Adaptive Hardcore Bit of LWE and Its Application in Key Leasing

Weiqiang Wen
Based on joint work with Hieu Phan, Xingyu Yan and Jinwei Zheng

Télécom Paris, Institut Polytechnique de Paris

CHARM Workshop, Institut de Mathématiques de Bordeaux
June 19th, 2025

- Lattice-based **classical** cryptography with **post-quantum security**

Lattice-based cryptography: from classical to quantum?

- Lattice-based **classical** cryptography with **post-quantum security**

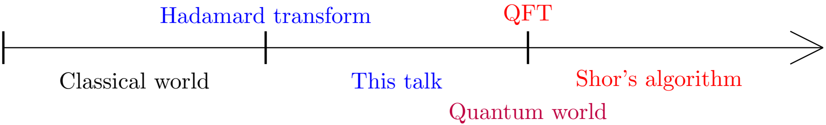
- Lattice-based **quantum** cryptography

Lattice-based cryptography: from classical to quantum?

- Lattice-based **classical** cryptography with **post-quantum security**
- Lattice-based **quantum** cryptography with **new functionalities**

Lattices in a quantum world

⋆ **Lattices + Hadamard transform?**



QFT for Quantum Fourier Transform.

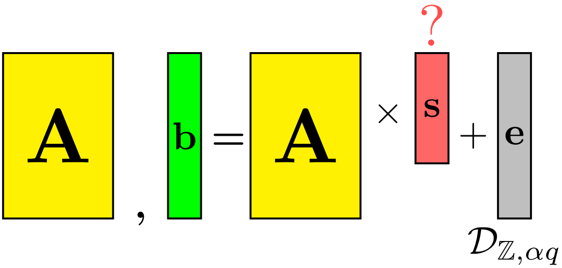
- ⋆ **$|$Lattices + Hadamard transform$\rangle$ brings new functionalities:**
  - Proof of quantumness [BCM+18]
  - Public key encryption with secure key leasing [CGJL25a]
  - Classical delegation of quantum computation [Mah18]
  - Multi-party quantum computation over classical channel [Bar21]
  - ...

- ⋆ **$|$Lattices + Hadamard transform$\rangle$ brings new functionalities:**
  - **Proof of quantumness** [BCM+18]
  - **Public key encryption with secure key leasing** [CGJL25a]
  - Classical delegation of quantum computation [Mah18]
  - Multi-party quantum computation over classical channel [Bar21]
  - ...

[O. Regev, FOCS'02]

Quantum Computation and Lattice Problems

Learning With Errors

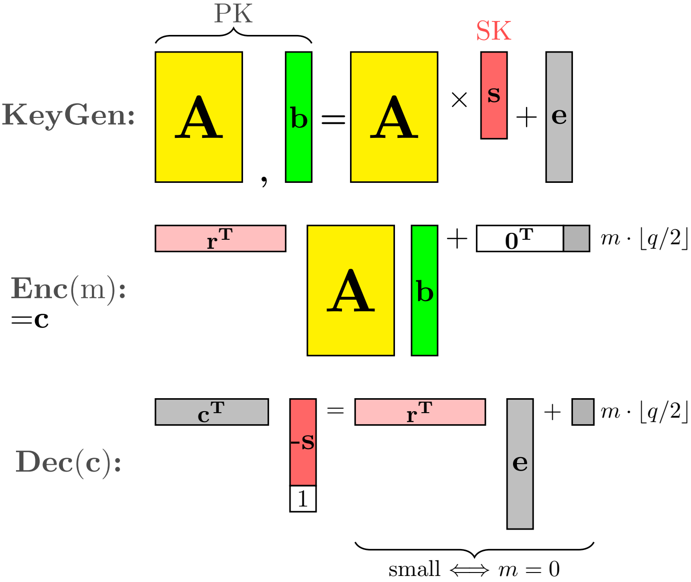


Learning With Errors Problem for n, q, m and $\mathcal{D}_{\mathbb{Z},\alpha q}$ ($\mathrm{LWE}^m_{n,q,\alpha}$)

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 $\mathbf{s} \in_R \mathbb{Z}_q^n$.

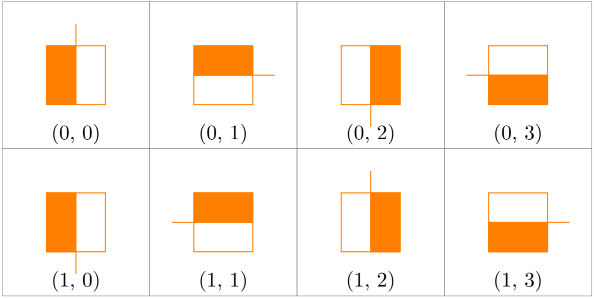
Output: the secret vector $\mathbf{s}$.

Public-key encryption based on LWE [Reg05]

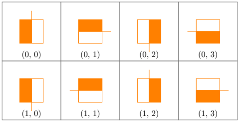


The Dihedral Coset Problem

- Dihedral group: $D_N \simeq \mathbb{Z}_2 \ltimes \mathbb{Z}_N$.



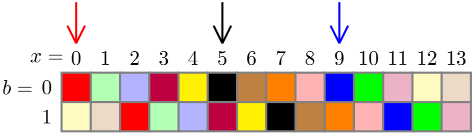
- Dihedral group: $D_N \simeq \mathbb{Z}_2 \ltimes \mathbb{Z}_N$.



Dihedral Coset Problem (DCP) for D_N and ℓ (DCP_N^ℓ)

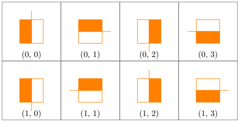
Input: $\left\{ \frac{1}{\sqrt{2}} \left(|0, 0 + x_i\rangle + |1, s + x_i\rangle \right) \right\}_{i \leq \ell}$ (coset of hidden subgroup: $\{(0,0),(1,s)\}$).
Output: the secret s.

Example:



- Dihedral group: D_{14}; Hidden subgroup: $\{(0,0),(1,2)\}$.

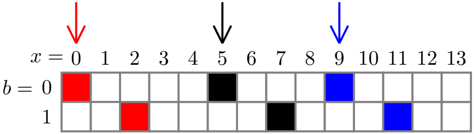
- Dihedral group: $D_N \simeq \mathbb{Z}_2 \ltimes \mathbb{Z}_N$.



Dihedral Coset Problem (DCP) for D_N and ℓ (DCP_N^ℓ)

Input: $\left\{ \frac{1}{\sqrt{2}} \left(|0, 0 + x_i\rangle + |1, s + x_i\rangle \right) \right\}_{i \le \ell}$ (coset of hidden subgroup: $\{(0,0),(1,s)\}$).
Output: the secret s.

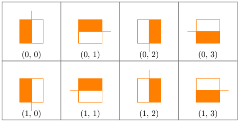
Example:



- Dihedral group: D_{14}; Hidden subgroup: $\{(0,0),(1,2)\}$.
- Samples: $\frac{1}{\sqrt{2}}(|0,0\rangle + |1,2\rangle)$; $\frac{1}{\sqrt{2}}(|0,5\rangle + |1,7\rangle)$; $\frac{1}{\sqrt{2}}(|0,9\rangle + |1,11\rangle)$.

The Dihedral Coset Problem

- Dihedral group: $D_N \simeq \mathbb{Z}_2 \ltimes \mathbb{Z}_N$.

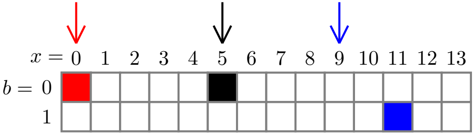


Dihedral Coset Problem (DCP) for D_N and ℓ (DCP_N^{ℓ})

Input: $\left\{ \frac{1}{\sqrt{2}} \left(|0, 0 + x_i\rangle + |1, s + x_i\rangle \right) \right\}_{i \leq \ell}$ (coset of hidden subgroup: $\{(0,0),(1,s)\}$).

Output: the secret s.

Example:



- Dihedral group: D_{14}; Hidden subgroup: $\{(0,0),(1,2)\}$.
- ***Measured*** Samples: $|0,0\rangle$; $|0,5\rangle$; $|1,11\rangle$.

