Advances and Open Challenges in Quantum Algorithms for Lattice Problems

Elena Kirshanova

based on joint works with

Shi Bai Zvika Brakerski Hansraj Jangir Tran Ngo
Damien Stehlé Weiqiang Wen William Youmans

at PQCrypto 2026

Part I

Learning With Errors Quantumly

The Dihedral Group D_{2N}

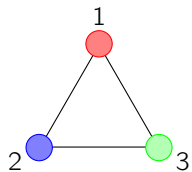
is a group of rotations and reflections of a regular $N-$gon.

$D_{2N} = \{r, s : s^2 = r^N = 1\ ,\ srs^{-1} = r^{-1}\}$, where r is a rotation, s is a reflection.

The Dihedral Group D_{2N}

is a group of rotations and reflections of a regular $N-$gon.

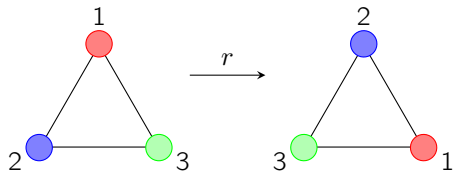
$D_{2N} = \{r, s : s^2 = r^N = 1\ ,\ srs^{-1} = r^{-1}\}$, where r is a rotation, s is a reflection.



The Dihedral Group D_{2N}

is a group of rotations and reflections of a regular $N-$gon.

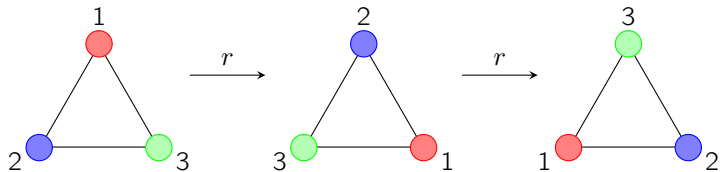
$D_{2N} = \{r, s : s^2 = r^N = 1\ ,\ srs^{-1} = r^{-1}\}$, where r is a rotation, s is a reflection.



The Dihedral Group D_{2N}

is a group of rotations and reflections of a regular $N-$gon.

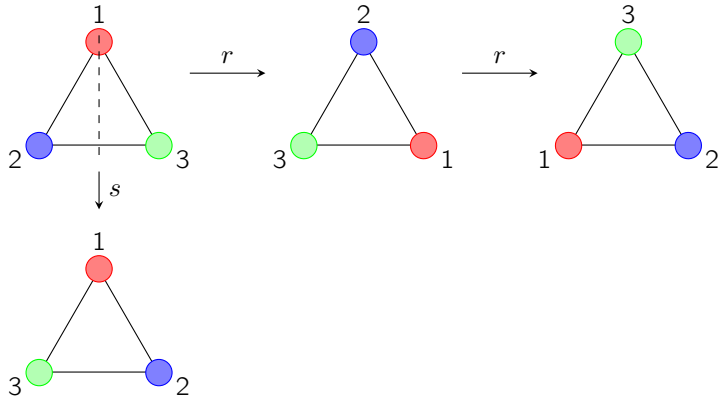
$D_{2N} = \{r, s : s^2 = r^N = 1\ ,\ srs^{-1} = r^{-1}\}$, where r is a rotation, s is a reflection.



The Dihedral Group D_{2N}

is a group of rotations and reflections of a regular $N-$gon.

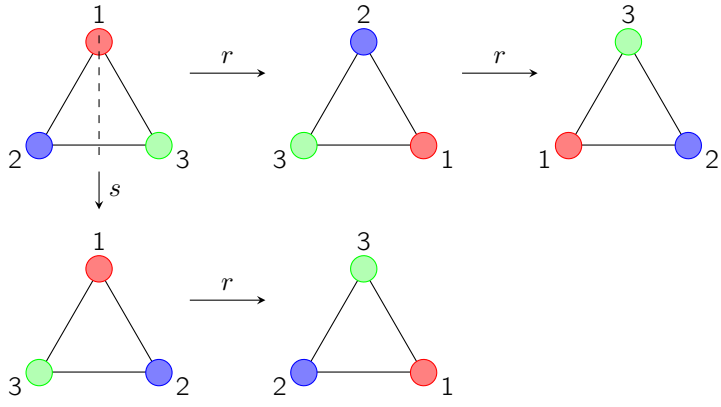
$D_{2N} = \{r, s : s^2 = r^N = 1\ ,\ srs^{-1} = r^{-1}\}$, where r is a rotation, s is a reflection.



The Dihedral Group D_{2N}

is a group of rotations and reflections of a regular $N-$gon.

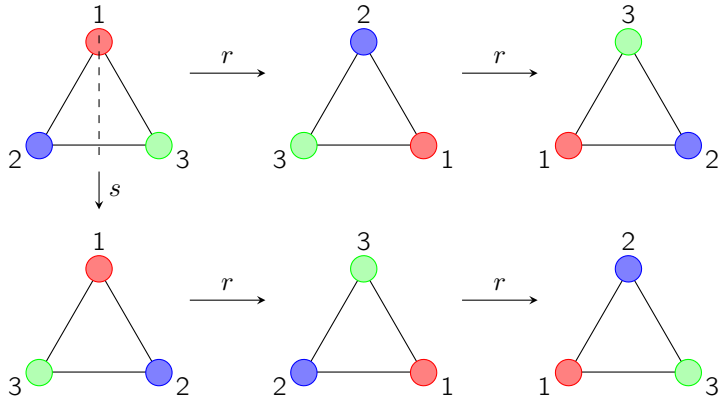
$D_{2N} = \{r, s : s^2 = r^N = 1\ ,\ srs^{-1} = r^{-1}\}$, where r is a rotation, s is a reflection.



