Let $w = (w_1, \dots, w_n)$ 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 $\iota(w_i)$ (resp. $\tilde{\iota}(w_i)$).

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 $\rho_\sigma : \mathbb{R}^n \rightarrow [0, 1]$ as $\rho_\sigma(x) = e^{-\|x\|^2/2\sigma^2}$ (our σ is equal to $r/\sqrt{2\pi}$ for the parameter r in [LPR13a]).

Definition 2.2. For a lattice $\Lambda \subset \mathbb{R}^n$ 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 distribution

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

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

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

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

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

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

We use the shorthand notation $(a, b) \leftarrow \mathcal{R}$ to represent that (a, b) is sampled from the RLWE dsitribution of \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 $\text{SRLWE}(\mathcal{R})$, 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 $\text{DRLWE}(\mathcal{R})$, 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 $R_q \times R_q$.

2.2. Sampling methods. There exist different ways to approximately sample from the RLWE error distribution $D_{\mathcal{R}}$, and we will switch between three sampling methods in our paper. While searching for weak Galois RLWE instances, we use the sampling algorithm in [GPV08]; when analyzing the security of cyclotomics, we defined a modified error distribution $MD_{m,q,k}$ (see Definition 7.2); when proving the vulnerability of prime cyclotomics at the ramified prime, we used the PLWE sampling method, which samples each coefficient of the error polynomial independently from a discrete Gaussian over the integers. We mention that [LPR13b] has an efficient algorithm for cyclotomic fields. Since it is primarily related to the dual version of RLWE, we will not use it in our paper.

3. SEARCH-TO-DECISION REDUCTION

The main result of this section (Corollary 3.6) is a reduction from SRLWE to DRLWE for Galois fields K and unramified primes q . We will prove the reduction from SRLWE to an intermediate problem which we denote by $\text{SRLWE}(\mathcal{R}, \mathfrak{q})$ (it is denoted by \mathfrak{q}_i -LWE in [LPR13a]). This result can be viewed as a generalization of [EHL14, Theorem 2] to primes of higher degree. Since our attack in Section ?? is targeting at $\text{SRLWE}(\mathcal{R}, \mathfrak{q})$, we could attack SRLWE for any Galois RLWE instances vulnerable to our attack.

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 $\text{SRLWE}(\mathcal{R}, \mathfrak{q})$ is: given access to arbitrarily many independent samples $(a, b) \leftarrow \mathcal{R}$, find $s \pmod{\mathfrak{q}}$.

We recall some algebraic number theoretical facts in the following lemma.

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 $\mathfrak{q}_1, \dots, \mathfrak{q}_g$ of R such that*

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

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

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

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

(fixme: move this) $D_{\mathcal{R}, \mathfrak{q}}$ to denote the reduced error distribution $D_{\mathcal{R}} \pmod{\mathfrak{q}}$.

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 residual degree f . Suppose there is an algorithm \mathcal{A} which solves $\text{SRLWE}(\mathcal{R}, \mathfrak{q})$ using a list S of samples. Assume that the running time of the algorithm \mathcal{A} is t . Then the problem $\text{SRLWE}(\mathcal{R})$ can be solved in time $T = \frac{n}{f}t$ using the samples in S .*

Proof. The Galois group $G = \text{Gal}(K/\mathbb{Q})$ acts on the set $\{\mathfrak{q}_1, \dots, \mathfrak{q}_g\}$ transitively. Hence for each i , we can take $\sigma \in \text{Gal}(K/\mathbb{Q})$, such that $\sigma_i(\mathfrak{q}) = \mathfrak{q}_i$. Then we run the algorithm \mathcal{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. \square

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

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 cyclotomic fields with normal integral bases, the Galois automorphisms are simply permutations of coordinates, so the time needed to apply these automorphisms is trivial.

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

Lemma 3.5. *There is a probabilistic polynomial time reduction from $\text{SRLWE}(\mathcal{R}, \mathfrak{q})$ to $\text{DRLWE}(\mathcal{R})$.*

Proof. This is a rephrasing of [LPR13a, Lemma 5.9 and Lemma 5.12]. \square

Corollary 3.6. *Suppose \mathcal{R} is an RLWE instance where K is Galois and q is an unramified prime in K . Then there is a probabilistic polynomial-time reduction from $\text{SRLWE}(\mathcal{R})$ to $\text{DRLWE}(\mathcal{R})$.*

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 $S = \bigsqcup_{j=1}^r S_j$. Suppose there are M samples $y_1, \dots, y_M \in S$. 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., $t_j := |\{1 \leq i \leq M : y_i \in S_j\}|$. 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 distribution, 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 $N(d, 2d)$.

