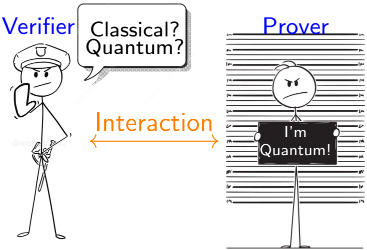
Adaptive Hardcore Bit and Quantum Key Leasing over Classical Channel from LWE with Polynomial Modulus

Duong Hieu Phan[1], Weiqiang Wen[1], Xingyu Yan[2] and **Jinwei Zheng**[1]

[1]Telecom Paris, IP Paris, [2]Beijing University of Posts and Telecommunications
[1]{hieu.phan, weiqiang.wen, jinwei.zheng} @telecom-paris.fr
[2]yanxy2020@bupt.edu.cn

December 2024, IACR Asiacrypt 2024

What is Proofs of Quantumness



Schemes	Assumptions
[BCM+18]	LWE
[BKVV20]	Random Oracle & Ring-LWE
[KMCVY22, KLVY23,BGKM+23]	Bell's inequality & (*Ring*-)LWE

What is Secure Key Leasing?

Revoke the key

Schemes	Channels
[APV23,AKN$^+$23]	Quantum Channel
[CGJL24]	Classical Channel

Our Results

Schemes	Assumptions	Modulus
[BCM+18]'s PoQ	LWE	superpoly
[BKVV20]'s PoQ	Random Oracle & Ring-LWE	poly
[KMCVY22,KLVY23 BGKM+23]'s PoQs	Bell's inequality & (*Ring*-)LWE	poly
Our PoQ	LWE	poly
[CGJL23]'s PKE-SKL	LWE	superpoly
Our PKE-SKL	LWE	poly

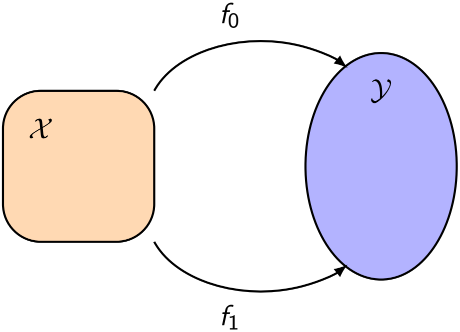
* PoQ: Proofs of Quantumness;
* PKE-SKL: Public Key Encryption with Secure Key Leasing.

Road Map

1. Proofs of Quantumness
   - Claw-Free Function
   - Noisy Claw-Free Function
   - Proofs of Quantumness
   - Our improvements on Proofs of Quantumness
2. Public Key Encryption with Secure Key Leasing
   - What is PKE-SKL?
   - How to realize?
3. Future works?

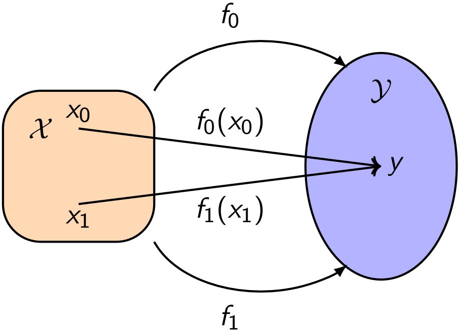
1. Proofs of Quantumness
   - Claw-Free Function
   - Noisy Claw-Free Function
   - Proofs of Quantumness
   - Our improvements on Proofs of Quantumness
2. Public Key Encryption with Secure Key Leasing
   - What is PKE-SKL?
   - How to realize?
3. Future works?

Claw-Free Functions



A pair of public injective functions f_0 and f_1 with the same range. It has the following two essential properties:

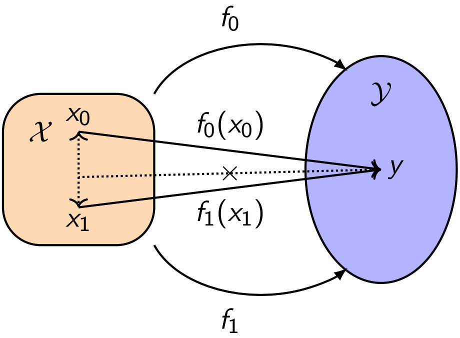
Claw-Free Functions



A pair of public injective functions f_0 and f_1 with the same range. It has the following two essential properties:

- **Claw:**
  For any $\mathbf{y}$ in the range, $\exists \mathbf{x}_0, \mathbf{x}_1$, $f_0(\mathbf{x}_0) = f_1(\mathbf{x}_1) = \mathbf{y}$.

Claw-Free Functions



A pair of public injective functions f_0 and f_1 with the same range. It has the following two essential properties:

- **Claw:**
  For any $\mathbf{y}$ in the range, $\exists \mathbf{x}_0, \mathbf{x}_1$, $f_0(\mathbf{x}_0) = f_1(\mathbf{x}_1) = \mathbf{y}$.
- **Claw-Free:**
  For any $\mathbf{y}$ in the range, hard to find $(\mathbf{x}_0, \mathbf{x}_1)$: $f_0(\mathbf{x}_0) = f_1(\mathbf{x}_1) = \mathbf{y}$.

LWE-based Noisy Claw-Free Function [BCM+18]:

Given $k = (\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e}_0)$, **can we get Claw-Free function?**

-

LWE-based Noisy Claw-Free Function [BCM+18]:

Given $k = (\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e}_0)$,

- $f_{k,0}(\mathbf{x}) = \mathbf{A}\mathbf{x}$
  $f_{k,1}(\mathbf{x}) = \mathbf{A}\mathbf{x} + b(\mathbf{A}\mathbf{s} + \mathbf{e}_0)$**?**

$f_{k,0}(\mathbf{x}) \quad \bullet \bullet \, f_{k,1}(\mathbf{x} - \mathbf{s})$

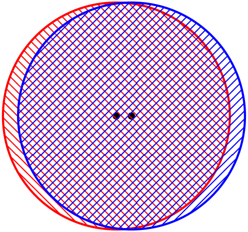
Not claw,

but close!

LWE-based Noisy Claw-Free Function [BCM+18]:

Given $k = (\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e}_0)$, the distribution function:

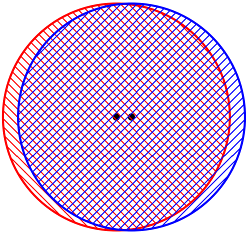
- $\forall \mathbf{y} \in \mathbb{Z}_q^m$: $(f'_{k,b}(\mathbf{x}))(\mathbf{y}) = D_{\mathbb{Z}^m, r, 2r\sqrt{m}}(\mathbf{y} - \mathbf{A}\mathbf{x} - b \cdot (\mathbf{A}\mathbf{s} + \mathbf{e}_0))$

$f'_{k,0}(\mathbf{x})$  $f'_{k,1}(\mathbf{x} - \mathbf{s})$

LWE-based Noisy Claw-Free Function [BCM+18]:

Given $k = (\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e}_0)$,

- $\forall \mathbf{y} \in \mathbb{Z}_q^m$: $(f'_{k,b}(\mathbf{x}))(\mathbf{y}) = D_{\mathbb{Z}^m, r, 2r\sqrt{m}}(\mathbf{y} - \mathbf{A}\mathbf{x} - b \cdot (\mathbf{A}\mathbf{s} + \mathbf{e}_0))$

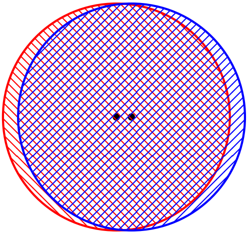


- Claw: $supp(f'_{k,0}(\mathbf{x})) \bigcap supp(f'_{k,1}(\mathbf{x} - \mathbf{s})) \neq \varnothing$.

LWE-based Noisy Claw-Free Function [BCM+18]:

Given $k = (\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e}_0)$,

- $\forall \mathbf{y} \in \mathbb{Z}_q^m$: $(f'_{k,b}(\mathbf{x}))(\mathbf{y}) = D_{\mathbb{Z}^m, r, 2r\sqrt{m}}(\mathbf{y} - \mathbf{A}\mathbf{x} - b \cdot (\mathbf{A}\mathbf{s} + \mathbf{e}_0))$

$f'_{k,0}(\mathbf{x})$  $f'_{k,1}(\mathbf{x} - \mathbf{s})$

- Claw: $supp(f'_{k,0}(\mathbf{x})) \bigcap supp(f'_{k,1}(\mathbf{x} - \mathbf{s})) \neq \varnothing$.
- Claw-Free: Finding a claw $\Rightarrow$ breaking LWE.

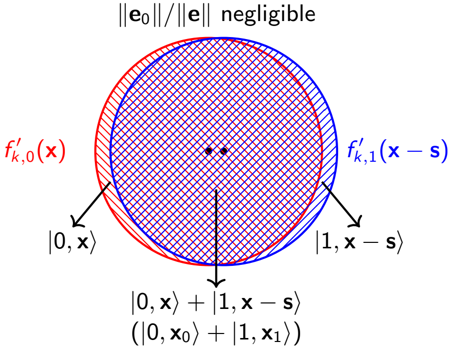
How to generate claw in superposition? [BCM+18]

- Generate $\sum_{\substack{b\in\{0,1\}\\ \mathbf{x}\in\mathcal{X}}} \sum_{\|\mathbf{e}\|\leq 2r\sqrt{m}} \sqrt{D_{\mathbb{Z}^m,r}(\mathbf{e})}|b\rangle|\mathbf{x}\rangle|\mathbf{e}\rangle$; [GR02]

How to generate claw in superposition? [BCM+18]

- Generate $\sum_{\substack{b\in\{0,1\}\\ \mathbf{x}\in\mathcal{X}}} \sum_{\|\mathbf{e}\|\leq 2r\sqrt{m}} \sqrt{D_{\mathbb{Z}^m,r}(\mathbf{e})}|b\rangle|\mathbf{x}\rangle|\mathbf{e}\rangle$; [GR02]
- Given $k = (\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e}_0 \bmod q)$ Compute

$$\sum_{\substack{b\in\{0,1\}\\ \mathbf{x}\in\mathcal{X}}} \sum_{\|\mathbf{e}\|\leq 2r\sqrt{m}} \sqrt{D_{\mathbb{Z}^m,r}(\mathbf{e})}|b\rangle|\mathbf{x}\rangle|\underbrace{\mathbf{A}(\mathbf{x}+b\mathbf{s}) + b\mathbf{e}_0 + \mathbf{e}}_{f'_{k,b}(\mathbf{x})}\rangle$$



Measurement $\mathbf{y} = \mathbf{A}\mathbf{x} + \mathbf{e}'$

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

- $\mathbf{d} \sim U(\{0,1\}^{n\lceil \log q \rceil})$, [BCM+18] shows $c = \mathbf{d}^\top \cdot (\mathbf{x}_0 \oplus \mathbf{x}_1) = \langle I_{b,\mathbf{x}_b}(\mathbf{d}), \mathbf{s} \rangle$.

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

- $\mathbf{d} \sim U(\{0,1\}^{n\lceil \log q \rceil})$, [BCM+18] shows $c = \mathbf{d}^\top \cdot (\mathbf{x}_0 \oplus \mathbf{x}_1) = \langle I_{b,\mathbf{x}_b}(\mathbf{d}), \mathbf{s} \rangle$.

Can we get both values of measurements?

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

- $\mathbf{d} \sim U(\{0,1\}^{n\lceil \log q \rceil})$, [BCM+18] shows $c = \mathbf{d}^\top \cdot (\mathbf{x}_0 \oplus \mathbf{x}_1) = \langle I_{b,\mathbf{x}_b}(\mathbf{d}), \mathbf{s} \rangle$.

Can we get both values of measurements? No!

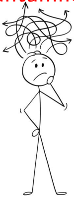
$$
\begin{tikzcd}
 & |0, \mathbf{x}_0\rangle + |1, \mathbf{x}_1\rangle \arrow[dl, "\text{Standard Measure}"'] \arrow[dr, "\text{Hadamard Measure}"] & \\
(b, \mathbf{x}_b) & & (c, \mathbf{d})
\end{tikzcd}
$$

- $\mathbf{d} \sim U(\{0,1\}^{n\lceil \log q \rceil})$, [BCM$^+$18] shows $c = \mathbf{d}^\top \cdot (\mathbf{x}_0 \oplus \mathbf{x}_1) = \langle I_{b,\mathbf{x}_b}(\mathbf{d}), \mathbf{s}\rangle$.

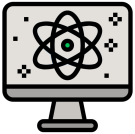
Can we get both values of measurements? No!

- **Adaptive hardcore bit [BCM$^+$18]**: Given $(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e}_0)$ with superpolynomail modulus and $\mathbf{d} \xleftarrow{\$} \{0,1\}^{n\lceil \log q \rceil}$, the adversary picks $(b, \mathbf{x}_b)$, hard to get $c = \mathbf{d}^\top \cdot (\mathbf{x}_0 \oplus \mathbf{x}_1) = \langle I_{b,\mathbf{x}_b}(\mathbf{d}), \mathbf{s}\rangle$.

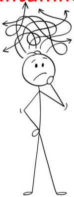
Can we prove the quantumness?



Quantum

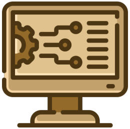


Can we prove the quantumness?

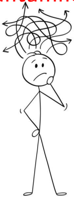


Randomly ask for values under either Hadamard or Standard measurement

Classical

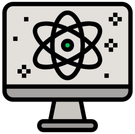


Can we prove the quantumness?



Randomly ask for values under either Hadamard or Standard measurement

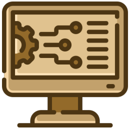
Quantum



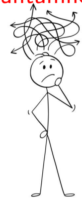
Do either measurement accordingly under quantum computation

$\Longrightarrow$ Completeness

Classical

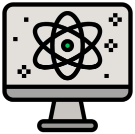


Can we prove the quantumness?



Randomly ask for values under either Hadamard or Standard measurement

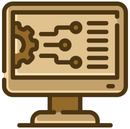
Quantum



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

NTCF-based Proofs of Quantumness[BCM+18]:

For $i \in [N]$, repeat:

1. Generate , $\mathsf{td}_{\mathbf{A}_i}$, $k_i = (\mathbf{A}_i, \mathbf{A}_i\mathbf{s}_i + \mathbf{e}_{0,i})$

$\xrightarrow{k_i}$

2. Generate $|0, \mathbf{x}_{i,0}\rangle + |1, \mathbf{x}_{i,1}\rangle$ measurement $\mathbf{y}_i$

$\xleftarrow{\mathbf{y}_i}$

3. $r_i \leftarrow \{0, 1\}$

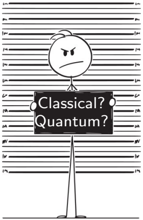
$\xrightarrow{r_i}$

4. 1) $r_i = 0$, Standard measure, $\sigma_{r_i,i} = (b_i, \mathbf{x}_{b_i,i})$
2) $r_i = 1$, Hadamard measure, $\sigma_{r_i,i} = (c, \mathbf{d}_i)$

$\xleftarrow{\sigma_{r_i,i}}$

5. Check validity of the measured values.

Verifier



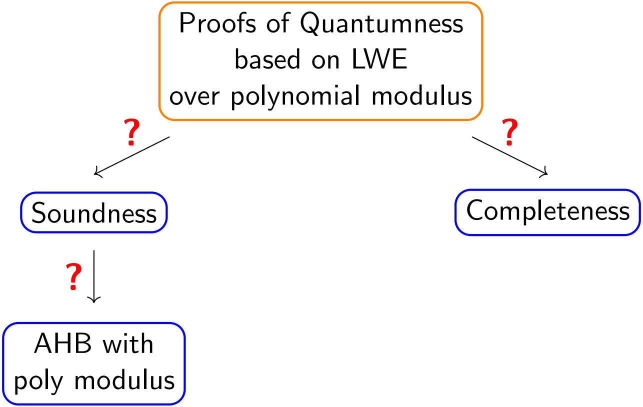
Prover

Proofs of Quantumness
based on LWE
over polynomial modulus

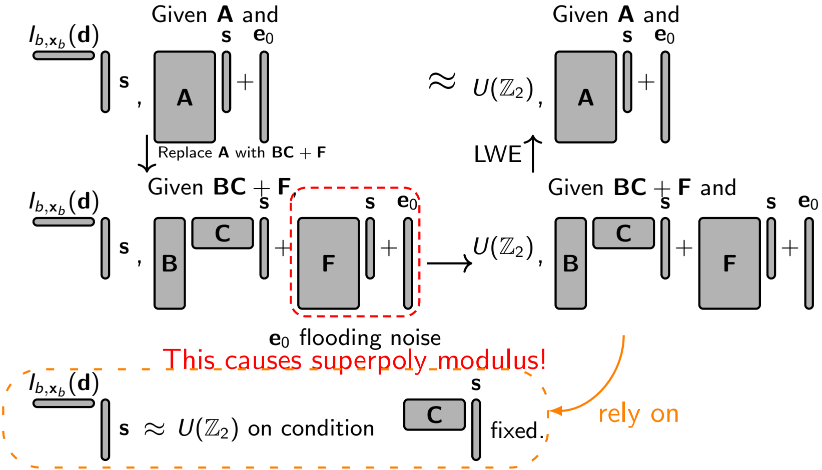
? ?

Soundness

Completeness

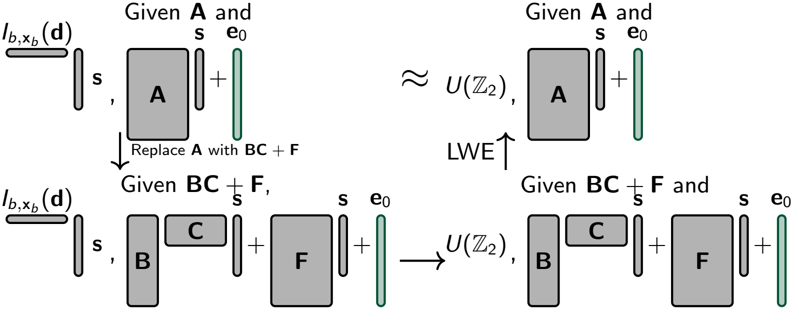

Proofs of Quantumness
based on LWE
over polynomial modulus
?
?
Soundness
Completeness
?
AHB with
poly modulus

Sketch of proof of AHB in [BCM+18]:



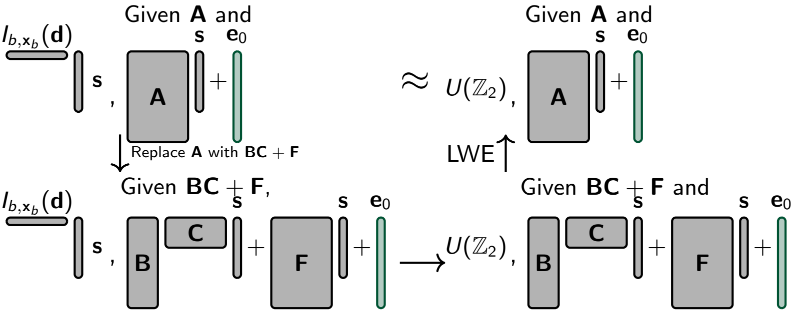
- $\Rightarrow$ Given $(\mathbf{A}, \mathbf{As} + \mathbf{e}_0 \bmod q)$, $\langle I_{b,\mathbf{x}_b}(\mathbf{d}), \mathbf{s}\rangle \approx U(\mathbb{Z}_2) \Rightarrow$ AHB.

Our Proof:



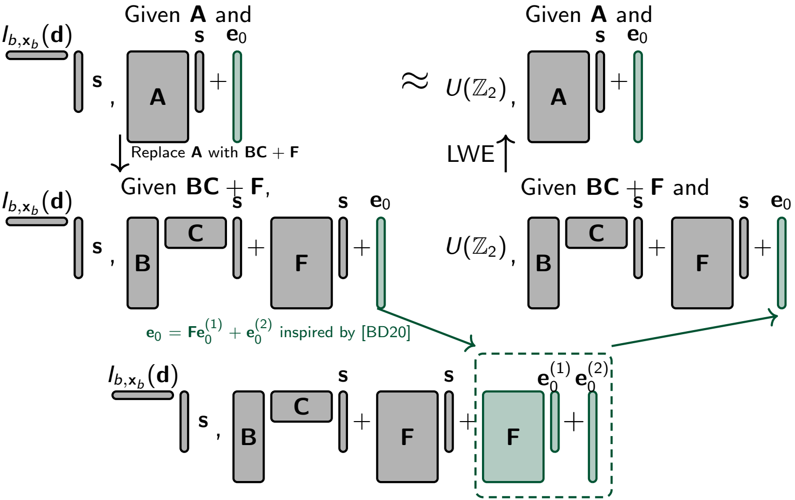
e_0 covers Fs completely, Necessary?

Our Proof:

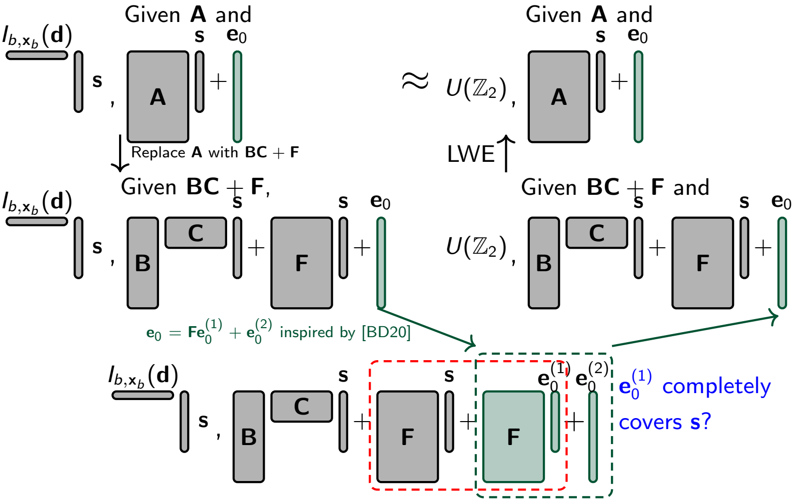


$\mathbf{e}_0$ covers Fs completely, Necessary? **No!**

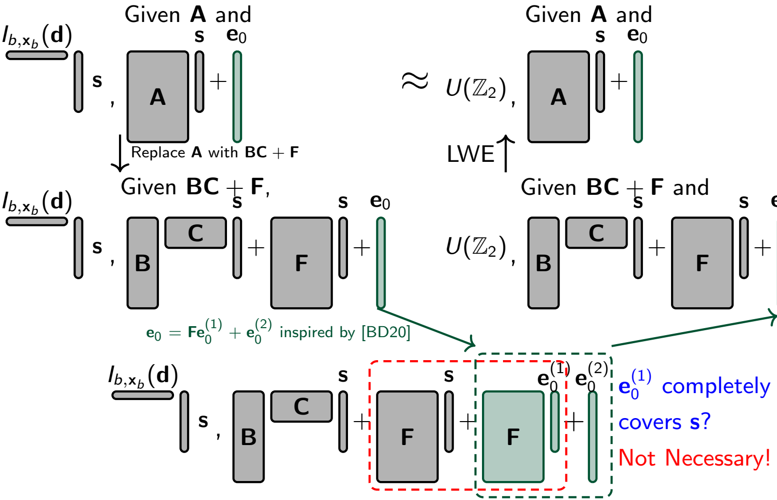
Our Proof:


Given A and
$I_{b,\mathbf{x}_b}(\mathbf{d})$
s
s e0
A
$\approx$
$U(\mathbb{Z}_2)$,
Replace A with BC + F
LWE
Given BC + F,
Given BC + F and
B
C
F
$\mathbf{e}_0 = \mathbf{F}\mathbf{e}_0^{(1)} + \mathbf{e}_0^{(2)}$ inspired by [BD20]
$\mathbf{e}_0^{(1)}$ $\mathbf{e}_0^{(2)}$

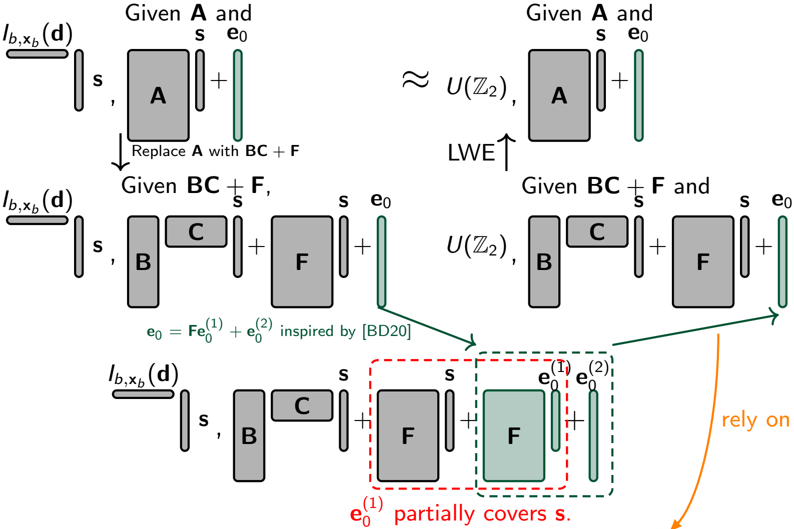
Our Proof:


Given A and
$I_{b,\mathbf{x}_b}(\mathbf{d})$
s
A
$\mathbf{e}_0$
≈
$U(\mathbb{Z}_2)$
Replace A with BC + F
LWE
Given BC + F,
Given BC + F and
B
C
F
$\mathbf{e}_0 = \mathbf{F}\mathbf{e}_0^{(1)} + \mathbf{e}_0^{(2)}$ inspired by [BD20]
$\mathbf{e}_0^{(1)}$
$\mathbf{e}_0^{(2)}$
$\mathbf{e}_0^{(1)}$ completely covers s?

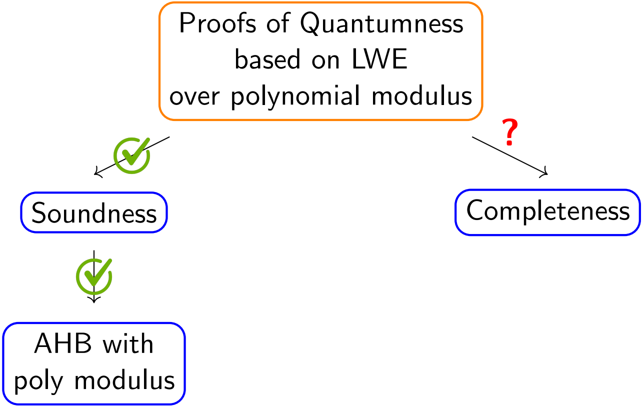
Our Proof:


Given **A** and
$I_{b,\mathbf{x}_b}(\mathbf{d})$
s
e_0
A
$\approx$
$U(\mathbb{Z}_2)$
Replace **A** with **BC** + **F**
LWE
Given **BC** + **F**,
Given **BC** + **F** and
B
C
F
$\mathbf{e}_0 = \mathbf{F}\mathbf{e}_0^{(1)} + \mathbf{e}_0^{(2)}$ inspired by [BD20]
$\mathbf{e}_0^{(1)}$ $\mathbf{e}_0^{(2)}$
$\mathbf{e}_0^{(1)}$ completely covers **s**?
Not Necessary!

Our Proof:



$\langle I_{b,\mathbf{x}_b}(\mathbf{d}), \mathbf{s}\rangle \approx U(\mathbb{Z}_2)$ on condition $\mathbf{Cs}$ 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

Proofs of Quantumness
based on LWE
over polynomial modulus

Soundness

AHB with
poly modulus

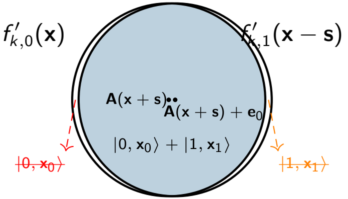
?

Completeness

?

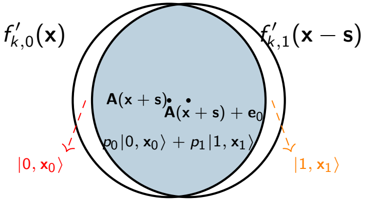
$\|\mathbf{e}_0\|/\|\mathbf{e}\|$ noticeable

$\|\mathbf{e}_0\|/\|\mathbf{e}\|$ negligible [BCM+18]



- 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.

$\|\mathbf{e}_0\|/\|\mathbf{e}\|$ noticeable [BKVV20]



- 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.

Can Quantum Computer pass the check?

- 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_1 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_1 times,
  * $c = \mathbf{d}^\top \cdot (\mathbf{x}_0 \oplus \mathbf{x}_1) \bmod 2$ with probability at least 0.8.
  * Claim a threshold $0.75N_1$.

Proofs of Quantumness based on LWE over polynomial modulus

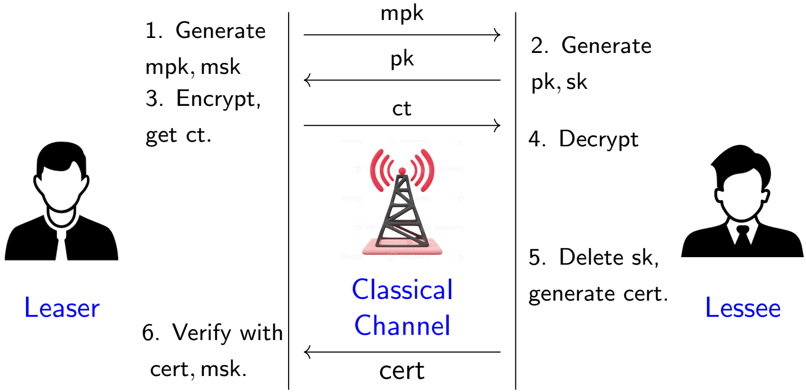
Soundness

AHB with poly modulus

Completeness

$\|\mathbf{e}_0\|/\|\mathbf{e}\|$ noticeable

What is Public Key Encryption with Secure Key Leasing over Classical Channel?[CGJL23]



How to generate key?[CGJL23]

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 $\mathbf{y} = \mathbf{A}\mathbf{x} + \mathbf{e}$.

let $\mathsf{pk} = (\mathbf{A}, \mathbf{b}, \mathbf{y})$,

$\mathsf{sk} = |0, \mathbf{x}\rangle + |1, \mathbf{x} - \mathbf{s}\rangle$

Lessee

How to generate key?[CGJL23]

Leaser

1. Generate

$k = (\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}_0)$

$\mathsf{msk} = \mathbf{T}_{\mathbf{A}}$.

$\xrightarrow{\quad k \quad}$

2. Generate

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

and $\mathbf{y} = \mathbf{A}\mathbf{x} + \mathbf{e}$.

let $\mathsf{pk} = (\mathbf{A}, \mathbf{b}, \mathbf{y})$,

$\mathsf{sk} = |0, \mathbf{x}\rangle + |1, \mathbf{x} - \mathbf{s}\rangle$

Lessee

Polynomial?

How to generate key?[CGJL23]

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

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

and $\mathbf{y} = \mathbf{A}\mathbf{x} + \mathbf{e}$.

let $\mathsf{pk} = (\mathbf{A}, \mathbf{b}, \mathbf{y})$,

$\mathsf{sk} = p_0|0, \mathbf{x}\rangle + p_1|1, \mathbf{x} - \mathbf{s}\rangle$

Lessee

Polynomial?

How to encrypt and decrypt?[CGJL23]

With ciphertext $\mathsf{ct}_1 = \mathbf{r}^\top \mathbf{A}$, $\mathsf{ct}_2 = \mathbf{r}^\top \mathbf{b}$, $\mathsf{ct}_3 = \mathbf{r}^\top \mathbf{y} + \mathbf{e}' + \lceil q/2 \rceil \mu$:

$$\begin{tikzcd}
 & \begin{array}{c}\left(p_0|0,\mathbf{x}\rangle + p_1|1,\mathbf{x}-\mathbf{s}\rangle\right)\\ \otimes|\mathsf{ct}_3 - b\cdot \mathsf{ct}_2\rangle\end{array} \arrow[dl, "b=0"'] \arrow[dr, "b=1"] & \\
|\mathbf{r}^\top \mathbf{A}\mathbf{x} + \mathbf{r}^\top \mathbf{e} + \mathbf{e}' + \lceil q/2 \rceil \mu\rangle \arrow[d, "\text{with } \mathsf{ct}_1,\ \mathbf{x}"'] & & |\mathbf{r}^\top \mathbf{A}(\mathbf{x}-\mathbf{s}) + \mathbf{r}^\top(\mathbf{e}-\mathbf{e}_0) + \mathbf{e}' + \lceil q/2 \rceil \mu\rangle \arrow[d, "\text{with } \mathsf{ct}_1,\ \mathbf{x}-\mathbf{s}"] \\
|\left(\mathbf{r}^\top \mathbf{e} + \mathbf{e}' + \lceil q/2 \rceil \mu\right)/\lceil q/2 \rceil\rangle \arrow[dr, "="] & & |\left(\mathbf{r}^\top(\mathbf{e}-\mathbf{e}_0) + \mathbf{e}' + \lceil q/2 \rceil \mu\right)/\lceil q/2 \rceil\rangle \arrow[dl, "="'] \\
 & |\mu\rangle &
\end{tikzcd}$$

IND-CPA

$$\mathsf{Enc}(\mathsf{pk}, 0) \quad \xleftarrow{\text{indistinguishable}} \!\!\!\!\rightarrow \quad \mathsf{Enc}(\mathsf{pk}, 1)$$

$$\Uparrow$$

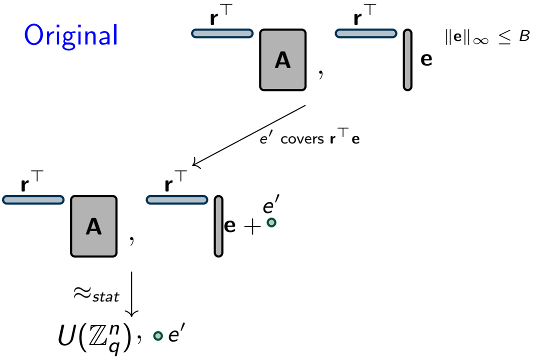
$$\mathsf{ct}_3 = \mathbf{r}^\top \mathbf{y} + \mathbf{e}' = \mathbf{r}^\top \mathbf{A}\mathbf{x} + \mathbf{r}^\top \mathbf{e} + \mathbf{e}' \quad \xleftarrow{\text{indistinguishable}} \!\!\!\!\rightarrow \quad \mathsf{ct}_3 = \mathbf{r}^\top \mathbf{y} + \mathbf{e}' + \lceil q/2 \rceil = \mathbf{r}^\top \mathbf{A}\mathbf{x} + \mathbf{r}^\top \mathbf{e} + \mathbf{e}' + \lceil q/2 \rceil$$

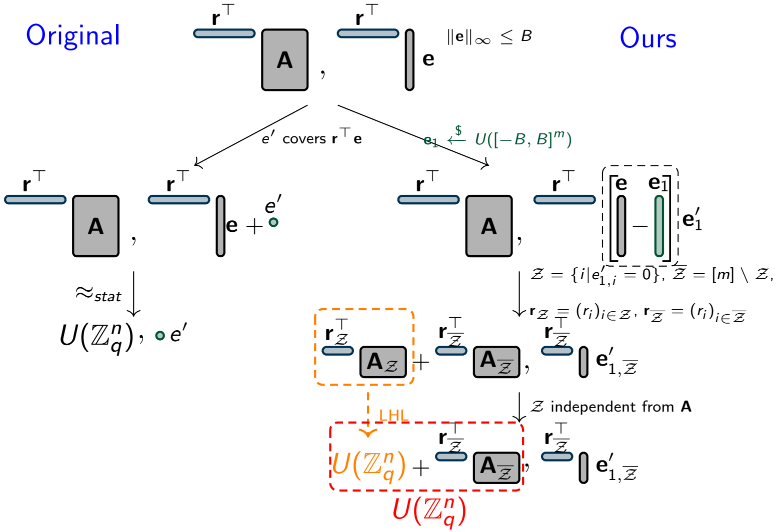
$$\Uparrow \text{ One-time Pad}$$

$$\mathbf{r}^\top \mathbf{A}\mathbf{x} + \mathbf{r}^\top \mathbf{e} + \mathbf{e}' \quad \xleftarrow{\text{indistinguishable}} \!\!\!\!\rightarrow \quad U(\mathbb{Z}_q)$$

$$\Uparrow \text{ [CGJL23]}$$

$$\mathbf{r}^\top \mathbf{A} \approx U(\mathbb{Z}_q^n) \text{ condition on } \mathbf{r}^\top \mathbf{e}$$


Original
$\mathbf{r}^\top$ $\mathbf{A}$, $\mathbf{r}^\top$ $\mathbf{e}$
$\|\mathbf{e}\|_\infty \leq B$
e' covers $\mathbf{r}^\top \mathbf{e}$
$\mathbf{r}^\top$ $\mathbf{A}$, $\mathbf{r}^\top$ $\mathbf{e} + e'$
$\approx_{stat}$
$U(\mathbb{Z}_q^n)$, e'


Original
Ours
$\mathbf{r}^\top \mathbf{A}$, $\mathbf{r}^\top \mathbf{e}$
$\|\mathbf{e}\|_\infty \le B$
e' covers $\mathbf{r}^\top \mathbf{e}$
$\mathbf{e}_1 \xleftarrow{\$} U([-B, B]^m)$
$\mathbf{r}^\top \mathbf{A}$, $\mathbf{r}^\top \mathbf{e} + e'$
$\approx_{stat}$
$U(\mathbb{Z}_q^n)$, e'
$\mathbf{r}^\top \mathbf{A}$, $\mathbf{r}^\top [\mathbf{e} - \mathbf{e}_1]$ $\mathbf{e}'_1$
$\mathcal{Z} = \{i | e'_{1,i} = 0\}$, $\overline{\mathcal{Z}} = [m] \setminus \mathcal{Z}$,
$\mathbf{r}_{\mathcal{Z}} = (r_i)_{i \in \mathcal{Z}}$, $\mathbf{r}_{\overline{\mathcal{Z}}} = (r_i)_{i \in \overline{\mathcal{Z}}}$
$\mathbf{r}_{\mathcal{Z}}^\top \mathbf{A}_{\mathcal{Z}} + \mathbf{r}_{\overline{\mathcal{Z}}}^\top \mathbf{A}_{\overline{\mathcal{Z}}}$, $\mathbf{r}_{\overline{\mathcal{Z}}}^\top \mathbf{e}'_{1,\overline{\mathcal{Z}}}$
$\mathcal{Z}$ independent from $\mathbf{A}$
LHL
$U(\mathbb{Z}_q^n) + \mathbf{r}_{\overline{\mathcal{Z}}}^\top \mathbf{A}_{\overline{\mathcal{Z}}}$, $\mathbf{r}_{\overline{\mathcal{Z}}}^\top \mathbf{e}'_{1,\overline{\mathcal{Z}}}$
$U(\mathbb{Z}_q^n)$

How to delete?[CGJL23]

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

two keys

Hadamard Measure

$(b, \mathbf{x} - b\mathbf{s})$

$(c, \mathbf{d})$

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

Leasor: check $c = \mathbf{d}^\top(\mathbf{x} \oplus (\mathbf{x} - \mathbf{s}))$

How to delete?[CGJL23]

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

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

Polynomial?

How to delete?[CGJL23]

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

two keys

Hadamard
Measure

$(b, \mathbf{x} - b\mathbf{s})$ $\xleftarrow{\times}$ $(c, \mathbf{d})$

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

Leasor: check
$c = \mathbf{d}^\top(\mathbf{x} \oplus (\mathbf{x} - \mathbf{s}))$

Polynomial?

How to delete?[CGJL23]

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

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.

$$c = \mathbf{d}^\top(\mathbf{x} \oplus (\mathbf{x} - \mathbf{s}))$$
with probability at least 0.8.

Polynomial?

How to delete?[CGJL23]

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

two keys

Hadamard
Measure

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

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

$c = \mathbf{d}^\top(\mathbf{x} \oplus (\mathbf{x} - \mathbf{s}))$
with probability at least 0.8.

Set a threshold 0.75

Polynomial?

Future works?

- Applications of Noticeable NTCF?
  - Efficient Revocable quantum digital signature based on Noticeable NTCF?
  - Quantum delegated computation based on NTCF?
- Applications of Secure key leasing?
  - Revocable broadcast encryption?
- ......

[AKN+23] S. Agrawal et al. "Public Key Encryption with Secure Key Leasing", Eurocrypt'23.

[AMR23] N. Alamati et al. "Candidate trapdoor claw-free functions from group actions with applications to quantum protocols", TCC'22.

[APV23] P. Ananth et al. "Revocable cryptography from learning with errors", TCC'23.

[BCM+18] Z. Brakerski et al. "A Cryptographic Test of Quantumness and Certifiable Randomness from a Single Quantum Device", FOCS'18.

[BD20] Z. Brakerski et al. "Hardness of LWE on general entropic distributions", Eurocrypt'20.

[BGKM+23] Z. Brakerski et al. "Simple tests of quantumness also certify qubits", Crypto'23.

[BKVV20] Z. Brakerski et al. "Simpler Proofs of Quantumness", TQC'20.

[CGJL23] O. Chardouveils et al. "Quantum key leasing for pke and fhe with a classical lessor", QCrypt'24.

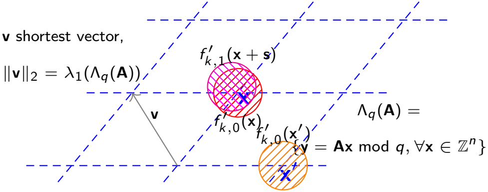
[GR02] L. Grover et al."Creating superpositions that correspond to efficiently integrable probability distributions", https://arxiv.org/pdf/quant-ph/0208112

[KMC+22] G. Kahanamoku-Meyer et al. "Classically verifiable quantum advantage from a computational bell test", Nature Physics'22.

[KLVY23] Y. Kalai et al. "Quantum advantage from any non-local game", STC'23.

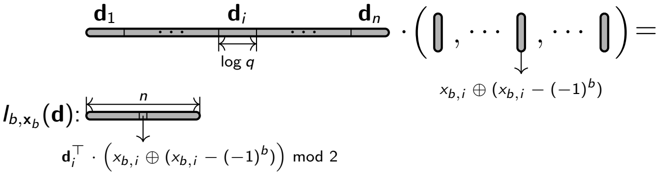
[Reg05] O. Regev "On lattices, learning with errors, random linear codes, and cryptography", STOC'05.

Questions?



- Injection: Since $\|\mathbf{e}\| \ll \lambda_1(\Lambda_q(\mathbf{A}))$, for $\mathbf{x} \neq \mathbf{x}'$, $supp(f'_{k,b}(\mathbf{x})) \bigcap supp(f'_{k,b'}(\mathbf{x}')) = \varnothing,\ b, b' \in \{0,1\}$.

- Given $(b, \mathbf{x}_b, \mathbf{d})$, compute
$I_{b,\mathbf{x}_b}(\mathbf{d}) = \left(\mathbf{d}_i^\top \cdot \left(x_{b,i} \oplus (x_{b,i} - (-1)^b)\right) \bmod 2\right)_{i\in[n]}$



- [BCM+18] shows $c = \mathbf{d}^\top \cdot (\mathbf{x}_0 \oplus \mathbf{x}_1) = \langle I_{b,\mathbf{x}_b}(\mathbf{d}), \mathbf{s}\rangle$.