Parameters: $n = \mathcal{O}(\lambda)$

$\underline{\text{LWE}_{n,q,\alpha}}$: Given

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

where $\forall i, \mathbf{a}_i \in_R \mathbb{Z}_q^n, e_i \hookleftarrow \lfloor \mathcal{D}_{\mathbb{R},\alpha q} \rceil$, find $\mathbf{s}$.

$\leq$ [Reg02]

$\underline{\text{DCP}_{1,N}}$: Given

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

where $\forall i, x_i \in_R \mathbb{Z}_N$, find s.

We have $\ell \leq \widetilde{\mathcal{O}}(2^{\log q})$, $N = q^n = 2^{n \log n}$ [BKSW18]
(Originally, [Reg02] gives $N = 2^{n^2}$.)

LWE and (Extended-)DCP

Parameters: $n = \mathcal{O}(\lambda)$

$\underline{\mathrm{LWE}_{n,q,\alpha}}$: Given $\underset{\text{[Reg02]}}{\leq}$ $\underline{\mathrm{DCP}_{1,N}}$: Given

$$(\mathbf{a}_1, \langle \mathbf{a}_1, \mathbf{s}\rangle + e_1 \bmod q) \qquad |0, x_1\rangle + |1, x_1 + s \bmod N\rangle$$
$$\vdots \qquad\qquad \vdots$$
$$(\mathbf{a}_m, \langle \mathbf{a}_m, \mathbf{s}\rangle + e_m \bmod q) \qquad |0, x_\ell\rangle + |1, x_\ell + s \bmod N\rangle$$

where $\forall i, \mathbf{a}_i \in_R \mathbb{Z}_q^n, e_i \hookleftarrow \lfloor \mathcal{D}_{\mathbb{R},\alpha q} \rceil$, find $\mathbf{s}$. where $\forall i, x_i \in_R \mathbb{Z}_N$, find s.

$\underline{\mathrm{LWE}_{n,q,\alpha}}$: Given $\underset{\text{[BKSW18]}}{\leq}$ $\underline{\text{Extended DCP}_{n,q}}$: Given

$$(\mathbf{a}_1, \langle \mathbf{a}_1, \mathbf{s}\rangle + e_1 \bmod q) \qquad |0, \mathbf{x}_1\rangle + |1, \mathbf{x}_1 + \mathbf{s} \bmod q\rangle$$
$$\vdots \qquad\qquad \vdots$$
$$(\mathbf{a}_m, \langle \mathbf{a}_m, \mathbf{s}\rangle + e_m \bmod q) \qquad |0, \mathbf{x}_\ell\rangle + |1, \mathbf{x}_\ell + \mathbf{s} \bmod q\rangle$$

where $\forall i, \mathbf{a}_i \in_R \mathbb{Z}_q^n, e_i \hookleftarrow \lfloor \mathcal{D}_{\mathbb{R},\alpha q} \rceil$, find $\mathbf{s}$. where $\forall i, \mathbf{x}_i \in_R \mathbb{Z}_q^n$, find $\mathbf{s}$.

We have $\ell \leq \widetilde{\mathcal{O}}(2^{\log q})$, $N = q^n = 2^{n \log n}$ [BKSW18]
(Originally, [Reg02] gives $N = 2^{n^2}$.)

Parameters: $n = \mathcal{O}(\lambda)$

$\underline{\mathrm{LWE}_{n,q,\alpha}}$: Given

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

where $\forall i, \mathbf{a}_i \in_R \mathbb{Z}_q^n, e_i \hookleftarrow \lfloor \mathcal{D}_{\mathbb{R},\alpha q} \rceil$, find $\mathbf{s}$.

$\underset{\text{[Reg02]}}{\leq}$

$\underline{\mathrm{DCP}_{1,N}}$: Given

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

where $\forall i, x_i \in_R \mathbb{Z}_N$, find s.

The Extended-DCP is not hard with $n^{\mathcal{O}(\log q)}$ samples [BJK+25; BNP18; Bon19]

$\underline{\mathrm{LWE}_{n,q,\alpha}}$: Given

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

where $\forall i, \mathbf{a}_i \in_R \mathbb{Z}_q^n, e_i \hookleftarrow \lfloor \mathcal{D}_{\mathbb{R},\alpha q} \rceil$, find $\mathbf{s}$.

$\underset{\text{[BKSW18]}}{\leq}$

$\underline{\text{Extended DCP}_{n,q}}$: Given

$$|0, \mathbf{x}_1\rangle + |1, \mathbf{x}_1 + \mathbf{s} \bmod q\rangle$$
$$\vdots$$
$$|0, \mathbf{x}_\ell\rangle + |1, \mathbf{x}_\ell + \mathbf{s} \bmod q\rangle$$

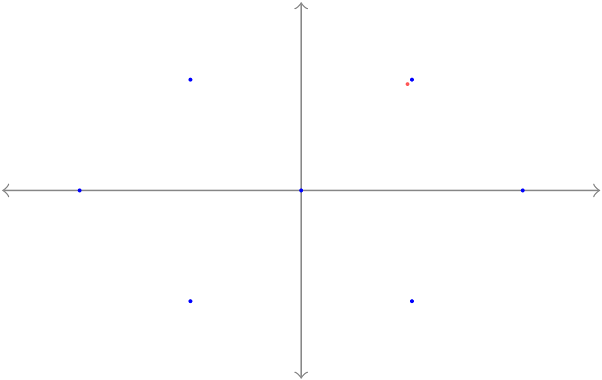
where $\forall i, \mathbf{x}_i \in_R \mathbb{Z}_q^n$, find $\mathbf{s}$.

We have $\ell \leq \widetilde{\mathcal{O}}(2^{\log q})$, $N = q^n = 2^{n \log n}$ [BKSW18]

(Originally, [Reg02] gives $N = 2^{n^2}$.)

LWE to Extended-DCP reduction

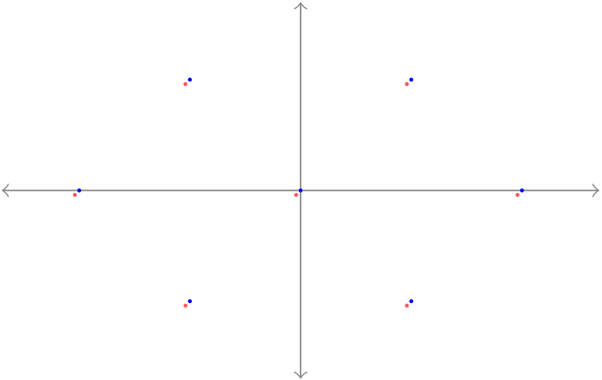
- Input an LWE instance: $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s}+\mathbf{e}\_0\ [q])$. Consider the lattice $\Lambda_q(\mathbf{A}) = \{\mathbf{A}\mathbf{x} \bmod q \mid \mathbf{x} \in \mathbb{Z}_q^n\}$.



$$\sum_{\mathbf{x}\in\mathbb{Z}_q^n} (|0, \mathbf{x}, \mathbf{A}\mathbf{x}\rangle + |1, \mathbf{x}, \mathbf{A}\mathbf{x}\rangle) .$$

LWE to Extended-DCP reduction

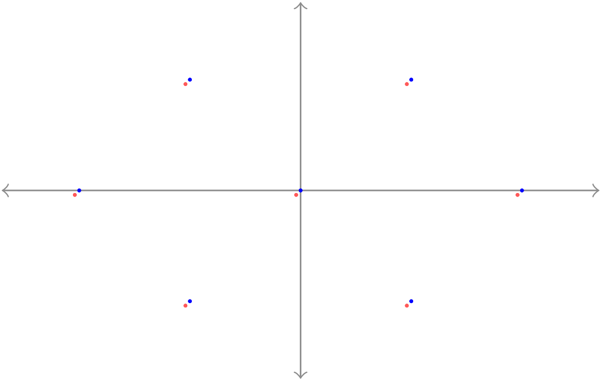
- Shift lattice $\Lambda_q(\mathbf{A})$ by $\mathbf{b} = \mathbf{As}+\mathbf{e}_0$ $[q]$, according to the value of first register.