The Dihedral Group D_{2N}

is a group of rotations and reflections of a regular $N-$gon.

$D_{2N} = \{r, s : s^2 = r^N = 1\ ,\ srs^{-1} = r^{-1}\}$, where r is a rotation, s is a reflection.

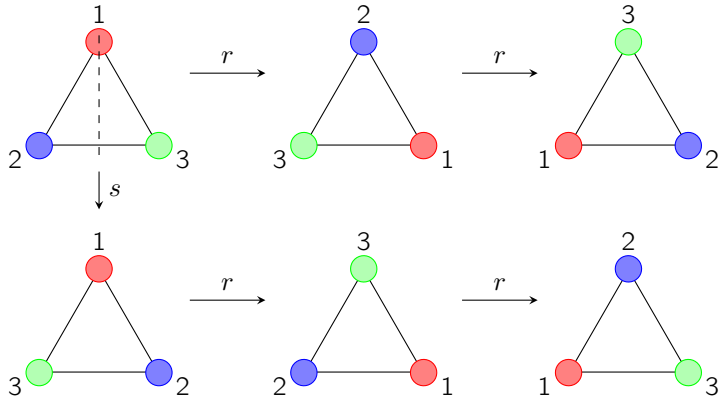


The Dihedral Group D_{2N}

is a group of rotations and reflections of a regular $N-$gon.

$D_{2N} = \{r, s : s^2 = r^N = 1\ ,\ srs^{-1} = r^{-1}\}$, where r is a rotation, s is a reflection.

Non-Abelian!



The Dihedral Coset Problem

Given quantum states of the form

$$\frac{1}{\sqrt{2}}|0, x\rangle + \frac{1}{\sqrt{2}}|1, x + s \bmod N\rangle,$$

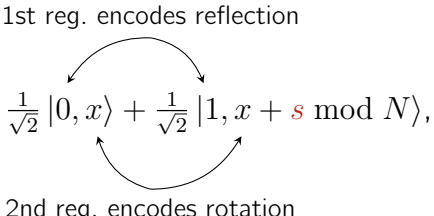
for $x \leftarrow \mathcal{U}(\mathbb{Z}_N)$, find s.

This problem arises from the dihedral Hidden Subgroup problem.

Here, the hidden subgroup of D_{2N} if generated by $(1, s)$

The Dihedral Coset Problem

Given quantum states of the form



for $x \leftarrow \mathcal{U}(\mathbb{Z}_N)$, find s.

This problem arises from the dihedral Hidden Subgroup problem.

Here, the hidden subgroup of D_{2N} if generated by $(1, s)$

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 $\mathbf{s}$.

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.

Best known attacks:

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.

Best known attacks:

BKW / lattices:

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

Kuperberg, Regev:

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

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

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 distribution $\mathcal{D}$

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

DCP

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

Extrapolated DCP

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

Examples:

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

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

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

$$\sum_{j \in \mathbb{Z}} \rho_r(j) \lvert j \rangle \lvert \mathbf{x} + j \cdot \mathbf{s} \rangle, \qquad \rho_r - \text{Gaussian with parameter } r$$

Extrapolated DCP

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

Examples: $\underline{\text{U-EDCP}_{n,q,M}}$ $\sum_{j=0}^{M-1} \lvert j \rangle \lvert \mathbf{x} + j \cdot \mathbf{s} \bmod q \rangle$

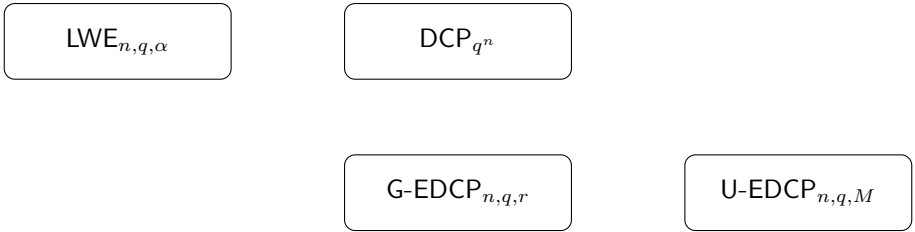
$\underline{\text{G-EDCP}_{n,q,r}}$

$$\sum_{j \in \mathbb{Z}} \rho_r(j) \lvert j \rangle \lvert \mathbf{x} + j \cdot \mathbf{s} \rangle, \qquad \rho_r - \text{Gaussian with parameter } r$$

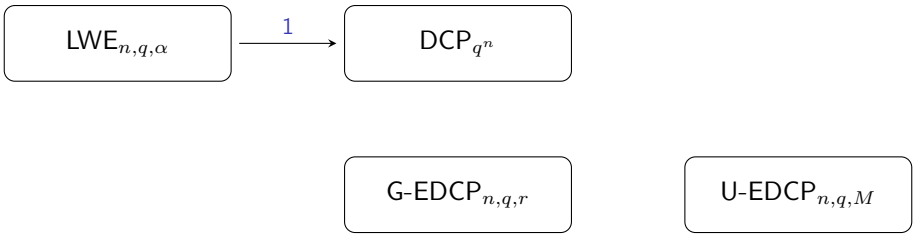
Main result of [BKSW18]:

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

Reductions btw LWE, DCP, EDCP

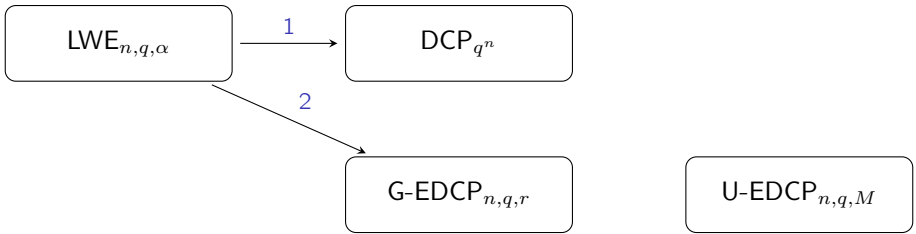


Reductions btw LWE, DCP, EDCP



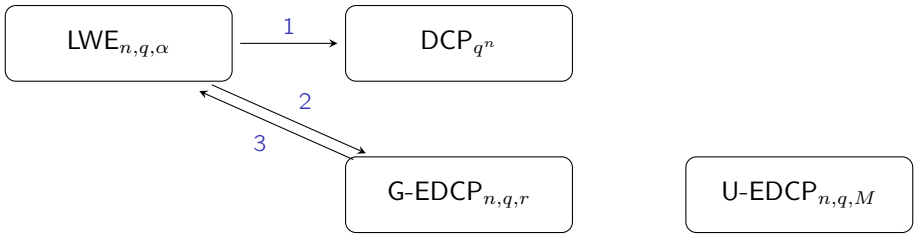
1. LWE$_{n,q,1/\mathrm{poly}} \leq$ DCP$_{q^n}$, [R02,R07]

Reductions btw LWE, DCP, EDCP



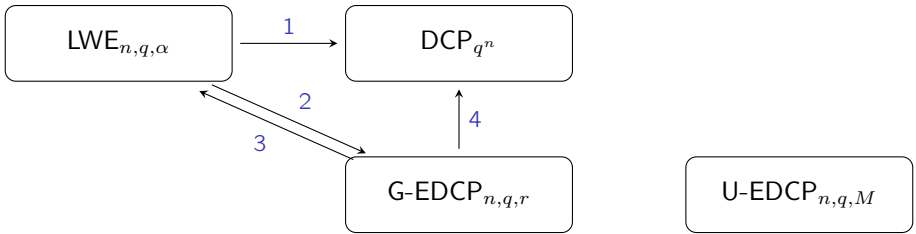
1. LWE$_{n,q,1/\mathrm{poly}} \leq$ DCP$_{q^n}$, [R02,R07]
2. LWE$_{n,q,\alpha} \leq$ G-EDCP$_{n,q,r}$ where $r \cdot \#\text{EDCP samples} \approx \mathrm{poly}(n)$. [BKSW18]

Reductions btw LWE, DCP, EDCP



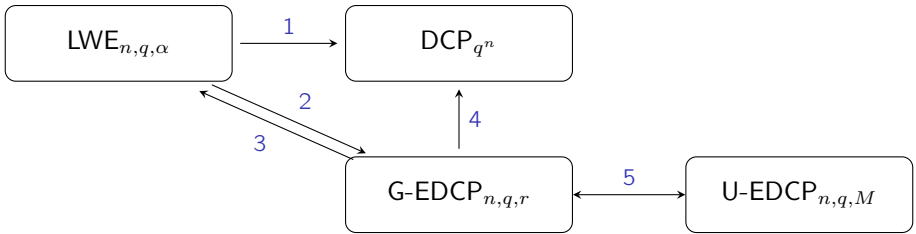
1. LWE$_{n,q,1/\mathrm{poly}} \leq$ DCP$_{q^n}$, [R02,R07]
2. LWE$_{n,q,\alpha} \leq$ G-EDCP$_{n,q,r}$ where $r \cdot \#\text{EDCP samples} \approx \mathrm{poly}(n)$. [BKSW18]
3. G-EDCP$_{n,q,r} \leq$ LWE$_{n,q,\alpha}$ where $\alpha \approx 1/r$. [BKSW18]

Reductions btw LWE, DCP, EDCP



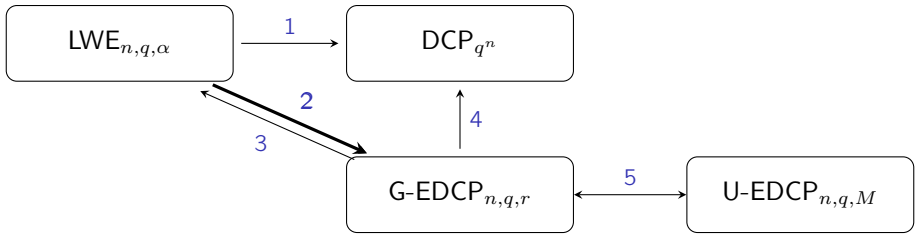
1. LWE$_{n,q,1/\mathrm{poly}} \leq$ DCP$_{q^n}$, [R02,R07]
2. LWE$_{n,q,\alpha} \leq$ G-EDCP$_{n,q,r}$ where $r \cdot \#\text{EDCP samples} \approx \mathrm{poly}(n)$. [BKSW18]
3. G-EDCP$_{n,q,r} \leq$ LWE$_{n,q,\alpha}$ where $\alpha \approx 1/r$. [BKSW18]
4. G-EDCP$_{n,q,r} \leq$ DCP$_{q^n}$. [BKSW18,D20]

Reductions btw LWE, DCP, EDCP



1. LWE$_{n,q,1/\mathrm{poly}} \leq$ DCP$_{q^n}$, [R02,R07]
2. LWE$_{n,q,\alpha} \leq$ G-EDCP$_{n,q,r}$ where $r \cdot \#\text{EDCP samples} \approx \mathrm{poly}(n)$. [BKSW18]
3. G-EDCP$_{n,q,r} \leq$ LWE$_{n,q,\alpha}$ where $\alpha \approx 1/r$. [BKSW18]
4. G-EDCP$_{n,q,r} \leq$ DCP$_{q^n}$. [BKSW18,D20]
5. G-EDCP$_{n,q,r} =$ U-EDCP$_{n,q,M}$ for $M = \Theta(r)$. [BKSW18]

