# SECURITY OF CYCLOTOMIC EXTENSIONS AGAINST THE [ELOS] ATTACK ON RLWE

HAO CHEN, KRISTIN LAUTER, AND KATE STANGE

## 1. INTRODUCTION

Let $m \geq 1$ be any integer and let $K = \mathbb{Q}(\zeta_m)$. We will show that under a simplifying assumption, the image of a reduced RLWE error distribution $D_{\mathcal{R}} \pmod{\mathfrak{q}}$ for a prime $\mathfrak{q}$ above $q$, will be non-distinguishable from the uniform distribution $U(\mathbb{F}_q)$. The tool we use is Fourier analysis on finite fields.

First, we introduce a class of distributions indexed by even integers $k \geq 2$, aiming at approximating discrete Gaussians over $\mathbb{Z}$. Here $k$ plays the role of the standard deviation $\sigma$ for discrete Gaussians.

**Definition 1.1.** For any even integer $k \geq 2$, let $\mathcal{V}_k$ denote the distribution over $\mathbb{Z}$ such that

$$\mathrm{Prob}(\mathcal{V}_k = m) = \begin{cases} \binom{k}{m + \frac{k}{2}} & \text{if } |m| \leq \frac{k}{2} \\ 0 & \text{otherwise} \end{cases}$$

When $q > k$, we abuse notations and let $\mathcal{V}_k : \mathbb{F}_q \to \mathbb{R}$ denote the probability density function of the distribution '$\mathcal{V}'_k$' over $\mathbb{F}_q$ defined by the same formula.
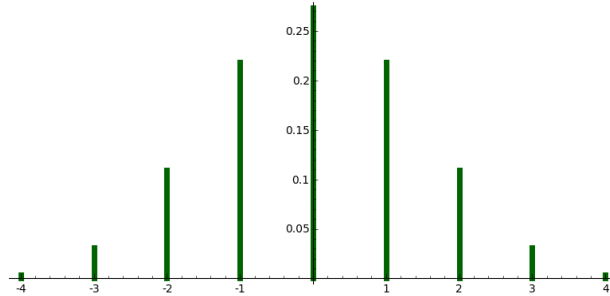


FIGURE 1.1. Probability density function of $\mathcal{V}_8$

**Definition 1.2** (Modified error distribtuion). Let $K = \mathbb{Q}(\zeta_m)$ with degree $n$ ring of integers $R$. Let $q$ be a prime and let $k \geq 2$ be an even integer. Then a sample from the distribtuion $PD_{m,q,k}$ is

$$e = \sum_{i=0}^{n-1} e_i \zeta_m^i \pmod{qR},$$

where the $e_i$ are sampled independently from $\mathcal{V}_k$.

**Assumption** Keeping the above notations, $\mathcal{R} = (K, q, \sigma, s)$ be an RLWE instance. We assume that the distribtutions $PD_{m,q,[\sqrt{2\pi}\sigma]}$ are $D_{\mathcal{R}}$ are "close modulo $\mathfrak{q}$", in the sense that the two distributions $PD_{m,q,[\sqrt{2\pi}\sigma]}$ (mod $\mathfrak{q}$) and $D_{\mathcal{R}} \pmod{\mathfrak{q}}$ are indistinguishable.

We will analyze the distance between $PD_{m,q,[\sqrt{2\pi}\sigma]} \pmod{\mathfrak{q}}$ and the uniform distribution over $R/\mathfrak{q}$.

## 2. AFTER INTRODUCTION

We recall the definition and key properties of Fourier transform over finite fields. Suppose $f$ is a real-valued function on $\mathbb{F}_q$. The *Fourier transform* of $f$ is defined as

$$\hat{f}(s) = \sum_{a \in \mathbb{F}_q} f(a) \bar{\chi}_s(a),$$

where

$$\chi_s(a) := e^{2\pi i a s / q}$$

We have the inversion formula:

$$f(a) = \frac{1}{q} \sum_{s \in \mathbb{F}_q} \hat{f}(s) \chi_s(a).$$

Let $\mathbf{1}$ denote the constant function $f \equiv 1$, and let $\delta$ denote the characteristic function of the one-point set $\{0\} \subseteq \mathbb{F}_q$.

**Proposition 2.1.**

  (1) *The transform of the $\delta$ function is $\hat{\delta} = \mathbf{1}$.*
  (2) *The transform of $\mathbf{1}$ is $\hat{\mathbf{1}} = q\delta$; if $U$ the uniform distribution over $\mathbb{F}_q$, then $\hat{U} = \delta$.*
  (3) *convolution becomes product.*

**Lemma 2.2.** *For all even integers $k \geq 2$,*

$$\hat{\mathcal{V}}_k(s) = \cos\left(\frac{\pi s}{q}\right)^k, (\forall s \in \mathbb{F}_q).$$

*Proof.* Routine calculation.                                                                 $\square$

Now we consider the error distribution we obtained from mapping RLWE errors to $\mathbb{F}_q$.

**Definition 2.3.** Suppose $\mathbf{a} = a_1, \cdots, a_n$ is a vector in $\mathbb{F}_q^n$. Define the following random variable with values in $\mathbb{F}_q$

$$e(\mathbf{a}, k, q) := \sum_{i=1}^{n} a_i e_i \pmod{q}$$

where the $e_i$ are independent variables with distribution $\mathcal{V}_k$. Let $E$ denote its probability density function: $E(b) = \text{Prob}(e = b)$ for $b \in \mathbb{F}_q$.

