SUB-CYCLOTOMICS

HAO CHEN, KRISTIN LAUTER AND KATE STANGE

1. Introduction

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 1.1. *$w = (w_c)_{c \in C}$ 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 1.2. *By spherical symmetry and the property of the normal integral basis, the error distribution $D \pmod{\mathfrak{q}}$ is independent of the choice of $\mathfrak{q}$.*

2. Searching

We 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 χ^2 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.

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 is taking a long time to finish. Instead of running the actual

Table 2.1. 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

Table 2.2. Some Vulnerable sub-cyclotomic RLWE instances

m	generators of H	n	q	f	σ_0	no. samples used	est.runtime (h)	prob. of success
255255Z)	[97943, 83656, 77351, 78541, 129403]	90	463	2	1	21436	1786.41	1.0 (*)

attack, we estimate the running time by doing a few chisuqare tests on some guesses, take the average, and multiply by the total number of tests. We list the probability of success in the column.