Overview of Quantum Cryptanalysis of Lattice Systems

Elena Kirshanova

I. Kant Baltic Federal University

based on joint works with G.Herold, T. Laarhoven

Quantum Cryptanalysis of Post-Quantum Cryptography
The Simons Institute for the Theory of Computing
March 1, 2020

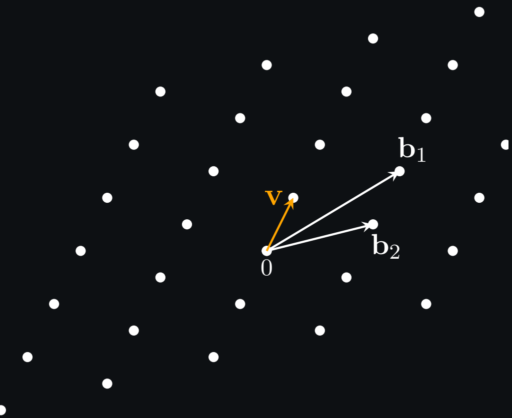
Outline

- The Shortest Vector Problem
- Classical & Quantum Sieve
- Other algorithms

SVP

Minimum

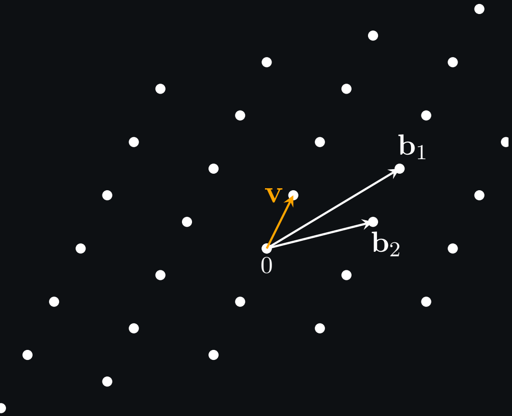
$$\lambda_1(\mathcal{L}) = \min_{\mathbf{v}\in\mathcal{L}\setminus\mathbf{0}} \|\mathbf{v}\|$$



The Shortest Vector Problem (SVP) asks to find $\mathbf{v}_{\text{shortest}} \in \mathcal{L}$:

$$\|\mathbf{v}_{\text{shortest}}\| = \lambda_1(\mathcal{L})$$

SVP



Minimum

$$\lambda_1(\mathcal{L}) = \min_{\mathbf{v}\in\mathcal{L}\setminus\mathbf{0}} \|\mathbf{v}\|$$

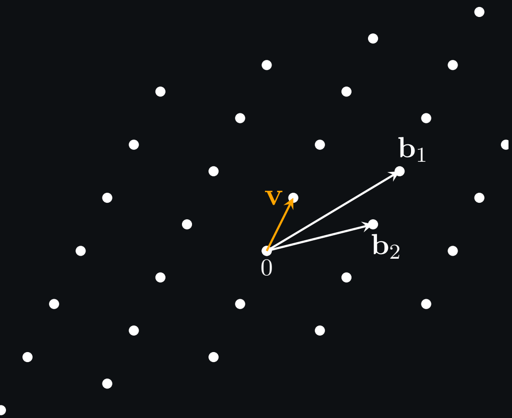
Determinant

$$\det(\mathcal{L}) = |\det(\mathbf{b}_i)_i|$$

The Shortest Vector Problem (SVP) asks to find $\mathbf{v}_{\text{shortest}} \in \mathcal{L}$:

$$\|\mathbf{v}_{\text{shortest}}\| = \lambda_1(\mathcal{L})$$

SVP



Minimum

$$\lambda_1(\mathcal{L}) = \min_{\mathbf{v}\in\mathcal{L}\setminus\mathbf{0}} \|\mathbf{v}\|$$

Determinant

$$\det(\mathcal{L}) = |\det(\mathbf{b}_i)_i|$$

Minkowski bound

$$\lambda_1(\mathcal{L}) \le \sqrt{n}(\det(\mathcal{L}))^{\frac{1}{n}}$$

The Shortest Vector Problem (SVP) asks to find $\mathbf{v}_{\text{shortest}} \in \mathcal{L}$:

$$\|\mathbf{v}_{\text{shortest}}\| = \lambda_1(\mathcal{L})$$

Asymptotics for SVP Algorithms

- Enumeration

- Sieving

Asymptotics for SVP Algorithms

- Enumeration

$$\text{Classical: Time} = 2^{((1/2e)+o(1))n\log n} \qquad \text{Mem.} = \mathrm{poly}(n)$$

$$\text{Quantum: Time} = 2^{((1/4e)+o(1))n\log n} \qquad \text{Mem.} = \mathrm{poly}(n)$$

