Simple and Efficient Secure Key Leasing IBE with Classical Revocation from LWE

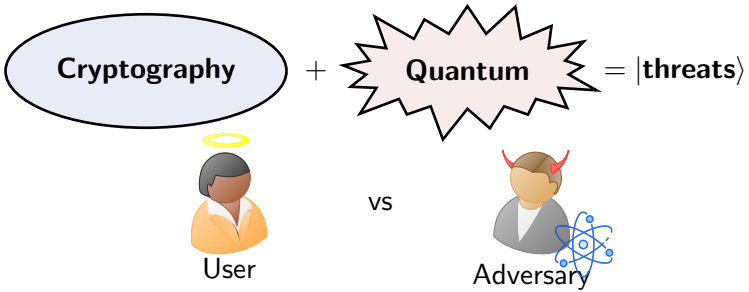
Ho Nguyen Pham[1], Duong Hieu Phan[1], Quoc Huy Vu[2], Weiqiang Wen[1]

[1]LTCI, Telecom Paris, Institut Polytechnique de Paris, France

[2]De Vinci Higher Education, De Vinci Research Center, Paris, France

Ottawa, August 28, 2026

Cryptography in the quantum world

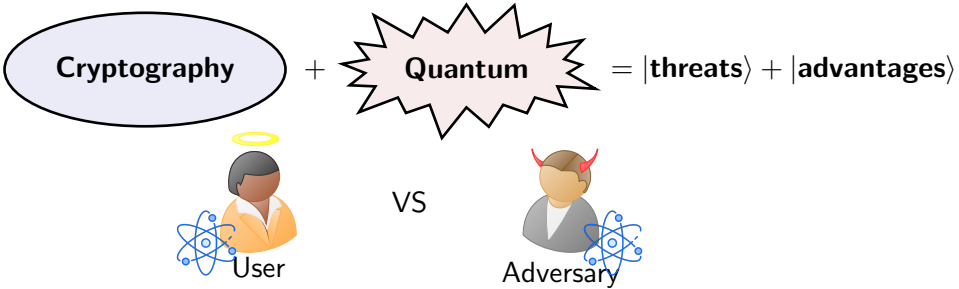


Quantum-capable adversary

- Quantum attacks: Grover's algorithm, Shor's algorithm, etc.

$\rightarrow$ Post-quantum cryptography.

Cryptography in the quantum world

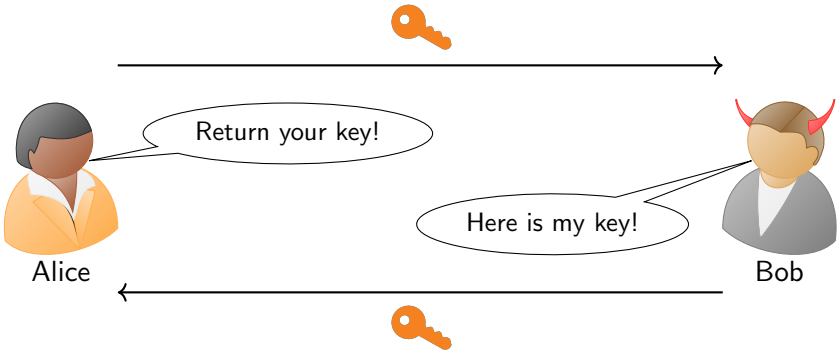


Quantum-capable users

- Unconditional security: QKD, etc.
- Classically impossible functionalities: Quantum Money, Unclonable Encryption, **Secure Key Leasing**, etc.

Secure Key Leasing (SKL)

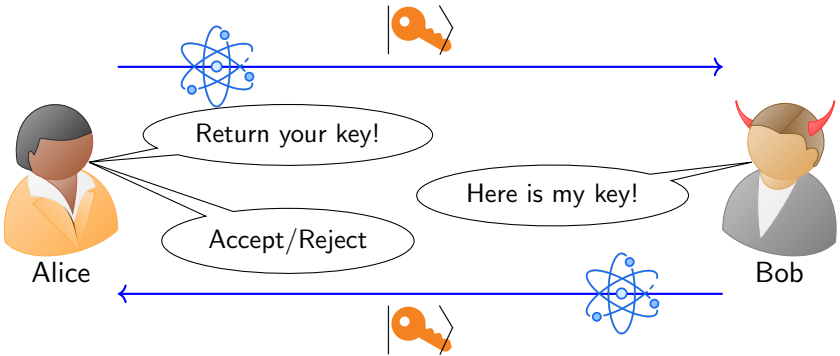
Note. Key = Secret cryptographic tasks, e.g., decryption key



