Internship Report, second version

Generalizing Algebraic Algorithms for Group-LWE

Author:
Xiaxi Ye

Supervisor:
Phong Q. Nguyen

Institute for Interdisciplinary Information Sciences
Tsinghua University

July 2022

Chapter 1

Structural Lattice Reduction and Generalizing Lattice Problems

1.1 Structural Lattice Reduction

GINX16 proposes structural lattice reduction which is a generalization of lattice reduction. Instead of finding a short basis of the original given lattice in lattice reduction, in structural lattice reduction, we are expected to find a short basis of the overlattice $\bar{L}$ of L, where $\bar{L}/L \simeq G$ and G is a given finite abelian group. Then we define the generalized lattice problems, namely Group-SIS and Group-LWE. As a result, structural lattice reduction genralizes the worst-case to average-case reductions for SIS and LWE to Group-SIS and Group-LWE.

Furthermore, through structural lattice reduction, we can view hidden number problem(HNP) as a special case of LWE by generalizing the corresponding finite abelian group from a cyclic group $\mathbb{Z}_q$ to a group $\mathbb{Z}_q^n$ which is a production of the same cyclic groups. Also, due to the fact that average-case bounded distance problem(BDD) corresponding to the lattice L is exactly the Group-LWE corresponding to the dual lattice L', then we can apply algorithms for Group-LWE to solve average-case BDD.

1.2 Generalizing Lattice Problems

Now we begin to define the generalized lattice problems.

1.2.1 Discretized Group-LWE

Parameters about a Discretized Group-LWE are as follows:

- an explicit finite Abelian group $G = \bigoplus_{k=1}^{n} \langle e_k \rangle$, where e_k has order $q_k = p_k^{\alpha_k}$, $\forall 1 \le k \le n$, (Assume p_k are distinct prime numbers and $p_1 < \cdots < p_n$.)
- a secret $\hat{s} \in \widehat{G}$, where the dual group $\widehat{G} := \mathrm{Hom}(G, \mathbb{T})$,
- the standard deviation α of the Gaussian distribution and an extra integer M for discretization.

Now we denote by $\bar{A}_{G,\alpha,M}(\hat{s})$ the distribution over $G \times \mathbb{T}$ obtained by choosing $a \in G$ uniformly at random, setting $b \leftarrow \mathscr{D}_{\mathbb{T}',\alpha,\hat{s}(a)}$ and outputting $(a,b) \in G \times \mathbb{T}$, where $\mathbb{T}' = \frac{1}{M}\mathbb{Z}/\mathbb{Z}$ and choosing $a \in G$ uniformly at random means choosing $a_k \in \mathbb{Z}_{q_k}$ uniformly at random for all $1 \le k \le n$ and setting $a = \sum_{k=1}^{n} a_k e_k$. Then Search-DGLWE$_{G,\alpha,M}(\mathscr{S})$ asks to find $\hat{s}(= \sum_{k=1}^{n} s_k \hat{e}_k$, i.e. find each $s_k \in \mathbb{Z}_{q_k}$) from $\bar{A}_{G,\alpha,M}(\hat{s})$ for a fixed $\hat{s} \leftarrow \mathscr{S}$ (a known distribution over $\widehat{G}$) given many independent samples.

1.2.2 Group-SIS

Parameters about GSIS are defined as follows:

- a finite abelian group G, a positive integer m,
- a bound $\beta \in \mathbb{R}_{\ge 0}$,
- a vector $\mathbf{g} = (g_1, \cdots, g_m)$ such that $g_i \in G, \forall 1 \le i \le m$.

Then GSIS asks us to find a vector $\mathbf{x} \in \mathbb{Z}^m$ satisfying that $\sum_{i=1}^{m} x_i g_i = 0$, where we define that $ng = \overbrace{g + \cdots + g}^{n\text{times}}$ (i.e. we view G as a $\mathbb{Z}$-module). Intuitively, GSIS is targerted to find a short vector in the lattice $\mathscr{L}_{\mathbf{g}} = \{\mathbf{x} \in \mathbb{Z}^m \text{s.t.} \sum_{i=1}^{m} x_i g_i = 0\}$.

CHAPTER 2

WARM-UP: USING INTERSECTION TO SOLVE GLWE

2.1 Solving Group-LWE using Intersection

2.1.1 Basic Background

GINX16 defines generalized LWE problem, namely Group-LWE problem. We want to extend A-G algorithm for LWE to a more generalized algorithm solving Group-LWE and then an algebraic algorithm for BDD. However, as the finite Abelian group associated with G-LWE changes from a special case $G = \mathbb{Z}_q^n$ to a general case $G = \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_n}$, the number of possibilities for linearized new variables increases from a polynomial in n to an exponent of n, which may lead to a larger sampling complexity and make our generalized A-G algorithm inefficient.

For this reason, we start with an extreme example and see how sampling complexity changes from the simple case to the general case. Now we state the basic notations used in this note as follows. In GLWE, we set the noise's distribution to be an arbitrary distribution over a small set rather than the Gaussian distribution:

- G of order n is the explicit finite Abelian group for GLWE,
- $\hat{s} \in \hat{G}$ is the secrete, where $\hat{G} := \mathrm{Hom}(G, \mathbb{T})$ is the dual group,
- $E = \{f_1, f_2, \cdots, f_d\}$ of size d is the set of all possible noises and $\mathscr{S}$ is a distribution over E where each noise e is sampled.
- m is the sampling complexity and the ith $(1 \le i \le m)$ sample gives us $b_i = \hat{s}(a_i) + e_i$, where $a_i \leftarrow_{\$} G$ and $e_i \leftarrow_{\mathscr{S}} E$.

