A quasi-poly. time quantum algorithm for EDCP over power-of-two moduli

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

Motivation

Motivation

- [R05] Cryptographic schemes rely on the hardness of LWE.

Motivation

- [R05] Cryptographic schemes rely on the hardness of LWE.
- Goal: understand the (quantum) complexity of solving these problems:

Motivation

- [R05] Cryptographic schemes rely on the hardness of LWE.
- Goal: understand the (quantum) complexity of solving these problems:
  - Use lattice reduction techniques to assess the underlying assumptions.

Motivation

- [R05] Cryptographic schemes rely on the hardness of LWE.
- Goal: understand the (quantum) complexity of solving these problems:
  - Use lattice reduction techniques to assess the underlying assumptions.
  - [R02,R07] Reduce to well-studied quantum problems, e.g., the Dihedral Coset Problem (DCP) or Hidden Subgroup problem.

Motivation

- [R05] Cryptographic schemes rely on the hardness of LWE.
- Goal: understand the (quantum) complexity of solving these problems:
  - Use lattice reduction techniques to assess the underlying assumptions.
  - [R02,R07] Reduce to well-studied quantum problems, e.g., the Dihedral Coset Problem (DCP) or Hidden Subgroup problem.
  - [BKSW18] LWE and EDCP (Extrapolated Dihedral Coset Problem) are equivalent (under certain parameters).

Motivation

- [R05] Cryptographic schemes rely on the hardness of LWE.
- Goal: understand the (quantum) complexity of solving these problems:
  - Use lattice reduction techniques to assess the underlying assumptions.
  - [R02,R07] Reduce to well-studied quantum problems, e.g., the Dihedral Coset Problem (DCP) or Hidden Subgroup problem.
  - [BKSW18] LWE and EDCP (Extrapolated Dihedral Coset Problem) are equivalent (under certain parameters).

Motivation

- [R05] Cryptographic schemes rely on the hardness of LWE.
- Goal: understand the (quantum) complexity of solving these problems:
  - Use lattice reduction techniques to assess the underlying assumptions.
  - [R02,R07] Reduce to well-studied quantum problems, e.g., the Dihedral Coset Problem (DCP) or Hidden Subgroup problem.
  - [BKSW18] LWE and EDCP (Extrapolated Dihedral Coset Problem) are equivalent (under certain parameters).

Complexity of EDCP?

This talk

This talk

- A quasi-polynomial time/sample quantum algorithm for EDCP

Learning with Errors (LWE)

(Search) $\mathsf{LWE}_{n,q,\alpha}$

Find a fixed secret $\mathbf{s} \in \mathbb{Z}_q^n$, given $\mathbf{a}_i \leftarrow\!\!\$\ \mathbb{Z}_q^n$ and $e_i \leftarrow\!\!\$\ \mathcal{D}$

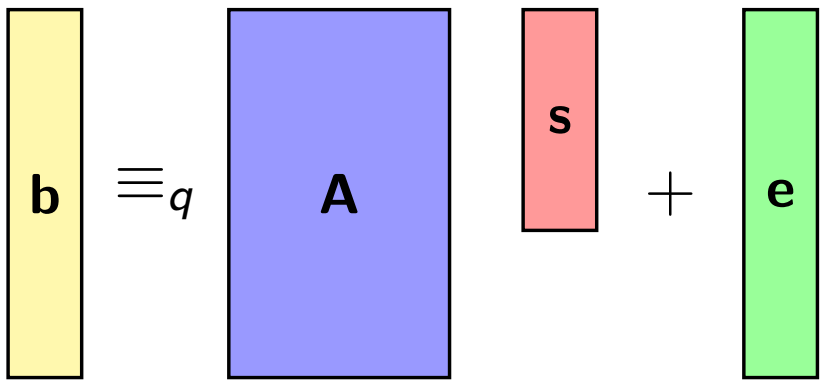
$$
\begin{aligned}
\mathbf{a}_1, b_1 &= \langle \mathbf{a}_1, \mathbf{s} \rangle + e_1 \pmod q \\
\mathbf{a}_2, b_2 &= \langle \mathbf{a}_2, \mathbf{s} \rangle + e_2 \pmod q \\
&\vdots \\
\mathbf{a}_m, b_m &= \langle \mathbf{a}_m, \mathbf{s} \rangle + e_m \pmod q
\end{aligned}
$$

Typically, $\mathcal{D} = D_{\alpha q}$

Learning with Errors (LWE)

(Search) $\mathrm{LWE}_{n,q,\alpha}$

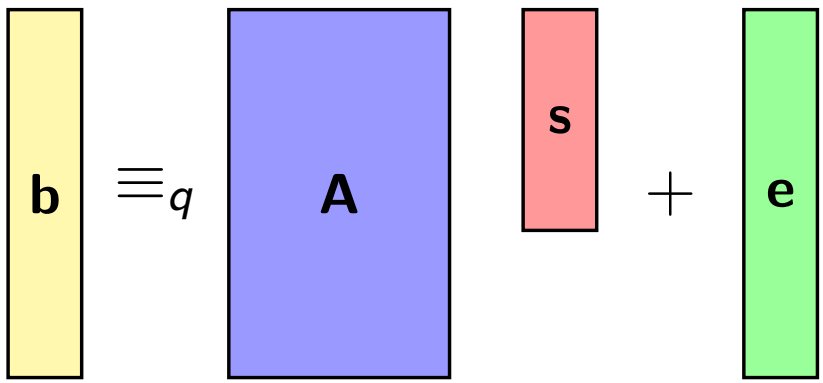
Find $\mathbf{s} \in \mathbb{Z}_q^n$, given $\mathbf{a}_i \leftarrow\!\!\$\ \mathbb{Z}_q^n$ and $e_i \leftarrow\!\!\$\ \mathcal{D}$



Learning with Errors (LWE)

(Search) $\mathrm{LWE}_{n,q,\alpha}$

Find $\mathbf{s} \in \mathbb{Z}_q^n$, given $\mathbf{a}_i \leftarrow\!\$\ \mathbb{Z}_q^n$ and $e_i \leftarrow\!\$\ \mathcal{D}$

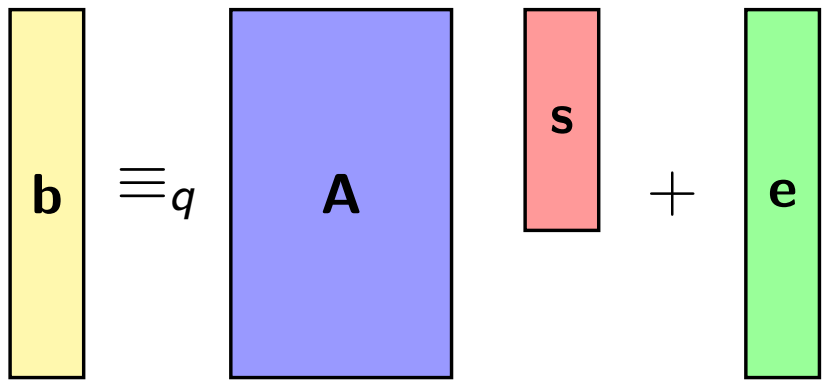


- Hardness of LWE depends on noise-to-modulus ratio $\alpha = \frac{\sigma}{q}$. The smaller α, the easier the LWE problem.

Learning with Errors (LWE)

(Search) $\mathrm{LWE}_{n,q,\alpha}$

Find $\mathbf{s} \in \mathbb{Z}_q^n$, given $\mathbf{a}_i \leftarrow\$\ \mathbb{Z}_q^n$ and $e_i \leftarrow\$\ \mathcal{D}$



- Hardness of LWE depends on noise-to-modulus ratio $\alpha = \frac{\sigma}{q}$. The smaller α, the easier the LWE problem.
- Standard LWE: $q = \mathrm{poly}(n)$, $m = n \log q$, $\chi = D_{\mathbb{Z},\alpha q}$ and $\alpha q = O(\sqrt{n})$.

Complexity: exponential

DCP vs EDCP

Find a secret s, given ℓ quantum samples

$\mathbf{DCP}_N^\ell$	$\mathbf{EDCP}_{n,q,\chi}^\ell$
$\lvert 0, x_i\rangle + \lvert 1, x_i + s \bmod N\rangle$	$\sum_{j \in \mathrm{Supp}(\mathcal{D})} \mathcal{D}(j) \lvert j\rangle \lvert \mathbf{x}_i + j \cdot \mathbf{s} \bmod q\rangle$

Most common distributions

DCP vs EDCP

Find a secret s, given ℓ quantum samples

$\mathbf{DCP}_N^\ell$	$\mathbf{EDCP}_{n,q,\chi}^\ell$
$\lvert 0, x_i\rangle + \lvert 1, x_i + s \bmod N\rangle$	$\sum_{j \in \mathrm{Supp}(\mathcal{D})} \mathcal{D}(j) \lvert j\rangle \lvert \mathbf{x}_i + j \cdot \mathbf{s} \bmod q\rangle$

Most common distributions

- G-EDCP: $\mathcal{D}$ is a Gaussian distribution

DCP vs EDCP

Find a secret s, given ℓ quantum samples

$\mathbf{DCP}_N^\ell$ $\qquad\qquad$ $\mathbf{EDCP}_{n,q,\chi}^\ell$

$|0, x_i\rangle + |1, x_i + s \bmod N\rangle$ $\qquad$ $\sum_{j \in \mathrm{Supp}(\mathcal{D})} \mathcal{D}(j)\,|j\rangle\,|\mathbf{x}_i + j \cdot \mathbf{s} \bmod q\rangle$

Most common distributions

- G-EDCP: $\mathcal{D}$ is a Gaussian distribution
- U-EDCP$_{n,q,M}$: $\sum_{j=0}^{M-1} |j\rangle\,|\mathbf{x}_i + j \cdot \mathbf{s} \bmod q\rangle$

$\Rightarrow n = 1, M = 2$: DCP instances.

$$\text{G-EDCP} \underset{\text{[BKSW18]}}{\overset{\text{comp}}{\Longleftrightarrow}} \text{U-EDCP}$$

Recall Relation between LWE, DCP and EDCP

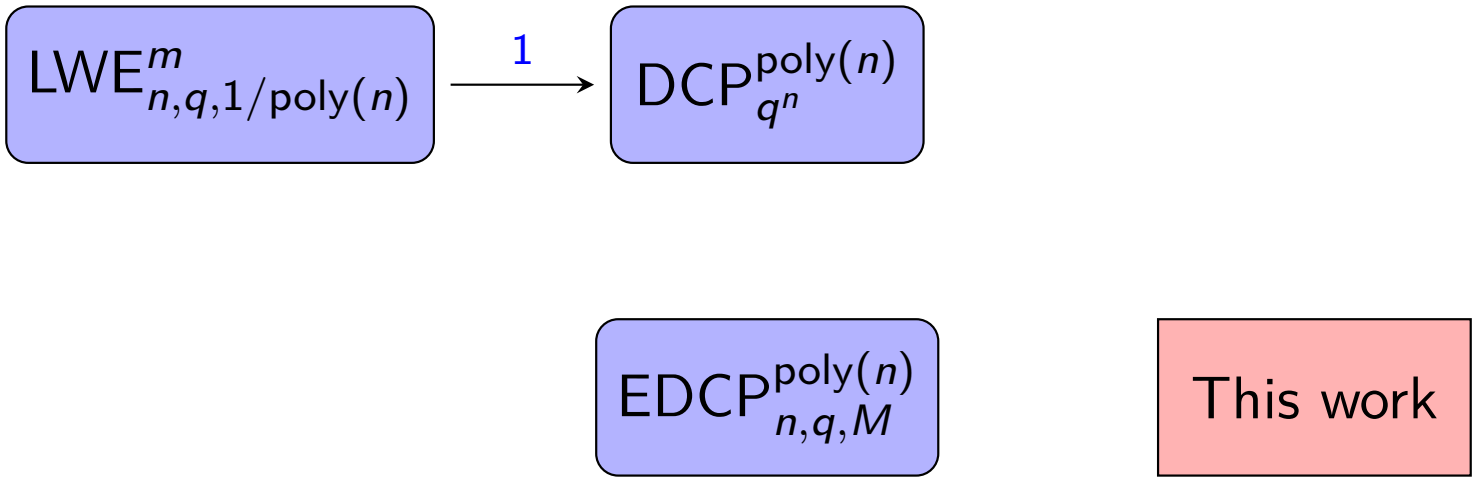
$\mathsf{LWE}^{m}_{n,q,1/\mathsf{poly}(n)}$

$\mathsf{DCP}^{\mathsf{poly}(n)}_{q^n}$

$\mathsf{EDCP}^{\mathsf{poly}(n)}_{n,q,M}$

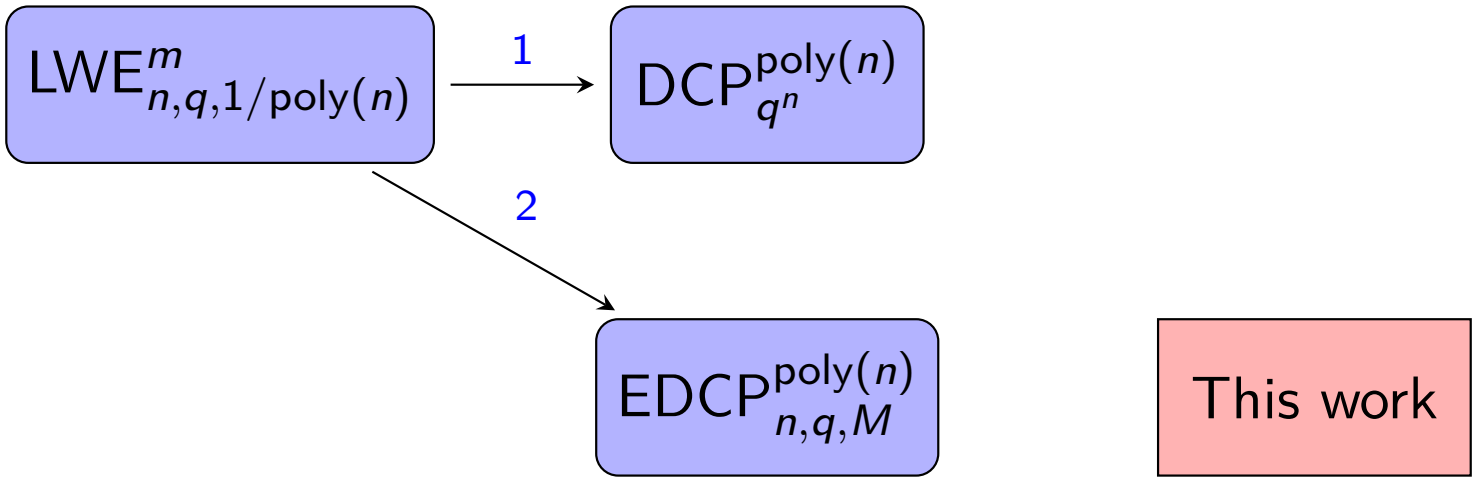
This work

Recall Relation between LWE, DCP and EDCP



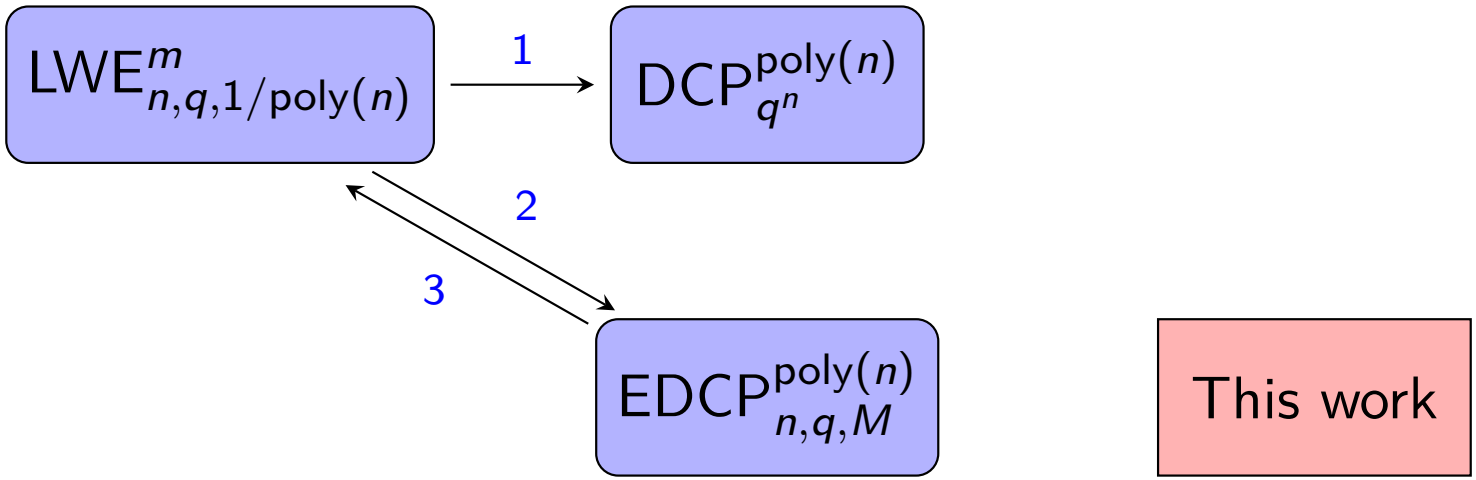
1. [R02,R07] $\mathsf{LWE}^{m}_{n,q,1/\mathrm{poly}(n)} \leq \mathsf{DCP}^{\mathrm{poly}(n)}_{q^n}$.

Recall Relation between LWE, DCP and EDCP



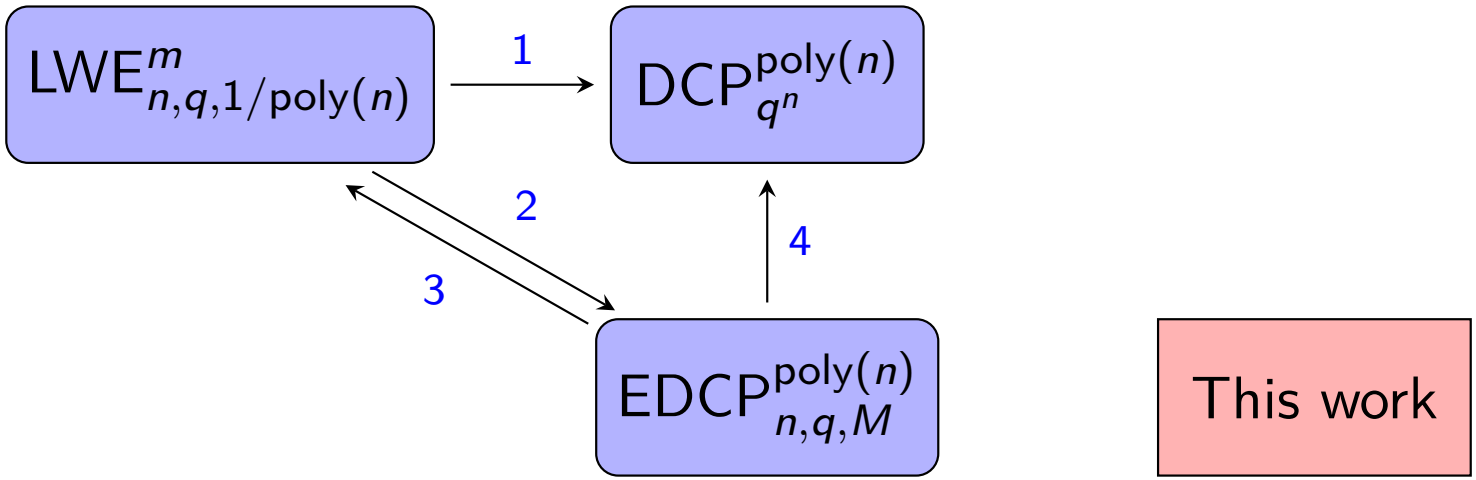
1. [R02,R07] $\mathsf{LWE}^{m}_{n,q,1/\mathrm{poly}(n)} \leq \mathsf{DCP}^{\mathrm{poly}(n)}_{q^n}$.
2. [BKSW18] $\mathsf{LWE}^{\Omega(n\log q)}_{n,q,\alpha} \leq \mathsf{EDCP}^{\ell}_{n,q,M}$ where $M \cdot \ell \approx 1/(\alpha \cdot n\log q)$.

Recall Relation between LWE, DCP and EDCP



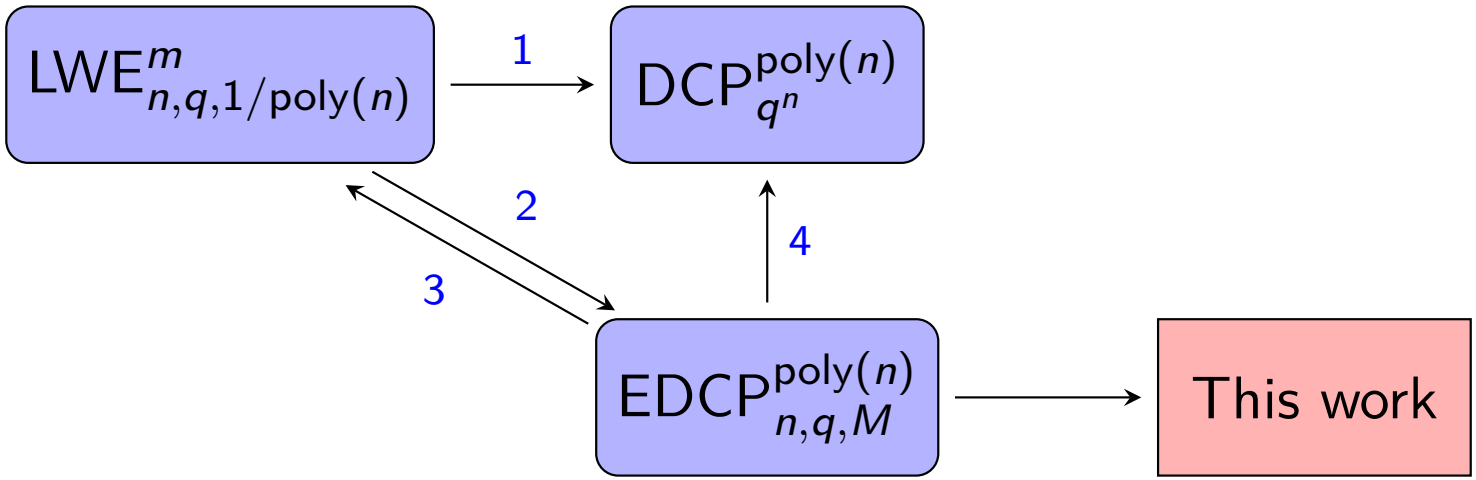
1. [R02,R07] $\mathsf{LWE}^{m}_{n,q,1/\mathrm{poly}(n)} \leq \mathsf{DCP}^{\mathrm{poly}(n)}_{q^n}$.
2. [BKSW18] $\mathsf{LWE}^{\Omega(n\log q)}_{n,q,\alpha} \leq \mathsf{EDCP}^{\ell}_{n,q,M}$ where $M \cdot \ell \approx 1/(\alpha \cdot n\log q)$.
3. [BKSW18] $\mathsf{EDCP}^{\ell}_{n,q,M} \leq \mathsf{LWE}^{\ell}_{n,q,\alpha}$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

Recall Relation between LWE, DCP and EDCP



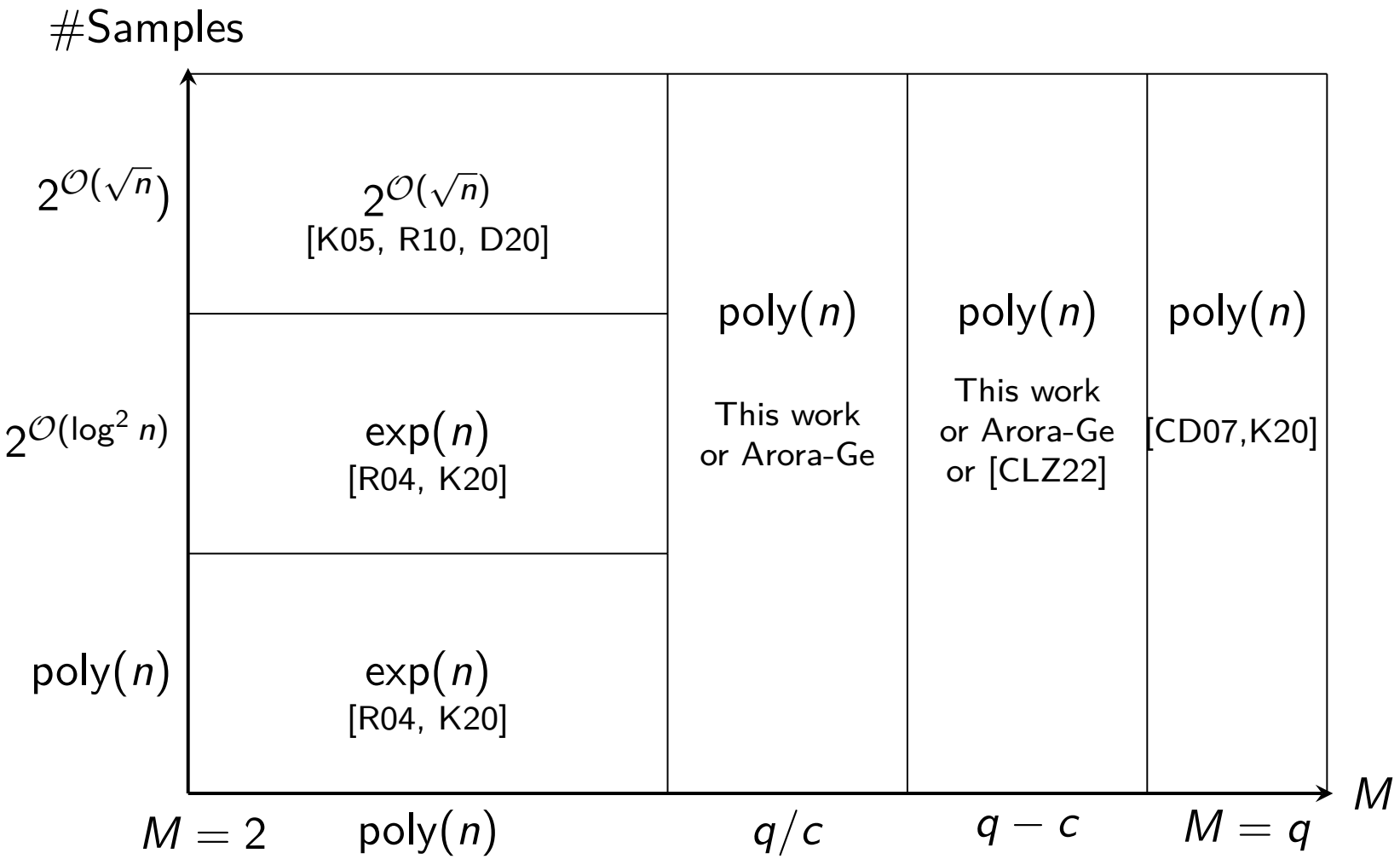
1. [R02,R07] $\mathsf{LWE}^{m}_{n,q,1/\mathsf{poly}(n)} \leq \mathsf{DCP}^{\mathsf{poly}(n)}_{q^n}$.
2. [BKSW18] $\mathsf{LWE}^{\Omega(n \log q)}_{n,q,\alpha} \leq \mathsf{EDCP}^{\ell}_{n,q,M}$ where $M \cdot \ell \approx 1/(\alpha \cdot n \log q)$.
3. [BKSW18] $\mathsf{EDCP}^{\ell}_{n,q,M} \leq \mathsf{LWE}^{\ell}_{n,q,\alpha}$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

Recall Relation between LWE, DCP and EDCP

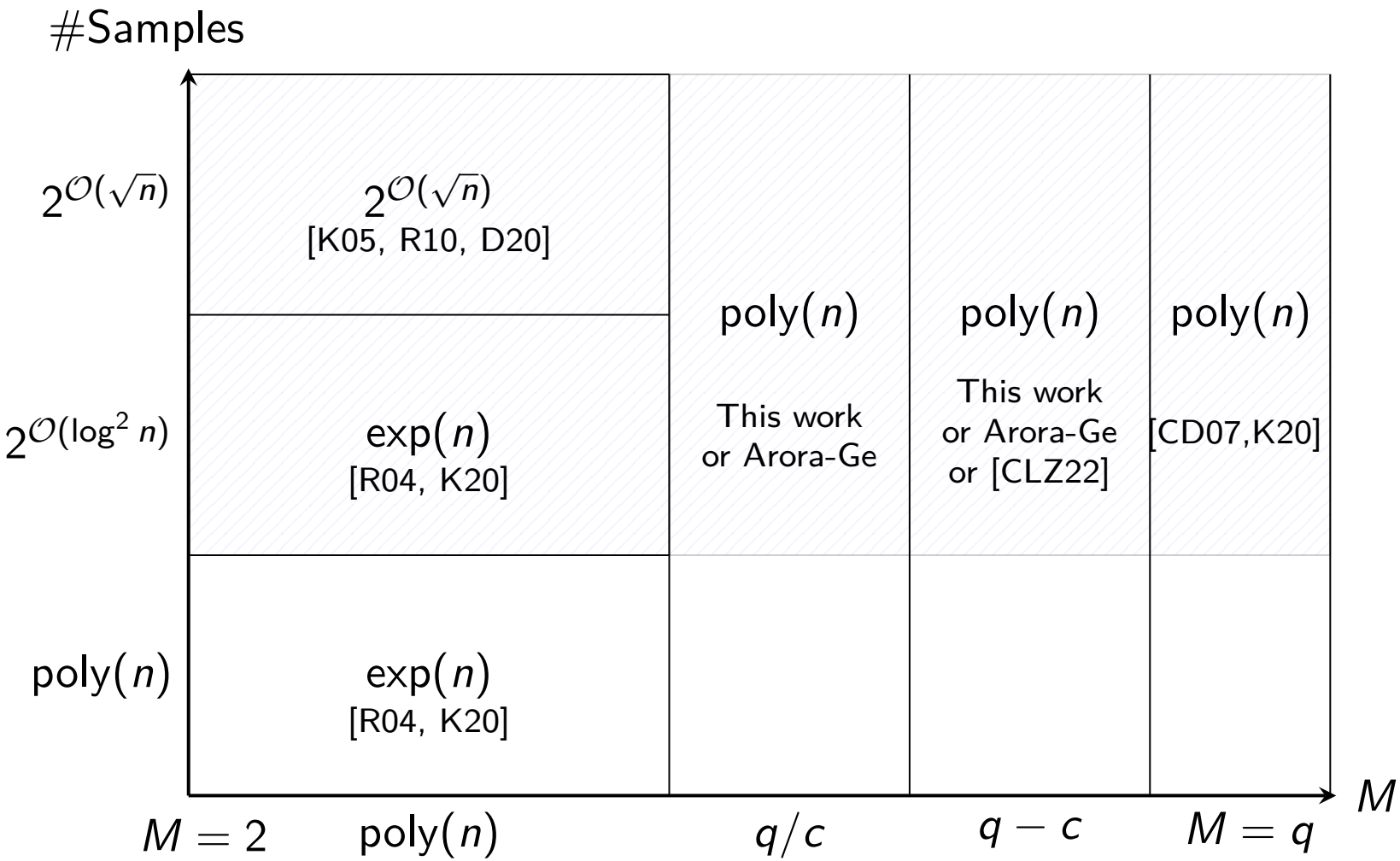


1. [R02,R07] $\mathsf{LWE}^{m}_{n,q,1/\mathsf{poly}(n)} \leq \mathsf{DCP}^{\mathsf{poly}(n)}_{q^n}$.
2. [BKSW18] $\mathsf{LWE}^{\Omega(n \log q)}_{n,q,\alpha} \leq \mathsf{EDCP}^{\ell}_{n,q,M}$ where $M \cdot \ell \approx 1/(\alpha \cdot n \log q)$.
3. [BKSW18] $\mathsf{EDCP}^{\ell}_{n,q,M} \leq \mathsf{LWE}^{\ell}_{n,q,\alpha}$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

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

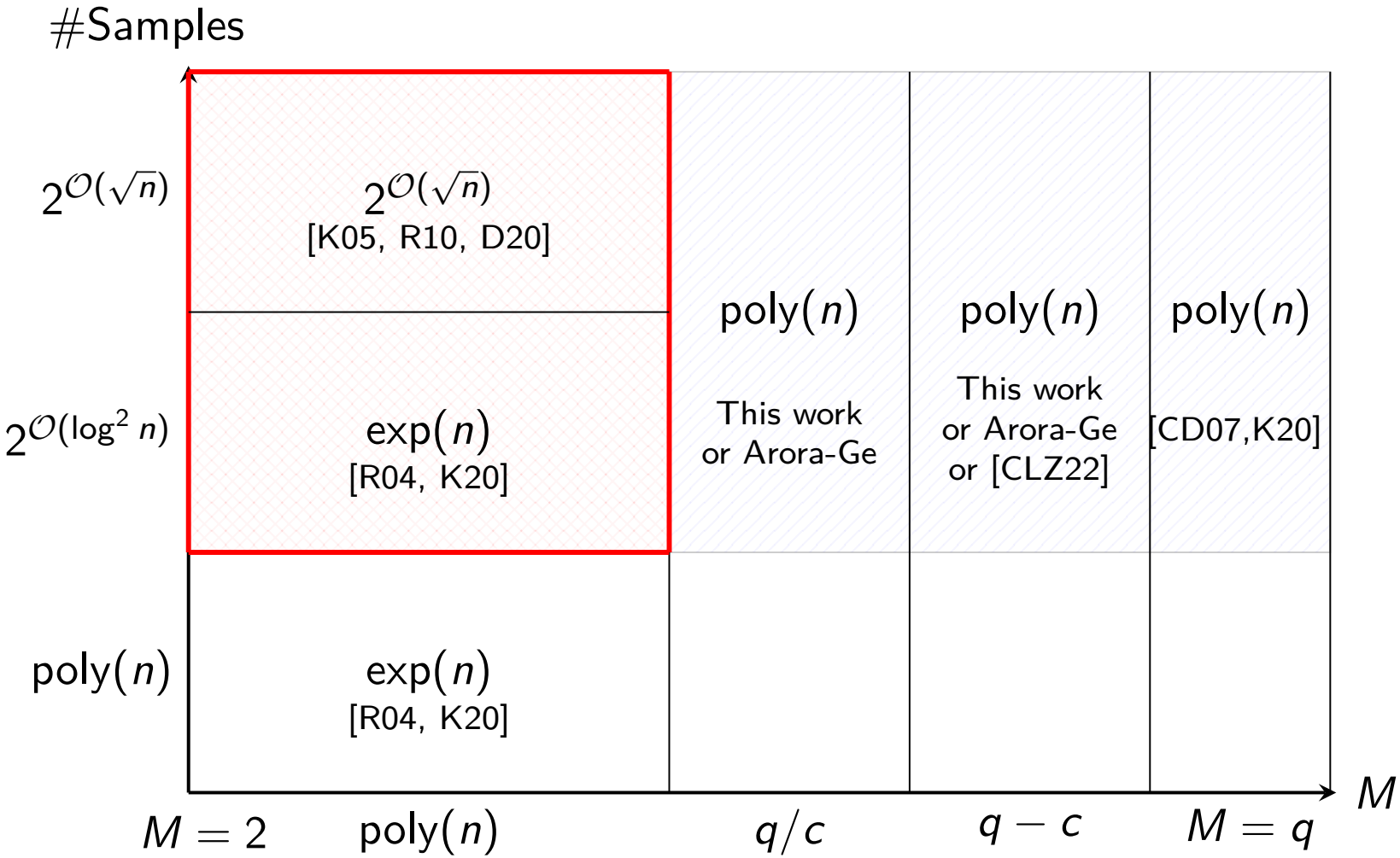


Our result for U-EDCP$_{n,q,M}$



Our algorithm applies

Our result for U-EDCP$_{n,q,M}$



Our algorithm applies

Improve state-of-the-art for power-of-two modulus q: $n^{\mathcal{O}(\log q)}$

Our Algorithm

Recall: Kuperberg's idea to solve DCP

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

Recall: Kuperberg's idea to solve DCP

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

(1) Given state $|\phi_i\rangle = |0, x_i\rangle + |1, x_i + s \bmod N\rangle$

Recall: Kuperberg's idea to solve DCP

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

(1) Given state $|\phi_i\rangle = |0, x_i\rangle + |1, x_i + s \bmod N\rangle$

(2) Apply QFT over $\mathbb{Z}_N$ and Measure y $|\psi_y\rangle := |0\rangle + \omega_N^{ys}\,|1\rangle$

Recall: Kuperberg's idea to solve DCP

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

(1) Given state $|\phi_i\rangle = |0, x_i\rangle + |1, x_i + s \bmod N\rangle$

(2) Apply QFT over $\mathbb{Z}_N$ and Measure y $|\psi_y\rangle := |0\rangle + \omega_N^{ys} |1\rangle$

Main Idea: Combine $|\psi_{y_i}\rangle = |0\rangle + \omega_N^{y_i s} |1\rangle$ samples, and construct a state:

$$|\psi_{N/2}\rangle := |0\rangle + (-1)^s |1\rangle$$

we recover one bit of s by measuring in the Hadamard basis.

Recall: Kuperberg's idea to solve DCP

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

(1) Given state $|\phi_i\rangle = |0, x_i\rangle + |1, x_i + s \bmod N\rangle$

(2) Apply QFT over $\mathbb{Z}_N$ and Measure y $|\psi_y\rangle := |0\rangle + \omega_N^{ys} |1\rangle$

Main Idea: Combine $|\psi_{y_i}\rangle = |0\rangle + \omega_N^{y_i s} |1\rangle$ samples, and construct a state:

$$|\psi_{N/2}\rangle := |0\rangle + (-1)^s |1\rangle$$

we recover one bit of s by measuring in the Hadamard basis.

Kuperberg's algorithm [K05]

Solves DCP_N^ℓ in time $2^{O(\sqrt{\log_2 N})}$ when $\ell = 2^{O(\sqrt{\log_2 N})}$.

This work – Outline

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

Kuperberg-like algorithm	This work

This work – Outline

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

Kuperberg-like algorithm	This work
U-EDCP$_{1,q,2}$	U-EDCP$_{n,q,2}$

This work – Outline

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

Kuperberg-like algorithm	This work
U-EDCP$_{1,q,2}$	U-EDCP$_{n,q,2}$
Prepare many "coset" samples	

This work – Outline

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

Kuperberg-like algorithm	This work
U-EDCP$_{1,q,2}$	U-EDCP$_{n,q,2}$
Prepare many "coset" samples	
$\lvert 0, x_i \bmod q\rangle + \lvert 1, x_i + s \bmod q\rangle$	

This work – Outline

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

Kuperberg-like algorithm	This work
$\text{U-EDCP}_{1,q,2}$	$\text{U-EDCP}_{n,q,2}$
Prepare many "coset" samples	
$\lvert 0, x_i \bmod q\rangle + \lvert 1, x_i + s \bmod q\rangle$	$\lvert 0, \mathbf{x}_i \bmod q\rangle + \lvert 1, \mathbf{x}_i + \mathbf{s} \bmod q\rangle$

This work – Outline

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

Kuperberg-like algorithm	This work
U-EDCP$_{1,q,2}$	U-EDCP$_{n,q,2}$
Prepare many "coset" samples	
$\lvert 0, x_i \bmod q\rangle + \lvert 1, x_i + s \bmod q\rangle$	$\lvert 0, \mathbf{x}_i \bmod q\rangle + \lvert 1, \mathbf{x}_i + \mathbf{s} \bmod q\rangle$
Construct many "phase" samples	

This work – Outline

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

Kuperberg-like algorithm	This work
U-EDCP$_{1,q,2}$	U-EDCP$_{n,q,2}$
Prepare many "coset" samples	
$\lvert 0, x_i \bmod q\rangle + \lvert 1, x_i + s \bmod q\rangle$	$\lvert 0, \mathbf{x}_i \bmod q\rangle + \lvert 1, \mathbf{x}_i + \mathbf{s} \bmod q\rangle$
Construct many "phase" samples	
$(y, \lvert\psi_y\rangle := \lvert 0\rangle + \omega_q^{ys} \lvert 1\rangle)$	

This work – Outline

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

Kuperberg-like algorithm	This work
$\text{U-EDCP}_{1,q,2}$	$\text{U-EDCP}_{n,q,2}$
Prepare many "coset" samples	
$\lvert 0, x_i \bmod q\rangle + \lvert 1, x_i + s \bmod q\rangle$	$\lvert 0, \mathbf{x}_i \bmod q\rangle + \lvert 1, \mathbf{x}_i + \mathbf{s} \bmod q\rangle$
Construct many "phase" samples	
$(y, \lvert\psi_y\rangle := \lvert 0\rangle + \omega_q^{ys} \lvert 1\rangle)$	$(\mathbf{y}, \lvert\psi_{\mathbf{y}}\rangle := \lvert 0\rangle + \omega_q^{\langle \mathbf{y}, \mathbf{s}\rangle} \lvert 1\rangle)$
	$\overline{\text{U-EDCP}}$

This work – Outline

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

Kuperberg-like algorithm	This work
U-EDCP$_{1,q,2}$	U-EDCP$_{n,q,2}$
Prepare many "coset" samples	
$\lvert 0, x_i \bmod q\rangle + \lvert 1, x_i + s \bmod q\rangle$	$\lvert 0, \mathbf{x}_i \bmod q\rangle + \lvert 1, \mathbf{x}_i + \mathbf{s} \bmod q\rangle$
Construct many "phase" samples	
$(y, \lvert\psi_y\rangle := \lvert 0\rangle + \omega_q^{ys} \lvert 1\rangle)$	$(\mathbf{y}, \lvert\psi_{\mathbf{y}}\rangle := \lvert 0\rangle + \omega_q^{\langle \mathbf{y}, \mathbf{s}\rangle} \lvert 1\rangle)$ U-EDCP
Merge samples	

This work – Outline

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

Kuperberg-like algorithm	This work
U-EDCP$_{1,q,2}$	U-EDCP$_{n,q,2}$
Prepare many "coset" samples	
$\lvert 0, x_i \bmod q\rangle + \lvert 1, x_i + s \bmod q\rangle$	$\lvert 0, \mathbf{x}_i \bmod q\rangle + \lvert 1, \mathbf{x}_i + \mathbf{s} \bmod q\rangle$
Construct many "phase" samples	
$(y, \lvert\psi_y\rangle := \lvert 0\rangle + \omega_q^{ys} \lvert 1\rangle)$	$(\mathbf{y}, \lvert\psi_{\mathbf{y}}\rangle := \lvert 0\rangle + \omega_q^{\langle \mathbf{y}, \mathbf{s}\rangle} \lvert 1\rangle)$ U-EDCP
Merge samples	
$\lvert 0\rangle + \omega_q^{(y_i \pm y_j)s} \lvert 1\rangle$	

This work – Outline

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

Kuperberg-like algorithm	This work
U-EDCP$_{1,q,2}$	U-EDCP$_{n,q,2}$
Prepare many "coset" samples	
$\lvert 0, x_i \bmod q\rangle + \lvert 1, x_i + s \bmod q\rangle$	$\lvert 0, \mathbf{x}_i \bmod q\rangle + \lvert 1, \mathbf{x}_i + \mathbf{s} \bmod q\rangle$
Construct many "phase" samples	
$(y, \lvert\psi_y\rangle := \lvert 0\rangle + \omega_q^{ys} \lvert 1\rangle)$	$(\mathbf{y}, \lvert\psi_{\mathbf{y}}\rangle := \lvert 0\rangle + \omega_q^{\langle \mathbf{y}, \mathbf{s}\rangle} \lvert 1\rangle)$ U-EDCP
Merge samples	
$\lvert 0\rangle + \omega_q^{(y_i \pm y_j)s} \lvert 1\rangle$	$\sum_{\mathbf{j} \in \mathbb{Z}_2^{n+1} : \mathbf{Y}\cdot\mathbf{j} = \mathbf{b} \bmod 2} \omega_q^{\langle \mathbf{Y}\cdot\mathbf{j}, \mathbf{s}\rangle} \lvert \mathbf{j}\rangle$

This work – Outline

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

Kuperberg-like algorithm	This work
U-EDCP$_{1,q,2}$	U-EDCP$_{n,q,2}$
Prepare many "coset" samples	
$\lvert 0, x_i \bmod q\rangle + \lvert 1, x_i + s \bmod q\rangle$	$\lvert 0, \mathbf{x}_i \bmod q\rangle + \lvert 1, \mathbf{x}_i + \mathbf{s} \bmod q\rangle$
Construct many "phase" samples	
$(y, \lvert\psi_y\rangle := \lvert 0\rangle + \omega_q^{ys} \lvert 1\rangle)$	$(\mathbf{y}, \lvert\psi_{\mathbf{y}}\rangle := \lvert 0\rangle + \omega_q^{\langle \mathbf{y}, \mathbf{s}\rangle} \lvert 1\rangle)$ U-EDCP
Merge samples	
$\lvert 0\rangle + \omega_q^{(y_i \pm y_j)s} \lvert 1\rangle$	$\sum_{\mathbf{j} \in \mathbb{Z}_2^{n+1}:\, \mathbf{Y}\cdot\mathbf{j} = \mathbf{b} \bmod 2} \omega_q^{\langle \mathbf{Y}\cdot\mathbf{j}, \mathbf{s}\rangle} \lvert \mathbf{j}\rangle$
Recover bits	

This work – Outline

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

Kuperberg-like algorithm	This work
U-EDCP$_{1,q,2}$	U-EDCP$_{n,q,2}$
Prepare many "coset" samples	
$\lvert 0, x_i \bmod q\rangle + \lvert 1, x_i + s \bmod q\rangle$	$\lvert 0, \mathbf{x}_i \bmod q\rangle + \lvert 1, \mathbf{x}_i + \mathbf{s} \bmod q\rangle$
Construct many "phase" samples	
$(y, \lvert\psi_y\rangle := \lvert 0\rangle + \omega_q^{ys} \lvert 1\rangle)$	$(\mathbf{y}, \lvert\psi_{\mathbf{y}}\rangle := \lvert 0\rangle + \omega_q^{\langle \mathbf{y}, \mathbf{s}\rangle} \lvert 1\rangle)$ U-EDCP
Merge samples	
$\lvert 0\rangle + \omega_q^{(y_i \pm y_j)s} \lvert 1\rangle$	$\sum_{\mathbf{j} \in \mathbb{Z}_2^{n+1}:\, \mathbf{Y}\cdot\mathbf{j} = \mathbf{b} \bmod 2} \omega_q^{\langle \mathbf{Y}\cdot\mathbf{j}, \mathbf{s}\rangle} \lvert \mathbf{j}\rangle$
Recover bits	
1 LSB bit	

This work – Outline

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

Kuperberg-like algorithm	This work
U-EDCP$_{1,q,2}$	U-EDCP$_{n,q,2}$
Prepare many "coset" samples	
$\lvert 0, x_i \bmod q\rangle + \lvert 1, x_i + s \bmod q\rangle$	$\lvert 0, \mathbf{x}_i \bmod q\rangle + \lvert 1, \mathbf{x}_i + \mathbf{s} \bmod q\rangle$
Construct many "phase" samples	
$(y, \lvert\psi_y\rangle := \lvert 0\rangle + \omega_q^{ys} \lvert 1\rangle)$	$(\mathbf{y}, \lvert\psi_{\mathbf{y}}\rangle := \lvert 0\rangle + \omega_q^{\langle \mathbf{y}, \mathbf{s}\rangle} \lvert 1\rangle)$ U-EDCP
Merge samples	
$\lvert 0\rangle + \omega_q^{(y_i \pm y_j)s} \lvert 1\rangle$	$\sum_{\mathbf{j} \in \mathbb{Z}_2^{n+1}:\, \mathbf{Y}\cdot\mathbf{j} = \mathbf{b} \bmod 2} \omega_q^{\langle \mathbf{Y}\cdot\mathbf{j}, \mathbf{s}\rangle} \lvert \mathbf{j}\rangle$
Recover bits	
1 LSB bit	n LSB bits

This work – Main step

Base case: $M = 2$

Merge $n+1$ $\overline{\text{U-EDCP}}_q$ to get one $\overline{\text{U-EDCP}}_{q/2}$.

$$\overline{\text{U-EDCP}}^{n+1}_{n,q,2} \rightarrow \overline{\text{U-EDCP}}^{1}_{n,q/2,2}$$

Merge $n+1$ $\overline{\text{U-EDCP}}_q$ to get one $\overline{\text{U-EDCP}}_{q/2}$.

$$\overline{\text{U-EDCP}}^{n+1}_{n,q,2} \to \overline{\text{U-EDCP}}^{1}_{n,q/2,2}$$

1. Tensor input states:

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

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

Merge $n+1$ $\overline{\text{U-EDCP}}_q$ to get one $\overline{\text{U-EDCP}}_{q/2}$.

$$\overline{\text{U-EDCP}}^{n+1}_{n,q,2} \to \overline{\text{U-EDCP}}^{1}_{n,q/2,2}$$

1. Tensor input states:

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

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

2. Compute $\mathbf{Y} \cdot \mathbf{j} \bmod 2$ in a new register and measure to get some $\mathbf{b} \in \mathbb{Z}_2^n$:

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

3. Recall $\mathbf{y}_k$ is uniform in $\mathbb{Z}_q^n$. So $\mathbf{Y} \pmod 2 \in \mathbb{Z}_2^{n \times (n+1)}$ has full rank with constant probability:

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

3. Recall $\mathbf{y}_k$ is uniform in $\mathbb{Z}_q^n$. So $\mathbf{Y} \pmod 2 \in \mathbb{Z}_2^{n\times(n+1)}$ has full rank with constant probability:

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

4. We have

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

3. Recall $\mathbf{y}_k$ is uniform in $\mathbb{Z}_q^n$. So $\mathbf{Y} \pmod 2 \in \mathbb{Z}_2^{n\times(n+1)}$ has full rank with constant probability:

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

4. We have

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

5. Since $\mathbf{Y}(\mathbf{j}_1 - \mathbf{j}_0) = 0 \bmod 2$, we have

$$|0\rangle + \omega_{q/2}^{\langle \mathbf{y}',\, \mathbf{s}\rangle} |1\rangle$$

where $2\mathbf{y}' = \mathbf{Y}(\mathbf{j}_1 - \mathbf{j}_0) \bmod q$.

3. Recall $\mathbf{y}_k$ is uniform in $\mathbb{Z}_q^n$. So $\mathbf{Y} \pmod 2 \in \mathbb{Z}_2^{n\times(n+1)}$ has full rank with constant probability:

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

4. We have

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

5. Since $\mathbf{Y}(\mathbf{j}_1 - \mathbf{j}_0) = 0 \bmod 2$, we have

$$|0\rangle + \omega_{q/2}^{\langle \mathbf{y}',\, \mathbf{s}\rangle} |1\rangle$$

where $2\mathbf{y}' = \mathbf{Y}(\mathbf{j}_1 - \mathbf{j}_0) \bmod q$.

This work – Recover n bits

$M = 2$, $\ell = n^{O(\log q)} = 2^{O(\log^2 n)}$

This work – Recover n bits

$M = 2$, $\ell = n^{O(\log q)} = 2^{O(\log^2 n)}$

$$\overline{\text{U-EDCP}}^{\ell}_{n,q,2} \rightarrow \overline{\text{U-EDCP}}^{\ell/(n+1)}_{n,q/2,2} \rightarrow \cdots \rightarrow \overline{\text{U-EDCP}}^{n}_{n,2,2}$$

This work – Recover n bits

$M = 2$, $\ell = n^{O(\log q)} = 2^{O(\log^2 n)}$

$$\overline{\text{U-EDCP}}^{\ell}_{n,q,2} \to \overline{\text{U-EDCP}}^{\ell/(n+1)}_{n,q/2,2} \to \cdots \to \overline{\text{U-EDCP}}^{n}_{n,2,2}$$

- Final Stage: we get n $\overline{\text{U-EDCP}}_{n,2,2}$ samples with known $\{\mathbf{y}_k\}_k$:

$$\left\{|0\rangle + (-1)^{\langle \mathbf{y}_k, \mathbf{s}\rangle} |1\rangle\right\}_{k=1}^{n}.$$

This work – Recover n bits

$M = 2$, $\ell = n^{O(\log q)} = 2^{O(\log^2 n)}$

$$\overline{\text{U-EDCP}}^{\ell}_{n,q,2} \to \overline{\text{U-EDCP}}^{\ell/(n+1)}_{n,q/2,2} \to \cdots \to \overline{\text{U-EDCP}}^{n}_{n,2,2}$$

- Final Stage: we get n $\overline{\text{U-EDCP}}_{n,2,2}$ samples with known $\{\mathbf{y}_k\}_k$:

$$\left\{|0\rangle + (-1)^{\langle \mathbf{y}_k, \mathbf{s}\rangle} |1\rangle\right\}_{k=1}^{n}.$$

- Measure each in Hadamard basis to learn $\langle \mathbf{y}_k, \mathbf{s}\rangle$ mod 2.

This work – Recover n bits

$M = 2$, $\ell = n^{O(\log q)} = 2^{O(\log^2 n)}$

$$\overline{\text{U-EDCP}}^{\ell}_{n,q,2} \to \overline{\text{U-EDCP}}^{\ell/(n+1)}_{n,q/2,2} \to \cdots \to \overline{\text{U-EDCP}}^{n}_{n,2,2}$$

- Final Stage: we get n $\overline{\text{U-EDCP}}_{n,2,2}$ samples with known $\{\mathbf{y}_k\}_k$:

$$\left\{|0\rangle + (-1)^{\langle \mathbf{y}_k, \mathbf{s}\rangle} |1\rangle\right\}_{k=1}^{n}.$$

- Measure each in Hadamard basis to learn $\langle \mathbf{y}_k, \mathbf{s}\rangle \bmod 2$.
- Use Gaussian elimination to recover $\bar{\mathbf{s}} := \mathbf{s} \bmod 2$.

The algorithm works for $M = 2$. What about general M?

Lemma (U-EDCP self-reduction) [D20]

Let $M' \leq M$. There is a polynomial time reduction from $\text{U-EDCP}^{\ell}_{n,q,M}$ to $\text{U-EDCP}^{\Theta(\ell)}_{n,q,M'}$ that succeeds with constant probability.

Main theorem

Let $q = \text{poly}(n)$ be a power of two, $2 \leq M \leq q$. There is an algorithm that solves $\text{U-EDCP}^{\ell}_{n,q,M}$ in time $2^{O(\log n \log q)} = 2^{O(\log^2 n)}$ using $\ell = 2^{O(\log^2 n)}$ samples.

Algorithm also applies for $\mathsf{S}\,|\mathrm{LWE}\rangle$

Solve $\mathsf{S}\,|\mathrm{LWE}\rangle^{m}_{n,q,\chi}$ [CLZ22]

Let a function $\chi : \mathbb{Z}_q \to \mathbb{C}$. Given m input states:

$$\Big\{ \sum_{e_i \in \mathbb{Z}_q} \chi(e_i)\, |\langle \mathbf{a}_i, \mathbf{s}\rangle + e_i \bmod q\rangle \Big\}_{i=1}^{m},$$

where $\mathbf{a}_i \sim \mathcal{U}(\mathbb{Z}_q^n)$ and known classically, and find $\mathbf{s} \in \mathbb{Z}_q^n$.

Algorithm also applies for $\mathsf{S}\,|\mathsf{LWE}\rangle$

Solve $\mathsf{S}\,|\mathsf{LWE}\rangle^{m}_{n,q,\chi}$ [CLZ22]

Let a function $\chi : \mathbb{Z}_q \to \mathbb{C}$. Given m input states:

$$\left\{ \sum_{e_i \in \mathbb{Z}_q} \chi(e_i) \,|\langle \mathbf{a}_i, \mathbf{s}\rangle + e_i \bmod q\rangle \right\}_{i=1}^{m},$$

where $\mathbf{a}_i \sim \mathcal{U}(\mathbb{Z}_q^n)$ and known classically, and find $\mathbf{s} \in \mathbb{Z}_q^n$.

$$\mathsf{S}\,|\mathsf{LWE}\rangle^{\ell}_{n,q,D_r} \leq \overline{\text{G-EDCP}}^{\ell}_{n,q,\sigma} \leq \overline{\text{U-EDCP}}^{O(\ell)}_{n,q,M}$$

where $\sigma = q/r$ and $M = c \cdot \sigma$.

Algorithm also applies for $\mathsf{S}\,|\mathrm{LWE}\rangle$

Solve $\mathsf{S}\,|\mathrm{LWE}\rangle^{m}_{n,q,\chi}$ [CLZ22]

Let a function $\chi : \mathbb{Z}_q \to \mathbb{C}$. Given m input states:

$$\Big\{ \sum_{e_i \in \mathbb{Z}_q} \chi(e_i)\,|\langle \mathbf{a}_i, \mathbf{s}\rangle + e_i \bmod q\rangle \Big\}_{i=1}^{m},$$

where $\mathbf{a}_i \sim \mathcal{U}(\mathbb{Z}_q^n)$ and known classically, and find $\mathbf{s} \in \mathbb{Z}_q^n$.

$$\mathsf{S}\,|\mathrm{LWE}\rangle^{\ell}_{n,q,D_r} \leq \overline{\text{G-EDCP}}^{\ell}_{n,q,\sigma} \leq \overline{\text{U-EDCP}}^{O(\ell)}_{n,q,M}$$

where $\sigma = q/r$ and $M = c \cdot \sigma$.

Theorem

Let $n, q = \mathrm{poly}(\kappa)$ be integers, where q is a power-of-two. Let $r = \Omega(\sqrt{\kappa})$ and $q/r = \Omega(\sqrt{\kappa})$. There exists a quantum algorithm for $\mathsf{S}\,|\mathrm{LWE}\rangle^{\ell}_{n,q,D_r}$ in time $2^{\mathcal{O}(\log^2 n)}$, when $\ell = 2^{\Omega(\log^2 n)}$.

Impact on LWE

Theorem [BKSW18]

Let $m \geq n \log q$ and $q = \mathsf{poly}(n)$. There is a probabilistic quantum reduction from $\mathsf{LWE}^{m}_{n,q,\alpha} \leq \text{U-EDCP}^{\ell}_{n,q,M}$, where

$$\ell < 1/(M \cdot \alpha \cdot \mathsf{poly}(n)).$$

Impact on LWE

Theorem [BKSW18]

Let $m \geq n \log q$ and $q = \mathsf{poly}(n)$. There is a probabilistic quantum reduction from $\mathsf{LWE}^{m}_{n,q,\alpha} \leq \text{U-EDCP}^{\ell}_{n,q,M}$, where

$$\ell < 1/(M \cdot \alpha \cdot \mathsf{poly}(n)).$$

- Our algorithm needs $\ell = 2^{\Omega(\log^2 n)}$ U-EDCP samples.

Impact on LWE

Theorem [BKSW18]

Let $m \geq n \log q$ and $q = \mathsf{poly}(n)$. There is a probabilistic quantum reduction from $\mathsf{LWE}^{m}_{n,q,\alpha} \leq \text{U-EDCP}^{\ell}_{n,q,M}$, where

$$\ell < 1/(M \cdot \alpha \cdot \mathsf{poly}(n)).$$

- Our algorithm needs $\ell = 2^{\Omega(\log^2 n)}$ U-EDCP samples.
- $M \cdot \ell < 1/(\alpha \cdot \mathsf{poly}(n)) \Rightarrow \alpha q < q/(M \cdot \ell \cdot \mathsf{poly}(n))$.

Impact on LWE

Theorem [BKSW18]

Let $m \geq n \log q$ and $q = \mathsf{poly}(n)$. There is a probabilistic quantum reduction from $\mathsf{LWE}^m_{n,q,\alpha} \leq \text{U-EDCP}^\ell_{n,q,M}$, where

$$\ell < 1/(M \cdot \alpha \cdot \mathsf{poly}(n)).$$

- Our algorithm needs $\ell = 2^{\Omega(\log^2 n)}$ U-EDCP samples.
- $M \cdot \ell < 1/(\alpha \cdot \mathsf{poly}(n)) \Rightarrow \alpha q < q/(M \cdot \ell \cdot \mathsf{poly}(n))$.
- Reduction yields only polynomially many EDCP samples.

Impact on LWE

Theorem [BKSW18]

Let $m \geq n \log q$ and $q = \mathsf{poly}(n)$. There is a probabilistic quantum reduction from $\mathsf{LWE}^m_{n,q,\alpha} \leq \text{U-EDCP}^\ell_{n,q,M}$, where

$$\ell < 1/(M \cdot \alpha \cdot \mathsf{poly}(n)).$$

- Our algorithm needs $\ell = 2^{\Omega(\log^2 n)}$ U-EDCP samples.
- $M \cdot \ell < 1/(\alpha \cdot \mathsf{poly}(n)) \Rightarrow \alpha q < q/(M \cdot \ell \cdot \mathsf{poly}(n))$.
- Reduction yields only polynomially many EDCP samples.

Impact on LWE

Theorem [BKSW18]

Let $m \geq n \log q$ and $q = \mathrm{poly}(n)$. There is a probabilistic quantum reduction from $\mathrm{LWE}^{m}_{n,q,\alpha} \leq \text{U-EDCP}^{\ell}_{n,q,M}$, where

$$\ell < 1/(M \cdot \alpha \cdot \mathrm{poly}(n)).$$

- Our algorithm needs $\ell = 2^{\Omega(\log^2 n)}$ U-EDCP samples.
- $M \cdot \ell < 1/(\alpha \cdot \mathrm{poly}(n)) \Rightarrow \alpha q < q/(M \cdot \ell \cdot \mathrm{poly}(n))$.
- Reduction yields only polynomially many EDCP samples.

  $\Rightarrow$ Our algorithm does not extend to standard LWE

Future work

1. Can the reduction from LWE to EDCP be improved, or can our algorithm be modified so that it requires only a poly(n) EDCP samples?

Future work

1. Can the reduction from LWE to EDCP be improved, or can our algorithm be modified so that it requires only a poly(n) EDCP samples?
2. Is it possible to handle NON power-of-two moduli (e.g. via modulus switching)?

Future work

1. Can the reduction from LWE to EDCP be improved, or can our algorithm be modified so that it requires only a poly(n) EDCP samples?
2. Is it possible to handle NON power-of-two moduli (e.g. via modulus switching)?
3. EDCP assumption for structured LWE problems?

Thanks for your time

Do you have any questions?

References

- [AG11] Sanjeev Arora and Rong Ge. "New Algorithms for Learning in Presence of Errors." ICALP 2011.
- [BKSW18] Zvika Brakerski, Elena Kirshanova, Damien Stehlé, and 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." ePrint 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." Talk at Simons Institute, 2020.
- [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.
- [R07] Oded Regev. "On the complexity of lattice problems with polynomial approximation factors." pp. 475–496. ISC, Springer (2010).