A quasi-polynomial time quantum algorithm for the extrapolated dihedral coset problem

Shi Bai[1], Hansraj Jangir[1], Elena Kirshanova[2], Tran Ngo[1], William Youmans[1]

[1]Florida Atlantic University, Boca Raton
[2]Technology Innovation Institute, Abu Dhabi

https://eprint.iacr.org/2025/1046

Seminar at COSMIQ

LWE and the Dihedral Coset Problem

Dimension: n, modulus: $q = \mathrm{poly}(n)$

LWE: Given

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

with $\|\mathbf{e}\| \ll q$, find $\mathbf{s}$.

LWE and the Dihedral Coset Problem

Dimension: n, modulus: $q = \mathrm{poly}(n)$

LWE: Given

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

with $\|\mathbf{e}\| \ll q$, find $\mathbf{s}$.

DCP: Given

$$|0, x_1\rangle + |1, x_1 + s \bmod N\rangle$$
$$\vdots$$
$$|0, x_\ell\rangle + |1, x_\ell + s \bmod N\rangle$$

find s.

LWE and the Dihedral Coset Problem

Dimension: n, modulus: $q = \mathrm{poly}(n)$

LWE: Given

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

with $\|\mathbf{e}\| \ll q$, find $\mathbf{s}$.

$\leq$
[Regev'02]

DCP: Given

$$|0, x_1\rangle + |1, x_1 + s \bmod N\rangle$$
$$\vdots$$
$$|0, x_\ell\rangle + |1, x_\ell + s \bmod N\rangle$$

find s.

LWE and the Dihedral Coset Problem

Dimension: n, modulus: $q = \mathrm{poly}(n)$

LWE: Given

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

with $\|\mathbf{e}\| \ll q$, find $\mathbf{s}$.

$\leq$
[Regev'02]

DCP: Given

$$|0, x_1\rangle + |1, x_1 + s \bmod N\rangle$$
$$\vdots$$
$$|0, x_\ell\rangle + |1, x_\ell + s \bmod N\rangle$$

find s.

Does not improve upon classical algorithms

LWE and the Dihedral Coset Problem

Dimension: n, modulus: $q = \text{poly}(n)$

$\leq$
[Regev'02]

LWE: Given

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

with $\|\mathbf{e}\| \ll q$, find $\mathbf{s}$.

DCP: Given

$$|0, x_1\rangle + |1, x_1 + s \bmod N\rangle$$
$$\vdots$$
$$|0, x_\ell\rangle + |1, x_\ell + s \bmod N\rangle$$

find s.

Does not improve upon classical algorithms

BKW / lattices:

$$2^{\mathcal{O}\left(n \cdot \frac{\log q \log n}{(\log q - \log e_i)^2}\right)}$$

Kuperberg:

$$2^{\mathcal{O}(\log \ell + \log N / \log \ell)}$$

The reduction produces $\ell = \text{poly}(n)$, $N = 2^{n^2}$

Inverse direction

Is DCP $\leq$ LWE?

- might give a strong evidence for quantum hardness of **LWE**
- DCP might be too ‘hard’ for LWE

Inverse direction

Is DCP $\leq$ LWE?

- might give a strong evidence for quantum hardness of **LWE**
- DCP might be too 'hard' for LWE

Answer:

No, but we known that $\underline{\text{E}}$DCP $\leq$ LWE [BKSW18]

Extrapolated DCP

EDCP for a distr. $\mathcal{D}$	DCP
$\sum_{j \in \mathsf{sup}(\mathcal{D})} \mathcal{D}(j) \lvert j \rangle \lvert \mathbf{x} + j \cdot \mathbf{s} \bmod q \rangle$	$\lvert 0 \rangle \lvert x \rangle + \lvert 1 \rangle \lvert x + s \bmod N \rangle$

Extrapolated DCP

<u>EDCP</u>

for a distr. $\mathcal{D}$

$$\sum_{j \in \mathsf{sup}(\mathcal{D})} \mathcal{D}(j) \left|j\right\rangle \left|\mathbf{x} + j \cdot \mathbf{s} \bmod q\right\rangle$$

<u>DCP</u>

$$\left|0\right\rangle \left|x\right\rangle + \left|1\right\rangle \left|x + s \bmod N\right\rangle$$

<u>U-EDCP$_{n,q,M}$</u>

Examples: $\sum_{j=0}^{M-1} \left|j\right\rangle \left|\mathbf{x} + j \cdot \mathbf{s} \bmod q\right\rangle$

<u>G-EDCP$_{n,q,r}$</u>

$$\sum_{j \in \mathbb{Z}} \rho_r(j) \left|j\right\rangle \left|\mathbf{x} + j \cdot \mathbf{s}\right\rangle$$

Extrapolated DCP

EDCP for a distr. $\mathcal{D}$

$$\sum_{j\in\mathsf{sup}(\mathcal{D})} \mathcal{D}(j)\,|j\rangle\,|\mathbf{x}+j\cdot\mathbf{s} \bmod q\rangle$$

DCP

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

Examples:

U-EDCP$_{n,q,M}$

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

G-EDCP$_{n,q,r}$

$$\sum_{j\in\mathbb{Z}} \rho_r(j)\,|j\rangle\,|\mathbf{x}+j\cdot\mathbf{s}\rangle$$

Main result of [BKSW18]:

$$\boxed{\text{LWE} \iff \text{G-EDCP} \iff \text{U-EDCP} < \text{DCP}}$$

Reductions btw LWE, DCP, EDCP

$\mathsf{LWE}^{m}_{n,q,1/\mathrm{poly}}$

$\mathsf{DCP}^{\mathrm{poly}}_{q^n}$

$\mathsf{U\text{-}EDCP}^{\mathrm{poly}}_{n,q,M}$

Reductions btw LWE, DCP, EDCP

$$\begin{array}{ccc} \boxed{\mathsf{LWE}^{m}_{n,q,1/\mathrm{poly}}} & \xrightarrow{1} & \boxed{\mathsf{DCP}^{\mathrm{poly}}_{q^n}} \\ & & \\ & & \boxed{\mathsf{U\text{-}EDCP}^{\mathrm{poly}}_{n,q,M}} \end{array}$$

1. [R02,R07] $\mathsf{LWE}^{m}_{n,q,1/\mathrm{poly}} \leq \mathsf{DCP}^{\mathrm{poly}}_{q^n}$

