Learning With Errors and Extrapolated Dihedral Coset Problem

Weiqiang Wen[1]

Joint work with Zvika Brakerski[2], Elena Kirshanova[1] and Damien Stehlé[1]

[1]École Normale Supérieure de Lyon
[2]Weizmann Institute of Science

PKC 2018, Rio de Janeiro

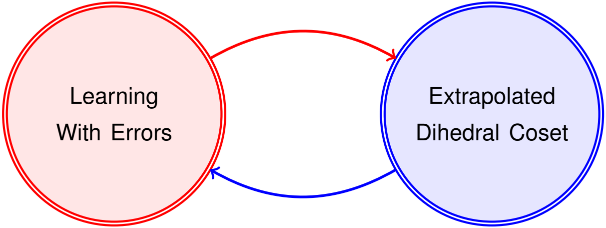
European Research Council

ENS DE LYON

This Talk

Main Result (Informal)

We show a (quantum) computational equivalence between Learning With Errors and an Extrapolated version of Dihedral Coset Problem.

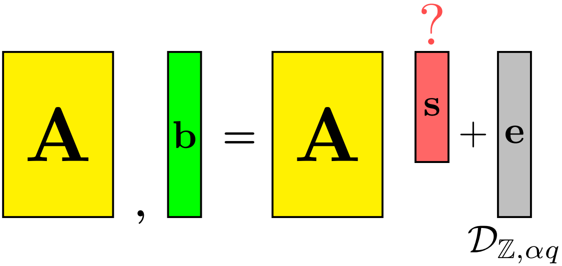


Learning With Errors

Learning With Errors Problem for n, q, m and $\mathcal{D}_{\mathbb{Z},\alpha q}$ ($\mathrm{LWE}^m_{n,q,\alpha}$)

Input: $m \geq n$ samples of the form $(\mathbf{a}, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$,
with $\mathbf{a} \hookleftarrow \mathbb{Z}_q^n$ and $b = \langle \mathbf{a}, \mathbf{s} \rangle + e$, where $e \hookleftarrow \mathcal{D}_{\mathbb{Z},\alpha q}$ and $\mathbf{s} \hookleftarrow \mathbb{Z}_q^n$.

Output: the secret vector $\mathbf{s}$.



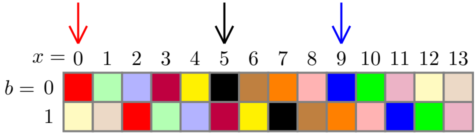
The Dihedral Coset Problem

Dihedral Coset Problem (DCP) for n, q and m $\quad$ ($\mathrm{DCP}^m_{n,q}$)

Input: $\{|{\color{red}0}, {\color{red}0} + \mathbf{x}_i\rangle + |{\color{red}1}, {\color{red}\mathbf{s}} + \mathbf{x}_i\rangle\}_{i \le m}$ with $\mathbf{x}_i \in \mathbb{Z}_q^n$ arbitrary and ${\color{red}\mathbf{s}} \in \mathbb{Z}_q^n$ fixed.

Output: the secret ${\color{red}\mathbf{s}}$.

Example:



- DCP with $n = 1$, $N = 14$, and secret ${\color{red}s} = 2$.

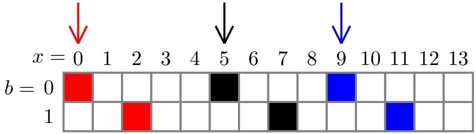
The Dihedral Coset Problem

Dihedral Coset Problem (DCP) for n, q and m $\quad$ ($\mathrm{DCP}^m_{n,q}$)

Input: $\{|0, 0 + \mathbf{x}_i\rangle + |1, \mathbf{s} + \mathbf{x}_i\rangle\}_{i \leq m}$ with $\mathbf{x}_i \in \mathbb{Z}_q^n$ arbitrary and $\mathbf{s} \in \mathbb{Z}_q^n$ fixed.

Output: the secret $\mathbf{s}$.

Example:



- DCP with $n = 1$, $N = 14$, and secret $s = 2$.
- Samples: $|0, 0\rangle + |1, 2\rangle$; $\quad |0, 5\rangle + |1, 7\rangle$; $\quad |0, 9\rangle + |1, 11\rangle$.

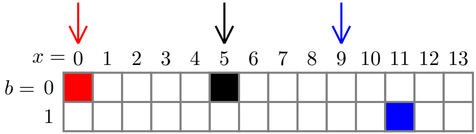
The Dihedral Coset Problem

Dihedral Coset Problem (DCP) for n, q and m ($\mathrm{DCP}^m_{n,q}$)

Input: $\{|0, 0 + \mathbf{x}_i\rangle + |1, \mathbf{s} + \mathbf{x}_i\rangle\}_{i \le m}$ with $\mathbf{x}_i \in \mathbb{Z}_q^n$ arbitrary and $\mathbf{s} \in \mathbb{Z}_q^n$ fixed.

Output: the secret $\mathbf{s}$.

Example:



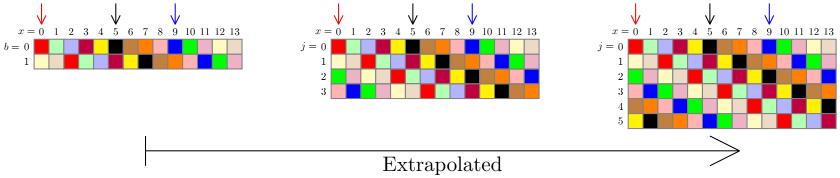
- DCP with $n = 1$, $N = 14$, and secret $s = 2$.
- ***Measured*** random results: $|0, 0\rangle$; $|0, 5\rangle$; $|1, 11\rangle$.

