Open questions in lattice-based cryptanalysis

Elena Kirshanova

I. Kant Baltic Federal University

Workshop on the Mathematics of Post-Quantum crypto
July 7, 2020

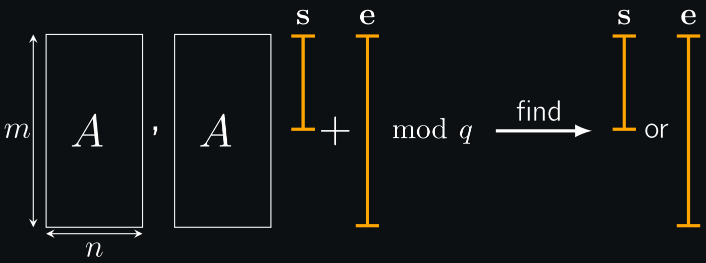
Outline

- Hardness of LWE
- Algorithms for SVP

Part I

Open problems related to LWE

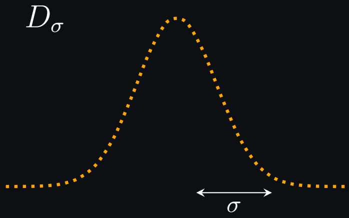
Learning with Errors (Regev'05)



$A \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$

$\mathbf{s} \leftarrow D_\sigma$ / binary / ternary

$\mathbf{e} \leftarrow D_\sigma$



Often: $n = \Theta(\text{bit security})$, $q = n^{\Theta(1)}$, $m = \Omega(n)$, $\sigma = \Omega(\sqrt{n})$

Classical hardness of LWE

BKZ, [HKM, AGVW]

BKW, [GJS, KF]

$$\mathbf{s} \leftarrow D_\sigma$$

$\lg \text{Time} = \mathsf{c} \cdot n$

$\lg \text{Mem} = \lg \text{Time}$

$\#\text{Samples} = \Theta(n)$

$\mathsf{c} = 0.292 \cdot \frac{\lg q \lg n}{\lg^2(q/\sigma)} = \Theta(1)$

Classical hardness of LWE

$$\mathbf{s} \leftarrow D_\sigma$$

BKZ, [HKM, AGVW]

$\lg \text{Time} = \mathsf{c} \cdot n$

$\lg \text{Mem} = \lg \text{Time}$

$\#\text{Samples} = \Theta(n)$

$\mathsf{c} = 0.292 \cdot \frac{\lg q \lg n}{\lg^2(q/\sigma)} = \Theta(1)$

BKW, [GJS, KF]

$\lg \text{Time} = \mathsf{c} \cdot n$

$\lg \text{Mem} = \lg \text{Time}$

$\#\text{Samples} = \text{Time}$

$\mathsf{c} = \left(\frac{\lg q}{\lg n} + 2 \ln\left(\frac{\lg q}{\lg \sigma}\right)\right)^{-1} = \Theta(1)$

c worsens if $\#\text{Samples} = \Theta(n)$

Classical hardness of LWE

BKZ, [HKM, AGVW]

BKW, [GJS, KF]

$$\mathbf{s} \leftarrow D_\sigma$$

BKZ:

$\lg \mathrm{Time} = \mathsf{c} \cdot n$

$\lg \mathrm{Mem} = \lg \mathrm{Time}$

$\#\mathrm{Samples} = \Theta(n)$

$\mathsf{c} = 0.292 \cdot \frac{\lg q \lg n}{\lg^2(q/\sigma)} = \Theta(1)$

BKW:

$\lg \mathrm{Time} = \mathsf{c} \cdot n$

$\lg \mathrm{Mem} = \lg \mathrm{Time}$

$\#\mathrm{Samples} = \mathrm{Time}$

$\mathsf{c} = \left(\frac{\lg q}{\lg n} + 2\ln\left(\frac{\lg q}{\lg \sigma}\right)\right)^{-1} = \Theta(1)$

c worsens if $\#\mathrm{Samples} = \Theta(n)$

$$\mathbf{s} \text{ – binary/ternary}$$

Lattice re-scaling improves c slightly, [BG]

$\lg \mathrm{Time} = \mathsf{c} \cdot \frac{1}{\lg \lg n} \cdot n$

$\#\mathrm{Samples} = \Omega(n)$

c depends on #Samples

Open questions

1. Why lattice-based attacks do not asymptotically profit from small $\mathbf{s}$?

Open questions

1. Why lattice-based attacks do not asymptotically profit from small $\mathbf{s}$?

2. Standard LWE in dim $n/\lg n$ reduces to LWE with binary $\mathbf{s}$ in dim n [BLPRS]. The best known attack on binary LWE is $2^{n/\lg\lg n}$. The picture is not complete here.

