# Revocable Cryptography from Learning with Errors

Prabhanjan Ananth, Alexander Poremba, Vinod Vaikuntanathan

# Unclonable Cryptography

*Leveraging the no-cloning principle of quantum mechanics to build fascinating cryptographic primitives.*

# Unclonable Cryptography

*Leveraging the no-cloning principle of quantum mechanics*
*to build fascinating cryptographic primitives.*

| Quantum money [Wie83] | Unclonable encryption [Got02] | Copy Protection [Aar09] | Certified deletion [BI19] | Software leasing [**A**LP21] |
|---|---|---|---|---|
| 1983 | 2002 | 2009 | 2019 | 2020 |

# Unclonable Cryptography

*Leveraging the no-cloning principle of quantum mechanics to build fascinating cryptographic primitives.*

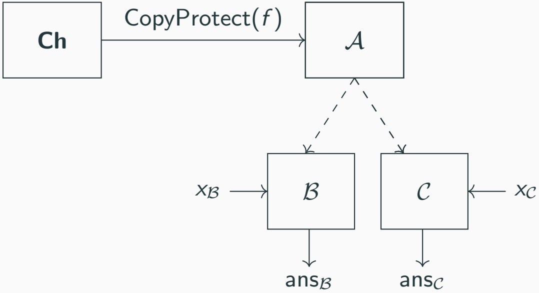
| 1983 | 2002 | 2009 | 2019 | 2020 |
|---|---|---|---|---|
| Quantum money [Wie83] | Unclonable encryption [Got02] | **Copy Protection** [Aar09] | Certified deletion [BI19] | Software leasing [**A**LP21] |

# Quantum Copy-Protection

Quantum no-cloning $\rightarrow$ Preventing Illegal Distribution of Software

# Quantum Copy-Protection

Quantum no-cloning $\rightarrow$ Preventing Illegal Distribution of Software




$\mathcal{A}$ creates a bipartite state: one partition to $\mathcal{B}$ and the other to $\mathcal{C}$

$(\mathcal{A}, \mathcal{B}, \mathcal{C})$ wins if $\text{ans}_{\mathcal{B}} = f(x_{\mathcal{B}})$ and $\text{ans}_{\mathcal{C}} = f(x_{\mathcal{C}})$.

# Quantum Copy-Protection

- Introduced by Aaronson in 2009.

# Quantum Copy-Protection

- Introduced by Aaronson in 2009.
- Impossibility for Contrived Unlearnable Functionalities [**A**-LaPlaca'21].

# Quantum Copy-Protection

- Introduced by Aaronson in 2009.
- Impossibility for Contrived Unlearnable Functionalities [**A**-LaPlaca'21].
- Feasibility: Copy-Protection for Pseudorandom Functions [Coladangelo-Liu-Liu-Zhandry'21]
- Feasibility: Copy-Protection for Decryption Functionalities [Coladangelo-Liu-Liu-Zhandry'21]
- Feasibility: Copy-Protection for Signing Functionalities [Liu-Liu-Qian-Zhandry'21]

# Quantum Copy-Protection

- Introduced by Aaronson in 2009.
- Impossibility for Contrived Unlearnable Functionalities [**A**-LaPlaca'21].
- Feasibility: Copy-Protection for Pseudorandom Functions **(assumes iO)** [Coladangelo-Liu-Liu-Zhandry'21]
- Feasibility: Copy-Protection for Decryption Functionalities **(assumes iO)** [Coladangelo-Liu-Liu-Zhandry'21]
- Feasibility: Copy-Protection for Signing Functionalities **(assumes iO)** [Liu-Liu-Qian-Zhandry'21]

# Quantum Copy-Protection

- Introduced by Aaronson in 2009.

- Impossibility for Contrived Unlearnable Functionalities [**A**-LaPlaca'21].

