How to meet low entropy LWE keys: SMAUG and TiGER

Changmin Lee

Korea Institute for Advanced Study

The LWE problem

$$b \equiv_q A \cdot s + e,$$

where $A \in \mathbb{Z}_q^{m \times n}, \quad s \in \mathcal{D}^n, \quad e \in \mathcal{D}^m$

- Search version: Given (A, b), find s (or e)
- Decisional version: Given samples (A, b), (either LWE or uniform), decide whether they are LWE samples or uniformly random samples

LWE-based scheme is an all-rounder?

	LWE	Wish
Computing time	$\tilde{O}(n^2)$	$\tilde{O}(n)$
Known attack time	$2^{\Omega(n)}$	$2^{\Omega(n)}$

- (Pros) LWE-based scheme is secure enough
- (Cons) It is inefficient

The sparse secret LWE problem (sLWE)

$$\Big| b \Big| \equiv_q \begin{bmatrix} & & \\ & A & \\ & & \end{bmatrix} \cdot \Big| s \Big| + \Big| e \Big|,$$

where $A \in \mathbb{Z}_q^{m \times n}$, $s \in \mathcal{S}_h^n(H.w(s) \leq h)$, $e \in \mathcal{D}^*$

- Search version: Given (A, b), find s (or e)
- Decisional version: Given samples (A, b), (either sLWE or uniform), decide whether they are sLWE samples or uniformly random samples

Relation between sLWE and LWE; hardness of sLWE

LWE of h-dimension $\leq$ sLWE

$$\begin{array}{c|c|c}
b & \equiv_q \begin{bmatrix} \\ A_0 \\ \\ \end{bmatrix} \cdot \begin{array}{|c} s \\ \\ \\ \end{array} + & e,
\end{array}$$

Relation between sLWE and LWE; hardness of sLWE

LWE of h-dimension $\leq$ sLWE

$$\left[\, b \,\right] \equiv_q \left[\, A_0 \;\; \color{red}{A_1} \,\right] \cdot \begin{bmatrix} s \\ \color{red}{0} \end{bmatrix} + \left[\, e \,\right]$$

LWE of h-dimension $\leq$ sLWE

After permutation:

$$b \; \equiv_q \; \begin{bmatrix} A \end{bmatrix} \cdot s + e$$

Relation between sLWE and LWE; weakness of sLWE

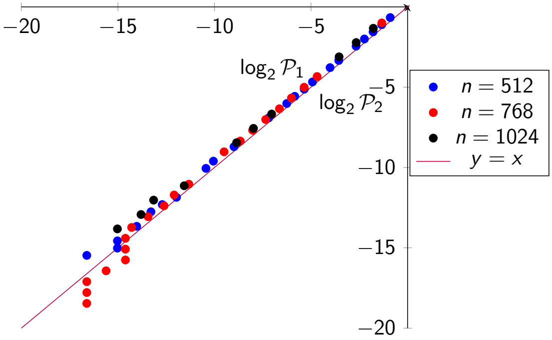
sLWE $\leq$ LWE of n-dimension : Trivial

- Lattice-based attack
  - Primal attack
  - Dual attack
- Combinatorial attack
  - MitM attack
  - BKW algorithm
- Algebraic attack
  - Arora-Ge algorithm
- Hybrid algorithm

Question: Is there an effective algorithm for sLWE?

Technical Idea: Why need more?

Main idea: $[b - A \cdot x]_q \sim \mathbb{Z}_q^m$ for $x \neq s$: $\mathcal{P}_1 = \frac{[-r,r]^m \cap \mathcal{L}}{\mathcal{L}}$, $\mathcal{P}_2 = \frac{[-r,r]^m \cap \mathbb{Z}_q^m}{\mathbb{Z}_q^m}$, $q = 3329$



Technical Idea: Why need more?

When $s \in \mathcal{S}_h^n$ and $n \sim q$, $|\mathcal{S}_h^n| = \binom{n}{h} < (q/\sigma)^h$.
It implies that an LWE sample (A, b) has a unique solution s such that

$$b \equiv_q \begin{bmatrix} A \end{bmatrix} \cdot s + e,$$

where $A \in \mathbb{Z}_q^{h \times n}$, $s \in \mathcal{D}^n$, $e \in \mathcal{D}^h$.