Observation

- Classical: requires updating public keys & re-encryption; Quantum: **?**

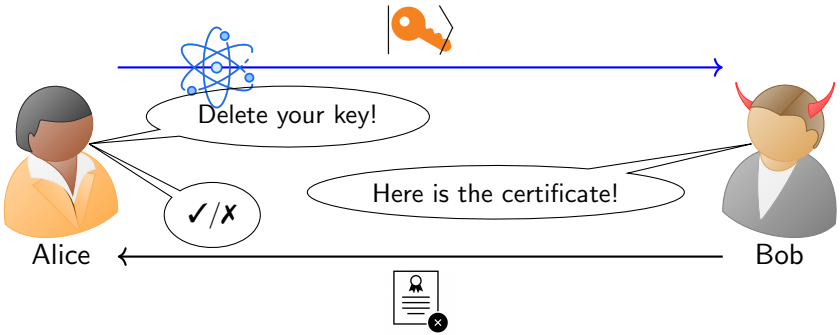
Secure Key Leasing with Quantum Revocation



Observation

- Classical: ✗; Quantum: ✓ ← No-cloning theorem.
- Reusable keys : ✓ ← Gentle measurement lemma.
- Less quantum resources: **?**

Secure Key Leasing with Classical Revocation



Observation

- Classical: ✗; Quantum: ✓ ← No-cloning theorem.
- Reusable keys: ✓ ← Gentle measurement lemma.
- Less quantum resources: ✓ ← Classical channels, **reducing qubit-complexity**.

Previous works - Secure Key Leasing for Encryption

	Primitives	Revocation	Assumption	Quantum Resources
[Agr+23][1]	PKE,IBE	Quantum	PKE,IBE	$\Omega(\lambda^2)$
[KMY25][2]	PKE	Classical	PKE	$\Omega(\lambda^2)$
[APV23; AHH24][3]	PKE	Classical	LWE	$\omega(\lambda \log^2 \lambda)$
[Cha+25; Pha+24][4]	PKE	Classical	LWE	$\mathcal{O}(\lambda^2 \log \lambda)$

- Quantum resources: qubit-complexity required for long-term quantum memory
- [APV23; AHH24] requires sub-exponential modulus-to-noise ratio.
- [Agr+23] requires $\mathcal{O}(\lambda)$ parallel instances of IBE and garbled circuits.

[1] Agrawal et al. *EUROCRYPT 2023*.
[2] Kitagawa, Morimae, Yamakawa. *EUROCRYPT 2025*.
[3] Ananth, Poremba, Vaikuntanathan. *TCC 2023*; Ananth, Hu, Huang. *TCC 2024*.
[4] Chardouvelis et al. *EUROCRYPT 2025*; Phan et al. *ASIACRYPT 2024*.

Our contributions

- Efficient SKL-PKE from LWE with *polynomial modulus*
- Simple and efficient SKL-IBE from LWE

	Primitives	**Revocation**	**Assumption**	**Quantum Resources**
[Agr+23]	PKE, IBE	Quantum	PKE,IBE	$\Omega(\lambda^2)$
[KMY25]	PKE	Classical	PKE	$\Omega(\lambda^2)$
[APV23; AHH24]	PKE	Classical	LWE	$\omega(\lambda \log^2 \lambda)$
[Cha+25; Pha+24]	PKE	Classical	LWE	$\mathcal{O}(\lambda^2 \log \lambda)$
Ours	PKE, IBE	Classical	LWE	$\mathcal{O}(\lambda \log^2 \lambda)$

Secure Key Leasing - Definitions

Definition (SKL-PKE $= (\mathcal{KG}, \mathsf{Enc}, \mathcal{Dec}, \mathcal{Del}, \mathsf{Vrfy})$)

- $\mathcal{KG}(1^\lambda) \to (\mathsf{pk}, \mathit{sk}, \mathsf{vk})$.
- $\mathcal{Del}(\mathit{sk}) \to \mathsf{cert}$.
- $\mathsf{Vrfy}(\mathsf{vk}, \mathsf{cert}) \to \top/\bot$.
- $\mathsf{Enc}(\mathsf{pk}, \mu) \to \mathsf{ct}_\mu$.
- $\mathcal{Dec}(\mathit{sk}, \mathsf{ct}_\mu) \to \mu'$.

Secure Key Leasing - Definitions

Definition (SKL-PKE $= (\mathcal{KG}, \mathsf{Enc}, \mathcal{Dec}, \mathcal{Del}, \mathsf{Vrfy})$)

- $\mathcal{KG}(1^\lambda) \to (\mathsf{pk}, \mathit{sk}, \mathsf{vk})$.
- $\mathcal{Del}(\mathit{sk}) \to \mathsf{cert}$.
- $\mathsf{Vrfy}(\mathsf{vk}, \mathsf{cert}) \to \top/\bot$.
- $\mathsf{Enc}(\mathsf{pk}, \mu) \to \mathsf{ct}_\mu$.
- $\mathcal{Dec}(\mathit{sk}, \mathsf{ct}_\mu) \to \mu'$.