- Feasibility: Copy-Protection for Pseudorandom Functions **(assumes iO)** [Coladangelo-Liu-Liu-Zhandry'21]
- Feasibility: Copy-Protection for Decryption Functionalities **(assumes iO)** [Coladangelo-Liu-Liu-Zhandry'21]
- Feasibility: Copy-Protection for Signing Functionalities **(assumes iO)** [Liu-Liu-Qian-Zhandry'21]

**Basing post-quantum iO on concrete assumptions: challenging open problem!**

**Our Goal**

- Weaker (yet meaningful) definitions of copy-protection
- Base it on weaker assumptions

**Our Goal**

- Weaker (yet meaningful) definitions of copy-protection
- Base it on weaker assumptions

**Our Work: Revocable Cryptography from Learning With Errors**

**Our Goal**

- Weaker (yet meaningful) definitions of copy-protection
- Base it on weaker assumptions

## Our Work: Revocable Cryptography from Learning With Errors

- Revocable Public-Key Encryption
- Revocable Fully Homomorphic Encryption
- Revocable Pseudorandom Functions

# Revocable Public-Key Encryption

Informal:

- Challenger gives a quantum decryption key $|\psi_{\mathsf{sk}}\rangle$ to adversary $\mathcal{A}$.

# Revocable Public-Key Encryption

Informal:

- Challenger gives a quantum decryption key $|\psi_{\mathsf{sk}}\rangle$ to adversary $\mathcal{A}$.
- **Revocation phase**:
  - $\mathcal{A}$ returns a state $\rho$ back to the challenger.
  - Challenger checks if $\rho$ is the same as $|\psi_{\mathsf{sk}}\rangle$ by performing a projective measurement $\mathcal{M}$.
  - The resulting residual state handed over to $\mathcal{C}$.

# Revocable Public-Key Encryption

Informal:

- Challenger gives a quantum decryption key $|\psi_{\mathsf{sk}}\rangle$ to adversary $\mathcal{A}$.
- **Revocation phase**:
  - $\mathcal{A}$ returns a state $\rho$ back to the challenger.
  - Challenger checks if $\rho$ is the same as $|\psi_{\mathsf{sk}}\rangle$ by performing a projective measurement $\mathcal{M}$.
  - The resulting residual state handed over to $\mathcal{C}$.
- **Security Guarantee**: the following should not simultaneously hold:
  - Revocation succeeds and,
  - $\mathcal{C}$ can break the semantic security of public-key encryption.

# Revocable Public-Key Encryption

Informal:

- Challenger gives a quantum decryption key $|\psi_{\mathsf{sk}}\rangle$ to adversary $\mathcal{A}$.
- **Revocation phase**:
  - $\mathcal{A}$ returns a state $\rho$ back to the challenger.
  - Challenger checks if $\rho$ is the same as $|\psi_{\mathsf{sk}}\rangle$ by performing a projective measurement $\mathcal{M}$.
  - The resulting residual state handed over to $\mathcal{C}$.
- **Security Guarantee**: the following should not simultaneously hold:
  - Revocation succeeds and,
  - $\mathcal{C}$ can break the semantic security of public-key encryption.

# Revocable Public-Key Encryption

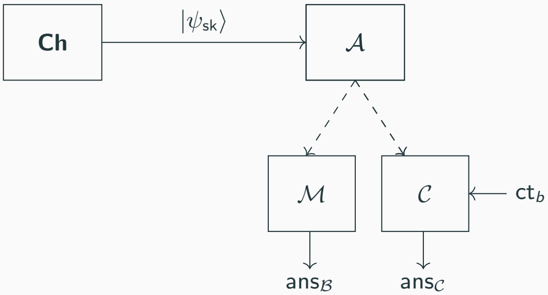
Informal:

- Challenger gives a quantum decryption key $|\psi_{\mathsf{sk}}\rangle$ to adversary $\mathcal{A}$.
- **Revocation phase**:
  - $\mathcal{A}$ returns a state $\rho$ back to the challenger.
  - Challenger checks if $\rho$ is the same as $|\psi_{\mathsf{sk}}\rangle$ by performing a projective measurement $\mathcal{M}$.
  - The resulting residual state handed over to $\mathcal{C}$.
- **Security Guarantee**: the following should not simultaneously hold:
  - Revocation succeeds and,
  - $\mathcal{C}$ can break the semantic security of public-key encryption.