Reductions btw LWE, DCP, EDCP

$$\begin{tikzcd}
\boxed{\mathsf{LWE}^{m}_{n,q,1/\mathrm{poly}}} \arrow[r, "1"] \arrow[dr, "2"] & \boxed{\mathsf{DCP}^{\mathrm{poly}}_{q^n}} \\
& \boxed{\mathsf{U\text{-}EDCP}^{\mathrm{poly}}_{n,q,M}}
\end{tikzcd}$$

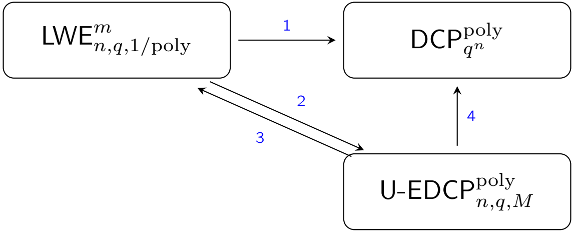
1. [R02,R07] $\mathsf{LWE}^{m}_{n,q,1/\mathrm{poly}} \leq \mathsf{DCP}^{\mathrm{poly}}_{q^n}$
2. [BKSW18] $\mathsf{LWE}^{\Omega(n\log q)}_{n,q,\alpha} \leq \mathsf{EDCP}^{\ell}_{n,q,M}$ where $M \cdot \ell \approx 1/(\alpha \cdot n \log q)$.

Reductions btw LWE, DCP, EDCP

$$
\begin{tikzcd}
\mathsf{LWE}^{m}_{n,q,1/\mathrm{poly}} \arrow[r, "1"] \arrow[dr, shift left, "2"] & \mathsf{DCP}^{\mathrm{poly}}_{q^n} \\
& \mathsf{U\text{-}EDCP}^{\mathrm{poly}}_{n,q,M} \arrow[ul, shift left, "3"]
\end{tikzcd}
$$

1. [R02,R07] $\mathsf{LWE}^{m}_{n,q,1/\mathrm{poly}} \leq \mathsf{DCP}^{\mathrm{poly}}_{q^n}$
2. [BKSW18] $\mathsf{LWE}^{\Omega(n \log q)}_{n,q,\alpha} \leq \mathsf{EDCP}^{\ell}_{n,q,M}$ where $M \cdot \ell \approx 1/(\alpha \cdot n \log q)$.
3. [BKSW18] $\mathsf{EDCP}^{\ell}_{n,q,M} \leq \mathsf{LWE}^{\ell}_{n,q,\alpha}$ where $\alpha \approx 1/M$.

Reductions btw LWE, DCP, EDCP



1. [R02,R07] $\mathsf{LWE}^m_{n,q,1/\mathrm{poly}} \leq \mathsf{DCP}^{\mathrm{poly}}_{q^n}$
2. [BKSW18] $\mathsf{LWE}^{\Omega(n\log q)}_{n,q,\alpha} \leq \mathsf{EDCP}^{\ell}_{n,q,M}$ where $M \cdot \ell \approx 1/(\alpha \cdot n \log q)$.
3. [BKSW18] $\mathsf{EDCP}^{\ell}_{n,q,M} \leq \mathsf{LWE}^{\ell}_{n,q,\alpha}$ where $\alpha \approx 1/M$.
4. [BKSW18,D20] $\mathsf{EDCP}^{\ell}_{n,q,M} \leq \mathsf{DCP}^{\Theta(\ell)}_{q^n}$.

State-of-the-art complexity of U-EDCP

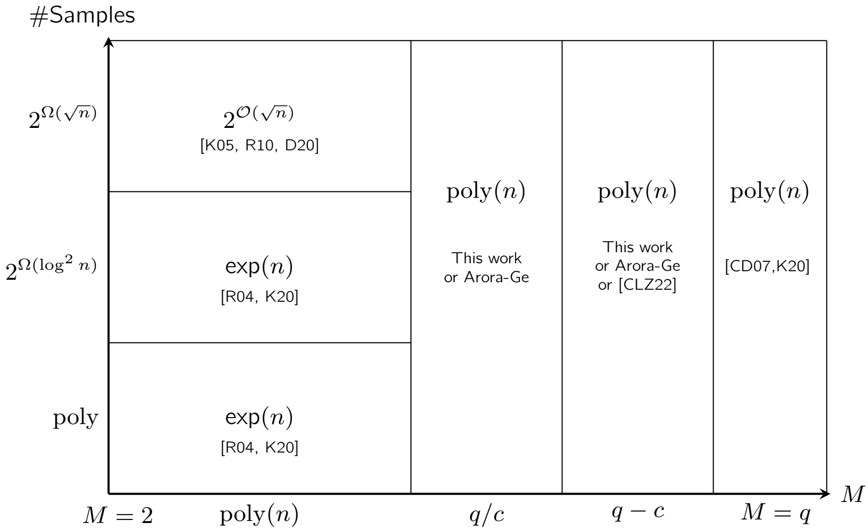


Figure: Complexity of U-EDCP$_{n,q,M}$.

Our result

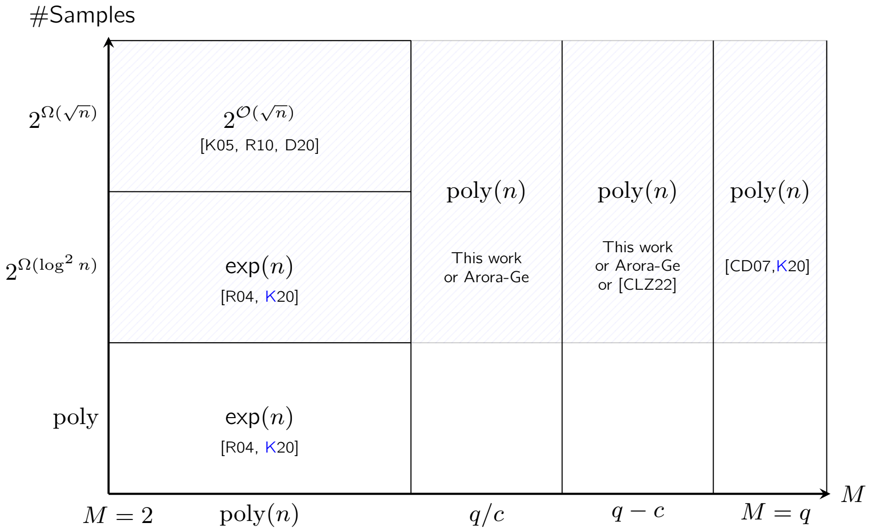


Figure: Complexity of U-EDCP$_{n,q,M}$. Our algorithm applies.

