MSR-NOTES

HAO CHEN AND KRISTIN LAUTER

ABSTRACT. This set of notes contains our work when Hao is interning at Microsoft Research, working with Kristin, from June 22 to Sept 11, 2015.

1. GOALS

The EHL-ELOS attack is an attack on the decision version of the RLWE problem.

- First, we would like to generate families of Galois extensions which are weak against our attack (because for Galois extensions there is also a search-to-decision reduction).
- I would also like to see if we can figure out how to extend the search-to-decision reduction beyond Galois fields.
- Then, I think we should consider how modulus switching (changing q) in various cryptosystems could make them vulnerable to our attack.
- Then we should consider the vulnerability of the non-2-power cyclotomics and the possibility of using the weak polynomial bases to attack cyclotomics in general.

2. Root of order 3 analysis

Suppose $\alpha^3 \equiv 1 \pmod{q}$, then the analysis we have is

$$e(\alpha) = E_0 + E_1\alpha + E_2\alpha^2 = (E_0 - E_2) + (E_1 - E_2)\alpha,$$

where $\sigma(E_i) = \sigma_0 \cdot \sqrt{2n/3}$.

3. New quaity analysis 8-2

The crucial new input is we do LLL first before running the sampler, compute vectors modulo q, and everything.

We simulate error generation using 20 samples, and cap the $2|s|/q$ ratio at 0.9. Now if we have a uniform sample, then it passes the test with probability

$$(0.8)^2 0 = 0.011...$$

We run 25 of these simulations, so if the sample is uniform, we expect to see ¡ 1 instances pass; Hence if we see a lot of instances that passes, then we are positive that this will be a non-uniform sample.

An example can be found here: (past link)

4. Diary on 7-6

For the definition of LWE, see [Reg05].

(1) (Kim): From RLWE samples we can produce LWE samples easily by taking the constant term, then we got

$$b(0) = \tilde{a} \cdot s + e_0,$$

where $\tilde{a}$ is some permutation of a. In particular, if we can solve D-LWE then we can solve D-RLWE; similarly, S-RLWE will reduce to S-LWE.

Warning: the other side of reduction does not necessarily work! i.e., even if we have a solver to D-RLWE (in some dimension $n > 1$, of course), it is not clear how to use the solver to solve D-LWE. The same is true for the search versions. If D-LWE is equivalent to D-RLWE, then we would automatically have search-to-decision reduction. This is summarized in the following diagram.

$$\begin{tikzcd}
D - LWE \arrow[r, Rightarrow] \arrow[d, "Reg05"] & D - RLWE \arrow[d, "LPR10Galois"] \\
S - LWE \arrow[r, Rightarrow] & S - RLWE
\end{tikzcd}$$

What are some of the good things? Well, I could go back to field constructing in general, but note that I want to construct fields with a good basis, where good means the normalized spectral norm is small compared to q.

5. Diary on 7-6

For the definition of LWE, see [Reg05].

(1) (Kim): From RLWE samples we can produce LWE samples easily by taking the constant term, then we got

$$b(0) = \tilde{a} \cdot s + e_0,$$

where $\tilde{a}$ is some permutation of a. In particular, if we can solve D-LWE then we can solve D-RLWE; similarly, S-RLWE will reduce to S-LWE.

Warning: the other side of reduction does not necessarily work! i.e., even if we have a solver to D-RLWE (in some dimension $n > 1$, of course), it is not clear how to use the solver to solve D-LWE. The same is true for the search versions. If D-LWE is equivalent to D-RLWE, then we would automatically have search-to-decision reduction. This is summarized in the following diagram.

$$\begin{tikzcd}
D - LWE \arrow[r, Rightarrow] \arrow[d, "Reg05"] & D - RLWE \arrow[d, "LPR10Galois"] \\
S - LWE \arrow[r, Rightarrow] & S - RLWE
\end{tikzcd}$$

What are some of the good things? Well, I could go back to field constructing in general, but note that I want to construct fields with a good basis, where good means the normalized spectral norm is small compared to q.

