SUB-CYCLOTOMICS

HAO CHEN, KRISTIN LAUTER AND KATE STANGE

1. Introduction

The fields considered in this section are 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.

We search for vulnerable instances among fields of form $K_{m,H}$. The searching 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.

The field searching requires sampling efficiently from a discete Gaussian $D_{\Lambda,\sigma}$. Hence one needs to compute an integral basis for K and the embedding matrix A_v, which is time-consuming for general fields. Luckily, every field of form $K_{m,H}$ always possess a *normal integral basis}, which takes a simple form. In addition, its embedding matrix is easy to compute.*

Let $K = K_{m,H}$ and let C denote a set of coset representatives of the group G/H.

Definition 1.1. For each $i \in C$, define

$$b_i = \sum_{h \in H} \zeta_m^{hi}.$$

Proposition 1.2. *Suppose $m \geq 1$ is odd and squarefree. Then the elements $(b_i)_{i \in C}$ form a $\mathbb{Z}$-basis for $K_{m,H}$.*

Proof. Application of Hilbert-Speiser theorem. □

To work with real matrices, following [DD], we define a matrix T

Definition 1.3.

Let n, and let $\sigma_1, \cdots, \sigma_n$ be the embeddings of K into the field of complex numbers. Assume that the σ_i are ordered such that if σ_i is a complex embedding, then $\sigma_{i+n/2} = \bar{\sigma}_i$.

Definition 1.4. For any sequence $\mathbf{a} = (a_1, \cdots, a_n)$ of n elements in K, define the *canonical embedding matrix* of $\mathbf{a}$ to be

$$A^0_{\mathbf{a}} = (\sigma_i(a_j))_{i,j}.$$

Define the *real embedding matrix* of $\mathbf{a}$ to be

$$A_{\mathbf{a}} = \begin{cases} T^* A^0_{\mathbf{a}} & \text{if } K \text{ is totally complex} \\ A^0_{\mathbf{a}} & \text{otherwise} \end{cases}$$

Note that the entries of $A_{\mathbf{a}}$ are always real numbers. In particular, if $\mathbf{a}$ consists of a $\mathbb{Z}$-basis of $\mathcal{O}_K$, then we could use the columns of $A_{\mathbf{a}}$ as the basis for our sampling purposes.

since by spherical symmetry and the property of the normal integral basis, the error distribution $D \pmod{\mathfrak{q}}$ is independent of the choice of $\mathfrak{q}$.

TABLE 2.1. Vulnerable sub-cyclotomic RLWE instances

m	*gensH*	n	q	f	σ	M	t
90321	*[90320, 18514, 43405]*	*80*	*67*	*2*	*1*	*26934*	*17322.9*

2. EXAMPLES

In table, we list some vulnerable instance we found. The columns are as follows. Note that we ommited the prime ideal $\mathfrak{q}$ *due to Lemma .* $s = \sqrt{2\pi}\sigma$ *denotes the width of the error, and* t *denotes the running time in seconds.*

3. PROOFS

3.1. Scaling. *The above analysis needs to be strengthened to take scaling into account. If* $a \in \mathbb{Z}$ *is coprime to* q*, then the set of values of* ae *and* e *will have the same size, but this scaling multiplies the norm of the vector* $||\bar{b}||_2$ *by* a*. To deal with this issue, we considered scaling the vector* $\bar{\mathbf{b}}$ *by every* $a \in \mathbb{F}_q^*$ *and find the one that yields the smallest 2-norm:*

$$\sigma_{\pi,opt} = \min\{||a\bar{\mathbf{b}}||_2 : a \in \mathbb{F}_q^*\}$$

and

$$r_{opt} = \frac{2\sigma_{\pi,opt}}{q}.$$

For examples, see these files: