PKE and ABE with Collusion-Resistant Secure Key Leasing

Fuyuki Kitagawa

NTT

Ryo Nishimaki

NTT

Nikhil Pappu

Portland State University

PKE with Secure Key Leasing

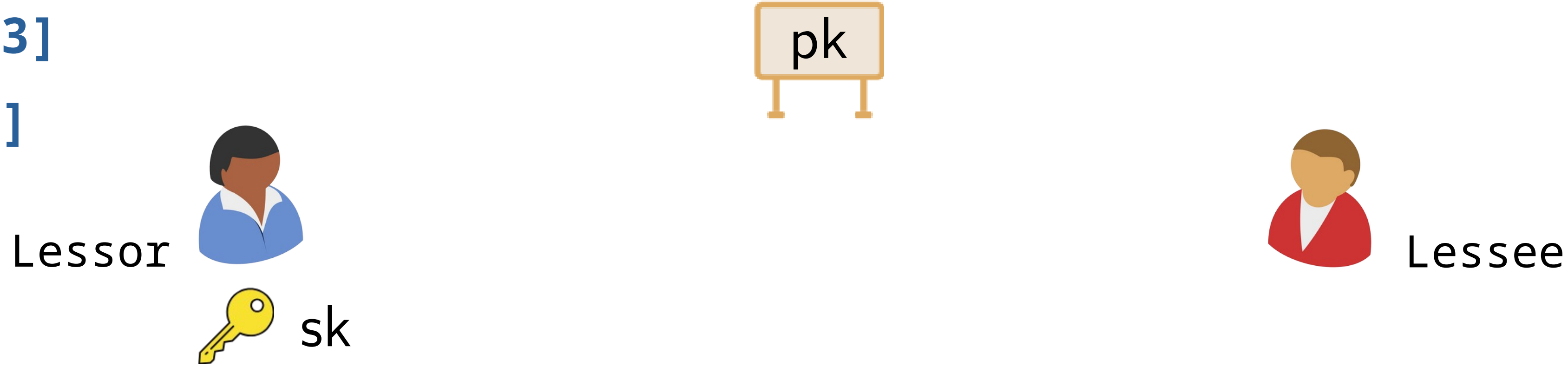
[AKN+23]

[APV23]

PKE with Secure Key Leasing

[AKN+23]

[APV23]



pk

Lessor

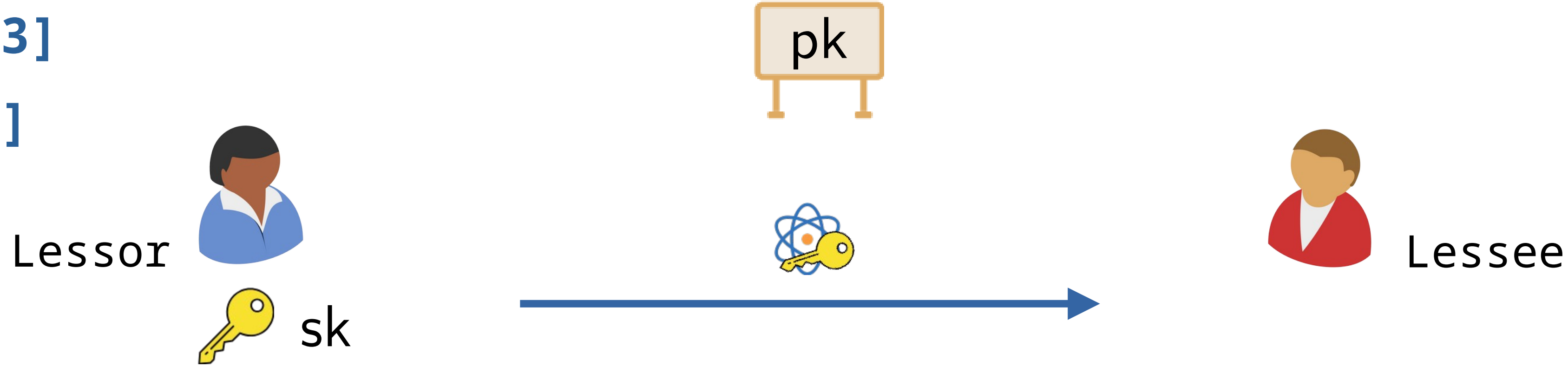
Lessee

sk

PKE with Secure Key Leasing

[AKN+23]

[APV23]



pk

Lessor

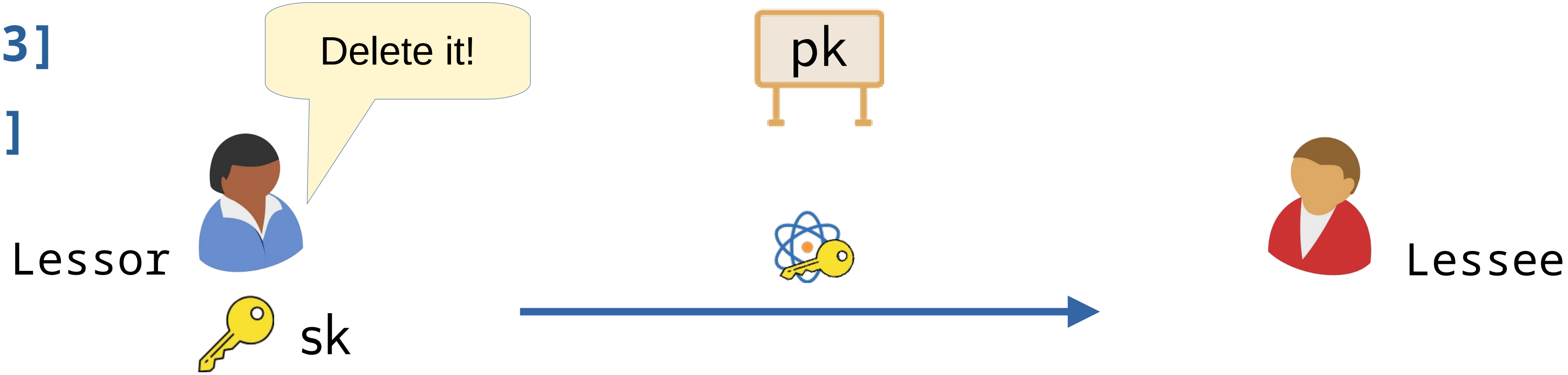
Lessee

sk

PKE with Secure Key Leasing

[AKN+23]

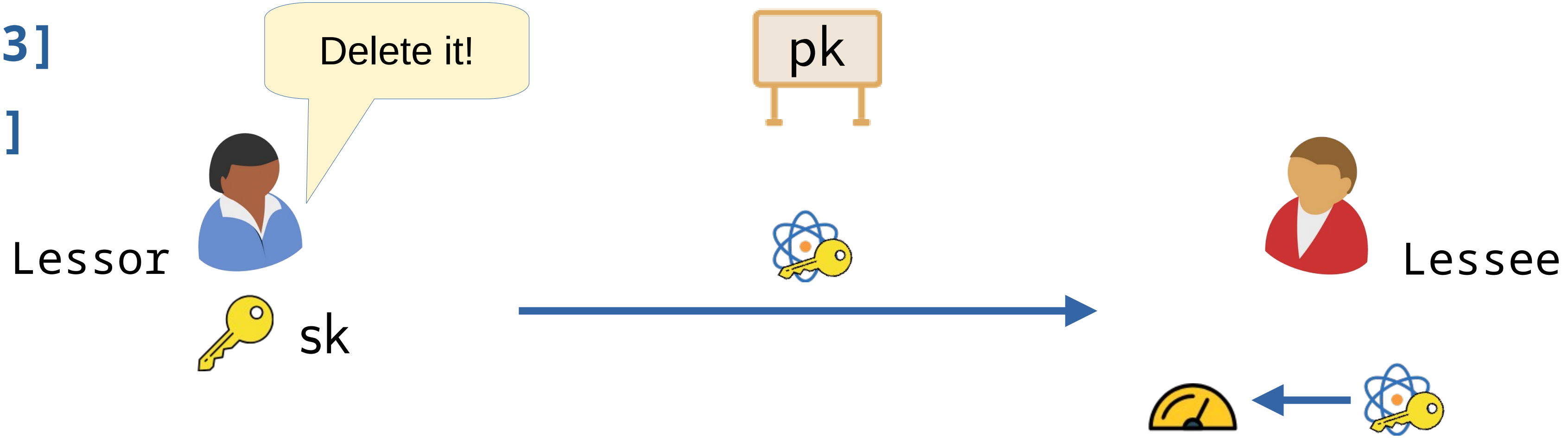
[APV23]



PKE with Secure Key Leasing

[AKN+23]

[APV23]



Delete it!

pk

Lessor

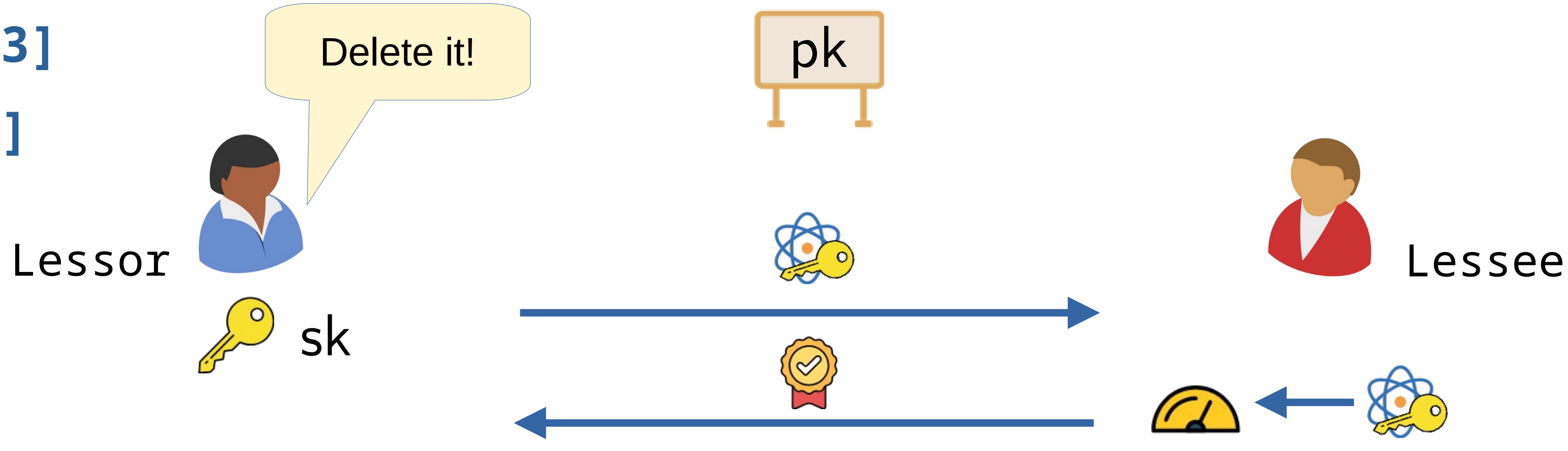
sk

Lessee

PKE with Secure Key Leasing

[AKN+23]

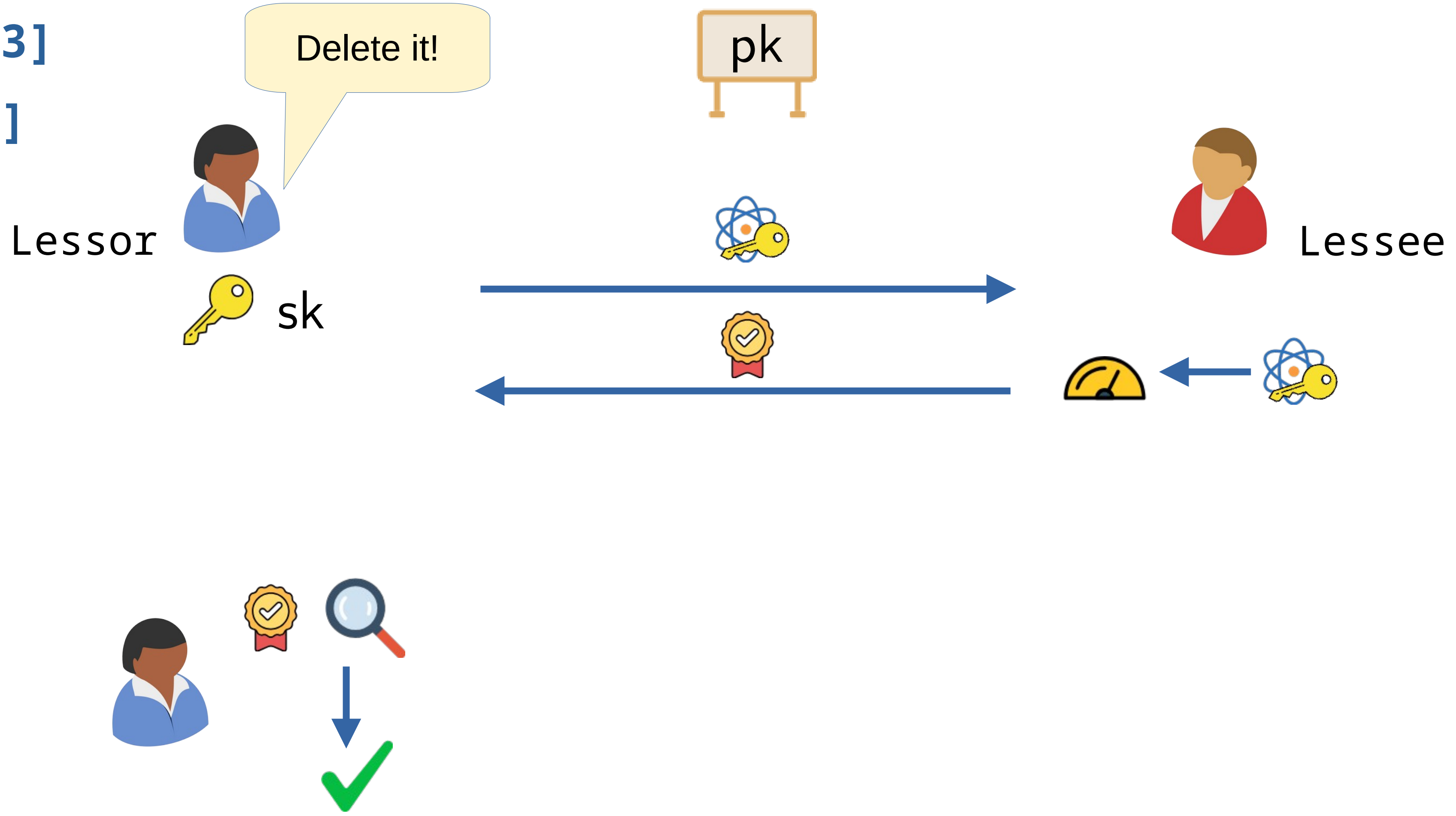
[APV23]



PKE with Secure Key Leasing

[AKN+23]

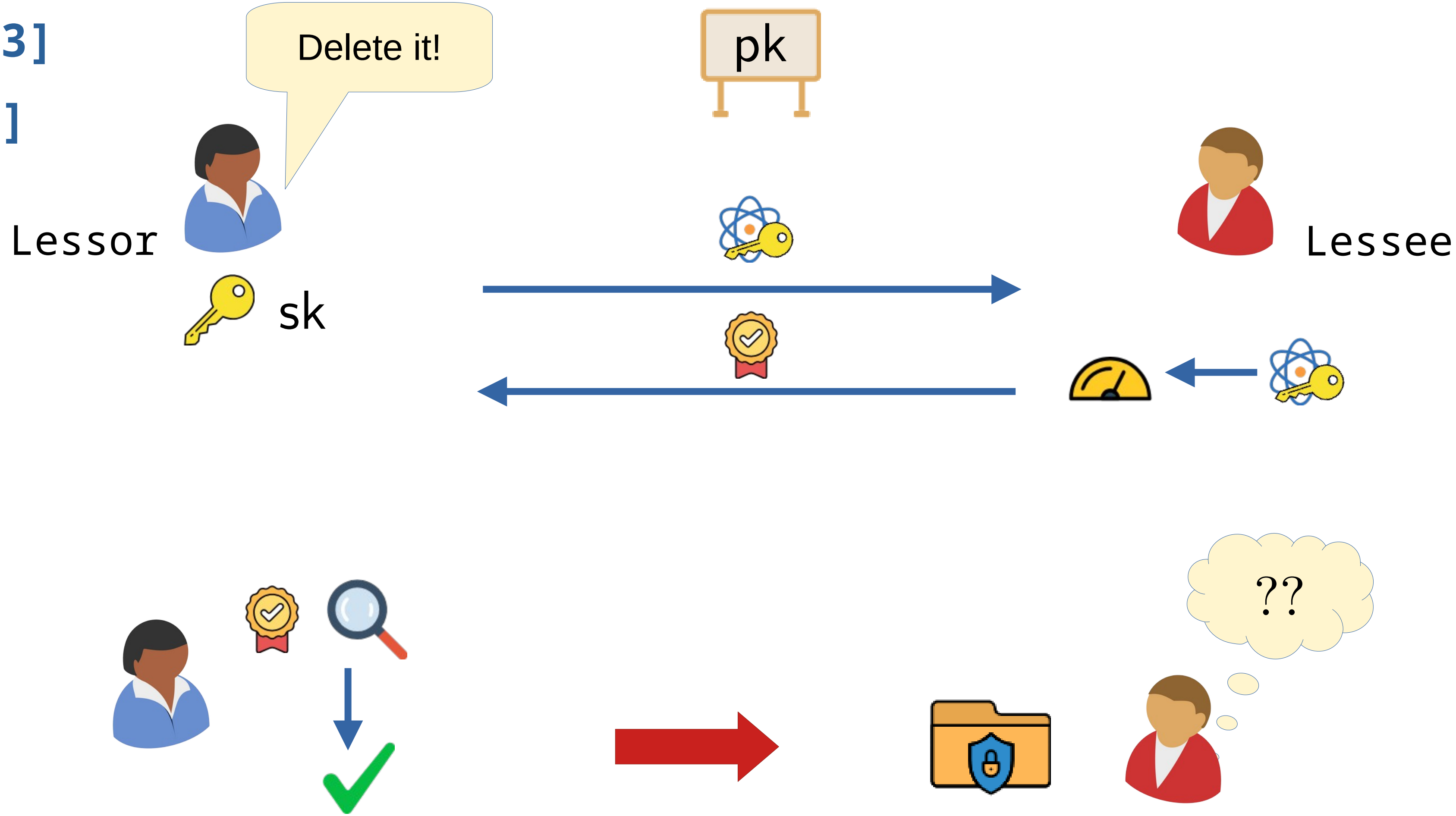
[APV23]



PKE with Secure Key Leasing

[AKN+23]

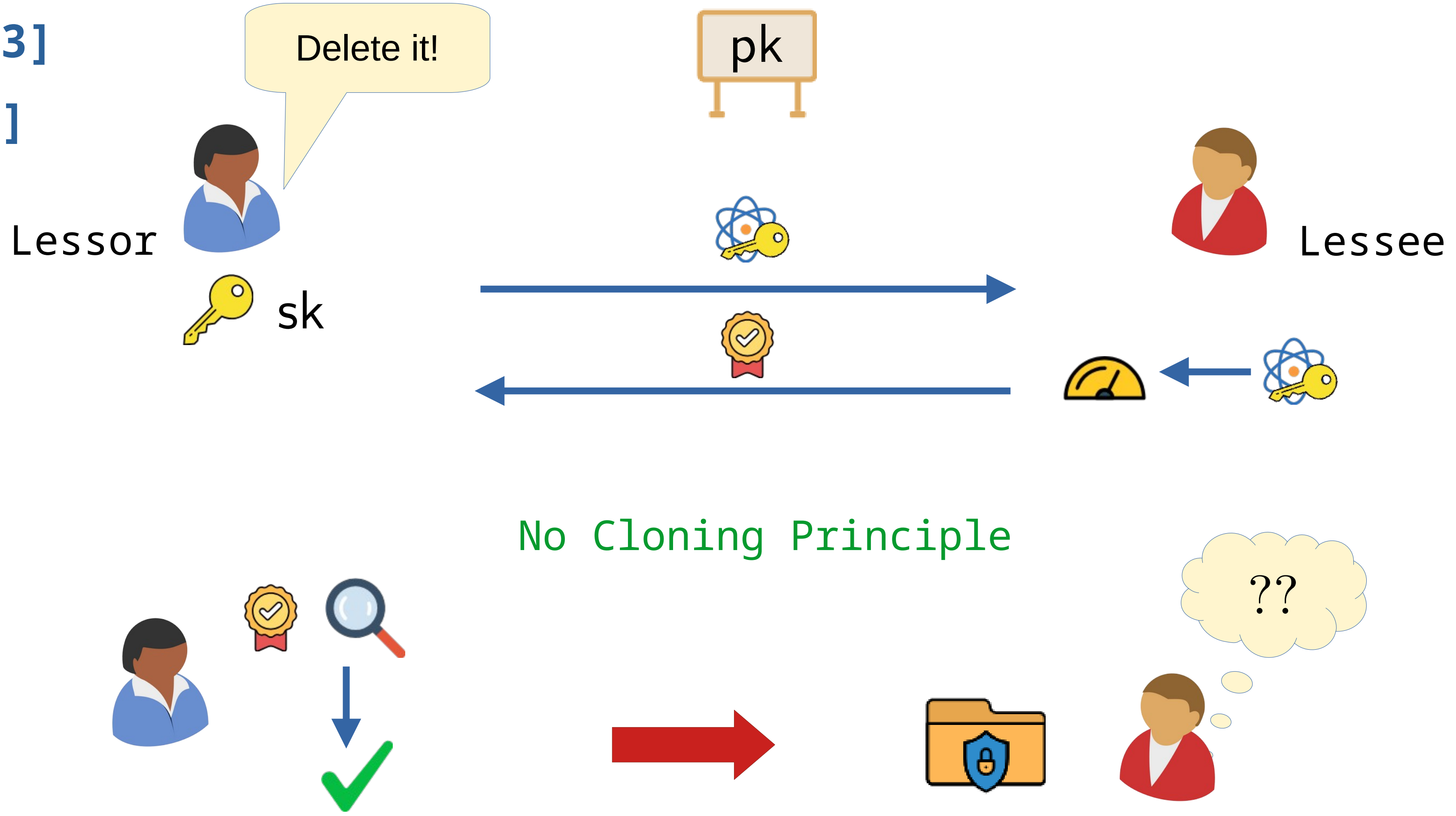
[APV23]