Desired samples with concrete parameters*

Scheme	λ	n	q	h	m
TiGER	128	512	256	128	73
	192	1024	256	84	74
	256	1024	256	198	127
SMAUG	128	512	1024	140	56
	192	768	2048	198	73
	256	1280	2048	176	85

* $\sigma = 5$

How to solve the sLWE? (Another reduction)

- Previous reduction: (n, h)-sLWE $\leq$ LWE
- New reduction: (n, h)-sLWE $\leq (n^*, h^*)$-sLWE where $n^* \leq n$ and $h^* \leq h$

Current problem:
Given $\bar{A} = (b \| A) \in \mathbb{Z}^{m \times (n+1)}$ and q, find $\bar{s}$ such that $\bar{A} \cdot \bar{s} \equiv_q e$:

$$L = \left\langle \begin{pmatrix} I_{n+1} & \\ \bar{A} & qI_h \end{pmatrix} \right\rangle \ni \begin{pmatrix} \bar{s} \\ e \end{pmatrix}$$

How to solve the sLWE? (Another reduction)

- Previous reduction: (n, h)-sLWE $\leq$ LWE
- New reduction: (n, h)-sLWE $\leq (n^*, h^*)$-sLWE where $n^* \leq n$ and $h^* \leq h$

Current problem:
Given $\bar{A} = (A_0 \| A_1)$ and q, find $(s_0 \| s_1)$ such that $A_0 \cdot s_0 + A_1 \cdot s_1 \equiv_q e$:

$$L = \left\langle \begin{pmatrix} I_{n-d+1} & & \\ & I_d & \\ A_0 & A_1 & qI_m \end{pmatrix} \right\rangle \ni \begin{pmatrix} s_0 \\ s_1 \\ e \end{pmatrix}$$

How to solve the sLWE? (Another reduction)

- Previous reduction: (n, h)-sLWE $\leq$ LWE
- New reduction: (n, h)-sLWE $\leq (n^*, h^*)$-sLWE where $n^* \leq n$ and $h^* \leq h$

Current problem:
Given $A_0 \in \mathbb{Z}^{m \times (n-d+1)}$ and B, find s_0 such that $A_0 \cdot s_0 \equiv_B s_1'$:

$$L = \left\langle \begin{pmatrix} I_{n-d+1} & \\ A_0 & B \end{pmatrix} \right\rangle \ni \begin{pmatrix} s_0 \\ s_1' \end{pmatrix}, \quad B = \begin{pmatrix} I_d & \\ A_1 & qI_m \end{pmatrix}, s_1' = \begin{pmatrix} s_1 \\ e \end{pmatrix}$$

How to solve the sLWE? (Another reduction)

- Previous reduction: (n, h)-sLWE $\leq$ LWE
- New reduction: (n, h)-sLWE $\leq (n^*, h^*)$-sLWE where $n^* \leq n$ and $h^* \leq h$

Current problem:
Given $A_0 \in \mathbb{Z}^{m\times(n-d+1)}$ and B, find s_0 such that $A_0 \cdot s_0 \equiv_B s_1'$:

$$L = \left\langle \begin{pmatrix} I_{n-d+1} & \\ A_0 & B \end{pmatrix} \right\rangle \ni \begin{pmatrix} s_0 \\ s_1' \end{pmatrix}, \quad B = BKZ_\beta\left(\begin{pmatrix} I_d & \\ A_1 & qI_m \end{pmatrix}\right), s_1' = \begin{pmatrix} s_1 \\ e \end{pmatrix}$$

Note: BKZ algorithm

Definition (Geometric Series Assumption.)