The Dihedral Coset Problem

Dihedral Coset Problem (DCP) for n, q and m $\quad(\mathrm{DCP}^m_{n,q})$

Input: $\{|0, 0 + \mathbf{x}_i\rangle + |1, \mathbf{s} + \mathbf{x}_i\rangle\}_{i \leq m}$ with $\mathbf{x}_i \in \mathbb{Z}_q^n$ arbitrary and $\mathbf{s} \in \mathbb{Z}_q^n$ fixed.

Output: the secret $\mathbf{s}$.



Extrapolated Dihedral Coset Problem

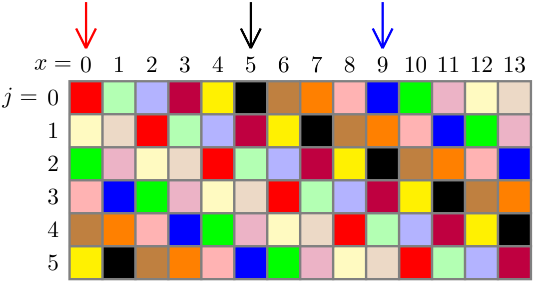
Extrapolated Dihedral Coset Problem for n, q, m and $\mathcal{U}[M]$ (U-EDCP)

Input: m registers of the form:

$$\sum_{j \in [M]} |j, (\mathbf{x} + j \cdot \mathbf{s}) \bmod q\rangle ,$$

where $\mathbf{x} \in \mathbb{Z}_q^n$ is arbitrary and $\mathbf{s} \in \mathbb{Z}_q^n$ is fixed.

Output: the secret $\mathbf{s}$.



Extrapolated Dihedral Coset Problem

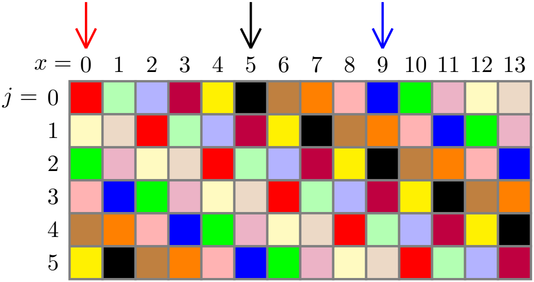
Extrapolated Dihedral Coset Problem for n, q, m and $\mathcal{D}_{\mathbb{Z},r}$ (G-EDCP)

Input: m registers of the form:

$$\sum_{j \in \mathbb{Z}} e^{-\pi \frac{|j|^2}{r^2}} \left| j, (\mathbf{x} + j \cdot \mathbf{s}) \bmod q \right\rangle ,$$

where $\mathbf{x} \in \mathbb{Z}_q^n$ is arbitrary and $\mathbf{s} \in \mathbb{Z}_q^n$ is fixed.

Output: the secret $\mathbf{s}$.



An Example - EDCP with $n = 1$, $q = 14$, $m = 3$ and $\mathcal{U}[6]$

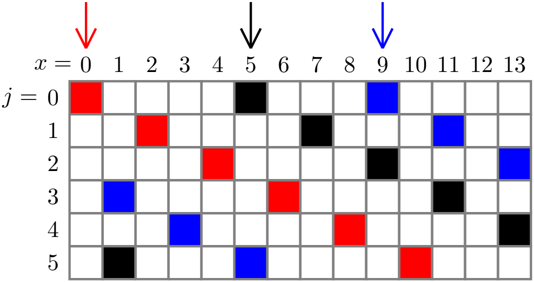
Input:

$$\frac{1}{\sqrt{6}}\left(|0,0\rangle + |1,2\rangle + |2,4\rangle + |3,6\rangle + |4,8\rangle + |5,10\rangle\right)$$

$$\frac{1}{\sqrt{6}}\left(|0,5\rangle + |1,7\rangle + |2,9\rangle + |3,11\rangle + |4,13\rangle + |5,1\rangle\right)$$

$$\frac{1}{\sqrt{6}}\left(|0,9\rangle + |1,11\rangle + |2,13\rangle + |3,1\rangle + |4,3\rangle + |5,5\rangle\right)$$

Output: the secret s $(= 2)$.



Main Result: equivalence between LWE and U-EDCP

- For $m \leq \mathrm{poly}(n)$, $1/M = \alpha$, we have

$$\mathrm{LWE}^{m}_{n,q,\alpha} =_{\mathrm{poly}(n)} \text{U-EDCP}^{m}_{n,q,M}$$

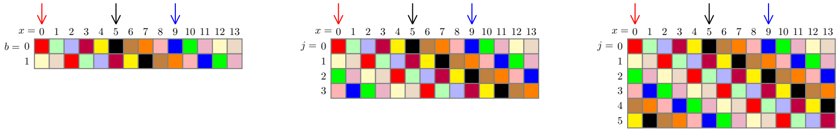
Why is LWE interesting?

$$\mathbf{A}, \quad \mathbf{b} = \mathbf{A} \times \overset{?}{\mathbf{s}} + \mathbf{e}$$

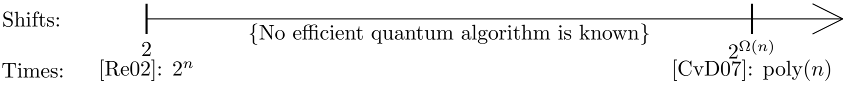
- Presumed hardness:
  - Worst-case to average-case reduction [Re05] $\rightarrow$ using average-case LWE but relying on hardness of problems over worst-case lattices.
  - The best known algorithm for LWE takes 2^n time $\rightarrow$ conjectured hard.

