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

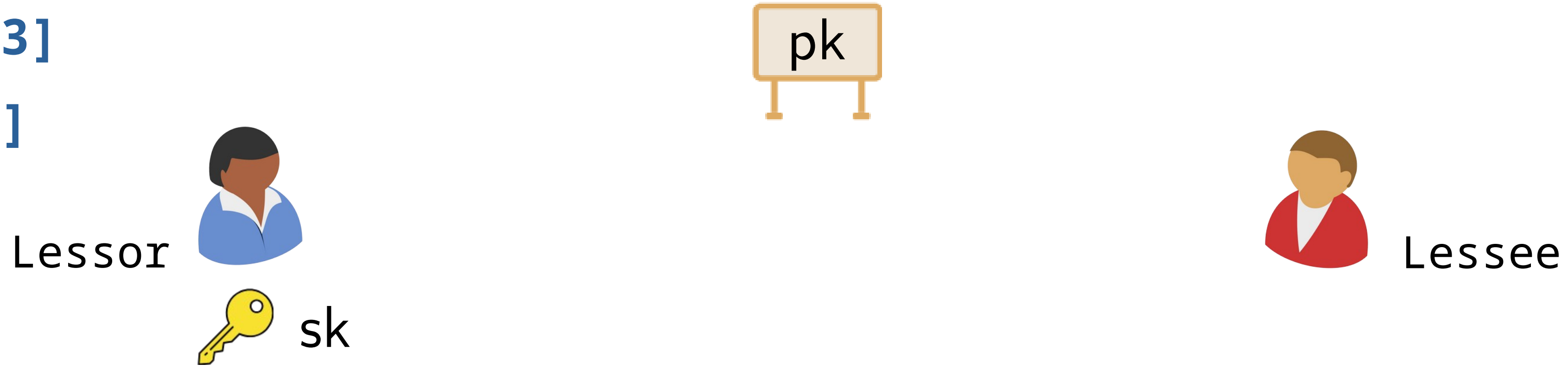
[AKN+23]

[APV23]

PKE with Secure Key Leasing

[AKN+23]

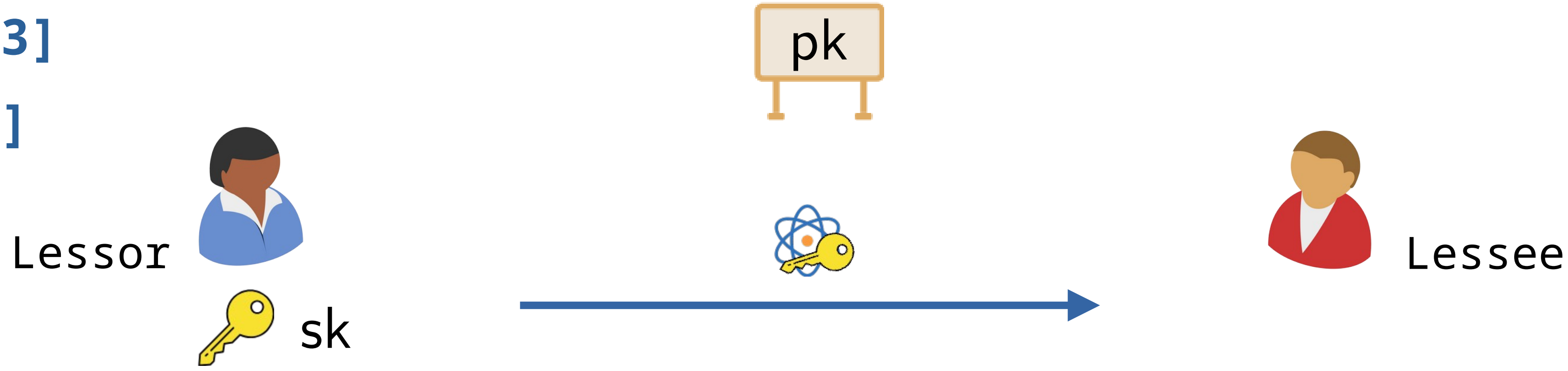
[APV23]



PKE with Secure Key Leasing

[AKN+23]