- Sieving

Asymptotics for SVP Algorithms

- Enumeration

Classical: Time $= 2^{((1/2e)+o(1))n \log n}$ Mem. $= \mathrm{poly}(n)$

Quantum: Time $= 2^{((1/4e)+o(1))n \log n}$ Mem. $= \mathrm{poly}(n)$

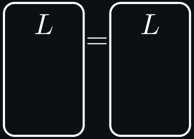
- Sieving (Heuristic)

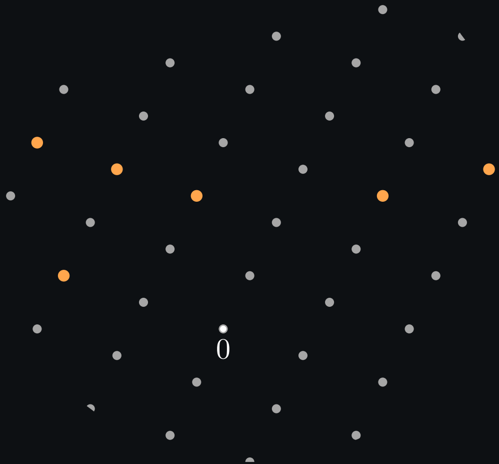
Classical: Time $= 2^{(0.292+o(1))n}$ Mem. $= 2^{(0.2075+o(1))n}$

Quantum: Time $= 2^{(0.265+o(1))n}$ Mem. $= 2^{(0.265+o(1))n}$

Basic 2-Sieve (Nguyen-Vidick sieve)

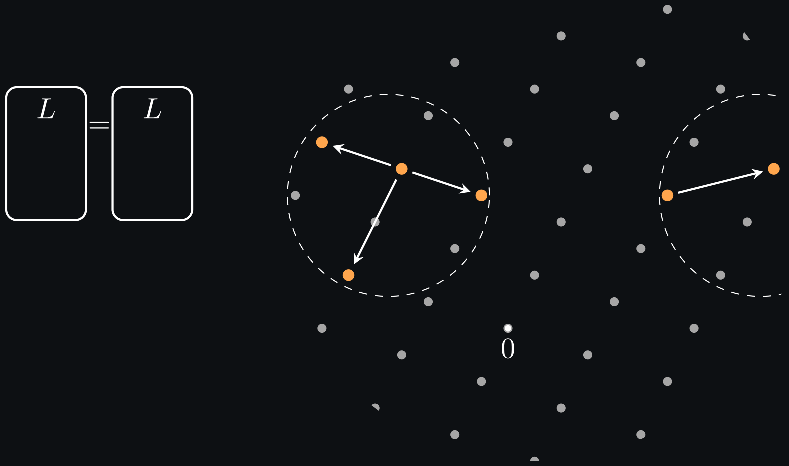
Main idea: Sample many Gaussian lattice vectors so that their sums give short(er) vectors





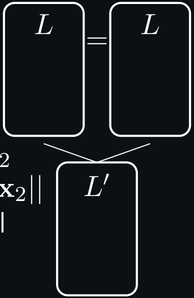
Basic 2-Sieve (Nguyen-Vidick sieve)

Main idea: Sample many Gaussian lattice vectors so that their sums give short(er) vectors

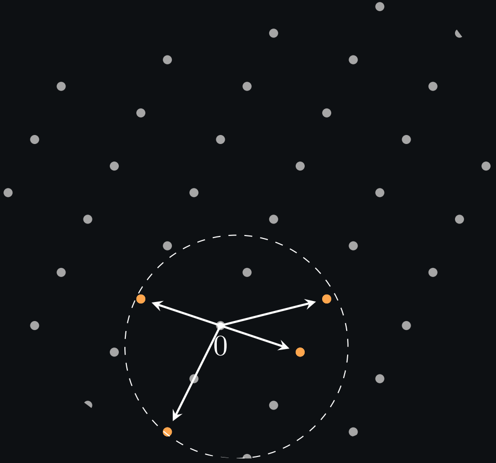


Basic 2-Sieve (Nguyen-Vidick sieve)

