Cryptography with Secure Key Leasing

Post-Quantum Cryptography Summer School

@Warsaw 2024 July 19th

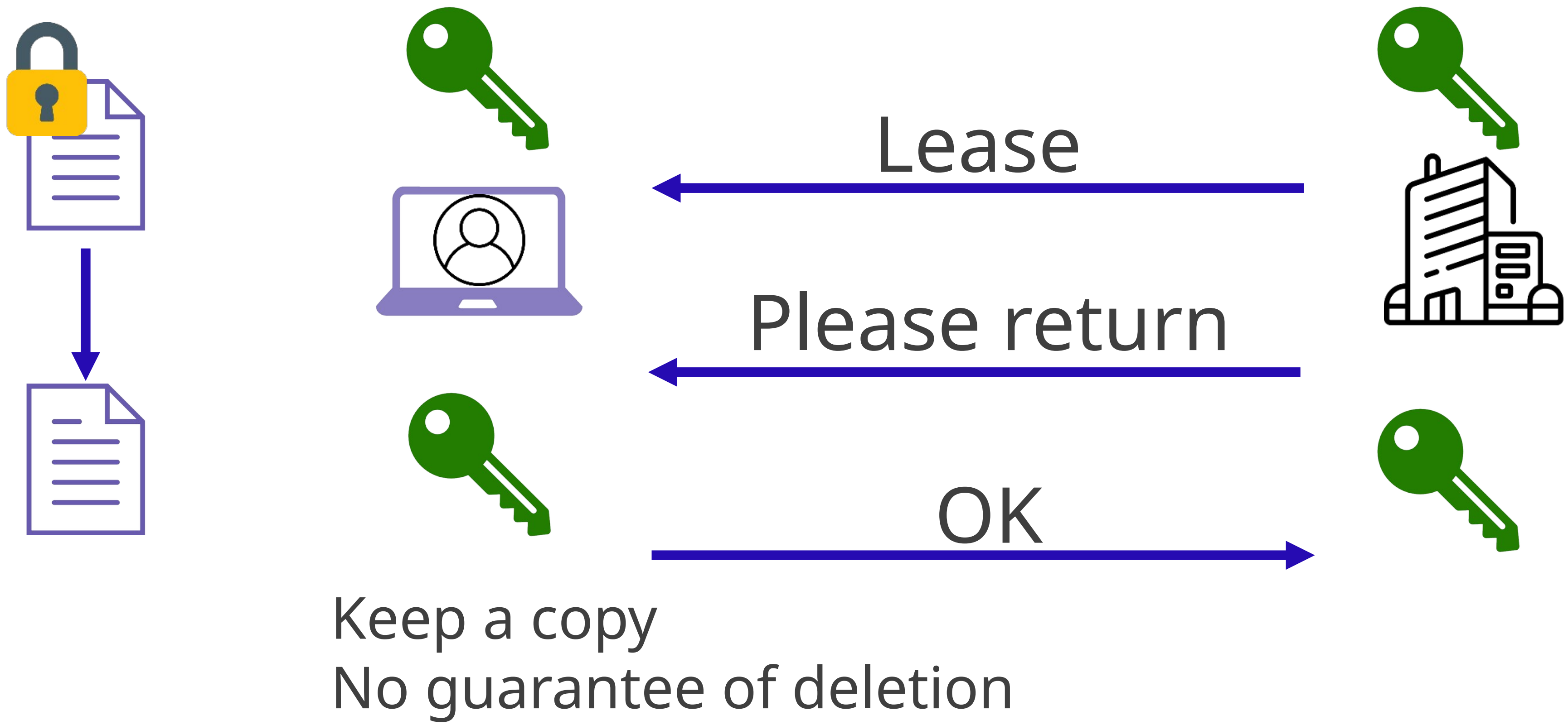
Ryo Nishimaki

NTT SIL & TQC

Outline

1. Cryptography and quantum information
2. Definition of secure key leasing
3. How to achieve PKE with secure key leasing
4. Other constructions with secure key leasing

Limitation of Classical Cryptography



Secure leasing is impossible by classical cryptography

Power of Quantum Information

No-cloning theorem

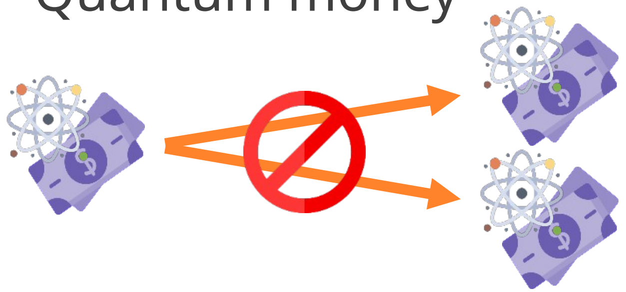
There is no general procedure for copying all unknown quantum states

Go beyond classical cryptography?
(Can achieve what classical cryptography cannot achieve?)

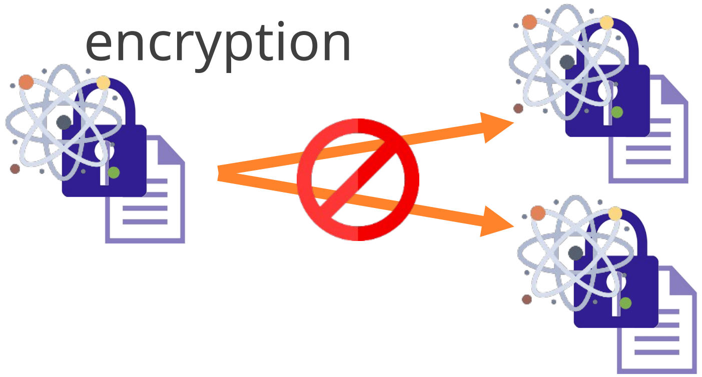
Yes!