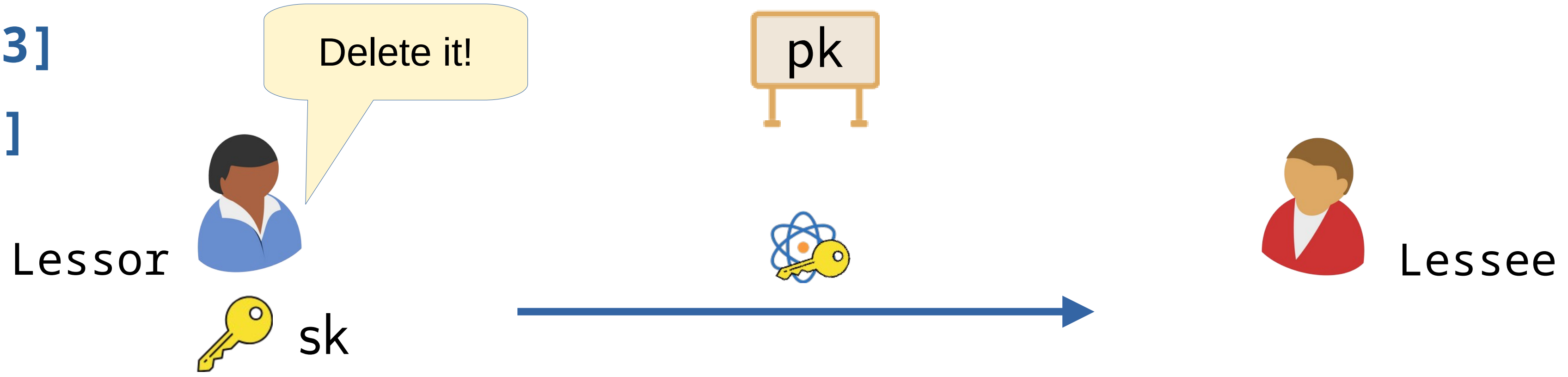
[APV23]



PKE with Secure Key Leasing

[AKN+23]

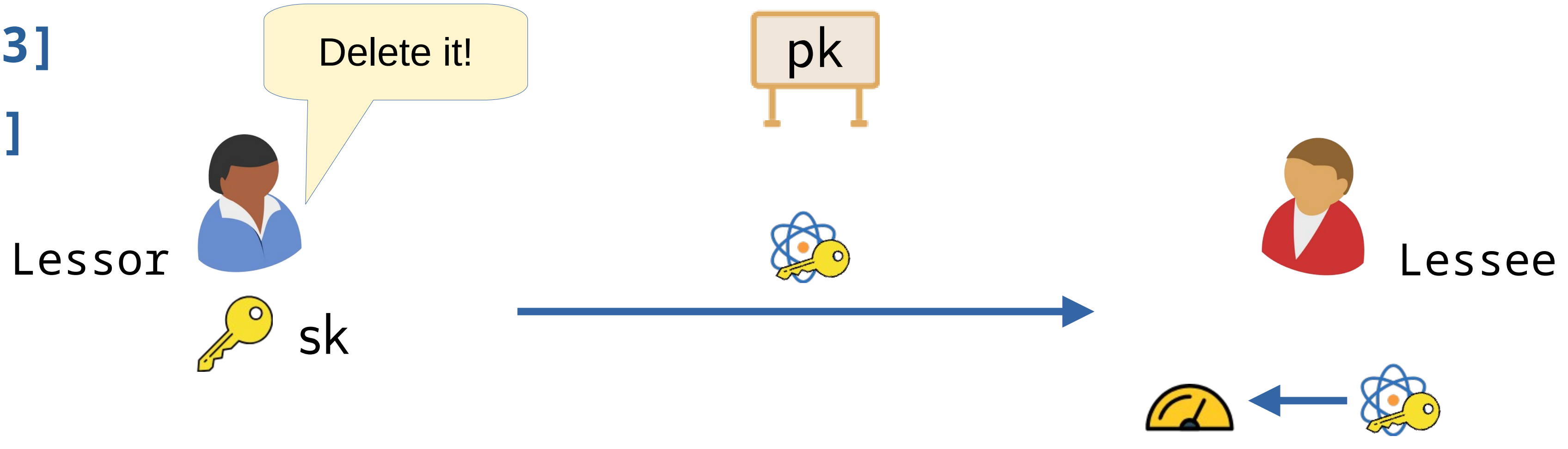
[APV23]



PKE with Secure Key Leasing

[AKN+23]

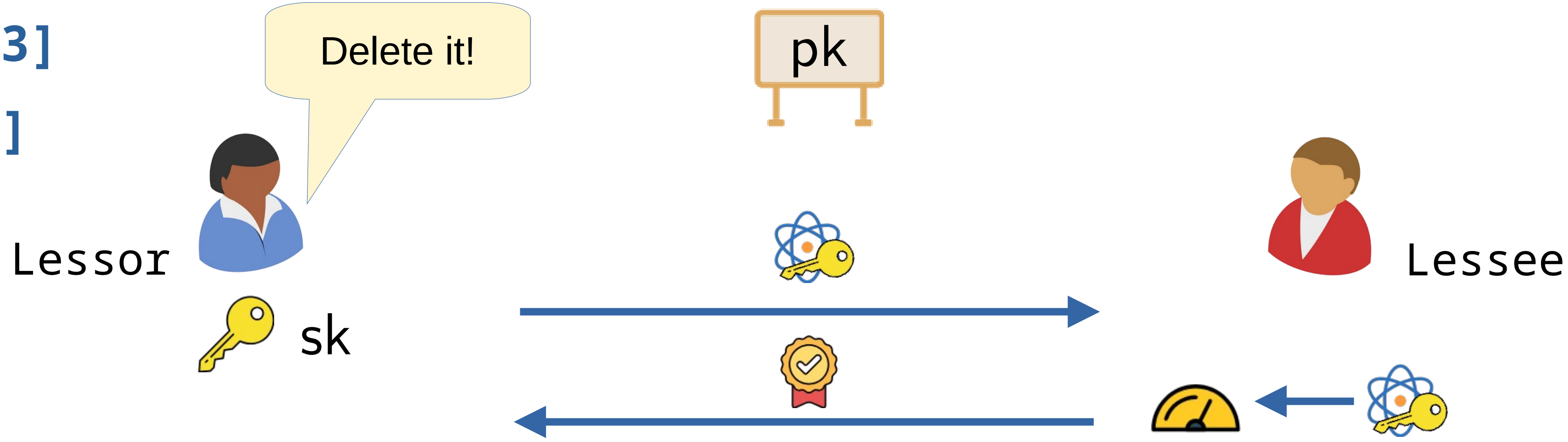
[APV23]