If P, Q are two probability distributions on the set 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 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 . The basic idea of 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 loops through all q^f possibilities of $\bar{s} = s \pmod{\mathfrak{q}}$, and 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 distribution in $(R_q)^2$, 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 test on the errors \bar{e}' to reject the null hypothesis.

Let $N = q^f$ denote the cardinality of F . 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 be rejected. For example, we may choose the confidence level to be $\alpha = 1 - \frac{1}{10N}$. The detailed attack is described in Algorithm 4.2. Note that the time complexity of the attack is $O(N)$ since there are N possible values for $s \pmod{\mathfrak{q}}$. The number of samples need for the attack is also $O(N)$.

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 ; B – the number of bins ($B \leq |F|$); \mathcal{S} – a collection of M ($M = \Omega(|F|)$) RLWE samples from \mathcal{R} .

Ensure: a guess of the value $s \pmod{\mathfrak{q}}$, or **NON-RLWE**, or **INSUFFICIENT-SAMPLES**

```

1:  $\omega \leftarrow \Phi^{-1}(1 - \frac{1}{20N})$ ,  $\mathcal{G} \leftarrow \emptyset$ 
2: for  $s$  in  $F$  do
3:    $\mathcal{E} \leftarrow \emptyset$ .
4:   for  $a, b$  in  $\mathcal{S}$  do
5:      $\bar{a}, \bar{b} \leftarrow a \pmod{\mathfrak{q}}, b \pmod{\mathfrak{q}}$ .
6:      $\bar{e} \leftarrow \bar{b} - \bar{a}s$ .
7:     add  $\bar{e}$  to  $\mathcal{E}$ .
8:   end for
9:   Run  $\chi^2$  test on the set  $\mathcal{E}$  and  $B$  bins to obtain the value  $\chi^2(\mathcal{E})$ .
10:  if  $|\chi^2(\mathcal{E}) - (B - 1)| > \omega\sqrt{2B - 2}$  then
11:    add  $s$  to  $\mathcal{G}$ .
12:  end if
13: end for
14: if  $G = \emptyset$  then
15:   return NOT RLWE
16: else if  $G = \{g\}$  then
17:   return  $g$ 
18: elsereturn INSUFFICIENT-SAMPLES
19: end if
```

The correctness of the attack is captured in Theorem 4.1. We use $D_{\mathcal{R}, \mathfrak{q}}$ as a shorthand notation for $D_{\mathcal{R}} \pmod{\mathfrak{q}}$. Let Φ denote the cumulative distribution function of the standard Gaussian distribution.

Theorem 4.1. *Let Δ denote the statistical distance between the distribution $D_{\mathcal{R}, \mathfrak{q}}$ and the uniform distribution on R/\mathfrak{q} . Let $\lambda = 4M\Delta^2$ and $\omega = \Phi^{-1}(1 - \frac{1}{20N})$. Finally, let p denote the probability of success of the attack in Algorithm 4.2. When $q \gg 1$, we have*

$$p \geq 0.904 \left(1 - \Phi \left(\frac{\omega \sqrt{2(N-1)} - \lambda}{\sqrt{2(N-1) + 4\lambda}} \right) \right).$$

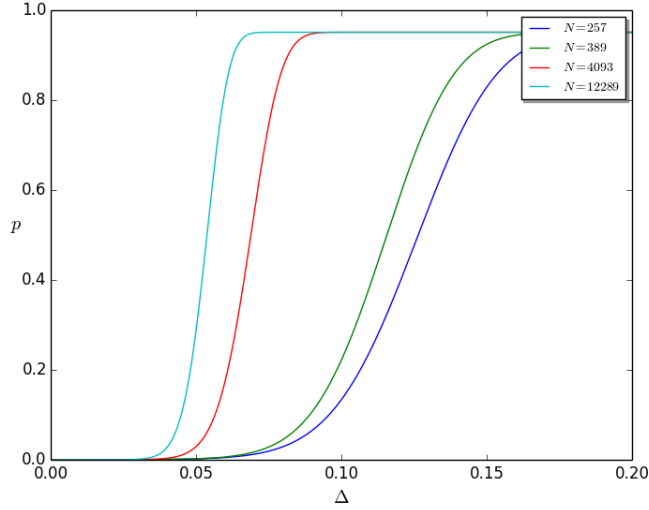
Proof. The chi-square value for uniformity on samples from $D_{\mathcal{R}, \mathfrak{q}}$ follow a noncentral chi-square distribution with the same degree of freedom and a parameter λ_0 given by