Note that we have used an integral to approximate the sum. The difference should be small enough.

6. Almost uniformity of cyclotomics

Let n be an integer. Let q be a prime with $q \equiv 1 \pmod{n}$, and let α be any primitive n-th root of unity in $\mathbb{F}_q$. In this section we are going to explore the distribution of

$$e(\alpha) = e_0 + e_1\alpha + \cdots + e_{n-1}\alpha^{n-1},$$

where the e_i are iid normal modulo q. For simplicity, we are going to assume that for every index i, e_i takes on value 0 with probability 1/2, and $e_i = \pm 1$ with probability 1/4 each. Let $P(t) = Prob(e(\alpha) = t)$, then $P(t) : \mathbb{F}_q \to \mathbb{R}$ is a function, so we could take its Fourier transform.

Lemma 6.1.

$$\hat{P}(s) = \prod_{i=0}^{n-1} \cos^2\left(\frac{\alpha^i \pi s}{q}\right)$$

We wanted to consider a more general question: let $\{a_1, \cdots a_n\}$ be integers such that they are distinct modulo q, where $q = poly(n)$, we wanted to bound the l_2 norm of the function

$$\begin{aligned} p_a &: \mathbb{F}_q \to \mathbb{R} \\ s &\mapsto \prod_{i=1}^{n} \cos^2\left(\frac{a_i \pi s}{q}\right). \end{aligned}$$

By "bound", I meant proving something like

$$\lim_{n\to\infty} ||(p_a(s)||_2 = 0.$$

Note that the assumption that a_i are distinct can not be dropped, otherwise, for example, the l-2 norm squared will be approximated by

$$const \cdot q \cdot \int_0^{2\pi} \cos^{4n}(x)dx,$$

and the last term is asymptotically $\frac{c}{\sqrt{n}}$. So when $q = \Omega(n)$ the product will approch infinity as $n \to \infty$.

Consider the l^2 norm. Say a residue mod q is bad if it lies inside $[-(q-1)/4, (q-1)/4]$. Suppose we have $q = \Theta(p^n)$ (a reasonable assumption). Then set λ = number of cosets of H that contains more than q/p bad elements. Then $\lambda \leq q - 1/(q/p) < p$. We would have the estimate that

$$\begin{aligned} l^2(\hat{p} - \hat{u}) &\leq (1/\sqrt{2})^{p/2}(q - 1 - \lambda p) + \lambda(1 - 1/q)^p \\ &\leq q(1/\sqrt{2})^{p/2} + p(1 - p/q). \end{aligned}$$

We know from our version of Fourier transform that

$$l^2(P - u) = \frac{l^2(\hat{P} - \hat{u})}{q}.$$

Hence we have

$$l^2(P - u) \leq (1/\sqrt{2})^{p/2} + p^{1-n},$$

which tends to zero as $p \to \infty$ (assuming $n > 1$).

7. Cyclotomics

In this section p is always an odd prime.

Claim: If A is the canonical embedding matrix of ζ_p, and $v \in \mathbb{R}^n$ has length 1, then

$$\sqrt{p - \sqrt{p}} \leq ||Av|| \leq \sqrt{p}.$$

Let $\alpha_p = \zeta_p + (\zeta_p)^{-1}$. Then $Tr(\alpha_p) = -1$, and we have, for $n \geq 0$ an integer,

Well, it seems that $||A||_2 \leq \sqrt{mn}||A||_{max}$. But we need to bound the spectral norm of the inverse.

8. non-2-power cyclotomics

The idea is $e_0 = e_1 = \cdots = e_{n-1}$ will be more likely to happen (in the RLWE case). So by multiplying samples by $-x$, we get

$$b(x) = a(x)s(x) + e_0,$$

where $e_0 \in \mathbb{F}_q$. Now we loop through q^2 choices of the tuple $(s(\alpha), e_0)$ and compute the difference

$$b(\alpha) - a(\alpha)s(\alpha) - e_0,$$

If the distribution is RLWE, we expect to get a lot of zeros. If the distribution is uniform, then no.