PKE with Secure Key Leasing

[AKN+23]

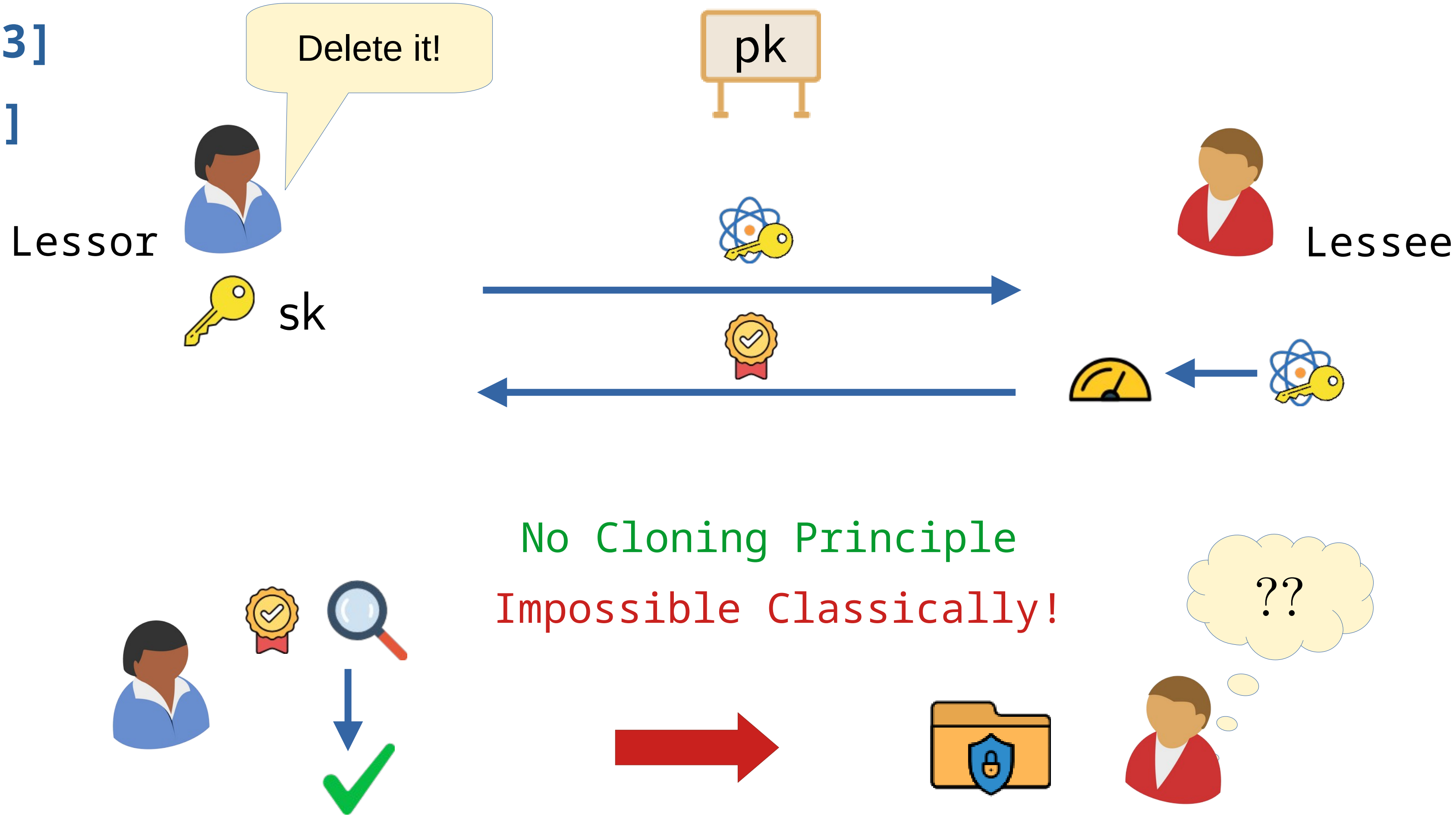
[APV23]



PKE with Secure Key Leasing

[AKN+23]

[APV23]



Delete it!

pk

Lessor

sk

Lessee

No Cloning Principle

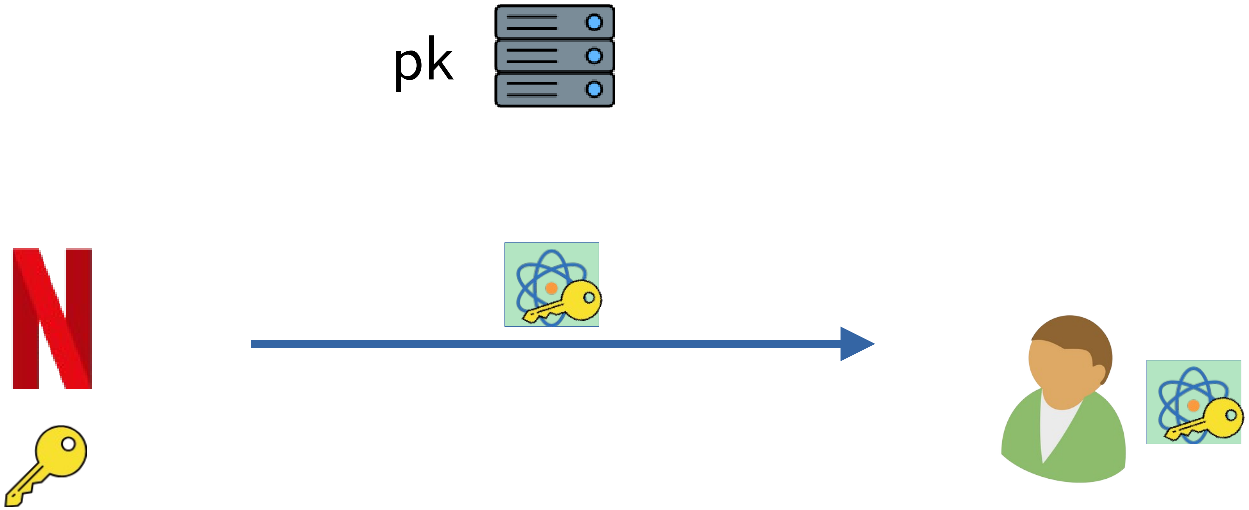
Impossible Classically!

??