In the language of [**A**LP21]: finite-term key leasing except that $\mathcal{C}$ is malicious.

# Revocable Public-Key Encryption

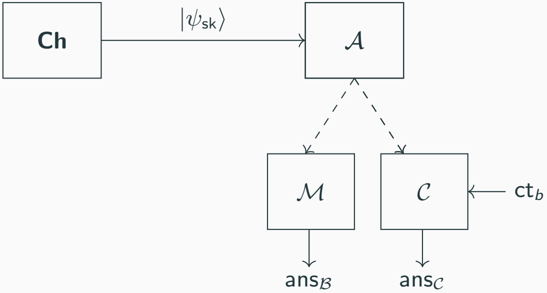
Quantum decryption key: $|\psi_{\mathsf{sk}}\rangle$.




‘

# Revocable Public-Key Encryption

Quantum decryption key: $|\psi_{\mathsf{sk}}\rangle$.

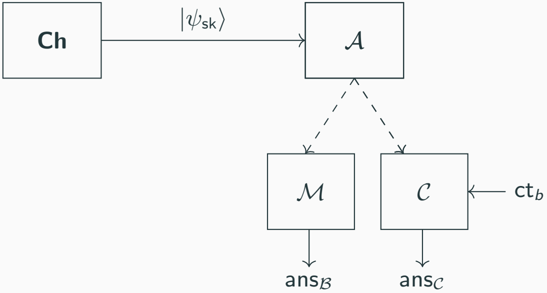



‘

- $\mathcal{M} = \{|\psi_{\mathsf{sk}}\rangle\langle\psi_{\mathsf{sk}}|, I - |\psi_{\mathsf{sk}}\rangle\langle\psi_{\mathsf{sk}}|\}$
- $\mathsf{ct}_0 = \mathsf{Enc}(\mathsf{pk}, 0)$ and $\mathsf{ct}_1 = \mathsf{Enc}(\mathsf{pk}, 1)$.

# Revocable Public-Key Encryption

Quantum decryption key: $|\psi_{\mathsf{sk}}\rangle$.




‘

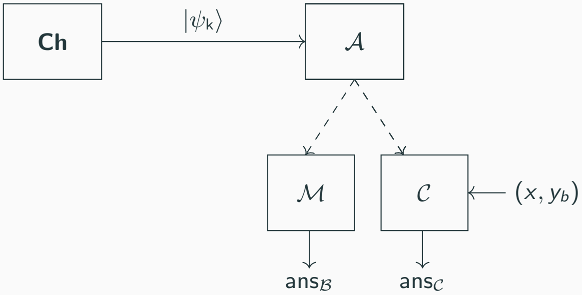
- $\mathcal{M} = \{|\psi_{\mathsf{sk}}\rangle\langle\psi_{\mathsf{sk}}|, I - |\psi_{\mathsf{sk}}\rangle\langle\psi_{\mathsf{sk}}|\}$
- $\mathsf{ct}_0 = \mathsf{Enc}(\mathsf{pk}, 0)$ and $\mathsf{ct}_1 = \mathsf{Enc}(\mathsf{pk}, 1)$.

$$\left|\Pr\left[\mathsf{ans}_{\mathcal{B}} = 0 \text{ and } \mathsf{ans}_{\mathcal{C}} = 1 | b = 0\right] - \Pr\left[\mathsf{ans}_{\mathcal{B}} = 0 \text{ and } \mathsf{ans}_{\mathcal{C}} = 1 | b = 1\right]\right| \leq \mathsf{negl}(\lambda)$$

# Revocable Pseudorandom Functions

$\mathsf{PRF} : \{0,1\}^\lambda \times \{0,1\}^n \to \{0,1\}^m$.

Quantum PRF evaluation key: $|\psi_\mathsf{k}\rangle$.