Reductions btw LWE, DCP, EDCP



1. LWE$_{n,q,1/\mathrm{poly}} \leq$ DCP$_{q^n}$, [R02,R07]
2. LWE$_{n,q,\alpha} \leq$ G-EDCP$_{n,q,r}$ where $r \cdot \#\text{EDCP samples} \approx \mathrm{poly}(n)$. [BKSW18]
3. G-EDCP$_{n,q,r} \leq$ LWE$_{n,q,\alpha}$ where $\alpha \approx 1/r$. [BKSW18]
4. G-EDCP$_{n,q,r} \leq$ DCP$_{q^n}$. [BKSW18,D20]
5. G-EDCP$_{n,q,r} =$ U-EDCP$_{n,q,M}$ for $M = \Theta(r)$. [BKSW18]

LWE $\leq$ G-EDCP

Input: $\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$

LWE $\leq$ G-EDCP

Input: $\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$

Start with $\sum_{j \in \mathbb{Z}} \rho(j) \, |j\rangle \otimes \sum_{\mathbf{x} \in \mathbb{Z}_q^n} |\mathbf{x}\rangle \otimes |0\rangle$

LWE $\leq$ G-EDCP

Input: $\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$

Start with $\sum_{j\in\mathbb{Z}} \rho(j)\,|j\rangle \otimes \sum_{\mathbf{x}\in\mathbb{Z}_q^n} |\mathbf{x}\rangle \otimes |0\rangle$

$\downarrow$

Apply $\mathbf{A}\mathbf{x} - j\mathbf{b}$ to the third register

$\downarrow$

$$\sum_{\mathbf{x}\in\mathbb{Z}_q^n, j\in\mathbb{Z}} \rho(j)\,|j\rangle\,|\mathbf{x}\rangle\,|\mathbf{A}(\mathbf{x} - j\mathbf{s}) - j\mathbf{e}\rangle$$

LWE $\leq$ G-EDCP

Input: $\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$

Start with $\sum_{j \in \mathbb{Z}} \rho(j) \left|j\right\rangle \otimes \sum_{\mathbf{x} \in \mathbb{Z}_q^n} \left|\mathbf{x}\right\rangle \otimes \left|0\right\rangle$

$\Big\downarrow$

Apply $\mathbf{A}\mathbf{x} - j\mathbf{b}$ to the third register

$\Big\downarrow$

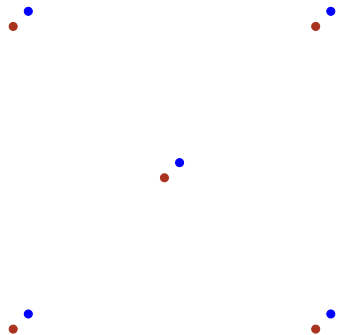
$$\sum_{\mathbf{x} \in \mathbb{Z}_q^n, j \in \mathbb{Z}} \rho(j) \left|j\right\rangle \left|\mathbf{x}\right\rangle \left|\mathbf{A}(\mathbf{x} - j\mathbf{s}) - j\mathbf{e}\right\rangle$$

$$=$$

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

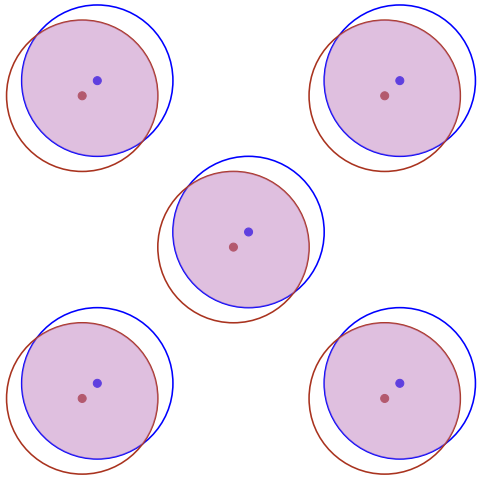
LWE $\leq$ G-EDCP

$$\sum_{\mathbf{x}\in\mathbb{Z}_q^n, j\in\mathbb{Z}} \rho(j)\,|j\rangle\,|\mathbf{x}+j\mathbf{s}\rangle\,|\mathbf{A}\mathbf{x}-j\mathbf{e}\rangle$$



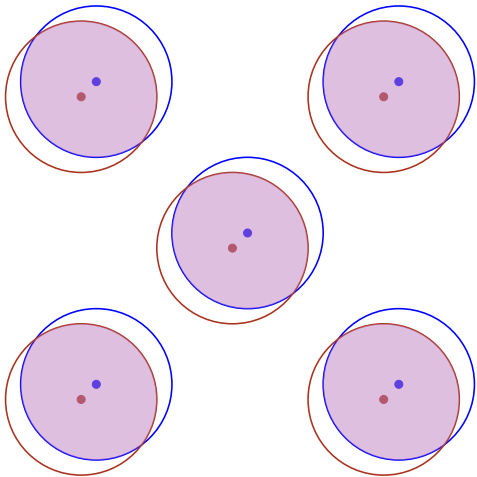
LWE $\leq$ G-EDCP

$$\sum_{\mathbf{x}\in\mathbb{Z}_q^n, j\in\mathbb{Z}} \rho(j)\,|j\rangle\,|\mathbf{x}+j\mathbf{s}\rangle\,|\mathbf{A}\mathbf{x}-j\mathbf{e}\rangle \rightarrow \sum_{\mathbf{x}\in\mathbb{Z}_q^n, j\in\mathbb{Z}} \rho(j)\,|j\rangle\,|\mathbf{x}+j\mathbf{s}\rangle\,|\mathbf{A}\mathbf{x}-j\mathbf{e}\rangle\,|\mathcal{B}(\mathbf{A}\mathbf{x}-j\mathbf{e})\rangle$$