Our result

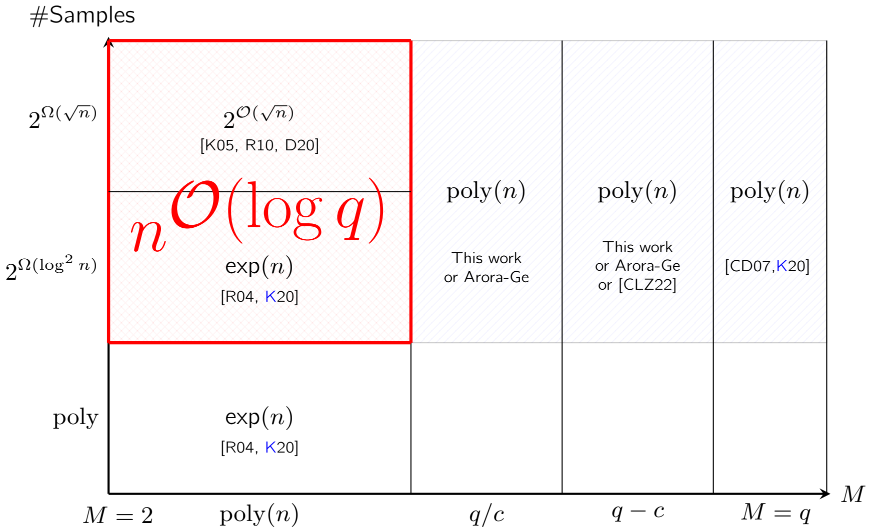


Figure: Complexity of U-EDCP$_{n,q,M}$. Our algorithm applies. Our algorithm improves state-of-the-art for power-of-two q.

Our algorithm for $M = 2$: Step 0

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

Our algorithm for $M = 2$: Step 0

$\omega_q = e^{2\pi i/q}$

$$|0\rangle |\mathbf{x}\rangle + |1\rangle |\mathbf{x} + \mathbf{s} \bmod q\rangle$$

$$\Big\downarrow \text{QFT over } \mathbb{Z}_q^n \text{ on the 2nd register}$$

$$\sum_{\mathbf{y}\in\mathbb{Z}_q^n} \left(\omega_q^{\langle \mathbf{y},\mathbf{x}\rangle} |0\rangle + \omega_q^{\langle \mathbf{y},\mathbf{x}+\mathbf{s}\rangle} |1\rangle\right) |\mathbf{y}\rangle = \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \left(|0\rangle + \omega_q^{\langle \mathbf{y},\mathbf{s}\rangle} |1\rangle\right) |\mathbf{y}\rangle$$

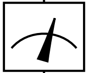
Our algorithm for $M = 2$: Step 0

$\omega_q = e^{2\pi i/q}$

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

QFT over $\mathbb{Z}_q^n$ on the 2nd register

$$\sum_{\mathbf{y}\in\mathbb{Z}_q^n} \left(\omega_q^{\langle \mathbf{y},\mathbf{x}\rangle}\,|0\rangle + \omega_q^{\langle \mathbf{y},\mathbf{x}+\mathbf{s}\rangle}\,|1\rangle\right)|\mathbf{y}\rangle = \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \left(|0\rangle + \omega_q^{\langle \mathbf{y},\mathbf{s}\rangle}\,|1\rangle\right)|\mathbf{y}\rangle$$



$$\mathbf{y}, \quad |0\rangle + \omega_q^{\langle \mathbf{y},\mathbf{s}\rangle}\,|1\rangle$$

Our algorithm for $M = 2$: Goal

$\omega_q = e^{2\pi i/q}$

Given $\left(\mathbf{y}, |0\rangle + \omega_q^{\langle \mathbf{y}, \mathbf{s} \rangle} |1\rangle\right)$, construct a state with $\mathbf{y} = 0 \bmod q/2$.

Why useful?

Our algorithm for $M = 2$: Goal

$\omega_q = e^{2\pi i/q}$

Given $\left(\mathbf{y}, |0\rangle + \omega_q^{\langle \mathbf{y}, \mathbf{s} \rangle} |1\rangle\right)$, construct a state with $\mathbf{y} = 0 \bmod q/2$.

Why useful? For $\mathbf{y}' = \mathbf{y}/(q/2)$:

$$|0\rangle + \omega_q^{q/2\langle \mathbf{y}', \mathbf{s} \rangle} |1\rangle = |0\rangle + e^{\frac{2\pi i q/2 \langle \mathbf{y}', \mathbf{s} \rangle}{q}} |1\rangle = |0\rangle + (-1)^{\langle \mathbf{y}', \mathbf{s} \rangle} |1\rangle$$

Our algorithm for $M = 2$: Goal

$\omega_q = e^{2\pi i/q}$

Given $\left(\mathbf{y}, |0\rangle + \omega_q^{\langle \mathbf{y}, \mathbf{s}\rangle} |1\rangle\right)$, construct a state with $\mathbf{y} = 0 \bmod q/2$.

Why useful? For $\mathbf{y}' = \mathbf{y}/(q/2)$:

$$|0\rangle + \omega_q^{q/2\langle \mathbf{y}', \mathbf{s}\rangle} |1\rangle = |0\rangle + e^{\frac{2\pi i q/2 \langle \mathbf{y}', \mathbf{s}\rangle}{q}} |1\rangle = |0\rangle + (-1)^{\langle \mathbf{y}', \mathbf{s}\rangle} |1\rangle$$

1. Measure the state in Hadamard basis, receive $\langle \mathbf{y}', \mathbf{s}\rangle \bmod 2$
2. Do it n times, learn $\bar{\mathbf{s}} := \mathbf{s} \bmod 2$ via linear algebra
3. To proceed to the next LSBs of $\mathbf{s}$, transform fresh EDCP samples:

$$|0\rangle |\mathbf{x}\rangle + |1\rangle |\mathbf{x} + \mathbf{s}\rangle \to |0\rangle |\mathbf{x}\rangle + |1\rangle |\mathbf{x} + \mathbf{s} - \bar{\mathbf{s}}\rangle$$

Our algorithm for $M = 2$: Main step

We have

$$|0\rangle + \omega_q^{\langle \mathbf{y}, \mathbf{s} \rangle} |1\rangle$$

Warm-up: consider tensoring $|0\rangle + \omega_q^{\langle \mathbf{y}, \mathbf{s} \rangle} |1\rangle$ and $|0\rangle + \omega_q^{\langle \mathbf{y}', \mathbf{s} \rangle} |1\rangle$:

$$|00\rangle + \omega_q^{\langle \mathbf{y}', \mathbf{s} \rangle} |01\rangle + \omega_q^{\langle \mathbf{y}, \mathbf{s} \rangle} |10\rangle + \omega_q^{\langle \mathbf{y}' + \mathbf{y}, \mathbf{s} \rangle} |11\rangle = \sum_{\mathbf{j} \in \mathbb{Z}_2^2} \omega_q^{\langle \mathbf{Y}\mathbf{j}, \mathbf{s} \rangle} |\mathbf{j}\rangle ,$$

where $\mathbf{Y} = [\mathbf{y}' | \mathbf{y}]$.

