A k-List Algorithm for LWE

Elena Kirshanova

I. Kant Baltic Federal University

based on joint work with Z.Brakerski, D. Stehlé, W.Wen

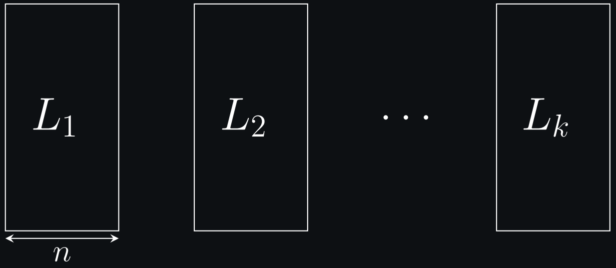
Lattices: Geometry, Algorithms and Hardness
The Simons Institute for the Theory of Computing
March 1, 2020

Outline

- The k-List Problem
- The Learning with Errors Problem (LWE)
- The (Extended) Dihedral Coset Problem (DCP)
- Reduction from LWE to EDCP
- Solving EDCP/LWE via k-Lists

Definition: the k-List problem

Given k-lists $L_1, \ldots, L_k \subset \mathbb{R}^n$ of iid. elements and a relation $\mathcal{R}$



find all/almost all/a fraction of $(x_1, \ldots, x_k) \in L_1 \times \ldots \times L_k$ s.t.

$\mathcal{R}(x_1, \ldots, x_k)$ is satisfied

- L_i are of the same size and can be identical
- $|L_i|$ is set s.t. enough solutions exist

Example: k-XOR (Wagner'02)

Given k-lists $L_1, \ldots, L_k \subset \mathbb{F}_2^n$ of iid. elements

$$\boxed{L_1} \qquad \boxed{L_2} \qquad \cdots \qquad \boxed{L_k}$$

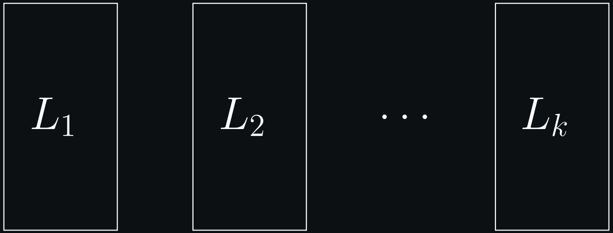
find almost all $(x_1, \ldots, x_k) \in L_1 \times \ldots \times L_k$ s.t.

$$x_1 \oplus \ldots \oplus x_k = 0$$

- $|L_i| = 2^{\mathcal{O}(\sqrt{n})}$, Runtime: $2^{\mathcal{O}(\sqrt{n})}$

This talk

Given k-lists $L_1, \ldots, L_k \subset \mathbb{Z}_q^n$ of iid. elements



find almost all $(x_1, \ldots, x_k) \in L_1 \times \ldots \times L_k$ s.t.

$$x_1 + \ldots + x_k = [0,\, 0, \ldots, 0]$$

- BKW algorithm for LWE
- Kuperberg's algorithm for the Dihedral Coset Problem

The <u>L</u>earning <u>W</u>ith <u>E</u>rrors Problem (Regev'05)

Dimension: n, modulus: $q = \mathrm{poly}(n)$, $0 < \alpha < 1$

<u>LWE</u>: For fixed secret $\mathbf{s} \in \mathbb{Z}_q^n$,
given

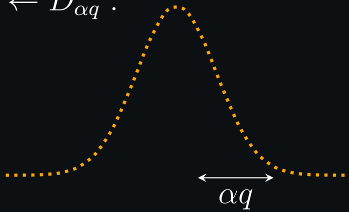
$(\mathbf{a}_1, \langle \mathbf{a}_1 , \mathbf{s} \rangle + e_1 \bmod q) \in \mathbb{Z}_q^{n+1}$

$\vdots$

$(\mathbf{a}_m, \langle \mathbf{a}_m , \mathbf{s} \rangle + e_m \bmod q) \in \mathbb{Z}_q^{n+1}$,

find $\mathbf{s}$.