Open questions

1. Why lattice-based attacks do not asymptotically profit from small $\mathbf{s}$?

2. Standard LWE in dim $n/\lg n$ reduces to LWE with binary $\mathbf{s}$ in dim n [BLPRS]. The best known attack on binary LWE is $2^{n/\lg\lg n}$. The picture is not complete here.

3. Combination of lattice-based and combinatorial algorithms (aka hybrid attacks)? Complete analysis for small-secret LWE/LWR under hybrid attacks

I. Speed-ups of classical attacks

BKZ

$\lg \text{Time} = \mathsf{c} \cdot n$

$\mathsf{c} = 0.265 \cdot \frac{\lg q \lg n}{\lg^2(q/\sigma)} = \Theta(1)$

BKW

No known speed-ups for LWE

For LPN see [EHKMS]

Quantum hardness of LWE

I. Speed-ups of classical attacks

BKZ

$\lg \mathsf{Time} = \mathsf{c} \cdot n$

$\mathsf{c} = 0.265 \cdot \frac{\lg q \lg n}{\lg^2(q/\sigma)} = \Theta(1)$

BKW

No known speed-ups for LWE

For LPN see [EHKMS]

II. Quantum specific attacks

1. Kuperberg's algorithm [Kup]
2. LWE with quantum samples [GKZ]

Kuperberg's algorithm [Kup]

1. From LWE obtain $\ell \sim$ (LWE gap) samples of the form (Reg, BKSW)
$$\sum_{j\in\mathbb{Z}} \rho_r(j)\,|j\rangle\,|\mathbf{x} + j\cdot\mathbf{s}\rangle$$
2. Apply Kuperberg's algorithm to find $\mathbf{s}$
3. Complexity of this approach is
$$\exp\left(\mathsf{c}'\left(\log\ell + \frac{n\log q}{\log\ell}\right)\right)$$

This algorithm is no better than classical lattice-based approaches.

Kuperberg's algorithm [Kup]

1. From LWE obtain $\ell \sim$ (LWE gap) samples of the form (Reg, BKSW)
$$\sum_{j\in\mathbb{Z}} \rho_r(j)\,|j\rangle\,|\mathbf{x}+j\cdot\mathbf{s}\rangle$$
2. Apply Kuperberg's algorithm to find $\mathbf{s}$
3. Complexity of this approach is
$$\exp\left(\mathsf{c}'\left(\log\ell+\frac{n\log q}{\log\ell}\right)\right)$$

This algorithm is no better than classical lattice-based approaches.

Open question: Quantum speed-ups for the problem of enumerating (almost) all ℓ_2-small solutions $\mathbf{x}$ to the equation $A\mathbf{x}=\mathbf{t}$ (SIS problem).

LWE with quantum samples

Thm. IV.1. in [GKZ]

For $V \subseteq q^n$, given

$$|\Psi\rangle = \frac{1}{|V|} \sum_{\mathbf{a} \in V} |\mathbf{a}\rangle \, |\langle \mathbf{a} \, , \mathbf{s} \rangle + e_{\mathbf{a}} \bmod q \rangle \, ,$$

a version of Bernstein-Vazirani algorithm finds $\mathbf{s}$ w.p. $\frac{|V|}{20|e|_\infty q^n}$.

LWE with quantum samples

Thm. IV.1. in [GKZ]

For $V \subseteq q^n$, given

$$|\Psi\rangle = \frac{1}{|V|} \sum_{\mathbf{a} \in V} |\mathbf{a}\rangle \, |\langle \mathbf{a} \, , \mathbf{s} \rangle + e_{\mathbf{a}} \bmod q\rangle \, ,$$

a version of Bernstein-Vazirani algorithm finds $\mathbf{s}$ w.p. $\frac{|V|}{20|e|_\infty q^n}$.

If we do not have enough samples (an idea):

1. Use sample amplification to produce

$$\sum_{\mathbf{x}} |\mathbf{x}\rangle \, |\mathbf{x}A\rangle \, |\langle \mathbf{x}A \, , \mathbf{s} \rangle + e_{\mathbf{a}} \bmod q\rangle$$

2. Solve SIS to "forget" the amplifier $\mathbf{x}$ and obtain $|\Psi\rangle$
3. Apply the above theorem

Open question: Analyse it.