So I guess the PLWE for the non-2-power cyclotomics should be suggested? Since in that case we do not have a valid attack yet. In this case there exists weak basis, but the transformation matrix will distort the error distribution so much, if we do consider a weak basis.

9. An issue of non-cyclotomics

If we take a algebraic integer α, which is **not** a root of unity, then by a theorem in ANT, there exists an embedding $\sigma : K = \mathbb{Q}(\alpha) \to \mathbb{C}$ such that $|\sigma(\alpha)| > 1$. So $\sigma(\alpha^{n-1})$ will go to infinity as the degree n goes to infinity. Therefore, the canonical embedding vector of α^{n-1} will have uncontrolled length!

For example, if we take $\alpha = \zeta_p + \zeta_p^{-1}$. Then $\alpha = 2\cos(2\pi/p) \to 2\,(p \to \infty)$. So $\alpha^{(p-3)/2} > 1.5^{(p-3)/2}$ (say). Hence the embeding vector of α^{n-1} has length that grows like 2^n. Imagine that $p \to \infty$, then this vector will lie out side any small ball, hence if we use a small ball to sample the vectors, the vector α^{n-1} then won't be sampled at all!

This provides a challenge of sampling, since if we sample from a spherical Gaussian distribution, then the standard deviation parameter needs to grow exponentially to accomodate α^{n-1}.

If we use any power basis, we will be faced with the same problem of unequal length? maybe?

This brings me to the question of the adjoining a root of $q-1$ example in [ELOS]. How is the choice of parameter fix the sampling?

10. Comment on the example in [ELOS]

Well, the thing is if we take the suggested parameters for RLWE, then roughly only the α^m with $0 \le m \le n/2$ will be sampled, and the others are not sampled at all! (For the non-dual version). This would mean that $e(x)$ will have degree $\le n/2$, which may not be what we'd like to do...(Well, I guess this is another reason why one wanted to use cyclotomics, since in this case all vectors have the same length, and it makes sense to sample from a ball).

One can enlarge the ball to contain all vectors, but that would mean.. still there's more probability that one will sample a combination of the short vectors.

Now the possible to-do's are:

1. See if we could get other fields so that the embedding vectors are small, but not too small.
2. Consider the dual version of RLWE. Maybe it is better-suited?
3. Consider the cyclotomics again. See how the error is transformed.

11. Cyclotomics

In this section p is always an odd prime.

Claim: If A is the canonical embedding matrix of ζ_p, and $v \in \mathbb{R}^n$ has length 1, then

$$\sqrt{p - \sqrt{p}} \le ||Av|| \le \sqrt{p}.$$

Let $\alpha_p = \zeta_p + (\zeta_p)^{-1}$. Then $Tr(\alpha_p) = -1$, and we have, for $n \ge 0$ an integer,

$$Tr(\alpha^n) = \begin{cases} -2^{n-1} & \text{if } n \equiv 1 \pmod 2 \\ -2^{n-1} + (m+1/2)\binom{n}{n/2} & \text{if } n \equiv 0 \pmod 2 \end{cases}$$

Well, it seems that $||A||_2 \le \sqrt{mn}||A||_{max}$. But we need to bound the spectral norm of the inverse.

12. Goal 1: generate Galois extensions vulnerable to the EHL-ELOS attack

In [ELOS], weak instance of Ring-LWE are found when we have a number field K and a prime q satisfying the following properties:

(1) K is monogenic, i.e., $O_K = \mathbb{Z}[\theta]$ for some algebraic integer $\theta \in K$.
(2) Let f be the minimal polynomial of θ, then $f(1) \equiv 0 \pmod{q}$.
(3) The spectral norm of a certain matrix is small (I have to figure this out).

In our work, we would like to add a condition to the above three:

$$(4) : K/\mathbb{Q} \text{ is Galois .}$$

(Hao) I will present my ideas below.