2.1.2 Simple Example when $n = 1$ and $G = \mathbb{Z}_q$

Suppose $q = \prod_{l=1}^{k} p_l^{\alpha_l}$, where $p_l, 1 \le l \le k$ are distinct prime numbers and $\alpha_l \ge 1$. First we construct the polynomial according to the noise constraint

$$P(x) = \prod_{j=1}^{d}(x - f_j).$$

We substitute x with $e_i = b_i - a_i \times z$ and get

$$P(b_i - a_i \times z) = \prod_{j=1}^{d}(b_i - a_i \times z - f_j).$$

Applying the fact that $b_i = a_i \times s + e_i$, we get

$$P(a_i \times (s-z) + e_i) = \prod_{j=1}^{d}(a_i \times (s-z) + e_i - f_j). \tag{2.1}$$

Notice each sampling gives us such a constraint of z. Now we view (2.1) as a polynomial $H_i(s-z)$ in $y := s - z$ and suppose the polynomial H_i according to the ith sampling leads to a set F_i consisting all solutions satisfying $H_i(y) = 0$ (i.e. $F_i = \{y \in \mathbb{Z}_q | H_i(y) = 0\}$). Then our goal is to prove with m samples,

$$\cap_{i=1}^{m} F_i = \{0\}$$

with high probability. Now we compute this probability as follows. Consider a single equation

$$a_i \times y = f_j - e_i, 1 \le j \le d.$$

Now we suppose $f_j - e_i = x_{i,j}$. Then we have that

$$y = \frac{x_{i,j}}{(a_i, x_{i,j})}[\frac{a_i}{(a_i, x_{i,j})}^{-1}(\text{mod } \frac{q}{(a_i, x_{i,j}, q)})] + k\frac{q}{(a_i, x_{i,j}, q)},$$

if $(\frac{a_i}{(a_i,x_{i,j})}, \frac{q}{(a_i,x_{i,j},q)}) = 1$. Otherwise, there are no solutions. Observe that there are $(\frac{q}{(a_i,x_{i,j},q)} - 1)$ numbers between two adjacent solutions according to the same $x_{i,j}$. Thus, by union bound, we get

$$\Pr_{e_i \leftarrow_{\mathscr{S}} E}\{r \in F_i\} \le \sum_{j=1}^{d} \frac{(a_i, x_{i,j}, q)}{q} \le \sum_{j=1}^{d} \frac{(a_i, q)}{q} \le \frac{d(a_i, q)}{q}.$$

Furthermore, note that

$$\mathbb{E}_{a_i \leftarrow_{\S} \mathbb{Z}_q}[(a_i, q)] = \prod_{l=1}^{k}(1 \times \frac{p_l - 1}{p_l} + p_l \times \frac{p_l - 1}{p_l^2} + \cdots + p_l^{\alpha_l - 1} \times \frac{p_l - 1}{p_l^{\alpha_l}} + p_l^{\alpha_l} \times \frac{1}{p_l^{\alpha_l}}) < \prod_{l=1}^{k}(\alpha_l + 1).$$

Then we have

$$\mathbb{E}_{a_i \leftarrow_{\S} \mathbb{Z}_q}[\Pr_{e_i \leftarrow_{\mathscr{S}} E}\{r \in F_i\}] < \frac{d \prod_{l=1}^{k}(\alpha_k + 1)}{q}.$$

Since samples are mutually independent, we get

$$\mathbb{E}_{a_1,\cdots,a_m\leftarrow_{\S}\mathbb{Z}_q^m}[\Pr_{e_i\leftarrow_{\mathscr{S}}E}\{r\in\cap_{i=1}^m F_i\}]<(\frac{d\prod_{l=1}^k(\alpha_k+1)}{q})^m.$$

And thus,

$$\mathbb{E}_{a_1,\cdots,a_m\leftarrow_{\S}\mathbb{Z}_q^m,e_i\leftarrow_{\mathscr{S}}E}[\#\cap_{i=1}^m F_i]<(\frac{d\prod_{l=1}^k(\alpha_l+1)}{q})^m(q-1)+1<2,$$

where $m>\frac{\log q}{\log\frac{q}{d\prod_{l=1}^k(\alpha_k+1)}}$.

2.1.3 General Example

In this subsection, we consider the case where $G=\mathbb{Z}_{q_1}\times\cdots\times\mathbb{Z}_{q_n}$, $q_l=p_l^{\alpha_l}$ and $p_l(1\leq l\leq n)$ are distinct prime numbers. To simplify the analysis, we suppose $E\subset\frac{1}{M}\mathbb{Z}/\mathbb{Z}$, where $M=\prod_{j=1}^n q_j$. Similarly, we first construct a polynomial for noise constraint

$$P(x)=\prod_{j=1}^d(x-f_j).$$

Then by substituting $e_i=b_i-\hat{z}(a_i)$ with x and applying $b_i=\hat{s}(a_i)+e_i$, we get

$$P((\hat{s}-\hat{z})(a_i)+e_i)=\prod_{j=1}^d((\hat{s}-\hat{z})(a_i)+e_i-f_j).$$

By setting $\hat{s}=\sum_{l=1}^n s_k\hat{e_l},\hat{z}=\sum_{l=1}^n z_l\hat{e_l}$ and $a_i=\sum_{l=1}^n a_{i,l}e_l$, $0\leq s_l,z_l,a_{i,l}<q_l$, we have

$$P(\sum_{l=1}^n\frac{(s_l-z_l)a_{i,l}}{q_l}+e_i)=\prod_{j=1}^d(\sum_{l=1}^n\frac{(s_l-z_l)a_{i,l}}{q_l}+e_i-f_j). \tag{2.2}$$