Our algorithm for $M = 2$: Main step

1. Tensor $n+1$ states:

$$\bigotimes_{k=1}^{n+1} \left(|0\rangle + \omega_q^{\langle \mathbf{y}_k, \mathbf{s} \rangle} |1\rangle \right) = \sum_{\mathbf{j} \in \mathbb{Z}_2^{n+1}} \omega_q^{\langle \mathbf{Y} \cdot \mathbf{j}, \mathbf{s} \rangle} |\mathbf{j}\rangle ,$$

   where $\mathbf{Y} = (\mathbf{y}_1, \ldots, \mathbf{y}_{n+1}) \in \mathbb{Z}_q^{n \times n+1}$

2. Compute $\mathbf{Y} \cdot \mathbf{j} \bmod 2$ in a new register:

$$\sum_{\mathbf{j} \in \mathbb{Z}_2^{n+1}} \omega_q^{\langle \mathbf{Y} \cdot \mathbf{j}, \mathbf{s} \rangle} |\mathbf{j}\rangle \, |\mathbf{Y} \cdot \mathbf{j} \bmod 2\rangle$$

Our algorithm for $M = 2$: Main step

1. Tensor $n+1$ states:

$$\bigotimes_{k=1}^{n+1} \left(|0\rangle + \omega_q^{\langle \mathbf{y}_k, \mathbf{s} \rangle} |1\rangle \right) = \sum_{\mathbf{j} \in \mathbb{Z}_2^{n+1}} \omega_q^{\langle \mathbf{Y} \cdot \mathbf{j}, \mathbf{s} \rangle} |\mathbf{j}\rangle ,$$

   where $\mathbf{Y} = (\mathbf{y}_1, \ldots, \mathbf{y}_{n+1}) \in \mathbb{Z}_q^{n \times n+1}$

2. Compute $\mathbf{Y} \cdot \mathbf{j} \bmod 2$ in a new register:

$$\sum_{\mathbf{j} \in \mathbb{Z}_2^{n+1}} \omega_q^{\langle \mathbf{Y} \cdot \mathbf{j}, \mathbf{s} \rangle} |\mathbf{j}\rangle \, |\mathbf{Y} \cdot \mathbf{j} \bmod 2\rangle$$

3. Measure the last register to get some $\mathbf{b} \in \mathbb{Z}_2^n$ and

$$\sum_{\mathbf{j} \in \mathbb{Z}_2^{n+1} : \mathbf{Y} \cdot \mathbf{j} = \mathbf{b}} \omega_q^{\langle \mathbf{Y} \cdot \mathbf{j}, \mathbf{s} \rangle} |\mathbf{j}\rangle$$

Our algorithm for $M = 2$: Main step

$$\sum_{\mathbf{j} \in \mathbb{Z}_2^{n+1} : \mathbf{Y} \cdot \mathbf{j} = \mathbf{b}} \omega_q^{\langle \mathbf{Y} \cdot \mathbf{j}, \mathbf{s} \rangle} |\mathbf{j}\rangle , \quad \mathbf{b}$$

Our algorithm for $M = 2$: Main step

$$\sum_{\mathbf{j} \in \mathbb{Z}_2^{n+1} : \mathbf{Y} \cdot \mathbf{j} = \mathbf{b}} \omega_q^{\langle \mathbf{Y} \cdot \mathbf{j}, \mathbf{s} \rangle} |\mathbf{j}\rangle , \quad \mathbf{b}$$

4. Compute classically the set ($\mathbf{Y} \bmod 2$ is full rank w.h.p.):

$$\{\mathbf{j} \in \mathbb{Z}_2^{n+1} : \mathbf{Y} \cdot \mathbf{j} = \mathbf{b} \bmod 2\} = \{\mathbf{j}_0, \mathbf{j}_1\}$$

Our algorithm for $M = 2$: Main step

$$\sum_{\mathbf{j} \in \mathbb{Z}_2^{n+1} : \mathbf{Y} \cdot \mathbf{j} = \mathbf{b}} \omega_q^{\langle \mathbf{Y} \cdot \mathbf{j}, \mathbf{s} \rangle} |\mathbf{j}\rangle , \quad \mathbf{b}$$

4. Compute classically the set ($\mathbf{Y}$ mod 2 is full rank w.h.p.):

$$\{\mathbf{j} \in \mathbb{Z}_2^{n+1} : \mathbf{Y} \cdot \mathbf{j} = \mathbf{b} \bmod 2\} = \{\mathbf{j}_0, \mathbf{j}_1\}$$

5. We have

$$\omega_q^{\langle \mathbf{Y} \cdot \mathbf{j}_0, \mathbf{s} \rangle} |\mathbf{j}_0\rangle + \omega_q^{\langle \mathbf{Y} \cdot \mathbf{j}_1, \mathbf{s} \rangle} |\mathbf{j}_1\rangle = |0\rangle + \omega_q^{\langle \mathbf{Y} \cdot (\mathbf{j}_1 - \mathbf{j}_0), \mathbf{s} \rangle} |1\rangle .$$

Our algorithm for $M = 2$: Main step

$$\sum_{\mathbf{j}\in\mathbb{Z}_2^{n+1}:\mathbf{Y}\cdot\mathbf{j}=\mathbf{b}} \omega_q^{\langle \mathbf{Y}\cdot\mathbf{j},\mathbf{s}\rangle} |\mathbf{j}\rangle \,, \quad \mathbf{b}$$

4. Compute classically the set ($\mathbf{Y} \bmod 2$ is full rank w.h.p.):
$$\{\mathbf{j}\in\mathbb{Z}_2^{n+1} \,:\, \mathbf{Y}\cdot\mathbf{j} = \mathbf{b} \bmod 2\} = \{\mathbf{j}_0, \mathbf{j}_1\}$$