Next, using the fact that the probability of a sum of two varaibles is a convolution, we prove

**Lemma 2.4.**

$$\hat{E_{\mathbf{a}, k, q}}(s) = \prod_{i=1}^{n} \cos\left(\frac{a_i \pi s}{q}\right)^k$$

*In particular, $\hat{E}(0) = 1$ for all $\mathbf{a}$, $k$ and $q$.*

*Proof.* Routine calculation.                                                                 $\square$

Next we restrict our attention to cyclotomic fields. Let $m \geq 1$ be an integer and let $q \equiv 1 \pmod{m}$ be a prime. Then $q$ splits completely in the cyclotomic field $K = \mathbb{Q}(\zeta_m)$. Let $\alpha \in \mathbb{F}_q$ be a primitive $n$-th root of unity. Let

$$e = e(\alpha) = \sum_{i=0}^{n-1} e_i \alpha^i.$$

Then $e \leftarrow PD_{m,q,k}$. Let $E$ denote its density function of $e$. Recall that $U$ denotes the density function of the uniform distribution: $U(a) = 1/q$ for all $a \in \mathbb{F}_q$. Now We can compute $(E - U)(a)$ for any $a \in \mathbb{F}_q$ using the Fourier inversion formula, using the notations in the beginning of this section,

$$E(a) - U(a) = \frac{1}{q} \sum_{s \in \mathbb{F}_q} (\hat{E}(s) - \hat{U}(s)) \chi_s(a)$$

$$= \frac{1}{q} \sum_{s \in \mathbb{F}_q} (\hat{E}(s) - \delta(s)) \chi_s(a)$$

$$= \frac{1}{q} \sum_{s \in \mathbb{F}_q, s \neq 0} \hat{E}(s) \chi_s(a).$$

Since $|\chi_s(a)| \leq 1$ for all $a$ and all $s$, we have

**Proposition 2.5.**

$$\left| E(a) - 1/q \right| \leq \frac{1}{q} \sum_{y \in \mathbb{F}_q, y \neq 0} |\hat{E}(y)|, \ (\forall a \in \mathbb{F}_q)$$

Let $\epsilon(m, q, k, \alpha)$ denote the right hand side of the above inequality, i.e.,

$$\epsilon(m, q, k, \alpha) = \frac{1}{q} \sum_{y \in \mathbb{F}_q, y \neq 0} \prod_{i=0}^{n-1} \cos\left(\frac{\alpha^i \pi y}{q}\right)^k.$$

We let $\alpha$ run over all primitive n-th root of unities in $\mathbb{F}_q$ and define

$$\epsilon(m, q, k) := \max_{\alpha : \varphi_m(\alpha) = 0} \epsilon(m, q, k, \alpha)$$

The punchline of our argument is: the value $\epsilon(m, q, k)$ is usually negligibly small. As a result, the distribution $PD_{m,q,k} \pmod{\mathfrak{q}}$ is computationally indistinguishable from uniform for all $\mathfrak{q}$. The following is a table of data, to demonstrate how small it is.

TABLE 2.1. $f = 1$

| $m$ | $q$ | $\lceil \log_2(\epsilon(m, q, 2)) \rceil$ |
|-----|------|------|
| 244 | 1709 | $-230$ |
| 101 | 1213 | $-177$ |
| 256 | 3329 | $-194$ |
| 256 | 14081 | $-208$ |
| 55 | 10891 | $-44$ |
| 197 | 3547 | $-337$ |
| 96 | 4513 | $-35$ |
| 160 | 20641 | -61 |
| 145 | 19163 | $-176$ |
| 101 | 101 | $-4$ |
| 13 | 1000039 | $-12$ |
| 512 | 7681 | -455 |
| 512 | 10753 | -431 |
| 512 | 19457 | -414 |

On row $-1$ and $-2$ from the above table, we can see the effect of taking the ramified prime, or taking $q \gg n$.

*Remark* 2.6. It is possible to generalize this cryptoanalysis to higher degree primes, where we are looking at general finite fields $\mathbb{F}_{q^f}$. In this situation we should interpret $\chi_s(a) = e^{2\pi i Tr(as)/q}$. Separability tells us this is an isomorphism between $\mathbb{F}_q$ and its dual, and we can define the Fourier transform this way. So everything goes through? We just want to add a trace to everything, i.e.,

$$\hat{E}_{\mathbf{a}, k, q}(s) = \prod_{i=1}^{n} \cos\left(\frac{\pi Tr(a_i s)}{q}\right)^k$$

Note this is well-defined when $k$ is even, which we always assume.

We have a table for degree 2 primes.

TABLE 2.2. $f = 2$

| $m$ | $q$ | $-[\log_2(\epsilon(m, q, 2))]$ |
| --- | --- | --- |
| 53 | 211 | 61 |
| 55 | 109 | 48 |
| 63 | 881 | 33 |
| 64 | 127 | 37 |
| 64 | 191 | 35 |
| 64 | 383 | 31 |
| 512 | 257 | 263 |

## 3. References

https://en.wikipedia.org/wiki/Fourier_transform_on_finite_groups
http://arxiv.org/pdf/0909.5471v1.pdf
https://books.google.com/books?id=-B2TA669dJMC&pg=PA251#v=onepage&q&f=false