Connections between Learning with Errors and the Dihedral Coset Problem

Elena Kirshanova

joint work with Zvika Brakerski, Damien Stehlé, and Weiqiang Wen

LWE and DCP

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

LWE: Given

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

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

LWE and DCP

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 DCP

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

$\leq$
[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.

LWE and DCP

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 DCP

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

BKW / lattices:

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

Kuperberg:

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

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:

$$\text{DCP} \leq \text{SubsetSum}_{1 \cdot c} \text{ [Reg'02], but}$$

$$\text{SubsetSum}_{\frac{1}{\log n}} \leq \text{LWE} \leq \text{Vec. SubsetSum}_{> \log n}$$

Inverse direction

Is DCP $\leq$ LWE?

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

$$\text{DCP} \leq \text{SubsetSum}_{1 \cdot c} \text{ [Reg'02], but}$$

$$\text{SubsetSum}_{\frac{1}{\log n}} \leq \text{LWE} \leq \text{Vec. SubsetSum}_{>\log n}$$

No, but we show that $\underline{\text{E}}$DCP $\leq$ LWE

Extended DCP

<u>EDCP</u>

for a distr. $\mathcal{D}$

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

<u>DCP</u>

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

Extended DCP

EDCP

for a distr. $\mathcal{D}$

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

DCP

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

G-EDCP

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

U-EDCP

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

Extended DCP

EDCP

for a distr. $\mathcal{D}$

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

DCP

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

G-EDCP

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

U-EDCP

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

Main result:

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

$\iff$ hides polynomial loses

Extended DCP

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

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

DCP

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

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

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

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

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

$$\begin{array}{ccccccc}
\mathsf{LWE}_{n,q,\frac{q}{r \cdot \mathrm{poly}(n)}} & \Longrightarrow & \mathsf{G\text{-}EDCP}_{n,q,r} & \Longrightarrow & \mathsf{U\text{-}EDCP}_{n,q,c \cdot r} & \Longrightarrow & \mathsf{DCP}_{2^{n \log q}} \\
 & & \Downarrow & & \Downarrow & & \\
 & & \mathsf{LWE}_{n,q,q/r} & & \mathsf{G\text{-}EDCP}_{n,q,r/\sqrt{n}} & &
\end{array}$$

Dimension modulus st. dev.

Extended DCP

<u>EDCP</u>

for a distr. $\mathcal{D}$

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

<u>DCP</u>

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

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

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

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

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

Quantum rejection sampling, Ozols et al.

$$\begin{tikzcd}
\mathsf{LWE}_{n,q,\frac{q}{r\cdot \mathrm{poly}(n)}} \arrow[r, Rightarrow] & \mathsf{G\text{-}EDCP}_{n,q,r} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \mathsf{U\text{-}EDCP}_{n,q,c\cdot r} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \mathsf{DCP}_{2^{n\log q}} \\
 & \mathsf{LWE}_{n,q,q/r} & \mathsf{G\text{-}EDCP}_{n,q,r/\sqrt{n}} &
\end{tikzcd}$$

Dimension modulus st. dev.

Results

$$\begin{tikzcd}
\mathrm{LWE}_{n,q,\frac{q}{r\cdot \mathrm{poly}(n)}} \arrow[r, Rightarrow] \arrow[rrr, Rightarrow, bend left, "\text{via average case lattice problems [Reg02]+[LM09]}"] & \text{G-EDCP}_{n,q,r} \arrow[r, Rightarrow] & \text{U-EDCP}_{n,q,c\cdot r} \arrow[r, Rightarrow] & \mathrm{DCP}_{2^{n\log q}[2^{n^2}]}
\end{tikzcd}$$

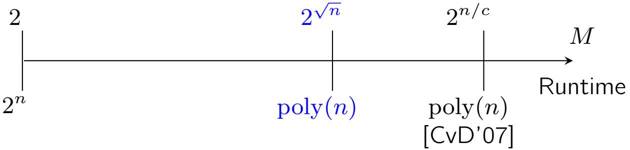
Results

via average case lattice problems [Reg02]+[LM09]

$$\text{LWE}_{n,q,\frac{q}{r\cdot \mathrm{poly}(n)}} \Longrightarrow \text{G-EDCP}_{n,q,r} \Longrightarrow \text{U-EDCP}_{n,q,c\cdot r} \Longrightarrow \text{DCP}_{2^{n\log q}[2^{n^2}]}$$

1-dim UDCP was already considered in [Childs-van Dam'07]:

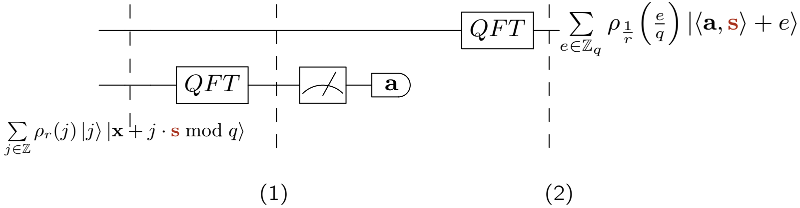
$$\sum_{j=0}^{M-1} |j\rangle\, |x + j \cdot s \bmod 2^n\rangle$$



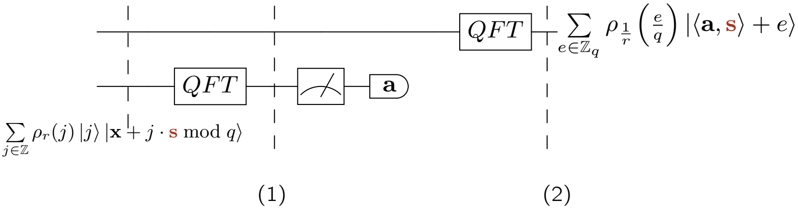
[Brakerski et. al]

$$\text{LWE}_{\sqrt{n},2^{\sqrt{n}},\frac{2^{\sqrt{n}}}{M}} \Longleftarrow \text{LWE}_{1,2^n,\frac{2^n}{M}} \Longleftarrow \text{G-EDCP}_{1,2^n,M} \Longleftarrow \text{U-EDCP}_{1,2^n,M}$$

G-EDCP $\leq$ LWE

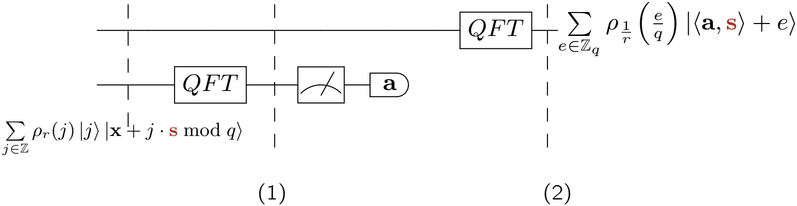


G-EDCP $\leq$ LWE



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

G-EDCP $\leq$ LWE



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

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

Open questions

- how to make use of several shifts (exact complexity of Kuperberg's algorithm with multiple shifts).
- trade samples vs. shifts: UDCP self-reduction allowing to trade ℓ for M?
- extend quantum rejection sampling to ring-lwe states