5. We have
$$\omega_q^{\langle \mathbf{Y}\cdot\mathbf{j}_0,\mathbf{s}\rangle} |\mathbf{j}_0\rangle + \omega_q^{\langle \mathbf{Y}\cdot\mathbf{j}_1,\mathbf{s}\rangle} |\mathbf{j}_1\rangle = |0\rangle + \omega_q^{\langle \mathbf{Y}\cdot(\mathbf{j}_1-\mathbf{j}_0),\mathbf{s}\rangle} |1\rangle \,.$$

6. Since $\mathbf{Y}\cdot(\mathbf{j}_1 - \mathbf{j}_0) = 0 \bmod 2$,
$$|0\rangle + \omega_{q/2}^{\langle \mathbf{y}',\mathbf{s}\rangle} |1\rangle \quad \text{where } \; 2\mathbf{y}' = \mathbf{Y}(\mathbf{j}_1 - \mathbf{j}_0) \bmod q.$$

Our algorithm for $M = 2$: Main step

$$\sum_{\mathbf{j} \in \mathbb{Z}_2^{n+1} : \mathbf{Y} \cdot \mathbf{j} = \mathbf{b}} \omega_q^{\langle \mathbf{Y} \cdot \mathbf{j}, \mathbf{s} \rangle} |\mathbf{j}\rangle , \quad \mathbf{b}$$

4. Compute classically the set ($\mathbf{Y} \bmod 2$ is full rank w.h.p.):

$$\{\mathbf{j} \in \mathbb{Z}_2^{n+1} : \mathbf{Y} \cdot \mathbf{j} = \mathbf{b} \bmod 2\} = \{\mathbf{j}_0, \mathbf{j}_1\}$$

5. We have

$$\omega_q^{\langle \mathbf{Y} \cdot \mathbf{j}_0, \mathbf{s} \rangle} |\mathbf{j}_0\rangle + \omega_q^{\langle \mathbf{Y} \cdot \mathbf{j}_1, \mathbf{s} \rangle} |\mathbf{j}_1\rangle = |0\rangle + \omega_q^{\langle \mathbf{Y} \cdot (\mathbf{j}_1 - \mathbf{j}_0), \mathbf{s} \rangle} |1\rangle .$$

6. Since $\mathbf{Y} \cdot (\mathbf{j}_1 - \mathbf{j}_0) = 0 \bmod 2$,

$$|0\rangle + \omega_{q/2}^{\langle \mathbf{y}', \mathbf{s} \rangle} |1\rangle \quad \text{where } \ 2\mathbf{y}' = \mathbf{Y}(\mathbf{j}_1 - \mathbf{j}_0) \bmod q.$$

Proceed in the same way to obtain samples

$$|0\rangle + \omega_{\frac{q}{4}}^{\langle \mathbf{y}, \mathbf{s} \rangle} |1\rangle$$

Our algorithm for $M = 2$: Main step

$$\sum_{\mathbf{j} \in \mathbb{Z}_2^{n+1} : \mathbf{Y} \cdot \mathbf{j} = \mathbf{b}} \omega_q^{\langle \mathbf{Y} \cdot \mathbf{j}, \mathbf{s} \rangle} |\mathbf{j}\rangle , \quad \mathbf{b}$$

4. Compute classically the set ($\mathbf{Y} \bmod 2$ is full rank w.h.p.):

$$\{\mathbf{j} \in \mathbb{Z}_2^{n+1} \;:\; \mathbf{Y} \cdot \mathbf{j} = \mathbf{b} \bmod 2\} = \{\mathbf{j}_0, \mathbf{j}_1\}$$

5. We have

$$\omega_q^{\langle \mathbf{Y} \cdot \mathbf{j}_0, \mathbf{s} \rangle} |\mathbf{j}_0\rangle + \omega_q^{\langle \mathbf{Y} \cdot \mathbf{j}_1, \mathbf{s} \rangle} |\mathbf{j}_1\rangle = |0\rangle + \omega_q^{\langle \mathbf{Y} \cdot (\mathbf{j}_1 - \mathbf{j}_0), \mathbf{s} \rangle} |1\rangle .$$

6. Since $\mathbf{Y} \cdot (\mathbf{j}_1 - \mathbf{j}_0) = 0 \bmod 2$,

$$|0\rangle + \omega_{q/2}^{\langle \mathbf{y}', \mathbf{s} \rangle} |1\rangle \quad \text{where} \;\; 2\mathbf{y}' = \mathbf{Y}(\mathbf{j}_1 - \mathbf{j}_0) \bmod q.$$

Proceed in the same way to obtain samples

$$|0\rangle + \omega_{\frac{q}{4}}^{\langle \mathbf{y}, \mathbf{s} \rangle} |1\rangle \to |0\rangle + \omega_{\frac{q}{8}}^{\langle \mathbf{y}, \mathbf{s} \rangle} |1\rangle$$

Our algorithm for $M = 2$: Main step

$$\sum_{\mathbf{j} \in \mathbb{Z}_2^{n+1} : \mathbf{Y} \cdot \mathbf{j} = \mathbf{b}} \omega_q^{\langle \mathbf{Y} \cdot \mathbf{j}, \mathbf{s} \rangle} |\mathbf{j}\rangle , \quad \mathbf{b}$$

4. Compute classically the set ($\mathbf{Y}$ mod 2 is full rank w.h.p.):

$$\{\mathbf{j} \in \mathbb{Z}_2^{n+1} \ : \ \mathbf{Y} \cdot \mathbf{j} = \mathbf{b} \bmod 2\} = \{\mathbf{j}_0, \mathbf{j}_1\}$$

5. We have

$$\omega_q^{\langle \mathbf{Y} \cdot \mathbf{j}_0, \mathbf{s} \rangle} |\mathbf{j}_0\rangle + \omega_q^{\langle \mathbf{Y} \cdot \mathbf{j}_1, \mathbf{s} \rangle} |\mathbf{j}_1\rangle = |0\rangle + \omega_q^{\langle \mathbf{Y} \cdot (\mathbf{j}_1 - \mathbf{j}_0), \mathbf{s} \rangle} |1\rangle .$$

6. Since $\mathbf{Y} \cdot (\mathbf{j}_1 - \mathbf{j}_0) = 0 \bmod 2$,

$$|0\rangle + \omega_{q/2}^{\langle \mathbf{y}', \mathbf{s} \rangle} |1\rangle \quad \text{where} \ \ 2\mathbf{y}' = \mathbf{Y}(\mathbf{j}_1 - \mathbf{j}_0) \bmod q.$$