12.1. **Splitting fields of $x^p - u$.** Fix an odd prime p and let $K_0 = \mathbb{Q}(\zeta_p)$. Let $\pi := 1 - \zeta_p$, so that $p\mathcal{O}_{K_0} = (\pi)^{p-1}$; For each $u \in K_0 - (K_0)^p$, set $K_u = K_0(\sqrt[p]{u})$. Then by Galois theory and Kummer theory, the following holds:

- $K_u/\mathbb{Q}$ is a Galois extension of degree $p(p-1)$.
- The extension $K_u/\mathbb{Q}$ is ramified only at p and the primes dividing $Norm(u)$. In particular, if u is a unit in K_0, then $K_u/\mathbb{Q}$ is ramified at p.
- Moreover, if $v_\pi(u^p - u) = 1$, then $K_u/\mathbb{Q}$ is totally ramified at p.

We prove the last item:

Proof. Consider the polynomial $g(x) = x^p - u$. We have $g_1(x) = g(x+u) = x^p + ph(x) + u^p - u$, where $h(x) \in \mathcal{O}_{K_0}[x]$. From this we see that: if $v_\pi(u^p - u) = 1$, then $g_1(x)$ is Eisenstein at π. This implies that π is totally ramified in K/K_0. Now the claims follows from the fact that $K_0/\mathbb{Q}$ is totally ramified at p. □

Accepting the last claim, we will see that $K_u/\mathbb{Q}$ is monogenic, from the following Lemma: (warning: there is a gap and the lemma is false).

Lemma 12.1. *Let $K/\mathbb{Q}$ be a number field such that the only ramified prime is p and that p is totally ramified. Let $\mathfrak{p}$ be the unique prime ideal lying over p, then K is monogenic. Even better, for any $\alpha \in \mathfrak{p} - \mathfrak{p}^2$, we have*

$$\mathcal{O}_K = \mathbb{Z}[\alpha].$$

Now, what about the spectral norm? First, I'm not sure if it is equal to the l_2-norm.

However, note that by the wikepedia page on matrix norms, there are certain upper and lower bounds related to l_2 norm and spectral norm So I hope we could obtain some sort of bound on these spectral norms.

Update 6/23: Instead of using u we should use πu to guarantee monogenicity. Or actually, use p.

Update: Use p would guarantee Galois and using π would guarantee monogenic. But I'm not sure now how to get both...However we might not need both.

13. Spectral norms

In this section let K be a number field in general. Let B denote the matrix of the canonical embedding, and let A denote the matrix of the θ-embedding. Then we have

$$det(B) = (-2i)^s det(A),$$

where $2s$ is the number of complex embeddings of K.

Now suppose $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and let A_α be the matrix under the basis in terms of powers of α, then B_α is a Van der mont matrix and we thus have $det(B_\alpha) = disc(\mathbb{Z}[\alpha])$. Hence we have

$$|\det(A_\alpha)| = \frac{|disc(\mathbb{Z}[\alpha])|}{2^s} = \frac{disc(\mathcal{O}_K)}{2^s} = \frac{disc(\mathcal{O}_K)}{2^s}.$$

Now suppose further that K is ramified at p and totally and wildly ramified at p. Then $|disc(\mathcal{O}_K)| \geq p^n$.

Now we take the spectral norm into play: for any n by n matrix A. Let $\rho(A)$ denote its maximum (in abs value) eigenvalue, i.e.,

$$\rho(A) = \max_i \{|\lambda_i(A)|\}$$

where $\lambda_i(A), i = 1, 2, \cdots, n$ are the eigenvalues of A.

We then have $||A|| \geq \rho(A) \geq (\det(A))^{1/n}$. Hence we have

$$||A_\alpha|| \geq p/2^{s/n} \geq p.$$

Another possible approach is to bound the Frobenius norm. I'll think more about that.

What's nice is that this bound does not depend on α.

14. Cyclotomic Invulnerability: Kate's argument

15. Kate's construction of families of cyclic Galois extensions

Waiting to get more information on that... Now suppose further that K is ramified at p and totally and wildly ramified at p. Then $|disc(\mathcal{O}_K)| \geq p^n$.