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

LWE to Extended-DCP reduction

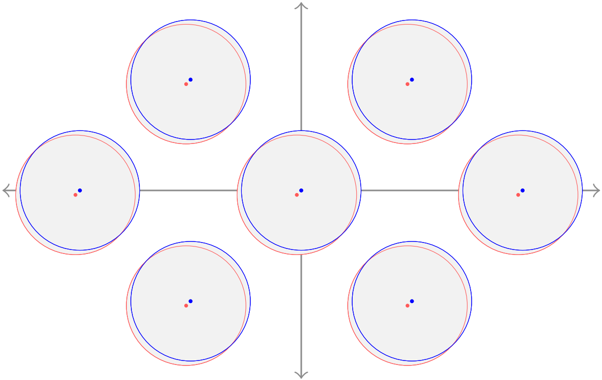
- Rewrite $\mathbf{x}$ in the second register by $\mathbf{x} + b\mathbf{s}$, according to the value k in the first register.



$$\sum_{\mathbf{x}\in\mathbb{Z}_q^n} \left(|0, \mathbf{x}, \mathbf{A}\mathbf{x}\rangle + |1, \mathbf{x}+\mathbf{s}, \mathbf{A}(\mathbf{x}+\mathbf{s}) - \mathbf{b}\rangle\right) = \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \left(|0, \mathbf{x}, \mathbf{A}\mathbf{x}\rangle + |1, \mathbf{x}+\mathbf{s}, \mathbf{A}\mathbf{x} - \mathbf{e}_0\rangle\right).$$

LWE to Extended-DCP reduction

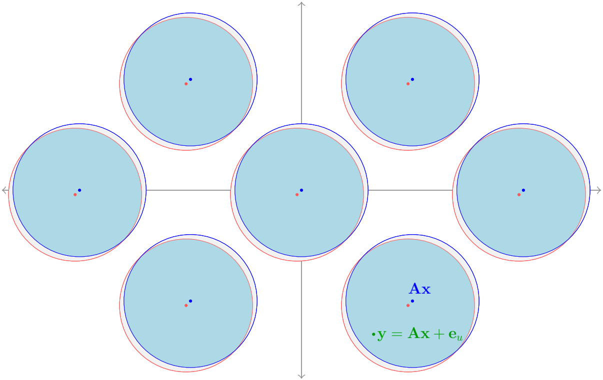
- Create spheres with centers lattice points as well as the noisy ones.



$$\sum_{\mathbf{x}\in\mathbb{Z}_q^n} \left(|0, \mathbf{x}, \mathbf{Ax}, \mathcal{B}(\mathbf{Ax})\rangle + |1, \mathbf{x}+\mathbf{s}, \mathbf{Ax}-\mathbf{e}_0, \mathcal{B}(\mathbf{Ax}-\mathbf{e}_0)\rangle\right); \mathcal{B}(\mathbf{c}) = \sum_{\substack{\mathbf{e}_u\in\mathbb{R}^m \\ \|\mathbf{e}_u\|\leq r}} |\mathbf{c}+\mathbf{e}_u\rangle .$$

LWE to Extended-DCP reduction

- Measure and once the shading area is measured, Extended-DCP state is obtained.



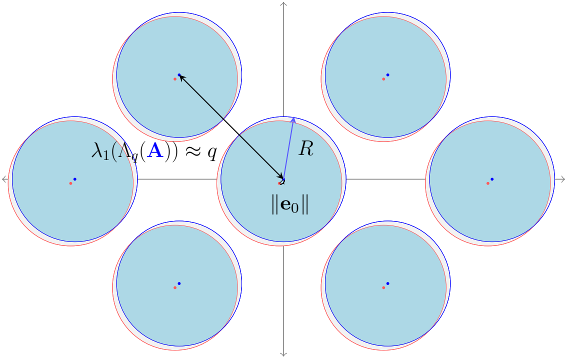
$$|0, \mathbf{x}, \mathbf{Ax}, \mathbf{y}\rangle + |1, \mathbf{x} + \mathbf{s}, \mathbf{Ax} - \mathbf{e}_0, \mathbf{y}\rangle = |0, \mathbf{x}, \mathbf{0}, \mathbf{y}\rangle + |1, \mathbf{x} + \mathbf{s}, \mathbf{0}, \mathbf{y}\rangle \,; \mathbf{y} = \mathbf{Ax} + \mathbf{e}_u.$$

Lemma (Adapted from [Reg02, Claim 3.7])

For any $R \geq 1$ and some vector $\mathbf{e}$, *let* $\mathcal{B}_n(\mathbf{v}, R) = \{\mathbf{x} \mid \|\mathbf{x} - \mathbf{v}\| \leq R\}$, *Then we have*

$$\frac{\mathrm{vol}(\mathcal{B}_n(\mathbf{0}, R) \cap \mathcal{B}_n(\mathbf{e}, R))}{\mathrm{vol}(\mathcal{B}_n(\mathbf{0}, R))} \geq 1 - \mathcal{O}(\sqrt{n}\|\mathbf{e}\|/R).$$

- We pick $R \approx q/2$, the probability to measure the intersection is $1 - \mathcal{O}(\sqrt{n}\|\mathbf{e}_0\|/q)$. As a result, we can obtain at most $\widetilde{\mathcal{O}}(q/(\sqrt{n}\|\mathbf{e}_0\|))$ ($\leq \widetilde{\mathcal{O}}(2^{\log q})$) Extended-DCP states.



Quantum Fourier transform and Hadamard transform

- Quantum Fourier transform (QFT, underlying Shor's algorithm): $\left[\omega_q = \mathrm{e}^{\frac{2\pi i}{q}}\right]$

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

- Can be viewed as quantum implementation of classical Fourier transform circuit.
  - Classical FT: from $\underline{\{x_j\}_{j\in[q]}}$ to $\underline{\{y_k\}_{k\in[q]}}$ such that

$$y_k = \frac{1}{\sqrt{q}} \sum_{j\in[q]} x_j \cdot \omega_q^{j\cdot k}, \forall k \in [q].$$

  - Quantum FT: from $\underline{\sum_{j\in[q]} x_j |j\rangle}$ to $\underline{\sum_{k\in[q]} y_k |k\rangle}$ with the same conditions.

Quantum Fourier transform and Hadamard transform

- Quantum Fourier transform (QFT, underlying Shor's algorithm): $\left[\omega_q = \mathrm{e}^{\frac{2\pi i}{q}}\right]$

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

- Can be viewed as quantum implementation of classical Fourier transform circuit.
  - Classical FT: from $\underline{\{x_j\}_{j\in[q]}}$ to $\underline{\{y_k\}_{k\in[q]}}$ such that

$$y_k = \frac{1}{\sqrt{q}} \sum_{j\in[q]} x_j \cdot \omega_q^{j\cdot k}, \forall k \in [q].$$

  - Quantum FT: from $\underline{\sum_{j\in[q]} x_j |j\rangle}$ to $\underline{\sum_{k\in[q]} y_k |k\rangle}$ with the same conditions.

- Hadamard transform (QFT with $q = 2$):

$$\mathcal{H} : |x\rangle \mapsto \frac{1}{\sqrt{2}} \sum_{y \in \mathbb{Z}_2} \omega_q^{\langle x, y\rangle} |y\rangle .$$

- Extension to multiple dimension:

$$\mathcal{H}^n : |\mathbf{x}\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{\mathbf{y} \in \mathbb{Z}_2^n} \omega_q^{\langle \mathbf{x}, \mathbf{y}\rangle} |\mathbf{y}\rangle .$$

Adaptive hardcore bit [BCM+18]

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

Adaptive hardcore bit [BCM+18]

$$\begin{tikzcd} & {|0,\mathbf{x}_0\rangle + |1,\mathbf{x}_1\rangle} \arrow[dl, "\text{Standard Measure}"'] \arrow[dr, "\text{Hadamard Measure}"] & \\ (b,\mathbf{x}_b) & & (c,\mathbf{d}) \end{tikzcd}$$

- $\mathbf{d} \sim U(\{0,1\}^{n \log q})$ and $c = \langle \mathbf{d}, J(\mathbf{x}_0) \oplus J(\mathbf{x}_1) \rangle$.