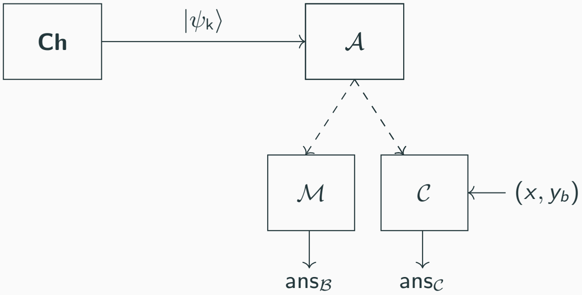



'

# Revocable Pseudorandom Functions

$\mathsf{PRF} : \{0,1\}^\lambda \times \{0,1\}^n \to \{0,1\}^m$.

Quantum PRF evaluation key: $|\psi_{\mathsf{k}}\rangle$.




'

$$\left|\Pr\left[\mathsf{ans}_{\mathcal{B}} = 0 \text{ and } \mathsf{ans}_{\mathcal{C}} = 1 | b = 0\right] - \Pr\left[\mathsf{ans}_{\mathcal{B}} = 0 \text{ and } \mathsf{ans}_{\mathcal{C}} = 1 | b = 1\right]\right| \leq \mathsf{negl}(\lambda)$$

# Our Results

**Result #1**: Assuming simultaneous dual-Regev conjecture,

Dual Regev public-key encryption is key revocable.

**Result #2**: Assuming simultaneous dual-Regev conjecture,

Dual Regev fully homomorphic encryption is key revocable.

**Result #3**: Assuming simultaneous dual-Regev conjecture,

there exist revocable pseudorandom functions.

# Our Results

**Result #1**: Assuming simultaneous dual-Regev conjecture,

Dual Regev public-key encryption is key revocable.

**Concurrent Work**: [Agrawal-Kitagawa-Nishimaki-Yamada-Yamakawa'23]
Assuming post-quatum PKE, there exists public-key encryption that is key revocable.

**Result #2**: Assuming simultaneous dual-Regev conjecture,

Dual Regev fully-homomorphic encryption is key revocable.

**Result #3**: Assuming simultaneous dual-Regev conjecture,

there exist revocable pseudorandom functions.

# Our Results

**Result #1**: Assuming simultaneous dual-Regev conjecture,

Dual Regev public-key encryption is key revocable.

**Result #2**: Assuming simultaneous dual-Regev conjecture,

Dual Regev fully homomorphic encryption is key revocable.

**Not studied before!**

**Result #3**: Assuming simultaneous dual-Regev conjecture,

there exist revocable pseudorandom functions.

# Our Results

**Result #1**: Assuming simultaneous dual-Regev conjecture,

Dual Regev public-key encryption is key revocable.

**Result #2**: Assuming simultaneous dual-Regev conjecture,

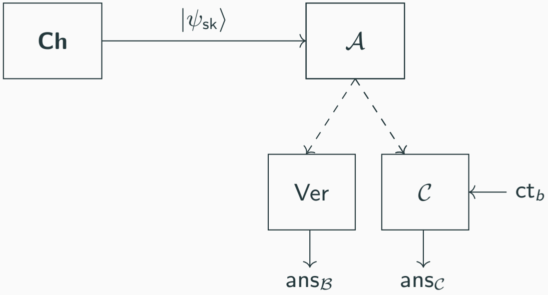
Dual Regev fully homomorphic encryption is key revocable.

**Result #3**: Assuming simultaneous dual-Regev conjecture,

there exist revocable pseudorandom functions.

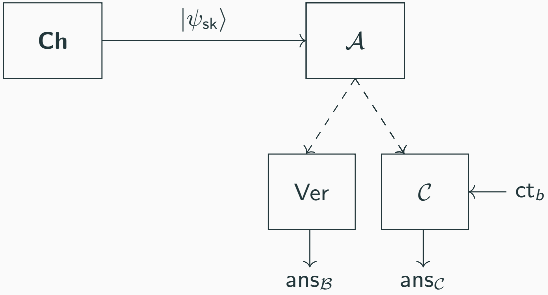
**Prior Work**: Copy-protecting pseudorandom functions based on iO

# Classical Revocation




'

# Classical Revocation




‘

- Ver: verification of classical certificate of revocation.
- $\mathsf{ct}_0 = \mathsf{Enc}(\mathsf{pk}, 0)$ and $\mathsf{ct}_1 = \mathsf{Enc}(\mathsf{pk}, 1)$.