Also, we set $\hat{y}=\hat{s}-\hat{z}$ and view (2.2) as a polynomial $H_i(y)$ in y. Then this polynomial gives a set F_i of solutions satisfying H_i. Then we can prove given $\hat{r}\in\hat{G},\hat{r}\neq 0$,

$$\mathbb{E}_{a_i\leftarrow_{\$}G}[\Pr_{e_i\leftarrow_{\mathscr{S}}E}\{\hat{r}\in F_i\}]\leq\frac{d^n}{\prod_{l=1}^n q_l}\prod_{l=1}^n(\alpha_l+1).$$

Hence, we have

$$\mathbb{E}_{a_1,\cdots,a_m\leftarrow_{\$}G^m}[\Pr_{e_i\leftarrow_{\mathscr{S}}E}\{\hat{r}\in\cap_{i=1}^m F_i\}]=(\frac{d^n}{\prod_{l=1}^n q_l}\prod_{l=1}^n(\alpha_l+1))^m.$$

And thus we claim

$$\mathbb{E}_{a_1,\cdots,a_m\leftarrow_{\$}G^m,e_i\leftarrow_{\mathscr{S}}E}[\#\cap_{i=1}^m F_i]=(\frac{d^n\prod_{l=1}^n(\alpha_l+1)}{\prod_{l=1}^n q_l})^m(\prod_{l=1}^n p_l-1)+1=(\frac{d^n\prod_{l=1}^n(\alpha_l+1)}{M})^m(M-1)+1<2,$$

if $m>\frac{\log M}{\log M-\log(d^n\prod_{l=1}^n(\alpha_l+1))}$. If we set $M=q^n,\alpha^n=\prod_{l=1}^n(\alpha_l+1)$, then we get

$$\frac{\log M}{\log M-n\log d\alpha}=\frac{\log q}{\log q-\log(d\alpha)},$$

which is similar to that in the case where $n = 1$. Moreover, according to the method mentioned in Polynomial complexity of solving systems of few algebraic equations with small degrees, it promises the solvability of such a polynomial system with small degrees can be tested in $\mathsf{poly}(\prod_{l=1}^{n} p_l, n^{d^{3m}})$ time, which is a polynomial in n if d and m are fixed. Note that if we define a new polynomial system as follows

$$Q_i(\hat{z}) = P((\hat{s}-\hat{z})(a_i)+e_i) = \prod_{1\le j\le d, j\ne j_i} ((\hat{s}-\hat{z})(a_i)+e_i-f_j), \tag{2.3}$$

where $e_i = f_{j_i}, 1 \le i \le m$. Then the original polynomial system has no solutions other than $\hat{z} = \hat{s}$ if the new polynomial system has no solutions.

CHAPTER 3

GENERALIZING ARORA-GE ALGORITHMS FOR GLWE

3.1 Generlized Arora-Ge Algorithm for Discretized-GLWE

Similar to Arora-Ge algorithm proposed in AG11 for LWE, we first construct a polynomial $P(\eta)$ for discrete Gaussian noise as

$$P(\eta) = \eta \prod_{i=1}^{\frac{D-1}{2}} (\eta - \frac{i}{M})(\eta + \frac{i}{M}).$$

The reason why we can set $D = k\alpha M$ here is that Gaussian distribution gives us a narrow noise:

$$\Pr_{\eta \sim \Psi_\alpha}\{|\eta| > k\alpha q\} \leq e^{-O(k^2)}.$$

For each sample (a,b), now we assume

$$b = \hat{z}(a) + \eta.$$

And our goal is to derive that $\hat{z} = \hat{s}$ is the unique solution when the number of samples is large enough. After substituting η with $b - \hat{z}(a)$, we have

$$P(b - \hat{z}(a)) = (b - \hat{z}(a)) \prod_{i=1}^{\frac{D-1}{2}} (b - \hat{z}(a) - \frac{i}{M})(b - \hat{z}(a) + \frac{i}{M}).$$

Furthermore, by using the fact

$$b = \hat{s}(a) + \eta,$$

we get

$$P((\hat{s} - \hat{z})(a) + \eta) = ((\hat{s} - \hat{z})(a) + \eta) \prod_{i=1}^{\frac{D-1}{2}} ((\hat{s} - \hat{z})(a) + \eta - \frac{i}{M})((\hat{s} - \hat{z})(a) + \eta + \frac{i}{M}). \tag{3.1}$$

To take advantage of the variant of Schwartz-Zippel Lemma, we view (1) as a polynomial on a chosen from G at random by linearizing $(\hat{s}-\hat{z})$. In particular, we set

$$\hat{s}=\sum_{i=1}^{n} s_i\hat{e_i}, \hat{z}=\sum_{i=1}^{n} z_i\hat{e_i}, a=\sum_{i=1}^{n} a_i e_i.$$

