Attack on Galois RLWE

Kristin Lauter, Kate Stange, Hao Chen

August 31, 2015

Abstract

We describe a new attack on decision RLWE for number fields based on χ^2 test, and give examples of Galois fields vulnerable to our attack. Then, we analyze the security of cyclotomic extensions under our attack, using Fourier analysis on finite fields.

1 Introduction

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 *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* as follows. Let r_1, r_2 denote the number of real and conjugate pairs of complex embeddings of K. Without loss of generality, assume $\sigma_1, \cdots, \sigma_{r_1}$ are the real embeddings of K, and $\sigma_{r_1+r_2+j} = \bar{\sigma}_{r_1+j}$ for $1 \leq j \leq r_2$. Then we define

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

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 1.1. 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

$$T =$$

Then we have

$$\tilde{A_w} = T^* A_w.$$

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 [LPR]).

Definition 1.2. For a lattiace $\Lambda \subset \mathbb{R}^n$ and $\sigma > 0$, the *discrete Gaussian distribution* on Λ with parameter σ is:

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

1.1 Ring LWE problems for general number fields

Definition 1.3. 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 1.4. 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 $\tilde{\iota}(R)$. 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 1.5 (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 versions, referred to as search and decision, respectively.

Definition 1.6 (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 1.7 (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 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 [EHL, 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 of [EHL, Theorem 2].

Definition 2.1. Given an RLWE instance $R = (K, q, \sigma, s)$ and a prime ideal $\mathfrak{q}$ of K lying above q. The problem $SRLWE(R, \mathfrak{q})$ is: given access to arbitrarily many independent samples $(a, b) \leftarrow \mathcal{R}$, find $s \pmod{\mathfrak{q}}$.

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

Lemma 2.2. *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 2.3. *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 2.4. 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 sub-cyclotomic fields and the normal integral basis, the Galois autormophisms are simply permutations of coordinates, so it could be done very fast.

Remark 2.5. 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.

3 χ^2 attack

See chisquare

4 sub-cyclotomics and vulnerable instances

See sub-cyclotomics

5 Invulnerability of cyclotomic extensions

See cyclo-secure