# Our Results

**Result #4**: Assuming simultaneous dual-Regev classical revocation conjecture,

Dual Regev public-key encryption is key revocable with classical revocation.

**Result #5**: Assuming simultaneous dual-Regev classical revocation conjecture,

Dual Regev fully-homomorphic encryption is key revocable with classical revocation.

**Result #6**: Assuming simultaneous dual-Regev classical revocation conjecture,

there exist revocable pseudorandom functions with classical revocation.

# High Level Ideas

# Key-revocable Dual-Regev Encryption

Key generation: The public key is $\mathbf{A} = [\bar{\mathbf{A}} \mid \mathbf{y}] \in \mathbb{Z}_q^{n \times m}$ for a random matrix $\bar{\mathbf{A}} \leftarrow \mathbb{Z}_q^{n \times (m-1)}$ and some $\mathbf{y} \in \mathbb{Z}_q^n$.

Classical decryption key:

Short $\mathbf{x} \in \mathbb{Z}^m$ s.t.

$$\mathbf{y} = \bar{\mathbf{A}} \cdot \mathbf{x} \pmod{q}$$

→

Quantum decryption key:

$$|\psi_{\mathbf{y}}\rangle = \sum_{\substack{\mathbf{x} \in \mathbb{Z}^m: \\ \bar{\mathbf{A}}\mathbf{x} = \mathbf{y} \pmod{q}}} \rho_\sigma(\mathbf{x}) |\mathbf{x}\rangle$$

# Key-revocable Dual-Regev Encryption

Key generation: The public key is $\mathbf{A} = [\bar{\mathbf{A}} \mid \mathbf{y}] \in \mathbb{Z}_q^{n \times m}$ for a random matrix $\bar{\mathbf{A}} \leftarrow \mathbb{Z}_q^{n \times (m-1)}$ and some $\mathbf{y} \in \mathbb{Z}_q^n$.

**Classical decryption key:**

Short $\mathbf{x} \in \mathbb{Z}^m$ s.t.

$$\mathbf{y} = \bar{\mathbf{A}} \cdot \mathbf{x} \pmod{q}$$

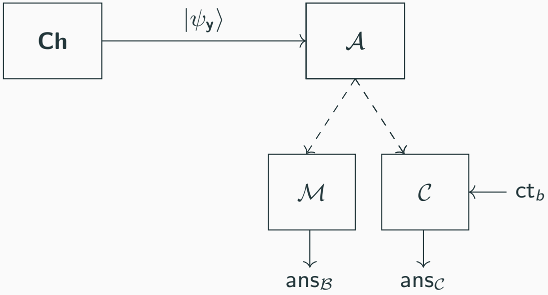
→

**Quantum decryption key:**

$$|\psi_{\mathbf{y}}\rangle = \sum_{\substack{\mathbf{x} \in \mathbb{Z}^m: \\ \bar{\mathbf{A}}\mathbf{x} = \mathbf{y} \pmod{q}}} \rho_\sigma(\mathbf{x}) |\mathbf{x}\rangle$$

$$\mathsf{Enc}(\mathsf{pk}, \mu): \ \mathsf{CT} \approx \left(\mathbf{s}^\intercal \mathbf{A}, \quad \mathbf{s}^\intercal \mathbf{y} + \mu \cdot \lfloor \tfrac{q}{2} \rfloor\right).$$

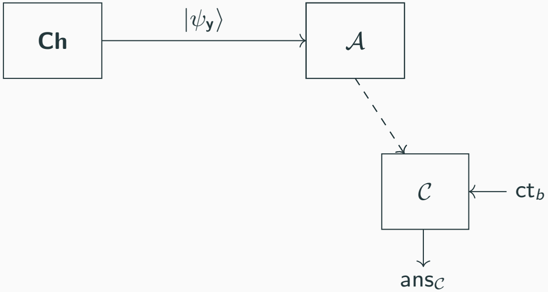
# Proof Idea




'

- $\mathcal{M} = \{|\psi_{\mathbf{y}}\rangle\langle\psi_{\mathbf{y}}|, I - |\psi_{\mathbf{y}}\rangle\langle\psi_{\mathbf{y}}|\}$
- $\mathsf{ct}_0 = \mathsf{Enc}(\mathsf{pk}, 0)$ and $\mathsf{ct}_1 = \mathsf{Enc}(\mathsf{pk}, 1)$.