LWE $\leq$ G-EDCP

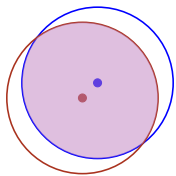
$$\sum_{\mathbf{x}\in\mathbb{Z}_q^n, j\in\mathbb{Z}} \rho(j)\,|j\rangle\,|\mathbf{x}+j\mathbf{s}\rangle\,|\mathbf{A}\mathbf{x}-j\mathbf{e}\rangle \rightarrow \sum_{\mathbf{x}\in\mathbb{Z}_q^n, j\in\mathbb{Z}} \rho(j)\,|j\rangle\,|\mathbf{x}+j\mathbf{s}\rangle\,|\mathbf{A}\mathbf{x}-j\mathbf{e}\rangle\,\underline{|\mathcal{B}(\mathbf{A}\mathbf{x}-j\mathbf{e})\rangle}$$



LWE $\leq$ G-EDCP

If we measure a point in the intersection, the resulting state is

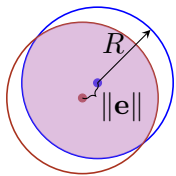
$$\sum_{j\in\mathbb{Z}} \rho(j)\,|j\rangle\,|\mathbf{x}+j\mathbf{s}\rangle\,|\mathbf{A}\mathbf{x}-j\mathbf{e}\rangle$$



LWE $\leq$ G-EDCP

If we measure a point in the intersection, the resulting state is

$$\sum_{j\in\mathbb{Z}} \rho(j)\,|j\rangle\,|\mathbf{x}+j\mathbf{s}\rangle\,|\mathbf{A}\mathbf{x}-j\mathbf{e}\rangle$$



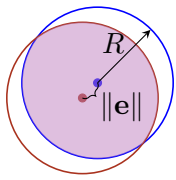
We hit a point in the intersection with probability([R02]):

$$1-\mathcal{O}(\sqrt{n}\|\mathbf{e}\|/R).$$

LWE $\leq$ G-EDCP

If we measure a point in the intersection, the resulting state is

$$\sum_{j\in\mathbb{Z}} \rho(j)\,|j\rangle\,|\mathbf{x}+j\mathbf{s}\rangle\,|\mathbf{A}\mathbf{x}-j\mathbf{e}\rangle$$



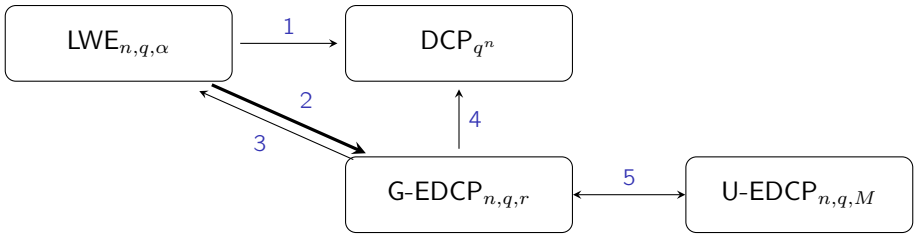
We hit a point in the intersection with probability([R02]):

$$1-\mathcal{O}(\sqrt{n}\|\mathbf{e}\|/R).$$

Take $R\approx\lambda_1(\Lambda_q(\mathbf{A}))\approx q \implies \mathcal{O}(q/(\sqrt{n}\|\mathbf{e}\|))$ 'good' measurements that result in

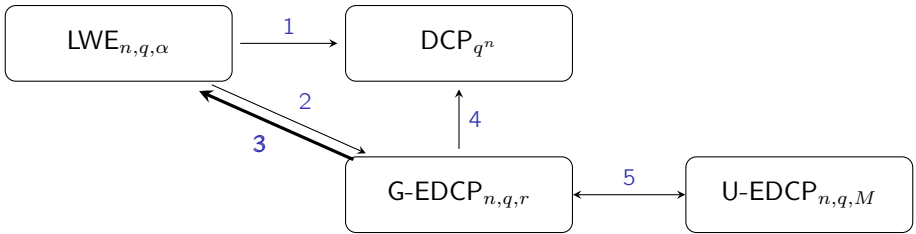
$$\sum_{j\in\mathbb{Z}} \rho(j)\,|j\rangle\,|\mathbf{x}+j\mathbf{s}\rangle\,|\mathbf{A}\mathbf{x}-j\mathbf{e}\rangle \xrightarrow{\text{0-ize the last register}} \sum_{j\in\mathbb{Z}} \rho(j)\,|j\rangle\,|\mathbf{x}-j\mathbf{s}\rangle$$

Reductions btw LWE, DCP, EDCP



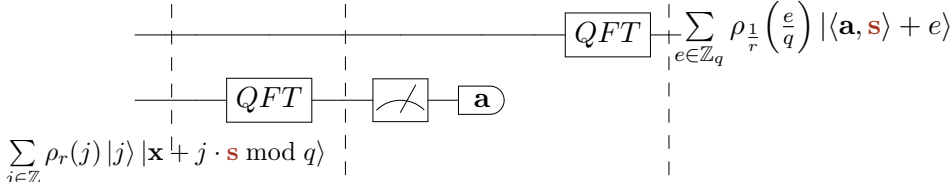
1. LWE$_{n,q,1/\mathrm{poly}} \leq$ DCP$_{q^n}$, [R02,R07]
2. LWE$_{n,q,\alpha} \leq$ G-EDCP$_{n,q,r}$ where $r \cdot \#\text{samples} \approx \mathrm{poly}(n)$. [BKSW18]
3. G-EDCP$_{n,q,r} \leq$ LWE$_{n,q,\alpha}$ where $\alpha \approx 1/r$. [BKSW18]
4. G-EDCP$_{n,q,r} \leq$ DCP$_{q^n}$. [BKSW18,D20]
5. G-EDCP$_{n,q,r} =$ U-EDCP$_{n,q,M}$ for $M = \Theta(r)$. [BKSW18]