Main idea: Sample many Gaussian lattice vectors so that their sums give short(er) vectors

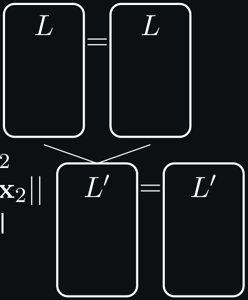


$\mathbf{x}_1 \pm \mathbf{x}_2$
$||\mathbf{x}_1 \pm \mathbf{x}_2||$
is small



Basic 2-Sieve (Nguyen-Vidick sieve)

Main idea: Sample many Gaussian lattice vectors so that their sums give short(er) vectors



$\mathbf{x}_1 \pm \mathbf{x}_2$

$||\mathbf{x}_1 \pm \mathbf{x}_2||$

is small

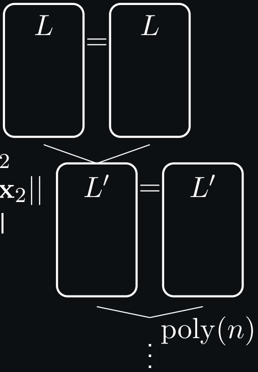
Basic 2-Sieve (Nguyen-Vidick sieve)

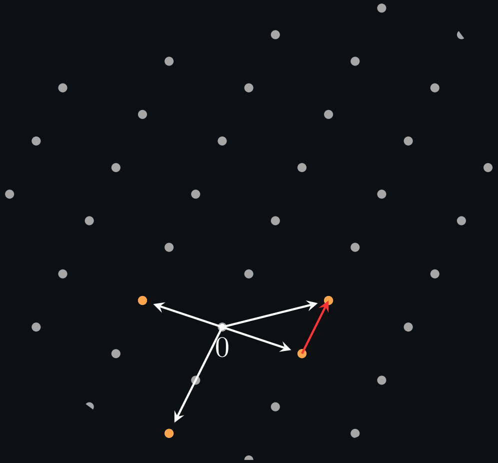
Main idea: Sample many Gaussian lattice vectors so that their sums give short(er) vectors

$\mathbf{x}_1 \pm \mathbf{x}_2$

$||\mathbf{x}_1 \pm \mathbf{x}_2||$

is small

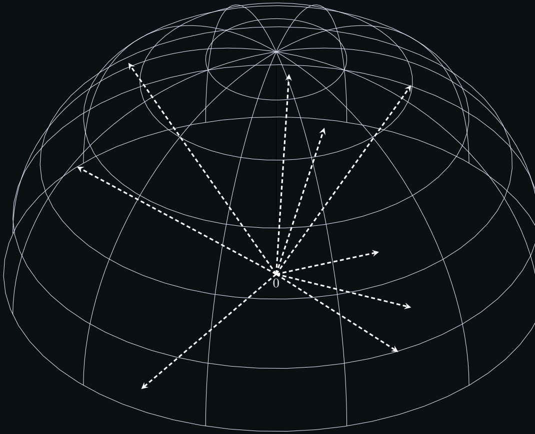




Main Routine in Sieving: 2-List problem on the unit sphere

Given 2-lists $L_1, L_2 \subset \mathcal{S}^{n-1}$ of iid. elements

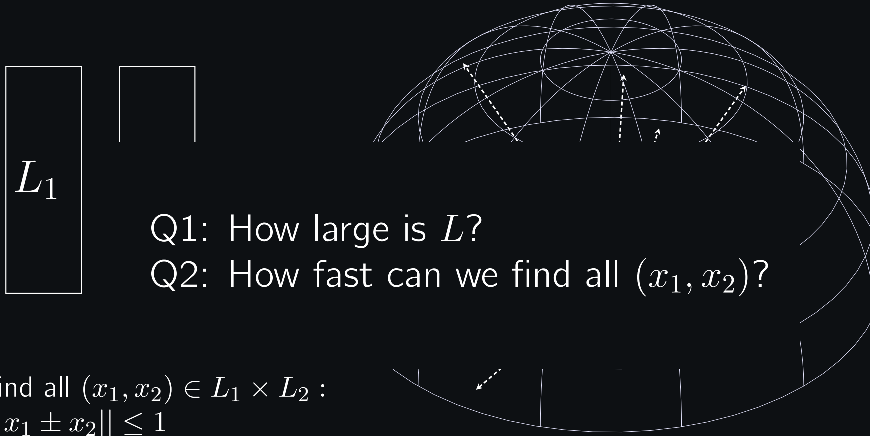
$$\boxed{L_1} \quad \boxed{L_2} \quad \subset$$