Now we take the spectral norm into play: for any n by n matrix A. Let $\rho(A)$ denote its maximum (in abs value) eigenvalue, i.e.,

$$\rho(A) = \max_i\{|\lambda_i(A)|\}$$

where $\lambda_i(A), i = 1, 2, \cdots, n$ are the eigenvalues of A.

We then have $||A|| \geq \rho(A) \geq (\det(A))^{1/n}$. Hence we have

$$||A_\alpha|| \geq p/2^{s/n} \geq p.$$

Another possible approach is to bound the Frobenius norm. I'll think more about that.

What's nice is that this bound does not depend on α.

16. Cyclotomic Invulnerability: Kate's argument

The argument works: it reduces search to the case where R is represented by the cyclotomic polynomial. The only thing left is that if the distribution getting from the pushforward $R \to \mathbb{F}_q$ is really indistinguishable from the uniform distribution. To-do: test this.

17. Kate's construction of families of cyclic Galois extensions

Waiting to get more information on that...

18. Constructing Galois Extensions, second try

Let $a_1, a_2, \cdots, a_m$ be cube-free integers and set

$$K = \mathbb{Q}(\zeta_3, \sqrt[3]{a_1}, \cdots, \sqrt[3]{a_m}).$$

For convenience, we write $\alpha_i = \sqrt[3]{a_i}$. We claim and will prove later that it is not so hard to choose a_i carefully, such that the ring of integers

$$\mathcal{O}_K = \sum_{e_0\in\{0,1\}, e_i\in\{0,1,2\}} \mathbb{Z}\,\zeta_3^{e_0}\alpha_1^{e_1}\cdots\alpha_n^{e_m}.$$

We have also for carefully chosen a_i's, that $n = [K : \mathbb{Q}] = 2 \cdot 3^n$. Let B denote the basis, and let A denote the canonical embedding matrix. We have

Lemma 18.1.

$$A^*A = n \cdot diag(\prod_i \alpha^{2e_i} : e_i) \oplus (1, -1/2, -1/2, 1).$$

From the lemma it follows that the minimum singular value of A is $\sigma_{\min} = \frac{\sqrt{n}}{2}$. So the spectral norm of A^{-1} is $\rho = \frac{2}{\sqrt{n}}$.

Also we can compute

$$\det(A) = \frac{\sqrt{3}}{2} \cdot (\sqrt{n}\prod_i \alpha_i)^n.$$

Hence the scaling factor in [ELOS] becomes

$$\det(A)^{1/n} \sim \sqrt{n}\prod_i \alpha_i.$$

Now we consider the roots modulo q. We choose a_i carefully so that the minpoly of each α_i has a root 1 modulo q. As a result, half of the elements in B (3^m) will become 1 modulo q, and the other half will become ζ_3 modulo q (whatever that is). So when we map the error to $\mathbb{F}_q$, we obtain $e + e'\zeta_3$, where e, e' are distributed in $D_{\mathbb{Z}, \frac{ns}{2}}$. By using another root, we could get $e - e'\zeta_3$. So upon guessing 2 roots, the corresponding inequality is

$$const \cdot \prod_i \alpha_i \cdot n < q.$$

However, the construction requires $\alpha_i \sim \sqrt[3]{q}$, so we could only have at most 2 α's, and the degree is constrained above by blah blah blah. How-however, we do not need to adjoin integers! We can adjoin as many units as we like, and the orthognoality condition would still hold (right?) but the ring of integers might be way off....

Another direction is to increase ζ_3 to higher ones in general, but that would require dealing with arbitrary degree cyclotomic fields, which is the thing that I wanted to avoid in the first place.

To-do: think about adjoining unitsand blah blah blah...

19. Constructing Galois extensions: iterated square roots

Let K be a number field and $\Omega = \{\omega_1, \cdots, \omega_n\}$ be a orthogonal basis of $\mathcal{O}_K$. Let $u \in \mathcal{O}_K$ and $u_1 = u, \cdots, u_n$ be its Galois conjugates. We are going to analyze what happens when we consider $L = K(\sqrt{u})$.