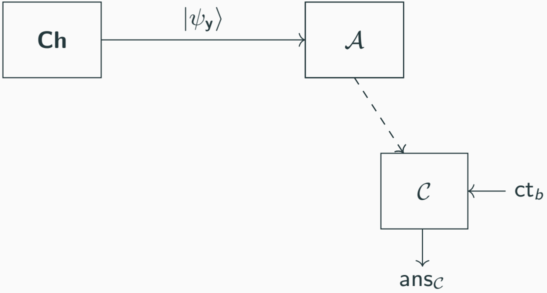
# Initial Observations




'

- $\mathsf{ct}_0 = \mathsf{Enc}(\mathsf{pk}, 0)$ and $\mathsf{ct}_1 = \mathsf{Enc}(\mathsf{pk}, 1)$.

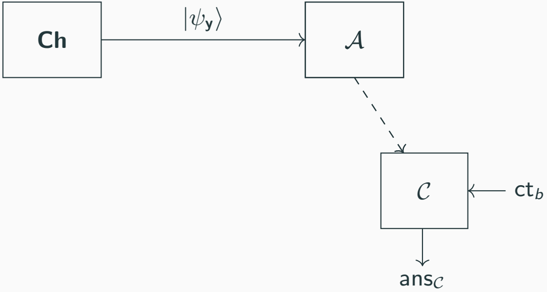
# Initial Observations




'

- $\mathsf{ct}_0 \approx \left(\mathbf{s}^\intercal \mathbf{A}, \quad \mathbf{s}^\intercal \mathbf{y}\right)$ and $\mathsf{ct}_1 \approx \left(\mathbf{s}^\intercal \mathbf{A}, \quad \mathbf{s}^\intercal \mathbf{y} + \lfloor \frac{q}{2} \rfloor\right)$.

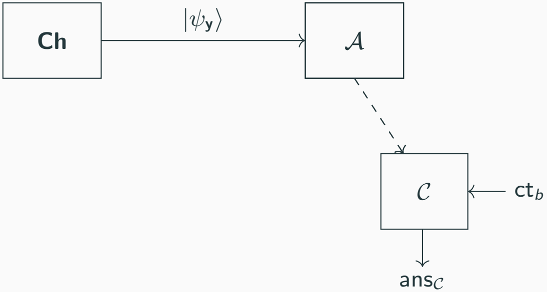
# Initial Observations




- ~~$\mathsf{ct}_0 \approx (\mathbf{s}^\intercal\mathbf{A}, \quad \mathbf{s}^\intercal\mathbf{y})$ and $\mathsf{ct}_1 \approx \left(\mathbf{s}^\intercal\mathbf{A}, \quad \mathbf{s}^\intercal\mathbf{y} + \lfloor \frac{q}{2} \rfloor\right)$.~~
- $\mathsf{ct}_0 \approx (\mathbf{u}, \quad \langle \mathbf{u}, \mathbf{x}_0 \rangle)$ and $\mathsf{ct}_1 \approx \left(\mathbf{s}^\intercal\mathbf{A}, \quad \langle \mathbf{u}, \mathbf{x}_0 \rangle + \lfloor \frac{q}{2} \rfloor\right)$,
  where $\mathbf{A}\mathbf{x}_0 = \mathbf{y}$ and $\|\mathbf{x}_0\|_\infty = O(\mathrm{poly}(n))$.

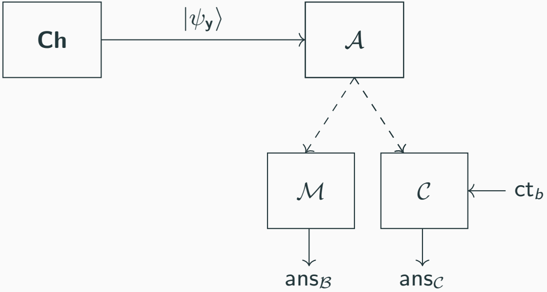
Using gaussian collapsing [Poremba'23] and leakage-resilience techniques [Dodis et al.'10].