Part I

Open problems related to SVP

SVP in ℓ_2-norm (asymptotics, n–lattice rank)

Sieving (heuristic) [BDGL16, HK17]

time optimal:

$\log \mathsf{Time} = 0.292n$

$\log \mathsf{Mem} = 0.208n$

Enumeration, [ABF+]

$\log \mathsf{Time} = \frac{1}{8} n \log n$

$\mathsf{Mem} = \mathrm{poly}(n)$

SVP in ℓ_2-norm (asymptotics, n–lattice rank)

Sieving (heuristic) [BDGL16, HK17]

time optimal:
$\log \mathsf{Time} = 0.292n$
$\log \mathsf{Mem} = 0.208n$

mem. optimal for $k = \Theta(1)$:
$\log \mathsf{Time}$: see Eq.(8) in [HK]
$\log \mathsf{Mem} = \left(\frac{k^{k/k+1}}{k+1}\right)^{n/2}$

Enumeration, [ABF+]

$\log \mathsf{Time} = \frac{1}{8} n \log n$
$\mathsf{Mem} = \mathrm{poly}(n)$

Open question:

Extend the analysis of memory efficient sieving to non-constant k ($k = \lg(n)$ will tell which approach is asymptotically better)

SVP in ℓ_∞-norm

- SVP_∞ is relevant for lattice-based signatures (e.g., Kyber)
- Currently the complexity of SVP_∞ relies on norm-equivalence and average-case weight distribution
- The result of Aggarwal-Mukhopadhyay [AM] for SVP_∞ yields heuristic time complexity $2^{0.62n}$ using 2-lvl hashing.

SVP in ℓ_∞-norm

- SVP_∞ is relevant for lattice-based signatures (e.g., Kyber)
- Currently the complexity of SVP_∞ relies on norm-equivalence and average-case weight distribution
- The result of Aggarwal-Mukhopadhyay [AM] for SVP_∞ yields heuristic time complexity $2^{0.62n}$ using 2-lvl hashing.

Open questions:

Analyse SVP_∞ alg. of [AM] using locality-sensitive techniques from [BDGL16].

Combinatorial algorithms for SVP_∞?

Sieving in ideal lattices

- Significant speed-ups for SVP algorithms (enumeration/sieving) on ideal/structural lattices are not known
- Recent results [KEF] show that one can exploit the structure of tower fields

Open question:

Can similar ideas speed-up sieving algorithms?

List of open problems

- Hardness of LWE for small secret
- Quantum hardness of LWE
- Memory efficient sieving
- SVP in ℓ_∞-norm
- Use of subfields/subrings to speed-up sieving algorithms

List of open problems

- Hardness of LWE for small secret
- Quantum hardness of LWE
- Memory efficient sieving
- SVP in ℓ_∞-norm
- Use of subfields/subrings to speed-up sieving algorithms

Thank you!
Q?

References I

- [ABF+] M. R. Albrecht, S. Bai, P. Fouque, P. Kirchner, D. Stehlé, W. Wen Faster Enumeration-based Lattice Reduction: Root Hermite Factor $k^(1/(2k))$ in Time $k^(k/8 + o(k))$
- [AGVW] M.R. Albrecht, F. Göpfert, F. Virdia, T. Wunderer. Revisiting the Expected Cost of Solving uSVP and Applications to LWE.
- [AM] D.Aggarwal, P.Mukhopadhyay. Improved algorithms for the Shortest Vector Problem and the Closest Vector Problem in the infinity norm
- [BDGL] A. Becker, L. Ducas, N. Gama, T. Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving.
- [BG] S.Bai, S.Galbraith. Lattice Decoding Attacks on Binary LWE.
- [BKSW] Z. Brakerski, E.Kirshanova, W.Wen, D. Stehlé. Learning With Errors and Extrapolated Dihedral Cosets
- [BLPRS] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, D. Stehlé. Classical Hardness of Learning with Errors
- [GHS] Q. Guo, T. Johansson, P. Stankovski. Coded-BKW: Solving LWE Using Lattice Codes
- [GKZ] A. B. Grilo, I. Kerenidis, T. Zijlstra. Learning with Errors is easy with quantum samples

References II

- [HK] G.Herold, E.Kirshanova. Improved Algorithms for the Approximate k-List Problem in Euclidean norm
- [HKM] G.Herold, E.Kirshanova, A.May. On the asymptotic complexity of LWE.
- [KF] P. Kirchner, P.Fouque. An Improved BKW Algorithm for LWE with Applications to Cryptography and Lattices
- [KEF] P. Kirchner, T.Espitau, P.Fouque. Fast Reduction of Algebraic Lattices over Cyclotomic fields
- [Kup] G. Kuperberg. Another sub-exponential time algorithm for the Dihedral Hidden Subgroup Problem
- [Reg] O. Regev. Quantum computation and lattice problems.