Claim: if u is not a square in $\mathcal{O}_K/4$, then $P = \Omega \cup \Omega\sqrt{u}$ is a basis of $\mathcal{O}_L$.

Assuming the claim, the embedding matrix M_P will be

$$M_P = \begin{pmatrix} M_\Omega & UM_\Omega \\ M_\Omega & -UM_\Omega \end{pmatrix}$$

where M_Ω is the embedding matrix of Ω, adn U is the diagonal matrix $U = diag(\sqrt{u_i})_i$. Considering the dot products between columns of M_P, we can see that

Lemma 19.1. *If the columns of M_Ω is orthogonal, then the columns of M_P are not necessarily so. But the non-trivial dot products only happens in the last n columns.*

But what if we adjoin other roots as well? Well, it happens that orthogonal numbers are always orthogonal, and non-ortnogonal ones are always non-orthogona: taking an extension will only repeat the vectors, so it does not change this situation.

In fact, we can define the notion of orthogonality of algebraic numbers:

Definition 19.2. Suppose α, β are algebraic numbers. Let $K = \mathbb{Q}(\alpha, \beta)$, and let $\sigma : K \to \mathbb{C}^n$ be its canonical embedding. The numbers α and β are *orthogonal* if

$$\sigma(\alpha) \cdot \sigma(\beta) = 0.$$

Some examples of orthogonal algebraic numbers: $\sqrt[3]{2}$ and $(\sqrt[3]{2})^2$, $\sqrt{2}$ and $\sqrt{3}$.

We need to investigate this situation more: what is, this orthogonality, after all?]

If α, β are totally real, then this orthogonality simply means that $Tr(\alpha\beta) = 0$, which is true when they are linearly disjoint?

20. Why there is no Galois extension of large degree vulnerable to the [ELOS] attack

Reason: The [ELOS] attack works because we have a basis $B = \{\omega_1, \cdots, \omega_n\}$ of the ring of integers $\mathcal{O}_K$ such that the following holds:

(1) short vectors in $\sigma(\mathcal{O}_K)$ have small coefficients when expressed in the basis B.
(2) There exists a ring map $f : \mathcal{O}_K \to \mathbb{F}_q$ such that $f(\omega_i)$ have small order for all $i = 1, \cdots, n$.

Okay, suppose ω is one of the short vectors. Then $\sigma_i(\omega)$ is also short for all Galois conjugates.

20.1. **Consider the shortest vector.** Let B defined as above be our "magic basis", and let ω be the shortest vector in the embedded lattice $\mathcal{L}_K \overset{def}{=} \sigma(\mathcal{O}_K)$. Let $h = ||\omega||$ be the length of the shortest vector. Let $V_{\mathcal{L}_K}$ denote the covolume of $\mathcal{L}_K$ (This is equal to $|\det(M)|$ in [ELOS]). Then we have an upperbound of h by Minkowski's bound:

$$2^n \cdot V_{\mathcal{L}_K} \geq \frac{\pi^{n/2}}{\Gamma(1+n/2)} h^n.$$

Taking n-th roots on both sides and applying Stirling's approximation for the factorial, we obtain

$$h \leq C \cdot V_{\mathcal{L}_K}^{1/n} \sqrt{n} = b_{n,K}$$

where C is a constant close to 1. (C is about $\frac{2}{\sqrt{\pi e}} \cdot (2\pi n)^{\frac{1}{2n}}$ when $n \to \infty$).

Now we go back to the Gaussian parameter proposed in [ELOS]: it is $\sigma' = \sigma \cdot V_{\mathcal{L}_K}^{1/n}$, and σ is around 10. Note that there is no vector of length $\leq h$, and the Gaussian can be effectively truncated at length $c_{n,K} = 2\sqrt{n}\sigma'$. Note that we have

$$c_{n,K} \approx 2\sigma b_{n,K}.$$

Therefore, intuitively, any small integer linear comibination of the linearly independent vectors $\{\sigma_i(\omega)\}$ will be "very likely" to be sampled, but this needs to be quantified...