Proceed in the same way to obtain samples

$$|0\rangle + \omega_{\frac{q}{4}}^{\langle \mathbf{y}, \mathbf{s} \rangle} |1\rangle \ \rightarrow |0\rangle + \omega_{\frac{q}{8}}^{\langle \mathbf{y}, \mathbf{s} \rangle} |1\rangle \ \rightarrow \ldots |0\rangle + \omega_{\frac{q}{q/2}}^{\langle \mathbf{y}, \mathbf{s} \rangle} |1\rangle = |0\rangle + (-1)^{\langle \mathbf{y}, \mathbf{s} \rangle} |1\rangle$$

Analysis

- To produce one state $|0\rangle + (-1)^{\langle \mathbf{y}, \mathbf{s} \rangle} |1\rangle$, we need
  - $\Theta(n)$ states $|0\rangle + \omega_{q/q/4}^{\langle \mathbf{y}, \mathbf{s} \rangle} |1\rangle$
  - $\Theta(n^2)$ states $|0\rangle + \omega_{q/q/8}^{\langle \mathbf{y}, \mathbf{s} \rangle} |1\rangle$
  - $\vdots$
  - $\Theta(n^{\log q - 1})$ states $|0\rangle + \omega_{q}^{\langle \mathbf{y}, \mathbf{s} \rangle} |1\rangle$
- To recover $\mathbf{s} \bmod q$, we need $n \log q$ states $|0\rangle + (-1)^{\langle \mathbf{y}, \mathbf{s} \rangle} |1\rangle$.

Analysis

- To produce one state $|0\rangle + (-1)^{\langle \mathbf{y}, \mathbf{s} \rangle} |1\rangle$, we need
  - $\Theta(n)$ states $|0\rangle + \omega_{q/q/4}^{\langle \mathbf{y}, \mathbf{s} \rangle} |1\rangle$
  - $\Theta(n^2)$ states $|0\rangle + \omega_{q/q/8}^{\langle \mathbf{y}, \mathbf{s} \rangle} |1\rangle$
  - $\vdots$
  - $\Theta(n^{\log q - 1})$ states $|0\rangle + \omega_{q}^{\langle \mathbf{y}, \mathbf{s} \rangle} |1\rangle$
- To recover $\mathbf{s} \bmod q$, we need $n \log q$ states $|0\rangle + (-1)^{\langle \mathbf{y}, \mathbf{s} \rangle} |1\rangle$.

Theorem

There exists a quantum algorithm that given on input $2^{\Omega(\log n \log q)}$ EDCP samples, solves the problem in time $2^{\mathcal{O}(\log n \log q)}$ and $\mathrm{poly}(n)$ space.

The main challenge: to show that $\mathbf{y}'$ obtained at Step 6 are uniform (see paper).

Going from $M = \mathrm{poly}(n)$ to $M = 2$, [DoI19, This work]

$$\sum_{j=0}^{M-1} \omega_q^{j\langle \mathbf{y},\mathbf{s}\rangle} |j\rangle$$

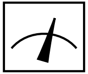
Going from $M = \mathrm{poly}(n)$ to $M = 2$, [Dol19, This work]

$$\sum_{j=0}^{M-1} \omega_q^{j\langle \mathbf{y}, \mathbf{s} \rangle} |j\rangle$$

$$\downarrow$$

$$\sum_{j=0}^{M-1} \omega_q^{j\langle \mathbf{y}, \mathbf{s} \rangle} |j\rangle \left| \lfloor \tfrac{j}{2} \rfloor \right\rangle$$

$$\downarrow$$



$$\downarrow$$

$$\sum_{j \in [0,M) \cap [2 \cdot k, 2(k+1)]} \omega_q^{j\langle \mathbf{y}, \mathbf{s} \rangle} |j\rangle \,, \qquad k = \lfloor \tfrac{j}{2} \rfloor$$

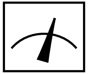
Going from $M = \mathrm{poly}(n)$ to $M = 2$, [Dol19, This work]

$$\sum_{j=0}^{M-1} \omega_q^{j\langle \mathbf{y}, \mathbf{s} \rangle} |j\rangle$$

$$\downarrow$$

$$\sum_{j=0}^{M-1} \omega_q^{j\langle \mathbf{y}, \mathbf{s} \rangle} |j\rangle \left| \lfloor \tfrac{j}{2} \rfloor \right\rangle$$

$$\downarrow$$



$$\downarrow$$

$$\sum_{j \in [0, M) \cap [2 \cdot k, 2(k+1)]} \omega_q^{j\langle \mathbf{y}, \mathbf{s} \rangle} |j\rangle , \quad k = \lfloor \tfrac{j}{2} \rfloor$$

with probability $(2 \cdot \lfloor M/2 \rfloor)/M$:

$$= \sum_{j=2k}^{2(k+1)-1} \omega_q^{j\langle \mathbf{y}, \mathbf{s} \rangle} |j\rangle$$

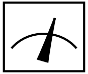
Going from $M = \mathrm{poly}(n)$ to $M = 2$, [Dol19, This work]

$$\sum_{j=0}^{M-1} \omega_q^{j\langle \mathbf{y},\mathbf{s}\rangle} |j\rangle$$

$$\downarrow$$

$$\sum_{j=0}^{M-1} \omega_q^{j\langle \mathbf{y},\mathbf{s}\rangle} |j\rangle \left| \lfloor \tfrac{j}{2} \rfloor \right\rangle$$

$$\downarrow$$



$$\downarrow$$

$$\sum_{j\in[0,M)\cap[2\cdot k,2(k+1)]} \omega_q^{j\langle \mathbf{y},\mathbf{s}\rangle} |j\rangle \,, \qquad k = \lfloor \tfrac{j}{2} \rfloor$$

with probability $(2 \cdot \lfloor M/2 \rfloor)/M$:

$$= \sum_{j=2k}^{2(k+1)-1} \omega_q^{j\langle \mathbf{y},\mathbf{s}\rangle} |j\rangle = \sum_{j=2k}^{2(k+1)-1} \omega_q^{(j-2k)\langle \mathbf{y},\mathbf{s}\rangle} |j\rangle$$