find all $(x_1, x_2) \in L_1 \times L_2$:
$||x_1 \pm x_2|| \leq 1$

Main Routine in Sieving: 2-List problem on the unit sphere

Given 2-lists $L_1, L_2 \subset \mathcal{S}^{n-1}$ of iid. elements



Q1: How large is L?

Q2: How fast can we find all (x_1, x_2)?

find all $(x_1, x_2) \in L_1 \times L_2$:
$||x_1 \pm x_2|| \leq 1$

Distribution of Gram matrices

Let $\mathcal{C} \in \mathbb{R}^{k \times k}$ be the Gram matrix of $x_1, \ldots, x_k \in \mathcal{S}^{n-1}$:

$$\mathcal{C}_{i.j} = \langle x_i \, , x_j \rangle$$

Distribution of Gram matrices

Let $\mathcal{C} \in \mathbb{R}^{k \times k}$ be the Gram matrix of $x_1, \ldots, x_k \in \mathcal{S}^{n-1}$:

$$\mathcal{C}_{i.j} = \langle x_i \,, x_j \rangle$$

- $\mathcal{C}$ determines the 2-norm of the sum:

$$|| \sum x_i ||^2 = k + 2 \sum_{i<j} \langle x_i \,, x_j \rangle$$

Distribution of Gram matrices

Let $\mathcal{C} \in \mathbb{R}^{k \times k}$ be the Gram matrix of $x_1, \ldots, x_k \in \mathcal{S}^{n-1}$:

$$\mathcal{C}_{i.j} = \langle x_i \, , x_j \rangle$$

- $\mathcal{C}$ determines the 2-norm of the sum:

$$|| \sum x_i ||^2 = k + 2 \sum_{i<j} \langle x_i \, , x_j \rangle$$

- The Gram matrix $\mathcal{C}(x_1, \ldots, x_k)$ follows a distribution with density function

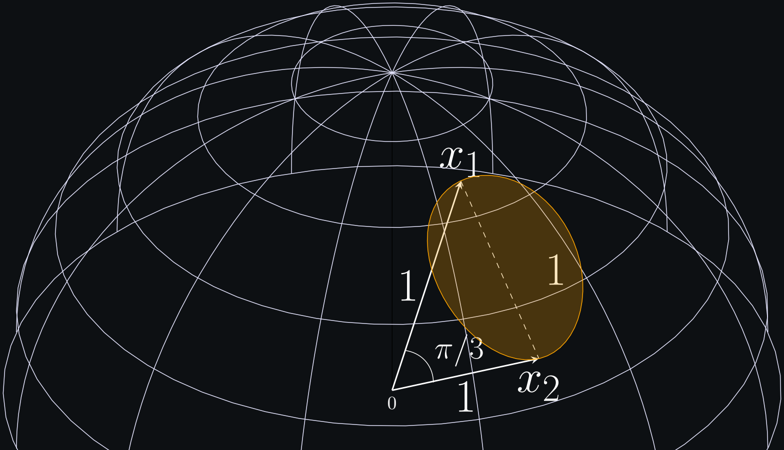
$$\mu_{\mathcal{C}} = \mathcal{O}(\det(\mathcal{C})^{\frac{1}{2}(n-k)}) \mathrm{d}C_{1,2} \ldots \mathrm{d}C_{k-1,k}$$

A proof is in [HK'17] and relies on the Wishart distribution

Q1: How large is L?