$$\lambda_0 = MN d_2(D_{\mathcal{R}, \mathfrak{q}}, U(R/\mathfrak{q}))^2.$$

In particular, we have $\lambda_0 \geq 4M\Delta^2 = \lambda$. Since $q \gg 1$, we may approximate a noncentral chi-square distribution with degree of freedom k and parameter λ_0 with a Gaussian distribution of mean $k + \lambda_0$ and variance $2k + 4\lambda_0$ (see [RSS04], for example). Recall that our attack succeeds if the set \mathcal{E} from all $(N-1)$ wrong guesses passes the test, and the true errors modulo \mathfrak{q} fail the test. The first event happens with probability $(1 - \frac{1}{10N})^{N-1} \geq e^{-1/10} = 0.904 \dots$. The second event has probability $1 - \Phi \left(\frac{\omega \sqrt{2(N-1)} - \lambda_0}{\sqrt{2(N-1) + 4\lambda_0}} \right)$, which is an increasing function in λ_0 . The theorem now follows. \square

Remark 4.2. One has the freedom to vary the choice of ω in the above algorithm and theorem based on the specific instance. The probability of success will change accordingly. When we expect the statistical distance Δ to be large, it is preferable to choose a larger ω to increase the probability of success.

The following is a plot of p versus Δ for various choices of N , made according to Theorem 4.1, where we fix the number of samples to be $M = 5N$.



5. VULNERABLE INSTANCES AMONG SUBFIELDS OF CYCLOTOMIC FIELDS

In our searching for vulnerable instances to our attack, we restrict our attention to subfields of cyclotomic fields $\mathbb{Q}(\zeta_m)$, where we assume m is *odd and squarefree*. The Galois group $\text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is canonically isomorphic to $G = (\mathbb{Z}/m\mathbb{Z})^*$. For each subgroup H of G , let $K_{m,H} = \mathbb{Q}(\zeta_m)^H$ be the subfield of elements fixed by H . Then the extension $K_{m,H}/\mathbb{Q}$ is Galois with 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 $w := (w_c)_{c \in C}$ is a \mathbb{Z} -basis of R . (For a proof of this fact, see [Joh11, Proposition 6.1]). Setting $\zeta = \exp(2\pi i/m)$, the canonical 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 the reduced error distribution $D_{\mathcal{R},q}$ is independent of the choice of prime ideal \mathfrak{q} above q .*

Proof. From the proof of Theorem ??, we know that the change from a prime \mathfrak{q} to \mathfrak{q}' can be done via applying an element of the galois group $\text{Gal}(K/\mathbb{Q})$ to the RLWE samples. On the other hand, the Galois group acts on the embedded lattice $\Lambda := \iota(R)$ by permuting the set of embeddings of K . Hence we have a group homomorphism

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

Since permutation matrices are orthogonal, the Galois group action on Λ given by ϕ is distance-preserving. In particular, it preserves any discrete Gaussian distribution on Λ . This completes the proof. \square

5.1. Searching. Algorithm 4.2 allows us to search for vulnerable instances among fields of form $K_{m,H}$ by generating actual RLWE samples and running the attack. Success of the attack will indicate vulnerability of the instance. Note that our field searching requires sampling efficiently from a discrete Gaussian $D_{\Lambda,\sigma}$, for which we use the efficient algorithm of [GPV08].

In Table 5.1, we list some instances on which the attack has succeeded. The columns of Table 5.1 are as follows. The first two columns specify m and the generators of H ; the column labeled f is the residual degree of q . The running time column consists of the time taken for running the actual attack, where if we first run the chi-square test on the correct error samples, and then a few chi-square tests on some random

guesses of $s \pmod{\mathfrak{q}}$. We then estimate the success rate and runtime for the actual attack from the data we obtained.

Note that we omitted our choice of prime ideal \mathfrak{q} , since due to Lemma 5.1 the choice of \mathfrak{q} is irrelevant to our attack.