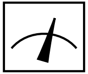
Going from $M = \mathrm{poly}(n)$ to $M = 2$, [Dol19, This work]

$$\sum_{j=0}^{M-1} \omega_q^{j\langle \mathbf{y}, \mathbf{s} \rangle} |j\rangle$$

$$\downarrow$$

$$\sum_{j=0}^{M-1} \omega_q^{j\langle \mathbf{y}, \mathbf{s} \rangle} |j\rangle \left| \lfloor \tfrac{j}{2} \rfloor \right\rangle$$

$$\downarrow$$



$$\downarrow$$

$$\sum_{j \in [0,M) \cap [2 \cdot k, 2(k+1)]} \omega_q^{j\langle \mathbf{y}, \mathbf{s} \rangle} |j\rangle , \quad k = \lfloor \tfrac{j}{2} \rfloor$$

with probability $(2 \cdot \lfloor M/2 \rfloor)/M$:

$$= \sum_{j=2k}^{2(k+1)-1} \omega_q^{j\langle \mathbf{y}, \mathbf{s} \rangle} |j\rangle = \sum_{j=2k}^{2(k+1)-1} \omega_q^{(j-2k)\langle \mathbf{y}, \mathbf{s} \rangle} |j\rangle \overset{j \to j-2k}{=} \sum_{j=0}^{1} \omega_q^{j\langle \mathbf{y}, \mathbf{s} \rangle} |j\rangle$$

Why can't we work directly with $M > 2$?

1. Recall Step 2 but now compute mod $M > 2$, for M prime:

$$\sum_{\mathbf{j} \in \mathbb{Z}_M^{n+1}} \omega_q^{\langle \mathbf{Y} \cdot \mathbf{j}, \mathbf{s} \rangle} |\mathbf{j}\rangle \, |\mathbf{Y} \cdot \mathbf{j} \bmod M\rangle$$

Why can't we work directly with $M > 2$?

1. Recall Step 2 but now compute mod $M > 2$, for M prime:

$$\sum_{\mathbf{j} \in \mathbb{Z}_M^{n+1}} \omega_q^{\langle \mathbf{Y} \cdot \mathbf{j}, \mathbf{s} \rangle} |\mathbf{j}\rangle |\mathbf{Y} \cdot \mathbf{j} \bmod M\rangle$$

2. Compute classically the set ($\mathbf{Y} \bmod M$ is full rank w.h.p.) for some measured $\mathbf{b}$:

$$\{\mathbf{j} \in \mathbb{Z}_M^{n+1} \,:\, \mathbf{Y} \cdot \mathbf{j} = \mathbf{b} \bmod M\} = \{\mathbf{j}_i = \mathbf{j}_0 + i\mathbf{u} \bmod M, 0 \leq i < M,\ \mathbf{u} \in \ker(\mathbf{Y})\}$$

Why can't we work directly with $M > 2$?

1. Recall Step 2 but now compute mod $M > 2$, for M prime:

$$\sum_{\mathbf{j}\in\mathbb{Z}_M^{n+1}} \omega_q^{\langle \mathbf{Y}\cdot\mathbf{j},\mathbf{s}\rangle} |\mathbf{j}\rangle\, |\mathbf{Y}\cdot\mathbf{j} \bmod M\rangle$$

2. Compute classically the set ($\mathbf{Y} \bmod M$ is full rank w.h.p.) for some measured $\mathbf{b}$:

$$\{\mathbf{j}\in\mathbb{Z}_M^{n+1} \,:\, \mathbf{Y}\cdot\mathbf{j} = \mathbf{b} \bmod M\} = \{\underbrace{\mathbf{j}_i = \mathbf{j}_0 + i\mathbf{u} \bmod M}_{\text{not true} \bmod q}, 0 \le i < M,\ \mathbf{u}\in\ker(\mathbf{Y})\}$$

Why can't we work directly with $M > 2$?

1. Recall Step 2 but now compute mod $M > 2$, for M prime:

$$\sum_{\mathbf{j}\in\mathbb{Z}_M^{n+1}} \omega_q^{\langle \mathbf{Y}\cdot\mathbf{j},\mathbf{s}\rangle} |\mathbf{j}\rangle\, |\mathbf{Y}\cdot\mathbf{j} \bmod M\rangle$$

2. Compute classically the set ($\mathbf{Y} \bmod M$ is full rank w.h.p.) for some measured $\mathbf{b}$:

$$\{\mathbf{j}\in\mathbb{Z}_M^{n+1} \,:\, \mathbf{Y}\cdot\mathbf{j} = \mathbf{b} \bmod M\} = \{\underbrace{\mathbf{j}_i = \mathbf{j}_0 + i\mathbf{u} \bmod M}_{\text{not true mod } q}, 0 \le i < M,\ \mathbf{u}\in\ker(\mathbf{Y})\}$$

3. Therefore, Step 5 fails:

$$\sum_{i=0}^{M-1} \omega_q^{\langle \mathbf{Y}\mathbf{j}_i,\mathbf{s}\rangle} |\mathbf{j}_i\rangle = \sum_{i=0}^{M-1} \omega_q^{\langle \mathbf{Y}\mathbf{j}_0 + i\mathbf{u} + M\mathbf{v}_i,\mathbf{s}\rangle} |\mathbf{j}_i\rangle \neq \sum_{i=0}^{M-1} \omega_q^{i\langle \mathbf{Y}\mathbf{u},\mathbf{s}\rangle} |\mathbf{j}_i\rangle\,.$$

Is LWE broken?

Is LWE broken?

No

Is LWE broken?

No

LWE to EDCP reduction [BKSW18]

There is a probabilistic quantum reduction from LWE samples with parameters (n, q, α) to ℓ-many EDCP samples with parameters (n, q, M), where

$$\ell \leq M/(\alpha \cdot \mathrm{poly}(n)).$$

Is LWE broken?

No

LWE to EDCP reduction [BKSW18]

There is a probabilistic quantum reduction from LWE samples with parameters (n, q, α) to ℓ-many EDCP samples with parameters (n, q, M), where

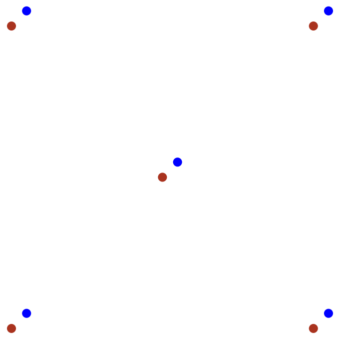
$$\ell \leq M/(\alpha \cdot \mathrm{poly}(n)).$$

- The reduction produces only $\mathrm{poly}(n)$ many EDCP samples
- For $\ell > q/M$, we need to start with 'trivial' LWE, i.e., with $q\alpha < 1/\mathrm{poly}(n)$.

Where does sample restriction come from?

