Analysis of the sparse secret LWE: SMAUG and TiGER

Changmin Lee

Korea Institute for Advanced Study

The LWE problem

$$
\left| b \right| \equiv_q \left[\quad A \quad \right] \cdot \left| s \right| + \left| e \right|,
$$

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)

$$\left.b\,\right| \equiv_q \begin{bmatrix} \\ A \\ \\ \end{bmatrix} \cdot \left| s \right. + \left| e, \right.$$

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

- 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

LWE of h-dimension $\leq$ sLWE

$$b \equiv_q \begin{bmatrix} A_0 \end{bmatrix} \cdot s + e,$$

Relation between sLWE and LWE; hardness of sLWE

LWE of h-dimension $\leq$ sLWE

$$b \equiv_q \begin{bmatrix} A_0 \end{bmatrix} \begin{bmatrix} \color{red}{A_1} \end{bmatrix} \cdot \begin{array}{c} s \\ \color{red}{0} \end{array} + e$$

Relation between sLWE and LWE; hardness of sLWE

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

Question: Is there an algorithm for sLWE with respect to h, not n

Goal of this research

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

Technical Idea: Why need more?

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

$$b \equiv_q \left[\; A \; \right] \cdot s + e,$$

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

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 LWE with h samples? (Another reduction)

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

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

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

How to solve the LWE with h samples? (Another reduction)

Current problem:
Given $\bar{A} = (A_0 \| A_1) \in \mathbb{Z}^{h\times(n-2h+1)} \times \mathbb{Z}^{h\times 2h}$ and q, find $(s_0 \| s_1)$ such that $A_0 \cdot s_0 + A_1 \cdot s_1 \equiv_q e$:

$$L = \left\langle \begin{pmatrix} I_{n-2h+1} & & \\ & I_{2h} & \\ A_0 & A_1 & qI_h \end{pmatrix} \right\rangle \ni \begin{pmatrix} s_0 \\ s_1 \\ e \end{pmatrix}$$

How to solve the LWE with h samples? (Another reduction)

Current problem:

Let $B = BKZ_{3h}\left(\begin{pmatrix} I_{2h} & \\ A_1 & qI_h \end{pmatrix}\right)$ be a matrix.

Given $A_0 \in \mathbb{Z}^{h\times(n-2h+1)}$ and B, find s_0 such that $A_0 \cdot s_0 \equiv_B \begin{pmatrix} s_1 \\ e \end{pmatrix}$:

$$L = \left\langle \begin{pmatrix} I_{n-2h+1} & \\ A_0 & B \end{pmatrix} \right\rangle \ni \begin{pmatrix} s_0 \\ s_1 \\ e \end{pmatrix}$$

How to solve the LWE with h samples? (Another reduction)

Current problem:
Given $Adj(B) \cdot A_0 \in \mathbb{Z}^{h \times (n-2h+1)}$ and $\det(B)$, find s_0 such that $Adj(B) \cdot A_0 \cdot s_0 \equiv_{\det(B)} e^*$:

$$L = \left\langle \begin{pmatrix} I_{n-2h+1} & \\ Adt(B) \cdot A_0 & \det(B) I_{3h} \end{pmatrix} \right\rangle \ni \begin{pmatrix} s_0 \\ e^* \end{pmatrix}, e^* = Adj(B) \cdot \begin{pmatrix} s_1 \\ e \end{pmatrix}$$

Note:

- $\det(B) = q^h$, $\|B\| \approx q^{h/3h}$, and $Adj(B) \approx q^{(3h-1)/3}$
- Dimension $n - 2h + 1$, $H.w(s_0) \approx h\frac{n-2h}{n}$
- Time: $O(2^{0.292 \cdot (3h)})$

After reduction

Scheme	λ	β	n	n^*	h^*	$S^{1/3}$
TiGER	128	329	512	256	64	89
	192	578	1024	772	63	124
	256	523	1024	628	121	186
SMAUG	128	336	512	232	63	84
	192	469	768	372	96	132
	256	613	1280	752	103	177

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