$e_i \leftarrow D_{\alpha q}$:



Typical parameters: $n = \Theta(\text{bit security})$, $q = n^{\Theta(1)}$,
$m = \Theta(n \log q)$, $\alpha = \sqrt{n}/q$

The (Extended) Dihedral Coset Problem

Dimension: n, modulus: q, an integer $M \geq 1$

EDCP: For secret $\mathbf{s} \in \mathbb{Z}_q^n$, given

$$\sum_{j=0}^{M-1} |j\rangle \, |\mathbf{x}_1 + j \cdot \mathbf{s} \bmod q\rangle \, ,$$
$$\vdots$$
$$\sum_{j=0}^{M-1} |j\rangle \, |\mathbf{x}_m + j \cdot \mathbf{s} \bmod q\rangle$$

find $\mathbf{s}$.

The (Extended) Dihedral Coset Problem

Dimension: n, modulus: q, an integer $M \geq 1$

EDCP: For secret $\mathbf{s} \in \mathbb{Z}_q^n$, given

$$\sum_{j=0}^{M-1} |j\rangle \, |\mathbf{x}_1 + j \cdot \mathbf{s} \bmod q\rangle \,,$$
$$\vdots$$
$$\sum_{j=0}^{M-1} |j\rangle \, |\mathbf{x}_m + j \cdot \mathbf{s} \bmod q\rangle$$

find $\mathbf{s}$.

- For $m = \mathcal{O}(n \log q)$, $\mathbf{s}$ is unique whp.
- For $n = 1, M = 2$ the problem is called the Dihedral Coset Problem. Samples are of the form

$$|0\rangle \, |x\rangle + |1\rangle \, |x + s \bmod q\rangle$$

LWE vs. DCP

<u>LWE</u>: Given

$$(\mathbf{a}_1, \langle \mathbf{a}_1 , \mathbf{s}\rangle + e_1 \bmod q)$$
$$\vdots$$
$$(\mathbf{a}_m, \langle \mathbf{a}_m, \mathbf{s}\rangle + e_m \bmod q),$$

find $\mathbf{s} \in \mathbb{Z}_q^n$

<u>DCP</u>: Given

$$|0, x_1\rangle + |1, x_1 + s \bmod q^n\rangle$$
$$\vdots$$
$$|0, x_\ell\rangle + |1, x_\ell + s \bmod q^n\rangle$$

find $s \in \mathbb{Z}_{q^n}$

LWE vs. DCP

LWE: Given

$(\mathbf{a}_1, \langle \mathbf{a}_1 , \mathbf{s}\rangle + e_1 \bmod q)$

$\vdots$

$(\mathbf{a}_m, \langle \mathbf{a}_m, \mathbf{s}\rangle + e_m \bmod q)$,

find $\mathbf{s} \in \mathbb{Z}_q^n$

$\leq$

[Regev'02]

DCP: Given

$|0, x_1\rangle + |1, x_1 + s \bmod q^n\rangle$

$\vdots$

$|0, x_\ell\rangle + |1, x_\ell + s \bmod q^n\rangle$

find $s \in \mathbb{Z}_{q^n}$

LWE vs. EDCP

LWE: Given

$(\mathbf{a}_1, \langle \mathbf{a}_1 , \mathbf{s}\rangle + e_1 \bmod q)$

$\vdots$

$(\mathbf{a}_m, \langle \mathbf{a}_m, \mathbf{s}\rangle + e_m \bmod q)$,

find $\mathbf{s} \in \mathbb{Z}_q^n$

$\Longleftrightarrow$ [BKSW'18]

EDCP: Given

$\sum_{j=0}^{M-1} |j\rangle \, |\mathbf{x}_1 + j \cdot \mathbf{s} \bmod q\rangle$

$\vdots$

$\sum_{j=0}^{M-1} |j\rangle \, |\mathbf{x}_\ell + j \cdot \mathbf{s} \bmod q\rangle$

find $s \in \mathbb{Z}_{q^n}$

LWE vs. EDCP

<u>LWE</u>:

dim: n
samples: m
modulus: q
st.dev: αq

$\longrightarrow$

<u>EDCP</u>:

dim: n
samples: ℓ
modulus: q

$$M \approx \frac{1}{mn\alpha\ell q^{n/m}}$$

LWE vs. EDCP

LWE:		EDCP:
dim: n	$\longrightarrow$	dim: n
# samples: m		# samples: ℓ
modulus: q		modulus: q
st.dev: αq		$M \approx \dfrac{1}{mn\alpha\ell q^{n/m}}$
dim: n	$\longleftarrow$	dim: n
# samples: ℓ		# samples: ℓ
modulus: q		modulus: q
st.dev: q/M		# shifts: M