After BKZ-β reduction on basis B of $\mathcal{L}$, we have

$$\|v_i^*\| = \delta_\beta^{2(1-i)} \cdot \|b_1\| = \delta_\beta^{n+1-2i} \cdot \det(\mathcal{L})^{1/n}.$$

$$B = BKZ_\beta\left(\begin{pmatrix} I_d & \\ A_1 & qI_m \end{pmatrix}\right) = Q \cdot \begin{pmatrix} \|v_1^*\| & \cdots & * \\ & \ddots & \vdots \\ & & \|v_n^*\| \end{pmatrix}, \text{ where } Q \in O(n)$$

After reduction

Scheme	λ	β	n	n^*	h^*
TiGER	128	329	512	256	64
	192	578	1024	772	63
	256	523	1024	628	121
SMAUG	128	375	512	292	80
	192	469	768	372	96
	256	613	1280	752	103

After reduction

Scheme	λ	β	n	n^*	h^*
TiGER	128	329	512	256	64
	192	578	1024	772	63
	256	523	1024	628	121
SMAUG	128	375	512	292	80
	192	469	768	372	96
	256	613	1280	752	103

How to conduct the $\bmod B$?

What is expected to get from $v \bmod B$?

- $13 \bmod 7 = -1$
- $\begin{pmatrix} 21 \\ 37 \end{pmatrix} \bmod 7 = \begin{pmatrix} 0 \\ 2 \end{pmatrix}$
- $\begin{pmatrix} 21 \\ 37 \end{pmatrix} \bmod 7 \cdot I_2 = \begin{pmatrix} 0 \\ 2 \end{pmatrix}$

How to conduct the $\bmod B$?

What is expected to get from $v \bmod B$?

- $13 \bmod 7 = -1$
- $\begin{pmatrix} 21 \\ 37 \end{pmatrix} \bmod 7 = \begin{pmatrix} 0 \\ 2 \end{pmatrix}$
- $\begin{pmatrix} 21 \\ 37 \end{pmatrix} \bmod 7 \cdot I_2 = \begin{pmatrix} 0 \\ 2 \end{pmatrix}$
- $\begin{pmatrix} 21 \\ 37 \end{pmatrix} \bmod \begin{pmatrix} 48 & 23 \\ 0 & 3 \end{pmatrix} = ?$

How to conduct the mod B?

What is expected to get from v mod B?

- $13 \bmod 7 = -1$
- $\begin{pmatrix} 21 \\ 37 \end{pmatrix} \bmod 7 = \begin{pmatrix} 0 \\ 2 \end{pmatrix}$
- $\begin{pmatrix} 21 \\ 37 \end{pmatrix} \bmod 7 \cdot I_2 = \begin{pmatrix} 0 \\ 2 \end{pmatrix}$
- $\begin{pmatrix} 21 \\ 37 \end{pmatrix} \bmod \begin{pmatrix} 48 & 23 \\ 0 & 3 \end{pmatrix} \Rightarrow \begin{pmatrix} -255 \\ 1 \end{pmatrix} \Rightarrow \begin{pmatrix} -15 \\ 1 \end{pmatrix}$

How to conduct the $\bmod B$?

What is expected to get from $v \bmod B$?

- $13 \bmod 7 = -1$
- $\begin{pmatrix} 21 \\ 37 \end{pmatrix} \bmod 7 = \begin{pmatrix} 0 \\ 2 \end{pmatrix}$
- $\begin{pmatrix} 21 \\ 37 \end{pmatrix} \bmod 7 \cdot I_2 = \begin{pmatrix} 0 \\ 2 \end{pmatrix}$
- $\begin{pmatrix} 21 \\ 37 \end{pmatrix} \bmod \begin{pmatrix} 48 & 23 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 8 \\ 4 \end{pmatrix}$

Two options for $\bmod B$

- Babai's nearest plane algorithm (BNP)
  - Polynomial-time in dimension
  - Quality depends on the size of diagonal terms
- Closest vector problem (CVP)
  - Exponential-time in dimension
  - Quality depends on what?

How to estimate the quality of CVP?