Then we get

$$P(\sum_{i=1}^{n}(s_i-z_i)a_i+\eta)=(\sum_{i=1}^{n}(s_i-z_i)a_i+\eta)\prod_{i=1}^{\frac{D-1}{2}}(\sum_{i=1}^{n}(s_i-z_i)a_i+\eta-\frac{i}{M})(\sum_{i=1}^{n}(s_i-z_i)a_i+\eta+\frac{i}{M}). \tag{3.2}$$

Now we linearize the polynomial (2) and get

$$L(P(\sum_{i=1}^{n}(s_i-z_i)a_i+\eta))=0. \tag{3.3}$$

In particular, we replace each monomial $\prod_{i=1}^{n} z^{u_i}$ with a single variable y_u. Then the number of variables is $N=\binom{n+D}{n}$. With similar indexing, we denote $\prod_{i=1}^{n}(s_i-z_i)^{v_i}$ by $\tilde{y}_v$. We can easily prove there exists an invertible matrix M_s such that $\tilde{y}=M_s y$, where $\tilde{y}$ (y) is a vector with its components to be $\tilde{y}_v$ (y_u) that are sorted by their degrees in ascending order. And thus we know $\tilde{y}_{e_i}\neq 0$ iff $y_{e_i}\neq s_i$, $\forall 1\le i\le n$. Furthermore, we denote by $\tilde{Y}_k$ the vector of n^k components indexed by $w\in[n]^k$. And define $v(w)\in\mathbb{Z}^n$ as $v(w)_i=\mathrm{card}\{1\le j\le k|w_j=i\}$. Then $\tilde{Y}_w^k=\tilde{y}_{v(w)}$. Note Gaussian distribution gives us

$$\Pr_{\eta\sim\Psi_\alpha}\{\eta=0\}=\Omega(1/\alpha M).$$

Letting $\eta=0$, we rewrite (3) as

$$\sum_{i=1}^{D} c_i(a^{\otimes i}\cdot\tilde{Y}^i)=0, \tag{3.4}$$

where $c_i(1\le i\le D)$ are the coefficients in $P(\eta)$. We can prove (4) is not an identically zero polynomial if $\hat{z}\neq\hat{s}$. Now we apply the variant of Schwartz-Zippel lemma stated in the following and get that the probability that a random assignment of a makes (4) equal to 0 is at most $\frac{D}{p_1}$ $(D<p_1)$.

Lemma 3.1. *Let $P(x_1,\cdots,x_n)$ be a polynomial of degree d, such that P is not a zero polynomial. Let S_i be the set of numbers from which a_i is drawn uniformly at random, $\forall 1\le i\le n$. Then we have*

$$Pr_{a_1,\cdots,a_n}\{P(a_1,\cdots,a_n)=0\}\le\frac{d}{min_{1\le i\le n}\{|S_i|\}}.$$

This lemma can be proved similarly to the original Schwartz-Zippel lemma by induction on n. Supposing the number of sampled constraints is $X=\alpha M p_1 \log(\prod_{i=1}^{n} p_i)2^n$, now we combine all the probabilities. For every candidate $\tilde{y}$ with $\tilde{y}^1\neq 0$, the probability that $\tilde{y}$ satisfies a randomly sampled constraint is at most

$$1-\frac{1}{\alpha M p_1}.$$

Then the probability that $\tilde{y}$ satisfies all X randomly samples constraints is at most

$$(1-\frac{1}{\alpha M p_1})^X.$$

By uninon bound, the probability that at least one incorrect solution satisfies all X constraints is at most

$$P(1-\frac{1}{\alpha M p_1})^X,$$

where $P=(\prod_{i=1}^n p_i)^{2^{n-1}}$ is the number of all possibilities of y. Hence, we get the probability that no incorrect solution satisfy all X constraints is at least

$$1-P(1-\frac{1}{\alpha M p_1})^X \geq 1-(\prod_{i=1}^n p_i)^{-2^{n-1}},$$

which is a high probability.

CHAPTER 4

GENERALIZING BLEICHENBACHER'S ALGORITHMS FOR GLWE

4.1 Generalizing Bleichenbacher's algorithm for GLWE

4.1.1 Bias

The following generalized algorithm follows the algorithm in MHMP13 which solves Hidden Number Problem originally. Recall the definition of the bias of a random variable over $\mathbb{Z}/q\mathbb{Z}$.

Definition 4.1. Let X be a random variable over $\mathbb{Z}/q\mathbb{Z}$. The bias of X is defined as

$$B_q(X) = E(e^{2\pi i X/q}).$$

And the sampled bias of $V = \{v_0, v_1, \cdots, v_{L-1}\}$ in $\mathbb{Z}/q\mathbb{Z}$ is defined as

$$B_q(V) = \frac{1}{L}\sum_{j=1}^{L} e^{2\pi i v_j/q}.$$

Moreover, if X is a random variable over $\mathbb{T} = \frac{1}{M}\mathbb{Z}/\mathbb{Z}$ (M is the parameter for discretizing Gaussian distribution), then we define the bias of X as

$$B(X) = E(e^{2\pi i X}).$$

And the sampled bias of $V = \{v_0, v_1, \cdots, v_{L-1}\}$ in $\mathbb{T}$ is defined as

$$B_q(V) = \frac{1}{L}\sum_{j=1}^{L} e^{2\pi i v_j}.$$

Similarly, we still have the follwoing lemma.