Collusion-Resistance

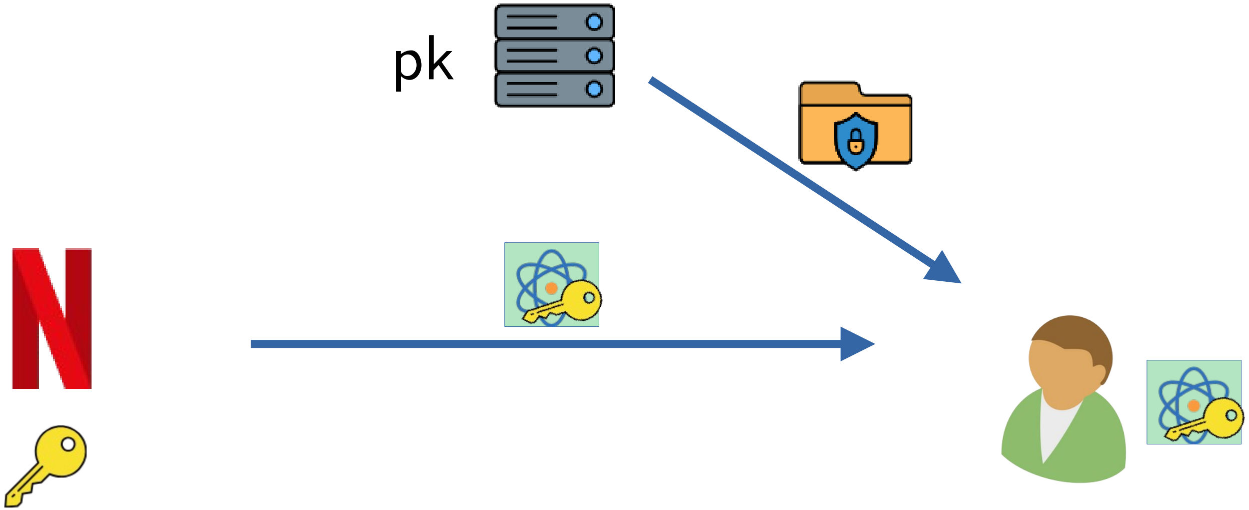
Collusion-Resistance

Collusion-Resistance

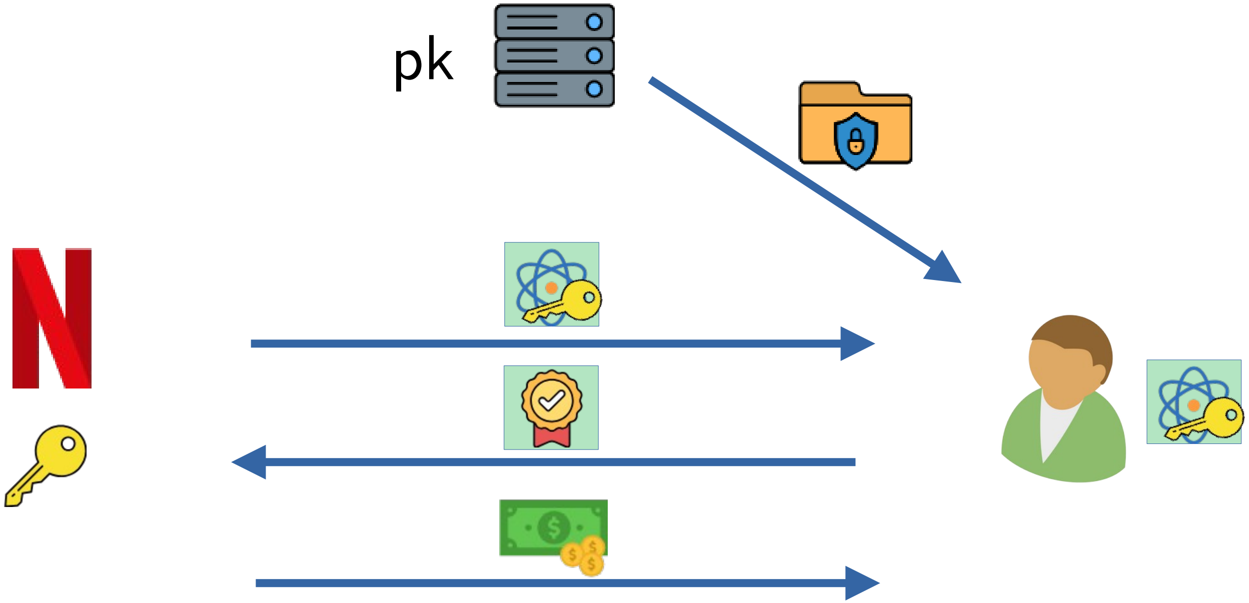


pk

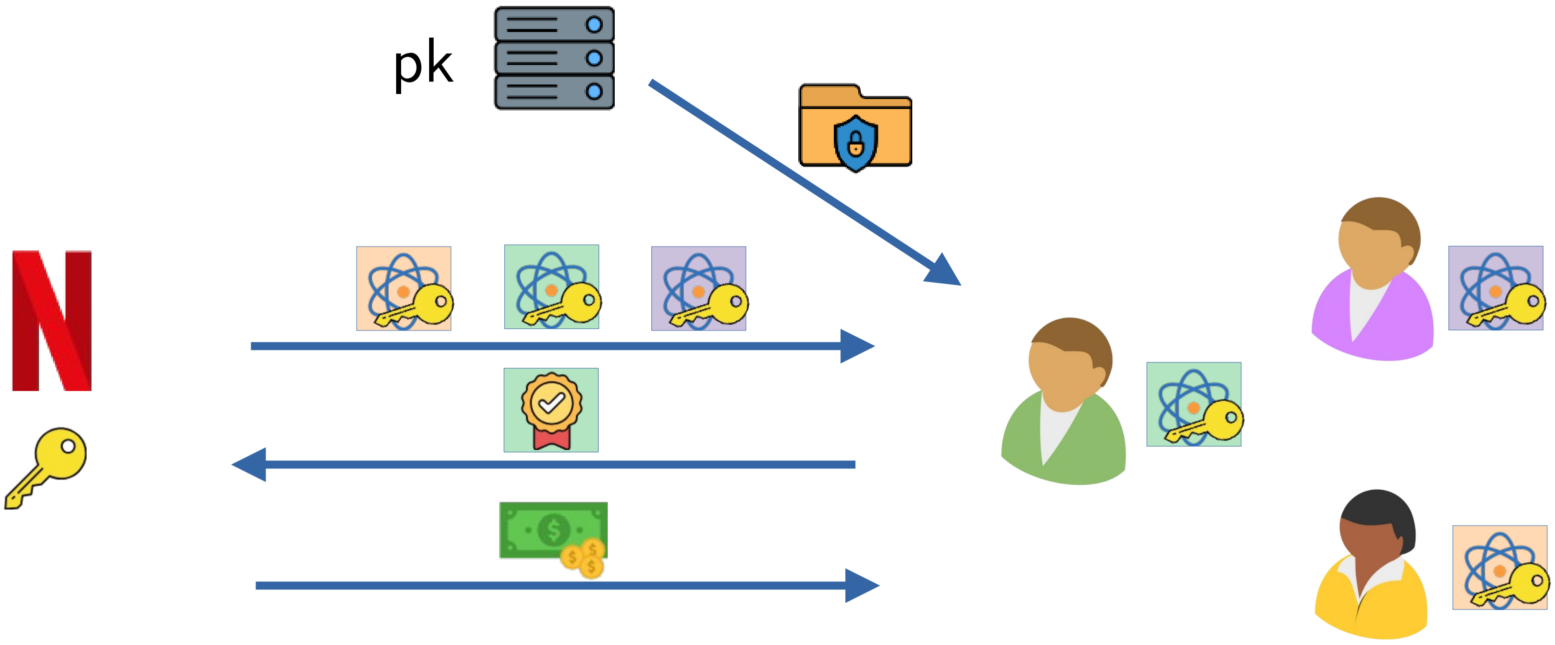
Collusion-Resistance



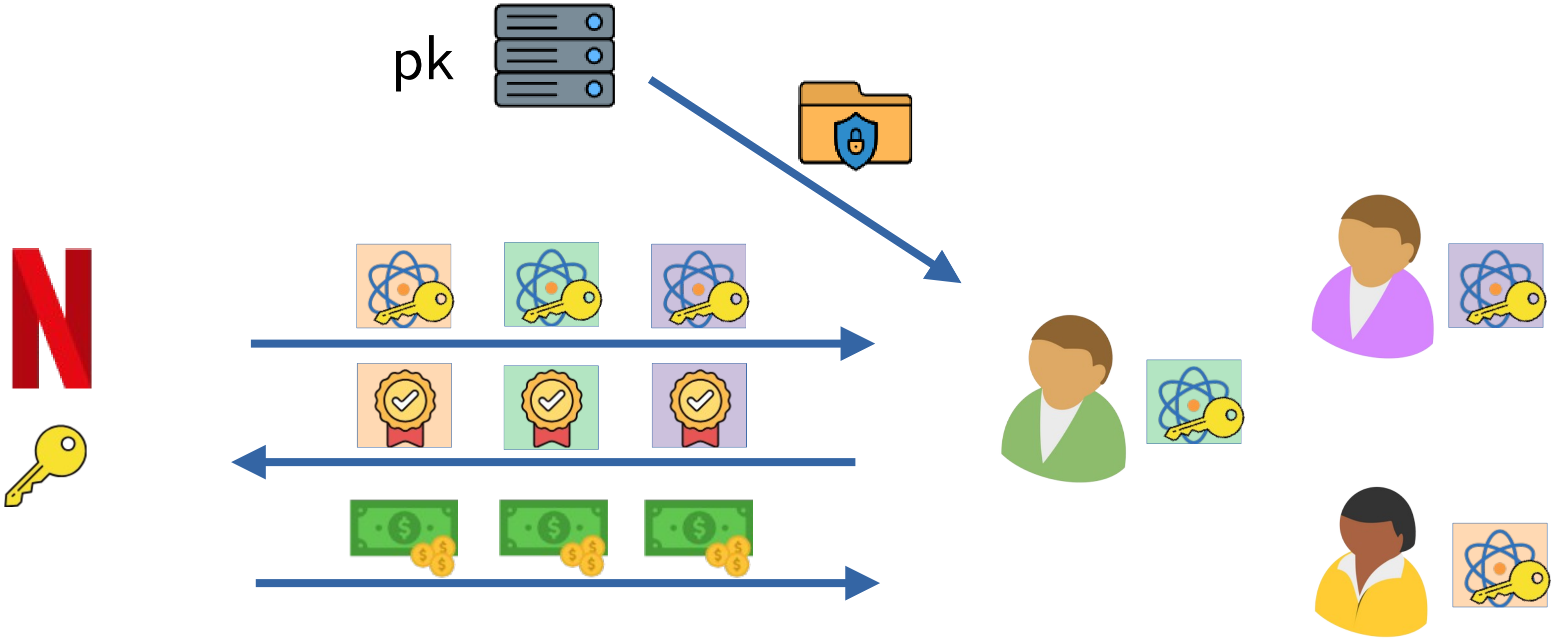
Collusion-Resistance



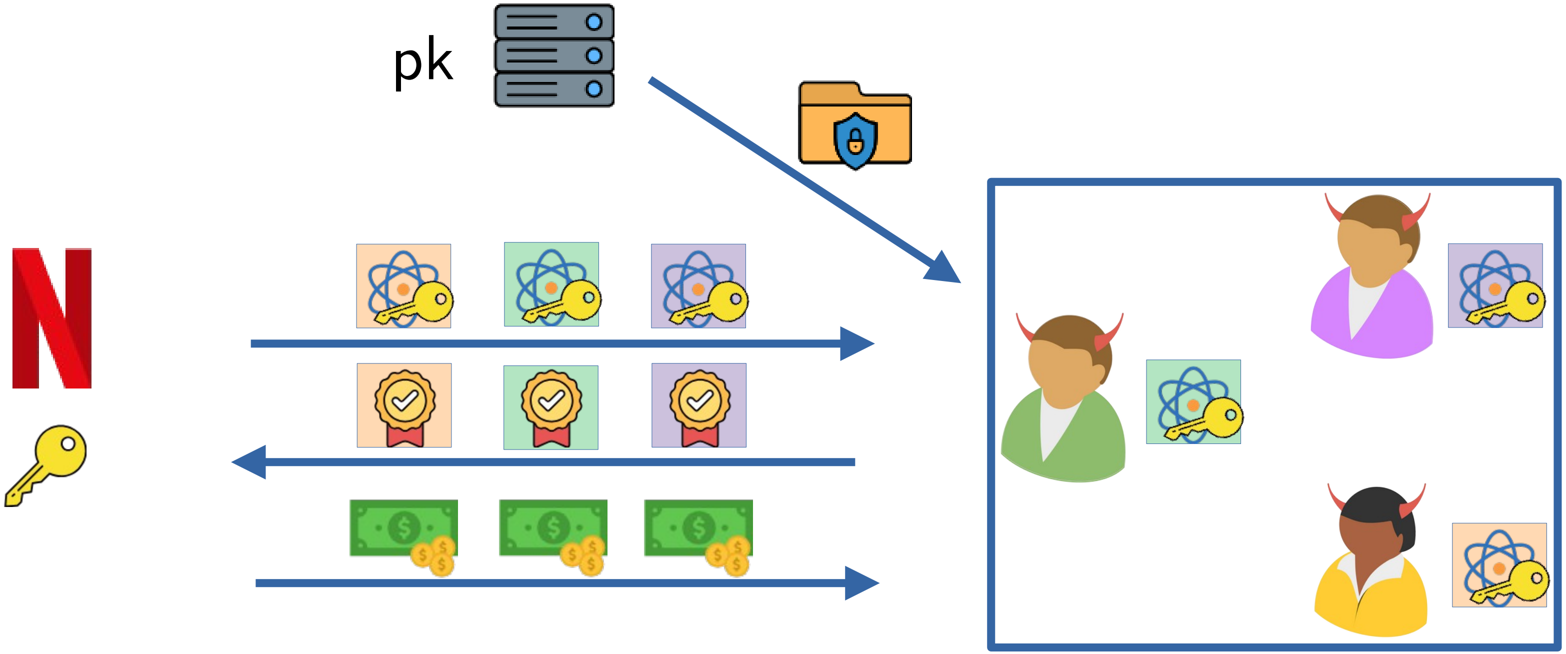
Collusion-Resistance



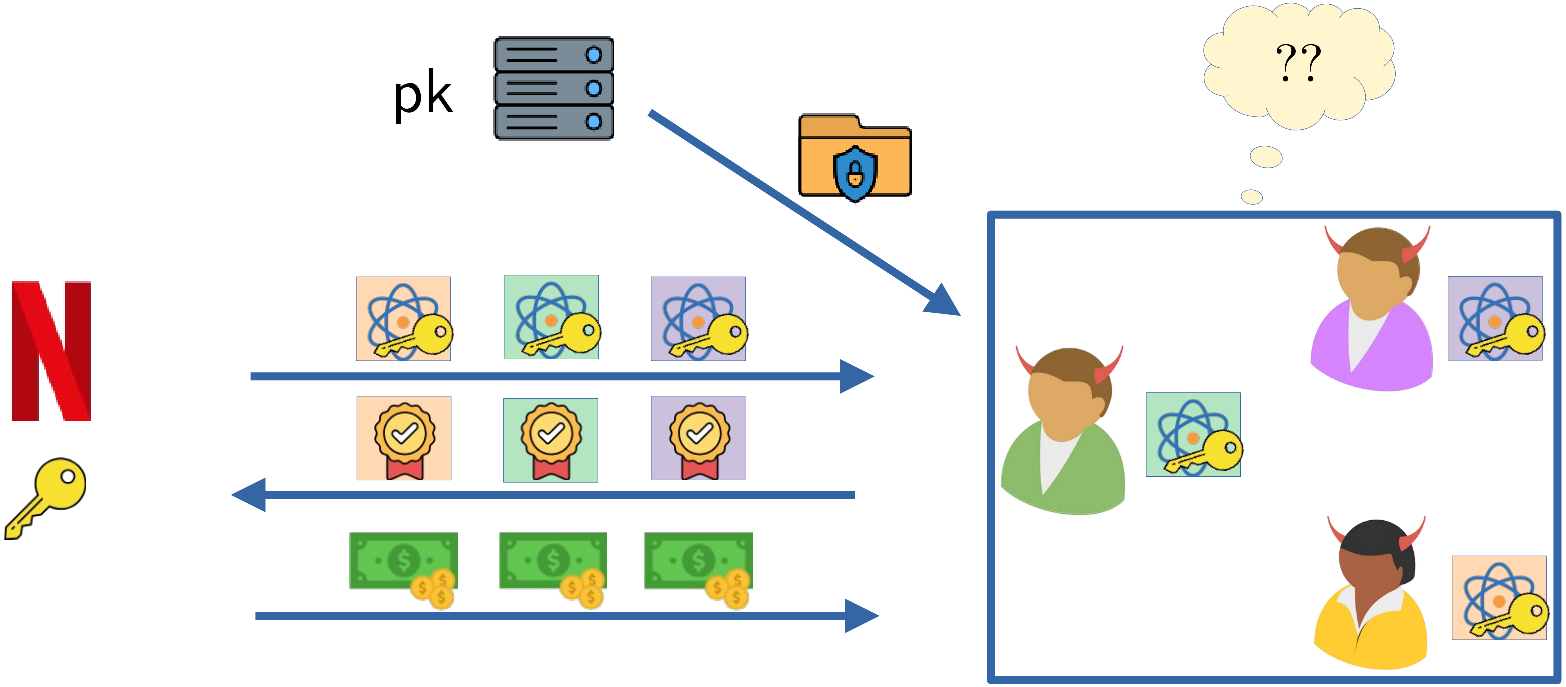
Collusion-Resistance



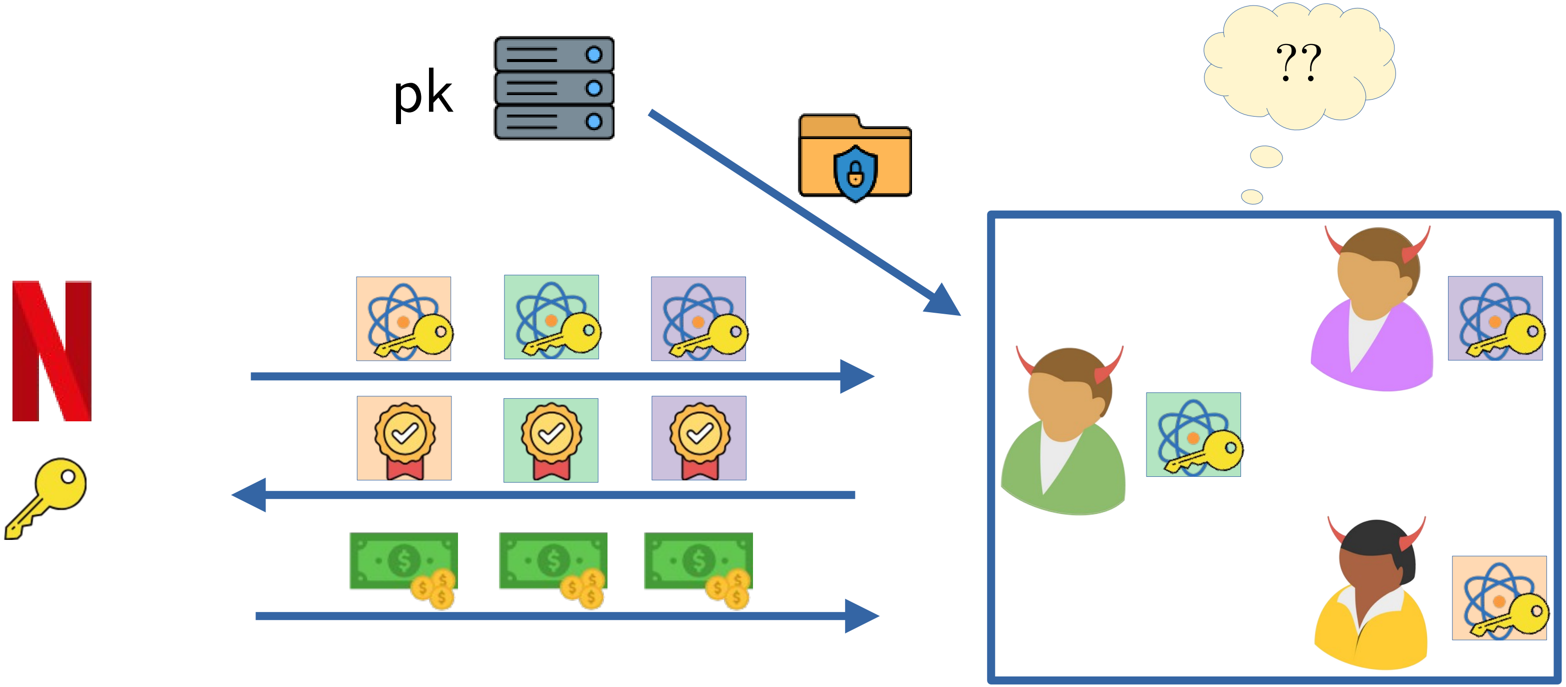
Collusion-Resistance



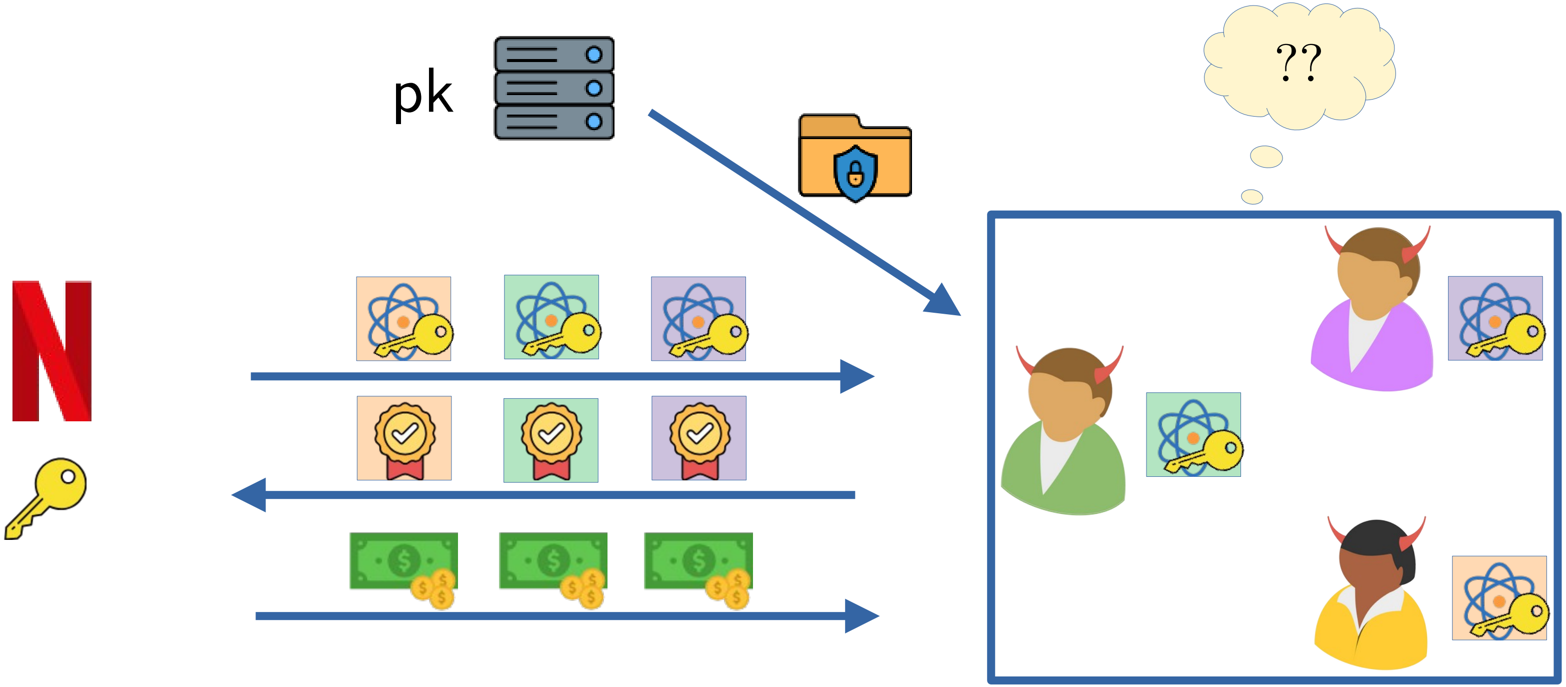
Collusion-Resistance



Collusion-Resistance



Collusion-Resistance



Unbounded Collusion-Resistance: Paramaters scale poly-logarithmically with the number of users.

Prior Work

Prior Work

[AKN+23, APV23, AHH24, CGJL25, KMY25]:

- Various PKE-SKL Constructions
- Standard Assumptions

Prior Work

[AKN+23, APV23, AHH24, CGJL25, KMY25]:

- Various PKE-SKL Constructions
- Standard Assumptions

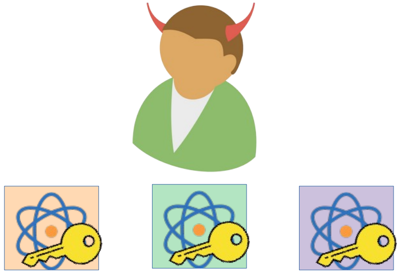
⚠ Completely Broken with Collusions

Prior Work

[AKN+23, APV23, AHH24, CGJL25, KMY25]:

- Various PKE-SKL Constructions
- Standard Assumptions

⚠ Completely Broken with Collusions

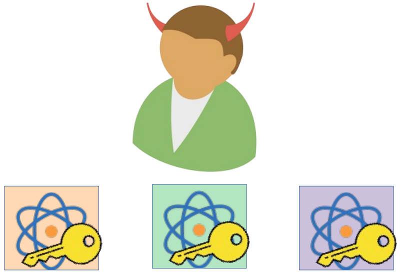


Prior Work

[AKN+23, APV23, AHH24, CGJL25, KMY25]:

- Various PKE-SKL Constructions
- Standard Assumptions

⚠ Completely Broken with Collusions



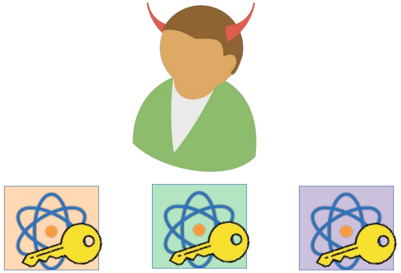
1) Correlate keys before deletion

Prior Work

[AKN+23, APV23, AHH24, CGJL25, KMY25]:

- Various PKE-SKL Constructions
- Standard Assumptions

⚠ Completely Broken with Collusions



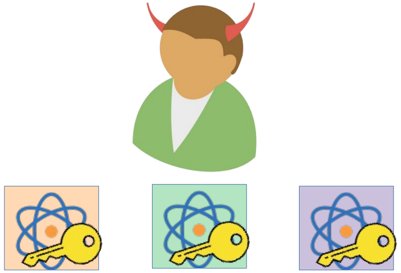
1) Correlate keys before deletion
2) Learn crucial classical info

Prior Work

[AKN+23, APV23, AHH24, CGJL25, KMY25]:

- Various PKE-SKL Constructions
- Standard Assumptions

⚠ Completely Broken with Collusions



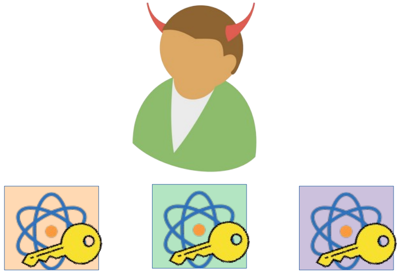
1) Correlate keys before deletion
2) Learn crucial classical info
3) Leave states undisturbed

Prior Work

[AKN+23, APV23, AHH24, CGJL25, KMY25]:

- Various PKE-SKL Constructions
- Standard Assumptions

⚠ Completely Broken with Collusions

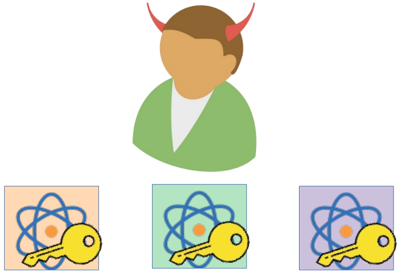


1) Correlate keys before deletion
2) Learn crucial classical info
3) Leave states undisturbed

⚠ Challenging Setting.

Prior Work

[AKN+23, APV23, AHH24, CGJL25, KMY25]:



- Various PKE-SKL Constructions
- Standard Assumptions

⚠ Completely Broken with Collusions

1) Correlate keys before deletion
2) Learn crucial classical info
3) Leave states undisturbed

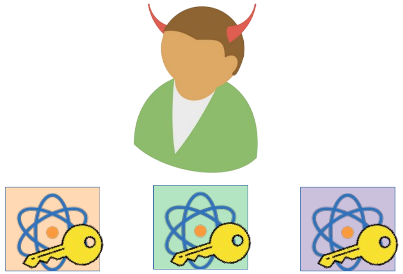
⚠ Challenging Setting.
Provable-Security even more so!

Prior Work

[AKN+23, APV23, AHH24, CGJL25, KMY25]:

- Various PKE-SKL Constructions
- Standard Assumptions

⚠ Completely Broken with Collusions



1) Correlate keys before deletion
2) Learn crucial classical info
3) Leave states undisturbed

⚠ Challenging Setting.
Provable-Security even more so!

[AKN+23, BGK+24]:

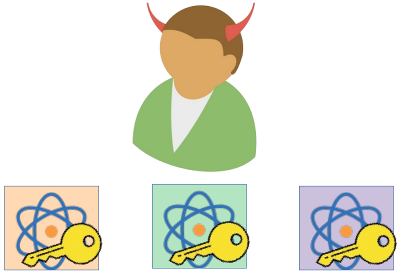
- (Bounded + Unbounded) Collusion-Resistant Constructions

Prior Work

[AKN+23, APV23, AHH24, CGJL25, KMY25]:

- Various PKE-SKL Constructions
- Standard Assumptions

⚠ Completely Broken with Collusions



1) Correlate keys before deletion
2) Learn crucial classical info
3) Leave states undisturbed

⚠ Challenging Setting.
Provable-Security even more so!

[AKN+23, BGK+24]:

- (Bounded + Unbounded) Collusion-Resistant Constructions

⚠ Bounded is Inefficient. Unbounded rely on FE/IO (Strong! Post-Quantum?)

Our Contributions

[KNP25]:

Our Contributions

[KNP25]:

1) Collusion-Resistant Definition:

Our Contributions

[KNP25]:

1) Collusion-Resistant Definition: PKE-CR-SKL

Our Contributions

[KNP25]:

1) Collusion-Resistant Definition: PKE-CR-SKL

2)

Our Contributions

[KNP25]:

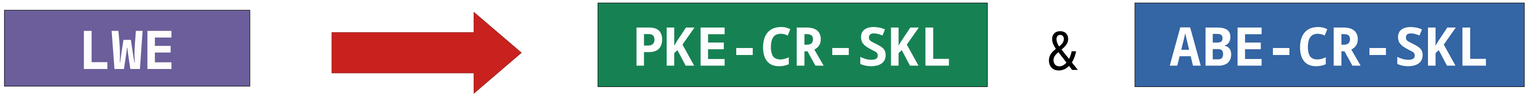
1) Collusion-Resistant Definition: **PKE-CR-SKL**

2) **LWE** → **PKE-CR-SKL**

Our Contributions

[KNP25]:

1) Collusion-Resistant Definition: PKE-CR-SKL

2)

LWE

PKE-CR-SKL & ABE-CR-SKL

Our Contributions

[KNP25]:

1) Collusion-Resistant Definition: PKE-CR-SKL

2) LWE → PKE-CR-SKL & ABE-CR-SKL

3) New Techniques and Building Blocks:

Our Contributions

[KNP25]:

1) Collusion-Resistant Definition: PKE-CR-SKL

2) LWE → PKE-CR-SKL & ABE-CR-SKL

3) New Techniques and Building Blocks: SKE-CR-SKL

Our Contributions

[KNP25]:

1) Collusion-Resistant Definition: PKE-CR-SKL

2) LWE → PKE-CR-SKL & ABE-CR-SKL

3) New Techniques and Building Blocks: SKE-CR-SKL

4) Multi-Input ABE → Variant w/ Classical

Main Result

[KNP25]

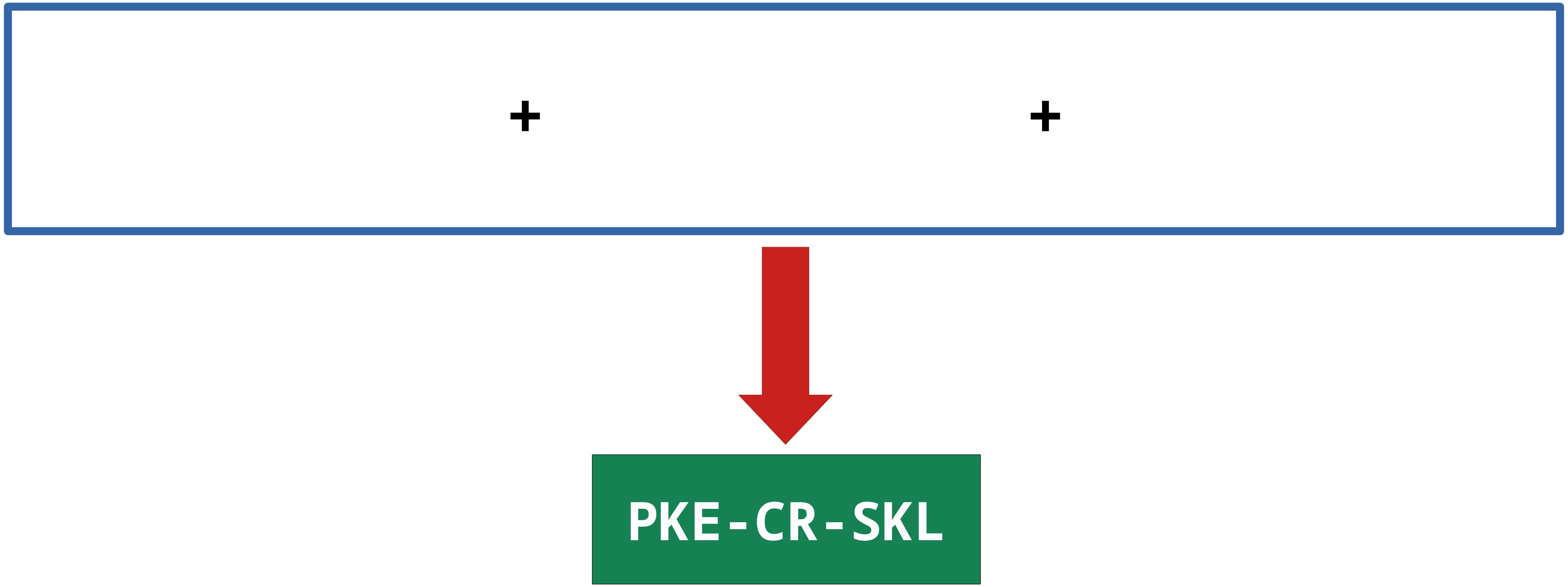
Main Result

[KNP25]

PKE-CR-SKL

Main Result

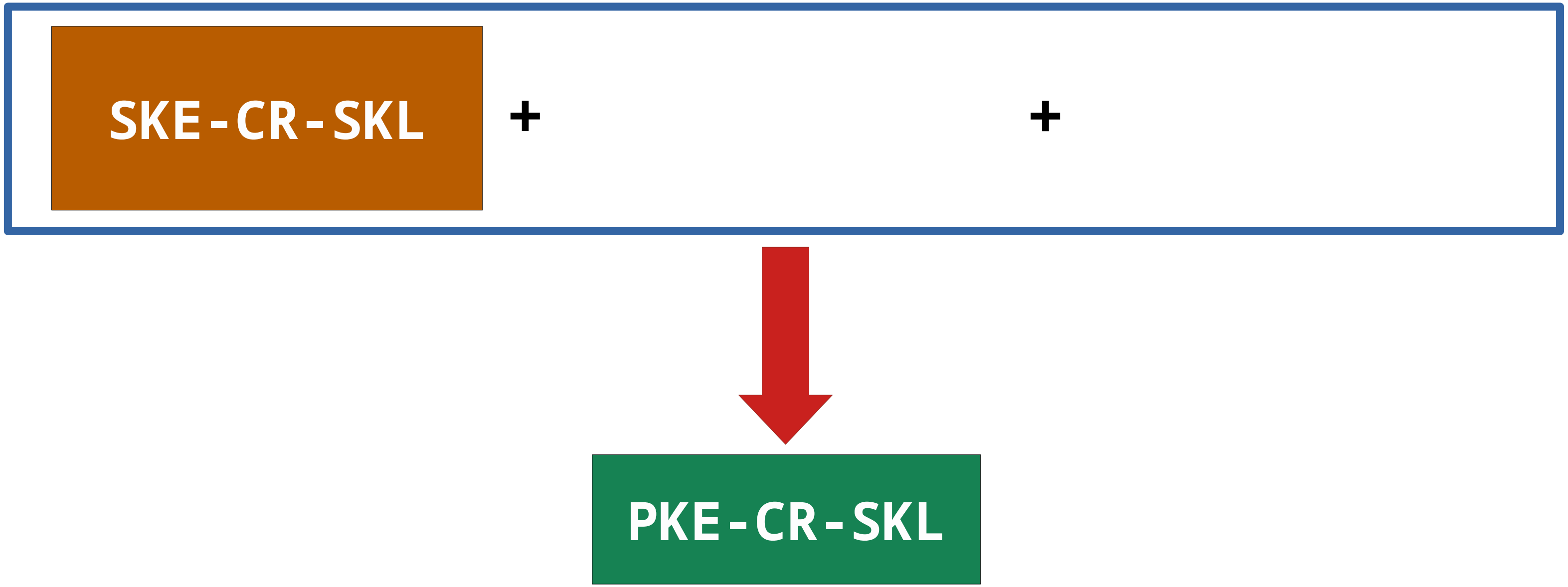
[KNP25]



PKE-CR-SKL

Main Result

[KNP25]