Adaptive hardcore bit [BCM+18]

$$|0,\mathbf{x}_0\rangle + |1,\mathbf{x}_1\rangle$$

Standard Measure ↙ ↘ Hadamard Measure

$$(b,\mathbf{x}_b) \qquad\qquad (c,\mathbf{d})$$

- $\mathbf{d} \sim U(\{0,1\}^{n\log q})$ and $c = \langle \mathbf{d}, J(\mathbf{x}_0)\oplus J(\mathbf{x}_1)\rangle$.

$$\begin{aligned}\mathcal{H}^{2nd}(|0,J(\mathbf{x}_0)\rangle + |1,J(\mathbf{x}_1)\rangle) &= \sum_{\mathbf{d}\in\mathbb{Z}_2^{n\log q}} \left((-1)^{\langle J(\mathbf{x}_0),\mathbf{d}\rangle}|0\rangle + (-1)^{\langle J(\mathbf{x}_1),\mathbf{d}\rangle}|1\rangle\right)|\mathbf{d}\rangle \\ &= \sum_{\mathbf{d}\in\mathbb{Z}_2^{n\log q}} \left||0\rangle + (-1)^{\langle J(\mathbf{x}_0)\oplus J(\mathbf{x}_1),\mathbf{d}\rangle}|1\rangle\right\rangle|\mathbf{d}\rangle.\end{aligned}$$

Adaptive hardcore bit [BCM+18]

$$
\begin{tikzcd}
 & {|0, \mathbf{x}_0\rangle + |1, \mathbf{x}_1\rangle} \arrow[dl, "\text{Standard Measure}"'] \arrow[dr, "\text{Hadamard Measure}"] & \\
(b, \mathbf{x}_b) & & (c, \mathbf{d})
\end{tikzcd}
$$

- $\mathbf{d} \sim U(\{0,1\}^{n \log q})$ and $c = \langle \mathbf{d}, J(\mathbf{x}_0) \oplus J(\mathbf{x}_1) \rangle$.

$$
\begin{aligned}
\mathcal{H}^{2nd}(|0, J(\mathbf{x}_0)\rangle + |1, J(\mathbf{x}_1)\rangle) &= \sum_{\mathbf{d} \in \mathbb{Z}_2^{n \log q}} \left((-1)^{\langle J(\mathbf{x}_0), \mathbf{d} \rangle} |0\rangle + (-1)^{\langle J(\mathbf{x}_1), \mathbf{d} \rangle} |1\rangle \right) |\mathbf{d}\rangle \\
&= \sum_{\mathbf{d} \in \mathbb{Z}_2^{n \log q}} \Big| |0\rangle + (-1)^{\langle J(\mathbf{x}_0) \oplus J(\mathbf{x}_1), \mathbf{d} \rangle} |1\rangle \Big\rangle |\mathbf{d}\rangle.
\end{aligned}
$$

$$
\mathcal{H}|x\rangle = \sum_{d \in \mathbb{Z}_2} (-1)^{x \cdot d} |d\rangle = |0\rangle + (-1)^{x} |1\rangle.
$$

Adaptive hardcore bit [BCM+18]

$$
\begin{tikzcd}
 & {|0, \mathbf{x}_0\rangle + |1, \mathbf{x}_1\rangle} \arrow[dl, "\text{Standard Measure}"'] \arrow[dr, "\text{Hadamard Measure}"] & \\
(b, \mathbf{x}_b) & & (c, \mathbf{d})
\end{tikzcd}
$$

- $\mathbf{d} \sim U(\{0,1\}^{n \log q})$ and $c = \langle \mathbf{d}, J(\mathbf{x}_0) \oplus J(\mathbf{x}_1) \rangle$.

$$
\begin{aligned}
\mathcal{H}^{2nd}(|0, J(\mathbf{x}_0)\rangle + |1, J(\mathbf{x}_1)\rangle) &= \sum_{\mathbf{d} \in \mathbb{Z}_2^{n \log q}} \left((-1)^{\langle J(\mathbf{x}_0), \mathbf{d} \rangle} |0\rangle + (-1)^{\langle J(\mathbf{x}_1), \mathbf{d} \rangle} |1\rangle \right) |\mathbf{d}\rangle \\
&= \sum_{\mathbf{d} \in \mathbb{Z}_2^{n \log q}} \Big| |0\rangle + (-1)^{\langle J(\mathbf{x}_0) \oplus J(\mathbf{x}_1), \mathbf{d} \rangle} |1\rangle \Big\rangle |\mathbf{d}\rangle.
\end{aligned}
$$

$$
\mathcal{H}^{1st}(\mathcal{H}^{2nd}(|0, J(\mathbf{x}_0)\rangle + |1, J(\mathbf{x}_1)\rangle)) = \sum_{\mathbf{d} \in \mathbb{Z}_2^{n \log q}} |\langle J(\mathbf{x}_0) \oplus J(\mathbf{x}_1), \mathbf{d} \rangle\rangle |\mathbf{d}\rangle.
$$

Adaptive hardcore bit [BCM+18]

$$
\begin{tikzcd}[column sep=large]
 & {|0, \mathbf{x}_0\rangle + |1, \mathbf{x}_1\rangle} \arrow[dl, "\text{Standard Measure}"'] \arrow[dr, "\text{Hadamard Measure}"] & \\
(b, \mathbf{x}_b) & & (c, \mathbf{d})
\end{tikzcd}
$$

- $\mathbf{d} \sim U(\{0,1\}^{n \log q})$ and $c = \langle \mathbf{d}, J(\mathbf{x}_0) \oplus J(\mathbf{x}_1) \rangle$.

$\star$ $\langle \mathbf{d}, J(\mathbf{x}_0) \oplus J(\mathbf{x}_1) \rangle = \left\langle \left(\langle \mathbf{d}_i, J(x_{b,i}) \oplus J(x_{b,i} + (-1)^b) \rangle \right)_{i \in [n]}, \mathbf{s} \right\rangle$

Adaptive hardcore bit [BCM+18]

$$\begin{tikzcd}[column sep=small] & \lvert 0, \mathbf{x}_0 \rangle + \lvert 1, \mathbf{x}_1 \rangle \arrow[dl, "\text{Standard Measure}"'] \arrow[dr, "\text{Hadamard Measure}"] & \\ (b, \mathbf{x}_b) & & (c, \mathbf{d}) \end{tikzcd}$$

- $\mathbf{d} \sim U(\{0,1\}^{n \log q})$ and $c = \langle \mathbf{d}, J(\mathbf{x}_0) \oplus J(\mathbf{x}_1) \rangle$.

$\star$ $\langle \mathbf{d}, J(\mathbf{x}_0) \oplus J(\mathbf{x}_1) \rangle = \left\langle \left(\langle \mathbf{d}_i, J(x_{b,i}) \oplus J(x_{b,i} + (-1)^b) \rangle \right)_{i \in [n]}, \mathbf{s} \right\rangle$

$\Leftrightarrow$ $\langle \mathbf{d}_i, J(x_{0,i}) \oplus J(x_{1,i}) \rangle = \langle \mathbf{d}_i, J(x_{b,i}) \oplus J(x_{b,i} + (-1)^b) \rangle \cdot s_i$.

Adaptive hardcore bit [BCM+18]

$$\begin{tikzcd}
 & {|0, \mathbf{x}_0\rangle + |1, \mathbf{x}_1\rangle} \arrow[dl, "\text{Standard Measure}"'] \arrow[dr, "\text{Hadamard Measure}"] & \\
(b, \mathbf{x}_b) & & (c, \mathbf{d})
\end{tikzcd}$$

- $\mathbf{d} \sim U(\{0,1\}^{n \log q})$ and $c = \langle \mathbf{d}, J(\mathbf{x}_0) \oplus J(\mathbf{x}_1) \rangle$.

$\star$ $\langle \mathbf{d}, J(\mathbf{x}_0) \oplus J(\mathbf{x}_1) \rangle = \Big\langle \big(\langle \mathbf{d}_i, J(x_{b,i}) \oplus J(x_{b,i} + (-1)^b) \rangle \big)_{i \in [n]}, \mathbf{s} \Big\rangle$

$\Leftrightarrow$ $\langle \mathbf{d}_i, J(x_{0,i}) \oplus J(x_{1,i}) \rangle = \langle \mathbf{d}_i, J(x_{b,i}) \oplus J(x_{b,i} + (-1)^b) \rangle \cdot s_i$.

$\Leftrightarrow$ $\langle \mathbf{d}_i, J(x_{0,i}) \oplus J(x_{0,i} + s_i) \rangle = \langle \mathbf{d}_i, J(x_{b,i}) \oplus J(x_{b,i} + (-1)^b) \rangle \cdot s_i$.

$$
\begin{tikzcd}
 & {|0, \mathbf{x}_0\rangle + |1, \mathbf{x}_1\rangle} \arrow[dl, "\text{Standard Measure}"'] \arrow[dr, "\text{Hadamard Measure}"] & \\
(b, \mathbf{x}_b) & & (c, \mathbf{d})
\end{tikzcd}
$$

- $\mathbf{d} \sim U(\{0,1\}^{n \log q})$ and $c = \langle \mathbf{d}, J(\mathbf{x}_0) \oplus J(\mathbf{x}_1) \rangle = \langle I_{b,\mathbf{x}_b}(\mathbf{d}), \mathbf{s} \rangle$.

$\star$ $\langle \mathbf{d}, J(\mathbf{x}_0) \oplus J(\mathbf{x}_1) \rangle = \left\langle \left(\langle \mathbf{d}_i, J(x_{b,i}) \oplus J(x_{b,i} + (-1)^b) \rangle \right)_{i \in [n]}, \mathbf{s} \right\rangle$

$\Rightarrow$ Denote $I_{b,\mathbf{x}_b}(\mathbf{d}) = \left(\langle \mathbf{d}_i, J(x_{b,i}) \oplus J(x_{b,i} + (-1)^b) \rangle \right)_{i \in [n]}$.

Adaptive hardcore bit [BCM+18]

$$|0, \mathbf{x}_0\rangle + |1, \mathbf{x}_1\rangle$$

Standard Measure $\swarrow$ $\searrow$ Hadamard Measure

$$(b, \mathbf{x}_b) \qquad\qquad (c, \mathbf{d})$$

- $\mathbf{d} \sim U(\{0,1\}^{n \log q})$ and $c = \langle \mathbf{d}, J(\mathbf{x}_0) \oplus J(\mathbf{x}_1)\rangle = \langle I_{b,\mathbf{x}_b}(\mathbf{d}), \mathbf{s}\rangle$.

$\star$ $\langle \mathbf{d}, J(\mathbf{x}_0) \oplus J(\mathbf{x}_1)\rangle = \left\langle \left(\langle \mathbf{d}_i, J(x_{b,i}) \oplus J(x_{b,i} + (-1)^b)\rangle\right)_{i\in[n]}, \mathbf{s} \right\rangle$

$\Rightarrow$ Denote $I_{b,\mathbf{x}_b}(\mathbf{d}) = \left(\langle \mathbf{d}_i, J(x_{b,i}) \oplus J(x_{b,i} + (-1)^b)\rangle\right)_{i\in[n]}$.

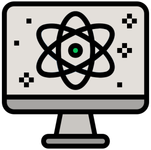
- **Adaptive hardcore bit [BCM+18]**: Given $(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e}_0)$ with superpolynomial modulus and $\mathbf{d} \hookleftarrow \{0,1\}^{n\lceil \log q\rceil}$ such that $I_{b,\mathbf{x}_b}(\mathbf{d}) \in \{0,1\}^n \setminus \{\mathbf{0}\}$, the adversary picks $(b, \mathbf{x}_b)$, hard to get c.

How does this help to prove quantumness?

Can we prove the quantumness?

How does this help to prove quantumness?

Quantum

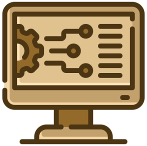


Can we prove the quantumness?

Send LWE instance

Randomly ask for values under either Hadamard or Standard measurement

Classical



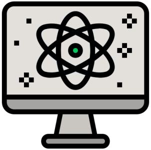
How does this help to prove quantumness?

Can we prove the quantumness?

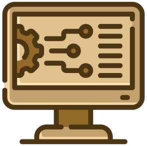
Send LWE instance

Randomly ask for values under either Hadamard or Standard measurement

Quantum



Classical



Do either measurement accordingly under quantum computation

$\Rightarrow$ Completeness

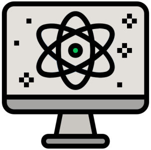
How does this help to prove quantumness?

Can we prove the quantumness?

Send LWE instance

Randomly ask for values under either Hadamard or Standard measurement

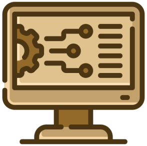
Quantum



Do either measurement accordingly under quantum computation

$\Longrightarrow$ Completeness

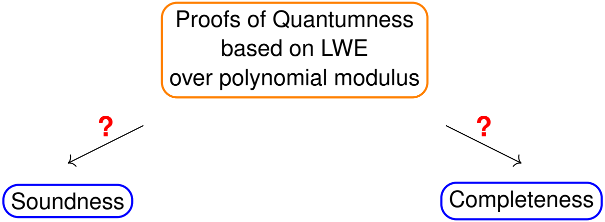
Classical

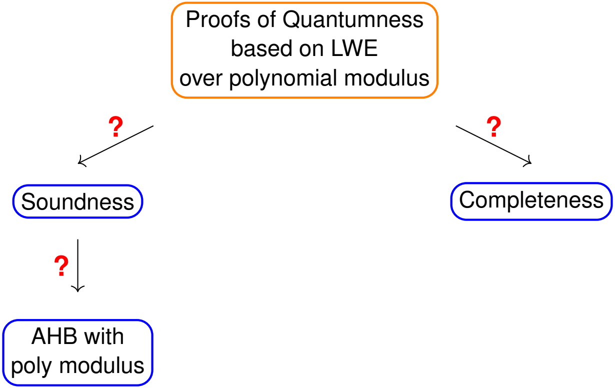


Need to know values under both measurement in advanced, impossible due to **AHB**.

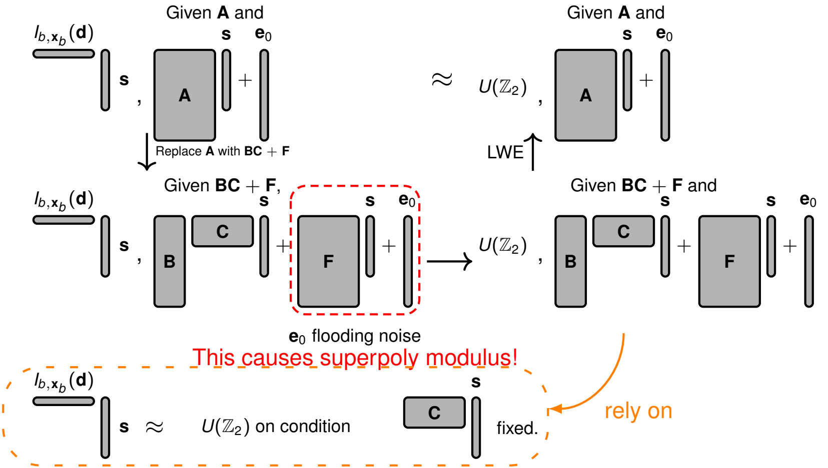
$\Longrightarrow$ Soundness

PoQ based on LWE over polynomial modulus



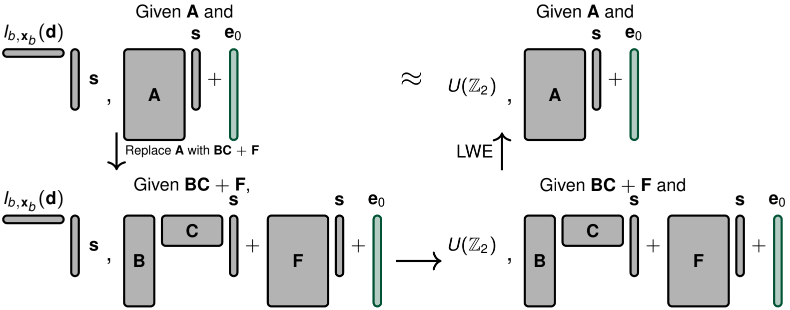

Proofs of Quantumness
based on LWE
over polynomial modulus
?
?
Soundness
Completeness
?
AHB with
poly modulus

Sketch of proof of AHB in [BCM+18]



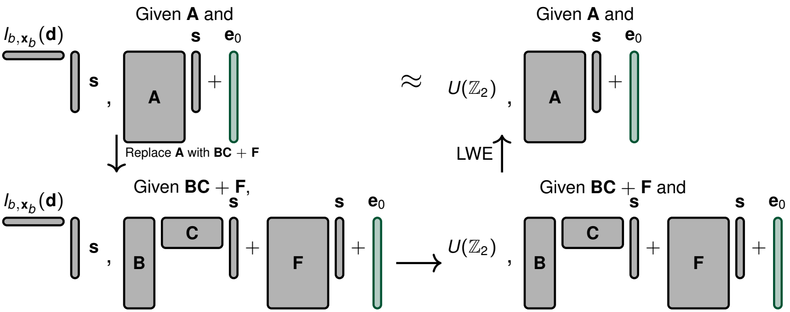
$\Rightarrow$ Given $(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e}_0 \bmod q)$, $\langle I_{b,\mathbf{x}_b}(\mathbf{d}), \mathbf{s}\rangle \approx U(\mathbb{Z}_2) \Rightarrow$ AHB.

Our proof with polynomial modulus



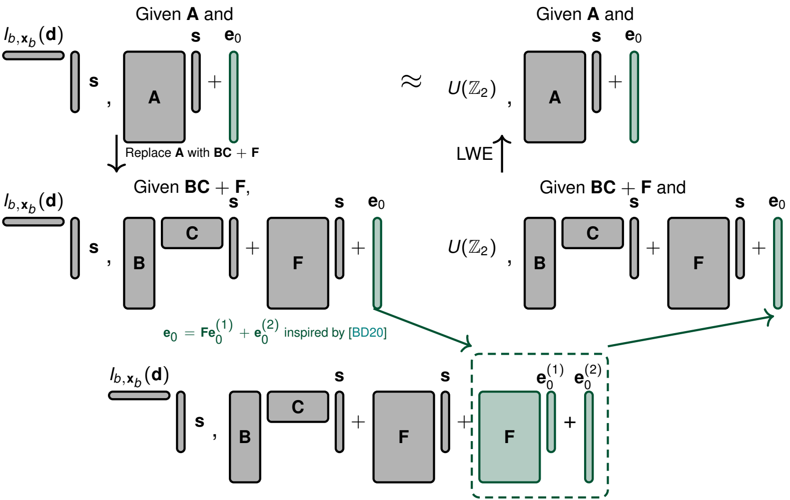
$\mathbf{e}_0$ covers Fs completely, Necessary?

Our proof with polynomial modulus

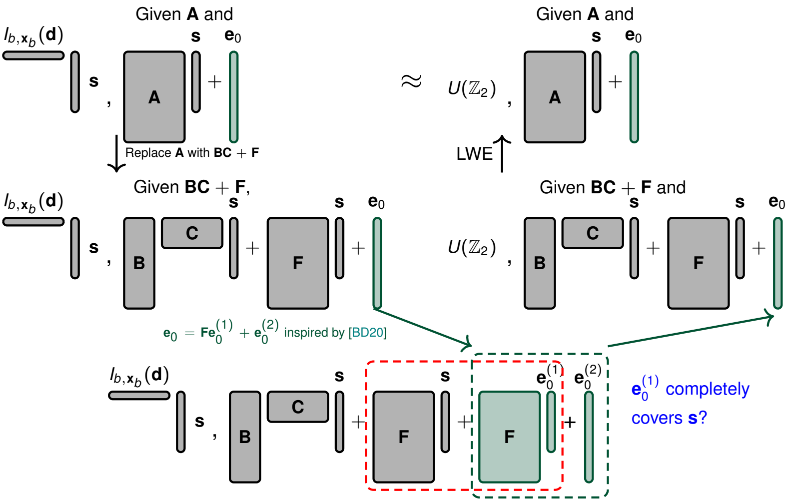


$\mathbf{e}_0$ covers Fs completely, Necessary? **No!**

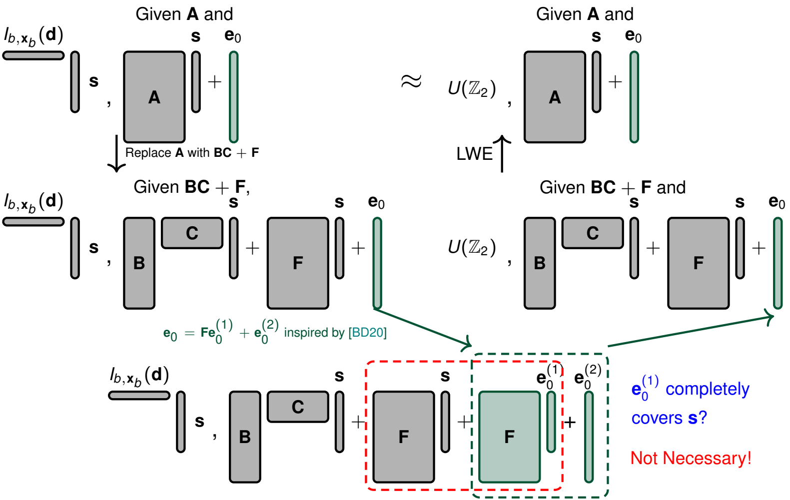
Our proof with polynomial modulus



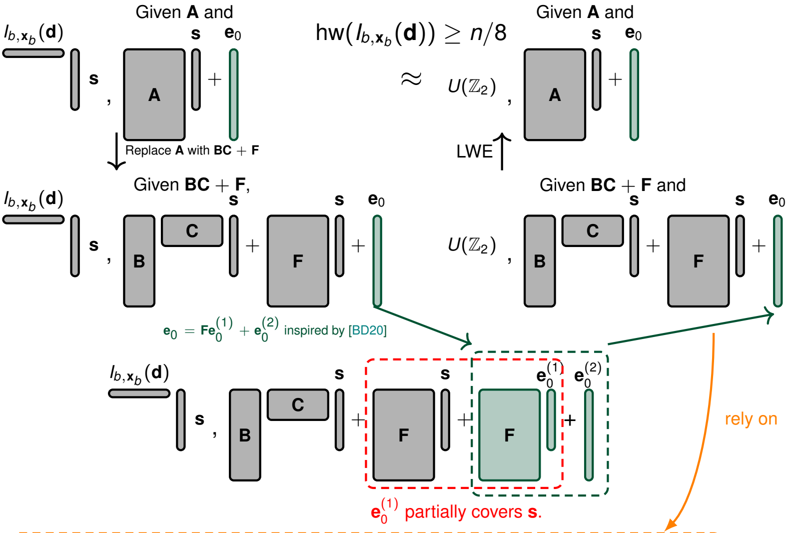
Our proof with polynomial modulus



Our proof with polynomial modulus



Our proof with polynomial modulus



$\langle l_{b,\mathbf{x}_b}(\mathbf{d}), \mathbf{s}\rangle \approx U(\mathbb{Z}_2)$ on condition **Cs** and $\mathbf{s} + \mathbf{e}_0^{(1)}$ are fixed, $\mathbf{e}_0^{(1)} \hookleftarrow D_{\mathbb{Z}^n, n, n^{3/2}}$

Proofs of Quantumness
based on LWE
over polynomial modulus

?

