Attack on Galois RLWE

Kristin Lauter, Kate Stange, Hao Chen

August 29, 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. Also, we sharpen the attack in [ELOS] and give examples of vulnerable instnaces of cryptographic size. Finally, we discuss the effect of modulus switching on our attacks.

1 Introduction

1.1 Ring LWE problems for general number fields

Definition 1.1. An RLWE instance is a triple $= (K, q, \sigma)$, where . An RLWE sample generated from is $(a, b) \sim$, where a ....

2 search-to-decision reduction

We prove the following reduction, which can be viewed as a generalization of to primes of higher degree. Note that we are proving the reduction of Search-RLWE for Galois extensions to the problem of recovering the secret modulo some prime ideal, which is the output of both [ELOS] and our Algorithm . The search-to-decision reduction can be proved by running the proof of [LPR]. We borrow some notations from

Definition 2.1. Given an RLWE instance $R = (K, q, \sigma)$ and a prime ideal $\mathfrak{q}$ of K lying above q. The problem $S - RLWE(R, \mathfrak{q})$ is, to ..... blah blah blah.

When q is an unramified prime. We prove the reduction from $RLWE(R)$ to $RLWE(R, \mathfrak{q})$.

Theorem 2.2. *Let $K/\mathbb{Q}$ be a finite Galois extension of degree n, and let q be a prime number such that q is unramified in K. Let $f = f(q; K/\mathbb{Q})$ denote the residue degree of q. Suppose there is an algorithm that works as follows: it takes as input $(S, \mathfrak{q})$, where $\mathfrak{q}$ is a prime ideal of K lying above q and S is a list of RLWE samples (a, b) $A_{s,}$, and outputs the value $s \pmod{\mathfrak{q}}$. Assume that the running time of the algorithm is t. Then the Search-RLWE problem for the instance (K, q, σ) can be solved, using the same set of samples S, in time $\frac{n}{f}t$.*

Proof. Galois group acts transitively. Let $\mathfrak{q}_1 = \mathfrak{q}, \cdots, \mathfrak{q}_n'$ denote the primes of K above q, then $n' = n/f$, and since $R/qR = \prod_{\mathfrak{q}_i|q} R/\mathfrak{q}_i R$, it suffices to recover $s \mod \mathfrak{q}_i$ for $1 \leq i \leq n'$.

Now for each i, take $\sigma \in Gal(K/\mathbb{Q})$, such that $\sigma_i(\mathfrak{q}) = \mathfrak{q}_i$, and run the algorithm on $(\sigma_i^{-1}(S), \mathfrak{q}_i)$. The algorithm outputs $\sigma_i^{-1}(s) \pmod{\mathfrak{q}}$, which is equal to $s \pmod{\mathfrak{q}_i}$. Hence we have recovered s. The complexity estimate comes from the fact that we are applying the algorithm n' times. □

Remark 2.3. 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 2.4. Although 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.

Corollary 2.5.

3 χ^2 attack

4 sub-cyclotomics and vulnerable instances

4.1 Background

4.2 A note on searching

5 Invulnerability of cyclotomic extensions

6 Sharpening [ELOS] attack

7 Modulus Swtiching