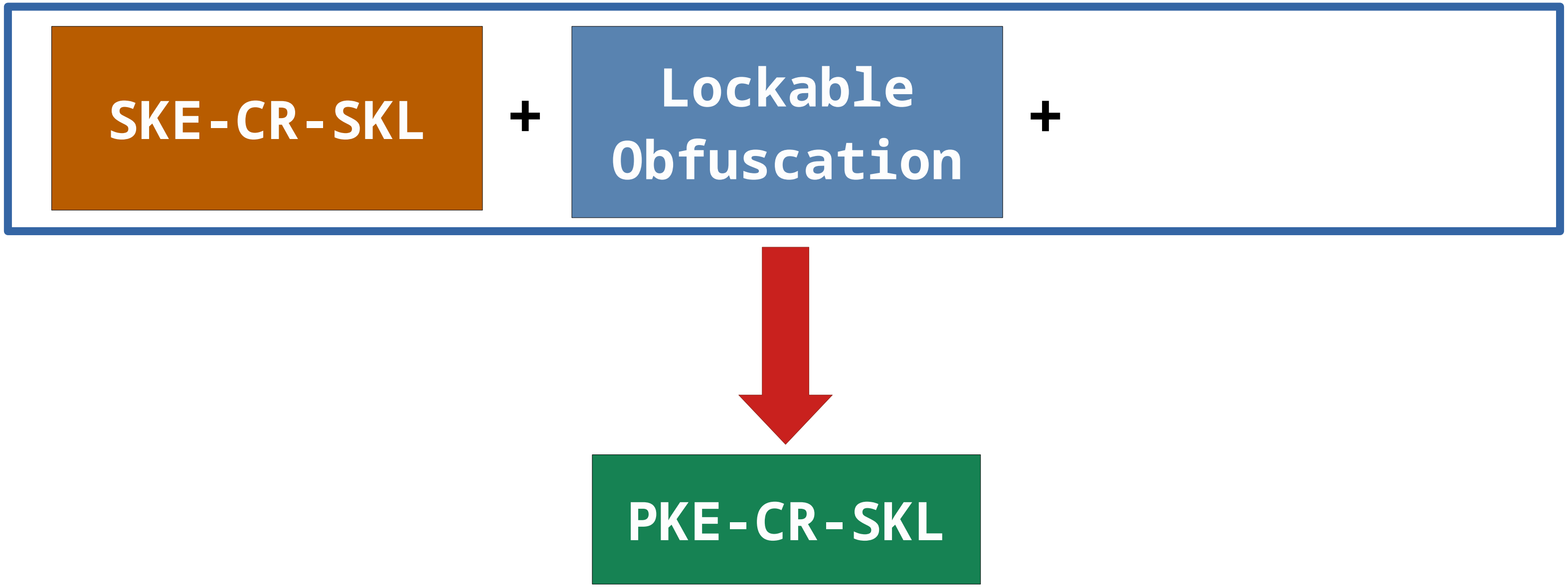


SKE-CR-SKL + +

PKE-CR-SKL

Main Result

[KNP25]

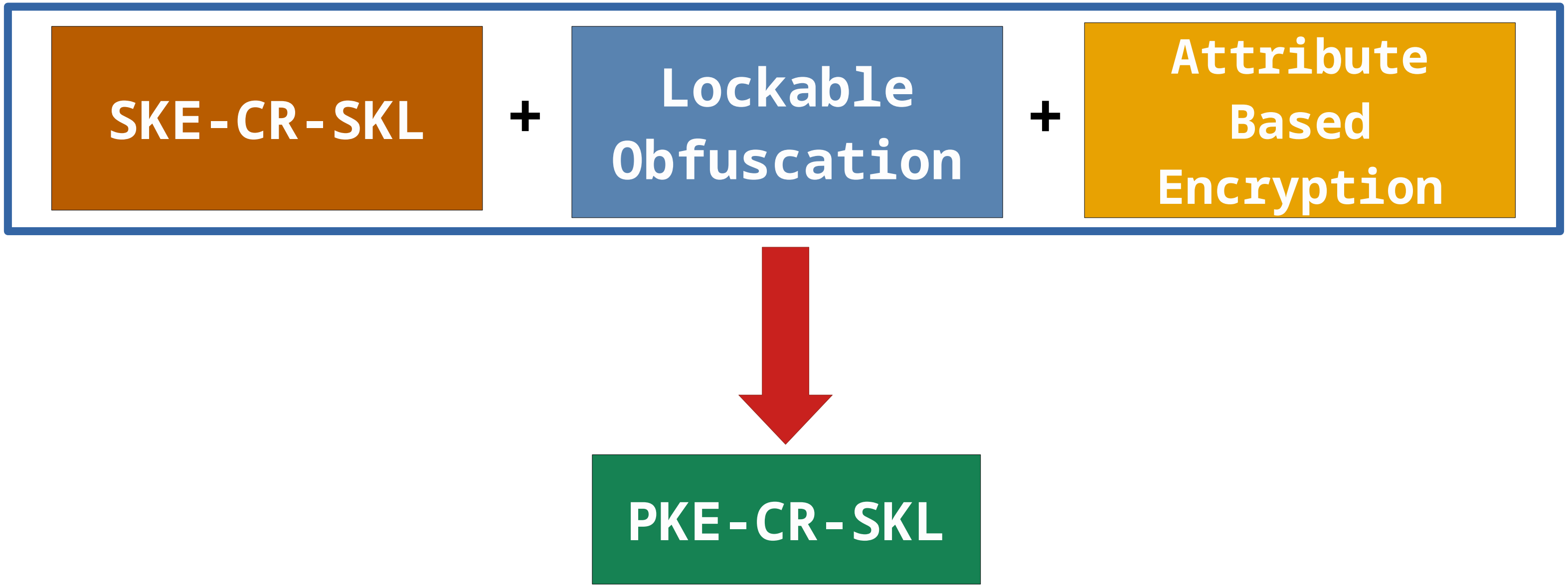


SKE-CR-SKL + Lockable Obfuscation +

PKE-CR-SKL

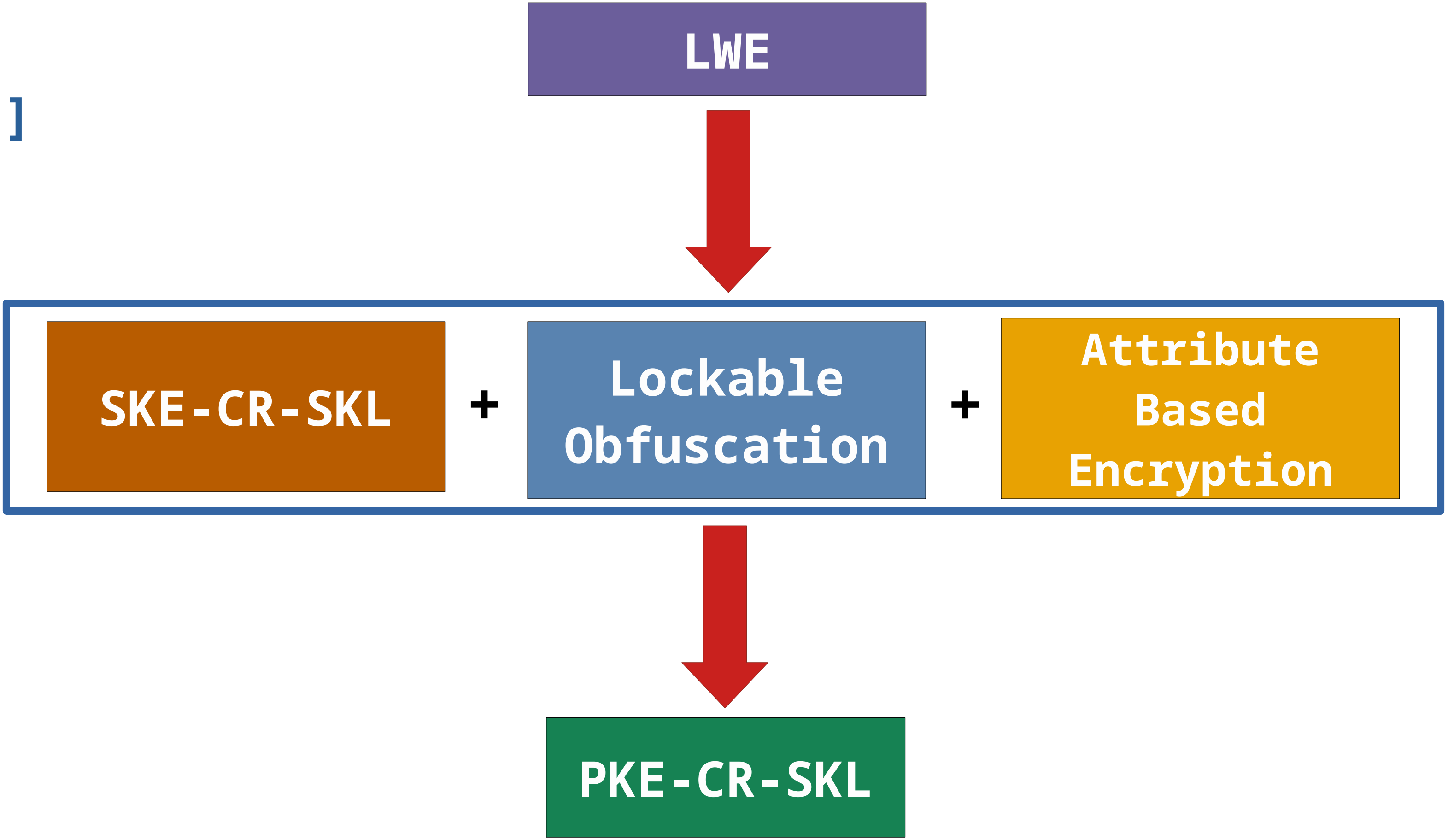
Main Result

[KNP25]



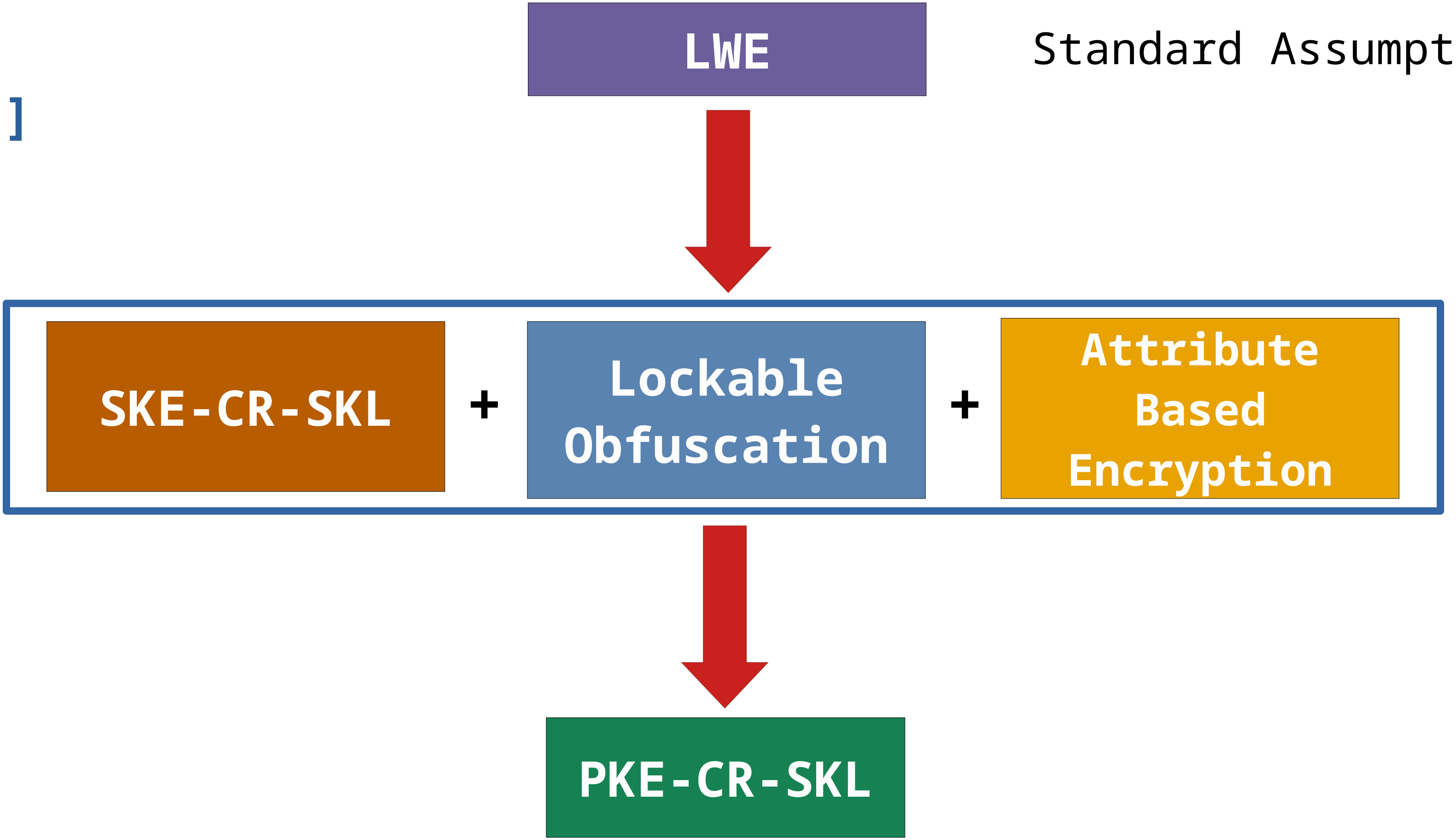
Main Result

[KNP25]



Main Result

[KNP25]



