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

HAO CHEN, KRISTIN LAUTER, AND KATE STANGE

1. Introduction

We expect that under some mild assumptions, the image of a discrete Gaussian error distribution under the ring maps $\mathcal{O}_K \to \mathbb{F}_q$ for a split prime q will be non-distinguishable from the uniform distribution $U(\mathbb{F}_q)$.

To aid the analysis, we use another class of distribution instead of discrete Gaussian distributions over the integers.

Tools: Fourier analysis on finite fields.

2. After introduction

Suppose f is a real-valued function on $\mathbb{F}_q$. The Fourier transform of f is defined as

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

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 δ denote the characteristic function of the one-point set $\{0\} \subseteq \mathbb{F}_q$. We recall some basic properties of the Fourier transform:

Proposition 2.1.

(1) The transform of the δ 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.

Next we introduce a class of distributions indexed by even integers $k \geq 2$, aiming at approximating discrete Gaussians over the integers. Here k plays the role of the standard deviation σ for discrete Gaussians.

Definition 2.2. For any even integer $k \geq 2$, $\mathcal{V}_k$ is the distribution over $\mathbb{Z}$ such that

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

When q is a prime such that $q > k$, 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.

Lemma 2.3. *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. □

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

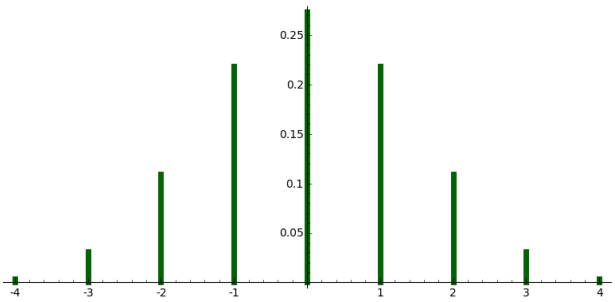

FIGURE 2.1. Probability density function of $\mathcal{V}_8$

Definition 2.4. 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 2.5.

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

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

Proof. Routine calculation. □

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. In the following discussion, we will take $k = 2$, and will take

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

Let E denote the 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,

$$\begin{aligned} E(a) - U(a) &= \frac{1}{q} \sum_{s \in \mathbb{F}_q} (\hat{E}(s) - \hat{U}(s)) \chi_s(a) \\ &= \frac{1}{q} \sum_{s \in \mathbb{F}_q} (\hat{E}(s) - \delta(s)) \chi_s(a) \\ &= \frac{1}{q} \sum_{s \in \mathbb{F}_q, s \neq 0} \hat{E}(s) \chi_s(a) \end{aligned}$$

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

$$\boxed{|E(a) - 1/q| \leq \frac{1}{q} \sum_{s \in \mathbb{F}_q, s \neq 0} |\hat{E}(s)| =: \epsilon(m, q, \alpha), \ (\forall a \in \mathbb{F}_q)}$$

The punchline is: $\epsilon(m, q, \alpha)$ is usually negligably small, and when it is, the distribution e is computationally indistinguishable from the uniform distribution over $\mathbb{F}_q$. The following is a table of data, to demonstrate how small it is.

m	q	$[\log_2(\epsilon(m,q,\alpha))]$
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

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 $\mathbb{F}_{q^r}$. 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.

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

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