O. Regev. On lattices, learning with errors, random linear codes, and cryptography. STOC'05.

Why is EDCP interesting (for LWE)?

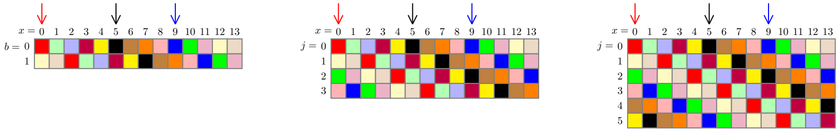


- Given $m = \mathrm{poly}(n)$ samples:

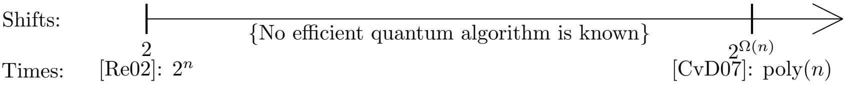


O. Regev. Quantum computation and lattice problems. FOCS'02.
A. M. Childs and W. van Dam. Quantum algorithm for a generalized hidden shift problem. SODA'07.

Why is EDCP interesting (for LWE)?



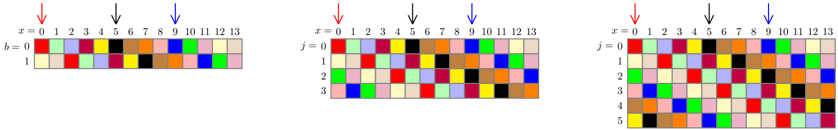
- Given $m = \mathrm{poly}(n)$ samples:



$\Rightarrow$ A connection to LWE might give a quantum hardness evidence for LWE.

O. Regev. Quantum computation and lattice problems. FOCS'02.
A. M. Childs and W. van Dam. Quantum algorithm for a generalized hidden shift problem. SODA'07.

Why is EDCP interesting (for LWE)?



- Given $m = \mathrm{poly}(n)$ samples:

Shifts: 2 —— {No efficient quantum algorithm is known} —— $2^{\Omega(n)}$

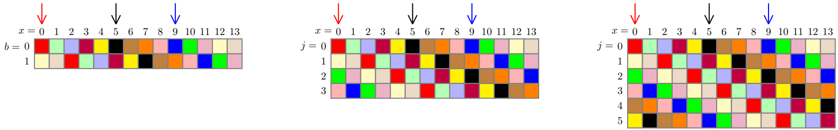
Times: [Re02]: 2^n …… [CvD07]: $\mathrm{poly}(n)$

$\Rightarrow$ A connection to LWE might give a quantum hardness evidence for LWE.

- Given $m = \mathrm{subexp}(n)$:
  - (E)DCP$^m_{n,q}$ can be solved in sub-exponential time [Ku05].

O. Regev. Quantum computation and lattice problems. FOCS'02.
A. M. Childs and W. van Dam. Quantum algorithm for a generalized hidden shift problem. SODA'07.
G. Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. SIAM J. Comput., 2005.

Why is EDCP interesting (for LWE)?



- Given $m = \mathrm{poly}(n)$ samples:

Shifts: 2 —— {No efficient quantum algorithm is known} —— $2^{\Omega(n)}$ →

Times: [Re02]: 2^n …… [CvD07]: $\mathrm{poly}(n)$

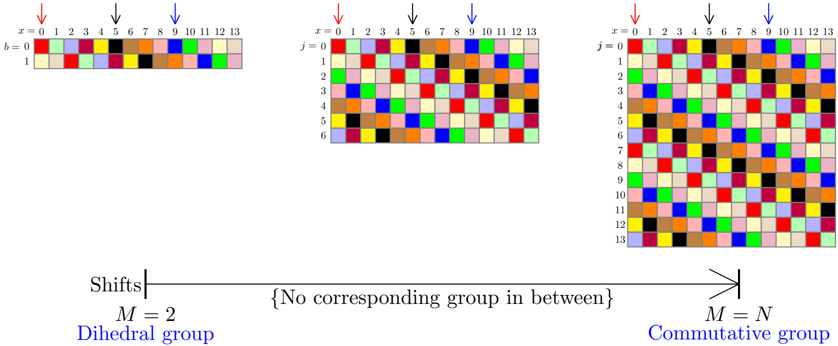
$\Rightarrow$ A connection to LWE might give a quantum hardness evidence for LWE.

- Given $m = \mathrm{subexp}(n)$:
  - (E)DCP$^m_{n,q}$ can be solved in sub-exponential time [Ku05].

$\Rightarrow$ A connection to LWE might give an efficient quantum algorithm for LWE.

O. Regev. Quantum computation and lattice problems. FOCS'02.
A. M. Childs and W. van Dam. Quantum algorithm for a generalized hidden shift problem. SODA'07.
G. Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. SIAM J. Comput., 2005.

Why is EDCP interesting (by itself)?



- EDCP with $M = N = 2^n$: coset problem over the group $\mathbb{Z}_N \times \mathbb{Z}_N$.
- EDCP with $M = \mathrm{poly}(n)$ is considered in this work.
- DCP serves as the security foundation of some symmetric primitives [AR17].