Theorem (Gaussian Heuristics)

The Gaussian heuristic says that the number of lattice points in a hyper ball $\mathbb{B}_r^i(t)$ of radius r with center t with respect to i-norm for $i \in \{2, \infty\}$ is estimated by

$$|\mathcal{L} \cap \mathbb{B}_r^i(t)| = \frac{\mathrm{vol}(\mathbb{B}_r^i(t))}{\det(\mathcal{L})}.$$

- $i = 2$, $\min_{v \in \mathcal{L}} \|v - t\| \leq \sqrt{\frac{n}{2\pi e}} \cdot \mathrm{vol}^{1/\dim}$
- $i = \infty$, $\min_{v \in \mathcal{L}} \|v - t\|_\infty \leq \frac{1}{2} \cdot \mathrm{vol}^{1/\dim}$

How to estimate the quality of CVP?

Theorem (Gaussian Heuristics)

The Gaussian heuristic says that the number of lattice points in a hyper ball $\mathbb{B}_r^i(t)$ of radius r with center t with respect to i-norm for $i \in \{2, \infty\}$ is estimated by

$$|\mathcal{L} \cap \mathbb{B}_r^i(t)| = \frac{\mathrm{vol}(\mathbb{B}_r^i(t))}{\det(\mathcal{L})}.$$

- $i = 2$, $\min_{v \in \mathcal{L}} \|v - t\| \leq \sqrt{\frac{n}{2\pi e}} \cdot \mathrm{vol}^{1/\dim}$
- $i = \infty$, $\min_{v \in \mathcal{L}} \|v - t\|_\infty \leq \frac{1}{2} \cdot \mathrm{vol}^{1/\dim}$

GREAT?

Two options for $\bmod B$

- Babai's nearest plane algorithm (BNP)
  - Polynomial-time in dimension
  - Quality depends on the size of diagonal terms
- Closest vector problem (CVP)
  - Exponential-time in dimension
  - Quality depends on $\mathrm{vol}^{1/\dim}$
- Hybrid algorithm
  - ??

Two options for $\bmod B$

- Babai's nearest plane algorithm (BNP)
  - Polynomial-time in dimension
  - Quality depends on the size of diagonal terms
- Closest vector problem (CVP)
  - Exponential-time in dimension
  - Quality depends on $\mathrm{vol}^{1/\dim}$
- Hybrid algorithm
  - ??

How to conduct the mod B?

What is expected to get from v mod B?

$$\begin{pmatrix} 49 \\ 21 \\ 37 \end{pmatrix} \bmod \begin{pmatrix} 57 & -19 & 17 \\ & 48 & 23 \\ & & 3 \end{pmatrix} \Rightarrow \begin{pmatrix} 35 \\ 8 \\ 4 \end{pmatrix} \Rightarrow \begin{pmatrix} 15 \\ 8 \\ 4 \end{pmatrix}$$

- The last two entries are reduced by CVP
- The first entry is reduced by BNP

How to conduct the mod B?

What is expected to get from v mod B?

$$\begin{pmatrix} 49 \\ 21 \\ 37 \end{pmatrix} \bmod \begin{pmatrix} 57 & -19 & 17 \\ & 48 & 23 \\ & & 3 \end{pmatrix} \Rightarrow \begin{pmatrix} 35 \\ 8 \\ 4 \end{pmatrix} \Rightarrow \begin{pmatrix} 15 \\ 8 \\ 4 \end{pmatrix}$$

- The last two entries are reduced by CVP
- The first entry is reduced by BNP

How to conduct the $\bmod B$?

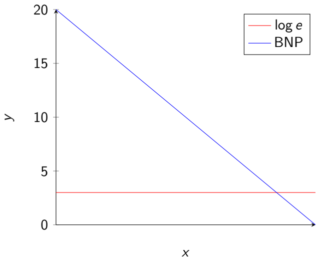
What is expected to get from v mod B?

$$\begin{pmatrix} 49 \\ 21 \\ 37 \end{pmatrix} \bmod \begin{pmatrix} 57 & -19 & 17 \\ & 48 & 23 \\ & & 3 \end{pmatrix} \Rightarrow \begin{pmatrix} 35 \\ 8 \\ 4 \end{pmatrix} \Rightarrow \begin{pmatrix} 15 \\ 8 \\ 4 \end{pmatrix}$$