$$\mu_{\mathcal{C}} \approx \det(\mathcal{C})^{\frac{n}{2}} = \det \begin{pmatrix} 1 & \langle x_1 , x_2 \rangle \\ \langle x_1 , x_2 \rangle & 1 \end{pmatrix}^{\frac{n}{2}}$$

$$\det \begin{pmatrix} 1 & 1/2 \\ 1/2 & 1 \end{pmatrix} = \frac{3}{4} \implies |L| = \left(\frac{4}{3}\right)^{n/2+o(n)} = 2^{(0.2075+o(1))n}$$



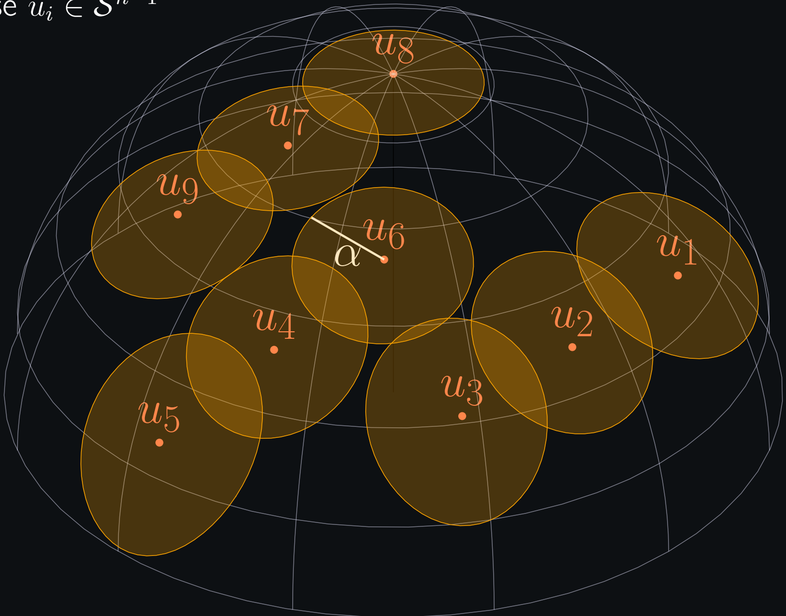
Q2: How fast can we find all (x_1, x_2)?

Brute force complexity: $|L|^2 = 2^{(0.415+o(1))n}$

To achieve $T = 2^{0.292+o(1)}$ use Near Neighbor search
(aka Locality-Sensitive techniques)

Locality-sensitive filtering [MO15, BGJ15, BDGL16]

choose $u_i \in \mathcal{S}^{n-1}$

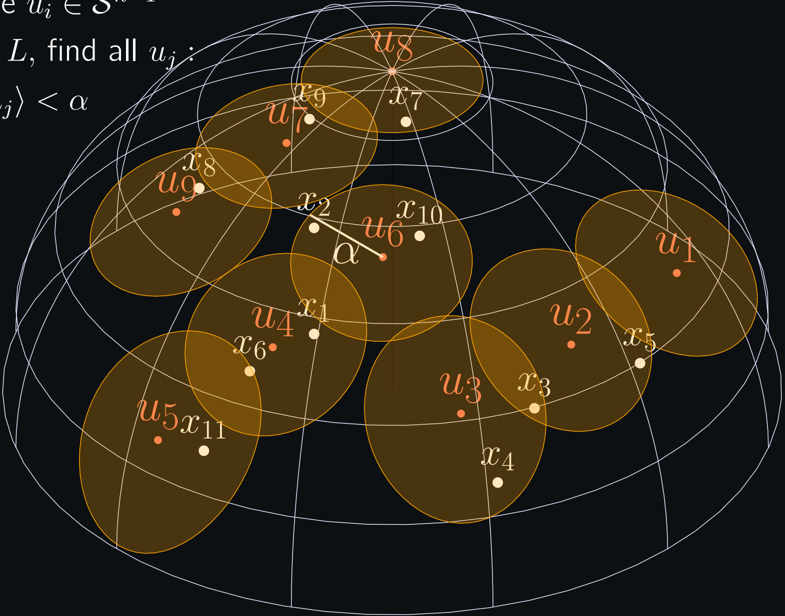


Locality-sensitive filtering [MO15, BGJ15, BDGL16]

choose $u_i \in \mathcal{S}^{n-1}$

$\forall x_i \in L$, find all u_j :

$\langle x_i \,, u_j \rangle < \alpha$



Locality-sensitive filtering [MO15, BGJ15, BDGL16]