LWE vs. EDCP

LWE:

dim: n
\# samples: m
modulus: q
st.dev: αq

$\boxed{\longrightarrow}$

EDCP:

dim: n
\# samples: ℓ
modulus: q
$M \approx \dfrac{1}{mn\alpha\ell q^{n/m}}$

dim: n
\# samples: ℓ
modulus: q
st.dev: q/M

$\longleftarrow$

dim: n
\# samples: ℓ
modulus: q
\# shifts: M

From LWE to ECDP (Regev'02, BKSW'18)

Given: LWE samples: $(A, \mathbf{b}_0 = A\mathbf{s}_0 + \mathbf{e}_0) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$

From LWE to ECDP (Regev'02, BKSW'18)

Given: LWE samples: $(A, \mathbf{b}_0 = A\mathbf{s}_0 + \mathbf{e}_0) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$

1. Prepare the state (normalisations omitted)

$$\sum_{\mathbf{s} \in \mathbb{Z}_q^n} \Big(\sum_{j \in \mathbb{Z}} \rho_r(j) \left| j \right\rangle \Big) \left| \mathbf{s} \right\rangle \approx \sum_{\substack{\mathbf{s} \in \mathbb{Z}_q^n \\ j \in \mathbb{Z} \cap [-M, M]}} \rho_r(j) \left| j \right\rangle \left| \mathbf{s} \right\rangle$$

From LWE to ECDP (Regev'02, BKSW'18)

Given: LWE samples: $(A, \mathbf{b}_0 = A\mathbf{s}_0 + \mathbf{e}_0) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$

1. Prepare the state (normalisations omitted)

$$\sum_{\mathbf{s} \in \mathbb{Z}_q^n} \left(\sum_{j \in \mathbb{Z}} \rho_r(j) \left| j \right\rangle \right) \left| \mathbf{s} \right\rangle \approx \sum_{\substack{\mathbf{s} \in \mathbb{Z}_q^n \\ j \in \mathbb{Z} \cap [-M, M]}} \rho_r(j) \left| j \right\rangle \left| \mathbf{s} \right\rangle$$

2. Evaluate the function $f(j, \mathbf{s}) \to A\mathbf{s} - j\mathbf{b} \bmod q$

$$\sum_{\mathbf{s}, j} \rho_r(j) \left| j \right\rangle \left| \mathbf{s} \right\rangle \left| A\mathbf{s} - j \cdot A\mathbf{s}_0 - j\mathbf{e}_0 \right\rangle \ =$$

From LWE to ECDP (Regev'02, BKSW'18)

Given: LWE samples: $(A, \mathbf{b}_0 = A\mathbf{s}_0 + \mathbf{e}_0) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$

1. Prepare the state (normalisations omitted)

$$\sum_{\mathbf{s} \in \mathbb{Z}_q^n} \left(\sum_{j \in \mathbb{Z}} \rho_r(j) \left| j \right\rangle \right) \left| \mathbf{s} \right\rangle \approx \sum_{\substack{\mathbf{s} \in \mathbb{Z}_q^n \\ j \in \mathbb{Z} \cap [-M, M]}} \rho_r(j) \left| j \right\rangle \left| \mathbf{s} \right\rangle$$

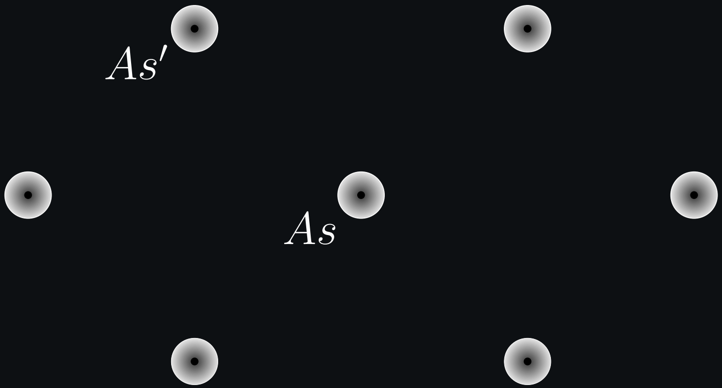
2. Evaluate the function $f(j, \mathbf{s}) \to A\mathbf{s} - j\mathbf{b} \bmod q$

$$\sum_{\mathbf{s}, j} \rho_r(j) \left| j \right\rangle \left| \mathbf{s} \right\rangle \left| A\mathbf{s} - j \cdot A\mathbf{s}_0 - j\mathbf{e}_0 \right\rangle \ =$$

$$\sum_{\mathbf{s}, j} \rho_r(j) \left| j \right\rangle \left| \mathbf{s} + j\mathbf{s}_0 \right\rangle \left| A\mathbf{s} - j\mathbf{e}_0 \right\rangle$$