Quantum Cryptography

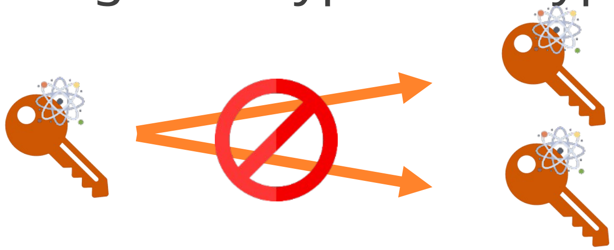
Quantum money



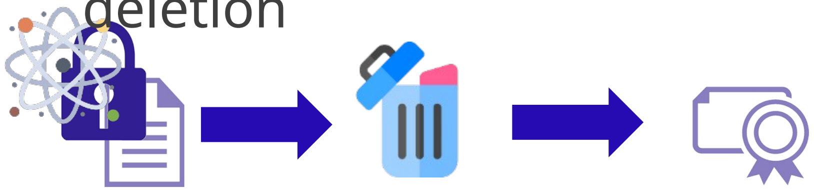
Unclonable encryption



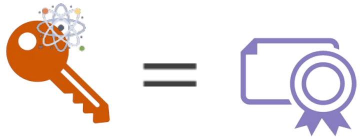
Single decryptor encryption



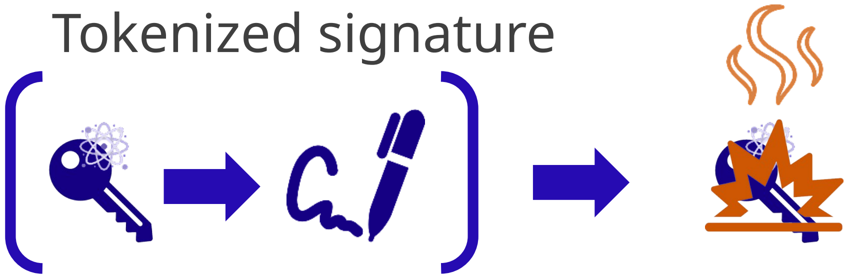
Encryption with certified deletion



Secure key leasing/Key revocation



Tokenized signature



More!

Difference between Secure Leasing and Deletion

Functionalities are similar, but...

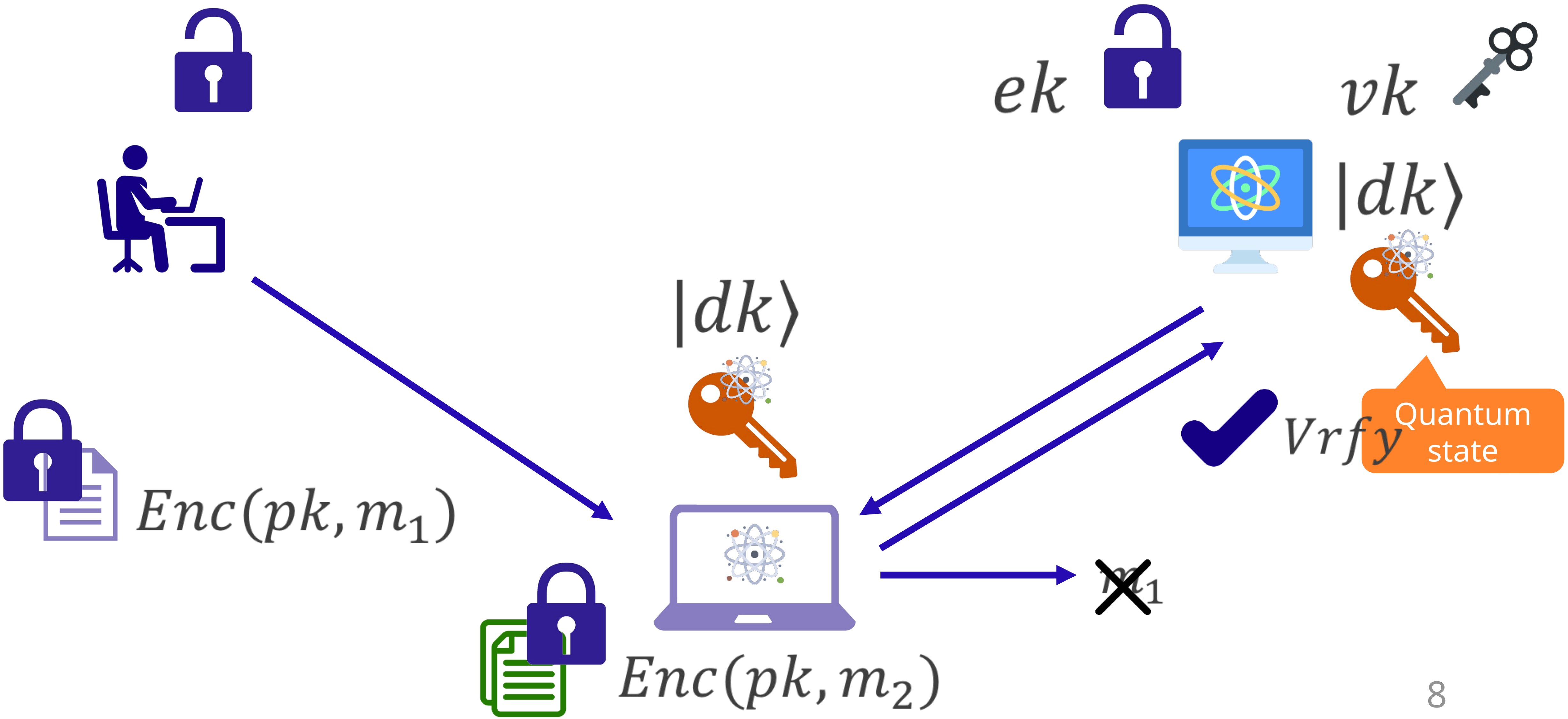
Deletion certificates are classical or quantum

Certified deletion

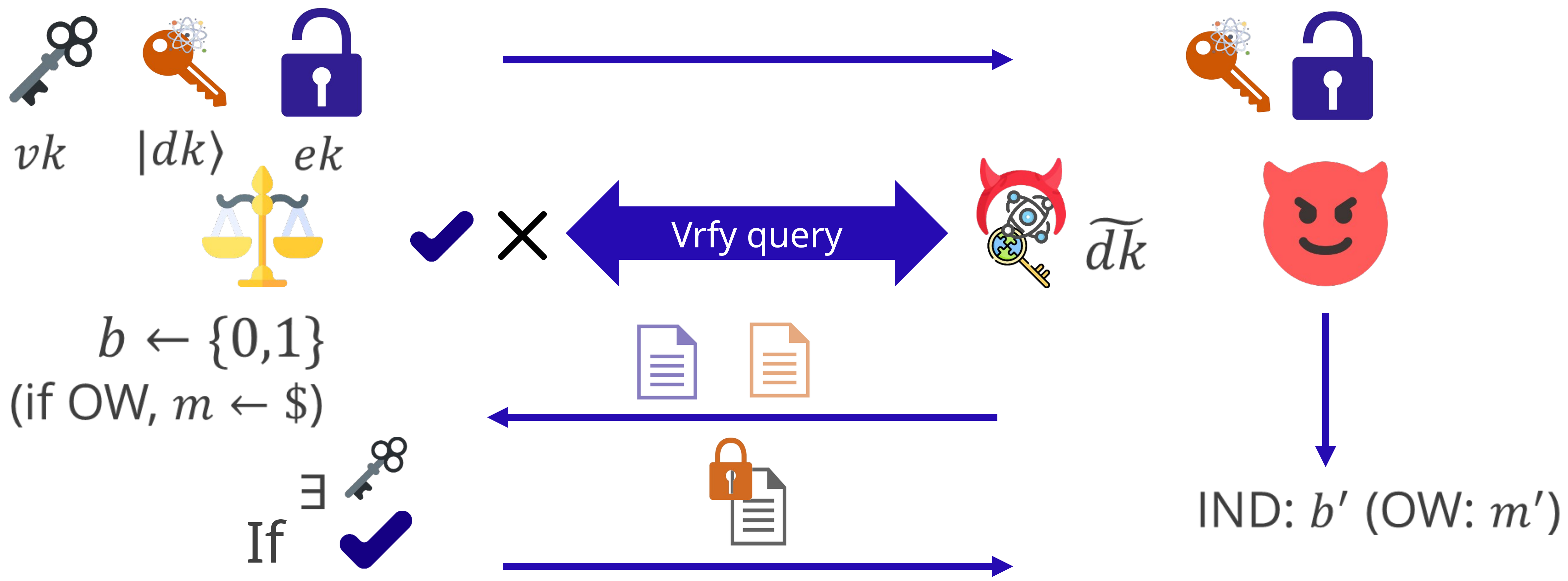
Secure leasing

What is Secure Key Leasing?

PKE with Secure Key Leasing

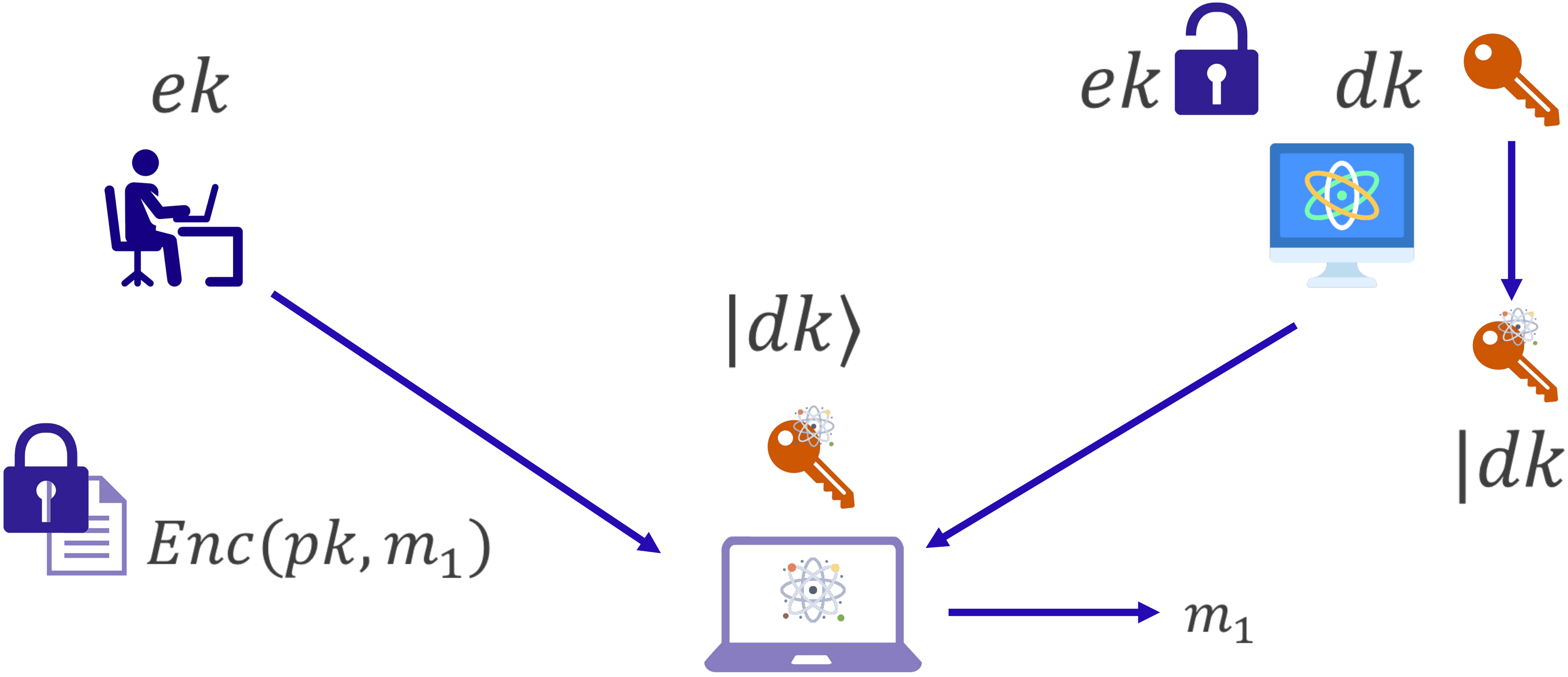


Key Leasing Attacks (KLA)