Definition (SKL-IBE $= (\mathsf{Setup}, \mathcal{KG}, \mathsf{Enc}, \mathcal{Dec}, \mathcal{Del}, \mathsf{Vrfy})$)

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{msk}, \mathsf{mpk})$.
- $\mathcal{KG}(\mathsf{msk}, \mathsf{id}) \to (\mathit{sk}_{\mathsf{id}}, \mathsf{vk}_{\mathsf{id}})$.
- $\mathcal{Del}(\mathit{sk}_{\mathsf{id}}) \to \mathsf{cert}$.
- $\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, \mu) \to \mathsf{ct}_\mu$.
- $\mathcal{Dec}(\mathit{sk}_{\mathsf{id}}, \mathsf{ct}_\mu) \to \mu'$.
- $\mathsf{Vrfy}(\mathsf{vk}_{\mathsf{id}}, \mathsf{cert}) \to \top/\bot$.

Secure Key Leasing - Definitions

Security: $\mathcal{A}$ cannot simultaneously return a valid certificate and guess the challenge bit.

Definition (SKL-PKE $= (\mathcal{KG}, \mathsf{Enc}, \mathcal{Dec}, \mathcal{Del}, \mathsf{Vrfy})$)

- $\mathcal{KG}(1^\lambda) \to (\mathsf{pk}, sk, \mathsf{vk})$.
- $\mathcal{Del}(sk) \to \mathsf{cert}$.
- $\mathsf{Vrfy}(\mathsf{vk}, \mathsf{cert}) \to \top/\bot$.
- $\mathsf{Enc}(\mathsf{pk}, \mu) \to \mathsf{ct}_\mu$.
- $\mathcal{Dec}(sk, \mathsf{ct}_\mu) \to \mu'$.

Definition (SKL-IBE $= (\mathsf{Setup}, \mathcal{KG}, \mathsf{Enc}, \mathcal{Dec}, \mathcal{Del}, \mathsf{Vrfy})$)

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{msk}, \mathsf{mpk})$.
- $\mathcal{KG}(\mathsf{msk}, \mathsf{id}) \to (sk_{\mathsf{id}}, \mathsf{vk}_{\mathsf{id}})$.
- $\mathcal{Del}(sk_{\mathsf{id}}) \to \mathsf{cert}$.
- $\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, \mu) \to \mathsf{ct}_\mu$.
- $\mathcal{Dec}(sk_{\mathsf{id}}, \mathsf{ct}_\mu) \to \mu'$.
- $\mathsf{Vrfy}(\mathsf{vk}_{\mathsf{id}}, \mathsf{cert}) \to \top/\bot$.

Secure Key Leasing PKE from LWE

Dual-Regev PKE [GPV08][5]

- $\mathsf{pk} = (\mathbf{A}, \mathbf{y}) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^n$
- $\mathsf{Enc}(\mathsf{pk}, \mu) \to \mathsf{ct} = (\underbrace{\mathbf{s}^\intercal \mathbf{A}}, \underbrace{\mathbf{s}^\intercal \mathbf{y}} + \lfloor \frac{q}{2} \rfloor \mu)$
- $\mathsf{sk} = \mathbf{x} \in \mathbb{Z}_q^m : \mathbf{A}\mathbf{x} = \mathbf{y}$
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \to \mu' \propto \mathsf{ct} \cdot (-\mathbf{x}, 1)$

[5] (Gentry, Peikert, Vaikuntanathan. *40th ACM STOC*)

Secure Key Leasing PKE from LWE

Dual-Regev PKE [GPV08][5]

- $\mathsf{pk} = (\mathbf{A}, \mathbf{y}) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^n$
- $\mathsf{Enc}(\mathsf{pk}, \mu) \to \mathsf{ct} = (\underbrace{\mathbf{s}^\intercal \mathbf{A}}, \underbrace{\mathbf{s}^\intercal \mathbf{y}} + \lfloor \frac{q}{2} \rfloor \mu)$
- $\mathsf{sk} = \mathbf{x} \in \mathbb{Z}_q^m : \mathbf{A}\mathbf{x} = \mathbf{y}$
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \to \mu' \propto \mathsf{ct} \cdot (-\mathbf{x}, 1)$

Dual-Regev SKL-PKE [APV23; AHH24]

- $\mathsf{sk} = \sum_{\mathbf{x} \in \mathbb{Z}_q^m : \mathbf{A}\mathbf{x} = \mathbf{y}} |\mathbf{x}\rangle$
- $U_{\mathsf{Dec}} : |\mathbf{x}\rangle |0\rangle \mapsto |\mathbf{x}\rangle |\mathsf{Dec}(\mathbf{x}, \mathsf{ct})\rangle$

[5] (Gentry, Peikert, Vaikuntanathan. *40th ACM STOC*)