LWE

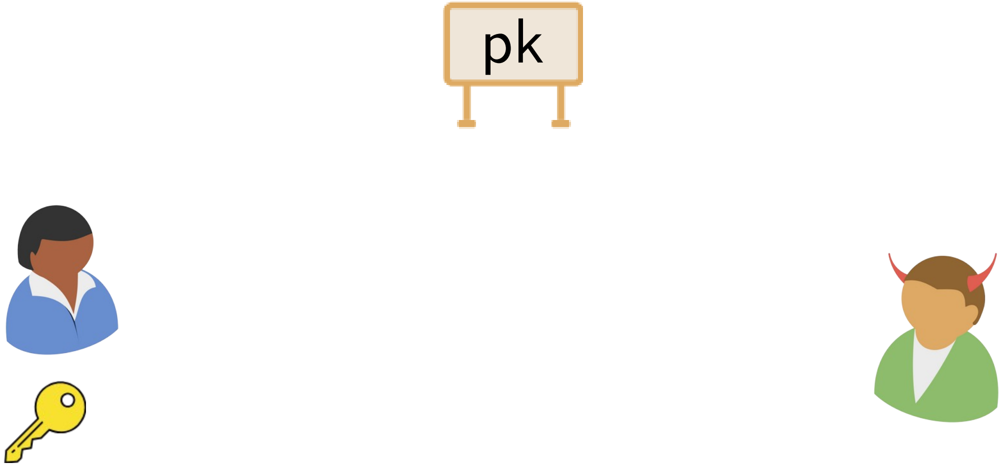
Standard Assumption

SKE-CR-SKL + Lockable Obfuscation + Attribute Based Encryption

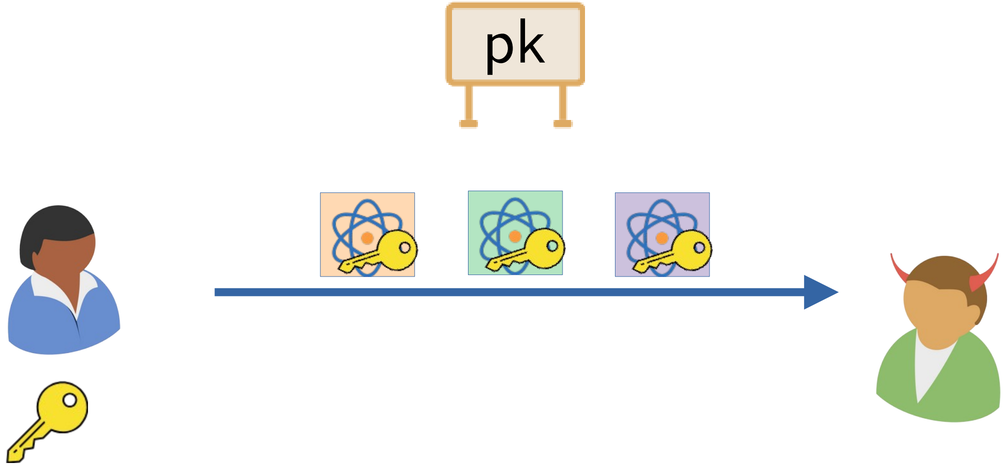
PKE-CR-SKL

PKE-CR-SKL and SKE-CR-SKL

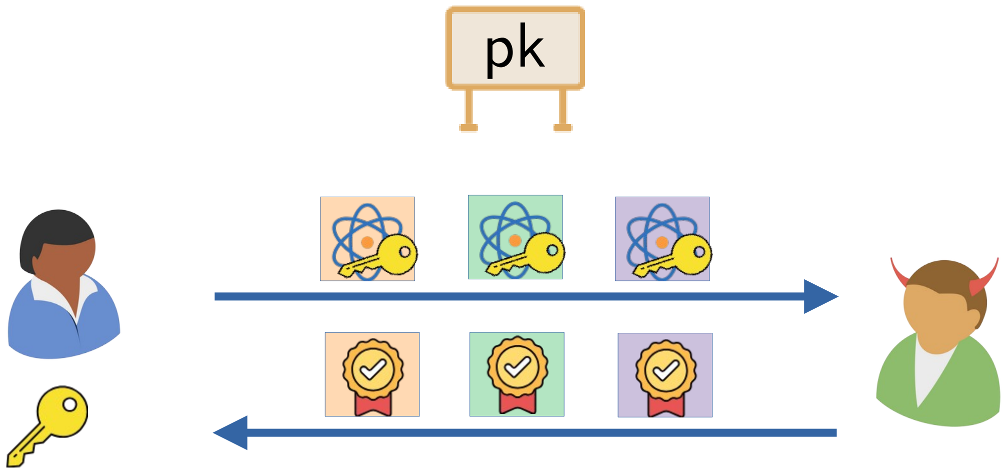
PKE-CR-SKL and SKE-CR-SKL



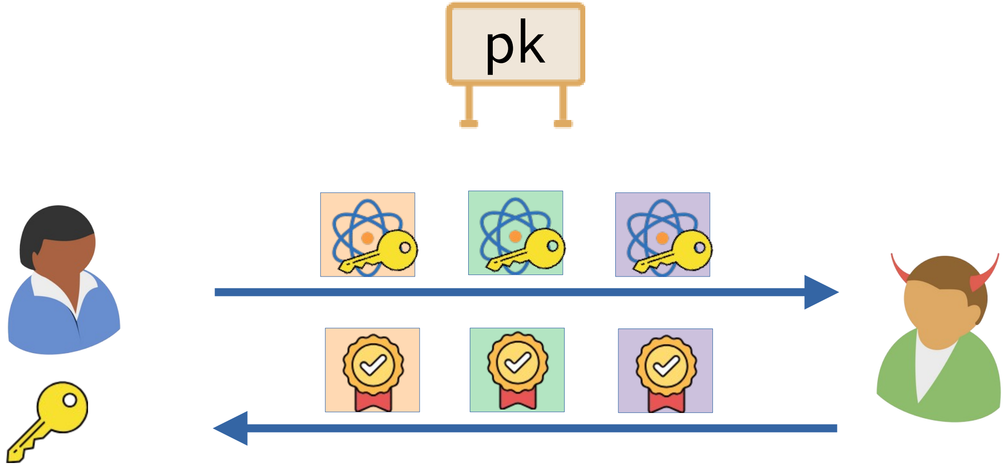
PKE-CR-SKL and SKE-CR-SKL

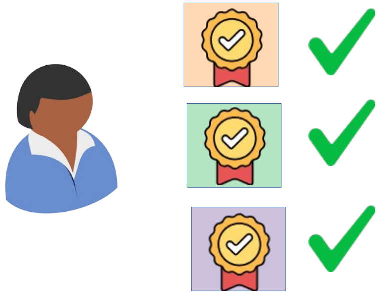


PKE-CR-SKL and SKE-CR-SKL

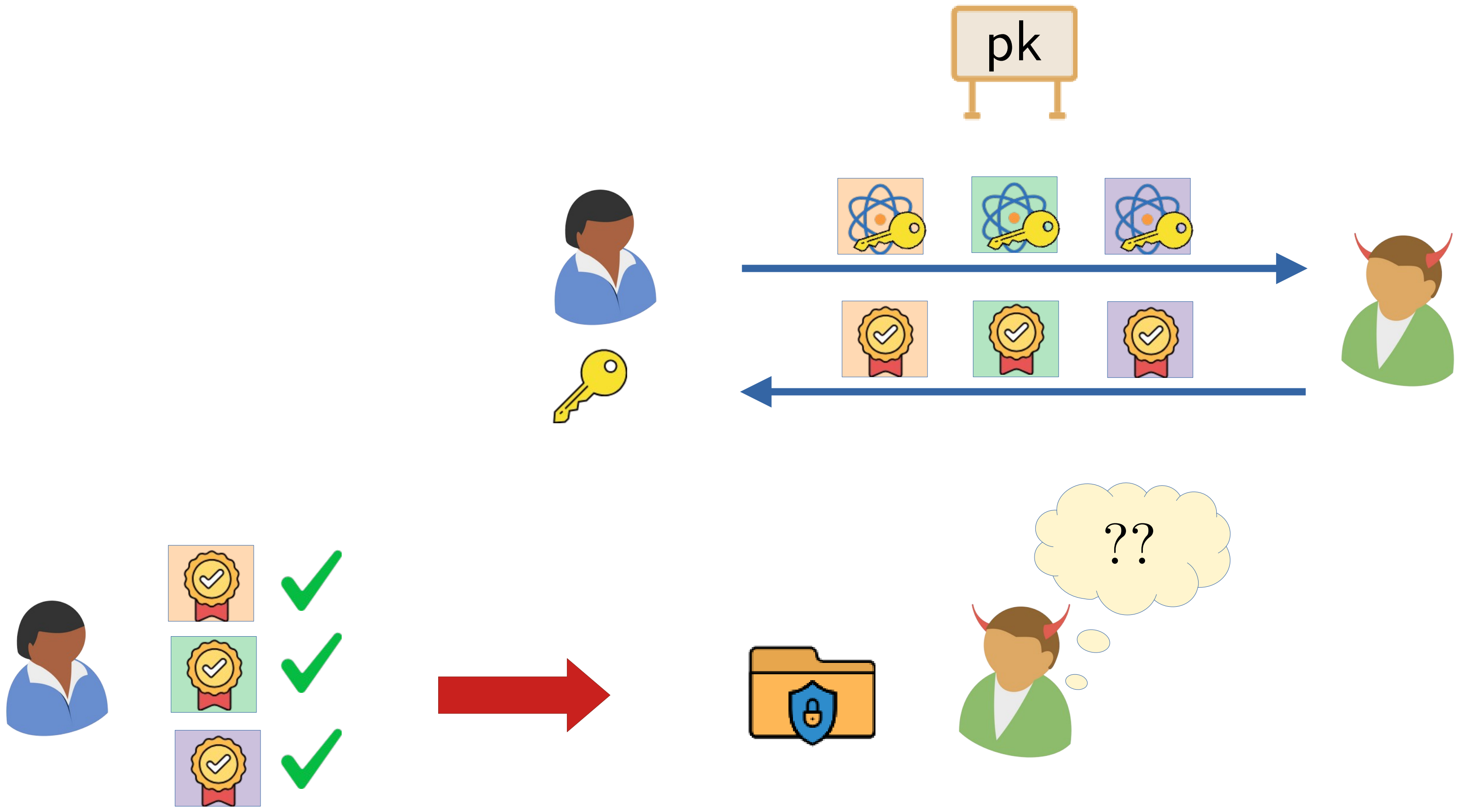


PKE-CR-SKL and SKE-CR-SKL



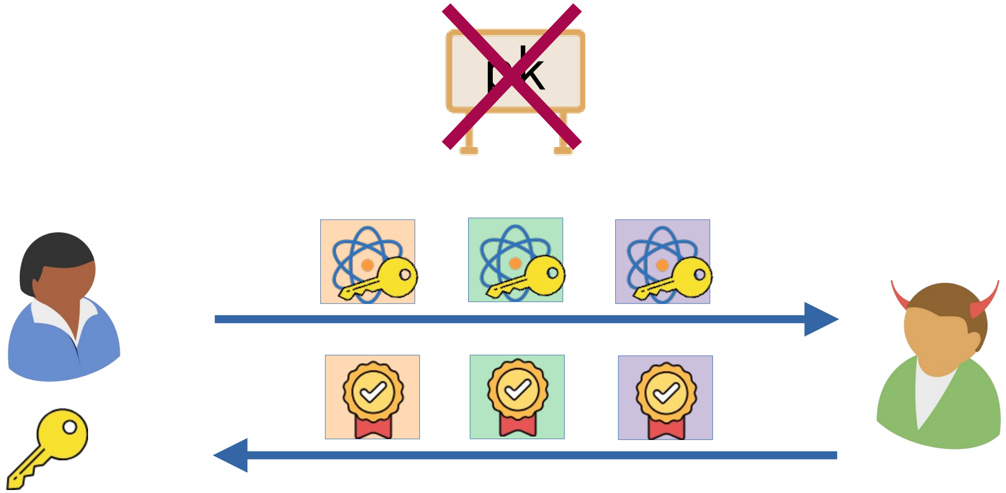


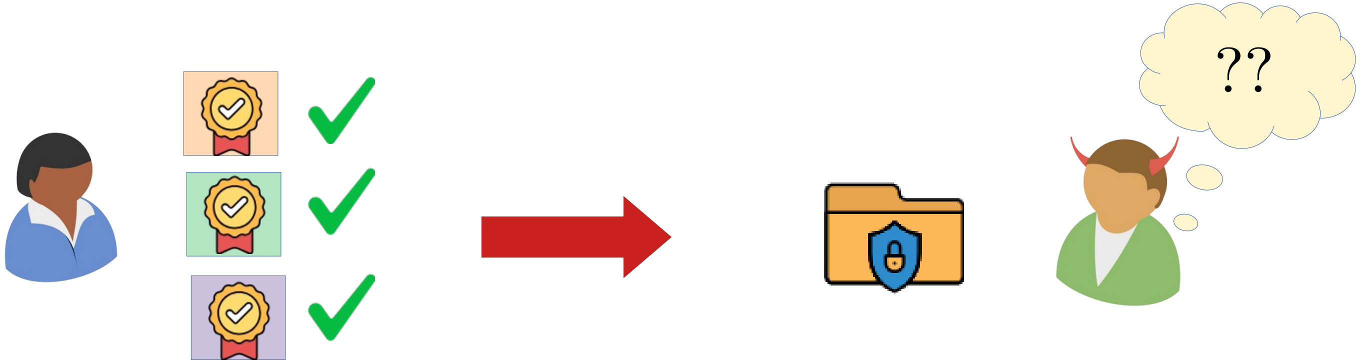
PKE-CR-SKL and SKE-CR-SKL



PKE-CR-SKL and SKE-CR-SKL

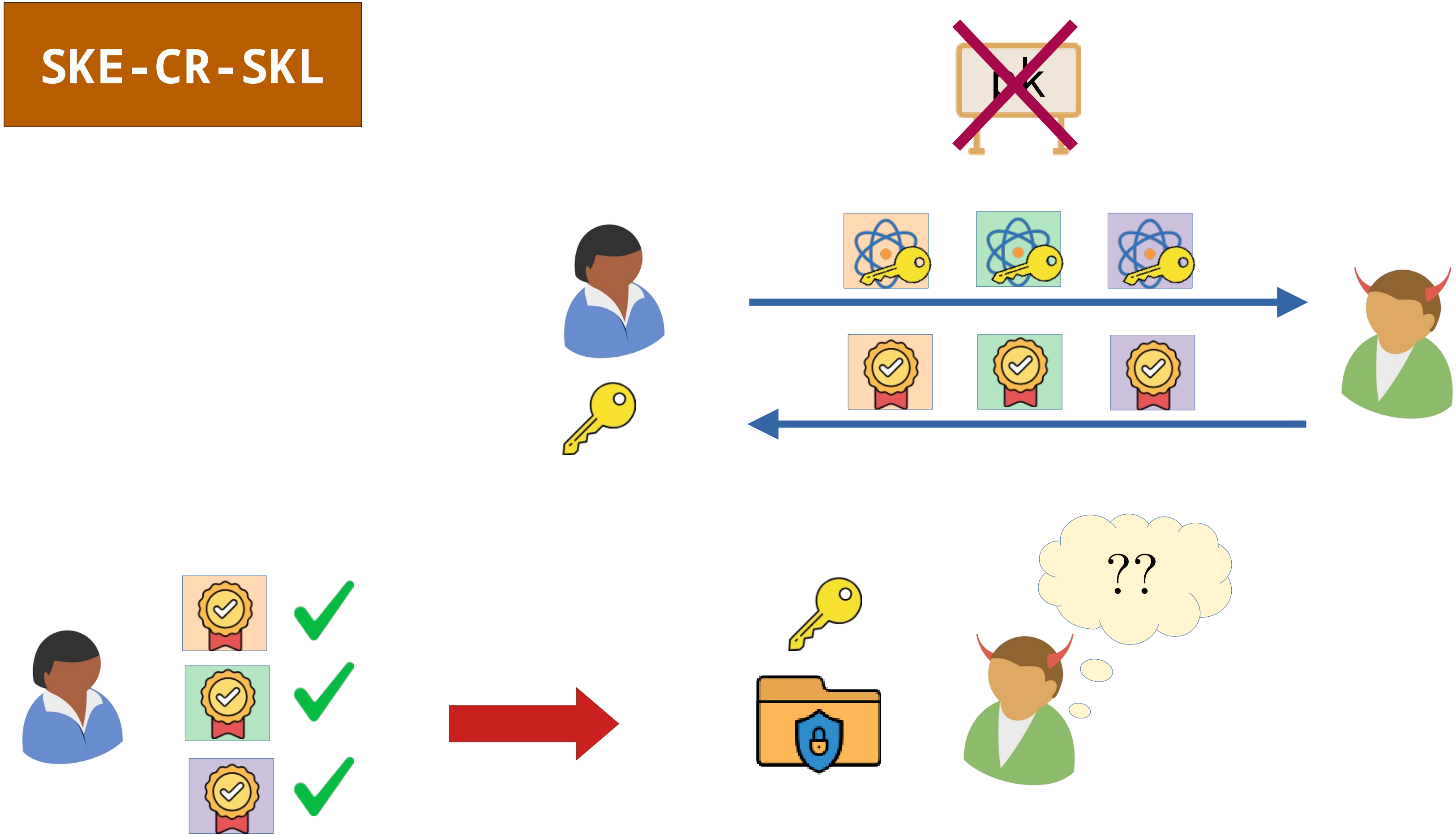
SKE-CR-SKL





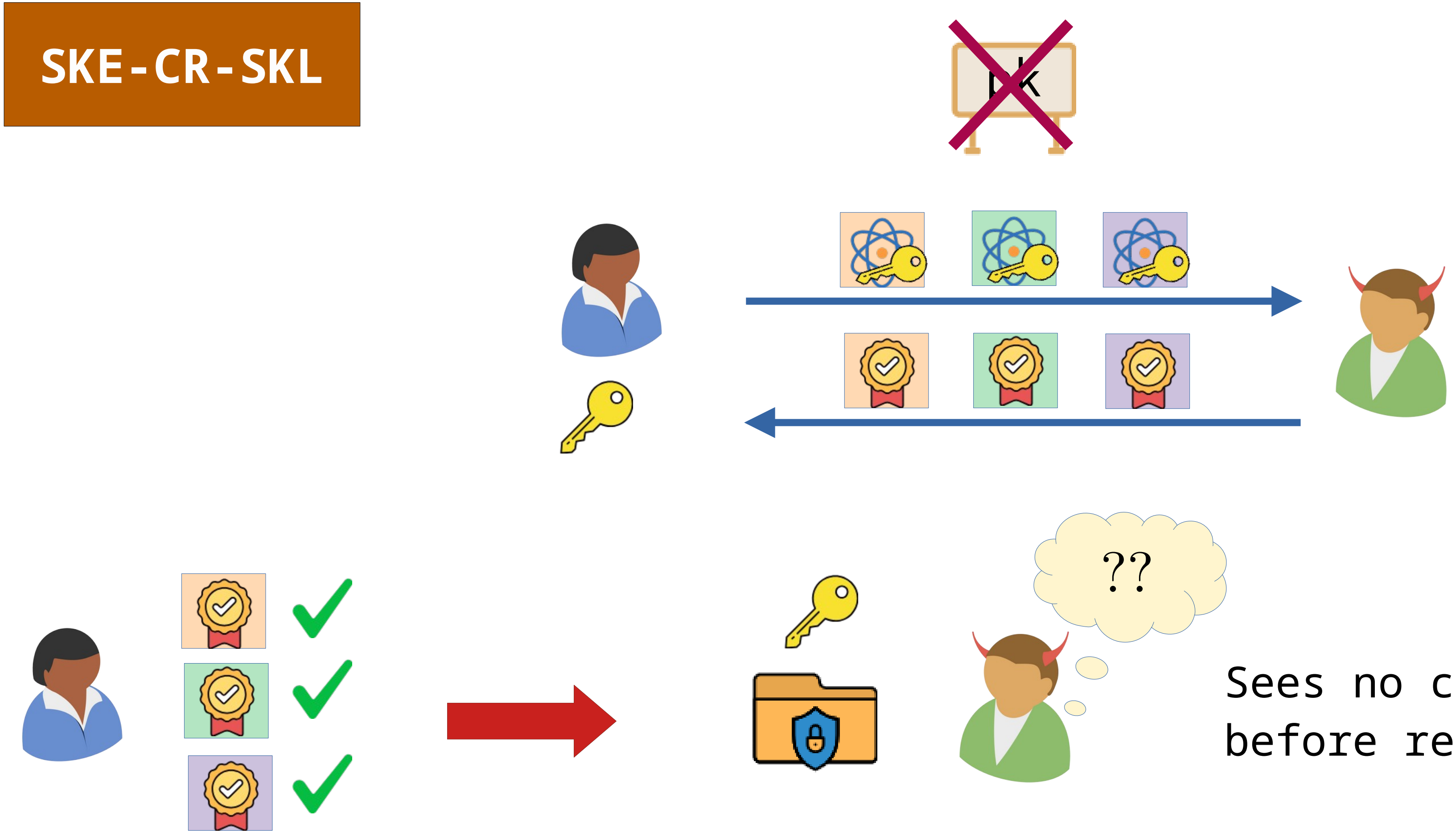
PKE-CR-SKL and SKE-CR-SKL

SKE-CR-SKL



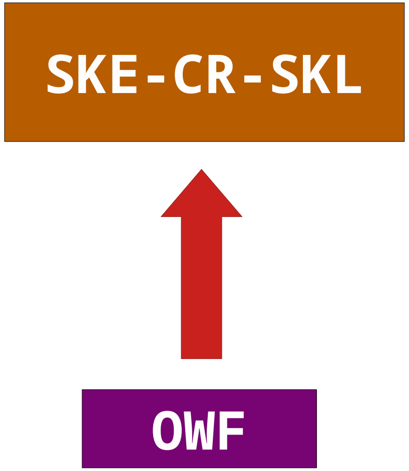
PKE-CR-SKL and SKE-CR-SKL

SKE-CR-SKL



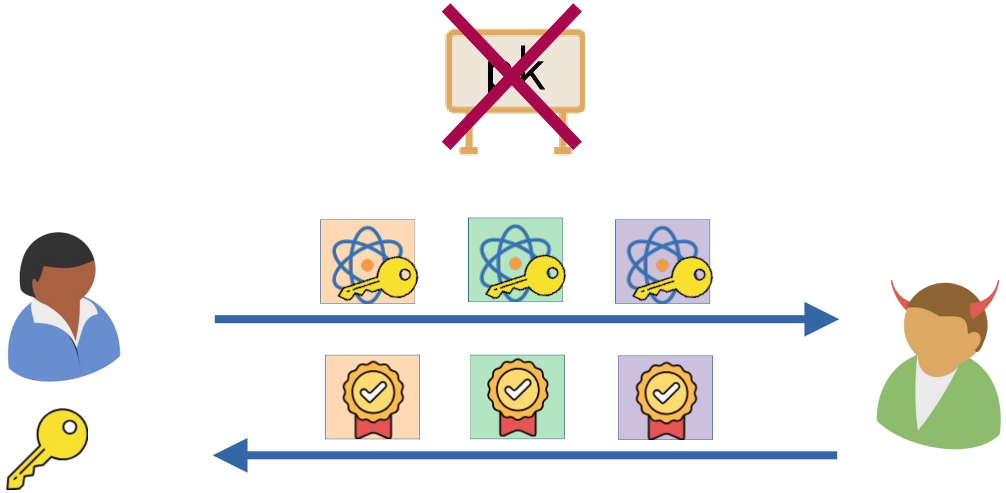
Sees no ciphertexts before returning!

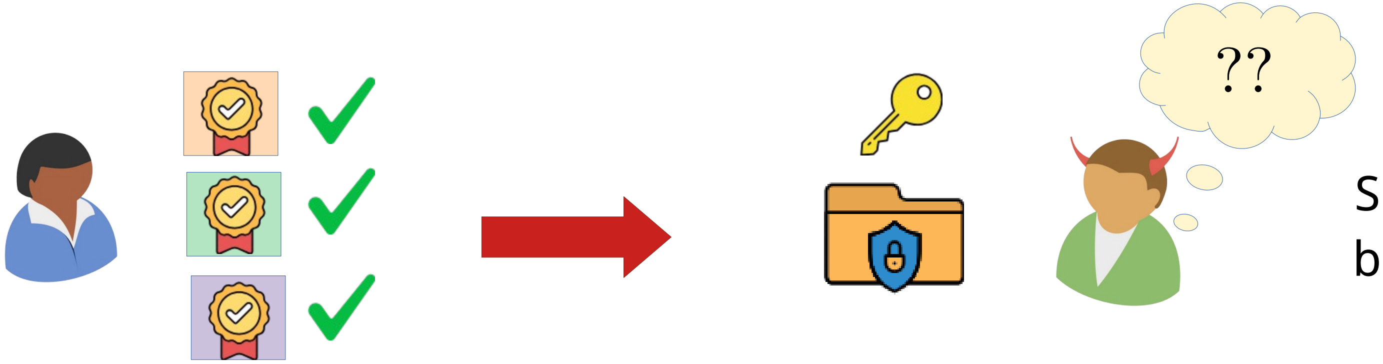
PKE-CR-SKL and SKE-CR-SKL



SKE-CR-SKL

OWF





Sees no ciphertexts before returning!

Building Block: ABE

Attribute Based Encryption

[GPS+06]

Building Block: ABE

Attribute Based Encryption

pk

[GPS+06]

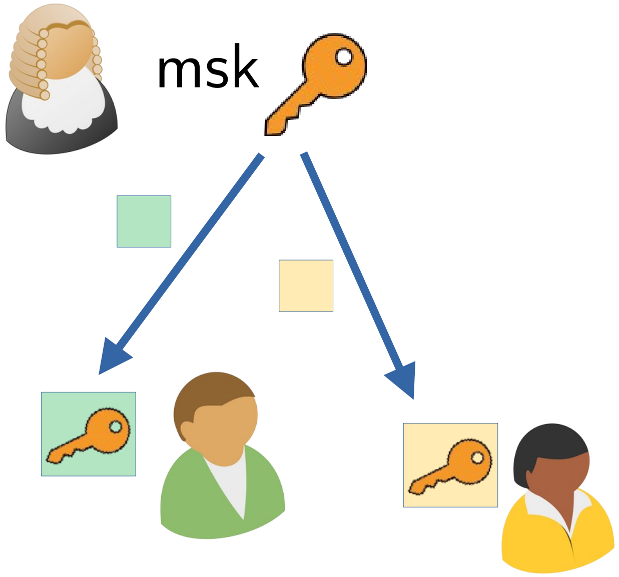
msk

Building Block: ABE

Attribute Based Encryption

pk

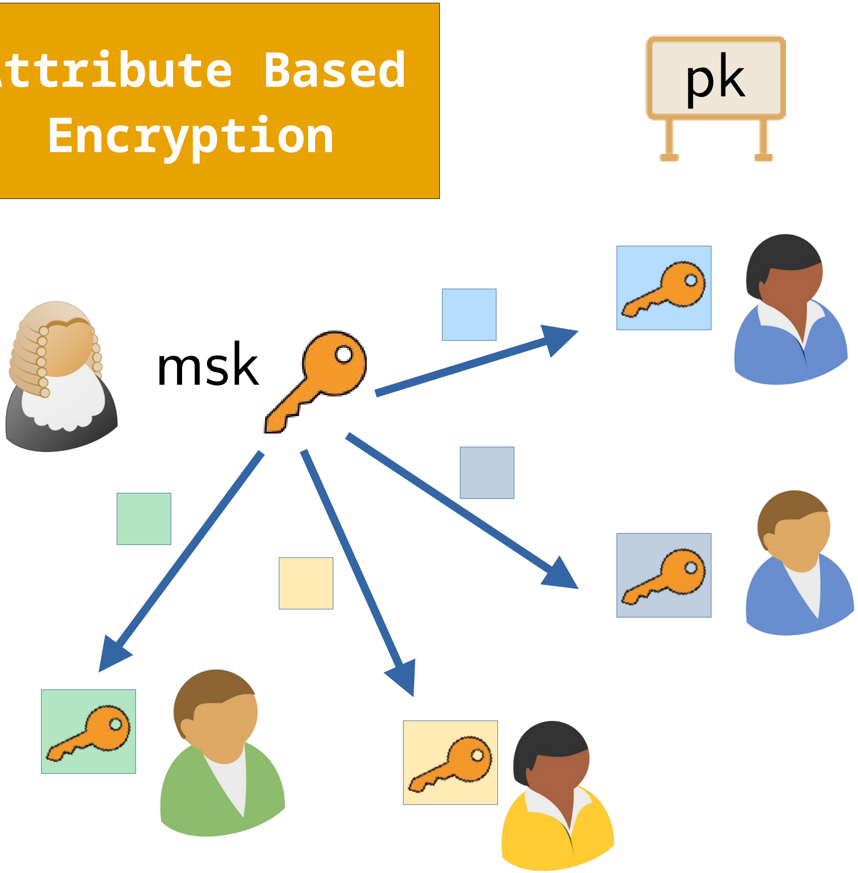
[GPS+06]



Building Block: ABE

Attribute Based Encryption

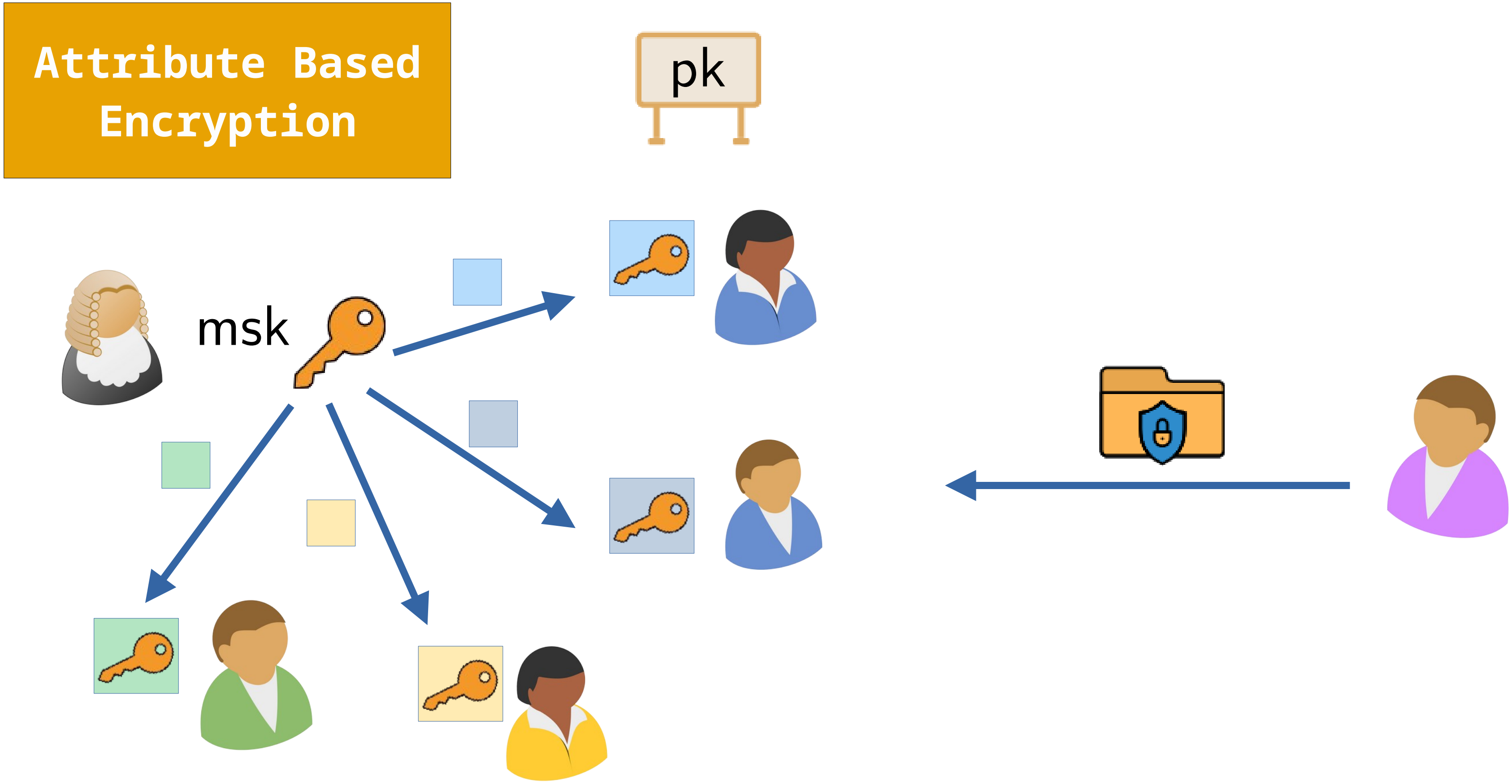
[GPS+06]



