MSR-NOTES

HAO CHEN, KRISTIN LAUTER AND KATE STANGE

Abstract. We try to attack prime cyclotomics when the modulus q is equal to the prime p.

1. Intro

Let p be an odd prime and $K = \mathbb{Q}(\zeta_p)$. First we deal with the case of sampling. A result of [DD] says that sampling from the Minkowski space of K with paremeter σ is the same as sampling a Discrete Gaussian from the quotient ring

$$\mathbb{Z}[x]/(x^p - 1)$$

with parameter $\sigma/\sqrt{p}$. We are going to take this point of view. The determinant factor is

$$Disc(K)^{\frac{1}{2[K:\mathbb{Q}]}} = p^{\frac{p-2}{2(p-1)}}.$$

Suppose we have chosen a base parameter σ_0. Then the adjustment $\sigma = \sigma_0/\sqrt{p} \cdot p^{\frac{p-2}{2(p-1)}} = \sigma_0 \cdot p^{\frac{-1}{2p-2}}$. Hence a general error term is

$$e = e_0 + e_1\zeta_p + \cdots + e_{p-1}\zeta_{p-1}$$

where $(e_i)_i$ are sampled from $D_{\mathbb{Z}^n,\sigma}$, and then reduced modulo p. Note that every ζ_p maps to 1 in $\mathbb{F}_p$. Hence we have

$$e(1) = e_0 + e_1 + \cdots + e_{p-1} \in \mathbb{F}_p.$$

Now we use the **independence** of the samples to conclude that $e_0 + e_1 + \cdots + e_{p-1} \sim D_{\mathbb{Z},\sqrt{p}\sigma}$, and assume that $|e(1)| \leq \sqrt{p}\sigma$.

Now for [ELOS] attack to work, we need

$$|e(1)| \leq p/4,$$

and we computed $p/|e(1)| \geq \sqrt{p}/\sigma_0$. So when p is not to small, this attack will work.