Lemma 4.1. *Let $0 < T \leq N$ be a bound such that X is uniformly distributed on the interval $[-(T-1)/2M, \cdots, (T-1)/2M]$. Then:*

- *a. For independent random variable X and X', $B(X+X') = B(X)B(X')$.*
- *b. $B(X) = \frac{1}{T}\frac{\sin(\pi T/M)}{\sin(\pi/M)}$. Hence, $B(X)$ is real-valued with $0 \le B(X) \le 1$.*
- *c. If X is uniformly distributed on the interval $[0/M, 1/M, \cdots, (M-1)/M]$, then $B(X) = 0$.*
- *d. Let a be an integer with $|a|T \le M$, and $Y = aX$. Then $B(Y) = \frac{1}{T}\frac{\sin(\pi aT/M)}{\sin(\pi a/M)}$.*
- *e. $B(Y) \le B(X)^{|a|}$.*

4.1.2 Connecting the GLWE to the Bias

To see how the bias helps solve the GLWE, we show three good properties of it.

4.1.2.1 Finding the secret by maximization

We can define a bias such that if our guess of the secret is correct, then the smapled bias is significantly nonzero. However, for any incorrect guess, we get a relatively small sampled bias. In particular, let $V_{\hat{w}} = \{b_j - \hat{w}(a_j) \bmod 1\}_{j=1}^{L}$, where $\hat{w} \in \hat{G}$ is a guess of the secret. Computing the sampled bias of $V_{\hat{w}}$, we get

$$\begin{aligned}
B(V_{\hat{w}}) &= \frac{1}{L}\sum_{j=1}^{L} e^{2\pi i(b_j - \hat{w}(a_j))} \\
&= \frac{1}{L}\sum_{j=1}^{L} e^{2\pi i b_j} e^{-2\pi i \hat{w}(a_j)} \\
&= \sum_{t\in G}\Big(\frac{1}{L}\sum_{\{j|a_j=t\}} e^{2\pi i b_j}\Big)e^{-2\pi i \hat{w}(t)} \\
&= \sum_{t\in G}\Big(\frac{1}{L}\sum_{\{j|a_j=t\}} e^{2\pi i (b_j - \hat{s}(t))}\Big)e^{-2\pi i (\hat{w}(t)-\hat{s}(t))} \\
&= \sum_{t\in G}\Big(\frac{1}{L}\sum_{\{j|a_j=t\}} e^{2\pi i e_j}\Big)e^{-2\pi i (\hat{w}(t)-\hat{s}(t))}. \qquad (4.1)
\end{aligned}$$

In GLWE, we are given an explicit finite Abelian group $G = \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_n\mathbb{Z}$ and a set of pairs $(a_j, b_j), 1 \le j \le L$, and we wish to find the secret and presumably unique $\hat{w}$ for which the set of values $V_{\hat{w}}$ all fall near 0 or 1. Then if $\hat{w} = \hat{s}$, we have $B(V_{\hat{w}}) = \frac{1}{L}\sum_{j=1}^{L} e^{2\pi i e_j}$ which is the sampled bias of the error points $(e_1, \cdots, e_L)$. Given enough samples, $B(V_{\hat{w}})$ will have a value close to 1, as the points $e^{2\pi i e_j}$ are confined to the part of the unit circle with small phase. $B(V_{\hat{w}})$ will be close to zero for any other value of $\hat{w}$. as the points will be scattered around the unit circle by the $e^{-2\pi i(\hat{w}(t)-\hat{s}(t))}$ terms. Thus, we are able to enumerate $\hat{w}$ to maximize $B(V_{\hat{w}})$ to find the secret $\hat{s}$.

Theorem 4.1. *With high probability, $B(V_{\hat{w}})$ is maximized by a unique value of $\hat{w}$ which is $\hat{s}$ exactly.*

4.1.2.2 Searching in a sparse space

Notice in (1), $B(V_{\hat{w}})$ is a sum of terms $e^{2\pi i\hat{w}(t)} = e^{2\pi i \sum_{k=1}^{n} \frac{w_k t_k}{q_k}}$, with frequency $\frac{t_k}{q_k}$ for each $w_k (1 \le k \le n)$. Hence, if those frequencies are much smaller than 1 (i.e. t_k are small relative to q_k), then the peak of $B(V_{\hat{w}})$ will be broad, which makes it possible for us to search in an evenly spaced values that are sparse. In particular, we set $0 \le a_{j,k} < C_k, \forall 1 \le k \le n, 1 \le j \le L$. And we approximately maximize $B(V_{\hat{w}})$ by calculating the values of $B(V_{\hat{w}_{\boldsymbol{v}}})$ and then choosing $\hat{w}_{\boldsymbol{v}}$ at which $B(V_{\hat{w}_{\boldsymbol{v}}})$ is maximized, where

$$\hat{w}_{\boldsymbol{v}} = \sum_{k=1}^{n} \frac{v_k}{d_k} q_k \hat{e}_k, \boldsymbol{v} \in [0, d_1 - 1] \times [0, d_2 - 1] \times \cdots \times [0, d_n - 1], d_k = \max(p_k^{D_k}, 2C_k), \forall 1 \le k \le n.$$

Theorem 4.2. *Let* $d_k = \max(p_k^{D_k}, 2C_k), 1 \le k \le n$. *Then with high probability,* $msb_{D_k}(s_k) = msb_{D_k}(\frac{v_k}{d_k} q_k), \forall 1 \le k \le n$, *where* $\hat{w}_{\boldsymbol{v}} = \sum_{k=1}^{n} \frac{v_k}{d_k} q_k \hat{e}_k$ *and* $B(V_{\hat{w}_{\boldsymbol{v}}})$ *is maximal.*

