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

2. Background

Let K be a number field of degree n with ring of integers $R = \mathcal{O}_K$ 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

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

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

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

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

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

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:

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

2.1. Ring LWE problems for general number fields.

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

Definition 2.4. Let $\mathcal{R} = (K, q, s)$ 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

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

Let n denote the degree of K, and let V denote the covolume of the lattice $\tilde{\imath}(R)$. As is pointed out by [ELOS], when analyzing the error distribution, one needs to take into account the sparsity of the lattice $\tilde{\imath}(R)$, 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 $R_q \times R_q$.

2.2. **Organization of this paper.** In section , we prove search-to-decision reduction for Galois extensions K and unramified primes of any degree. In section, we introduce the chi-square attack to SRLWE and DRLWE. In section, we give example instances of sub-cyclotomic fields (subfields of cyclotomic fields) which are vunlerable to our attack. The time complexity of our attack is $O(\frac{n}{f}q^{2f})$ for DRLWE (more precisely, an intermediate problem we denote by SRLWE($\mathcal{R}, \mathfrak{q}$)). Finally in section , under some simplifying assumptions, we show that cyclotomic extensions are invulnerable to our attack using Fourier analysis on finite fields.

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 [LPR]), 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 Algorithm are targeting at $SRLWE(\mathbb{R}, \mathfrak{q})$, we could attack SRLWE for any Galois RLWE instances we found vulnerable to Algorithm . We remark that a search-to-decision reduction theorem for higher degree primes can be proved by carrying out almost the exact same proof in [EHL14].

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 $s \pmod{\mathfrak{q}}$.

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 $R = \mathcal{O}_K$, 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. □

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, we, from an attacker's perspective, 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.

4. The chi-square attack for uniform distribution

We briefly recall the property and usage of the chi-square test for uniform distributions over a finite set S. Suppose M samples $y_1, \cdots, y_M \in S$. We partition S into r subsets

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

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

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

Note that degree of freedom in this test is $d = r - 1$. 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 *df* 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 $d(P, Q) \leq \frac{\sqrt{|S|}}{2} d_2(P, Q)$.

4.1. **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. 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-test attack of $SRLWE(\mathcal{R}, \mathfrak{q})$

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

$\alpha \leftarrow 1 - \frac{1}{10N}$.
$\omega \leftarrow \Phi^{-1}((1+\alpha)/2)$
$G = \emptyset$
for s in F **do**
  for a, b in S **do**
    $E \leftarrow \emptyset$.
    $\bar{a}, \bar{b} \leftarrow a \pmod{\mathfrak{q}}, b \pmod{\mathfrak{q}}$.
    $\bar{e} \leftarrow \bar{b} - \bar{a}s$.
    add e to E.
  end for
  Run χ^2 test on E and obtain the value $\chi^2(E)$.
  if $|\chi^2(E) - B - 1| > \omega\sqrt{2B-2}$ **then**
    add s to G
  end if
end for
if $G = \emptyset$ **then**
  return NOT RLWE
else if $G = \{g\}$ **then**
  return g
else
  return INSUFFIICNET-SAMPLES
end if

Note that the time complexity of the attack is $O(q^f)$ since we have q^f possible values for $s \pmod{\mathfrak{q}}$. 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 $D_{\mathcal{R},\mathfrak{q}} := D_{\mathcal{R}} \pmod{\mathfrak{q}}$ 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 chisquare 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. □

To get a sense of how the constants behave, we give a table containing some p values for various choices of N and Δ, computed using theorem. 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 $n = \frac{\varphi(m)}{|H|}$; a prime q splits completely in $K_{m,H}$ if and only if $q \pmod m \in H$. In general, the degree of a prime q in $K_{m,H}$ is equal to the order of $[q]$ in the quotient group G/H.

Every field of form $K_{m,H}$ comes with a 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 $c \in C$, set

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

Then we have

Proposition 5.1. *$w = (w_c)_{c\in C}$ is a $\mathbb{Z}$-basis of $R = \mathcal{O}_K$. Let $\zeta = \exp(2\pi i/m)$. Then the canonical embedding embedding matrix of w is*

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

Proposition 5.2. *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. □

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 $\mathfrak{q}$.

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	?	?	?