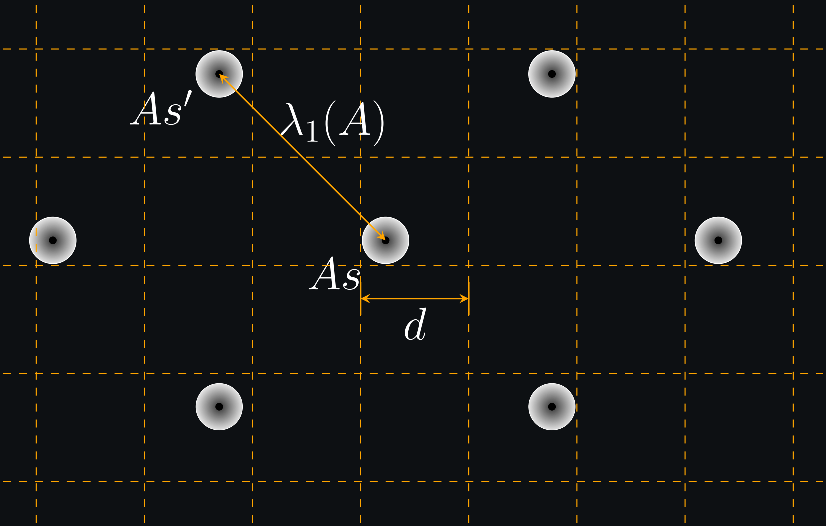
From LWE to ECDP (Regev'02, BKSW'18)

$$\sum_{\mathbf{s},\,j} \rho_r(j)\,|j\rangle\,|\mathbf{s}+j\mathbf{s}_0\rangle\,|A\mathbf{s}-j\mathbf{e}_0\rangle$$



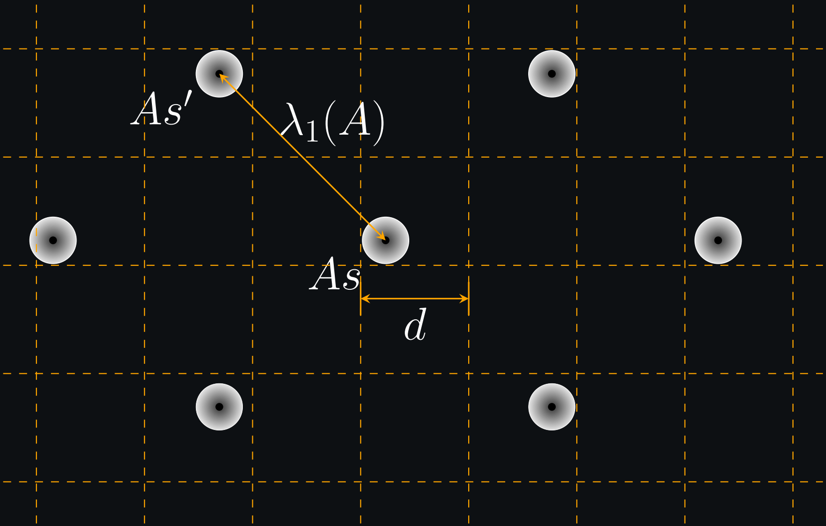
From LWE to ECDP (Regev'02, BKSW'18)

$$\sum_{\mathbf{s},\, j} \rho_r(j)\, |j\rangle\, |\mathbf{s} + j\mathbf{s}_0\rangle\, |A\mathbf{s} - j\mathbf{e}_0\rangle$$



From LWE to ECDP (Regev'02, BKSW'18)

$$\sum_{\mathbf{s},\, j} \rho_r(j)\,|j\rangle\,|\mathbf{s}+j\mathbf{s}_0\rangle\,\underline{|A\mathbf{s}-j\mathbf{e}_0\rangle} \to \underline{|\lceil (A\mathbf{s}-j\mathbf{e}_0)/d \rfloor\rangle}$$