4.1.2.3 Using multidimensional FFT to compute efficiently

Now we compute $B(V_{\hat{w}_{\boldsymbol{v}}})$ explicitly to show that multidimensional FFT can be applied to efficiently compute them.

$$\begin{aligned}
B(V_{\hat{w}_{\boldsymbol{v}}}) &= \frac{1}{L} \sum_{j=1}^{L} e^{2\pi i (b_j - \hat{w}_{\boldsymbol{v}}(a_j))} \\
&= \frac{1}{L} \sum_{j=1}^{L} e^{2\pi i b_j} e^{-2\pi i \sum_{k=1}^{n} \frac{v_k}{d_k} q_k a_{j,k} / q_k} \\
&= \sum_{t \in G} (\frac{1}{L} \sum_{\{j | a_j = t\}} e^{2\pi i b_j}) e^{-2\pi i \sum_{k=1}^{n} \frac{v_k}{d_k} t_k} \\
&= \sum_{t \in G} Z_{\boldsymbol{t}} e^{-2\pi i \sum_{k=1}^{n} \frac{v_k}{d_k} t_k} \\
&= \sum_{t \in G} Z_{\boldsymbol{t}} e^{-2\pi i \boldsymbol{v} \cdot (\boldsymbol{t}/\boldsymbol{d})}, \qquad (4.2)
\end{aligned}$$

where

$$Z_t = \frac{1}{L} \sum_{j | a_j = t} e^{2\pi i b_j}, \boldsymbol{t} = (t_1, \cdots, t_n), d - 1 = (d_1 - 1, \cdots, d_n - 1), \boldsymbol{t}/\boldsymbol{d} = (t_1/d_1, \cdots, t_n/d_n).$$

According to (2), we can clearly recognize that $B(V_{\hat{w}_{\boldsymbol{v}}}), \boldsymbol{v} \in [0, d_1 - 1] \times [0, d_2 - 1] \times \cdots \times [0, d_n - 1]$ are the multidimensional FFT of $Z_{\boldsymbol{t}}, \boldsymbol{t} \in [0, d_1 - 1] \times [0, d_2 - 1] \times \cdots \times [0, d_n - 1]$. Note that we can derive multidimensional FFT by applying n one-dimensional FFT, which leads to the complexity to be $O(d \log d)$ and $d = \prod_{k=1}^{n} d_k$.

4.1.3 Recovering the secret $\hat{s}$ with bounded a_j

Suppose we can compute $d = \prod_{k=1}^{n} d_k (= \prod_{k=1}^{n} p_k^{D_k})$-point multidimensional FFT, where $d_k = p_k^{D_k}, \forall 1 \le k \le n$. Then we are able to recover the high-order D_k bits of the s_k as follows for all $1 \leq k \leq n$. (Note that the bit here is defined differently as usual. For simplicity, we write w_k in p_k-number system.) First zero $Z_{\boldsymbol{t}}, \boldsymbol{t} \in [0, d_1 - 1] \times [0, d_2 - 1] \times \cdots \times [0, d_n - 1]$. Then:

- 1. Loop over all L pairs (a_j, b_j). For each pair add $e^{2\pi i b_j}$ to $Z_{\boldsymbol{t}}$, where $\boldsymbol{t} = a_j$.
- 2. Compute the multidimensional FFT of $Z_{\boldsymbol{t}}$ and find the $\boldsymbol{v}$ for which $B(V_{\hat{w}_{\boldsymbol{v}}})$ is maximal.
- 3. The most significant D_k bits of s_k are $msb_{D_k}(s_k) = msb_{D_k}(\frac{v_k}{d_k} q_k), \forall 1 \leq k \leq n$.

We can then recover the secret iteratively. Let $w_k = p_k^{u_k} w_{k,hi} + w_{k,lo}$, where $w_{k,hi}$ are known while $w_{k,lo}$ of length u_k remains to be recovered. Observe that

$$
\begin{aligned}
e_j &= b_j - \sum_{k=1}^{n} w_k a_{j,k}/q_k \bmod 1 \\
&= b_j - \sum_{k=1}^{n} (p_k^{u_k} w_{k,hi} + w_{k,lo}) a_{j,k}/q_k \bmod 1 \\
&= (b_j - \sum_{k=1}^{n} p_k^{u_k} w_{k,hi} a_{j,k}/q_k) - \sum_{k=1}^{n} w_{k,lo} a_{j,k}/q_k \bmod 1 \\
&= b'_j - \sum_{k=1}^{n} w_{k,lo} a_{j,k}/q_k \bmod 1, \qquad (4.3)
\end{aligned}
$$

where $b'_j = b_j - \sum_{k=1}^{n} p_k^{u_k} w_{k,hi} a_{j,k}/q_k, \forall 1 \leq j \leq L$.