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 (Algorithm) on these samples. Success of the attack would indicate vulnerability. Our field search requires sampling efficiently from a discete Gaussian $D_{\Lambda,\sigma}$ for which we choose the method outlined in [GPV].

In the first table, we list some instances, for which the attack have succeeded. The columns are as follows. Note that we ommited the prime ideal $\mathfrak{q}$ due to Lemma . and t denotes the running time in seconds.

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

5.2. **another test.** 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 $R = \mathcal{O}_K$ 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. We demondstrate this phenomenon through the following example.

Example 5.3. 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.

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 $s \pmod{\mathfrak{q}}$. 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.

6. Attacking prime cyclotomic fields for the ramified prime

In this section, let p be an odd prime and $K = \mathbb{Q}(\zeta_p)$. First we deal with the case of sampling. A result of [DD] says that sampling from the Minkowski space of K with paremeter σ is the same as sampling a Discrete Gaussian from the quotient ring

$$\mathbb{Z}[x]/(x^p - 1)$$

with parameter $\sigma/\sqrt{p}$. We are going to take this point of view. The determinant factor is

$$Disc(K)^{\frac{1}{2[K:\mathbb{Q}]}} = p^{\frac{p-2}{2(p-1)}}.$$

Suppose we have chosen a base parameter σ_0. Then the adjustment $\sigma = \sigma_0/\sqrt{p} \cdot p^{\frac{p-2}{2(p-1)}} = \sigma_0 \cdot p^{\frac{-1}{2p-2}}$. Hence a general error term is

$$e = e_0 + e_1\zeta_p + \cdots + e_{p-1}\zeta_{p-1}$$

where $(e_i)_i$ are sampled from $D_{\mathbb{Z}^n,\sigma}$, and then reduced modulo p. Note that every ζ_p maps to 1 in $\mathbb{F}_p$. Hence we have

$$e(1) = e_0 + e_1 + \cdots + e_{p-1} \in \mathbb{F}_p.$$

Now we use the **independence** of the samples to conclude that $e_0 + e_1 + \cdots + e_{p-1} \sim D_{\mathbb{Z},\sqrt{p}\sigma}$, and assume that $|e(1)| \leq \sqrt{p}\sigma$.

Now for [ELOS] attack to work, we need

$$|e(1)| \leq p/4,$$

and we computed $p/|e(1)| \geq \sqrt{p}/\sigma_0$. So when p is not to small, this attack will work.

6.1. relationship between RLWE and PLWE.

Note that for the above analysis, we did not take the actual RLWE error distribution; instead, we generate the errors by sampling the coefficient of each basis vector independently from a discrete Gaussian integer distribution. This method of sampling is used in a related problem usually referred to as Poly-LWE (PLWE). The PLWE and RLWE error distributions are different. However, we will show that for our attack on ramified primes, they behave the same.

For the sake of simplicity, we consider the integral basis $v = (\zeta_p, \cdots, \zeta_p^{p-1})$. Let A_v and denote its canonical embedding matrix. We then prove that

Suppose an error vector e is sampled from the error distribution: $e \leftarrow D_{\Lambda,\sigma}$. Then the coefffificent vector of e is $e_c = A_v^{-1}(e)$. Let $\mathbf{1} = (1, 1, \cdots, 1)$ denote the n-dimensional vector of ones.

Lemma 6.1.
(1) $A_v = pI_{p-1} - 11^T$, (2) $A_v \cdot \mathbf{1} = \mathbf{1}$, (3) $A_v^{-1} \cdot \mathbf{1} = \mathbf{1}$.

Lemma 6.2.

$$e \pmod{\mathfrak{p}} = 1 \cdot e_c = \mathbf{1}A_v^{-1}e = \mathbf{1}^T e.$$

Proof. Clear. □

Now we are ready to prove the validity of our attack on the RLWE distribution.