Secure Key Leasing PKE from LWE

- $\mathcal{KG}(1^\lambda)$: sample $(\mathbf{A}, \mathsf{td}) \leftarrow \mathsf{GenTrap}(1^\lambda)$, $(\left|\psi_{\mathbf{A},\mathbf{y}}\right\rangle, \mathbf{y}) \leftarrow \mathcal{GenGauss}(\mathbf{A}, \sigma)$

$$\left|\psi_{\mathbf{A},\mathbf{y}}\right\rangle = \sum_{\mathbf{x}\in\mathbb{Z}_q^m : \mathbf{A}\mathbf{x}=\mathbf{y}} \rho_\sigma(\mathbf{x}) \ \left|\mathbf{x}\right\rangle .$$

Secure Key Leasing PKE from LWE

- $\mathcal{KG}(1^\lambda)$: sample $(\mathbf{A}, \mathsf{td}) \leftarrow \mathsf{GenTrap}(1^\lambda)$, $(\left|\psi_{\mathbf{A},\mathbf{y}}\right\rangle, \mathbf{y}) \leftarrow \mathcal{GenGauss}(\mathbf{A}, \sigma)$, $\mathbf{v} \leftarrow\!\$\ \{0,1\}^m$

$$\left|\psi^{\mathbf{v}}_{\mathbf{A},\mathbf{y}}\right\rangle = \mathbf{Z}_q^{\lfloor \frac{q}{\nu} \rfloor \cdot \mathbf{v}} \left|\psi_{\mathbf{A},\mathbf{y}}\right\rangle = \sum_{\mathbf{x} \in \mathbb{Z}_q^m : \mathbf{A}\mathbf{x} = \mathbf{y}} \rho_\sigma(\mathbf{x})\, \omega_q^{\langle \mathbf{x}, \lfloor \frac{q}{\nu} \rfloor \cdot \mathbf{v} \rangle} \left|\mathbf{x}\right\rangle .$$

- $\mathcal{Del}(\rho)$: apply QFT and measure to obtain certificate $\mathbf{w}^\intercal = \hat{\mathbf{s}}^\intercal \mathbf{A} + \hat{\mathbf{e}}^\intercal + \lfloor \frac{q}{\nu} \rfloor \cdot \mathbf{v}^\intercal \in \mathbb{Z}_q^m$

$$\mathsf{QFT}_q \left|\psi^{\mathbf{v}}_{\mathbf{A},\mathbf{y}}\right\rangle \approx_\epsilon \mathbf{X}_q^{\lfloor \frac{q}{\nu} \rfloor \cdot \mathbf{v}} \sum_{\mathbf{e} \in \mathbb{Z}^m} \rho_{q/\sigma}(\mathbf{e})\, \omega_q^{\langle \mathbf{s}, \mathbf{y} \rangle} \left|\mathbf{s}^\intercal \mathbf{A} + \mathbf{e}^\intercal \bmod q\right\rangle .$$

- $\mathsf{Vrfy}(\mathsf{msk}, \mathsf{cert})$: decode $\mathbf{w}$ with td to get $\mathbf{v}'$ and check $\mathbf{v}' \stackrel{?}{=} \mathbf{v}$.

Computational Hardness

Uncertainty principle for Gaussian coset states [APV23]

$\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$ consisting of a QPT algorithm $\mathcal{A}_0$ and an unbounded algorithm $\mathcal{A}_1$:

1. $\mathcal{CH}$ prepares $\left|\psi^{\mathbf{v}}_{\mathbf{A},\mathbf{y}}\right\rangle$ and sends $(\mathbf{A}, \mathbf{y}, \left|\psi^{\mathbf{v}}_{\mathbf{A},\mathbf{y}}\right\rangle)$ to $\mathcal{A}_0$.
2. $\mathcal{A}_0(\mathbf{A}, \mathbf{y}, \left|\psi^{\mathbf{v}}_{\mathbf{A},\mathbf{y}}\right\rangle \otimes \rho_{\mathsf{aux}}) \to \mathbf{x}_0 \in \mathbb{Z}_q^m$, then sends $\mathbf{x}_0$ to $\mathcal{CH}$ and $(\mathbf{A}, \mathbf{y}, \rho_{\mathsf{aux}})$ to $\mathcal{A}_1$.
3. $\mathcal{A}_1(\mathbf{A}, \mathbf{y}, \rho_{\mathsf{aux}}) \to \mathbf{v}' \in \{0,1\}^m$ and sends it to $\mathcal{CH}$.
4. $\mathcal{CH}$ outputs $\mathbf{v}' = \mathbf{v} \wedge \mathbf{A} \cdot \mathbf{x}_0 = \mathbf{y} \wedge \|\mathbf{x}_0\| \leq \sigma\sqrt{m/2}$.