Any way, for these fields, all we need is to demonstrate that there exists a "bad basis", then we can argue that change of basis does not change the error distribution, and then there's no "good basis": all effort that tries to find a nice basis will be in vain.

Question: if we knew the error are sampled from a lower-dimensional subspace, but not too low, what kind of attacks are available? For example, say $e(x)$ is sampled from a $n/2$-dimensional Gaussian, then what kind of attacks can we initialize?

In fact, all the analysis will depend on finding a basis with small spectral norm, so unless we can construct number fields with such bases, there's no further analysis.

21. A short note on cyclotomic subfields

Let m be any pos int and H be a subgroup of $(\mathbb{Z}/m\mathbb{Z})^*$ of order r. Then H determines a subfield F_H of $\mathbb{Q}(\zeta_m)$, and there is a natural basis for this extension, i.e.,

$$F_H = \mathbb{Q}(\alpha)$$

where $\alpha = \sum_{h\in H} \zeta^h$, and its conjugates are $\alpha^\sigma = \sum_{h\in H} \zeta^{\sigma h}$, a sum over cosets. Let M be the matrix of the basis $B = \{\alpha^\sigma : \sigma \in G/H\}$.

Claim:

$$M^* M = \varphi(m) \cdot I - r(\mathbf{1} \cdot \mathbf{1}^T)$$

. In particular, this shows that

$$||x||^2 \leq ||M(x)||^2 \leq n||x||^2$$

for all x, where $n := \varphi(m)$. In particular, the inverse spectral norm is exactly equal to 1.

Now we take m to be odd and squarefree. Then the basis B is a normal integral basis, by the Hilbert-Speiser theorem. Hence for any prime q that splits completely in the extension F_H, the minimal polynomial of α has distinct roots modulo q, and the same analysis for the cyclotomic fields will show that the [ELOS] attack will not work for this field (demonstrating one bad basis is enough).

Next: what if $r > \sqrt{n}$ or if m is not square free?

22. Playing with matrices

Set up some notations. Let v be a chosen integral basis of $\mathcal{O}_K$ and let $A = A_v$ denote the emedding matrix of v. i.e., $A_v[i,j] = \sigma_i(\omega_j)$. Let $A = U\Sigma V$ be its singular value decomposition. Then we have

$$A^{-1} = V^* \Sigma^{-1} U^*.$$

Let $\lambda_1 \geq \cdots \geq \lambda_n$ denote the singular values of A. In our case we will prove that U, V actually are real orthogonal matrices. Thus we could think of the error vector as

$$E = \omega_1(v_{11}\lambda_1^{-1}x_1 + \cdots + v_{n1}\lambda_n^{-1}x_n) + \cdots + \omega_n(v_{1n}\lambda_1^{-1}x_1 + \cdots + v_{nn}\lambda_n^{-1}x_n).$$

We describe the **"$a = 0$ attack"**: Suppose we have a map $\pi : \mathcal{O}_K \to \mathbb{F}_q$ such that $\pi(\omega_i) = 0$ for all $2 \leq i \leq n$. Then only the first term matters, and if we can prove that it is small compared to q, then this would give a possible attack on the decision version of the RLWE problem.

23. Some conclusions

- 2-power cyclotomics seems secure to [ELOS] attack.
- LWE is at least as hard as RLWE, we can get LWE instances from RLWE, and the search version can be solved with runtime polynomial in n when q is large.
- For general number fields, the variance depends on the embedding matrix A. New covariance matrix is AA^*.
- We can use the singular value decomposition of A to study the situation, a good basis means that the smallest singular value of A is not too small.
- Subfields of cyclotomic fields seems secure.
- Modulus switching is a technique where
$$newerror = (q'/q) \cdot olderror + (extra)$$
The key to use it for the attack is to bound the extra term.
- prime cyclotomics are vulnerable for $q = p$ (due to squareroot cancellation and evaluation at 1). However, since p is a ramified prime, the search-to-decision reduction does not work.

