Lattice Reduction Attacks on HE Schemes

Martin R. Albrecht

15/03/2018

Learning with Errors

The Learning with Errors (LWE) problem was defined by Oded Regev.[1]

Given $(\mathbf{A}, \mathbf{c})$ with uniform $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, uniform $\mathbf{s} \in \mathbb{Z}_q^n$ and small $\mathbf{e} \in \mathbb{Z}^m$ is $\mathbf{c} \leftarrow_\$ \mathcal{U}(\mathbb{Z}_q^m)$ or

$$\begin{pmatrix} \\ \mathbf{c} \\ \\ \end{pmatrix} = \begin{pmatrix} \leftarrow & n & \rightarrow \\ & & \\ & \mathbf{A} & \\ & & \end{pmatrix} \cdot \begin{pmatrix} \\ \mathbf{s} \\ \\ \end{pmatrix} + \begin{pmatrix} \\ \mathbf{e} \\ \\ \end{pmatrix}.$$

[1] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In: *37th ACM STOC*. ed. by Harold N. Gabow and Ronald Fagin. ACM Press, May 2005, pp. 84–93.

Where it all began . . .

Martin R. Albrecht, Carlos Cid, Jean-Charles Faugère, and Ludovic Perret. Algebraic Algorithms for LWE. Cryptology ePrint Archive, Report 2014/1018. `http://eprint.iacr.org/2014/1018`. 2014

- 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.

"Related Work"

Primal Attack (`primal_usvp`, `primal_decode`)

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

$$\text{find } \mathbf{s}' \text{ s.t. } \|\mathbf{w} - \mathbf{c}\| \text{is minimised, with } \mathbf{w} = \mathbf{A} \cdot \mathbf{s}' \text{ using}$$

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 $\mathbf{A}$, i.e.

$$\text{find a short } \mathbf{w} \text{ such that } \mathbf{w} \cdot \mathbf{A} = 0$$

and check if $\langle \mathbf{w}, \mathbf{c} \rangle = \mathbf{w} \cdot (\mathbf{A} \cdot \mathbf{s} + \mathbf{e}) = \langle \mathbf{w}, \mathbf{e} \rangle$ is short.

Bounded Distance Decoding and unique SVP

Given $\mathbf{A}, \mathbf{c}$ with $\mathbf{c} = \mathbf{A} \cdot \mathbf{s} + \mathbf{e}$, we know that for some $\mathbf{s}'$ we have that $\mathbf{A} \cdot \mathbf{s}' - \mathbf{c} \pmod{q}$ is rather small.

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

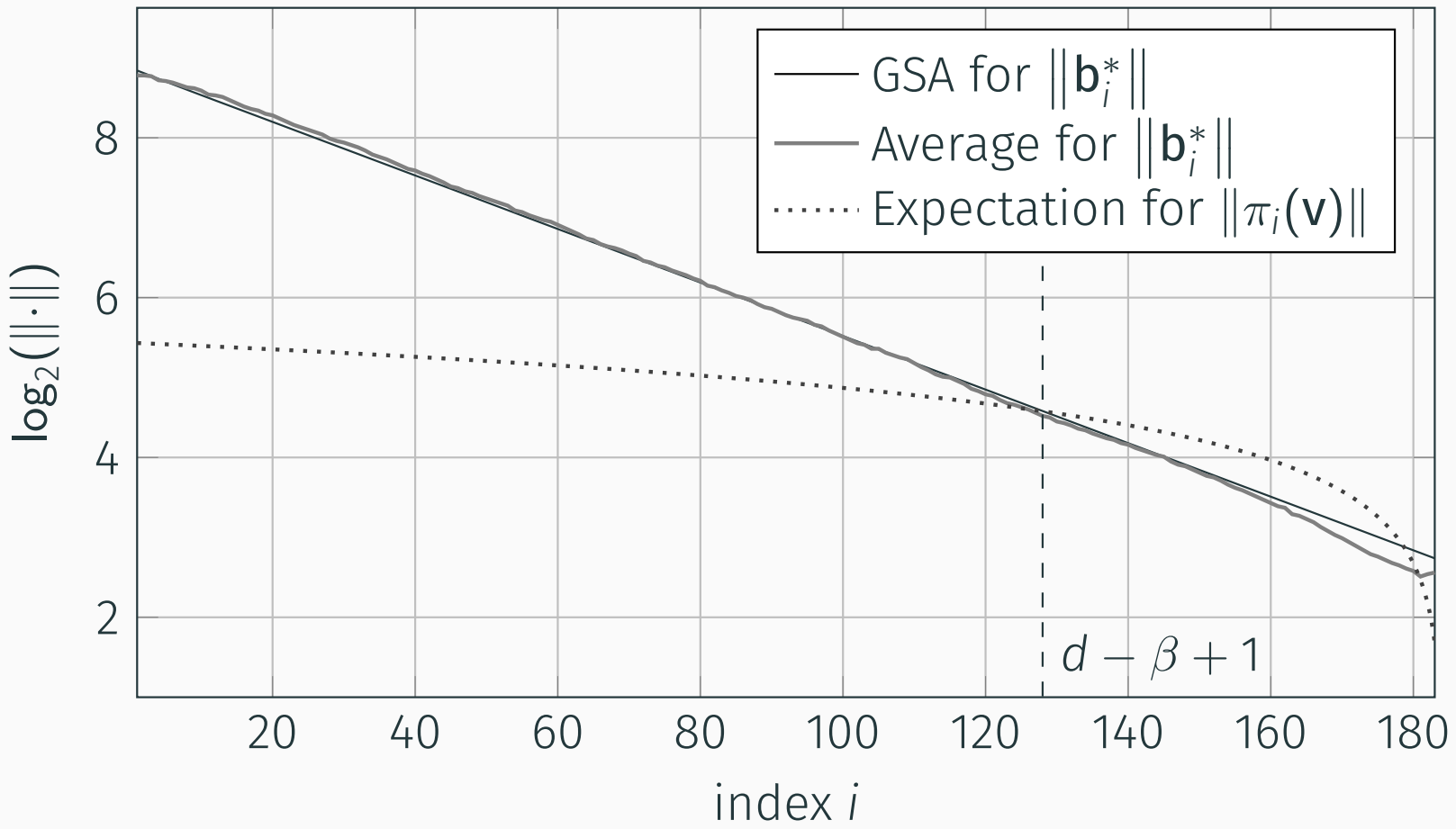
$$\mathbf{B} = \begin{pmatrix} \mathbf{A}^T & 0 \\ \mathbf{c}^T & t \end{pmatrix} \in \mathbb{Z}_q^{(n+1)\times(m+1)}$$