Reductions btw LWE, DCP, EDCP



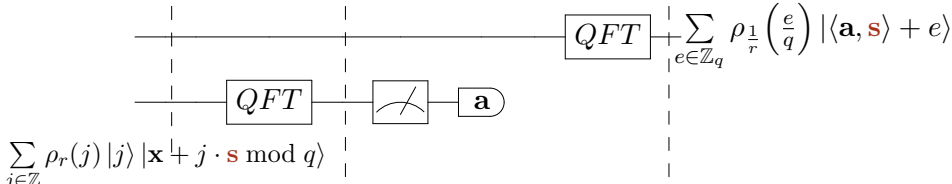
1. LWE$_{n,q,1/\mathrm{poly}} \leq$ DCP$_{q^n}$, [R02,R07]
2. LWE$_{n,q,\alpha} \leq$ G-EDCP$_{n,q,r}$ where $r \cdot \#\text{samples} \approx \mathrm{poly}(n)$. [BKSW18]
3. G-EDCP$_{n,q,r} \leq$ LWE$_{n,q,\alpha}$ where $\alpha \approx 1/r$. [BKSW18]
4. G-EDCP$_{n,q,r} \leq$ DCP$_{q^n}$. [BKSW18,D20]
5. G-EDCP$_{n,q,r} =$ U-EDCP$_{n,q,M}$ for $M = \Theta(r)$. [BKSW18]

G-EDCP $\leq$ LWE



G-EDCP $\leq$ LWE

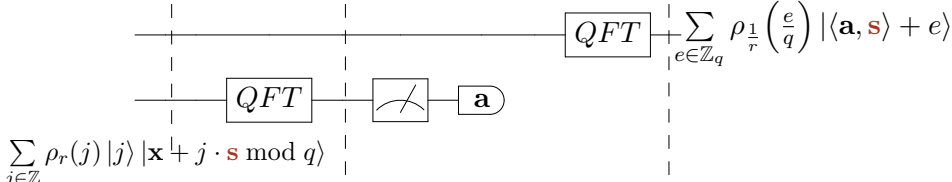
$$\omega_q = e^{2\pi i/q}$$



$$(1) : \sum_{\mathbf{a}\in\mathbb{Z}_q^n}\sum_{j\in\mathbb{Z}} \omega_q^{\langle(\mathbf{x}+j\cdot\mathbf{s}),\mathbf{a}\rangle}\cdot\rho_r(j)\,|j\rangle\,|\mathbf{a}\rangle$$

G-EDCP $\leq$ LWE

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



$$(1): \sum_{\mathbf{a}\in\mathbb{Z}_q^n}\sum_{j\in\mathbb{Z}} \omega_q^{\langle(\mathbf{x}+j\cdot\mathbf{s}),\mathbf{a}\rangle}\cdot\rho_r(j)\,|j\rangle\,|\mathbf{a}\rangle$$

$$(2): \sum_{b\in\mathbb{Z}_q}\sum_{j\in\mathbb{Z}} \omega_q^{j\cdot(\langle\mathbf{a},\mathbf{s}\rangle+b)}\cdot\rho_r(j)\,|b\rangle$$

G-EDCP $\leq$ LWE

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

Poisson summation (PSF):

$$\rho_r(\mathbb{Z}^n + \mathbf{u}) = r^n \sum_{\mathbf{x}\in\mathbb{Z}^n} e^{2\pi i\langle \mathbf{u},\mathbf{x}\rangle}\rho_{1/r}(\mathbf{u})$$

QFT

$$\sum_{e\in\mathbb{Z}_q} \rho_{\frac{1}{r}}\left(\frac{e}{q}\right)|\langle \mathbf{a},\mathbf{s}\rangle + e\rangle$$

(2)

$$(1): \sum_{\mathbf{a}\in\mathbb{Z}_q^n}\sum_{j\in\mathbb{Z}} \omega_q^{\langle(\mathbf{x}+j\cdot\mathbf{s}),\mathbf{a}\rangle}\cdot\rho_r(j)\,|j\rangle\,|\mathbf{a}\rangle$$

$$(2): \sum_{b\in\mathbb{Z}_q}\sum_{j\in\mathbb{Z}} \omega_q^{j\cdot(\langle \mathbf{a},\mathbf{s}\rangle+b)}\cdot\rho_r(j)\,|b\rangle \xrightarrow{\text{PSF}} \sum_{b\in\mathbb{Z}_q}\sum_{j\in\mathbb{Z}} \rho_{\frac{1}{r}}\left(j+\frac{\langle \mathbf{a},\mathbf{s}\rangle+b}{q}\right)|b\rangle$$

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

Poisson summation (PSF):

$$\rho_r(\mathbb{Z}^n + \mathbf{u}) = r^n \sum_{\mathbf{x}\in\mathbb{Z}^n} e^{2\pi i\langle \mathbf{u},\mathbf{x}\rangle} \rho_{1/r}(\mathbf{u})$$