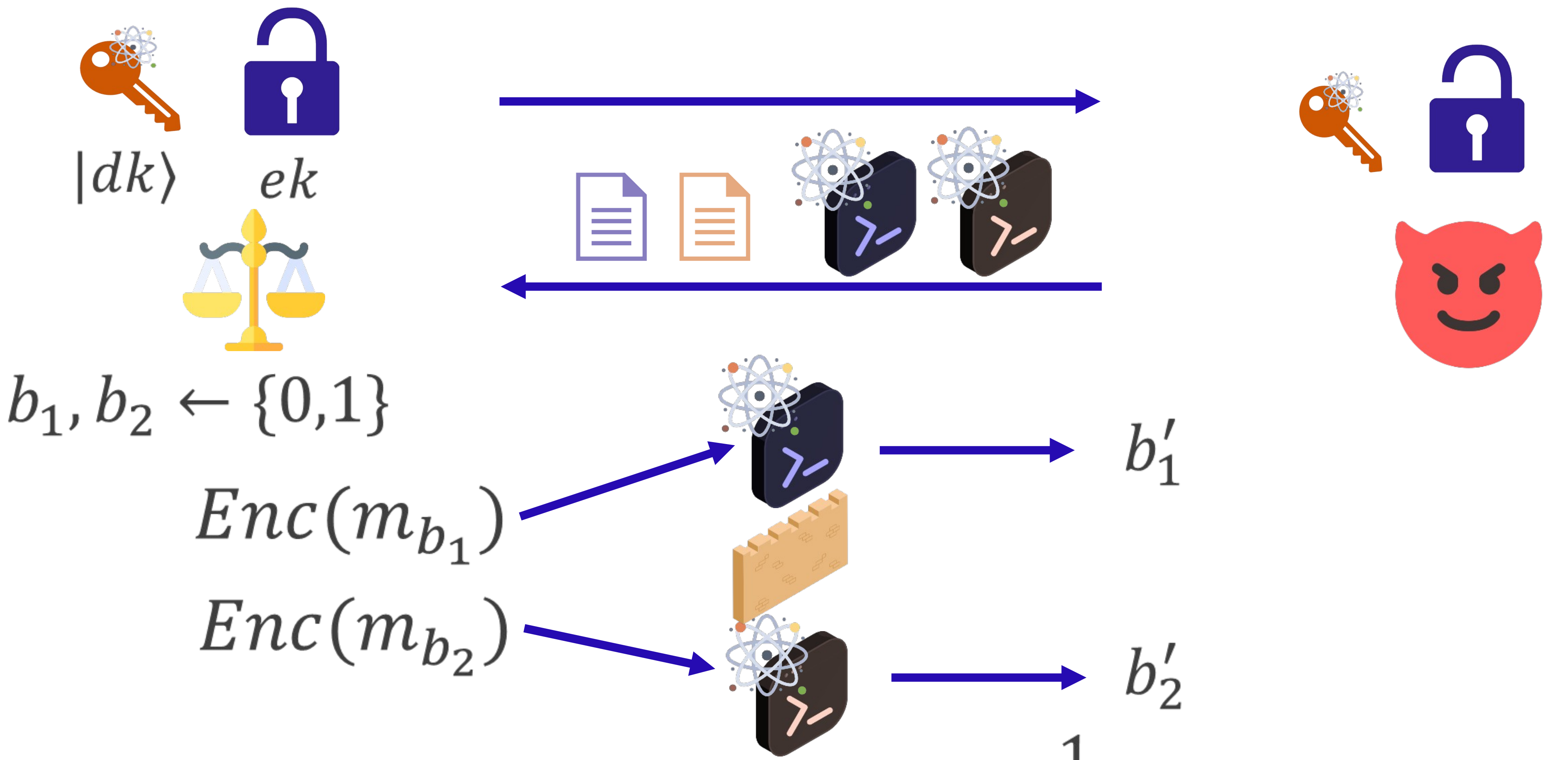


$$|\Pr[b' = 1 : b = 0] - \Pr[b' = 1 : b = 1]| = negl$$

Single Decryptor Encryption



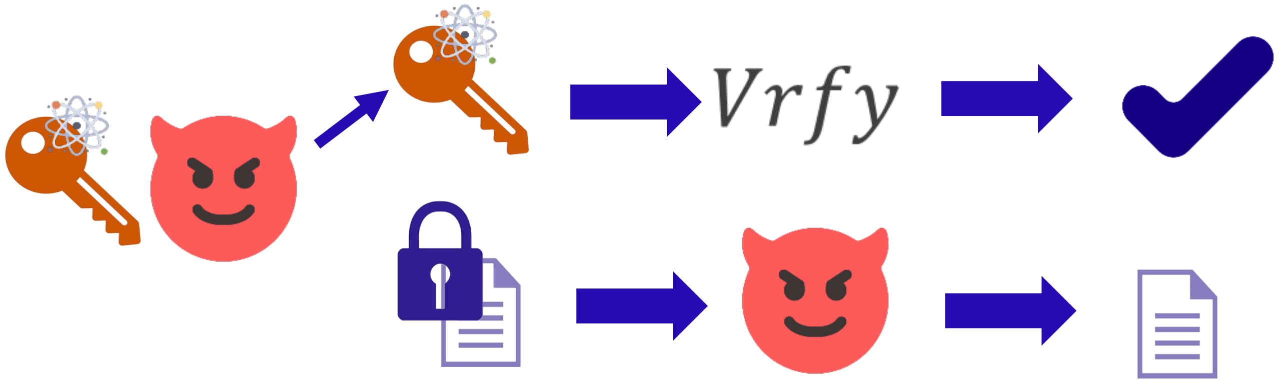
(CPA-style) Anti-Piracy Security

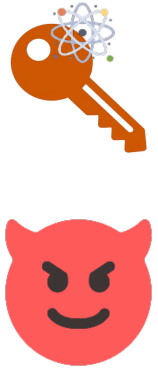


$$\Pr[b_1 = b_1' \wedge b_2 = b_2'] = \frac{1}{2} + negl$$

Unclonability and Secure Leasing

- Unclonability implies secure leasing

If 

Then, both  works as good decryptors

Works on Single Decryptor Encryption

1 Public-key SDE

[CLLZ21] (+[CV22]): from sub-exp. IO, OWFs, and LWE

[KN22a]: Functional encryption variant from sub-exp. IO, OWFs, and LWE

[LLQZ22]: Bounded collusion-resistant variants from sub-exp. IO, OWFs, and LWE

[CG24]: Collusion-resistant variants from sub-exp. IO, OWFs, and LWE

2 One-time secret key SDE

[AKL23]: Single-bit scheme without any assumption

[KN23]: Multi-bit scheme from LWE

Neither the standard hybrid argument nor hybrid encryption technique work

Issue and Question

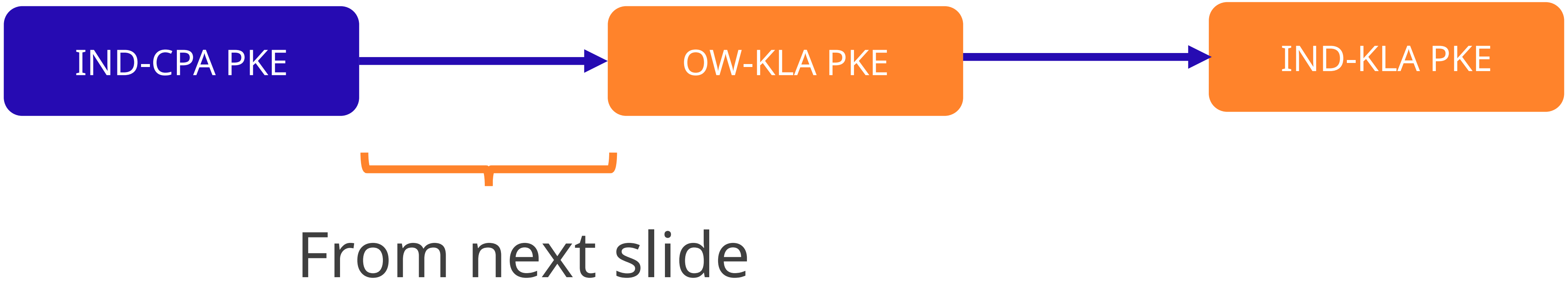
Indistinguishability obfuscation is a heavy tool

Post-quantum IO remains elusive

Can we achieve PKE with SKL from standard assumptions?

