

# 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  $\text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$  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 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  $\mathfrak{q}$ .

**1.1. 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 discrete 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 omitted the prime ideal  $\mathfrak{q}$  due to Lemma . and  $t$  denotes the running time in seconds.

TABLE 1.1. Attacked sub-cyclotomic RLWE instances

$m$	generators of $H$	$n$	$q$	$f$	$\sigma_0$	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

**1.2. 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  $w_1, \dots, w_n$  of  $R = \mathcal{O}_K$  with respect to the adjusted embedding. Fix a prime ideal  $\mathfrak{q}$  above  $q$ . Then the image  $\bar{w}_1, \dots, \bar{w}_n$  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,

TABLE 1.2. Some Vulnerable sub-cyclotomic RLWE instances

$m$	generators of $H$	$n$	$q$	$f$	$\sigma_0$	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	?	?	?

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 1.3.**

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  $\lambda$  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.