Soundness

Completeness

AHB with
poly modulus

PoQ based on LWE over polynomial modulus

Proofs of Quantumness
based on LWE
over polynomial modulus

Soundness

AHB with
poly modulus

?

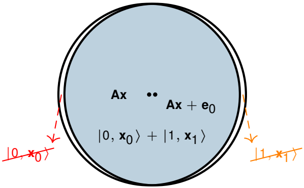
Completeness

?

$\|\mathbf{e}_0\|/q$ non-negligible

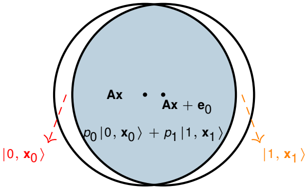
Larger error rate leads to imperfect DCP state

$\|\mathbf{e}_0\|/q$ negligible



- Generate $|0, \mathbf{x}\rangle + |1, \mathbf{x} + \mathbf{s}\rangle$
- Do Hadamard measurement, $(c, \mathbf{d})$ satisfies $c = \mathbf{d}^\top(\mathbf{x}_0 \oplus \mathbf{x}_1)$ overwhelmingly.

$\|\mathbf{e}_0\|/\|\mathbf{e}\|$ non-negligible



- Generate $p_0|0, \mathbf{x}\rangle + p_1|1, \mathbf{x} + \mathbf{s}\rangle$, not close to $|0, \mathbf{x}\rangle + |1, \mathbf{x} + \mathbf{s}\rangle$
- Do Hadamard measurement, $(c, \mathbf{d})$ satisfies $c = \mathbf{d}^\top(\mathbf{x}_0 \oplus \mathbf{x}_1)$ with probability at least 0.8.

- Do standard measurement $\Rightarrow$ still $(0, \mathbf{x}_0)$ or $(1, \mathbf{x}_1)$

Can Quantum Computer pass the check?

- Do standard measurement $\Rightarrow$ still $(0, \mathbf{x}_0)$ or $(1, \mathbf{x}_1)$

- Do Hadamard measurement for N times,

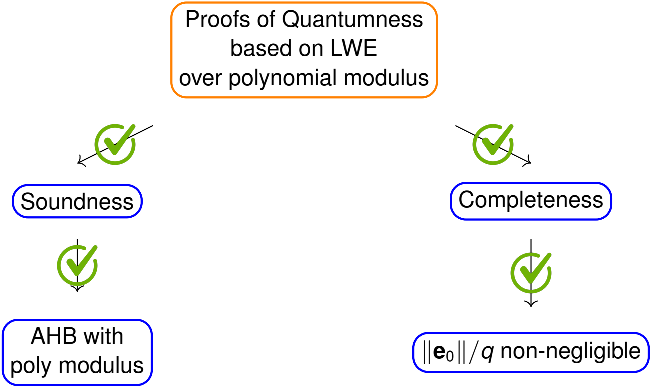
Can Quantum Computer pass the check?

- Do standard measurement $\Rightarrow$ still $(0, \mathbf{x}_0)$ or $(1, \mathbf{x}_1)$

- Do Hadamard measurement for N times,

  * $c = \mathbf{d}^\top \cdot (\mathbf{x}_0 \oplus \mathbf{x}_1) \bmod 2$ with probability at least 0.8.

  * Claim a threshold $0.75N$.


Proofs of Quantumness based on LWE over polynomial modulus
Soundness
Completeness
AHB with poly modulus
$\|\mathbf{e}_0\|/q$ non-negligible

Key Leasing over Classical Channel [CGJL25a]

Leaser

1. Generate mpk, msk

mpk →

← pk

2. Generate pk, sk

3. Encrypt, get ct.

ct →

4. Decrypt

Classical Channel

5. Delete sk, generate cert.

Lessee

6. Verify with cert, msk.

← cert

Key Generation [CGJL25a]

Leaser

1. Generate
$k = (\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}_0)$
$\mathsf{msk} = \mathbf{T}_{\mathbf{A}}$.

$\xrightarrow{k}$

2. Generate
$|0, \mathbf{x}\rangle + |1, \mathbf{x} + \mathbf{s}\rangle$
and $\mathbf{y} = \mathbf{A}\mathbf{x} + \mathbf{e}_u$.
let $\mathsf{pk} = (\mathbf{A}, \mathbf{b}, \mathbf{y})$,
$\mathsf{sk} = |0, \mathbf{x}\rangle + |1, \mathbf{x} + \mathbf{s}\rangle$

Lessee

Key Generation [CGJL25a]

Leaser

1. Generate
$k = (\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}_0)$
$\mathrm{msk} = \mathbf{T}_{\mathbf{A}}$.

$\xrightarrow{k}$

2. Generate
$|0, \mathbf{x}\rangle + |1, \mathbf{x} + \mathbf{s}\rangle$
and $\mathbf{y} = \mathbf{A}\mathbf{x} + \mathbf{e}_u$.
let $\mathrm{pk} = (\mathbf{A}, \mathbf{b}, \mathbf{y})$,
$\mathrm{sk} = |0, \mathbf{x}\rangle + |1, \mathbf{x} + \mathbf{s}\rangle$

Lessee

Polynomial?

Key Generation [CGJL25a]

Leaser

1. Generate
$k = (\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}_0)$
$\mathrm{msk} = \mathbf{T}_{\mathbf{A}}$.

$\xrightarrow{k}$

2. Generate
$p_0|0, \mathbf{x}\rangle + p_1|1, \mathbf{x} + \mathbf{s}\rangle$
and $\mathbf{y} = \mathbf{A}\mathbf{x} + \mathbf{e}_u$.
let $\mathrm{pk} = (\mathbf{A}, \mathbf{b}, \mathbf{y})$,
$\mathrm{sk} = p_0|0, \mathbf{x}\rangle + p_1|1, \mathbf{x} + \mathbf{s}\rangle$

Lessee

Polynomial?

- The secret key is of form $p_0|0,\mathbf{x}\rangle + p_1|1,\mathbf{x}+\mathbf{s}\rangle = \sum_{b\in\{0,1\}} p_b|b,\mathbf{x}_b\rangle$.
- The ciphertext is of form $\mathsf{ct}_1 = \mathbf{r}^\top\mathbf{A}$, $\mathsf{ct}_2 = \mathbf{r}^\top\mathbf{b}$, $\mathsf{ct}_3 = \mathbf{r}^\top\mathbf{y} + \mathbf{e}^\star + \lceil q/2 \rfloor m$.

$$
\begin{tikzcd}
 & \left(\sum_{b\in\{0,1\}} p_b|b,\mathbf{x}_b\rangle\right) \otimes |\mathrm{Dec}(\mathsf{sk}=\mathbf{x}_b, \mathsf{ct}=(\mathsf{ct}_1, \mathsf{ct}_3 + b\cdot\mathsf{ct}_2))\rangle \arrow[dl, "b=0"'] \arrow[dr, "b=1"] & \\
|\mathrm{Dec}(\mathsf{sk}=\mathbf{x}, \mathsf{ct}_{\mathsf{pk}=(\mathbf{A},\mathbf{y})} = (\mathsf{ct}_1, \mathsf{ct}_3))\rangle \arrow[dr, "="] & & |\mathrm{Dec}(\mathsf{sk}=\mathbf{x}+\mathbf{s}, \mathsf{ct}_{\mathsf{pk}=(\mathbf{A},\mathbf{b}+\mathbf{y})} = (\mathsf{ct}_1, \mathsf{ct}_3+\mathsf{ct}_2))\rangle \arrow[dl, "="'] \\
 & |m\rangle &
\end{tikzcd}
$$

⋆ This is another noise flooding that causes subexponential reduction loss.

How to delete? [CGJL25a]

$$
\begin{tikzcd}
 & {|0,\mathbf{x}\rangle + |1,\mathbf{x}+\mathbf{s}\rangle} \arrow[dl, dashed, "\text{two keys}"'] \arrow[dr, "\text{Hadamard Measure}"] & \\
(b, \mathbf{x}+b\mathbf{s}) & & (c, \mathbf{d}) \arrow[ll, "\times"] \arrow[d] \\
 & & \text{Leasor: check } c = \langle \mathbf{d}, J(\mathbf{x}) \oplus J(\mathbf{x}+\mathbf{s}) \rangle
\end{tikzcd}
$$

Due to AHB, one getting $(c, \mathbf{d})$ cannot get either $(b, \mathbf{x}+b\mathbf{s})$, hence cannot decrypt.