G. Alagic and A. Russell. Quantum-Secure Symmetric-Key Cryptography Based on Hidden Shifts. EUROCRYPT'17.

Prior works

$\text{BDD}_{n,1/\mathrm{poly}(n)}$

$\text{DCP}^{\mathrm{poly}(n)}_{n,2^n}$

SubsetSum

$\text{U-EDCP}^{\mathrm{poly}(n)}_{n,q,2^{\Omega(n)}}$

vectorial SubsetSum

$\text{LWE}_{n,q,1/\mathrm{poly}(n)}$

$\text{G-EDCP}^{\mathrm{poly}(n)}_{n,q,\mathrm{poly}(n)}$

$\text{BDD}_{n,1/\mathrm{poly}(n)}$ $\xrightarrow{\textbf{1}\text{ [Re02]}}$ $\text{DCP}^{\mathrm{poly}(n)}_{n,2^n}$

SubsetSum

$\text{U-EDCP}^{\mathrm{poly}(n)}_{n,q,2^{\Omega(n)}}$

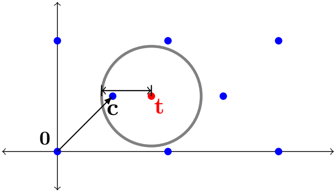
vectorial SubsetSum

$\text{LWE}_{n,q,1/\mathrm{poly}(n)}$

$\text{G-EDCP}^{\mathrm{poly}(n)}_{n,q,\mathrm{poly}(n)}$

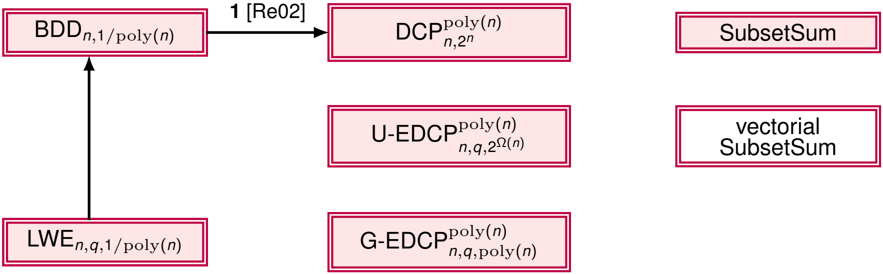
1. From BDD_n to DCP_n with modulus 2^n.

Bounded Distance Decoding:



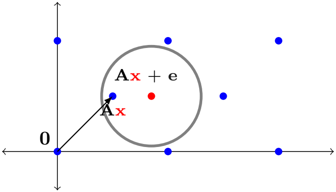
O. Regev. Quantum computation and lattice problems. FOCS'02.

Prior works



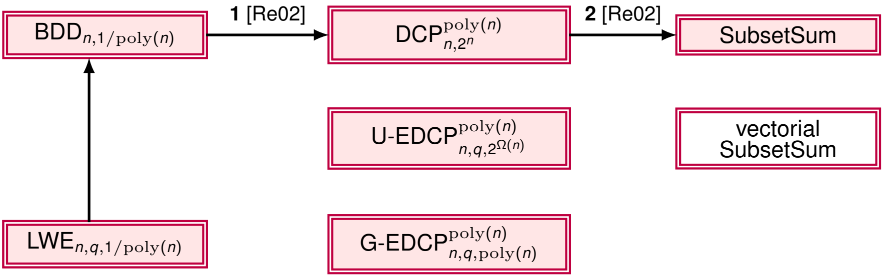
1. From BDD_n to DCP_n with modulus 2^n.

<ins>LWE = average-case BDD</ins>



O. Regev. Quantum computation and lattice problems. FOCS'02.

Prior works

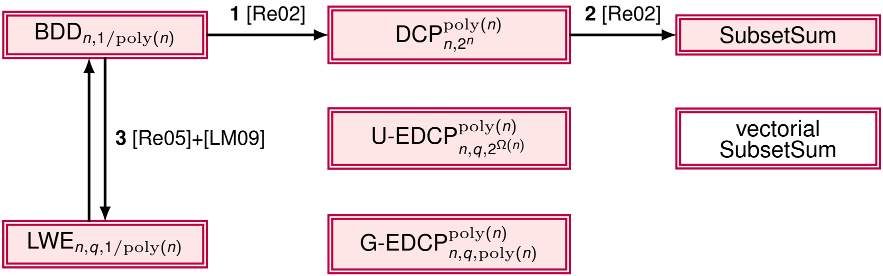


1. From BDD_n to DCP_n with modulus 2^n.

2. From DCP to SubsetSum with density ≈ 1.

O. Regev. Quantum computation and lattice problems. FOCS'02.

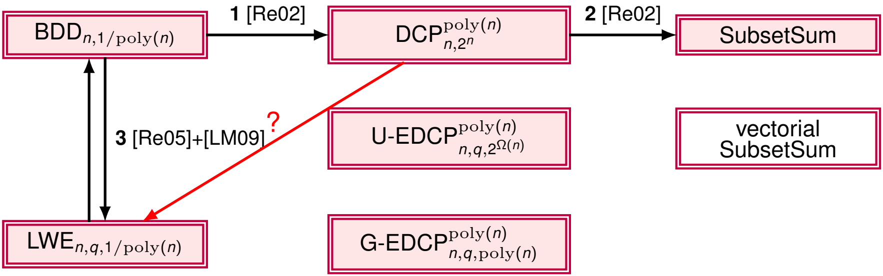
Prior works



1. From BDD_n to DCP_n with modulus 2^n.
2. From DCP to SubsetSum with density ≈ 1.
3. From BDD to LWE by worst-to-average reduction; LWE is average-case BDD.

O. Regev. Quantum computation and lattice problems. FOCS'02.
O. Regev. On lattices, learning with errors, random linear codes, and cryptography. STOC'05.
V. Lyubashevsky and D. Micciancio. On bounded distance decoding, unique shortest vectors, and the minimum distance problem, CRYPTO'09.

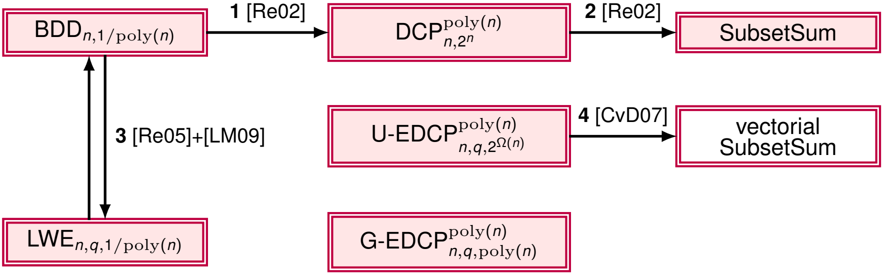
Prior works



1. From BDD_n to DCP_n with modulus 2^n.
2. From DCP to SubsetSum with density ≈ 1.
3. From BDD to LWE by worst-to-average reduction; LWE is average-case BDD.

O. Regev. Quantum computation and lattice problems. FOCS'02.
O. Regev. On lattices, learning with errors, random linear codes, and cryptography. STOC'05.
V. Lyubashevsky and D. Micciancio. On bounded distance decoding, unique shortest vectors, and the minimum distance problem, CRYPTO'09.

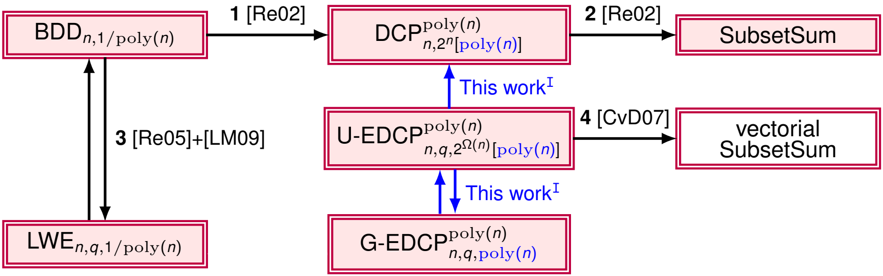
Prior works



1. From BDD_n to DCP_n with modulus 2^n.
2. From DCP to SubsetSum with density ≈ 1.
3. From BDD to LWE by worst-to-average reduction; LWE is average-case BDD.
4. Polynomial time algorithm for EDCP with $2^{\Omega(n)}$ many shifts.

O. Regev. Quantum computation and lattice problems. FOCS'02.
O. Regev. On lattices, learning with errors, random linear codes, and cryptography. STOC'05.
V. Lyubashevsky and D. Micciancio. On bounded distance decoding, unique shortest vectors, and the minimum distance problem, CRYPTO'09.
A. M. Childs and W. van Dam. Quantum algorithm for a generalized hidden shift problem. SODA'07.

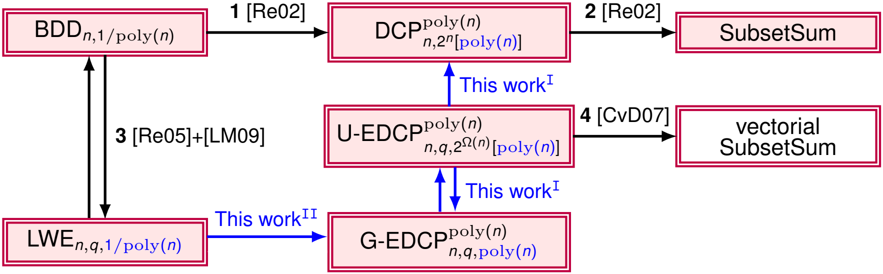
This work



I. Using quantum rejection sampling [ORR13].

O. Regev. Quantum computation and lattice problems. FOCS'02.
O. Regev. On lattices, learning with errors, random linear codes, and cryptography. STOC'05.
V. Lyubashevsky and D. Micciancio. On bounded distance decoding, unique shortest vectors, and the minimum distance problem, CRYPTO'09.
A. M. Childs and W. van Dam. Quantum algorithm for a generalized hidden shift problem. SODA'07.
M. Ozols, M. Roetteler, and J. Roland. Quantum rejection sampling. ACM Trans. Comput. Theory, 2013.

This work

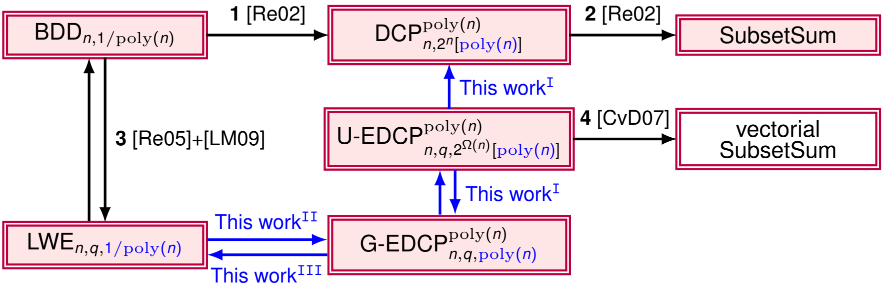


I. Using quantum rejection sampling [ORR13].

II. LWE $\leq$ EDCP: achieves a better parameter, compared to **1**+**3**.

O. Regev. Quantum computation and lattice problems. FOCS'02.
O. Regev. On lattices, learning with errors, random linear codes, and cryptography. STOC'05.
V. Lyubashevsky and D. Micciancio. On bounded distance decoding, unique shortest vectors, and the minimum distance problem, CRYPTO'09.
A. M. Childs and W. van Dam. Quantum algorithm for a generalized hidden shift problem. SODA'07.
M. Ozols, M. Roetteler, and J. Roland. Quantum rejection sampling. ACM Trans. Comput. Theory, 2013.

This work



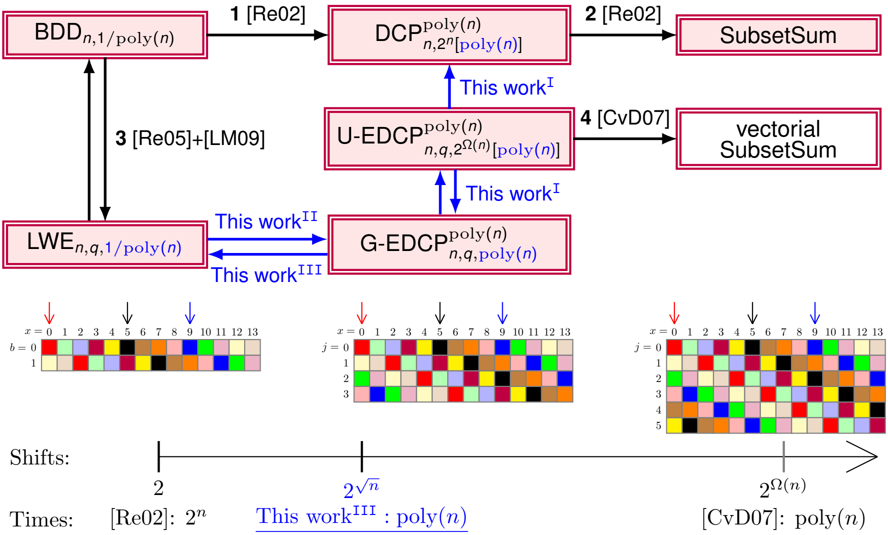
I. Using quantum rejection sampling [ORR13].

II. LWE $\leq$ EDCP: achieves a better parameter, compared to **1**+**3**.

III. EDCP $\leq$ LWE: shows computational equivalence; and this gives better algorithm than **4** for EDCP, using LWE algorithms.

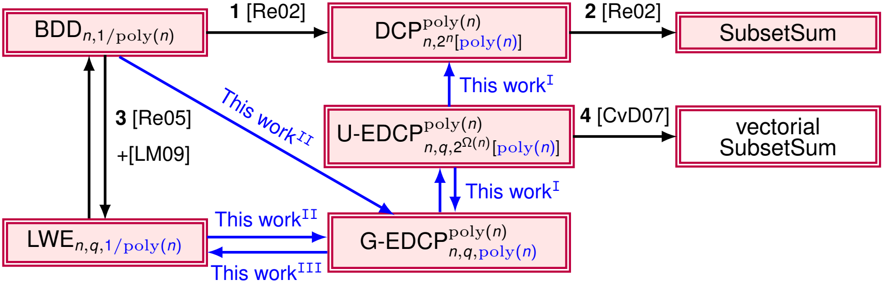
O. Regev. Quantum computation and lattice problems. FOCS'02.
O. Regev. On lattices, learning with errors, random linear codes, and cryptography. STOC'05.
V. Lyubashevsky and D. Micciancio. On bounded distance decoding, unique shortest vectors, and the minimum distance problem, CRYPTO'09.
A. M. Childs and W. van Dam. Quantum algorithm for a generalized hidden shift problem. SODA'07.
M. Ozols, M. Roetteler, and J. Roland. Quantum rejection sampling. ACM Trans. Comput. Theory, 2013.

This work



$\mathsf{BDD}_{n,1/\mathrm{poly}(n)}$
1 [Re02]
$\mathsf{DCP}^{\mathrm{poly}(n)}_{n,2^n}[\mathrm{poly}(n)]$
2 [Re02]
SubsetSum
This work$^{\mathrm{I}}$
3 [Re05]+[LM09]
$\mathsf{U\text{-}EDCP}^{\mathrm{poly}(n)}_{n,q,2^{\Omega(n)}}[\mathrm{poly}(n)]$
4 [CvD07]
vectorial SubsetSum
This work$^{\mathrm{I}}$
This work$^{\mathrm{II}}$
$\mathsf{LWE}_{n,q,1/\mathrm{poly}(n)}$
$\mathsf{G\text{-}EDCP}^{\mathrm{poly}(n)}_{n,q,\mathrm{poly}(n)}$
This work$^{\mathrm{III}}$
$x = 0$ 1 2 3 4 5 6 7 8 9 10 11 12 13
$b = 0$
1
$x = 0$ 1 2 3 4 5 6 7 8 9 10 11 12 13
$j = 0$
1
2
3
$x = 0$ 1 2 3 4 5 6 7 8 9 10 11 12 13
$j = 0$
1
2
3
4
5
Shifts:
2
$2^{\sqrt{n}}$
$2^{\Omega(n)}$
Times:
[Re02]: 2^n
This work$^{\mathrm{III}}$: $\mathrm{poly}(n)$
[CvD07]: $\mathrm{poly}(n)$

This work



An alternative worst-to-average case reduction:

$$\mathrm{BDD} \le \mathrm{G\text{-}EDCP} \le \mathrm{LWE}.$$

O. Regev. Quantum computation and lattice problems. FOCS'02.
O. Regev. On lattices, learning with errors, random linear codes, and cryptography. STOC'05.
V. Lyubashevsky and D. Micciancio. On bounded distance decoding, unique shortest vectors, and the minimum distance problem, CRYPTO'09.
A. M. Childs and W. van Dam. Quantum algorithm for a generalized hidden shift problem. SODA'07.
M. Ozols, M. Roetteler, and J. Roland. Quantum rejection sampling. ACM Trans. Comput. Theory, 2013.

First reduction: from LWE to EDCP

- Extension of Regev's BDD_n to $\text{DCP}_{n,2^n}$ reduction.
  - Replacing BDD by LWE is easy.
  - We reduce LWE_n to $\text{DCP}_{n,\mathrm{poly}(n)}$.
  - Replace DCP by EDCP.

First reduction: from LWE to EDCP

- Extension of Regev's BDD_n to $\text{DCP}_{n,2^n}$ reduction.
  - Replacing BDD by LWE is easy.
  - We reduce LWE_n to $\text{DCP}_{n,\mathrm{poly}(n)}$.
  - Replace DCP by EDCP.
- Contribution: come up with EDCP such that converse reduction also works.

Preliminaries for EDCP to LWE reduction

- Quantum Fourier transform: $\left[\omega_q = \mathrm{e}^{\frac{2\pi i}{q}}\right]$

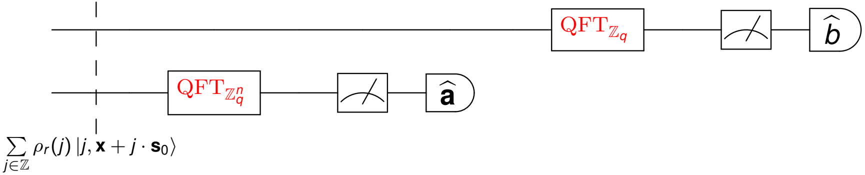
$$\mathcal{F}_q^n : |\mathbf{x}\rangle \mapsto \frac{1}{\sqrt{q}} \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \omega_q^{\langle \mathbf{x},\mathbf{y}\rangle} |\mathbf{y}\rangle .$$

- Poisson summation formula: $\left[\rho_r(x) = \mathrm{e}^{-\pi\frac{x^2}{r^2}}\right]$

$$\sum_{x\in\mathbb{Z}} \rho_r(x+u) = r \cdot \sum_{x^\star\in\mathbb{Z}} \mathrm{e}^{2\pi i(x^\star\cdot u)} \rho_{1/r}(x^\star)$$

holds for any $u \in \mathbb{R}$.

Second direction: from EDCP to LWE



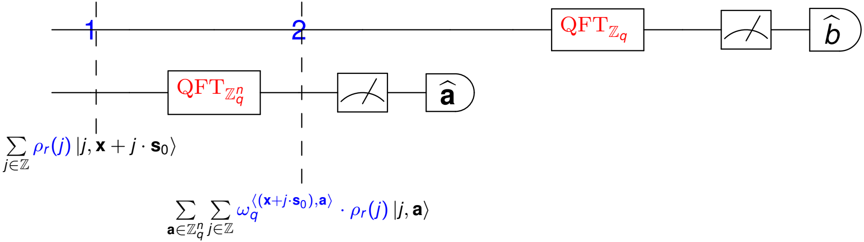
- Input an EDCP state:

$$\sum_{j\in\mathbb{Z}} \rho_r(j) \left|j, \mathbf{x} + j \cdot \mathbf{s}_0 \bmod q\right\rangle .$$

$\Rightarrow$ Output an LWE sample:

$$(\widehat{\mathbf{a}},\ \widehat{b} = \langle \widehat{\mathbf{a}}, \mathbf{s}_0 \rangle + e \bmod q).$$

Second direction: from EDCP to LWE



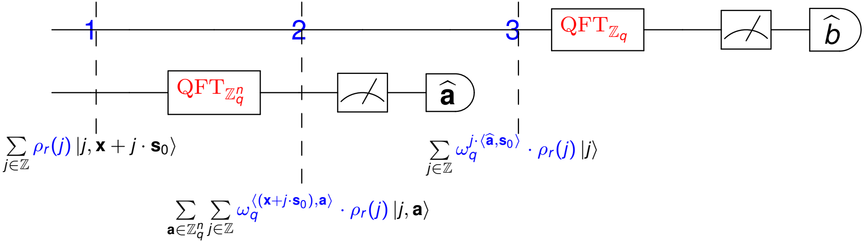
1. EDCP input state:

$$\sum_{j\in\mathbb{Z}} \rho_r(j)\,|j, \mathbf{x} + j\cdot\mathbf{s}_0 \bmod q\rangle\,.$$

2. Quantum Fourier Transform on the second register:

$$\sum_{\mathbf{a}\in\mathbb{Z}_q^n}\sum_{j\in\mathbb{Z}} \omega_q^{\langle(\mathbf{x}+j\cdot\mathbf{s}_0),\mathbf{a}\rangle}\cdot\rho_r(j)\,|j,\mathbf{a}\rangle\,.$$

Second direction: from EDCP to LWE



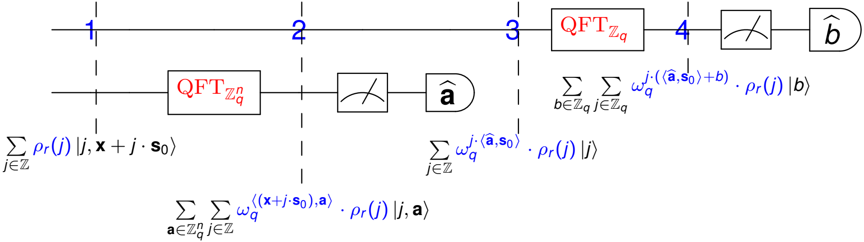
2. Result after Quantum Fourier Transform on the second register:

$$\sum_{\mathbf{a}\in\mathbb{Z}_q^n}\sum_{j\in\mathbb{Z}} \omega_q^{\langle(\mathbf{x}+j\cdot\mathbf{s}_0),\mathbf{a}\rangle}\cdot\rho_r(j)\,|j,\mathbf{a}\rangle\,.$$