- The last two entries are reduced by CVP
- The first entry is reduced by BNP

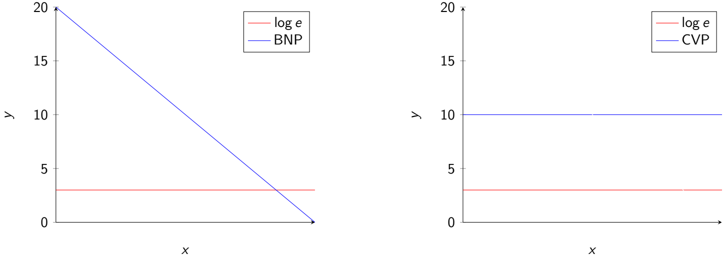
Comparison Results

$$M \cdot s = e \bmod B$$



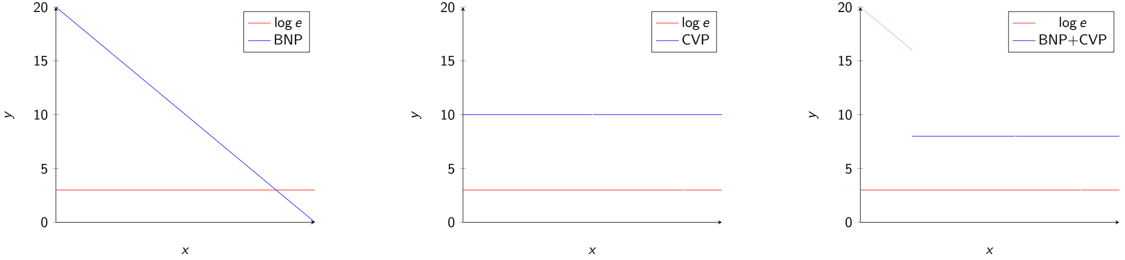
Comparison Results

$$M \cdot s = e \bmod B$$



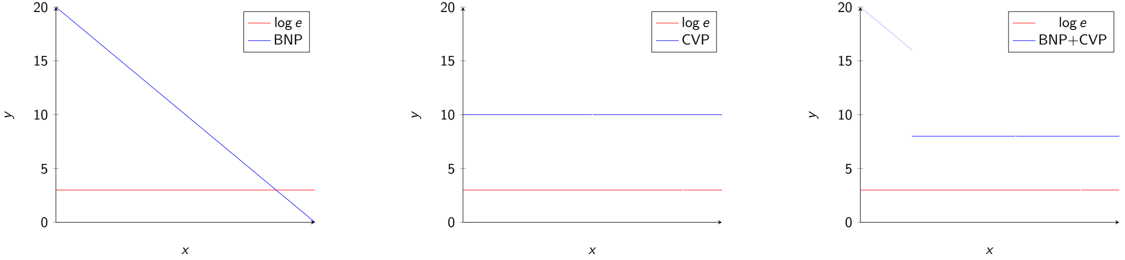
Comparison Results

$M \cdot s = e \bmod B$

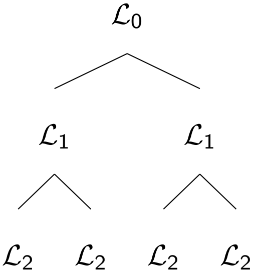


Comparison Results

$M \cdot s = e \bmod B$



Overview for finding s



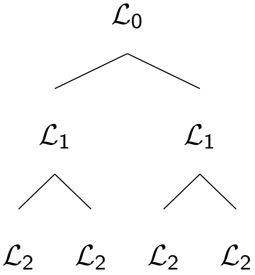
$$\mathcal{L}_0 = \{x \in \mathbb{Z}^n \mid Hw(x) = h_0 \wedge \|M \cdot x \bmod B\|_\infty \leq \eta\}$$

$$\mathcal{L}_1 = \{x \in \mathbb{Z}^n \mid HW(x) = h_1 \wedge \|\pi_r(M \cdot x \bmod B)\| \leq \eta\}$$

$$\mathcal{L}_2 \subset \{x \in \mathbb{Z}^n \mid HW(x) = h_2\}$$

Note: $h^* = h_0 > h_1 > h_2$

Overview for finding s



$$\mathcal{L}_0 = \{x \in \mathbb{Z}^{292} \mid Hw(x) = 80 \wedge \|M \cdot x \bmod B\|_\infty \leq 1.278\}$$