How to delete? [CGJL25a]

$$
\begin{tikzcd}
 & {|0,\mathbf{x}\rangle + |1,\mathbf{x}+\mathbf{s}\rangle} \arrow[dl, dashed, "\text{two keys}"'] \arrow[dr, "\text{Hadamard Measure}"] & \\
(b, \mathbf{x}+b\mathbf{s}) & & (c,\mathbf{d}) \arrow[ll, "\times" marking] \arrow[d] \\
 & & {\text{Leasor: check } c = \langle \mathbf{d}, J(\mathbf{x}) \oplus J(\mathbf{x}+\mathbf{s})\rangle}
\end{tikzcd}
$$

Due to AHB, one getting $(c, \mathbf{d})$
cannot get either $(b, \mathbf{x} + b\mathbf{s})$,
hence cannot decrypt.

Polynomial?

How to delete? [CGJL25a]

$$p_0|0, \mathbf{x}\rangle + p_1|1, \mathbf{x} + \mathbf{s}\rangle$$

two keys

Hadamard
Measure

$$(b, \mathbf{x} + b\mathbf{s}) \quad \not\longleftarrow \quad (c, \mathbf{d})$$

Due to AHB, one getting $(c, \mathbf{d})$
cannot get either $(b, \mathbf{x} + b\mathbf{s})$,
hence cannot decrypt.

Leasor: check
$c = \langle \mathbf{d}, J(\mathbf{x}) \oplus J(\mathbf{x} + \mathbf{s}) \rangle$

Polynomial?

How to delete? [CGJL25a]

$$
\begin{tikzcd}
 & p_0|0,\mathbf{x}\rangle + p_1|1,\mathbf{x}+\mathbf{s}\rangle \arrow[dl, dashed, "\text{two keys}"'] \arrow[dr, "\text{Hadamard Measure}"] & \\
(b, \mathbf{x} + b\mathbf{s}) & & (c, \mathbf{d}) \arrow[ll, "\times" marking] \arrow[d] \\
 & & c = \langle \mathbf{d}, J(\mathbf{x}) \oplus J(\mathbf{x}+\mathbf{s}) \rangle
\end{tikzcd}
$$

Due to AHB, one getting $(c, \mathbf{d})$
cannot get either $(b, \mathbf{x} + b\mathbf{s})$,
hence cannot decrypt.

$c = \langle \mathbf{d}, J(\mathbf{x}) \oplus J(\mathbf{x}+\mathbf{s}) \rangle$
with probability at least 0.8.

Polynomial?

How to delete? [CGJL25a]

$$\begin{tikzcd}
 & p_0|0,\mathbf{x}\rangle + p_1|1,\mathbf{x}+\mathbf{s}\rangle \arrow[dl, dashed, "\text{two keys}"'] \arrow[dr, "\text{Hadamard Measure}"] & \\
(b, \mathbf{x}+b\mathbf{s}) & & (c,\mathbf{d}) \arrow[ll, "\times"] \arrow[d] \\
 & & c = \langle \mathbf{d}, J(\mathbf{x}) \oplus J(\mathbf{x}+\mathbf{s})\rangle
\end{tikzcd}$$

with probability at least 0.8.

Due to AHB, one getting $(c, \mathbf{d})$ cannot get either $(b, \mathbf{x} + b\mathbf{s})$, hence cannot decrypt.

Set a threshold 0.75

Polynomial?

Polynomial modulus for PoQ and PKE-SKL

Schemes	Assumptions	Modulus
PoQ in [BCM+18]	LWE	superpoly
PoQ in [BKVV20]	Random Oracle & Ring-LWE	poly
PoQs in [KMCVY22; KLVY23; BGK+23]	Bell's inequality & (*Ring*-)LWE	poly
PoQ in [PWYZ24]	LWE	poly
PKE-SKL in [CGJL25a]	LWE	subexp
PKE-SKL in [PWYZ24]	LWE	poly

Future works?

- Adaptive hardcore bit over rings (e.g., Ring-LWE)?
- Adaptive hardcore bit from other assumptions (e.g., group action)?
- Smaller soundness with Extrapolated DCP [BKSW18]:

$$|0, \mathbf{x}\rangle + |1, \mathbf{x}+\mathbf{s}\rangle + |2, \mathbf{x}+2\mathbf{s}\rangle + \cdots + |p, \mathbf{x}+p\mathbf{s}\rangle \text{ for } p < q?$$

References I

[AKN+23] Shweta Agrawal, Fuyuki Kitagawa, Ryo Nishimaki, Shota Yamada, and Takashi Yamakawa, Public key encryption with secure key leasing, EUROCRYPT, 2023.

[APV23] Prabhanjan Ananth, Alexander Poremba, and Vinod Vaikuntanathan, Revocable cryptography from learning with errors, TCC, 2023.

[Bar21] James Bartusek, Secure quantum computation with classical communication, TCC, 2021.

[BCM+18] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh V. Vazirani, and Thomas Vidick, A cryptographic test of quantumness and certifiable randomness from a single quantum device, FOCS, 2018.

[BD20] Zvika Brakerski and Nico Döttling, Hardness of LWE on General Entropic Distributions, EUROCRYPT, 2020.

[BGK+23] Zvika Brakerski, Alexandru Gheorghiu, Gregory D. Kahanamoku-Meyer, Eitan Porat, and Thomas Vidick, Simple tests of quantumness also certify qubits, CRYPTO, 2023.

[BJK+25] Shi Bai, Hansraj Jangir, Elena Kirshanova, Tran Ngo and William Youmans, A Quasi-polynomial Time Algorithm for the Extrapolated Dihedral Coset Problem over Power-of-Two Moduli, CRYPTO, 2025.

[BNP18] Xavier Bonnetain and María Naya-Plasencia, Hidden Shift Quantum Cryptanalysis and Implications, ASIACRYPT, 2018.

[Bon19] Xavier Bonnetain, Hidden Structures and Quantum Cryptanalysis, PhD thesis, 2019.

[BKSW18] Zvika Brakerski, Elena Kirshanova, Damien Stehlé, and Weiqiang Wen, Learning with errors and extrapolated dihedral cosets, PKC, 2018.

[BKVV20] Zvika Brakerski, Venkata Koppula, Umesh V. Vazirani, and Thomas Vidick, Simpler proofs of quantumness, TQC, 2020.

[CGJL25a] Orestis Chardouvelis, Vipul Goyal, Aayush Jain, and Jiahui Liu, Quantum key leasing for PKE and FHE with a classical lessor, EUROCRYPT, 2025.

[HPS11] Guillaume Hanrot, Xavier Pujol, and Damien Stehlé, Analyzing blockwise lattice algorithms using dynamical systems, CRYPTO, 2011.

[HS07] Guillaume Hanrot and Damien Stehlé, Improved analysis of kannan's shortest lattice vector algorithm, CRYPTO, 2007.

[KLVY23] Yael Kalai, Alex Lombardi, Vinod Vaikuntanathan, and Lisa Yang, Quantum advantage from any non-local game, STOC, 2023.

[KMCVY22] Gregory D. Kahanamoku-Meyer, Soonwon Choi, Umesh V. Vazirani, and Norman Y. Yao, Classically verifiable quantum advantage from a computational bell test, Nat. Phys., 2022.

[Mah18] Urmila Mahadev, Classical verification of quantum computations, FOCS, 2018.

[PWYZ24] Duong Hieu Phan, Weiqiang Wen, Xingyu Yan, and Jinwei Zheng, Adaptive hardcore bit and quantum key leasing over classical channel from LWE with polynomial modulus, ASIACRYPT, 2024.

[Reg02] Oded Regev, Quantum computation and lattice problems, FOCS, 2002.

[Reg05] ———, On lattices, learning with errors, random linear codes, and cryptography, STOC, 2005.