How to achieve PKE with SKL

Road Map [AKN+23]



Simple Idea for OW-KLA PKE from PKE

- Two PKE keys in superposition

$$(ek_0, dk_0) \leftarrow Gen(1^\lambda), (ek_1, dk_1) \leftarrow Gen(1^\lambda)$$

$$dk = \frac{1}{\sqrt{2}}(|0\rangle|dk_0\rangle + |1\rangle|dk_1\rangle)$$

Enc

$$ct_0 = Enc(ek_0, m), ct_1 = Enc(ek_1, m)$$

Dec

$$U_{dec}|b\rangle|dk\rangle|(ct_0, ct_1)\rangle|0\rangle \rightarrow |b\rangle|dk\rangle|(ct_0, ct_1)\rangle|Dec(dk, ct_b)\rangle$$

Apply U_{dec} and measure the last register

Simple Idea for OW-KLA PKE from PKE

Verification

Projection:

$$\Pi_{vrfy} = \frac{1}{2}(|0\rangle|dk_0\rangle + |1\rangle|dk_1\rangle)(\langle 0|\langle dk_0| + \langle 1|\langle dk_1|)$$

Apply a binary outcome measurement $(I - \Pi_{vrfy}, \Pi_{vrfy})$ to $dk = \frac{1}{\sqrt{2}}(|0\rangle|dk_0\rangle + |1\rangle|dk_1\rangle)$

If projected onto Π_{vrfy}, output ⊤

½-OW-KLA Security

- Trivial attack strategy

measure

$dk = \frac{1}{\sqrt{2}}(|0\rangle|dk_0\rangle + |1\rangle|dk_1\rangle) \Rightarrow dk_0$ or dk_1

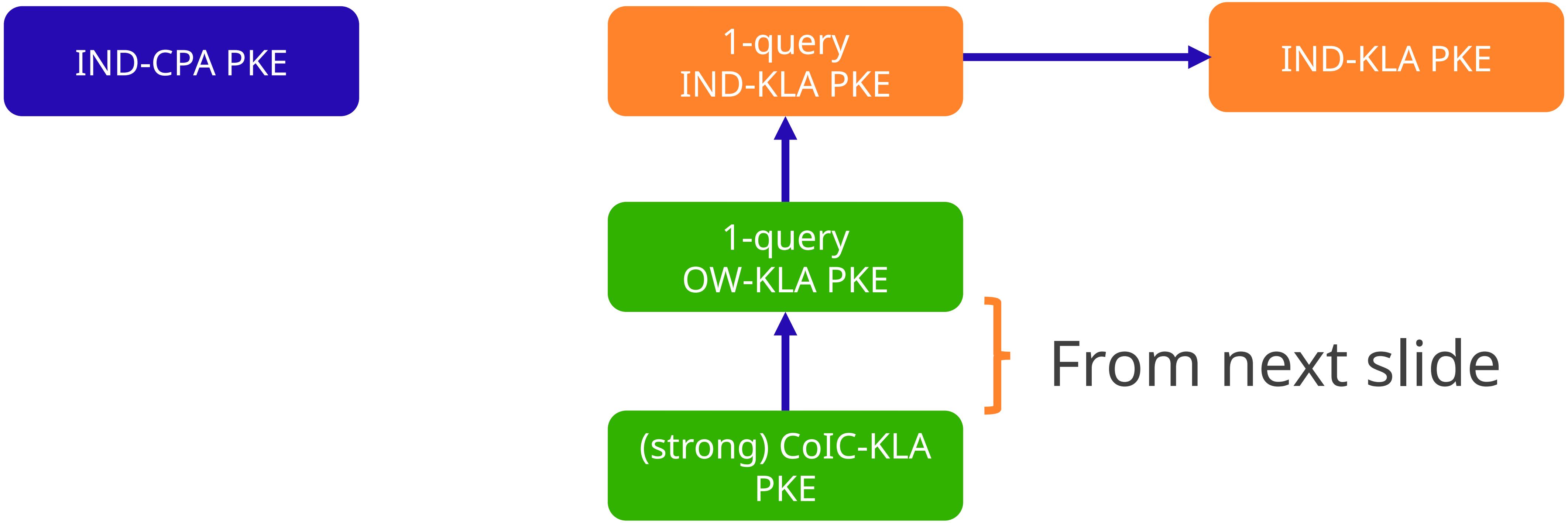
Pass verification with ½ and break the security

- This strategy is optimal

How to show? Non-trivial!

Shown by *Consistent or InConsistent (CoIC)* security

Road Map


IND-CPA PKE
1-query
IND-KLA PKE
IND-KLA PKE
1-query
OW-KLA PKE
(strong) CoIC-KLA
PKE
From next slide

Consistent or InConsistent (CoIC) Security

dk_0, dk_1

ek_0, ek_1

Projection Π_{vrfy} ✔ ✕

Vrfy query (once)

ek_0, ek_1

$dk = \frac{1}{\sqrt{2}}(|0\rangle|dk_0\rangle + |1\rangle|dk_1\rangle)$

$a, b \leftarrow \$$

$ct_0 = Enc(ek_0, m_a)$

$ct_1 = Enc(ek_1, m_{a \oplus b})$

(ct_0, ct_1)

b'

$b = b'?$

Fact

Given $dk = \frac{1}{\sqrt{2}}(|0\rangle|dk_0\rangle + |1\rangle|dk_1\rangle)$

$ct_0 \leftarrow Enc(ek_0, m^*), ct_1 \leftarrow Enc(ek_1, \widetilde{m})$

Cannot output $(dk_0, \widetilde{m})$ or (dk_1, m^*) with non-negligible probability if PKE is one-way secure

Proof. Even if we measure dk in the computational basis before giving it to $\mathcal{A}$, $\mathcal{A}$ has success probability at least $\frac{\epsilon}{2}$ (pinching lemma) [BZ13]

Intuition for OW-KLA Security

1. CoIC security

$ct_0 = Enc(ek_0, m^*) \quad ct_1 = Enc(ek_1, m^*)$

$\approx$ Under the Vrfy oracle

$ct_0 = Enc(ek_0, m^*) \quad ct_1 = Enc(ek_1, \tilde{m})$

$\mathcal{A}$ wins if $m' \in \{m^*, \tilde{m}\}$

2. Valid decryption key

If we measure a valid $\widetilde{dk}$ in the computational basis, we obtain dk_0 or dk_1