From LWE to ECDP (Regev'02, BKSW'18)

3. $$\sum_{\mathbf{s},\,j} \rho_r(j)\,|j\rangle\,|\mathbf{s}+j\mathbf{s}_0\rangle\,|A\mathbf{s}-j\mathbf{e}_0\rangle \to$$

$$\sum_{\mathbf{s},\,j} \rho_r(j)\,|j\rangle\,|\mathbf{s}+j\mathbf{s}_0\rangle\,|A\mathbf{s}-j\mathbf{e}_0\rangle\,|\mathsf{Box}(A\mathbf{s}-j\mathbf{e}_0)\rangle$$

From LWE to ECDP (Regev'02, BKSW'18)

3. $$\sum_{\mathbf{s},j} \rho_r(j) \left|j\right\rangle \left|\mathbf{s} + j\mathbf{s}_0\right\rangle \left|A\mathbf{s} - j\mathbf{e}_0\right\rangle \to$$
$$\sum_{\mathbf{s},j} \rho_r(j) \left|j\right\rangle \left|\mathbf{s} + j\mathbf{s}_0\right\rangle \left|A\mathbf{s} - j\mathbf{e}_0\right\rangle \left|\mathsf{Box}(A\mathbf{s} - j\mathbf{e}_0)\right\rangle$$

4. Measure the last register:

$$\sum_{j \in \mathbb{Z} \cap [-M,M]} \rho_r(j) \left|j\right\rangle \left|\mathbf{s} + j\mathbf{s}_0\right\rangle \left|A\mathbf{s} - j\mathbf{e}_0\right\rangle$$

for $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$

From LWE to ECDP (Regev'02, BKSW'18)

3. $$\sum_{\mathbf{s},j} \rho_r(j)\,|j\rangle\,|\mathbf{s}+j\mathbf{s}_0\rangle\,|A\mathbf{s}-j\mathbf{e}_0\rangle \to$$
$$\sum_{\mathbf{s},j} \rho_r(j)\,|j\rangle\,|\mathbf{s}+j\mathbf{s}_0\rangle\,|A\mathbf{s}-j\mathbf{e}_0\rangle\,|\mathsf{Box}(A\mathbf{s}-j\mathbf{e}_0)\rangle$$

4. Measure the last register:
$$\sum_{j\in\mathbb{Z}\cap[-M,M]} \rho_r(j)\,|j\rangle\,|\mathbf{s}+j\mathbf{s}_0\rangle\,|A\mathbf{s}-j\mathbf{e}_0\rangle$$
for $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$

5. Uncompute $A\mathbf{s}-j\mathbf{e}_0$ by applying $f'(j,\mathbf{s},\mathbf{b}) \to \mathbf{b}-A\mathbf{s}+j\mathbf{b}_0$
$$\sum_{j\in\mathbb{Z}\cap[-M,M]} \rho_r(j)\,|j\rangle\,|\mathbf{s}+j\mathbf{s}_0\rangle$$

How hard is EDCP?

$\omega(x) := \exp(2i\pi x)$

$$\sum_{j=0}^{M-1} |j\rangle\, |\mathbf{x} + j\mathbf{s} \bmod q\rangle$$

How hard is EDCP?

$\omega(x) := \exp(2i\pi x)$

$$\sum_{j=0}^{M-1} |j\rangle \, |\mathbf{x} + j\mathbf{s} \bmod q\rangle$$

$$\xrightarrow{QFT \text{ over } \mathbb{Z}_q^n}$$

$$\sum_{\mathbf{y} \in \mathbb{Z}_q^n} \sum_{j=0}^{M-1} \omega\left(\frac{\langle \mathbf{x} + j\mathbf{s} \, , \, \mathbf{y}\rangle}{q}\right) |j\rangle \, |\mathbf{y}\rangle$$

How hard is EDCP?