QFT

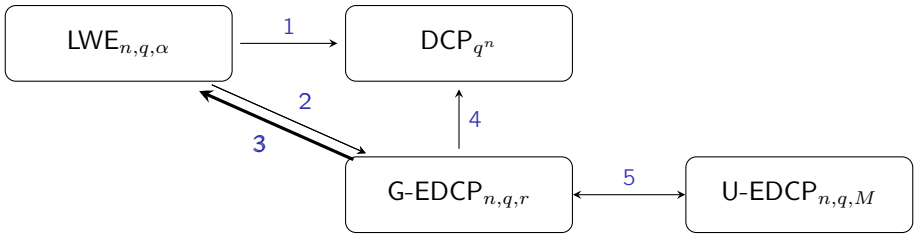
$$\sum_{e\in\mathbb{Z}_q} \rho_{\frac{1}{r}}\left(\frac{e}{q}\right) |\langle \mathbf{a},\mathbf{s}\rangle + e\rangle$$

(2)

$$(1): \sum_{\mathbf{a}\in\mathbb{Z}_q^n} \sum_{j\in\mathbb{Z}} \omega_q^{\langle (\mathbf{x}+j\cdot\mathbf{s}),\mathbf{a}\rangle} \cdot \rho_r(j)\,|j\rangle\,|\mathbf{a}\rangle$$

$$(2): \sum_{b\in\mathbb{Z}_q} \sum_{j\in\mathbb{Z}} \omega_q^{j\cdot(\langle \mathbf{a},\mathbf{s}\rangle + b)} \cdot \rho_r(j)\,|b\rangle \xrightarrow{\text{PSF}} \sum_{b\in\mathbb{Z}_q} \sum_{j\in\mathbb{Z}} \rho_{\frac{1}{r}}\left(j + \frac{\langle \mathbf{a},\mathbf{s}\rangle + b}{q}\right) |b\rangle = \sum_{e\in\mathbb{Z}} \rho_{\frac{1}{r}}\left(\frac{e}{q}\right) |\langle -\mathbf{a},\mathbf{s}\rangle + \mathbf{e}\rangle$$

Reductions btw LWE, DCP, EDCP



1. LWE$_{n,q,1/\mathrm{poly}} \leq$ DCP$_{q^n}$, [R02,R07]
2. LWE$_{n,q,\alpha} \leq$ G-EDCP$_{n,q,r}$ where $r \cdot \#\text{samples} \approx \mathrm{poly}(n)$. [BKSW18]
3. G-EDCP$_{n,q,r} \leq$ LWE$_{n,q,\alpha}$ where $\alpha \approx 1/r$. [BKSW18]
4. G-EDCP$_{n,q,r} \leq$ DCP$_{q^n}$. [BKSW18,D20]
5. G-EDCP$_{n,q,r} =$ U-EDCP$_{n,q,M}$ for $M = \Theta(r)$. [BKSW18]

Complexity of (U)-EDCP $\sum_{j=0}^{M-1} |j\rangle |\mathbf{x} + j \cdot \mathbf{s} \bmod q\rangle$

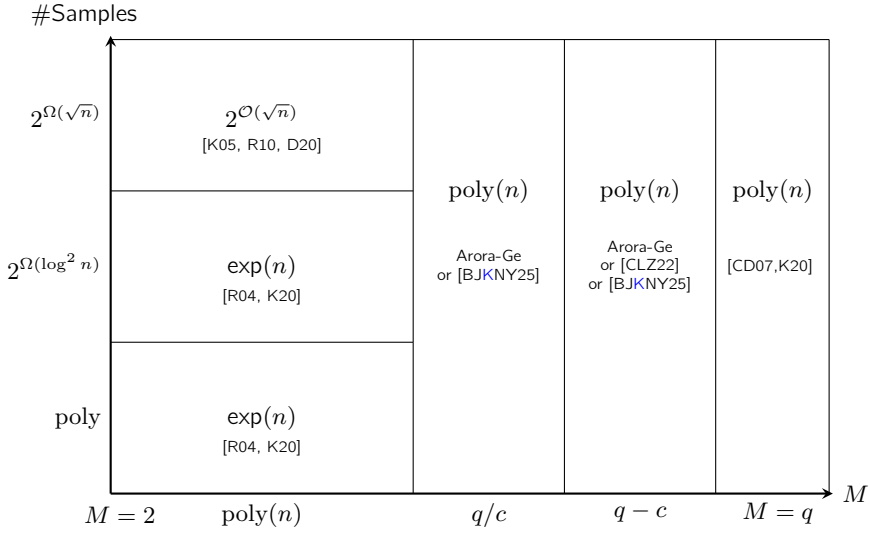


Figure: Complexity of U-EDCP$_{n,q,M}$.

Complexity of (U)-EDCP $\sum_{j=0}^{M-1} |j\rangle |\mathbf{x} + j \cdot \mathbf{s} \bmod q\rangle$

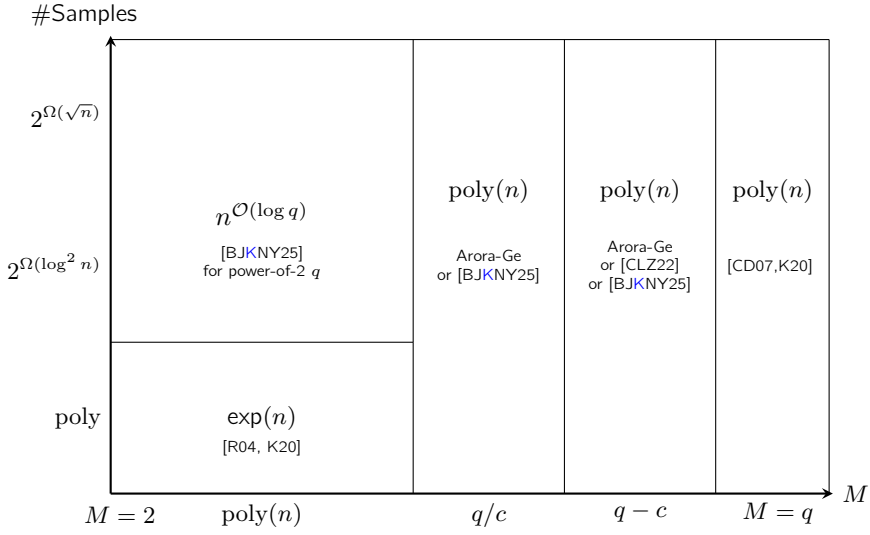


Figure: Complexity of U-EDCP$_{n,q,M}$.