If OW-KLA is broken, contradict the fact

From ½-OW-KLA to Full OW-KLA

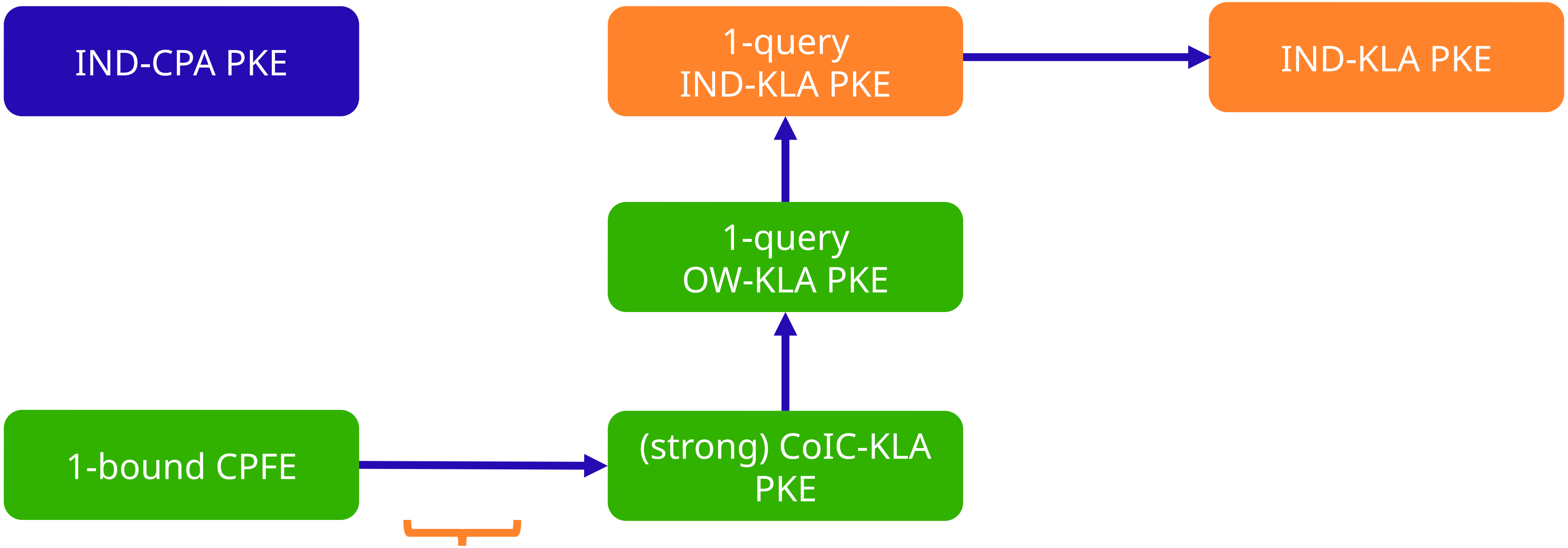
- Parallel repetition

$$dk_1 = \frac{1}{\sqrt{2}}(|0\rangle|dk_{1,0}\rangle + |1\rangle|dk_{1,1}\rangle), \ldots, dk_\lambda = \frac{1}{\sqrt{2}}(|0\rangle|dk_{\lambda,0}\rangle + |1\rangle|dk_{\lambda,1}\rangle)$$

$$m = m_1 || \cdots || m_\lambda \qquad ct_{i,b} = Enc(ek_{i,b}, m_i)$$

- Not black-box amplification from ½-OW-KLA

Road Map



From next slide

Ciphertext-Policy Functional Encryption

$Setup(1^\lambda) \rightarrow (pk, msk)$

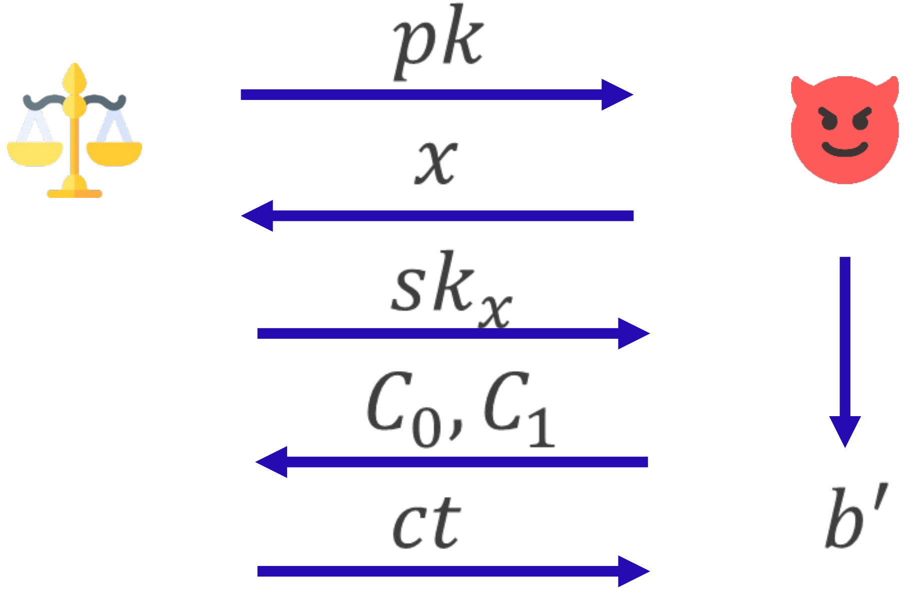
$KG(msk, x) \rightarrow sk_x$

$Enc(pk, C) \rightarrow ct_C$

$Dec(sk_x, ct_C) \rightarrow y$

<u>Correctness:</u> $y = C(x)$

<u>1-key security:</u>



$C_0(x) = C_1(x)$

CoIC-KLA secure PKE from 1-key CPFE

$\underline{Gen(1^\lambda):}$ $FE.Setup(1^\lambda) \rightarrow (pk, msk)$

$FE.KG(msk, x) \rightarrow sk_x$ for random x

$(ek, dk) = (pk, sk_x)$

$\underline{Enc(ek, m):}$

$FE.Enc(pk, C[m])$ For any x $m \leftarrow C[m](x)$

$\underline{Dec(dk, ct):}$

$FE.Dec(sk_x, ct)$

Fact

Given (pk_0, pk_1) $dk = \frac{1}{\sqrt{2}}(|0\rangle|sk_{x_0}\rangle + |1\rangle|sk_{x_1}\rangle)$

Cannot output both x_0 and x_1 with non-negligible probability

Even if we measure dk in the computational basis before giving it to $\mathcal{A}$, $\mathcal{A}$ has success probability at least $\frac{\epsilon}{2}$ (pinching lemma) [BZ13]

Tracing Property

$(ek, dk) = (pk, sk_x)$

(ek, dk)

$ct_b \leftarrow Enc(ek, m_b)$

b' $\Pr[b = b'] = \frac{1}{2} + 1/poly$

We can extract x from with $1/poly$

How to Trace?