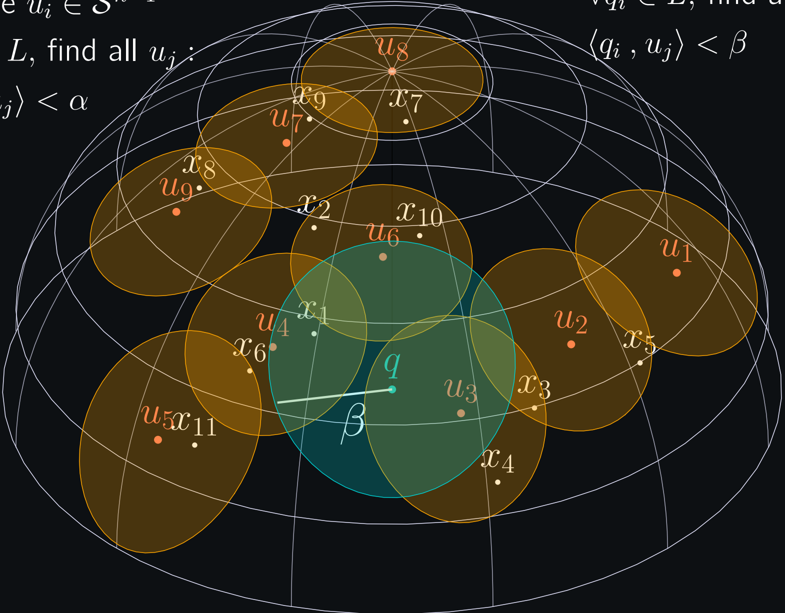
choose $u_i \in \mathcal{S}^{n-1}$

$\forall x_i \in L$, find all u_j :

$\langle x_i \, , u_j \rangle < \alpha$

$\forall q_i \in L$, find all u_j :

$\langle q_i \, , u_j \rangle < \beta$



Analysis I

1. How to find relevant centers fast?

Analysis I

1. How to find relevant centers fast?

   [MO15, BDGL16]: choose u from a product code.

   $$u \in C_1 \times C_2 \times \ldots \times C_t =: U,$$

   C_i - spherical codes of length $o(n)$.

   To obtain all close centers to $x = [x_1|x_2|\ldots|x_t]$, decode x_i wrt. C_i.

Analysis I

1. How to find relevant centers fast?

   [MO15, BDGL16]: choose u from a product code.

   $$u \in C_1 \times C_2 \times \ldots \times C_t =: U,$$

   C_i - spherical codes of length $o(n)$.

   To obtain all close centers to $x = [x_1|x_2|\ldots|x_t]$, decode x_i wrt. C_i.

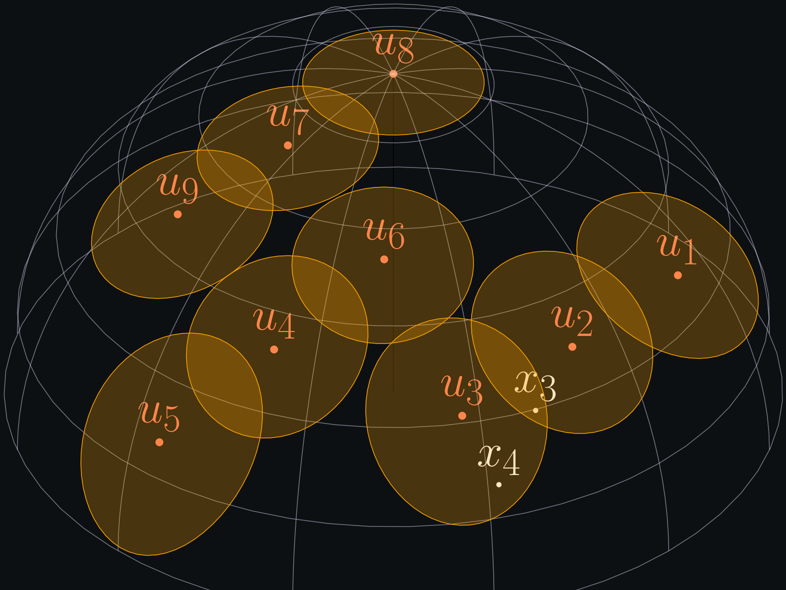
2. For each $x \in L$: finding all relevant $u_i \in U$:

   $$T_{\text{Update}} = |U| \cdot \Pr_{u_i \in \mathcal{S}^{n-1}} [\langle u_i\, , x\rangle < \alpha] = |U| \cdot (1-\alpha^2)^{n/2}.$$