3. Measure the second register: [omitting global phase: $\omega_q^{\langle\mathbf{x},\widehat{\mathbf{a}}\rangle}$]

$$\sum_{j\in\mathbb{Z}} \omega_q^{j\cdot\langle\widehat{\mathbf{a}},\mathbf{s}_0\rangle}\cdot\rho_r(j)\,|j\rangle\,\left|\widehat{\mathbf{a}}\right\rangle.$$

Second direction: from EDCP to LWE

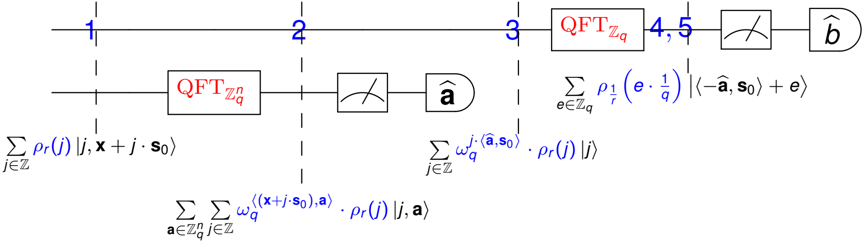


3. Result after measuring the second register: [omitting global phase: $\omega_q^{\langle\mathbf{x},\widehat{\mathbf{a}}\rangle}$]

$$\sum_{j\in\mathbb{Z}}\omega_q^{j\cdot\langle\widehat{\mathbf{a}},\mathbf{s}_0\rangle}\cdot\rho_r(j)\,\left|j,\widehat{\mathbf{a}}\right\rangle.$$

4. Quantum Fourier Transform on the first register:

$$\sum_{b\in\mathbb{Z}_q}\sum_{j\in\mathbb{Z}_q}\omega_q^{j\cdot(\langle\widehat{\mathbf{a}},\mathbf{s}_0\rangle+b)}\cdot\rho_r(j)\,|b\rangle.$$



4. Result after Quantum Fourier Transform on the first register:

$$\sum_{b\in\mathbb{Z}_q}\sum_{j\in\mathbb{Z}} \omega_q^{j\cdot(\langle\widehat{\mathbf{a}},\mathbf{s}_0\rangle+b)}\cdot \rho_r(j)\,|b\rangle\,.$$

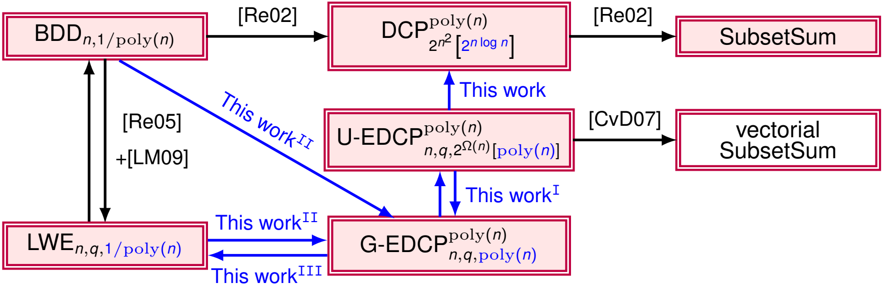
5. Use Poisson summation formula to reorganize:

$$\left[\omega_q = \mathrm{e}^{\frac{2\pi i}{q}}\right]$$

$$\sum_{b\in\mathbb{Z}_q}\sum_{j\in\mathbb{Z}} \rho_{1/r}\left(j + (\langle\widehat{\mathbf{a}},\mathbf{s}_0\rangle + b)\cdot\frac{1}{q}\right)|b\rangle \approx \sum_{e\in\mathbb{Z}} \rho_{1/r}\left(e\cdot\frac{1}{q}\right)\left|\langle -\widehat{\mathbf{a}},\mathbf{s}_0\rangle + e \bmod q\right\rangle.$$

Open questions

- The Gaussian distribution is heavily used in current reduction.



- Problem 1. Use other distributions to get *new* hardness for LWE variants.

O. Regev. Quantum computation and lattice problems. FOCS'02.
O. Regev. On lattices, learning with errors, random linear codes, and cryptography. STOC'05.
V. Lyubashevsky and D. Micciancio. On bounded distance decoding, unique shortest vectors, and the minimum distance problem, CRYPTO'09.
A. M. Childs and W. van Dam. Quantum algorithm for a generalized hidden shift problem. SODA'07.

Open questions

- Hardness of EDCP varies with both shifts and samples number.
  - EDCP with more samples number m: $2^{O\left(\frac{\log N}{\log m}+\log m\right)}$ by Kuperberg's algorithm [Ku05].
  - EDCP with more shifts number M: $2^{O\left(\frac{\log N}{(\log M)^2}\right)}$ by reducing to LWE.

$$\mathrm{EDCP}^{m}_{N,M} \leq \mathrm{EDCP}^{m'}_{N,M'}?$$
$$M < M' \;\&\; m > m'$$

- Problem 2. Trade samples for shifts? Is DCP $\leq$ EDCP?

G. Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. SIAM J. Comput., 2005.