Let $\tilde{C}[b, m_0, m_1, i](x) = m_{b \oplus x_i}$

$$FE.Enc\left(\tilde{C}\right) \approx FE.Enc(C[m_{b \oplus x_i}])$$

since $\tilde{C}[b, m_0, m_1, i](x) = m_{b \oplus x_i} = C[m_{b \oplus x_i}](x)$

$x_i = 0 \Rightarrow \quad ct \approx Enc(m_b) \Rightarrow \tilde{p} > 1/2$

$x_i = 1 \Rightarrow \quad ct \approx Enc\left(m_{1 \oplus b}\right) \Rightarrow \tilde{p} < 1/2$

Estimation

$ct \leftarrow FE.Enc\left(\tilde{C}\right)$

b'

$$\tilde{p} = \frac{\#[b' = b]}{N}$$

Watermarking extraction technique against quantum adversary [KN22b]

Quantum Tracing Property

$(ek_0, dk_0) = (pk_0, sk_{x_0})$

$(ek_1, dk_1) = (pk_1, sk_{x_1})$

$dk = \frac{1}{\sqrt{2}}(|0\rangle|sk_{x_0}\rangle + |1\rangle|sk_{x_1}\rangle)$

$Enc(ek_0, m_a), Enc(ek_1, m_{a\oplus b})$

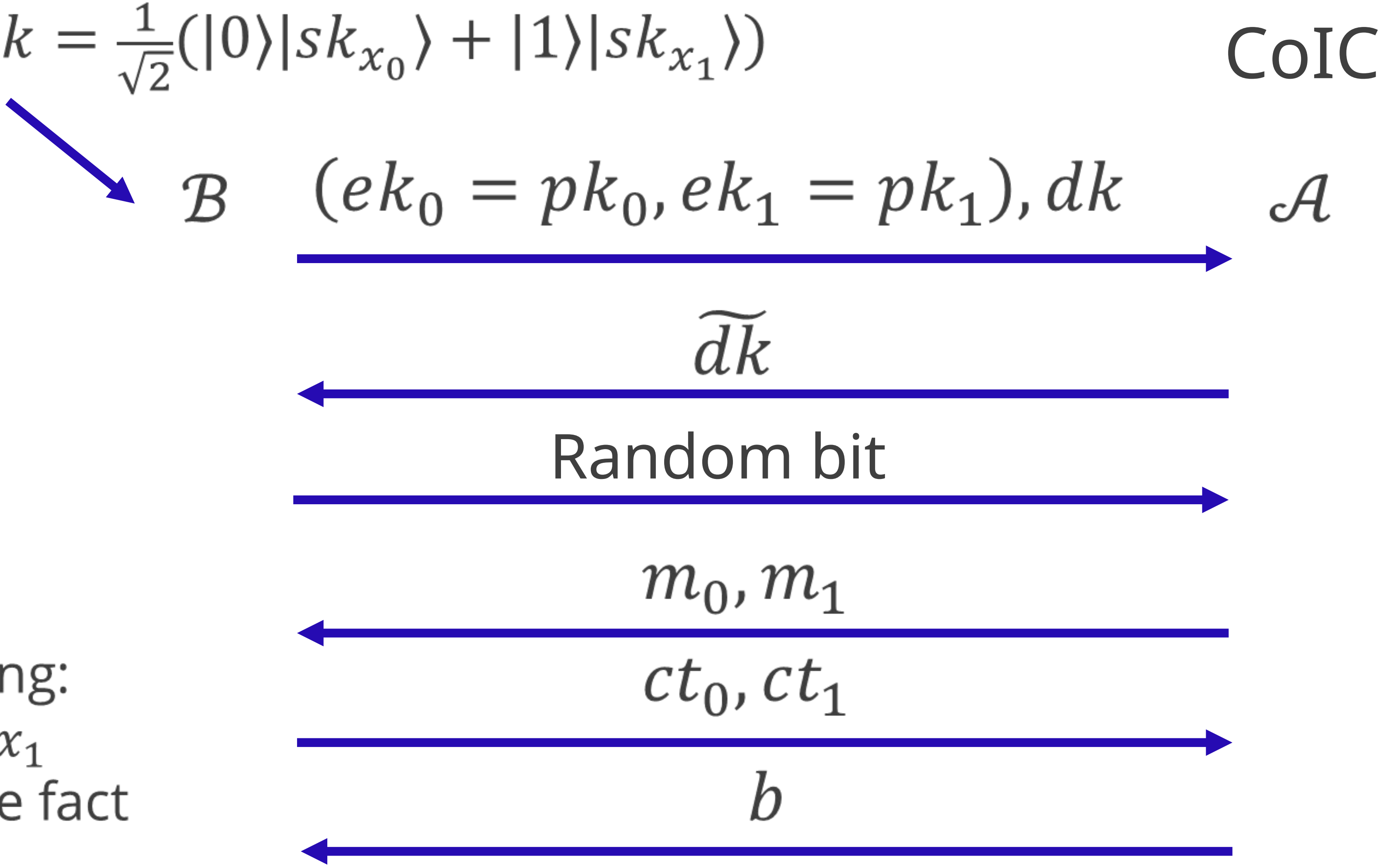
b' $\Pr[b = b'] = \frac{1}{2} + 1/poly$

We can extract x_0, x_1 from with $1/poly$

Approximate projective implementation technique
[Zhandry20,MW05] + [KN22b]