TABLE 5.1. Attacked sub-cyclotomic RLWE instances

m	generators of H	n	q	f	σ_0	no. samples	runtime (in hours)
2805	[1684, 1618]	40	67	2	1	22445	3.49
15015	[12286, 2003, 11936]	60	43	2	1	11094	1.05
15015	[12286, 2003, 11936]	60	617	2	1.25	8000	228.41 (estimated) ¹
90321	[90320, 18514, 43405]	80	67	2	1	26934	4.81
255255	[97943, 162436, 253826, 248711, 44318]	90	2003	2	1.25	15000	1114.44 (est)
285285	[181156, 210926, 87361]	96	521	2	1.1	5000	75.41 (est)
1468005Z	[312016, 978671, 956572, 400366]	100	683	2	1.1	5000	276.01 (est)
1468005	[198892, 978671, 431521, 1083139]	144	139	2	1	4000	5.72

5.2. Discussion. One may notice that in all the vulnerable instances in Table 5.1, the prime q has degree $f = 2$. We explain the reason behind this phenomenon. Let K a Galois number field and suppose q is a prime of degree r in K . Suppose we have found a reduced basis w_1, \dots, w_n of R with respect to the adjusted embedding. Fix a prime ideal \mathfrak{q} above q . Then the images of the basis under the reduction modulo \mathfrak{q} map are elements of $F = R/\mathfrak{q}$. Now if for some index i , the element w_i lies inside some proper subfield K' of K , and if q has residual degree $r' < r$ in K' , then $w_i \pmod{\mathfrak{q}}$ will lie in a proper subfield of F . If the above situation happens for a large amount of the basis elements w_i , then we could expect the reduced error distribution $D_{\mathcal{R}, \mathfrak{q}}$ to take values in a proper subfield of F more frequently. This would allow us to distinguish it from the uniform distribution on F .

5.3. A detailed example. In order to illustrate our discussion above together with the search-to-decision reduction, we study a vulnerable Galois RLWE instance in detail, where we generated RLWE samples, performed the attack, and used search-to-decision reduction to recover the entire secret key s .

Let $m = 3003$ and H be the subgroup of $(\mathbb{Z}/m\mathbb{Z})^*$ generated by 2276, 2729 and 1123. Then $K = K_{m,H}$ is a Galois number field of degree $n = 30$. After a LLL lattice reduction on the canonical basis w , we obtained an basis v_1, \dots, v_n for the ring of integers R , ordered by increasing embedding length. We take the moduli to be $q = 131$, a prime of degree two in K . Finally, we take $\sigma_0 = 1$ and generate the secret s from the discrete Gaussian $D_{i,\sigma}$.

There are 15 prime ideals in K lying above q , which we denote by $\mathfrak{q}_1, \dots, \mathfrak{q}_{15}$. 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 $R/\mathfrak{q} \cong \mathbb{F}_q^2$. It turns out that $\bar{v}_i \in \mathbb{F}_q$ for $1 \leq i \leq 15$. We generated 1000 RLWE samples from \mathcal{R} and used Algorithm 4.2 and Theorem 3.3 to recover $s \pmod{\mathfrak{q}_i}$ for each $1 \leq j \leq 15$. The attack succeeded in 32.8 hours.

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 . There is a unique prime ideal $\mathfrak{p} = (1 - \zeta_p)$ above p , and the reduction map $\pi : R/pR \rightarrow \mathbb{F}_p$ satisfies

$$\pi(\zeta_p^i) = 1, \quad \forall i.$$

It is conceivable that this property would make $\pi(e)$ small in \mathbb{F}_q , thus making the instance vulnerable to our attack.

Example 6.1. 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.

¹The “estimated” runtime means that we did not perform the full attack. Instead, we ran several chi-square tests and estimate the runtime based on the average time for running one test.