$$\mathcal{L}_1 = \{x \in \mathbb{Z}^{292} \mid HW(x) = 40 \wedge \|\pi_{33}(M \cdot x \bmod 8.158)\| \leq 1.278\}$$

$$\mathcal{L}_2 \subset \{x \in \mathbb{Z}^{292} \mid HW(x) = 20\}$$

SMAUG: $(n^*, h^*, m^*) = (256, 70, 656)$

$\mathcal{L}_0 \leq \mathcal{L}_1$

- $[M \cdot s]_B = e$, $Hw(s) = h_0 \Rightarrow s \in \mathcal{L}_0$
- Split s into $s_{i1} + s_{i2} \Rightarrow [M \cdot s_{i1}]_B + [M \cdot s_{i2}]_B = e \bmod B$ for $i \leq R$
- How many pairs $\{s_{i1}, s_{i2}\} \subset \mathcal{L}_1$?

$\mathcal{L}_0 \leq \mathcal{L}_1$

- $[M \cdot s_{i1}]_B \sim U(\mathcal{L}(B)) \Rightarrow \pi_r([M \cdot s_{i1}]_B) \sim U(\pi_r(\mathcal{L}(B)))$
- Suppose that M has a unit rank and B_1 is a modulo space of unit rank.
- $\Pr(\|[Ms_{i1}]_{B_1}\|_\infty \leq \eta) = \frac{2\eta}{B_1}$, $\Pr(\|[Ms_{i2}]_{B_1}\|_\infty \leq \eta) = \frac{2\eta - e_1}{2\eta} \Rightarrow \frac{2\eta - e_1}{B_1} \geq \frac{2\eta - \sigma}{B_1} = \frac{2\sigma}{B_1}$
- $\Pr(s_{i1}, s_{i2} \in \mathcal{L}_1) \geq \prod_{j=1}^{r} \frac{2\sigma}{B_j}$
- $\#\{s_{i1}, s_{i2}\} \subset \mathcal{L}_1 \geq R \cdot \prod_{j=1}^{r} \frac{2\sigma}{B_j} = 4$

$\mathcal{L}_0 \leq \mathcal{L}_1$

- $[M \cdot s_{i1}]_B \sim U(\mathcal{L}(B)) \Rightarrow \pi_r([M \cdot s_{i1}]_B) \sim U(\pi_r(\mathcal{L}(B)))$
- Suppose that M has a unit rank and B_1 is a modulo space of unit rank.
- $\Pr(\|[Ms_{i1}]_{B_1}\|_\infty \leq \eta) = \frac{2\eta}{B_1}$, $\Pr(\|[Ms_{i2}]_{B_1}\|_\infty \leq \eta) = \frac{2\eta - e_1}{2\eta} \Rightarrow \frac{2\eta - e_1}{B_1} \geq \frac{2\eta - \sigma}{B_1} = \frac{2\sigma}{B_1}$
- $\Pr(s_{i1}, s_{i2} \in \mathcal{L}_1) \geq \prod_{j=1}^{r} \frac{2\sigma}{B_j}$
- $\#\{s_{i1}, s_{i2}\} \subset \mathcal{L}_1 \geq R \cdot \prod_{j=1}^{r} \frac{2\sigma}{B_j} = 4$

$\mathcal{L}_0 \leq \mathcal{L}_1$

- $[M \cdot s_{i1}]_B \sim U(\mathcal{L}(B)) \Rightarrow \pi_r([M \cdot s_{i1}]_B) \sim U(\pi_r(\mathcal{L}(B)))$
- Suppose that M has a unit rank and B_1 is a modulo space of unit rank.
- $\Pr(\|[Ms_{i1}]_{B_1}\|_\infty \leq \eta) = \frac{2}{7}$, $\Pr(\|[Ms_{i2}]_{B_1}\|_\infty \leq \eta) = \frac{2}{3} \Rightarrow \frac{4}{21}$
- $\Pr(s_{i1}, s_{i2} \in \mathcal{L}_1) \geq \left(\frac{4}{21}\right)^{33}$
- $\#\{s_{i1}, s_{i2}\} \subset \mathcal{L}_1 \geq R \cdot \left(\frac{4}{21}\right)^{33} = 4, \quad |\mathcal{L}_1| = |Hw(x) = 40| \cdot \left(\frac{4}{21}\right)^{33} = 2^{110}$