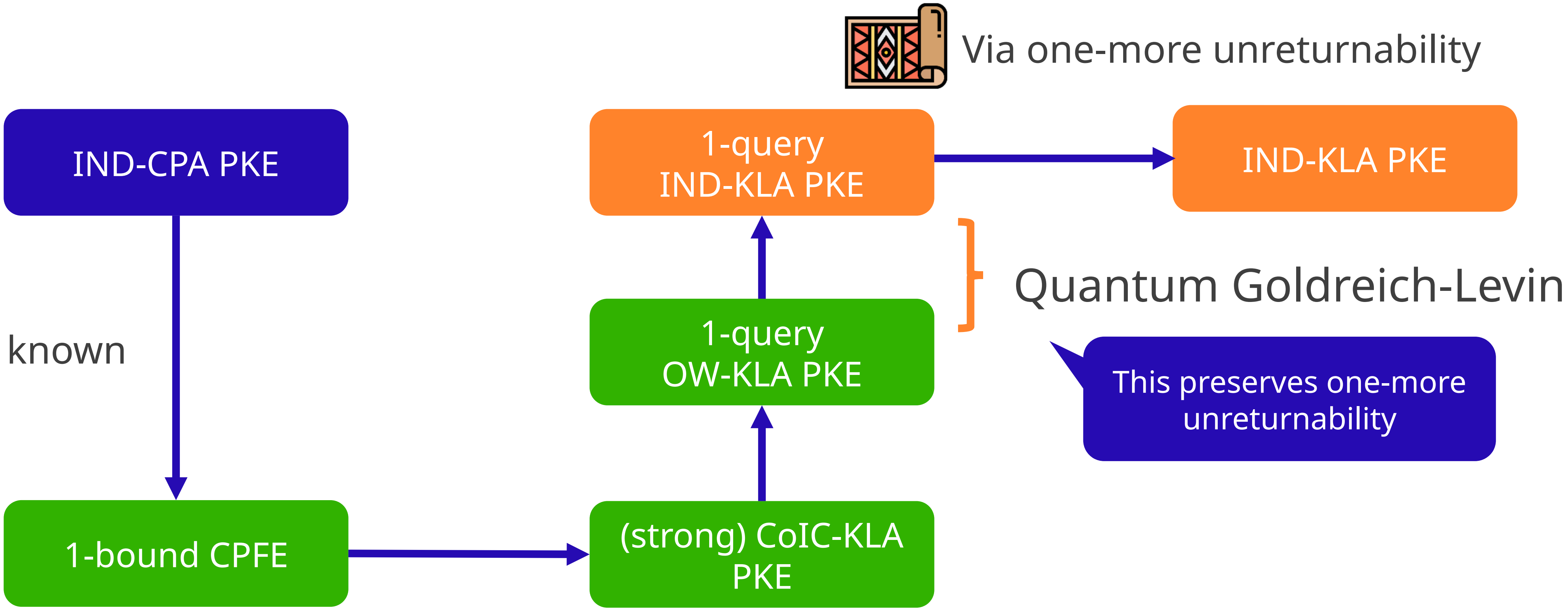
CoIC Security from Tracing and Fact

(pk_0, pk_1) $dk = \frac{1}{\sqrt{2}}(|0\rangle|sk_{x_0}\rangle + |1\rangle|sk_{x_1}\rangle)$



Quantum tracing:
Extract x_0 and x_1
⇒contradict the fact

Road Map


Via one-more unreturnability
IND-CPA PKE
1-query
IND-KLA PKE
IND-KLA PKE
Quantum Goldreich-Levin
known
1-query
OW-KLA PKE
This preserves one-more unreturnability
1-bound CPFE
(strong) CoIC-KLA
PKE

Extensions and Other Constructions

Extension to ABE and Public Key FE [AKN+23]

- Standard ABE + PKE with SKL $\Rightarrow$ ABE with SKL

  Bounded #distinguishing keys

- Standard PKFE + PKE with SKL $\Rightarrow$ PKFE with SKL

  [KN22a] achieved bounded collusion-resistant secret-key FE with SKL from OWF

Other Constructions

- Dual-Regev based construction [APV23, AHH24]

  [APV23]: LWE + unproven conjecture

  [AHH24]: LWE

  Classical certificate, other primitives (FHE, PRF)

- Regev based construction [CGJL23]

  LWE (noisy trapdoor claw-free family)

  Classical communication, FHE

Dual-Regev Based Quantum Decryption Key

$ek = (\boldsymbol{A}, \boldsymbol{y})$

$$dk = |\psi_{\boldsymbol{y}}\rangle = \sum_{\substack{\boldsymbol{x} \in \mathbb{Z}_q^m \\ \boldsymbol{Ax} = \boldsymbol{y} \bmod q}} \rho_\sigma(\boldsymbol{x}) |\boldsymbol{x}\rangle |\boldsymbol{y}\rangle$$

Instead of single vector $\boldsymbol{x}$

<u>Intuition</u>

A valid decryption key $\Rightarrow$ a valid pre-image of $\boldsymbol{y}$

Distinguishing $\Rightarrow$ searching a pre-image of $\boldsymbol{y}$

} SIS solution

Conclusion

1. **Quantum states are unclonable**

   Certified deletion, secure key leasing, unclonable cryptography

2. **Proving security is non-trivial**

   CoIC security & quantum extraction technique

3. **General constructions or LWE-based**

Auxiliary material

From CoIC-KLA to (1-query) ½-OW-KLA

$dk = \frac{1}{\sqrt{2}}(|0\rangle|dk_0\rangle + |1\rangle|dk_1\rangle)$

m'

Π_{vrfy} ✓ ✗

Vrfy query (once)

CoIC security

If ✓ $ct_0 = Enc(ek_0, m)$ $ct_1 = Enc(ek_1, \tilde{m})$

$m' \in \{m, \tilde{m}\}$?

If $\mathcal{A}$ wins w/ $\frac{1}{2} + 1/poly$, computational basis measurement $\widetilde{dk} \to dk_0$ or dk_1 w/ $1/poly$

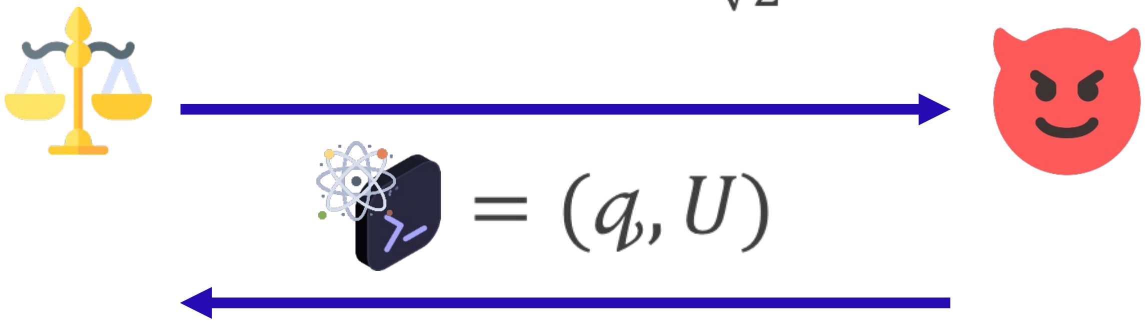
Deferred measurement Π_{vrfy} ✓ ✗

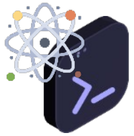
But cannot obtain $(dk_0, \tilde{m})$ or (dk_1, m) via OW-CPA & [BZ13]

(even if we measure dk in computational basis)

Strong CoIC Security

$$ek_0, ek_1 \quad dk = \frac{1}{\sqrt{2}}(|0\rangle|dk_0\rangle + |1\rangle|dk_1\rangle)$$



Check the success probability p of  for guessing b given $ct_0 = Enc(ek_0, m_a)$ $\quad ct_1 = Enc(ek_1, m_{a\oplus b})$

Give superposition of ciphertexts and check the guesses

$$\Pr[p \geq \frac{1}{2} + \epsilon] \leq negl$$

Boneh-Zhandry Lemma [BZ13]

QPT $\mathcal{A}$

QPT $\mathcal{A}'$: Pausing $\mathcal{A}$ at an arbitrary stage
partial measurement that obtains one of k outcomes
resuming $\mathcal{A}$

$$\Pr[x \leftarrow \mathcal{A}'] \geq \frac{\Pr[x \leftarrow \mathcal{A}]}{k}$$

Quantum Goldreich-Levin

With quantum auxiliary input

$$\Pr[\mathcal{A}(aux, r) \to x \cdot r \mid r \leftarrow \{0,1\}^n] \geq \frac{1}{2} + \epsilon$$

$$\Rightarrow \Pr[\mathcal{E}xt([\mathcal{A}], aux) \to x] \geq 4\epsilon^2$$