Differently from the previous iterations, we evaluate $B(V_{\hat{w}_{\boldsymbol{v}}})$ over $d = \prod_{k=1}^{n} d_k$ evenly spaced values of $(w_1, \cdots, w_n)$ within $[0, p_1^{u_1}) \times \cdots \times [0, p_n^{u_n})$. Now we set $\hat{w}_{\boldsymbol{v}} = \sum_{k=1}^{n} q_k^{u_k} v_k/d_k, v_k \in [0, d_k - 1]$. Similar to (2), we have

$$
B(V_{\hat{w}_{\boldsymbol{v}}}) = \sum_{t \in G} (\frac{1}{L} \sum_{\{j | a_{j,k} p_k^{u_k}/q_k = t_k, \forall k\}} e^{2\pi i b'_j})\, e^{-2\pi i \boldsymbol{v} \cdot (\boldsymbol{t}/\boldsymbol{d})} = \sum_{t \in G} Z_{\boldsymbol{t}} e^{-2\pi i \boldsymbol{v} \cdot (\boldsymbol{t}/\boldsymbol{d})},
$$

where $Z_{\boldsymbol{t}} = \frac{1}{L} \sum_{\{j | a_{j,k} p_k^{u_k}/q_k = t_k, \forall k\}} e^{2\pi i b'_j}$. As before, we compute the $B(V_{\hat{w}_{\boldsymbol{v}}})$ by taking the multidimentional FFT of Z, and find the $\boldsymbol{v}$ with the maximum value for $B(V_{\hat{w}_{\boldsymbol{v}}})$. The most significant D_k bits of $w_{k,lo}$ are $msb_{D_k}(p_k^{u_k} v_k/d_k), \forall 1 \leq k \leq n$.

Previously, $a_{j,k}$ is bounded by $C_k = \frac{d_k}{2}$. Now to guarantee $a_{j,k} p_k^{u_k}/q_k$ to range between 0 and $\frac{d_k}{2}$, we relax the bound to be $C_k = \frac{d_k q_k}{q_k^{u_k+1}}$. Thus, we can derive the following theorem. Note that we can apply BKZ reduction to convert a GLWE to the bounded version of GLWE.

Furthermore, the author is still trying to use statistical technique such as central limit theorem to analyze this process obtained by applying Bleichenbacher's algorithm in a more rigid manner and to unify this with improved BKW algorithms proposed in KF15 into a single algorithm.

Chapter 5

Generalizing Algorithms for GSIS

5.1 A folklore algorithm for Group-SIS

5.1.1 From SIS to Group-SIS

In this note, we focus on l_∞ norm only. A Group-SIS problem contains the following parameters:

- an explicit finite Abelian group $G = \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_{n-1}}$, where $q_k = p_k^{\alpha_k}, \alpha_k \in \mathbb{Z}^+, \forall 1 \le k \le n-1$ and p_k's are distinct prime numbers,
- m elements $g_j = \sum_{k=1}^{n-1} A_{k,j} e_k, 1 \le m$ selected from G, $A = [A_{k,j}] \in \mathbb{Z}^{(n-1)\times m}$,
- a parameter β to bound the solution.

Then $\mathsf{GSIS}^{\infty}_{n-1,m,\beta}$ asks to find $x \in \mathbb{Z}^m$ such that $\sum_{j=1}^{m} x_j g_j = 0, ||x||_\infty \le \beta$.

5.1.2 A folklore algorithm for GSIS

Now we state a straightforward algorithm to solve GSIS, which follows a folklore algorithm solving SIS stated in the appendix in CLZ21.

Theorem 5.1. *Suppose* $s = max_{1 \le k \le n-1} \alpha_k$. *Let* $m = n^s$ *and* $\beta = \frac{\prod_{k=1}^{n-1} q_k}{2^s}$. *There is a classical algprithm that solves* $\mathsf{GSIS}^{\infty}_{n-1,m,\beta}$ *in time* $\mathsf{poly}(m)$.

Proof. Suppose $\forall 1 \le k \le n-1$,

$$v_k(t) = \begin{cases} 1, \text{if } \alpha_k \ge 1, \\ 0, \text{otherwise.} \end{cases}$$

The algorithm runs the following procedure recursively for s times. Define the initial values as $A^{(1)} := A, m^{(1)} := m, \alpha^{(1)} = \alpha$. For $1 \le i \le s$:

- 1. Partition $A^{(i)}$ in $m^{(i)}/n$ blocks, each block is an $(n-1)\times n$-dimensional matrix. In particular, we have $A^{(i)} = [A^{(i)}_1, \ldots, A^{(i)}_{m^{(i)}/n}]$.
- 2. For $1 \le j \le m^{(i)}/n$, compute a non-zero vector $z_j \in \mathbb{Z}^n$ such that
$$[A^{(i)}_j]_{k,\cdot} \cdot z_j = 0(\text{mod } p_k) \text{ if } v_k(\alpha^{(i)}) = 1 \text{ and } ||z_j||_\infty \le [\prod_{k=1}^{n-1} p_k^{v_k(\alpha^{(i)})}/2].$$
The detailed computation of this step is elaborated later.
- 3. Put $\{z_1, \cdots, z_{m^{(i)}/n}\}$ into a matrix $Y_i \in \mathbb{Z}^{m^{(i)}\times(m^{(i)}/n)}$ as follows:
$$Y_i := \begin{pmatrix} z_1 & 0 & 0 & 0 \\ 0 & z_2 & 0 & 0 \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & z_{m^{(i)}/n} \end{pmatrix},$$
Note that $\forall 1 \le k \le n-1, \quad [A^{(i)}]_{k,\cdot} \cdot Y_i = 0_{1\times m^{(i)}/n}(\text{mod } p_k)$ if $v_k(\alpha^{(i)}) = 1$ and $||Y_i||_\infty \le [\prod_{k=1}^{n-1} p_k^{v_k(\alpha^{(i)})}/2]$.
- 4. Let $\forall 1 \le k \le n-1, \alpha^{(i+1)}_k := \alpha^{(i)}_k - v_k(\alpha^{(i)}), m^{(i+1)} = m^{(i)}/n, A^{(i+1)}_{k,\cdot} := (A^{(i)}_{k,\cdot} \cdot Y^{(i)})/p_k^{v_k(\alpha^{(i)})}$. Then we run a new iteration on $A^{(i+1)}, m^{(i+1)}, \alpha^{(i+1)}$.