Building Block: ABE

Attribute Based Encryption

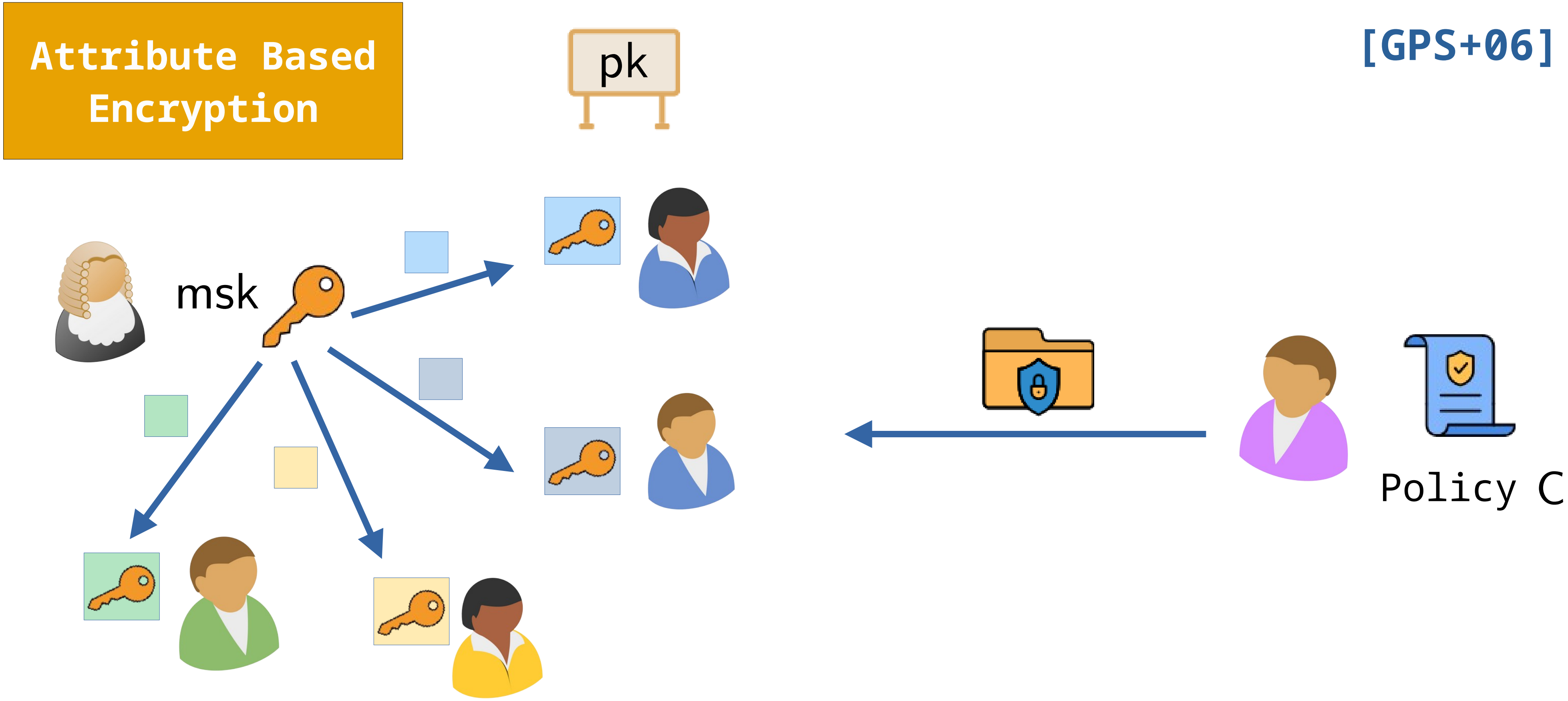
[GPS+06]



Building Block: ABE

Attribute Based Encryption

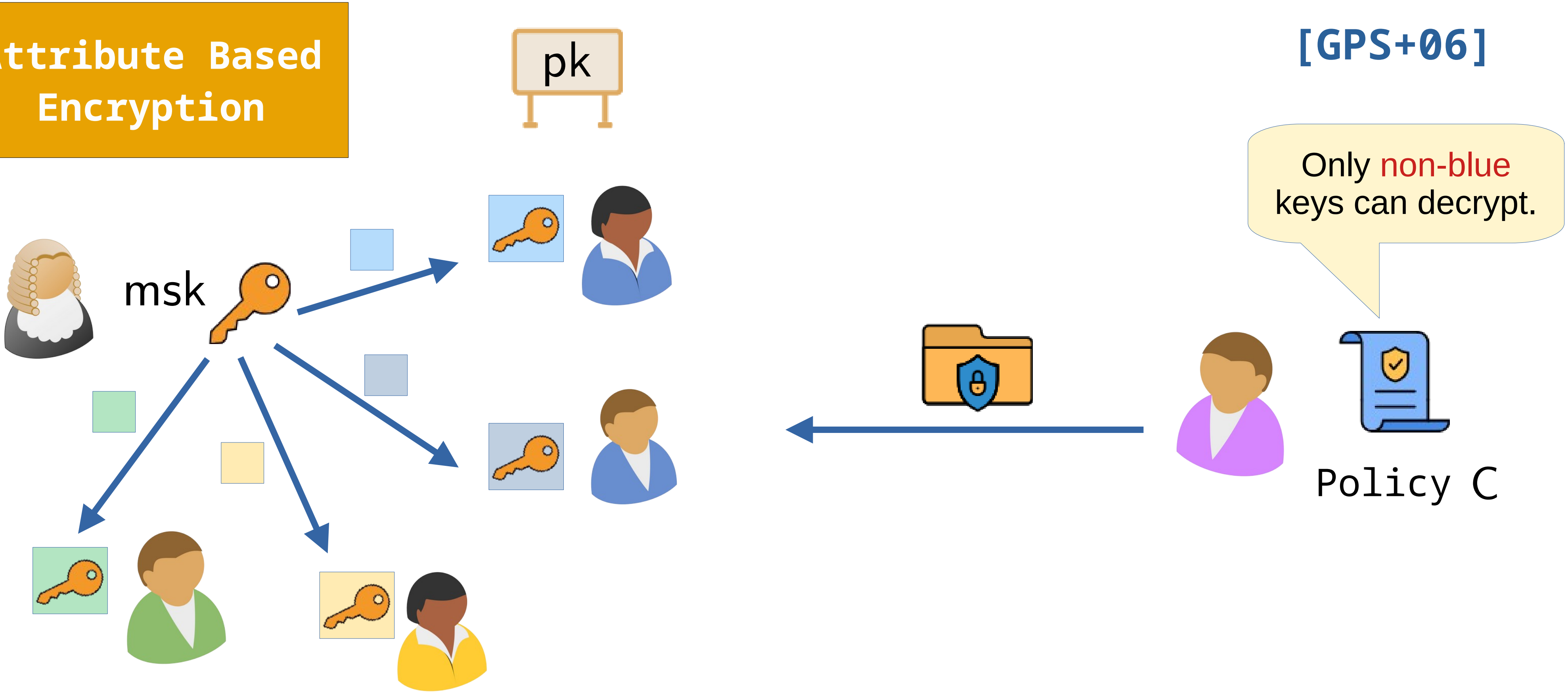
[GPS+06]



Building Block: ABE

Attribute Based Encryption

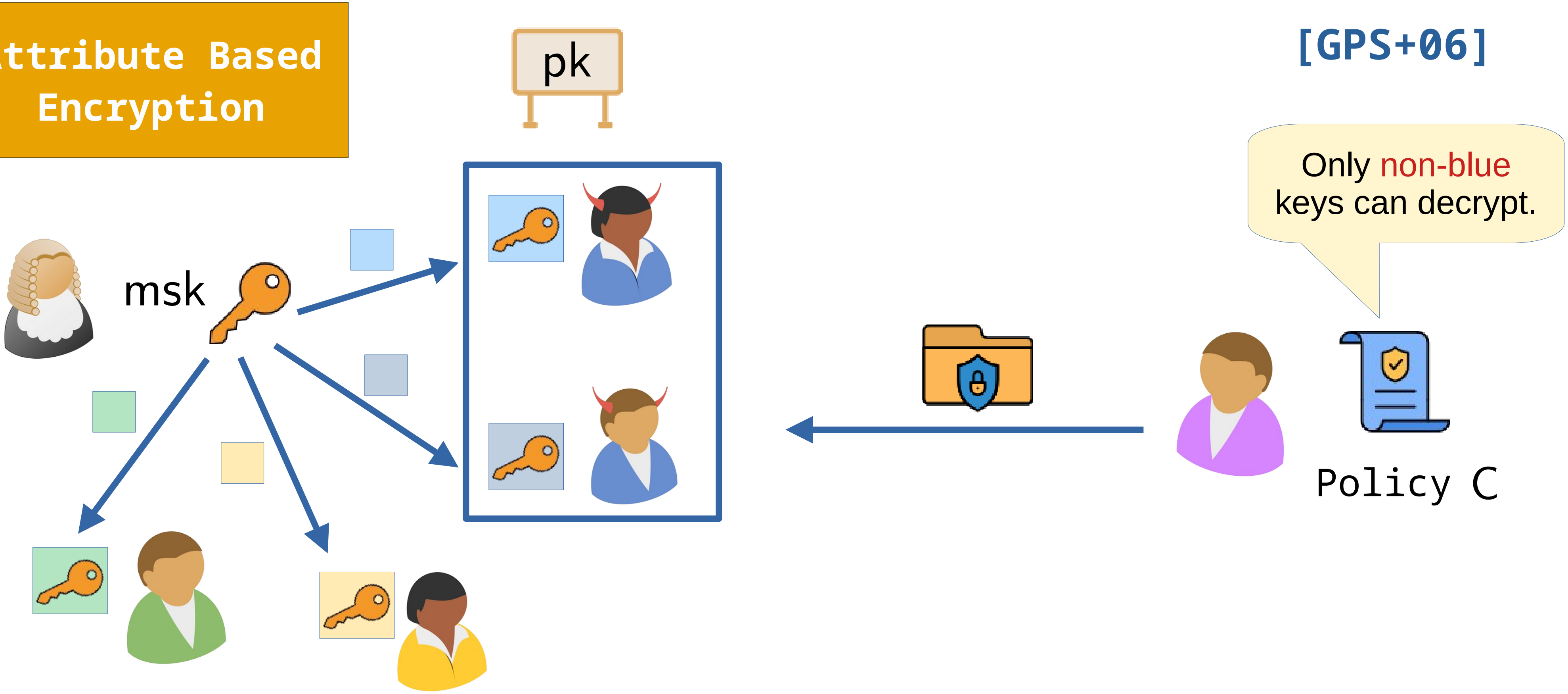
[GPS+06]



Building Block: ABE

Attribute Based Encryption

[GPS+06]

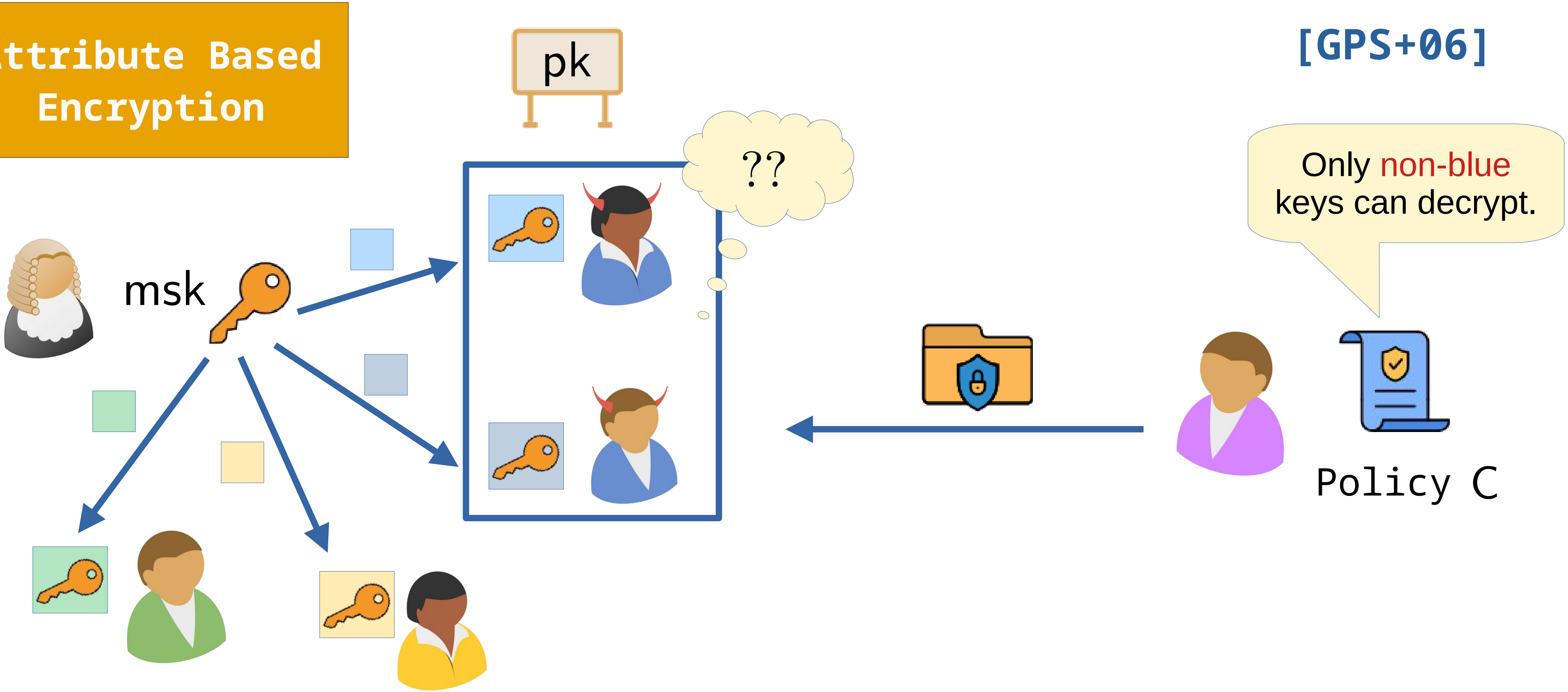


Only non-blue keys can decrypt.

Building Block: ABE

Attribute Based Encryption

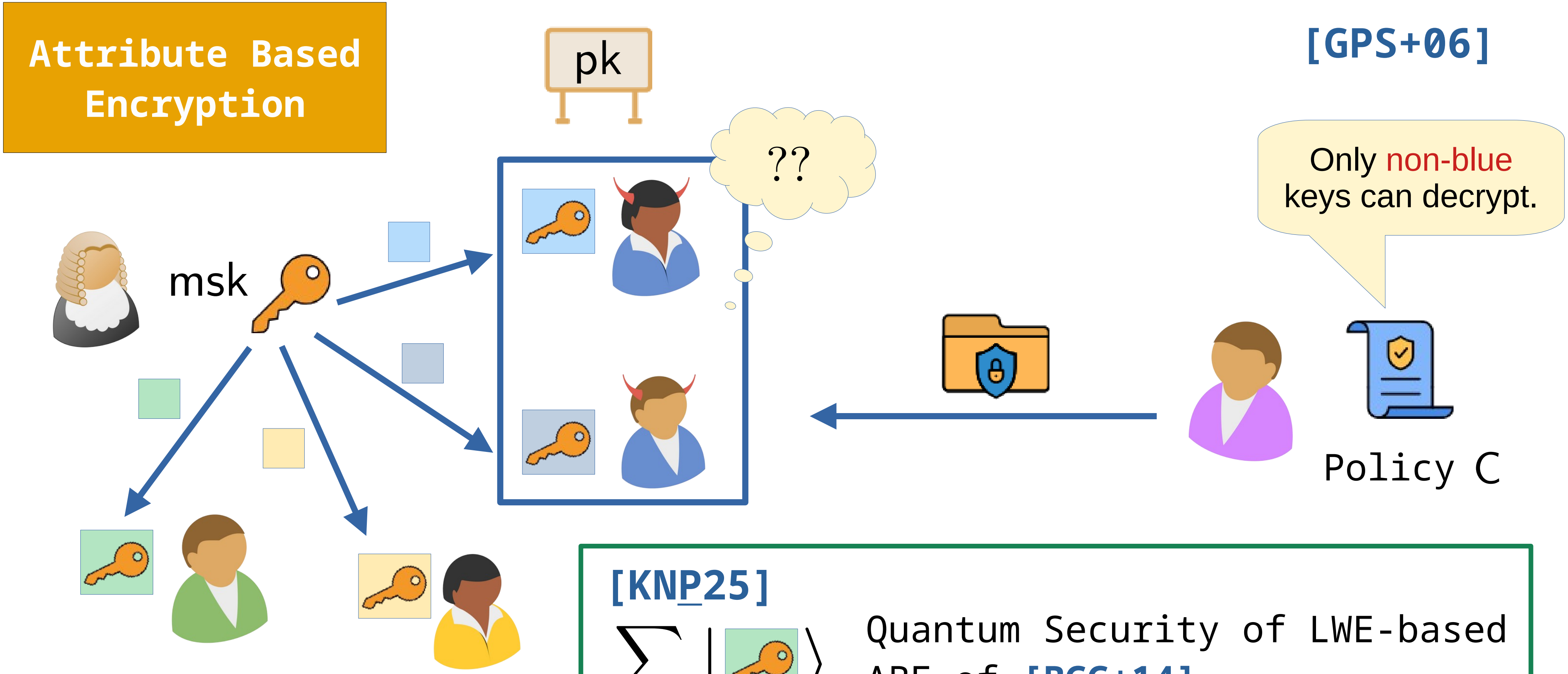
[GPS+06]



Building Block: ABE

Attribute Based Encryption

[GPS+06]



[KNP25]

$\sum |$🔑$\rangle$ Quantum Security of LWE-based ABE of [BGG+14].