Thoughts

- Having a reduction "LWE $\leq$ EDCP " that produces $n^{\log q}$ EDCP samples will lead to quasi-polynomial quantum algorithm for LWE
- Extending the algorithm from [BJKNY25] to moduli $q = p^t$ for $p = \mathrm{poly}(n)$, you'll get a $\mathrm{poly}(n)$ algorithm for LWE
- A sub-exponential algorithm for EDCP with $\mathrm{poly}(n)$ samples would lead to a sub-exponential attack on LWE
- Recent eprint 2026/155 shows a module-LWE analogue of EDCP. Is it easier than EDCP?

What about codes?

For $\mathbf{A} \in \mathbb{F}_2^{n \times k}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$, following the same steps as for LWE we can construct:

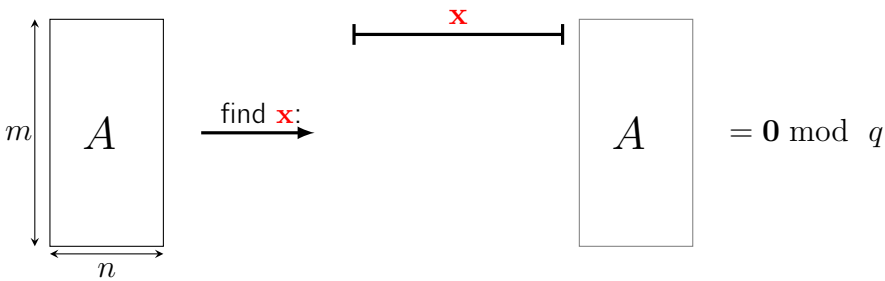
$$\sum_{\mathbf{x} \in \mathbb{F}_2^n} |0, \mathbf{x}, \mathbf{A}\mathbf{x} \bmod 2\rangle + |1, \mathbf{x} + \mathbf{s}, \mathbf{A}\mathbf{x} + \mathbf{e} \bmod 2\rangle$$

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

Part II

Short Integer Solution Quantumly

Definition of SIS

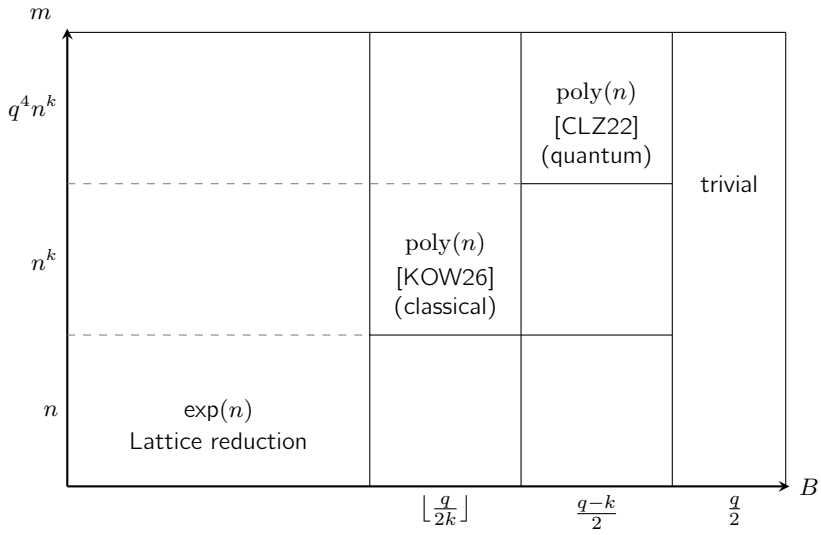


and $0 < \|\mathbf{x}\| \leq B$

Example: to break Dilithium signature, you need to solve SIS for $\|\mathbf{x}\|_\infty < \frac{q}{8}$.

Here we consider $\mod q \in \left[-\frac{q}{2}, \frac{q}{2}\right)$.

SIS_∞ Quantumly/Classically



$k = \Theta(1)$.

Final thoughts and open problems

- Does ball-intersection give the optimal state separation strategy? Consider costlier but more successful function to separate $\mathbf{A}\mathbf{x} + \mathbf{e}_1$ and $\mathbf{A}\mathbf{x} + \mathbf{e}_2$.
- Modulus-dimension switching for LWE allows to reduce LWE to dimension n/k with modulus q^k. If a converse reduction to LWE in dimension $n \log q$ and modulus 2 were possible, we could have solved $\mathsf{EDCP}_{n \log q, 2}$ in polynomial time
- Improve the reduction for binary/small/structured secrets

References

- Arora-Ge Sanjeev Arora and Rong Ge. "New Algorithms for Learning in Presence of Errors", ICALP 2011.
- [BJKNY25] Shi Bai, Hansraj Jangir, Elena Kirshanova, Tran Ngo, William Youmans. "A Quasi-polynomial Time Algorithm for the Extrapolated Dihedral Coset Problem over Power-of-Two Moduli". Crypto 2025.
- [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)
- [KOW26] Robin Kothari, Ryan O'Donnell, Kewen Wu. "No exponential quantum speedup for SIS$^\infty$ anymore"
- [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.