since

$$(\mathbf{s} \mid -1) \cdot \mathbf{B} = (\mathbf{e} \mid -t) \bmod q$$

and use lattice reduction to find it.

Success Condition (ADPS16)



Don't treat block-wise lattice reduction as a black box

- Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum Key Exchange - A New Hope. In: *25th USENIX Security Symposium, USENIX Security 16*. Ed. by Thorsten Holz and Stefan Savage. USENIX Association, 2016, pp. 327–343. URL: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/alkim
- Martin R. Albrecht, Florian Göpfert, Fernando Virdia, and Thomas Wunderer. Revisiting the Expected Cost of Solving uSVP and Applications to LWE. In: *ASIACRYPT 2017, Part I*. ed. by Tsuyoshi Takagi and Thomas Peyrin. Vol. 10624. LNCS. Springer, Heidelberg, Dec. 2017, pp. 297–322

Dual Attack

Given samples $\mathbf{A}, \mathbf{c}$:

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

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

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

Algorithm Sketch

$\varepsilon_d \leftarrow \mathsf{exp}(-\pi(\mathrm{Exp}[\mathsf{y}_i] \cdot \alpha)^2)$;
$m \leftarrow \lceil 2\ \mathsf{log}(2 - 2\,\varepsilon_t)/\,\mathsf{log}(1 - 4\,\varepsilon_d^2) \rceil$;
$\mathsf{P} \leftarrow\!\!\$\ n \times n$ permutation matrices;
$[\mathsf{A}_0 \mid \mathsf{A}_1] \leftarrow \mathsf{A} \cdot \mathsf{P}$ with $\mathsf{A}_0 \in \mathbb{Z}_q^{m \times (n-k)}$;
$\mathsf{L} \leftarrow$ basis for $\{(\mathsf{y}, \mathsf{x}/c) \in \mathbb{Z}^m \times (1/c \cdot \mathbb{Z})^n : \mathsf{y} \cdot \mathsf{A}_0 \equiv \mathsf{x} \bmod q\}$;
$\mathsf{L}' \leftarrow$ BKZ-β reduced basis for L;
for $i \leftarrow 0$ **to** $m - 1$ **do**
    $\mathsf{U} \leftarrow\!\!\$$ a sparse unimodular matrix with small entries;
    $\mathsf{L}_i \leftarrow \mathsf{U} \cdot \mathsf{L}'$;
    $\mathsf{L}_i' \leftarrow$ BKZ-β' reduced basis for L_i;
    $(\mathsf{w}_i, \mathsf{v}_i) \leftarrow$ shortest row vector in L_i';
    $e_i' \leftarrow \langle \mathsf{w}_i, \mathsf{c} \rangle$;
end
if e_i' *follow discrete Gaussian distribution* **then return** $\top$;
return $\bot$;

Opening Black Boxes

- Lattice reduction returns more than one somewhat short vector
- Inner products have algebraic meaning beyond returning somewhat short elements

Martin R. Albrecht. On Dual Lattice Attacks Against Small-Secret LWE and Parameter Choices in HElib and SEAL. In: *EUROCRYPT 2017, Part II*. ed. by Jean-Sébastien Coron and Jesper Buus Nielsen. Vol. 10211. LNCS. Springer, Heidelberg, May 2017, pp. 103–129

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.

[2] Léo Ducas. Shortest Vector from Lattice Sieving: a Few Dimensions for Free. Cryptology ePrint Archive, Report 2017/999. http://eprint.iacr.org/2017/999. 2017.

Code = Research

`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