# Initial Observations




‘

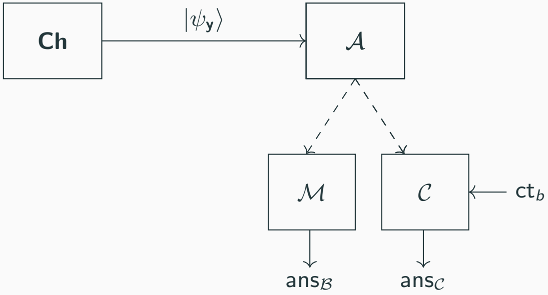
- ~~$\mathsf{ct}_0 \approx (\mathbf{s}^\intercal \mathbf{A}, \quad \mathbf{s}^\intercal \mathbf{y})$ and $\mathsf{ct}_1 \approx (\mathbf{s}^\intercal \mathbf{A}, \quad \mathbf{s}^\intercal \mathbf{y} + \lfloor \frac{q}{2} \rfloor)$.~~
- ~~$\mathsf{ct}_0 \approx (\mathbf{u}, \quad \langle \mathbf{u}, \mathbf{x}_0 \rangle)$ and $\mathsf{ct}_1 \approx (\mathbf{s}^\intercal \mathbf{A}, \quad \langle \mathbf{u}, \mathbf{x}_0 \rangle + \lfloor \frac{q}{2} \rfloor)$~~
- Using Quantum Goldreich-Levin over $\mathbb{Z}_q$: extract $\mathbf{x}_0$




‘

- $\mathcal{M} = \{|\psi_{\mathbf{y}}\rangle\langle\psi_{\mathbf{y}}|, I - |\psi_{\mathbf{y}}\rangle\langle\psi_{\mathbf{y}}|\}$
- $\mathsf{ct}_0 = \mathsf{Enc}(\mathsf{pk}, 0)$ and $\mathsf{ct}_1 = \mathsf{Enc}(\mathsf{pk}, 1)$.

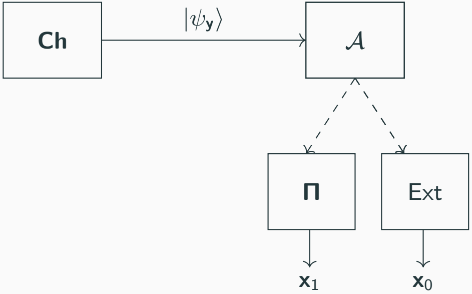
Simultaneous dual-Regev Conjecture $\Longrightarrow$ Simultaneous revocation and extraction of $\mathbf{x}_0$.




‘

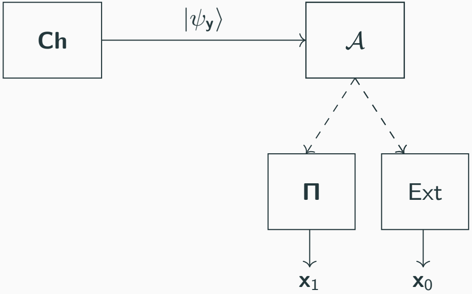
- $\mathcal{M} = \{|\psi_{\mathbf{y}}\rangle\langle\psi_{\mathbf{y}}|, I - |\psi_{\mathbf{y}}\rangle\langle\psi_{\mathbf{y}}|\}$
- $\mathsf{ct}_0 = \mathsf{Enc}(\mathsf{pk}, 0)$ and $\mathsf{ct}_1 = \mathsf{Enc}(\mathsf{pk}, 1)$.

Simultaneous dual-Regev Conjecture $\Longrightarrow$ Simultaneous revocation and extraction of $\mathbf{x}_0$.




‘

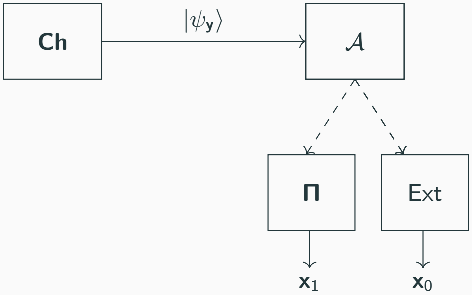
- ~~$\mathcal{M} = \{|\psi_{\mathbf{y}}\rangle\langle\psi_{\mathbf{y}}|, I - |\psi_{\mathbf{y}}\rangle\langle\psi_{\mathbf{y}}|\}$~~
- $\mathbf{\Pi} = \{|\mathbf{x}\rangle\langle\mathbf{x}|\}_{\mathbf{x}\in\mathbb{Z}_q^m}$




- ~~$\mathcal{M} = \{|\psi_{\mathbf{y}}\rangle\langle\psi_{\mathbf{y}}|, I - |\psi_{\mathbf{y}}\rangle\langle\psi_{\mathbf{y}}|\}$~~
- $\boldsymbol{\Pi} = \{|\mathbf{x}\rangle\langle\mathbf{x}|\}_{\mathbf{x}\in\mathbb{Z}_q^m}$

With inverse polynomial probability:

- $\mathbf{A}\mathbf{x}_0 = \mathbf{y}, \mathbf{A}\mathbf{x}_1 = \mathbf{y}$,
- $\mathbf{x}_0, \mathbf{x}_1$ are short,
- $\mathbf{x}_0 \neq \mathbf{x}_1$.




‘

- ~~$\mathcal{M} = \{|\psi_{\mathbf{y}}\rangle\langle\psi_{\mathbf{y}}|, I - |\psi_{\mathbf{y}}\rangle\langle\psi_{\mathbf{y}}|\}$~~
- $\Pi = \{|\mathbf{x}\rangle\langle\mathbf{x}|\}_{\mathbf{x}\in\mathbb{Z}_q^m}$

With inverse polynomial probability:

- $\mathbf{A}\mathbf{x}_0 = \mathbf{y}, \mathbf{A}\mathbf{x}_1 = \mathbf{y}$,
- $\mathbf{x}_0, \mathbf{x}_1$ are short,
- $\mathbf{x}_0 \neq \mathbf{x}_1$.

this breaks SIS!

# Revocable FHE and Pseudorandom Functions

**Revocable FHE**: Dual version of GSW fully homomorphic encryption.

# Revocable FHE and Pseudorandom Functions

**Revocable FHE**: Dual version of GSW fully homomorphic encryption.

**Revocable Pseudorandom Functions**:
Use Shift-Hiding pseudorandom functions (introduced by [Peikert-Shiehian'18]).

- Using evaluation key $\mathsf{sk}_F$, compute output of PRF on $x$ shifted by $F(x)$:

$$\mathrm{PRF}(k, x) + F(x) = \lfloor \mathbf{sA} + F(x) \rceil$$

- **Hiding property**: For any function $F$ and zero function $\mathcal{Z}$,

$$\{\mathsf{sk}_{\mathcal{Z}}\} \approx_c \{\mathsf{sk}_F\}$$

## Revocable Pseudorandom Functions

Idea:

- Set the output of the PRF on input $x \in \{0,1\}^n$ to be:

$$\lfloor \mathbf{S}_x \mathbf{y} \rceil$$

  $(\mathbf{S}_x \in \mathbb{Z}_q^{n \times n})$

- Set the quantum decryption key to be:

$$(sk_{\mathcal{Z}}, |\psi_{\mathbf{y}}\rangle)$$

# Conclusion

**Our Work**: Weaker (yet meaningful) notions of copy-protection from learning with errors

# Conclusion

**Our Work**: Weaker (yet meaningful) notions of copy-protection from learning with errors

**Open Problems**:

- Prove our construction is secure from learning with errors:
  - Subsequent Work: [Chardouvelis-Goyal-Jain-Liu'23] Assuming LWE, there exists PKE and FHE with classical communication
- Revocation for other cryptographic functionalities from LWE.
  - Digital signatures?
- Copy-Protection from LWE
  - Identify interesting cryptographic functionalities

**Thanks!**