LATTICE REDUCTION ATTACKS ON HE SCHEMES

Martin R. Albrecht
15/03/2018
The Learning with Errors (LWE) problem was defined by Oded Regev.\textsuperscript{1} Given $(A, c)$ with uniform $A \in \mathbb{Z}_q^{m \times n}$, uniform $s \in \mathbb{Z}_q^n$ and small $e \in \mathbb{Z}_m$ is $c \leftarrow \mathcal{U}(\mathbb{Z}_q^m)$ or

$$
\begin{pmatrix}
    c \\
    \end{pmatrix} = \begin{pmatrix}
    A \\
    \end{pmatrix} \cdot \begin{pmatrix}
    s \\
    \end{pmatrix} + \begin{pmatrix}
    e \\
    \end{pmatrix}.

Where it all began ...  

- We were writing a paper on using Gröbner bases for solving LWE instances.
- Ludovic Perret asked me to write the related work section.
- Our paper on using Gröbner bases for solving LWE still has not been published.

I am still working on that related work section.
Primal Attack (primal_usvp, primal_decode)

Solve Bounded Distance Decoding problem (BDD), i.e.

\[ \text{find } s' \text{ s.t. } \|w - c\| \text{ is minimised, with } w = A \cdot s' \] using uSVP embedding or Babai’s nearest planes resp. enumeration.

Dual Attack (dual, dual_scale)

Solve Short Integer Solutions problem (SIS) in the left kernel of \( A \), i.e.

\[ \text{find a short } w \text{ such that } w \cdot A = 0 \]

and check if \( \langle w, c \rangle = w \cdot (A \cdot s + e) = \langle w, e \rangle \) is short.
Given $A, c$ with $c = A \cdot s + e$, we know that for some $s'$ we have that $A \cdot s' - c \pmod q$ is rather small.

$\Rightarrow$ we know there is an unusually short vector in the $q$-ary lattice

$$B = \begin{pmatrix} A^T & 0 \\ c^T & t \end{pmatrix} \in \mathbb{Z}_q^{(n+1) \times (m+1)}$$

since

$$(s | -1) \cdot B = (e | -t) \pmod q$$

and use lattice reduction to find it.
Success Condition (ADPS16)

\[
\log_2(\|\cdot\|)
\]

Graph showing:
- GSA for \( \|b_i^*\| \)
- Average for \( \|b_i^*\| \)
- Expectation for \( \|\pi_i(v)\| \)

Index \( i \)

\( d - \beta + 1 \)

Given samples $A, c$:

1. Find a short $y$ solving SIS on $A$.
2. Compute $\langle y, c \rangle$.

Either $c = A \cdot s + e$ or $c$ uniformly random:

• If $c$ is uniformly random, so is $\langle y, c \rangle$.
• If $c = A \cdot s + e$, then $\langle y, c \rangle = \langle y \cdot A, s \rangle + \langle y, e \rangle \equiv \langle y, e \rangle \pmod{q}$. If $y$ is sufficiently short, then $\langle y, e \rangle$ will also be short, since $e$ is also small.
Algorithm Sketch

\[ \varepsilon_d \leftarrow \exp(-\pi (\text{Exp}[y_i] \cdot \alpha)^2); \]
\[ m \leftarrow \lceil 2 \log(2 - 2 \varepsilon_t) / \log(1 - 4 \varepsilon_d^2) \rceil; \]
\[ P \leftarrow n \times n \text{ permutation matrices}; \]
\[ [A_0 \mid A_1] \leftarrow A \cdot P \text{ with } A_0 \in \mathbb{Z}_{q}^{m \times (n-k)}; \]
\[ L \leftarrow \text{basis for } \{(y, x/c) \in \mathbb{Z}^m \times (1/c \cdot \mathbb{Z})^n : y \cdot A_0 \equiv x \mod q\}; \]
\[ L' \leftarrow \text{BKZ-} \beta \text{ reduced basis for } L; \]
\[ \text{for } i \leftarrow 0 \text{ to } m - 1 \text{ do} \]
\[ \quad U \leftarrow \text{a sparse unimodular matrix with small entries}; \]
\[ \quad L_i \leftarrow U \cdot L'; \]
\[ \quad L'_i \leftarrow \text{BKZ-} \beta' \text{ reduced basis for } L_i; \]
\[ \quad (w_i, v_i) \leftarrow \text{shortest row vector in } L'_i; \]
\[ \quad e'_i \leftarrow \langle w_i, c \rangle; \]
\[ \text{end} \]
\[ \text{if } e'_i \text{ follow discrete Gaussian distribution then return } \top; \]
\[ \text{return } \bot; \]
• Lattice reduction returns more than one somewhat short vector
• Inner products have algebraic meaning beyond returning somewhat short elements

Sources for future refinements

- There are more black boxes to be opened, e.g.:
  - enumeration/sieving inside BKZ\(^2\)
  - BDD enumeration and small/sparse secrets
- Cost of lattice reduction not fully understood

Note
Estimates in standards document are quite conservative and price some of these anticipated improvements in.

https://bitbucket.org/malb/lwe-estimator

- **relied upon** NIST PQC submissions and HE standard security document
- **one man show** about 300 commits, mostly by me
- **quality control** tests, documentation but **no peer review**
  - **bugs** there have been bugs leading to false security estimates and plenty of potential for more: numerical stability, heuristics for pruning branches in a search tree, ...
Thank You