Reductions from (E)DCP to LWE create a superposition

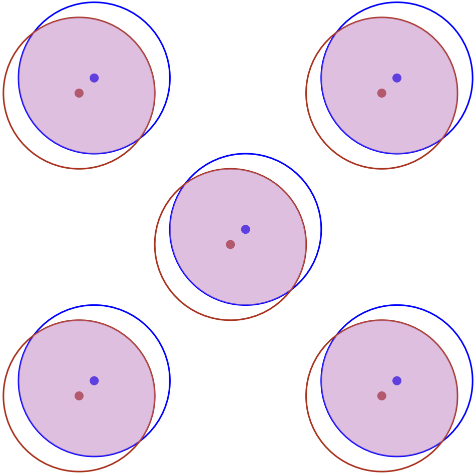
$$\sum_{\mathbf{x}\in\mathbb{Z}_q^n} \left(|0, \mathbf{x}, \mathbf{A}\mathbf{x}\rangle + |1, \mathbf{x}+\mathbf{s}, \mathbf{A}\mathbf{x}-\mathbf{e}\rangle\right)$$



Where does sample restriction come from?

Create around each center a sphere

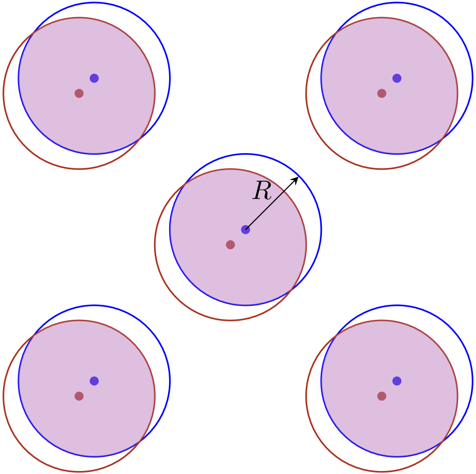
$$\sum_{\mathbf{x}\in\mathbb{Z}_q^n} \left(|0, \mathbf{x}, \mathbf{Ax}, \mathcal{B}(\mathbf{Ax})\rangle + |1, \mathbf{x}+\mathbf{s}, \mathbf{Ax}-\mathbf{e}, \mathcal{B}(\mathbf{Ax}-\mathbf{e})\rangle\right)$$



Where does sample restriction come from?

Measure the state. The probability of hitting a point in the intersection is

$$1 - \mathcal{O}(\sqrt{n}\|\mathbf{e}\|/R), \text{ for } R \approx \lambda_1(\Lambda_q(\mathbf{A})) \implies \text{ at most } \mathcal{O}(q/(\sqrt{n}\|\mathbf{e}\|)) \text{ samples}$$



Final thoughts

- If you manage to extend the algorithm to moduli $q = p^t$ for $p = \mathrm{poly}(n)$, you'll get a $\mathrm{poly}(n)$ algorithm and quantumly break LWE
- A sub-exponential algorithm for EDCP with $\mathrm{poly}(n)$ samples would lead to a sub-exponential attack on LWE
- We do not know yet a module-LWE analogue of EDCP

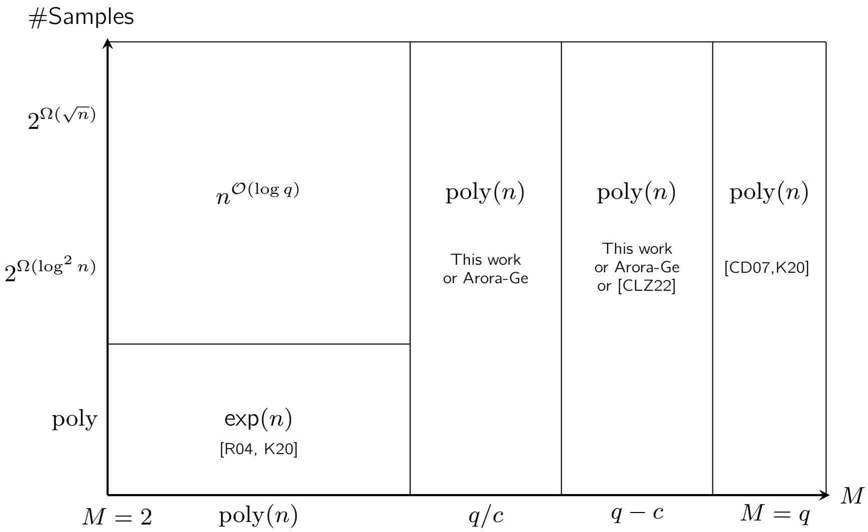
What about codes?

For $\mathbf{A} \in \mathbb{F}_2^{n \times k}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$, following existing reductions we can construct:

$$\sum_{\mathbf{x} \in \mathbb{F}_2^n} |0, \mathbf{x}, \mathbf{A}\mathbf{x} \bmod 2\rangle + |1, \mathbf{x} + \mathbf{s}, \mathbf{A}\mathbf{x} + \mathbf{e} \bmod 2\rangle$$

"Separating" $(\mathbf{A}\mathbf{x}, \mathbf{A}\mathbf{x} + \mathbf{e})$ from $(\mathbf{A}\mathbf{x}', \mathbf{A}\mathbf{x}' + \mathbf{e})$ is the decoding problem for $\mathbf{A}$.

Thank you! Questions?



References

- Arora-Ge Sanjeev Arora and Rong Ge. “New Algorithms for Learning in Presence of Errors”, ICALP 2011.
- [BKSW18] Zvika Brakerski, Elena Kirshanova, Damien Stehlé, Weiqiang Wen “Learning with Errors and Extrapolated Dihedral Cosets”, PKC 2018.
- [CD07] Andrew M. Childs and Wim van Dam. “Quantum algorithm for a generalized hidden shift problem”. SODA 2007
- [CLZ22] Yilei Chen, Qipeng Liu, and Mark Zhandry. “Quantum Algorithms for Variants of Average-Case Lattice Problems via Filtering”, EuroCrypt 2022.
- [D20] Javad Doliskani. “Efficient Quantum Public-Key Encryption From Learning With Errors.”. ePring 2020/1557
- [K05] Greg Kuperberg. “A Subexponential-Time Quantum Algorithm for the Dihedral Hidden Subgroup Problem”, Journal on Computing 2005.
- [K20] Elena Kirshanova. “A k-List Algorithm for LWE”. 2020 (talk at Simons Institute)
- [R04] Oded Regev. “A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem with Polynomial Space”. arXiv quant-ph/0406151
- [R02] Oded Regev. “Quantum computation and lattice problems”, FOCS 2002.