Analysis I

1. How to find relevant centers fast?
   [MO15, BDGL16]: choose u from a product code.
   $$u \in C_1 \times C_2 \times \ldots \times C_t =: U,$$
   C_i - spherical codes of length $o(n)$.
   To obtain all close centers to $x = [x_1|x_2|\ldots|x_t]$, decode x_i wrt. C_i.
2. For each $x \in L$: finding all relevant $u_i \in U$:
   $$T_{\text{Update}} = |U| \cdot \Pr_{u_i \in \mathcal{S}^{n-1}} [\langle u_i\, , x \rangle < \alpha] = |U| \cdot (1-\alpha^2)^{n/2}.$$
3. For each $x \in L$: query all relevant $u_i \in U$:
   $$T_{\text{Query}} = |U| \cdot \Pr_{u_i \in \mathcal{S}^{n-1}} [\langle u_i\, , x \rangle < \beta] = |U| \cdot (1-\beta^2)^{n/2}.$$

How large is U?



How large is U?

$|U|$ is determined by $P = 1/|U|$ that conditioned on $\langle x_3 , x_4 \rangle = 1/2$

1. $\langle u , x_3 \rangle = \alpha$
2. $\langle u , x_4 \rangle = \beta$

$$P = \Pr_{u \in \mathcal{S}^{n-1}} [\langle u , x_3 \rangle = \alpha, \langle u , x_4 \rangle = \beta \mid \langle x_3 , x_4 \rangle = 1/2]$$

How large is U?

$|U|$ is determined by $P = 1/|U|$ that conditioned on $\langle x_3\,, x_4\rangle = 1/2$

1. $\langle u\,, x_3\rangle = \alpha$
2. $\langle u\,, x_4\rangle = \beta$

$$P = \Pr_{u \in \mathcal{S}^{n-1}} \left[\langle u\,, x_3\rangle = \alpha, \langle u\,, x_4\rangle = \beta \mid \langle x_3\,, x_4\rangle = 1/2\right]$$

$$= \frac{\left(\det\begin{pmatrix} 1 & \alpha & \beta \\ \alpha & 1 & c \\ \beta & c & 1 \end{pmatrix}\right)^{n/2}}{\left(\det\left(\begin{smallmatrix} 1 & c \\ c & 1 \end{smallmatrix}\right)\right)^{n/2}}.$$

How large is U?

$|U|$ is determined by $P = 1/|U|$ that conditioned on $\langle x_3\,, x_4\rangle = 1/2$

1. $\langle u\,, x_3\rangle = \alpha$
2. $\langle u\,, x_4\rangle = \beta$

$$P = \Pr_{u \in \mathcal{S}^{n-1}} \left[\langle u\,, x_3\rangle = \alpha, \langle u\,, x_4\rangle = \beta \mid \langle x_3\,, x_4\rangle = 1/2\right]$$

$$= \frac{\left(\det\begin{pmatrix} 1 & \alpha & \beta \\ \alpha & 1 & c \\ \beta & c & 1 \end{pmatrix}\right)^{n/2}}{\left(\det\left(\begin{smallmatrix} 1 & c \\ c & 1 \end{smallmatrix}\right)\right)^{n/2}}.$$

For $\alpha = \beta = c = 1/2,\ P^{-1} = \left(\frac{3}{2}\right)^{n/2} = 2^{0.292n}$

Quantum LSF [Laa'15]

Main idea: apply Grover search inside each bucket

Classical:

1. $T_{\text{Update}} = |U| \cdot (1 - \alpha^2)^{n/2}$
2. $T_{\text{Query}} = |U| \cdot (1 - \beta^2)^{n/2}$
3. Set $\alpha : |L| \cdot (1 - \alpha^2)^{n/2} = 1$

Quantum LSF [Laa'15]

Main idea: apply Grover search inside each bucket

Classical:

1. $T_{\text{Update}} = |U| \cdot (1-\alpha^2)^{n/2}$
2. $T_{\text{Query}} = |U| \cdot (1-\beta^2)^{n/2}$
3. Set $\alpha : |L| \cdot (1-\alpha^2)^{n/2} = 1$

Quantum:

1. $T_{\text{Update}} = |U| \cdot (1-\alpha^2)^{n/2}$
2. $T^{\text{Q}}_{\text{Query}} = |U| \cdot (1-\beta^2)^{n/2} +$ Grover Search inside each relevant center

Quantum LSF [Laa'15]

Main idea: apply Grover search inside each bucket

Classical:

1. $T_{\text{Update}} = |U| \cdot (1-\alpha^2)^{n/2}$
2. $T_{\text{Query}} = |U| \cdot (1-\beta^2)^{n/2}$
3. Set $\alpha : |L| \cdot (1-\alpha^2)^{n/2} = 1$

Quantum:

1. $T_{\text{Update}} = |U| \cdot (1-\alpha^2)^{n/2}$
2. $T^{\text{Q}}_{\text{Query}} = |U| \cdot (1-\beta^2)^{n/2} +$ Grover Search inside each relevant center

$$T^{\text{Q}}_{\text{Query}} = |U| \cdot (1-\beta^2)^{n/2} + \sqrt{|\#\text{ relevant centers }| \cdot |\text{Bucket size}| \cdot |\#\text{ solutions}|} = |U| \cdot (1-\beta^2)^{n/2} + \sqrt{|U| \cdot (1-\beta^2)^{n/2} \cdot |L| \cdot (1-\alpha^2)^{n/2} \cdot |L| \cdot (1-c^2)^{n/2}}$$

$T^{\text{Q}}_{\text{Query}} = T^{\text{Q}}_{\text{Update}}$ for $\alpha = \frac{\sqrt{3}}{4}$ and $|U| = (\frac{13}{9})^{n/2} = 2^{0.265 \cdot n}$

Other Ways to Attack SVP/LWE/SIS?

1. Low-memory SVP: Enumeration

   Classical : depth-first traversal of a tree of size

   $$T_{\mathsf{Enum}} = 2^{((1/2e)+o(1))n\log n}$$

   Quantum: back-tracking technique [ANS18]

   $$T^{\mathsf{Q}}_{\mathsf{Enum}} = 2^{((1/4e)+o(1))n\log n}$$

Other Ways to Attack SVP/LWE/SIS?

1. Low-memory SVP: Enumeration

   Classical : depth-first traversal of a tree of size

   $$T_{\mathsf{Enum}} = 2^{((1/2e)+o(1))n \log n}$$

   Quantum: back-tracking technique [ANS18]

   $$T^{\mathsf{Q}}_{\mathsf{Enum}} = 2^{((1/4e)+o(1))n \log n}$$

2. Low-mem. Sparse/binary secret LWE: Grover search:

   $$T_{\mathsf{Grover}} = 2^{\frac{1}{2}|\mathsf{Search\ space}|}$$

3. Sparse/binary secret LWE: BKW: quantum speed-up for distinguishing phase.

Other Ways to Attack SVP/LWE/SIS?

1. Low-memory SVP: Enumeration

   Classical : depth-first traversal of a tree of size

   $$T_{\mathsf{Enum}} = 2^{((1/2e)+o(1))n\log n}$$

   Quantum: back-tracking technique [ANS18]

   $$T^{\mathsf{Q}}_{\mathsf{Enum}} = 2^{((1/4e)+o(1))n\log n}$$

2. Low-mem. Sparse/binary secret LWE: Grover search:

   $$T_{\mathsf{Grover}} = 2^{\frac{1}{2}|\mathsf{Search\ space}|}$$

3. Sparse/binary secret LWE: BKW: quantum speed-up for distinguishing phase.

Thank you!

References I

- [ANS18] Y. Aono, P. Q. Nguyen, Y. Shen. Quantum Lattice Enumeration and Tweaking Discrete Pruning
- [BDGL16] A. Becker, L. Ducas, N. Gama, T. Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving.
- [Laa15] T. Laarhoven. Search problems in cryptography. PhD thesis
- [MO15] A. May, I.Ozerov. On Computing Nearest Neighbors with Applications to Decoding of Binary Linear Codes