Theorem 6.3. *Let p be a prime and $\mathcal{R}$ be the RLWE instance $\mathcal{R} = (\mathbb{Q}(\zeta_p), p, \sigma, s)$. Finally, let $\mathfrak{p}$ denote the unique prime ideal in $\mathbb{Q}(\zeta_p)$. Suppose $\sigma = o(\sqrt{p})$. Then there is an $O(p)$ algorithm that solves $SRLWE(\mathcal{R}, \mathfrak{p})$.*

Proof. Since $\zeta_p \equiv 1 \pmod{\mathfrak{p}}$, all elements in the basis v reduces to one in the finite field $R/\mathfrak{p}$. Hence, we run the attack [ELOS], and notice that

by [LaSt] We set $\epsilon = 1/2$ and $t = 8$ to get

$$Prob(|\mathbf{1} \cdot e| \geq 6\sqrt{2(p-1)\pi}\sigma) \leq averysmallnumber.$$

Hence we may safely assume $|e \pmod{\mathfrak{p}}| \leq 6\sqrt{2(p-1)\pi}\sigma$. Using the fact that $\sigma = o(p)$, we see that $|e \pmod{\mathfrak{p}}| = o(p)$. So when $p \gg 1$, we have $|e \pmod{\mathfrak{p}}| \ll p$, which makes the attack in [ELOS] work. □

6.2. **Can modulus switching be used?** Given the previous discusssions, it is a natural question whether modulus switching, as introduced in [BGV], [LaSt], 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 $\mathfrak{q}$

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 $K = \mathbb{Q}(\zeta_m)$. We will show that under a simplifying assumption, the image of a reduced RLWE error distribution $D_{\mathcal{R}} \pmod{\mathfrak{q}}$ for a prime $\mathfrak{q}$ above q, will be non-distinguishable 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 $\mathbb{Z}$. Here k plays the role of the standard deviation σ for discrete Gaussians.

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

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

When $q > k$, we abuse notations and let $\mathcal{V}_k : \mathbb{F}_q \to \mathbb{R}$ denote the probability density function of the distribution '$\mathcal{V}'_k$ over $\mathbb{F}_q$ defined by the same formula.

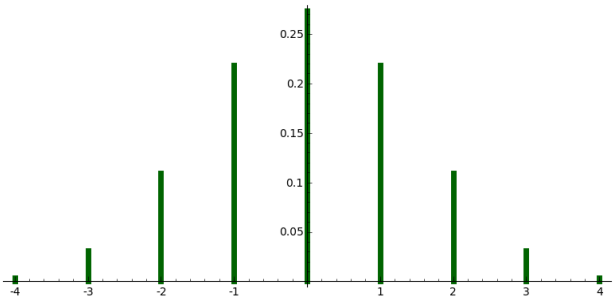

Figure 7.1. Probability density function of $\mathcal{V}_8$

Definition 7.2 (Modified error distribtuion)**.** Let $K = \mathbb{Q}(\zeta_m)$ with degree n ring of integers R. Let q be a prime and let $k \geq 2$ be an even integer. Then a sample from the distribtuion $PD_{m,q,k}$ is

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

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

Assumption Keeping the above notations, $\mathcal{R} = (K, q, \sigma, s)$ be an RLWE instance. We assume that the distribtutions $PD_{m,q,[\sqrt{2\pi}\sigma]}$ are $D_{\mathcal{R}}$ are "close modulo $\mathfrak{q}$", in the sense that the two distributions $PD_{m,q,[\sqrt{2\pi}\sigma]} \pmod{\mathfrak{q}}$ and $D_{\mathcal{R}} \pmod{\mathfrak{q}}$ are indistinguishable.

We will analyze the distance between $PD_{m,q,[\sqrt{2\pi}\sigma]} \pmod{\mathfrak{q}}$ 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

$$\hat{f}(s) = \sum_{a \in \mathbb{F}_q} f(a)\bar{\chi_s}(a),$$

where

$$\chi_s(a) := e^{2\pi i a s/q}$$

We have the inversion formula:

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

Let $\mathbf{1}$ denote the constant function $f \equiv 1$, and let δ denote the characteristic function of the one-point set $\{0\} \subseteq \mathbb{F}_q$.

Proposition 7.3.

(1) The transform of the δ function is $\hat{\delta} = \mathbf{1}$.
(2) The transform of $\mathbf{1}$ is $\hat{\mathbf{1}} = q\delta$; if U the uniform distribution over $\mathbb{F}_q$, then $\hat{U} = \delta$.
(3) convolution becomes product.