- A successful $\mathcal{A}$ should return a valid certificate and a short preimage

Computational Hardness

Uncertainty principle for Gaussian coset states [APV23]

$\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$ consisting of a QPT algorithm $\mathcal{A}_0$ and an unbounded algorithm $\mathcal{A}_1$:

1. $\mathcal{CH}$ prepares $\left|\psi^{\mathbf{v}}_{\mathbf{A},\mathbf{y}}\right\rangle$ and sends $(\mathbf{A}, \mathbf{y}, \left|\psi^{\mathbf{v}}_{\mathbf{A},\mathbf{y}}\right\rangle)$ to $\mathcal{A}_0$.
2. $\mathcal{A}_0(\mathbf{A}, \mathbf{y}, \left|\psi^{\mathbf{v}}_{\mathbf{A},\mathbf{y}}\right\rangle \otimes \rho_{\text{aux}}) \to \mathbf{x}_0 \in \mathbb{Z}_q^m$, then sends $\mathbf{x}_0$ to $\mathcal{CH}$ and $(\mathbf{A}, \mathbf{y}, \rho_{\text{aux}})$ to $\mathcal{A}_1$.
3. $\mathcal{A}_1(\mathbf{A}, \mathbf{y}, \rho_{\text{aux}}) \to \mathbf{v}' \in \{0,1\}^m$ and sends it to $\mathcal{CH}$.
4. $\mathcal{CH}$ outputs $\mathbf{v}' = \mathbf{v} \wedge \mathbf{A} \cdot \mathbf{x}_0 = \mathbf{y} \wedge \|\mathbf{x}_0\| \leq \sigma\sqrt{m/2}$.

- A successful $\mathcal{A}$ should return a valid certificate and a short preimage
- A successful SKL-PKE $\mathcal{A}$ should return a valid certificate and distinguish ciphertext

$\to$ A quantum search-to-decision reduction

Quantum Search-to-Decision Reduction [AHH24]

Input: $D_{\mathsf{lwe}}^{\mathbf{A},\mathbf{y}}$ or $D_{\mathsf{unif}}^{\mathbf{A},\mathbf{y}}$. **Output:** $\mathbf{x}$.

Distributions:

1. $D_{\mathsf{lwe}}^{\mathbf{A},\mathbf{y}} = \left(\mathbf{A}, \mathbf{y}, \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}^\intercal, \mathbf{s}^\intercal\mathbf{y} + e'\right),\ \mathbf{s} \leftarrow\$ \mathbb{Z}_q^n,\ \mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}^m,\chi},\ e' \leftarrow \mathcal{D}_{\mathbb{Z},\chi'}$
2. $\bar{D}_{\mathsf{lwe}}^{\mathbf{A},\mathbf{x}} = \left(\mathbf{A}, \mathbf{A}\mathbf{x}, \mathbf{c}_0^\intercal, \mathbf{c}_0^\intercal\mathbf{x} + e''\right),\ \mathbf{c}_0^\intercal = \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}^\intercal,\ e'' \leftarrow \mathcal{D}_{\mathbb{Z},\chi'}$
3. $D_{\mathsf{gl}}^{\mathbf{A},\mathbf{x}} = \left(\mathbf{A}, \mathbf{A}\mathbf{x}, \mathbf{c}_0^\intercal, \mathbf{c}_0^\intercal\mathbf{x} + e''\right),\ \mathbf{c}_0 \leftarrow\$ \mathbb{Z}_q^m$
4. $D_{\mathsf{unif}}^{\mathbf{A},\mathbf{y}} = \left(\mathbf{A}, \mathbf{y}, \mathbf{c}_0^\intercal, c_1\right)\ \mathbf{c}_0 \leftarrow\$ \mathbb{Z}_q^m, c \leftarrow\$ \mathbb{Z}_q$

Strategy: Extract by guessing entry-by-entry between $D_{\mathsf{gl}}^{\mathbf{A},\mathbf{x}}$ and $D_{\mathsf{unif}}^{\mathbf{A},\mathbf{y}}$

Quantum Search-to-Decision Reduction [AHH24]

Input: $D_{\mathsf{lwe}}^{\mathbf{A},\mathbf{y}}$ or $D_{\mathsf{unif}}^{\mathbf{A},\mathbf{y}}$. **Output:** $\mathbf{x}$.