$\omega(x) := \exp(2i\pi x)$

$$\sum_{j=0}^{M-1} |j\rangle \, |\mathbf{x} + j\mathbf{s} \bmod q\rangle$$

$$\xrightarrow{QFT \text{ over } \mathbb{Z}_q^n}$$

$$\sum_{\mathbf{y} \in \mathbb{Z}_q^n} \sum_{j=0}^{M-1} \omega\left(\frac{\langle \mathbf{x} + j\mathbf{s} \,, \mathbf{y}\rangle}{q}\right) |j\rangle \, |\mathbf{y}\rangle$$

Measure $\mathbf{y}$:

$$\sum_{j=0}^{M-1} \omega\left(\frac{\langle \mathbf{x} + j\mathbf{s} \,, \mathbf{y}\rangle}{q}\right) |j\rangle \,, \;\; \mathbf{y} \xleftarrow{\$} \mathbb{Z}_q^n$$

$$= \sum_{j=0}^{M-1} \omega\left(\frac{j\langle \mathbf{s} \,, \mathbf{y}\rangle}{q}\right) |j\rangle$$

How hard is EDCP?

$\omega(x) := \exp(2i\pi x)$

$$|\psi\rangle = \sum_{j=0}^{M-1} \omega\left(\frac{j\langle \mathbf{s},\mathbf{y}\rangle}{q}\right)|j\rangle\,,\ \mathbf{y} \xleftarrow{\$} \mathbb{Z}_q^n$$

How hard is EDCP?

$\omega(x) := \exp(2i\pi x)$

$$|\psi\rangle = \sum_{j=0}^{M-1} \omega\left(\frac{j\langle \mathbf{s}, \mathbf{y}\rangle}{q}\right) |j\rangle\,,\ \mathbf{y} \xleftarrow{\$} \mathbb{Z}_q^n$$

If $M = q$: $|\psi\rangle = \mathsf{QFT}\,|\langle \mathbf{s}\,, \mathbf{y}\rangle\rangle \Rightarrow \mathrm{poly}(n)$

If $M = q^\epsilon$ and n is "small" $\Rightarrow \mathrm{poly}(n)$ [Childs-vanDam'05]

If $M = o(n)$ or $M = \Theta(1)$: Kuperbeg's algorithm [Kup'05, Kup'11]

$$|\psi\rangle = \sum_{j=0}^{M-1} \omega\left(\frac{j\langle \mathbf{s},\mathbf{y}\rangle}{q}\right)|j\rangle\,,\ \mathbf{y} \xleftarrow{\$} \mathbb{Z}_q^n$$

Goal: find s_1.

$$|\psi\rangle = \sum_{j=0}^{M-1} \omega\left(\frac{j\langle \mathbf{s},\mathbf{y}\rangle}{q}\right)|j\rangle\ ,\ \mathbf{y} \xleftarrow{\$} \mathbb{Z}_q^n$$

Goal: find s_1.

Let $\mathbf{y} = [q/M, q,\ \ldots\ q]$. Then

$$|\psi\rangle = \sum_{j=0}^{M-1} \omega\left(\frac{j \cdot s_1}{M}\right)|j\rangle \xrightarrow{\text{QFT}} s_1 \bmod M$$

Such $\mathbf{y}$ appears with probability $1/q^n$.

Kuperberg's algorithm for EDCP

$\omega(x) := \exp(2i\pi x)$

$$|\psi\rangle = \sum_{j=0}^{M-1} \omega\left(\frac{j\langle \mathbf{s}, \mathbf{y}\rangle}{q}\right)|j\rangle\,,\ \mathbf{y} \xleftarrow{\$} \mathbb{Z}_q^n$$

Goal: find s_1. Assumption: $q = 2^k$.

Idea: combine several $|\psi_i\rangle$ to get $\mathbf{y} = [q/M, q,\ \dots\ q]$.

Kuperberg's algorithm for EDCP

$\omega(x) := \exp(2i\pi x)$

$$|\psi\rangle = \sum_{j=0}^{M-1} \omega\left(\frac{j\langle \mathbf{s},\mathbf{y}\rangle}{q}\right)|j\rangle\,,\ \mathbf{y} \xleftarrow{\$} \mathbb{Z}_q^n$$

Goal: find s_1. Assumption: $q = 2^k$.

