ANALYSIS2.0 TO ELOS AND MODULUS SWTICHING

HAO CHEN

Notations:
– α: an elemenf of K.
– $v : [1, \alpha, \cdots, \alpha^{n-1}]$.
– A_v : the embedding matrix of v. The i-th column being $(\sigma_1(\alpha^i), \cdots, \sigma_n(\alpha^i))$.
– $\lambda_1(A_v)$: the maximum singular value of A_v.
– $\lambda_n(A_v)$: the maximum singular value of A_v.
– $e = e(\alpha)$, the error polynomial

$$e = \sum e_i \alpha^i,$$

– **e**: the coefficient vector of e.
– σ: the 'base' standard deviation. (We could take $\sigma = 1$).

1. Analysis

First, we need to enlarge σ so that it reflects the sparsity of the lattice. This is done by computing

$$d_v := |det(A_v)|^{1/n}.$$

Next, let e_R denote the error vector embedded in Minkowski space, i.e.

$$e_R := A_v \mathbf{e}.$$

Then $\mathbf{e} = A_v^{-1} e_R$, and we know that $\sum_i e_i = \langle \mathbf{r}_v, e_R \rangle$, where $\mathbf{r}_v$ is the vector defined by

$$\mathbf{r}_v[i] = colsum(A_v^{-1}, i) = \sum_j A_v^{-1}[j][i].$$

Let $r_v = ||\mathbf{r}_v||_2$. Now we use the fact that e_R is sampled from a discrete Lattice Gaussian with $s = \sqrt{2\pi}\sigma d_v$. By Lemma 8 in [LaSt], assuming that $s > \eta_\epsilon(\Lambda)$, we have

$$Prob(|\sum_i e_i| \geq st||r_v||_2) \leq \frac{1+\epsilon}{1-\epsilon} t\sqrt{2\pi e} e^{-\pi t^2}$$

We set $\epsilon = 1/2$ and compute the right hand side for a range of t values.
—t — tail ——— – —3 —1.95475575312e-11— —4 — 7.33494327746e-21— —5 —4.81858570769e-33 — —6 — 5.67493565843e-48 —
As a reference , 2^{-128} is about 10^{-39}. So we can take t somewhere between 5 and 6. Say $t = 5$. Note that our adjusted width of the Gaussian is $s := \sqrt{2\pi}\sigma d_v$. Therefore, we obtain

$$|\sum_i e_i| \leq 4\sqrt{2\pi}\sigma d_v r_v.$$

Now if the right hand side is small compared with q, then we would have an attack. In light of this, we define

$$r_{elos} := \frac{q}{4\sqrt{2\pi}\sigma d_v r_v}.$$

Claim: if $r_{elos} > 1$, then the [ELOS] evaluation at one attack will work on the instance $(\mathbb{Z}[\alpha], q)$.
Remark: similar analysis holds for evaluating at 0 or -1.

2. Modulus switching attack

The analysis of modulus switching attack is similar, that we need to control the new error

$$e'_R = b' - a's + \alpha e_R \in \mathbb{R}^n$$

where we assume that $a' \sim D_{\Lambda+\alpha a,r}$ and $a' \sim D_{\Lambda+\alpha b,r}$ for some $r > 0$. **The essential difficulty of this attack is: the GPV sampler will only work and produce such a' and b' only if r is large enough.**

How large does r have to be? They proposed

$$r \geq ||\tilde{\mathbf{B}}|| \log(n),$$

where $\mathbf{B}$ is any input basis for the lattice. (For example, in our case, it could be the LLL of columns of A_v).

Note that the dominant term in e'_R is the term $a's$, whose width is bounded above by $||s||_\infty r$. Hence, if we have

$$r_{ms} := \frac{q}{4\sqrt{2\pi}||s||_\infty ||\tilde{B}|| \log(n) \cdot r_v}.$$

If $\min(r_{ms}, r_{elos}) > 1$, then the modulus switching attack will work for α sufficiently small (I will explain later).

In practice, the thing that is killing modulus switching is the smallness of r_{ms} due to largeness of the maximal gram-schmidt norm. So if we do a BKZ on the lattice, there is chance that we could get this ratio to be smaller.

3. What about Galois?

As a second work point, we are aiming towards finding Galois extensions with ring of integers. We define a similar r_{elos} measure. What would it be?

It would be like this: let v be our chosen "nice basis", and let $\mathbf{w} = (w_1, \cdots, w_n)$ be its reduction modulo some split prime q. Now we have

$$\bar{e} = \sum_i w_i e_i = \langle (A_v^{-1})^T \mathbf{w}, e_R \rangle.$$

So we want $\bar{e}$ to be small in $\mathbb{F}_q$. Okay.

Note the difference we have over the previous situations is in the previous case $\mathbf{w} = (1, 1, \cdots, 1)$, and now it is all over the place, and the power we have in our hand is maybe scaling by any element in the finite field.

So we actually define the r_{elos} exactly the same as we did before, only with scaling differently, i.e.,

$$r_v := \min_{t \in F_q - 0} ||(A_v^{-1})^T (t\mathbf{w})||_2.$$

and then the old

$$r_{elos} := \frac{q}{4\sqrt{2\pi}\sigma d_v r_v}.$$

We can see this for some prime cyclotomics.

4. some data