Distributions:

1. $D_{\mathsf{lwe}}^{\mathbf{A},\mathbf{y}} = \left(\mathbf{A}, \mathbf{y}, \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}^\intercal, \mathbf{s}^\intercal\mathbf{y} + e'\right),\ \mathbf{s} \leftarrow\$ \mathbb{Z}_q^n,\ \mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}^m,\chi},\ e' \leftarrow \mathcal{D}_{\mathbb{Z},\chi'}$
2. $\bar{D}_{\mathsf{lwe}}^{\mathbf{A},\mathbf{x}} = \left(\mathbf{A}, \mathbf{A}\mathbf{x}, \mathbf{c}_0^\intercal, \mathbf{c}_0^\intercal\mathbf{x} + e''\right),\ \mathbf{c}_0^\intercal = \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}^\intercal,\ e'' \leftarrow \mathcal{D}_{\mathbb{Z},\chi'},\ \chi'/\chi = \sigma\sqrt{m} \cdot 2^{o(n)}$
3. $D_{\mathsf{gl}}^{\mathbf{A},\mathbf{x}} = \left(\mathbf{A}, \mathbf{A}\mathbf{x}, \mathbf{c}_0^\intercal, \mathbf{c}_0^\intercal\mathbf{x} + e''\right),\ \mathbf{c}_0 \leftarrow\$ \mathbb{Z}_q^m$
4. $D_{\mathsf{unif}}^{\mathbf{A},\mathbf{y}} = \left(\mathbf{A}, \mathbf{y}, \mathbf{c}_0^\intercal, c_1\right)\ \mathbf{c}_0 \leftarrow\$ \mathbb{Z}_q^m, c \leftarrow\$ \mathbb{Z}_q$

Strategy: Extract by guessing entry-by-entry between $D_{\mathsf{gl}}^{\mathbf{A},\mathbf{x}}$ and $D_{\mathsf{unif}}^{\mathbf{A},\mathbf{y}}$

Quantum Search-to-Decision Reduction [AHH24]

Input: $D_{\mathsf{lwe}}^{\mathbf{A},\mathbf{y}}$ or $D_{\mathsf{unif}}^{\mathbf{A},\mathbf{y}}$. **Output:** $\mathbf{x}$.

Distributions:

1. $D_{\mathsf{lwe}}^{\mathbf{A},\mathbf{y}} = \left(\mathbf{A}, \mathbf{y}, \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}^\intercal, \mathbf{s}^\intercal\mathbf{y} + e'\right)$, $\mathbf{s} \leftarrow\$ \mathbb{Z}_q^n$, $\mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}^m,\chi}$, $e' \leftarrow \mathcal{D}_{\mathbb{Z},\chi'}$
2. $\bar{D}_{\mathsf{lwe}}^{\mathbf{A},\mathbf{x}} = \left(\mathbf{A}, \mathbf{A}\mathbf{x}, \mathbf{c}_0^\intercal, \mathbf{c}_0^\intercal\mathbf{x} + e''\right)$, $\mathbf{c}_0^\intercal = \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}^\intercal$, $e'' \leftarrow \mathcal{D}_{\mathbb{Z},\chi'}$, $\chi'/\chi = \sigma\sqrt{m} \cdot 2^{o(n)}$
3. $D_{\mathsf{gl}}^{\mathbf{A},\mathbf{x}} = \left(\mathbf{A}, \mathbf{A}\mathbf{x}, \mathbf{c}_0^\intercal, \mathbf{c}_0^\intercal\mathbf{x} + e''\right)$, $\mathbf{c}_0 \leftarrow\$ \mathbb{Z}_q^m$
4. $D_{\mathsf{unif}}^{\mathbf{A},\mathbf{y}} = \left(\mathbf{A}, \mathbf{y}, \mathbf{c}_0^\intercal, c_1\right)$ $\mathbf{c}_0 \leftarrow\$ \mathbb{Z}_q^m, c \leftarrow\$ \mathbb{Z}_q$

Strategy: Extract by guessing entry-by-entry between $D_{\mathsf{gl}}^{\mathbf{A},\mathbf{x}}$ and $D_{\mathsf{unif}}^{\mathbf{A},\mathbf{y}}$

Observation: e'' doesn't need to be independent noise $\rightarrow$ gentle noise smudging [BD20][6]

[6] Brakerski, Döttling. *EUROCRYPT 2020*.

Refined Quantum Search-to-Decision Reduction

Distributions:

- $D^{\mathbf{A},\mathbf{Ax}}_{0,c_1} = \mathbf{s}^\intercal\mathbf{Ax} + e'$, where $e' \leftarrow \mathcal{D}_{\mathbb{Z},\chi'}$,
- $D^{\mathbf{A},\mathbf{Ax}}_{1,c_1} = \mathbf{s}^\intercal\mathbf{Ax} + \tilde{e} + \bar{e}$, where $\tilde{e} \leftarrow \mathcal{N}_{1,\chi'/\sqrt{2}}$ and $\bar{e} \leftarrow \mathcal{D}_{\mathbb{Z}-\tilde{e},\chi'/\sqrt{2}}$,
- $D^{\mathbf{A},\mathbf{Ax}}_{2,c_1} = \mathbf{s}^\intercal\mathbf{Ax} + \tilde{\mathbf{e}}_0^\intercal\mathbf{x} + \tilde{e}_1 + \bar{e}$, where $\tilde{\mathbf{e}}_0 \leftarrow \mathcal{N}_{m,\chi\sqrt{2}}$, $\tilde{e}_1 \leftarrow \mathcal{N}_{1,\sqrt{\Sigma'}}$ with $\Sigma' = \chi'^2/2 - 2\chi^2\|\mathbf{x}\|^2$,
- $D^{\mathbf{A},\mathbf{Ax}}_{3,c_1} = \mathbf{s}^\intercal\mathbf{Ax} + (\mathbf{e}^\intercal + \tilde{\mathbf{e}}_2^\intercal)\mathbf{x} + \tilde{e}_1 + \bar{e}$, where $\mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}^m,\chi}$, $\tilde{\mathbf{e}}_2 \leftarrow \mathcal{N}_{m,\chi}$,
- $D^{\mathbf{A},\mathbf{Ax}}_{4,c_1} = (\mathbf{s}^\intercal\mathbf{A} + \mathbf{e})\mathbf{x} + e''$, where $e'' \leftarrow \mathcal{D}_{\mathbb{Z},\sqrt{\Sigma}}$ with $\Sigma = \chi'^2 - \chi^2\|\mathbf{x}\|^2$

Smudging noise: $\chi'/\chi > \sigma\sqrt{2m}$

Secure Key Leasing IBE from LWE

Dual-Regev IBE [ABB10; Cas+10][7]

- $\mathsf{mpk} = (\mathbf{A}, \bar{\mathbf{A}}, \mathbf{B}, \mathbf{y}) \in \mathbb{Z}_q^{n \times (3m+1)}$
- $\mathsf{pk}_{\mathsf{id}} = \mathbf{A}_{\mathsf{id}} = [\mathbf{A} \mid \bar{\mathbf{A}} + \mathsf{H}(\mathsf{id})\mathbf{B}]$
- $\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, \mu) \to (\mathbf{s}^\intercal \mathbf{A}_{\mathsf{id}}, \mathbf{s}^\intercal \mathbf{y} + \lfloor \frac{q}{2} \rfloor \mu)$
- $\mathsf{sk}_{\mathsf{id}} = \mathbf{x} \in \mathbb{Z}_q^m : \mathbf{A}_{\mathsf{id}} \mathbf{x} = \mathbf{y}$
- $\mathsf{Dec}(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct}) \to \mu' \propto \mathsf{ct} \cdot (-\mathbf{x}, 1)$

[7] (Agrawal, Boneh, Boyen. *EUROCRYPT 2010*; Cash et al. *EUROCRYPT 2010*)

Secure Key Leasing IBE from LWE

Dual-Regev IBE [ABB10; Cas+10][7]

- $\mathsf{mpk} = (\mathbf{A}, \bar{\mathbf{A}}, \mathbf{B}, \mathbf{y}) \in \mathbb{Z}_q^{n \times (3m+1)}$
- $\mathsf{pk}_{\mathsf{id}} = \mathbf{A}_{\mathsf{id}} = [\mathbf{A} \mid \bar{\mathbf{A}} + \mathsf{H}(\mathsf{id})\mathbf{B}]$
- $\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, \mu) \to (\mathbf{s}^\intercal \mathbf{A}_{\mathsf{id}}, \mathbf{s}^\intercal \mathbf{y} + \lfloor \frac{q}{2} \rfloor \mu)$
- $\mathsf{sk}_{\mathsf{id}} = \mathbf{x} \in \mathbb{Z}_q^m : \mathbf{A}_{\mathsf{id}} \mathbf{x} = \mathbf{y}$
- $\mathsf{Dec}(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct}) \to \mu' \propto \mathsf{ct} \cdot (-\mathbf{x}, 1)$

Dual-Regev SKL-IBE

$$\mathsf{sk}_{\mathsf{id}} = \left|\psi^{\mathbf{v}}_{\mathbf{A},\hat{\mathbf{y}}}\right\rangle \otimes |\mathbf{u}\rangle = \mathbf{Z}_q^{\lfloor \frac{q}{\nu} \rfloor \cdot \mathbf{v}} \sum_{\mathbf{x} \in \mathbb{Z}_q^m : \mathbf{A}\mathbf{x} = \hat{\mathbf{y}}} \rho_\sigma(\mathbf{x}) \, |\mathbf{x}\rangle \otimes |\mathbf{u}\rangle \,, \text{ where } \hat{\mathbf{y}} + (\bar{\mathbf{A}} + \mathsf{H}(\mathsf{id})\mathbf{B})\mathbf{u} = \mathbf{y}$$

$\to$ preparation requires trapdoor td for $\mathbf{A}_{\mathsf{id}}$

[7] (Agrawal, Boneh, Boyen. *EUROCRYPT 2010*; Cash et al. *EUROCRYPT 2010*)