Idea: combine several $|\psi_i\rangle$ to get $\mathbf{y} = [q/M, q, \ \dots \ q]$.

$$\begin{aligned}|\psi_1\rangle \otimes |\psi_2\rangle &= \sum_{j_1=0}^{M-1}\sum_{j_2=0}^{M-1} \omega\left(\frac{j_1\langle \mathbf{s}\,,\mathbf{y}_1\rangle + j_2\langle \mathbf{s}\,,\mathbf{y}_2\rangle}{q}\right)|j_1, j_2\rangle \\ &= \sum_{j_1=0}^{M-1}\sum_{j_2=0}^{M-1} \omega\left(\frac{\langle \mathbf{s}\,, j_1\cdot\mathbf{y}_1 + j_2\cdot\mathbf{y}_2\rangle}{q}\right)|j_1, j_2\rangle\end{aligned}$$

Kuperberg's algorithm for EDCP

$\omega(x) := \exp(2i\pi x)$

$$|\psi\rangle = \sum_{j=0}^{M-1} \omega\left(\frac{j\langle \mathbf{s}, \mathbf{y}\rangle}{q}\right)|j\rangle\,,\ \mathbf{y} \xleftarrow{\$} \mathbb{Z}_q^n$$

Goal: find s_1. Assumption: $q = 2^k$.

Idea: combine several $|\psi_i\rangle$ to get $\mathbf{y} = [q/M, q, \ \ldots \ q]$.

$$\begin{aligned}|\psi_1\rangle \otimes |\psi_2\rangle &= \sum_{j_1=0}^{M-1}\sum_{j_2=0}^{M-1} \omega\left(\frac{j_1\langle \mathbf{s}\,,\mathbf{y}_1\rangle + j_2\langle \mathbf{s}\,,\mathbf{y}_2\rangle}{q}\right)|j_1, j_2\rangle \\ &= \sum_{j_1=0}^{M-1}\sum_{j_2=0}^{M-1} \omega\left(\frac{\langle \mathbf{s}\,, j_1\cdot\mathbf{y}_1 + j_2\cdot\mathbf{y}_2\rangle}{q}\right)|j_1, j_2\rangle\end{aligned}$$

Go on board...

Kuperberg's algorithm for EDCP

- A strategy: zero-ize i bits on the i-th step. This gives

$$\begin{aligned}\text{Time / classical mem.:}\quad & 2^{\sqrt{2n\log q}+o(\sqrt{n\log q})}\\ \#\text{Samples}:\quad & 2^{\sqrt{2n\log q}+o(\sqrt{n\log q})}\\ \text{Quantum memory}:\quad & \mathrm{poly}(n)\end{aligned}$$

Kuperberg's algorithm for EDCP

- A strategy: zero-ize i bits on the i-th step. This gives

$$\text{Time / classical mem.:}\quad 2^{\sqrt{2n\log q}+o(\sqrt{n\log q})}$$
$$\#\text{Samples}:\quad 2^{\sqrt{2n\log q}+o(\sqrt{n\log q})}$$
$$\text{Quantum memory}:\quad \mathrm{poly}(n)$$

- In general, if ℓ samples are given

$$\text{Time}:\quad 2^{\mathcal{O}\left(\lg\ell+\frac{n\lg q}{\lg\ell}\right)}$$
$$\text{Quantum memory}:\quad \mathrm{poly}(n)$$

- Reduction from LWE gives $\ell = \mathrm{poly}(n)$ samples
- This is inferior (by the constant in the exponent) to lattice attacks

Conclusions / Open Problems

- Kuperberg's algorithm for EDCP is a quantum analogue of BKW for LWE.
  Does not require many samples.
  Asymptotically no better than lattice-based attacks on LWE

Conclusions / Open Problems

- Kuperberg's algorithm for EDCP is a quantum analogue of BKW for LWE.
  Does not require many samples.
  Asymptotically no better than lattice-based attacks on LWE
- Q1: Better (but may be slower) space separation?
- Q2: Improve the algorithm for binary $\mathbf{s}$

Conclusions / Open Problems

- Kuperberg's algorithm for EDCP is a quantum analogue of BKW for LWE.
  Does not require many samples.
  Asymptotically no better than lattice-based attacks on LWE
- Q1: Better (but may be slower) space separation?
- Q2: Improve the algorithm for binary $\mathbf{s}$

Thank you!

References

- [BKSW18] Z. Brakerski, E. Kirshanova, D. Stehlé, W. Wen. Learning With Errors and Extrapolated Dihedral Cosets
- [Regev02] O.Regev. Quantum computation and lattice problems
- [Regev05] O.Regev. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography
- [RSW18]M. Rosca, D.Stehlé, A. Wallet. On the ring-LWE and polynomial-LWE problems.
- [Wagner'02] D. Wagner. A Generalized Birthday Problem