24. Relook at ramified attack

First, write everything in $\mathcal{O}_K$ uniquely as
$$e = \sum_{i=0}^{p-1} e_i \zeta^i$$
with $\sum e_i \in (-p/2, p/2)$. Then the Minkowski embedding of e has length $||\sigma(e)||_2 = \sqrt{(p-1)\sum e_i^2 - 2\sum_{i<j} e_i e_j} = \sqrt{(p+1)\sum e_i^2 - (\sum_i e_i)^2}$.

What if half of the e_i's are 1? Then what happens is the embedding length is $\sqrt{(p+1)p/2 - p^2/4}$, which is about $p/\sqrt{2}$. We want to make sure that these vectors do not occur. So the standard deviation can not be too large.

In particular, suppose v is a short vector in $\sigma(\mathcal{O}_K)$, then v has a representation where $||e||_2 = ||v||/\sqrt{p+1}$,

25. Remarks on the sampler used in [ELOS] attack

To guarantee that the current implementation of discrete Gaussian lattice sampler in sage gives the correct result, it is required (See [GPV], theorem 4.1) that

$$s \geq ||\tilde{B}||\omega(\log(n)).$$

where $s = 2\pi\sigma$, and $||\tilde{B}||$ denotes the maximum length of the gram-schmidt vectors $||\tilde{b_i}||$.

In [ELOS], the discriminant adjustment is $\sqrt{n}(q-1)^{\frac{n-1}{2n}}$, and $||\tilde{B}|| = \sqrt{n}(q-1)^{n-1/n}$. So if we take $\sigma = O(1)$, then s is about the size of square root of $||\tilde{B}||$, so we can not guarantee that the lattice sampler will give correct results. There is also not enough room to increase s to the magnitude of $||\tilde{B}||$, since it is already greater than q. We could still run it, though, and hope for the best.

26. Discrete Gaussians

27. Prime cyclotomics: some lemmas on l_2 norms

Fact: for p cyclotomics where p is prime, an element

$$e = e_0 + \cdots + e_{p-2}\zeta_p^{p-2}$$

has l_2 norm

$$f(e_0, \cdots, e_{n-1}) = p(\sum_i e_i^2) - (\sum e_i)^2.$$

We make some observations on the plane

$$\sum_i e_i = k.$$

First, the mod p map is constant on this plane (equal to $k \pmod{p}$.). Second, if we want to minimize this l_2 norm, the all the e_i's must have the same sign; suppose not, then I have $(a, -b)$; where $a \geq b > 0$; then I can replace this pair by $(a - b, 0)$ and this keeps k invariant but decreases the l_2 norm, since

$$a^2 + (-b)^2 \geq (a - b)^2.$$

The next fact is: if $a, b \in \mathbb{Z}_{\geq 0}$, then $(a + b)^2 \geq a^2 + b^2$. This means we could 'split' any $e_i > 0$ as e_i-copies of one's and decrease the l_2 norm (WARNING: this part is not clear). So we arrive at the conclusion that

Lemma 27.1. *Let $k \geq 0$ be an integer. Then $\min_{e \in \mathbb{Z}^n : \sum_i e_i = k} l_2(e) = \sqrt{pk - k^2}$. The minimum is achieved by, for example, $1 + \zeta_p + \cdots + \zeta_p^{k-1}$.*

So if I want to get to $p/2$, the l_2-norm has to be greater than $p/2$. If I want to get to p/r, the l2 norm will have to be larger than $\frac{p}{r}\sqrt{r-1}$

In other words, if we can bound the l_2 norm by a constant smaller than $p/2$, then theoretically, we are good. We do need to verify that this can be achieved with the element $\{\alpha a\}s$. Using a partial Babai or discrete Gaussian sampling, we probably could hope to get $|\{\alpha a\}|_2$ small, but maybe not too small; then we need to bound $||s||_\infty$, which is the input. Well then, blah blah blah...