$\mathcal{L}_1 \leq \mathcal{L}_2$

- $\exists i$ s.t. $[M \cdot s_{i1}]_B = e_{i1}$, $Hw(s_{i1}) = h_1 \Rightarrow s_{i1} \in \mathcal{L}_1$
- $\delta = \frac{\mathcal{L}_2}{|Hw(x)=h_2|}$, $|Hw(x) = h_2| = 2^{93}$
- Split s_{i1} into $t_{j1} + t_{j2}$ s.t. $Hw(t_{j1}) = Hw(t_{j2}) = h_2$ for $j \leq R_2$
- $\#\{t_{j1}, t_{j2}\} \subset \mathcal{L}_2 \geq R_2 \cdot \delta^2 = 4$, $\delta = 2^{-18.5}$, $|\mathcal{L}_2| = 2^{74.5}$

Question: How to find the s_{i1} from $\mathcal{L}_2$?

$\mathcal{L}_1 \leq \mathcal{L}_2$

- $\exists i$ s.t. $[M \cdot s_{i1}]_B = e_{i1}$, $Hw(s_{i1}) = h_1 \Rightarrow s_{i1} \in \mathcal{L}_1$
- $\delta = \frac{\mathcal{L}_2}{|Hw(x)=h_2|}$, $|Hw(x) = h_2| = 2^{93}$
- Split s_{i1} into $t_{j1} + t_{j2}$ s.t. $Hw(t_{j1}) = Hw(t_{j2}) = h_2$ for $j \leq R_2$
- $\#\{t_{j1}, t_{j2}\} \subset \mathcal{L}_2 \geq R_2 \cdot \delta^2 = 4$, $\delta = 2^{-18.5}$, $|\mathcal{L}_2| = 2^{74.5}$

Question: How to find the s_{i1} from $\mathcal{L}_2$?

$\mathcal{L}_1 \leq \mathcal{L}_2$

- Construct a set $\{\ell^r(M \cdot x \bmod B) \mid x \in \mathcal{L}_2, \|\pi_r(M \cdot x)\|_\infty \leq \eta\}$, Where $\ell(x) = \lfloor \frac{x}{2\eta} \rceil$
- Idea: If two points y_1, y_2 are close, their value is the same
- For points of the same value, we check their closeness
- $\Pr(\ell(y_1) = \ell(y_2)) = \frac{2\eta - |y_1 - y_2|}{2\eta} \geq \frac{3}{4} \Rightarrow \Pr(\ell^r(y_1) = \ell^r(y_2)) \geq \left(\frac{3}{4}\right)^{33}$
- $\#$ of blocks $= (7/2)^r = (3.5)^{33}$
- $\#$ of pairs $|\mathcal{L}_2|^2 \cdot \left(\frac{8}{21}\right)^{33} = 2^{106}$

Summary

- m can be chosen flexibly
- n, h can be reduced via the BKZ algorithm
- The matrix modulus B be performed as $\bmod q$ with CVPP
- To solve the SMAUG-256
  - $(n, h, q) = (512, 140, 1024) \Rightarrow (292, 80, B)$: $2^{109.5}$
  - Build the list $\mathcal{L}_2$: 2^{92}
  - Build the list $\mathcal{L}_1$: 2^{106}
  - Build the list $\mathcal{L}_0$: 2^{110}

$$\left| \ :) \ \equiv_q \begin{bmatrix} \\ \textit{Question?} \\ \\ \textit{changminlee@kias.re.kr} \end{bmatrix} \cdot \begin{matrix} \mathsf{T} \\ \mathsf{H} \\ \mathsf{A} \\ \mathsf{N} \\ \mathsf{K} \\ \\ \mathsf{Y} \\ \mathsf{O} \\ \mathsf{U} \end{matrix} \right.$$