Lemma 7.4. *For all even integers $k \geq 2$,*

$$\hat{\mathcal{V}_k}(s) = \cos\left(\frac{\pi s}{q}\right)^k, (\forall s \in \mathbb{F}_q).$$

Proof. Routine calculation. □

Now we consider the error distribution we obtained from mapping RLWE errors to $\mathbb{F}_q$.

Definition 7.5. Suppose $\mathbf{a} = a_1, \cdots, a_n$ is a vector in $\mathbb{F}_q^n$. Define the following random variable with values in $\mathbb{F}_q$

$$e(\mathbf{a}, k, q) := \sum_{i=1}^{n} a_i e_i \pmod q$$

where the e_i are independent variables with distribution $\mathcal{V}_k$. Let E denote its probability density function: $E(b) = \text{Prob}(e = b)$ for $b \in \mathbb{F}_q$.

Next, using the fact that the probability of a sum of two varaibles is a convolution, we prove

Lemma 7.6.

$$\hat{E_{\mathbf{a},k,q}}(s) = \prod_{i=1}^{n} \cos\left(\frac{a_i \pi s}{q}\right)^k$$

In particular, $\hat{E}(0) = 1$ for all $\mathbf{a}$, k and q.

Proof. Routine calculation. □

Next we restrict our attention to cyclotomic fields. Let $m \geq 1$ be an integer and let $q \equiv 1 \pmod m$ be a prime. Then q splits completely in the cyclotomic field $K = \mathbb{Q}(\zeta_m)$. Let $\alpha \in \mathbb{F}_q$ be a primitive n-th root of unity. Let

$$e = e(\alpha) = \sum_{i=0}^{n-1} e_i \alpha^i.$$

Then $e \leftarrow PD_{m,q,k}$. Let E denote its density function of e. Recall that U denotes the density function of the uniform distribution: $U(a) = 1/q$ for all $a \in \mathbb{F}_q$. Now We can compute $(E - U)(a)$ for any $a \in \mathbb{F}_q$ using the Fourier inversion formula, using the notations in the beginning of this section,

$$\begin{aligned} E(a) - U(a) &= \frac{1}{q} \sum_{s \in \mathbb{F}_q} (\hat{E}(s) - \hat{U}(s)) \chi_s(a) \\ &= \frac{1}{q} \sum_{s \in \mathbb{F}_q} (\hat{E}(s) - \delta(s)) \chi_s(a) \\ &= \frac{1}{q} \sum_{s \in \mathbb{F}_q, s \neq 0} \hat{E}(s) \chi_s(a). \end{aligned}$$

Since $|\chi_s(a)| \leq 1$ for all a and all s, we have

Proposition 7.7.

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

Let $\epsilon(m, q, k, \alpha)$ denote the right hand side of the above inequality, 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 over all primitive n-th root of unities in $\mathbb{F}_q$ and define

$$\epsilon(m, q, k) := \max_{\alpha : \varphi_m(\alpha) = 0} \epsilon(m, q, k, \alpha)$$

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

TABLE 7.1. $f = 1$

m	q	$[\log_2(\epsilon(m, q, 2))]$
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
101	101	-4
13	1000039	-12
512	7681	-455
512	10753	-431
512	19457	-414

On row -1 and -2 from the above table, we can see the effect of taking the ramified prime, or taking $q \gg n$.

Remark 7.8. It is possible to generalize this cryptoanalysis to higher degree primes, where we are looking at general finite fields $\mathbb{F}_{q^f}$. In this situation we should interpret $\chi_s(a) = e^{2\pi i Tr(as)/q}$. Separability tells us this is an isomorphism between $\mathbb{F}_q$ and its dual, and we can define the Fourier transform this way. So everything goes through? We just want to add a trace to everything, i.e.,

$$\hat{E_{\mathbf{a},k,q}}(s) = \prod_{i=1}^{n} \cos\left(\frac{\pi Tr(a_i s)}{q}\right)^k$$

Note this is well-defined when k is even, which we always assume.

We have a table for degree 2 primes.

TABLE 7.2. $f = 2$

m	q	$-[\log_2(\epsilon(m, q, 2))]$
53	211	61
55	109	48
63	881	33
64	127	37
64	191	35
64	383	31
512	257	263

In terms of statistical distance, ...,

8. Conclusion and open problems

References

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

[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.