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

6.1. Can modulus switching be used? Modulus switching, as a technique to reduce absolute noise in homomorphic encryption, has been discussed extensively in [BGV12] and [LS14]. We recap the basic ideas of modulus switching. Let $\mathcal{R} = (K, q, \sigma, s)$ be an RLWE instance. Choose $p < q$ as the new modulus and consider the instance $\mathcal{R}' = (K, p, \sigma', s)$ for some $\sigma' > \sigma$. The main operation of modulus switching is a map

$$\pi_{q,p} : R_q \rightarrow R_p,$$

which ideally takes RLWE samples w.r.t. \mathcal{R} to RLWE samples w.r.t. \mathcal{R}' . One example of such map being used in practice is as follows. Take a in R_q , we first scale and get $\frac{p}{q}a \in 1/qR$. Then we sample a vector a'' from the shifted discrete Gaussian $D_{\Lambda_R, \tau, \alpha a}$ for some small $\tau > 0$, and output $a' = \alpha a - a''$. Since we expect a'' to be a short vector, the point a' can be viewed as a “rounding” of the point αa to the lattice Λ_R . One also requires that $\pi_{q,p}$ takes uniform distribution on R_q to almost uniform distribution on R_p , which can be by taking τ to be reasonably large (see).

It is a natural question then to ask whether modulus switching can be combined with our attack, to switch from a “strong” modulus to a “weak” modulus. However, a heuristic argument shows that the naive combination of our attack with modulus switching will not work.

To explain, suppose we have a sample $(a, b) \leftarrow \mathcal{R}$ and the switched sample $(a', b') = (\pi_{q,p}(a), \pi_{q,p}(b))$. Consider the error $e' := b' - a's$ and the distribution of $e' \pmod{\mathfrak{p}}$ for some prime ideal \mathfrak{p} above p . Suppose $b = as + e + \lambda q$ for some $\lambda \in R$. Then

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

Since p and q are coprime, the domain of the reducing modulo \mathfrak{p} map can be extended from R to $\frac{1}{q}R$. Hence $e' \equiv -b'' + a''s \pmod{\mathfrak{p}}$. Also, since $a'' + a' = \alpha a \equiv 0 \pmod{\mathfrak{p}}$, we have $a'' \pmod{\mathfrak{p}} = -a' \pmod{\mathfrak{p}}$. By assumption, the map $\pi_{q,p}$ algorithm maps uniform samples in R_q to uniform samples in R_p . An immediate consequence is that $a' \pmod{\mathfrak{p}}$ is uniformly distributed in R/\mathfrak{p} , hence so is $a'' \pmod{\mathfrak{p}}$. The same argument applies to b'' . Since the reduced rounding errors $a'' \pmod{\mathfrak{p}}$ and $b'' \pmod{\mathfrak{p}}$ are independent, the new reduced errors $e' \pmod{\mathfrak{p}}$ follows the uniform distribution. So our chi-square attack will fail on these modulus-switched samples, even though p might be a “weak” modulus.

7. INVULNERABILITY OF GENERAL CYCLOTOMIC EXTENSIONS FOR UNRAMIFIED PRIMES

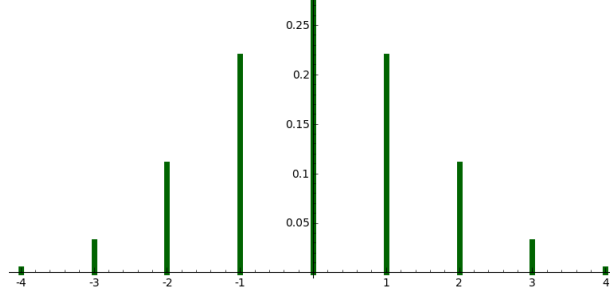
7.1. Introduction. Let $m \geq 1$ be any integer and let $K = \mathbb{Q}(\zeta_m)$. Let q be a prime and assume that q is unramified in K , and let \mathfrak{q} be a prime ideal above q . We show that under some simplifying assumptions, the image of a reduced RLWE error distribution $D_{\mathcal{R},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

First, we introduce a class of “shifted binomial distributions” indexed by even integers $k \geq 2$, aiming at approximating discrete Gaussians over \mathbb{Z} . Remark: this can be generalized to arbitrary real k , using extended binomial coefficients. (fixme)

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

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

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 $\mathcal{V}_k : \mathbb{F}_q \rightarrow \mathbb{R}$ 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 distribuion $MD_{m,q,k}$). Let $k \geq 2$ be an even integer. Then a sample from the modified error distribuion $MD_{m,q,k}$ is

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

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 distributions $MD_{m,q,k}$ 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

$$\widehat{f}(y) = \sum_{a \in \mathbb{F}_q} f(a) \chi_y(a),$$

where

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

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) $\widehat{\delta} = qu$.
- (2) $\widehat{u} = \delta$.
- (3) $\widehat{f * g} = \widehat{f} \cdot \widehat{g}$.
- (4) the inversion formula:

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

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

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

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

$$\begin{aligned} \text{Prob}(F + G = a) &= \sum_{b \in \mathbb{F}_q} \text{Prob}(F = a - b, G = b) \\ &= \sum_{b \in \mathbb{F}_q} \text{Prob}(F = a - b) \text{Prob}(G = b). \quad (\text{since } F, G \text{ are independent}) \\ &= (f * g)(a). \end{aligned}$$

The general case follows by an induction on n . □

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

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

$$\begin{aligned} 2^k \cdot \widehat{\mathcal{V}}_k(y) &= \sum_{m=-\frac{k}{2}}^{\frac{k}{2}} \binom{k}{m + \frac{k}{2}} e^{2\pi i y m / q} \\ &= e^{-\pi i y k / q} \sum_{m=-\frac{k}{2}}^{\frac{k}{2}} \binom{k}{m + \frac{k}{2}} e^{2\pi i y (m + k/2) / q} \\ &= e^{-\pi i y k / q} \sum_{m'=0}^k \binom{k}{m'} e^{2\pi i y m' / q} \\ &= e^{-\pi i y k / q} (1 + e^{2\pi i y / q})^k \\ &= (e^{-\pi i y / q} + e^{\pi i y / q})^k \\ &= (2 \cos(\pi y / q))^k. \end{aligned}$$

Dividing both sides by 2^k gives the result. □

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 a sample from $MD(m, q, k) \pmod{\mathfrak{q}}$ is

$$E_\alpha := \sum_{i=0}^{n-1} \alpha^i E_i \pmod{q},$$

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

Lemma 7.6.

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

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

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

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

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

Proof.

$$\begin{aligned}
e_\alpha(a) - 1/q &= e(a) - u(a) \\
&= \frac{1}{q} \sum_{y \in \mathbb{F}_q} (\widehat{e_\alpha}(y) - \widehat{u}(y)) \chi_y(a) \\
&= \frac{1}{q} \sum_{y \in \mathbb{F}_q} (\widehat{e_\alpha}(y) - \delta(y)) \chi_y(a) \\
&= \frac{1}{q} \sum_{y \in \mathbb{F}_q, y \neq 0} \widehat{e_\alpha}(y) \chi_y(a). \quad (\text{since } \widehat{e_\alpha}(0) = 1)
\end{aligned}$$

Now the theorem follows from taking absolute values on both sides, and noting that $|\chi_y(a)| \leq 1$ for all a and all y . \square

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

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

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. Since $\epsilon(m, q, k)$ is an upper bound of the distribution $MD(m, q, k) \pmod{q}$ is computationally indistinguishable from the uniform distribution for all 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

Now we address the issue whether our assumption makes sense. For a given σ , we can always find k such that $D_{\mathbb{Z}, \sigma} \pmod{q}$ and V_k differ at most by μ . Then

$$|\widehat{D} - \widehat{V}| \leq \mu.$$

So when we take the product,

$$\widehat{e}_0 = \prod D_i \leq \prod (V_i + \mu) = \prod V_i + \mu \prod_{j \neq i}$$

Remark 7.9. It is possible to generalize this cryptanalysis 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 $\chi_y(a) = e^{\frac{2\pi i \text{Tr}(a_i y)}{q}}$, and we will have

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

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	$-\lceil \log_2(\epsilon(m, q, 2)) \rceil$
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.

REFERENCES

- [BGV12] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan, *(leveled) fully homomorphic encryption without bootstrapping*, 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.
- [GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan, *Trapdoors for hard lattices and new cryptographic constructions*, Proceedings of the fortieth annual ACM symposium on Theory of computing, ACM, 2008, pp. 197–206.
- [Joh11] HENRI Johnston, *Notes on galois modules*, Notes accompanying the course Galois Modules given in Cambridge in (2011).
- [LPR13a] 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.
- [LPR13b] ———, *A toolkit for ring-lwe cryptography*, Advances in Cryptology–EUROCRYPT 2013, Springer, 2013, pp. 35–54.
- [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.
- [RSS04] B Ya Ryabko, VS Stognienko, and Yu I Shokin, *A new test for randomness and its application to some cryptographic problems*, Journal of statistical planning and inference **123** (2004), no. 2, 365–376.