Security Proof

- Adapt the quantum search-to-decision reduction with IBE ciphertext distribution
- Answer **1 decrypting-key** query without trapdoor ?
- Stateful verification $\mathbf{v}_{\mathsf{id}}$

Security Proof

- Adapt the quantum search-to-decision reduction with IBE ciphertext distribution
- Answer **1 decrypting-key** query without trapdoor $\rightarrow$ program $\mathbf{y}$ in pk from $\left|\psi_{\mathbf{A}_{\mathsf{id}^*},\mathbf{y}}\right\rangle$
- Stateful verification $\mathbf{v}_{\mathsf{id}} \rightarrow$ stateless verification by $\mathbf{v}_{\mathsf{id}} \leftarrow \mathsf{PRF.Eval}(\mathsf{k}, \mathsf{H}_2(\mathsf{id})\|\hat{\mathbf{y}})$

Future Directions

- Adaptive security for our construction?
- More efficiency from Ring/Module-LWE?
- Unbounded collusion-resistance from standard assumption? Currently requires iO.

Thank you!

References I

[ABB10] Shweta Agrawal, Dan Boneh, and Xavier Boyen. "Efficient Lattice (H)IBE in the Standard Model". In: *EUROCRYPT 2010*. Ed. by Henri Gilbert. Vol. 6110. LNCS. Springer, Berlin, Heidelberg, May 2010, pp. 553–572. DOI: 10.1007/978-3-642-13190-5_28.

[Agr+23] Shweta Agrawal et al. "Public Key Encryption with Secure Key Leasing". In: *EUROCRYPT 2023, Part I*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14004. LNCS. Springer, Cham, Apr. 2023, pp. 581–610. DOI: 10.1007/978-3-031-30545-0_20.

[AHH24] Prabhanjan Ananth, Zihan Hu, and Zikuan Huang. "Quantum Key-Revocable Dual-Regev Encryption, Revisited". In: *TCC 2024, Part III*. Ed. by Elette Boyle and Mohammad Mahmoody. Vol. 15366. LNCS. Springer, Cham, Dec. 2024, pp. 257–288. DOI: 10.1007/978-3-031-78020-2_9.

References II

[APV23] Prabhanjan Ananth, Alexander Poremba, and Vinod Vaikuntanathan. "Revocable Cryptography from Learning with Errors". In: *TCC 2023, Part IV*. Ed. by Guy N. Rothblum and Hoeteck Wee. Vol. 14372. LNCS. Springer, Cham, Nov. 2023, pp. 93–122. DOI: 10.1007/978-3-031-48624-1_4.

[BD20] Zvika Brakerski and Nico Döttling. "Hardness of LWE on General Entropic Distributions". In: *EUROCRYPT 2020, Part II*. Ed. by Anne Canteaut and Yuval Ishai. Vol. 12106. LNCS. Springer, Cham, May 2020, pp. 551–575. DOI: 10.1007/978-3-030-45724-2_19.

[Cas+10] David Cash et al. "Bonsai Trees, or How to Delegate a Lattice Basis". In: *EUROCRYPT 2010*. Ed. by Henri Gilbert. Vol. 6110. LNCS. Springer, Berlin, Heidelberg, May 2010, pp. 523–552. DOI: 10.1007/978-3-642-13190-5_27.

References III

[Cha+25] Orestis Chardouvelis et al. “Quantum Key Leasing for PKE and FHE with a Classical Lessor”. In: *EUROCRYPT 2025, Part III*. Ed. by Serge Fehr and Pierre-Alain Fouque. Vol. 15603. LNCS. Springer, Cham, May 2025, pp. 248–277. DOI: 10.1007/978-3-031-91131-6_9.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. “Trapdoors for hard lattices and new cryptographic constructions”. In: *40th ACM STOC*. Ed. by Richard E. Ladner and Cynthia Dwork. ACM Press, May 2008, pp. 197–206. DOI: 10.1145/1374376.1374407.

[KMY25] Fuyuki Kitagawa, Tomoyuki Morimae, and Takashi Yamakawa. “A Simple Framework for Secure Key Leasing”. In: *EUROCRYPT 2025, Part III*. Ed. by Serge Fehr and Pierre-Alain Fouque. Vol. 15603. LNCS. Springer, Cham, May 2025, pp. 217–247. DOI: 10.1007/978-3-031-91131-6_8.

References IV

[Pha+24] Duong Hieu Phan et al. "Adaptive Hardcore Bit and Quantum Key Leasing over Classical Channel from LWE with Polynomial Modulus". In: *ASIACRYPT 2024, Part IX*. Ed. by Kai-Min Chung and Yu Sasaki. Vol. 15492. LNCS. Springer, Singapore, Dec. 2024, pp. 185–214. DOI: 10.1007/978-981-96-0947-5_7.