Main Idea: Part I

Main Idea: Part I

$$\mathsf{ske.dk} = \alpha_1|\text{🟩}\rangle + \alpha_2|\text{🟨}\rangle + \ldots + \alpha_N|\text{🟦}\rangle$$

SKE-CR-SKL

Main Idea: Part I

$$\mathsf{ske.dk} = \alpha_1|\text{🟩}\rangle + \alpha_2|\text{🟨}\rangle + \ldots + \alpha_N|\text{🟦}\rangle$$

SKE-CR-SKL

<u>Classical Decryption Property</u>

$$\mathsf{CDec}(\mathsf{ske.ct},\text{🟩}) = \mathsf{CDec}(\mathsf{ske.ct},\text{🟨}) = \ldots = \mathsf{CDec}(\mathsf{ske.ct},\text{🟦}) = \mathsf{m}$$

Main Idea: Part I

ske.dk $= \alpha_1|$🟩$\rangle + \alpha_2|$🟨$\rangle + \ldots + \alpha_N|$🟦$\rangle$ **SKE-CR-SKL**

Classical Decryption Property

$\mathsf{CDec}(\mathsf{ske.ct},$ 🟩$) = \mathsf{CDec}(\mathsf{ske.ct},$ 🟨$) = \ldots = \mathsf{CDec}(\mathsf{ske.ct},$ 🟦$) = \mathsf{m}$

⚛🔑 $= \alpha_1|$🟩$\rangle|$🔑$\rangle + \alpha_2|$🟨$\rangle|$🔑$\rangle + \ldots + \alpha_N|$🟦$\rangle|$🔑$\rangle$ **PKE-CR-SKL**

Main Idea: Part I

$$\mathsf{ske.dk} = \alpha_1|\text{🟩}\rangle + \alpha_2|\text{🟨}\rangle + \ldots + \alpha_N|\text{🟦}\rangle$$

SKE-CR-SKL

Classical Decryption Property

$$\mathsf{CDec}(\mathsf{ske.ct}, \text{🟩}) = \mathsf{CDec}(\mathsf{ske.ct}, \text{🟨}) = \ldots = \mathsf{CDec}(\mathsf{ske.ct}, \text{🟦}) = \mathsf{m}$$

$$\text{🔑} = \alpha_1|\text{🟩}\rangle|\text{🔑}\rangle + \alpha_2|\text{🟨}\rangle|\text{🔑}\rangle + \ldots + \alpha_N|\text{🟦}\rangle\underbrace{|\text{🔑}\rangle}_{\text{ABE Secret-Key}}$$

PKE-CR-SKL

Main Idea: Part I

$$\mathsf{ske.dk} = \alpha_1|\text{🟩}\rangle + \alpha_2|\text{🟨}\rangle + \ldots + \alpha_N|\text{🟦}\rangle$$

SKE-CR-SKL

Classical Decryption Property

$$\mathsf{CDec}(\mathsf{ske.ct}, \text{🟩}) = \mathsf{CDec}(\mathsf{ske.ct}, \text{🟨}) = \ldots = \mathsf{CDec}(\mathsf{ske.ct}, \text{🟦}) = \mathsf{m}$$

$$\text{🔑} = \alpha_1|\text{🟩}\rangle|\text{🔑}\rangle + \alpha_2|\text{🟨}\rangle|\text{🔑}\rangle + \ldots + \alpha_N|\text{🟦}\rangle\underbrace{|\text{🔑}\rangle}_{\text{ABE Secret-Key}}$$

PKE-CR-SKL

Main Idea: Part I

$$\mathsf{ske.dk} = \alpha_1|🟩\rangle + \alpha_2|🟨\rangle + \ldots + \alpha_N|🟦\rangle$$

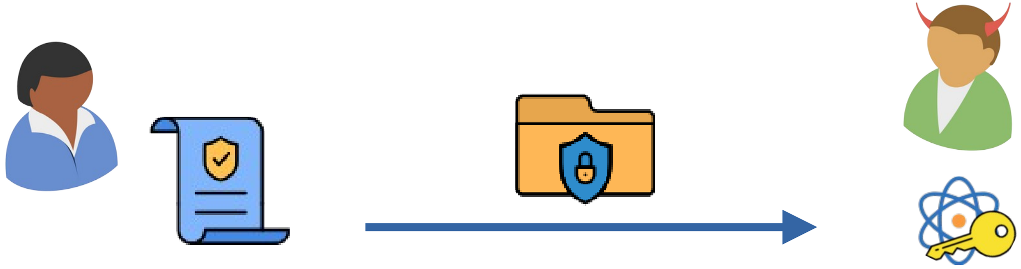
SKE-CR-SKL

Classical Decryption Property

$$\mathsf{CDec}(\mathsf{ske.ct}, 🟩) = \mathsf{CDec}(\mathsf{ske.ct}, 🟨) = \ldots = \mathsf{CDec}(\mathsf{ske.ct}, 🟦) = \mathsf{m}$$

$$⚛🔑 = \alpha_1|🟩\rangle|🔑\rangle + \alpha_2|🟨\rangle|🔑\rangle + \ldots + \alpha_N|🟦\rangle\underbrace{|🔑\rangle}_{\text{ABE Secret-Key}}$$

PKE-CR-SKL



Main Idea: Part I

$$\mathsf{ske.dk} = \alpha_1|\text{🟩}\rangle + \alpha_2|\text{🟨}\rangle + \ldots + \alpha_N|\text{🟦}\rangle$$

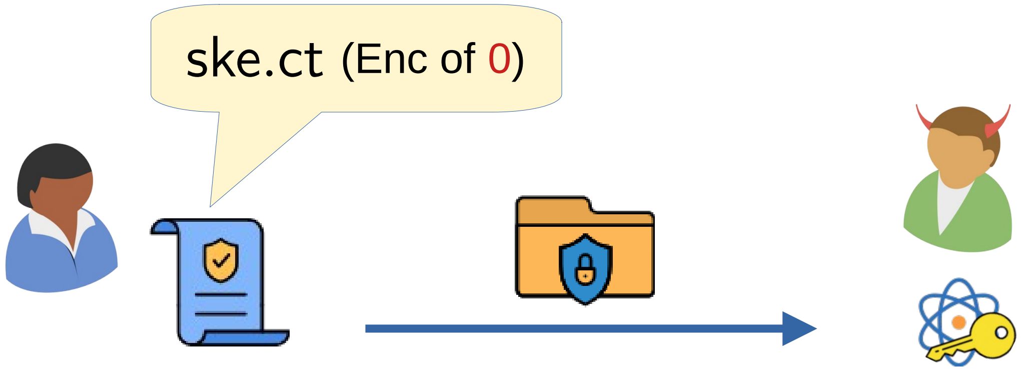
SKE-CR-SKL

Classical Decryption Property

$$\mathsf{CDec}(\mathsf{ske.ct}, \text{🟩}) = \mathsf{CDec}(\mathsf{ske.ct}, \text{🟨}) = \ldots = \mathsf{CDec}(\mathsf{ske.ct}, \text{🟦}) = \mathsf{m}$$

$$\text{🔑} = \alpha_1|\text{🟩}\rangle|\text{🔑}\rangle + \alpha_2|\text{🟨}\rangle|\text{🔑}\rangle + \ldots + \alpha_N|\text{🟦}\rangle\underbrace{|\text{🔑}\rangle}_{\texttt{ABE Secret-Key}}$$

PKE-CR-SKL



ske.ct (Enc of 0)

Main Idea: Part I

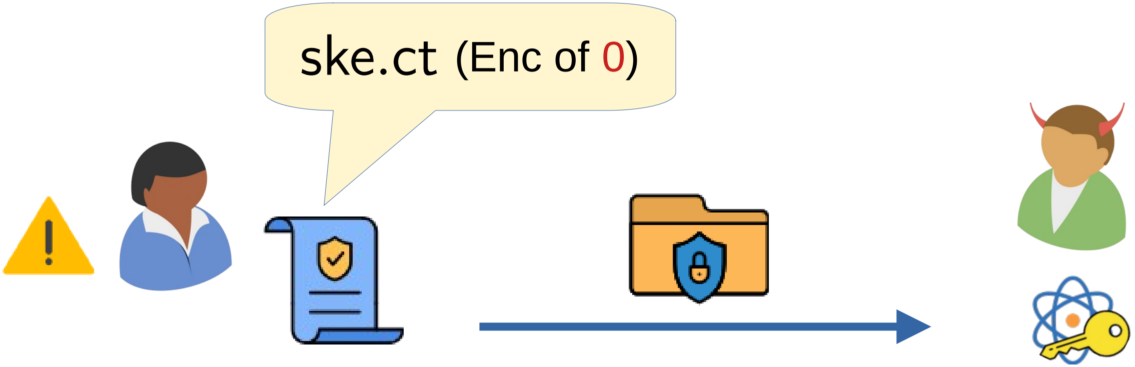
ske.dk $= \alpha_1|$🟩$\rangle + \alpha_2|$🟨$\rangle + \ldots + \alpha_N|$🟦$\rangle$ **SKE-CR-SKL**

Classical Decryption Property

CDec(ske.ct, 🟩) $=$ CDec(ske.ct, 🟨) $= \ldots =$ CDec(ske.ct, 🟦) $=$ m

🔑 $= \alpha_1|$🟩$\rangle|$🔑$\rangle + \alpha_2|$🟨$\rangle|$🔑$\rangle + \ldots + \alpha_N|$🟦$\rangle|$🔑$\rangle$ **PKE-CR-SKL**

ABE Secret-Key



Main Idea: Part I

$$\text{ske.dk} = \alpha_1|\text{🟩}\rangle + \alpha_2|\text{🟨}\rangle + \ldots + \alpha_N|\text{🟦}\rangle$$

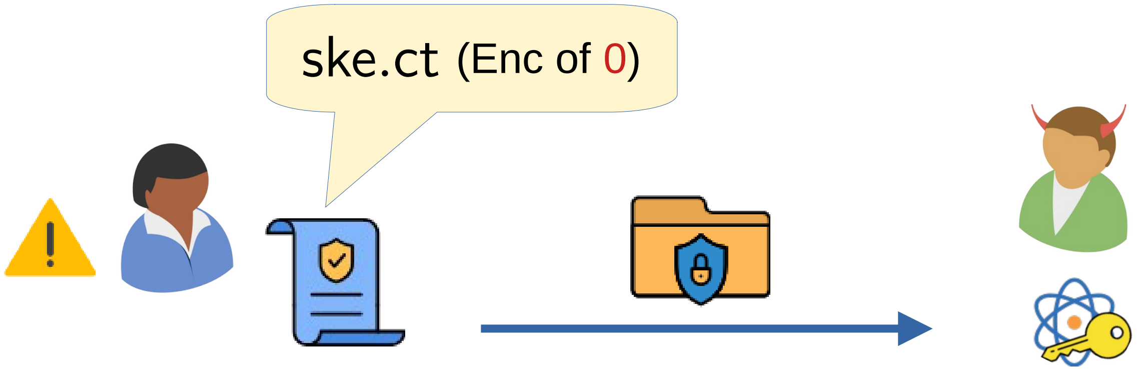
SKE-CR-SKL

<u>Classical Decryption Property</u>

$$\text{CDec}(\text{ske.ct}, \text{🟩}) = \text{CDec}(\text{ske.ct}, \text{🟨}) = \ldots = \text{CDec}(\text{ske.ct}, \text{🟦}) = \text{m}$$

$$\text{⚛🔑} = \alpha_1|\text{🟩}\rangle|\text{🔑}\rangle + \alpha_2|\text{🟨}\rangle|\text{🔑}\rangle + \ldots + \alpha_N|\text{🟦}\rangle\underbrace{|\text{🔑}\rangle}_{\text{ABE Secret-Key}}$$

PKE-CR-SKL



🔑 satisfies policy if:

$$\text{CDec}(\text{ske.ct}, \text{🟩}) = 0$$

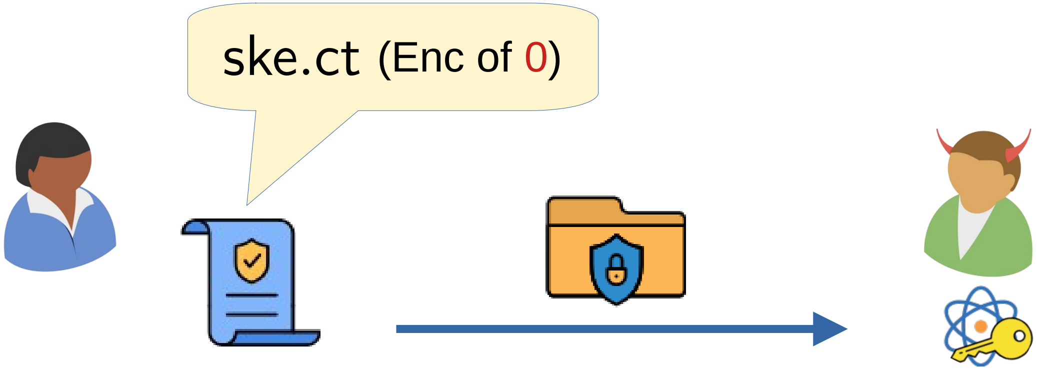
Main Idea: Part II

Main Idea: Part II

⚛🔑 $= \alpha_1|$🟩$\rangle|$🔑$\rangle + \alpha_2|$🟨$\rangle|$🔑$\rangle + \ldots + \alpha_N|$🟦$\rangle|$🔑$\rangle$

Main Idea: Part II

⚛🔑 $= \alpha_1|$🟩$\rangle|$🔑$\rangle + \alpha_2|$🟨$\rangle|$🔑$\rangle + \ldots + \alpha_N|$🟦$\rangle|$🔑$\rangle$

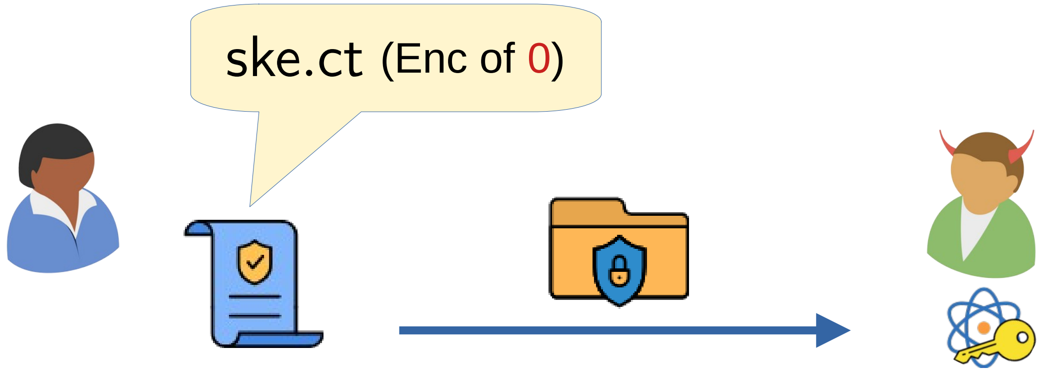


🔑 satisfies policy if:

CDec(ske.ct, 🟩) $= 0$

Main Idea: **Part II**

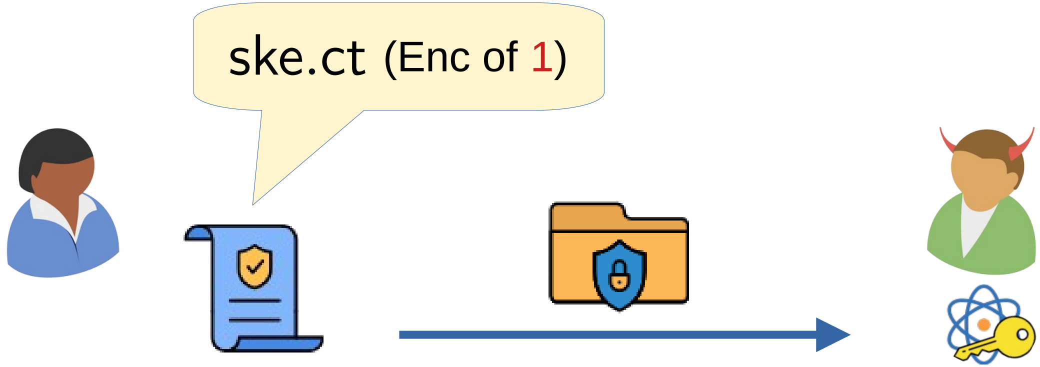
$$\text{🔑} = \alpha_1|\text{🟩}\rangle|\text{🔑}\rangle + \alpha_2|\text{🟨}\rangle|\text{🔑}\rangle + \ldots + \alpha_N|\text{🟦}\rangle|\text{🔑}\rangle$$



ske.ct (Enc of 0)

🔑 satisfies policy if:

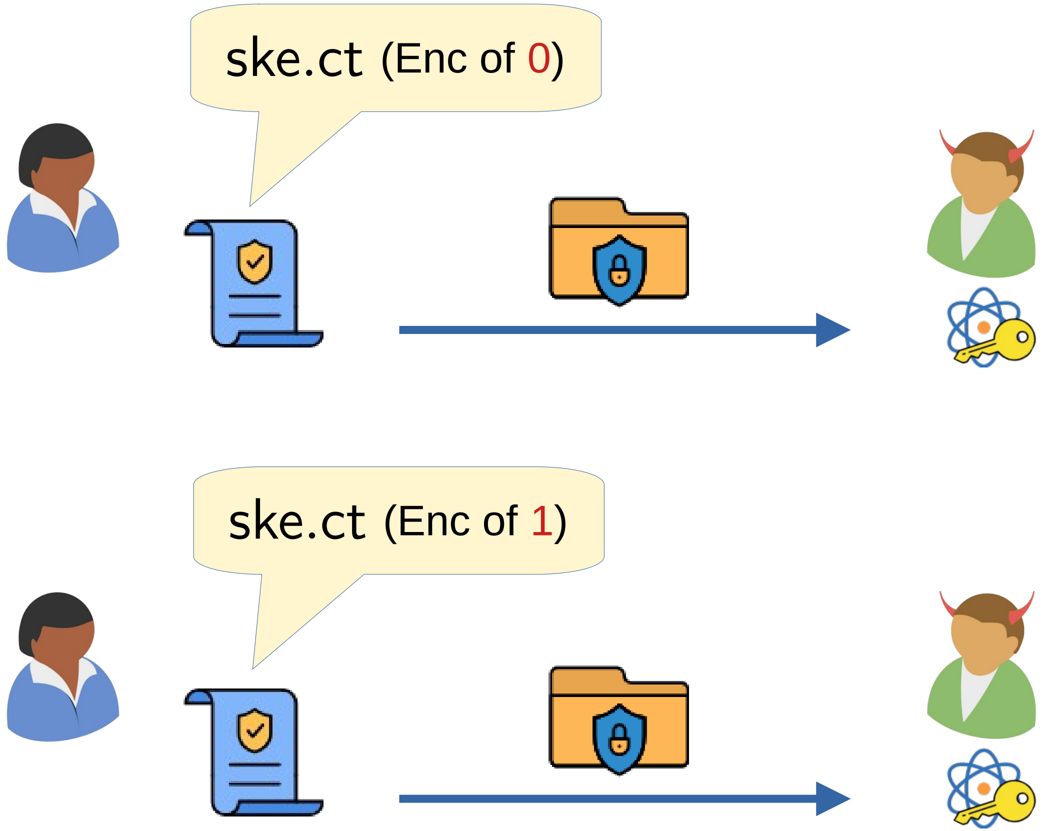
$\text{CDec}(\text{ske.ct}, \text{🟩}) = 0$



ske.ct (Enc of 1)

Main Idea: Part II

⚛🔑 $=\ \alpha_1|$🟩$\rangle|$🟩🔑$\rangle + \alpha_2|$🟨$\rangle|$🟨🔑$\rangle + \ldots + \alpha_N|$🟦$\rangle|$🟦🔑$\rangle$



ske.ct (Enc of 0)

ske.ct (Enc of 1)

🟩🔑 satisfies policy if:

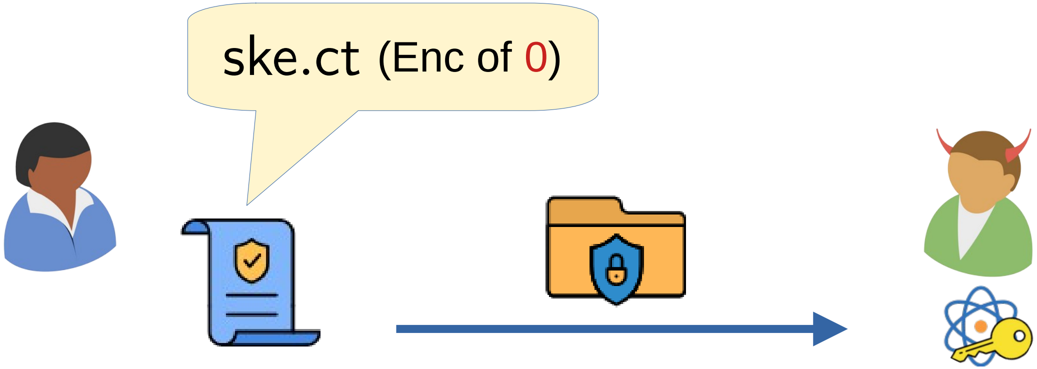
CDec(ske.ct, 🟩) $= 0$

All keys are unsatisfying:

🟩🔑 🟨🔑 … 🟦🔑

Main Idea: Part II

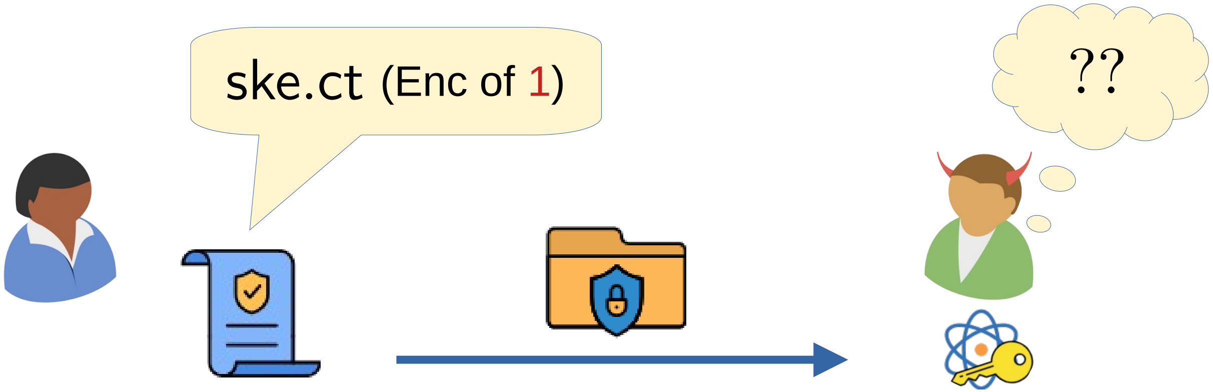
⚛🔑 $= \alpha_1|$🟩$\rangle|$🟩🔑$\rangle + \alpha_2|$🟨$\rangle|$🟨🔑$\rangle + \ldots + \alpha_N|$🟦$\rangle|$🟦🔑$\rangle$



ske.ct (Enc of 0)

🟩🔑 satisfies policy if:

CDec(ske.ct, 🟩) $= 0$



ske.ct (Enc of 1)

All keys are unsatisfying:

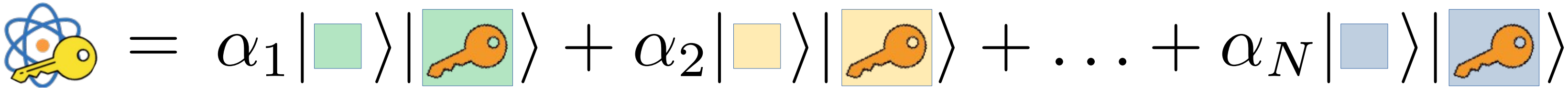
🟩🔑 🟨🔑 … 🟦🔑

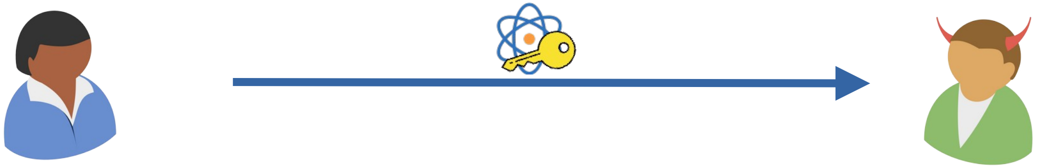
Main Idea: Part III

Main Idea: Part III

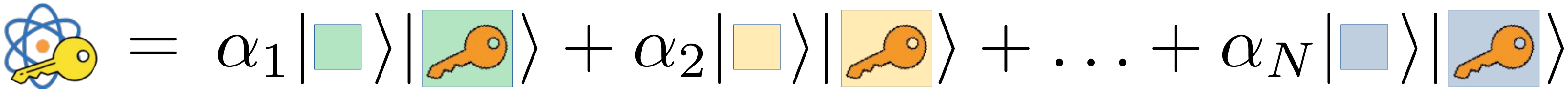
$$\text{⚛🔑} = \alpha_1|\text{🟩}\rangle|\text{🔑}\rangle + \alpha_2|\text{🟨}\rangle|\text{🔑}\rangle + \ldots + \alpha_N|\text{🟦}\rangle|\text{🔑}\rangle$$