In the second step, for simplicity of the notations, we need to solve
$$A_{k,\cdot} \cdot z = 0(\text{mod } p_k), \forall 1 \le k \le n-1 \text{ with } v_k(\alpha^{(i)}) = 1,$$
where $A_{k,\cdot} \in \mathbb{Z}^{1\times n}, z \in \mathbb{Z}^n$. Without loss of generality, we suppose $A_{1,1} \ne 0(\text{mod } p_1)$. Initially, we set $x^0 = (1, 0, \cdots, 0)$ and $S = \{1\}$. For the kth iteration $(1 \le k \le n-1)$, if $v_k(\alpha^{(i)}) = 0$, then $x^k = x^{k-1}$. Else if $v_k(\alpha^{(i)}) = 1$, suppose $A_{k,i_k} \ne 0(\text{mod } p_k)$ and $i_k \notin S$, then we set $S \leftarrow S \cup \{i_k\}$,
$$x^k_{i_k} = [(-A_{k,i_k} \prod_{1\le r\le k-1, v_k(\alpha^{(i)})=1} p_r)^{-1} \sum_{1\le l\le n-1, l\ne k} A_{k,l} \cdot x^{k-1}_l](\text{mod } p_k) \prod_{1\le r\le k-1, v_k(\alpha^{(i)})=1} p_r$$
and
$$x^k_l = x^{k-1}_l, \forall 1 \le l \le n, l \ne i_k.$$
Then we claim
$$A_{r,\cdot} \cdot x^r = 0(\text{mod } p_r) \forall 1 \le r \le k \text{ with } v_r(\alpha^P(i)) = 1$$
and
$$||x_k||_\infty \le [\frac{\prod_{1\le d\le k, v_d(\alpha^P(i))=1} p_d}{2}].$$
Thus after $(n-1)$ iterations we get a solution $z = x^{n-1}$ for the second step.

After s iterations, we let $y := Y_1 \cdot \cdots \cdot Y_s \in \mathbb{Z}^m$ be the final GSIS solution. Then it is clear that
$$\begin{aligned} A_{k,\cdot} \cdot y &= A_{k,\cdot} \cdot Y_1 Y_2 \cdots Y_s \\ &= p_k^{v_k(\alpha^{(1)})} A^{(1)}_{k,\cdot} \cdot Y_2 \cdots Y_s \\ &= p_k^{\sum_{i=1}^s v_k(\alpha^{(i)})} v \\ &= 0(\text{mod } q_k), \forall 1 \le k \le n-1, \end{aligned}$$

and

$$||y||_\infty \leq \prod_{i=1}^{s} ||Y_i||_\infty \leq \frac{\prod_{k=1}^{n-1} p_k^{\sum_{i=1}^{s} v_k(\alpha^{(i)})}}{2^s} = \frac{\prod_{k=1}^{n-1} p_k^{\alpha_k}}{2^s}.$$

Note the total complexity is obviously poly in m. □ ■

Intuitively, the algorithm above solves GSIS in a blockwise manner. To improve the algorithm, we can try to replace the second step with a more efficient one. Moreover, we can generalize the quantum algorithm via filtering which solves SIS with infinity norm to solve GSIS.

BIBLIOGRAPHY

[1] Nicolas Gama and Malika Izabachene and Phong Q. Nguyen and Xiang Xie. Structural Lattice Reduction: Generalized Worst-Case to Average-Case Reductions and Homomorphic Cryptosystems. In *EUROCRYPT*, volume 9666 of *Lecture Notes in Computer Science*, pages 528-558. Springer 2016. Also available on *eprint*.

[2] Sanjeev Arora and Rong Ge. New Algorithms for Learning in Presence of Errors. In *Automata, Languages and Programming - 38th International Colloquium, ICALP 2011, Zurich, Switzerland, July 4-8, 2011, Proceedings, Part I,* pages 403-415, 2011.

[3] Elke De Mulder, Micheal Hutter, Mark E. Marson and Peter Pearson. Using Bleichenbacher's Solution to the Hidden Number Problem to Attack Nonce Leaks in 384-Bit ECDSA. In *CHES*, volume 8086 of *Lecture Notes of Computer Science*, pages 435-452. Springer 2013.

[4] Yilei Chen and Qipeng Liu and Mark Zhandry. Quantum Algorithms for Variants of Average-Case Lattice Problems via Filtering. In *EUROCRYPT*, volume 13277 of *Lecture Notes of Computer Science*, pages 372-401. Springer 2022. Also available in *eprint*.

[5] Paul Kirchner and Pierre-Alain Fouque. An Improved BKW Algorithm for LWE with Applications to Cryptography and Lattices. In *Advances in Cryptology-CRYPTO 2015,* pages 43-62. Speinger 2015. Also available in *eprint*.