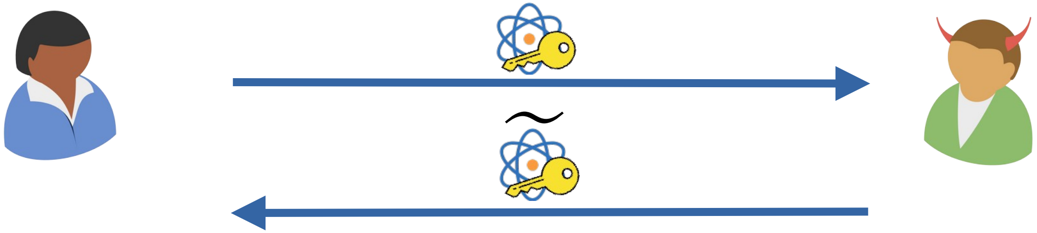
Main Idea: Part III


$= \alpha_1 | \quad \rangle | \quad \rangle + \alpha_2 | \quad \rangle | \quad \rangle + \ldots + \alpha_N | \quad \rangle | \quad \rangle$



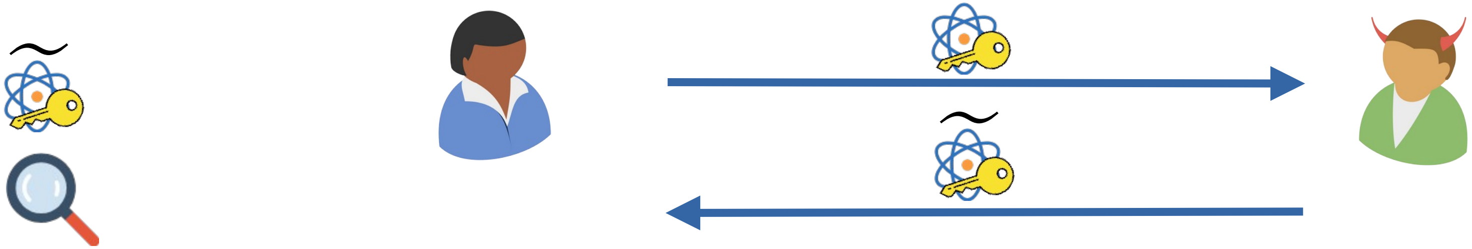
Main Idea: Part III


$= \alpha_1 |\ \rangle|\ \rangle + \alpha_2 |\ \rangle|\ \rangle + \ldots + \alpha_N |\ \rangle|\ \rangle$

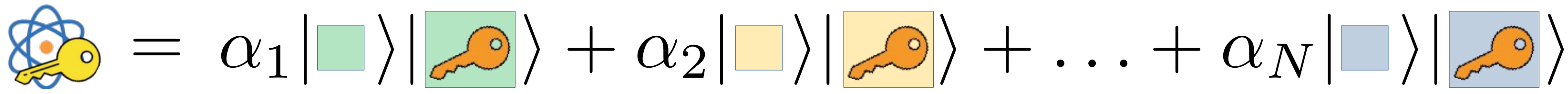


Main Idea: Part III

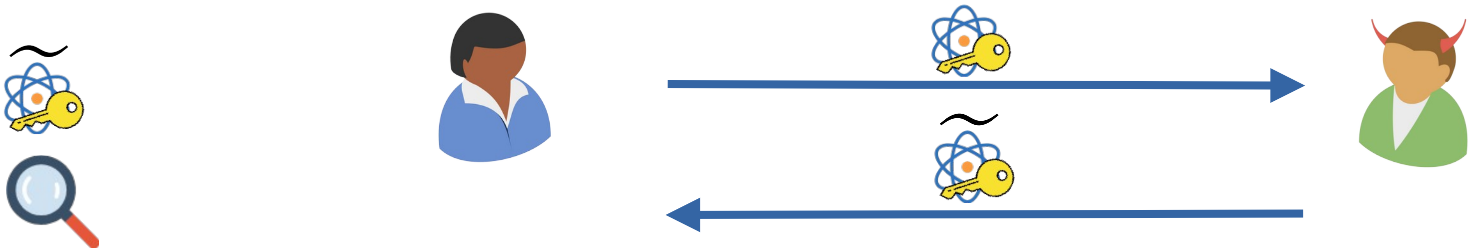
⚛🔑 = α_1|🟩⟩|🔑⟩ + α_2|🟨⟩|🔑⟩ + . . . + α_N|🟦⟩|🔑⟩



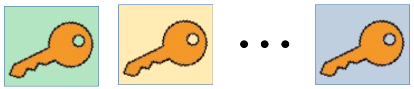
Main Idea: Part III



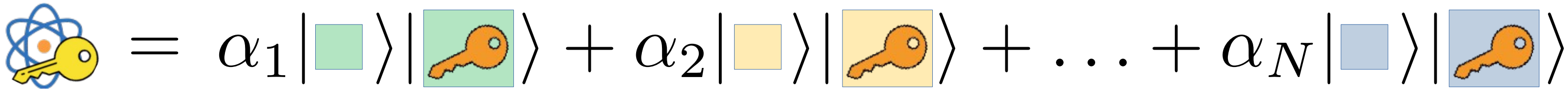
$= \alpha_1 | \; \rangle | \; \rangle + \alpha_2 | \; \rangle | \; \rangle + \ldots + \alpha_N | \; \rangle | \; \rangle$

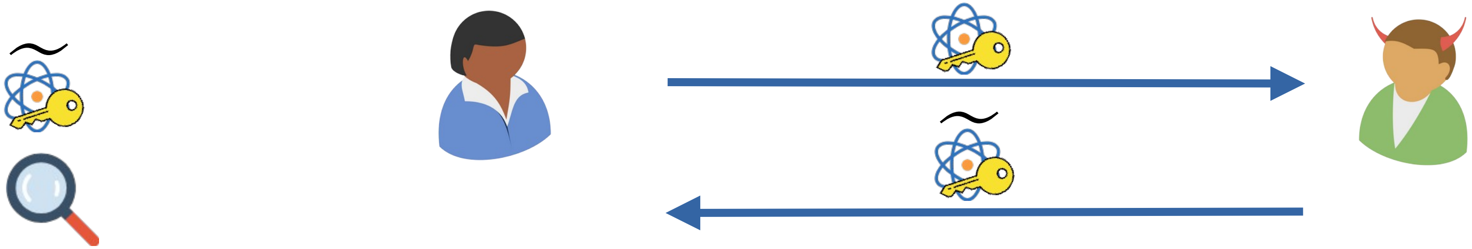


1. Uncompute ABE keys

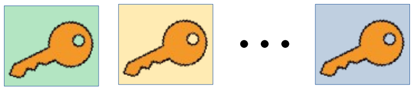


Main Idea: Part III



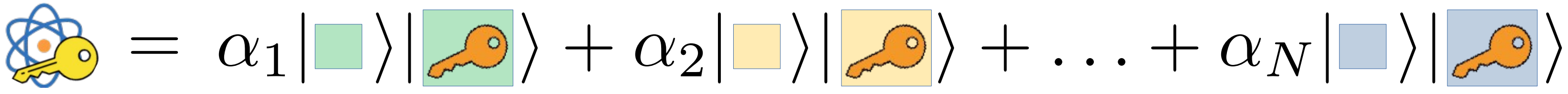


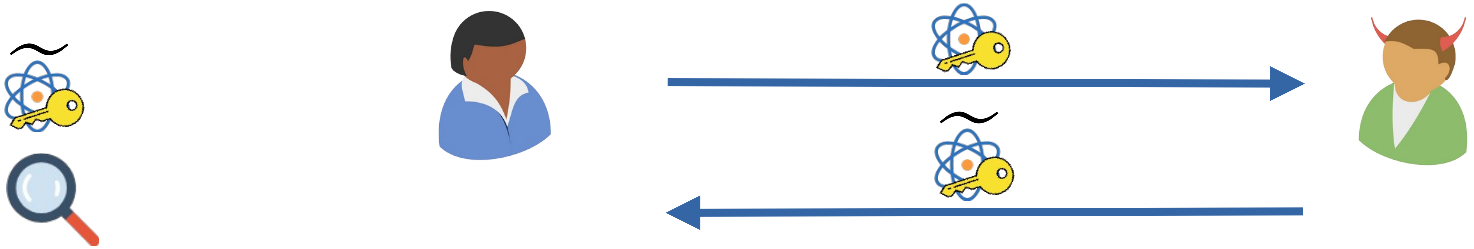
1. Uncompute ABE keys



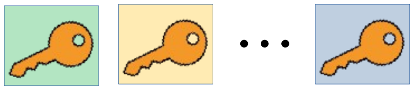
2. Verify $\widetilde{\text{ske.dk}}$.

Main Idea: Part III

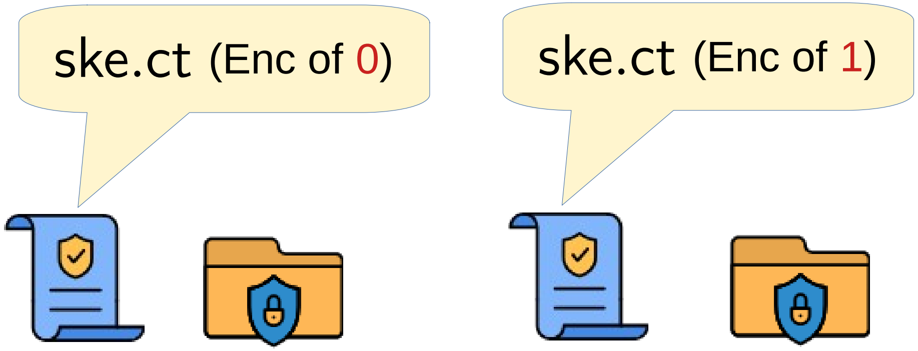

$= \alpha_1 |\ \rangle |\ \rangle + \alpha_2 |\ \rangle |\ \rangle + \ldots + \alpha_N |\ \rangle |\ \rangle$



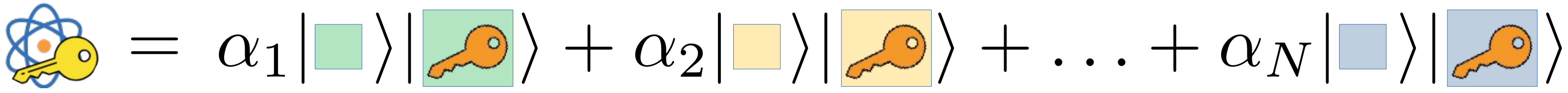
1. Uncompute ABE keys



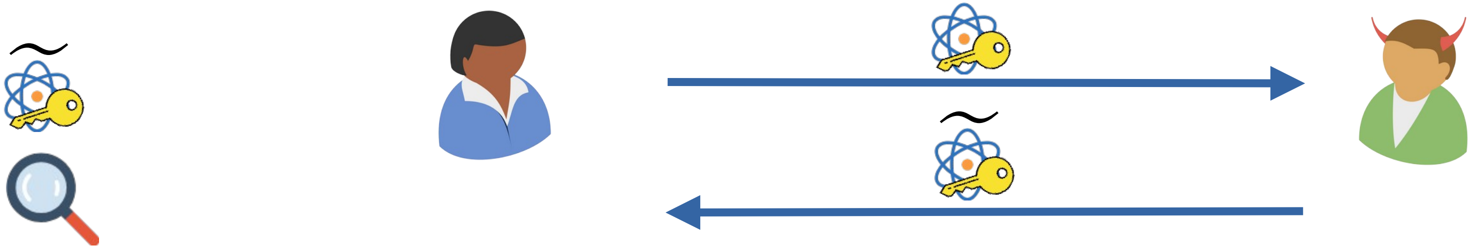
2. Verify ske.$\widetilde{\text{dk}}$.



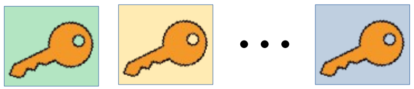
Main Idea: Part III



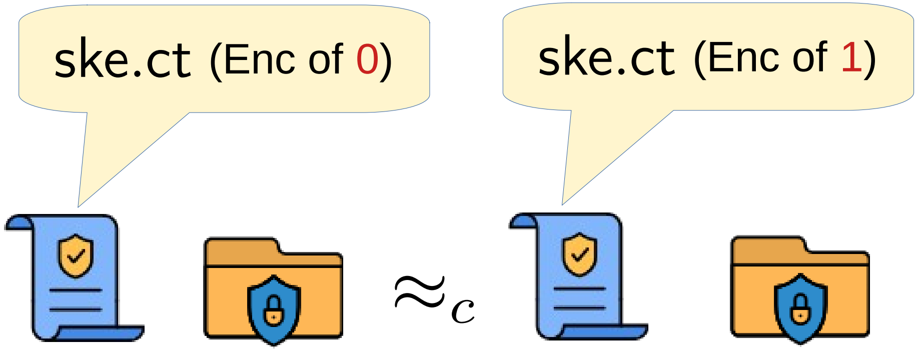
$= \alpha_1 | \rangle | \rangle + \alpha_2 | \rangle | \rangle + \ldots + \alpha_N | \rangle | \rangle$



1. Uncompute ABE keys

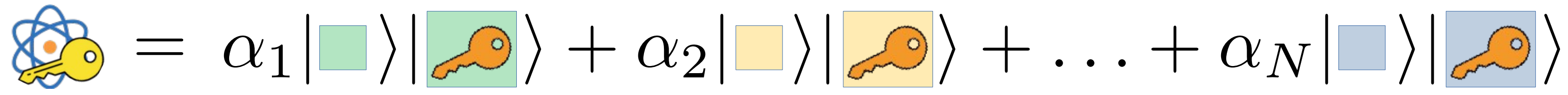


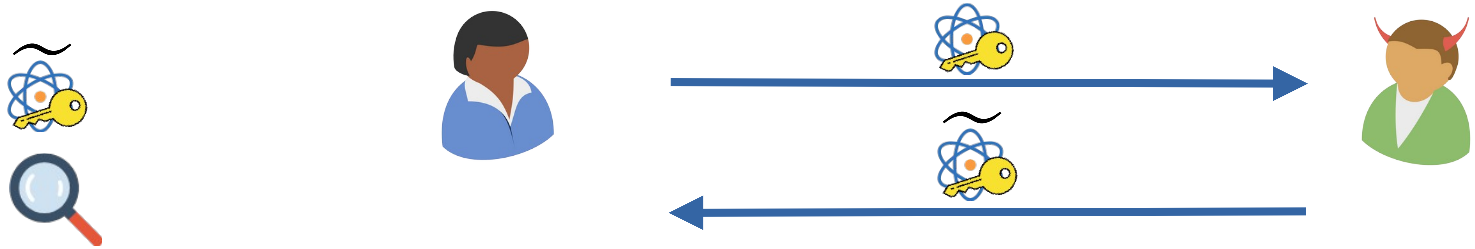
2. Verify $\widetilde{\text{ske.dk}}$.



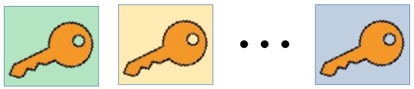
SKE-CR-SKL

Main Idea: Part III

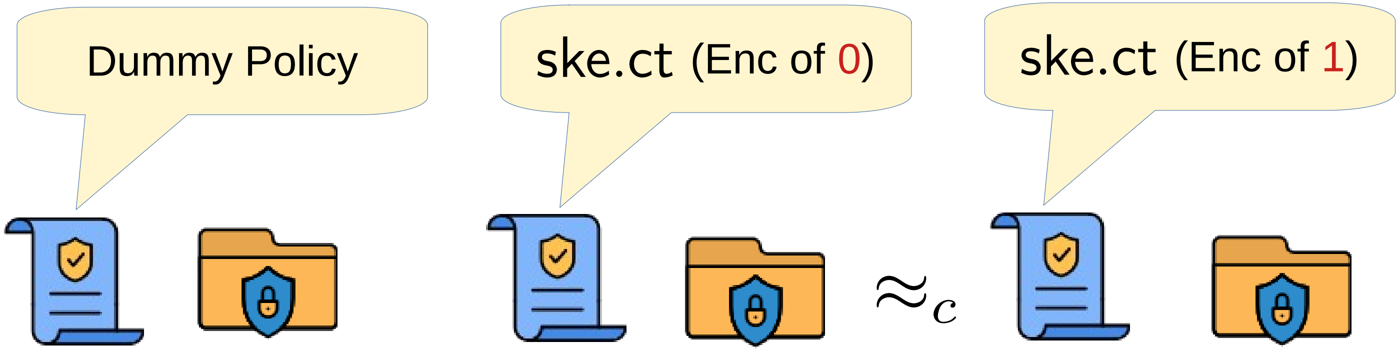

$= \alpha_1 | \; \rangle | \; \rangle + \alpha_2 | \; \rangle | \; \rangle + \ldots + \alpha_N | \; \rangle | \; \rangle$



1. Uncompute ABE keys

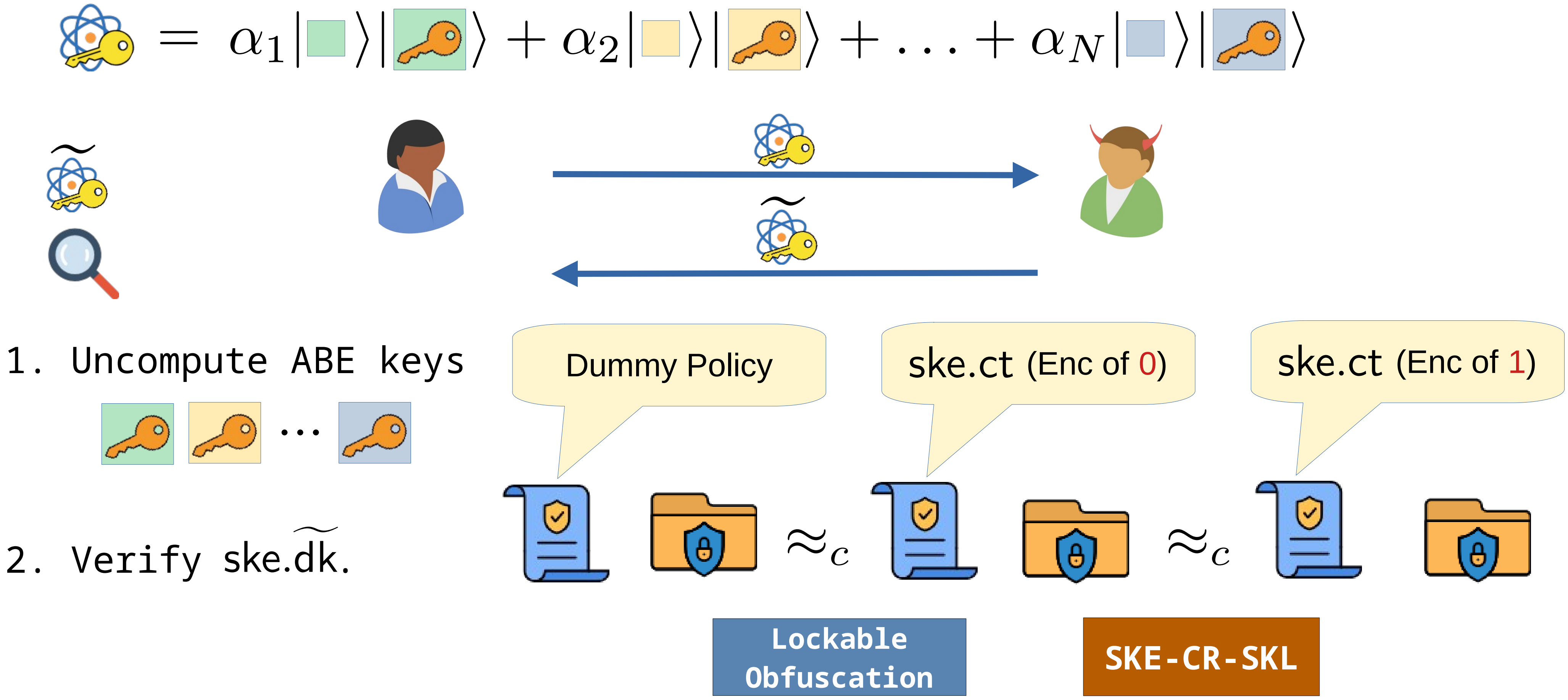


2. Verify $\widetilde{\text{ske.dk}}$.



SKE-CR-SKL

Main Idea: Part III


$= \alpha_1 | \; \rangle | \; \rangle + \alpha_2 | \; \rangle | \; \rangle + \ldots + \alpha_N | \; \rangle | \; \rangle$
$\sim$
$\sim$
…
$\approx_c$
$\approx_c$

1. Uncompute ABE keys

2. Verify $\widetilde{\text{ske.dk}}$.

Dummy Policy

ske.ct (Enc of 0)

ske.ct (Enc of 1)

Lockable Obfuscation

SKE-CR-SKL

References

- **[AKN+23]:** Agrawal, Shweta, et al. "Public key encryption with secure key leasing." Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer Nature Switzerland, 2023.
- **[APV23]:** Ananth, Prabhanjan, Alexander Poremba, and Vinod Vaikuntanathan. "Revocable cryptography from learning with errors." Theory of Cryptography Conference. Cham: Springer Nature Switzerland, 2023.
- **[CGJL25]:** Chardouvelis, Orestis, et al. "Quantum key leasing for PKE and FHE with a classical lessor." Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer Nature Switzerland, 2025.
- **[AHH24]:** Ananth, Prabhanjan, Zihan Hu, and Zikuan Huang. "Quantum Key-Revocable Dual-Regev Encryption, Revisited." Theory of Cryptography Conference. Cham: Springer Nature Switzerland, 2024.
- **[KNP25]:** Kitagawa, Fuyuki, Ryo Nishimaki, and Nikhil Pappu. "PKE and ABE with Collusion-Resistant Secure Key Leasing." arXiv preprint arXiv:2502.12491 (2025).

References

- **[KMY25]:** Kitagawa, Fuyuki, Tomoyuki Morimae, and Takashi Yamakawa. "A Simple Framework for Secure Key Leasing." Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer Nature Switzerland, 2025.

- **[BGK+24]:** Bartusek, James, et al. "Software with certified deletion." Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer Nature Switzerland, 2024.

- **[GPS+06]:** Goyal, Vipul, et al. "Attribute-based encryption for fine-grained access control of encrypted data." Proceedings of the 13th ACM conference on Computer and communications security. 2006.

- **[BGG+14]:** Boneh, Dan, et al. "Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits." Advances in Cryptology–EUROCRYPT 2014: 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings 33. Springer Berlin Heidelberg, 2014.

Thank You!