PKE with Secure Key Leasing

[AKN+23]

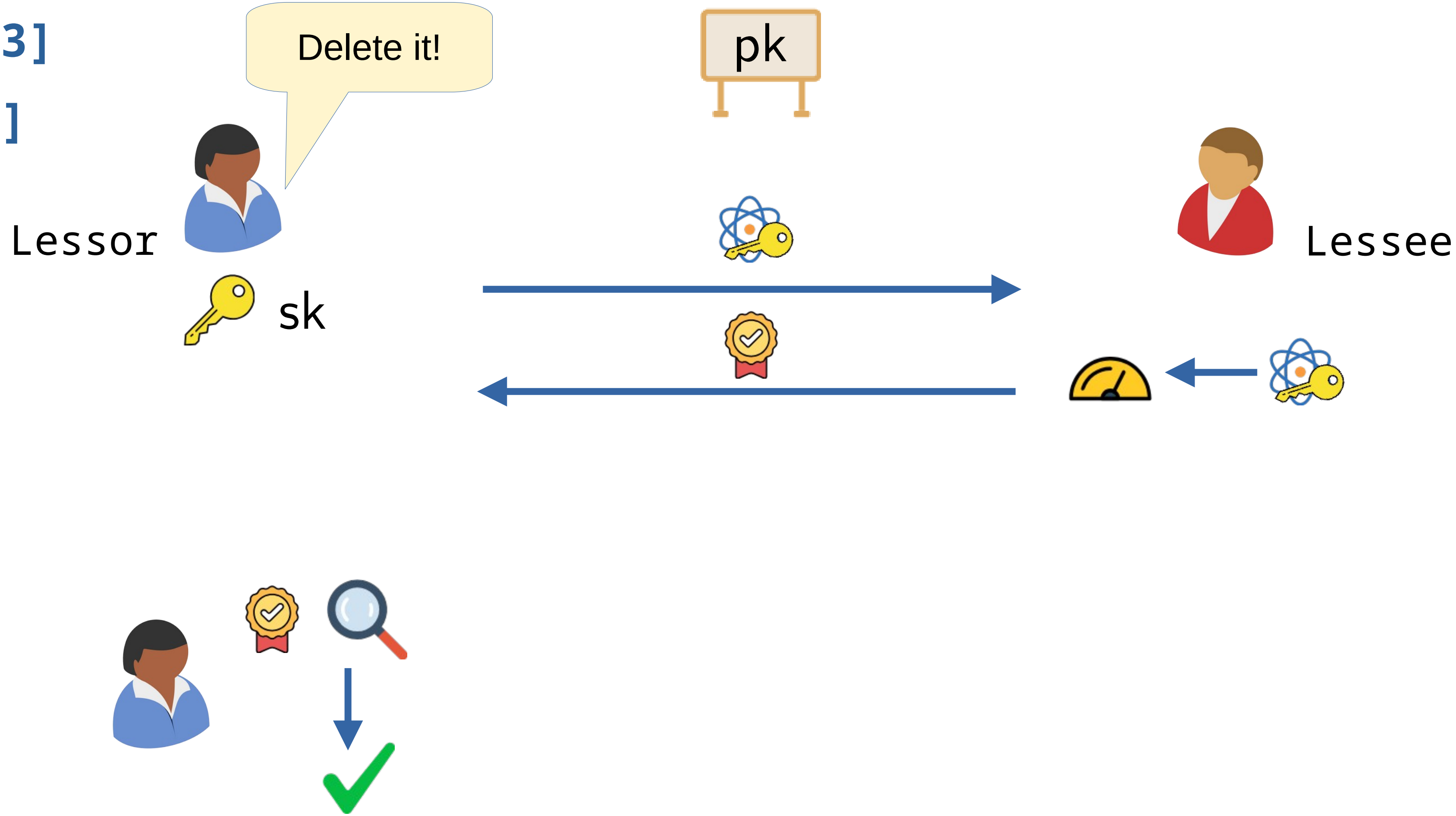
[APV23]



PKE with Secure Key Leasing

[AKN+23]

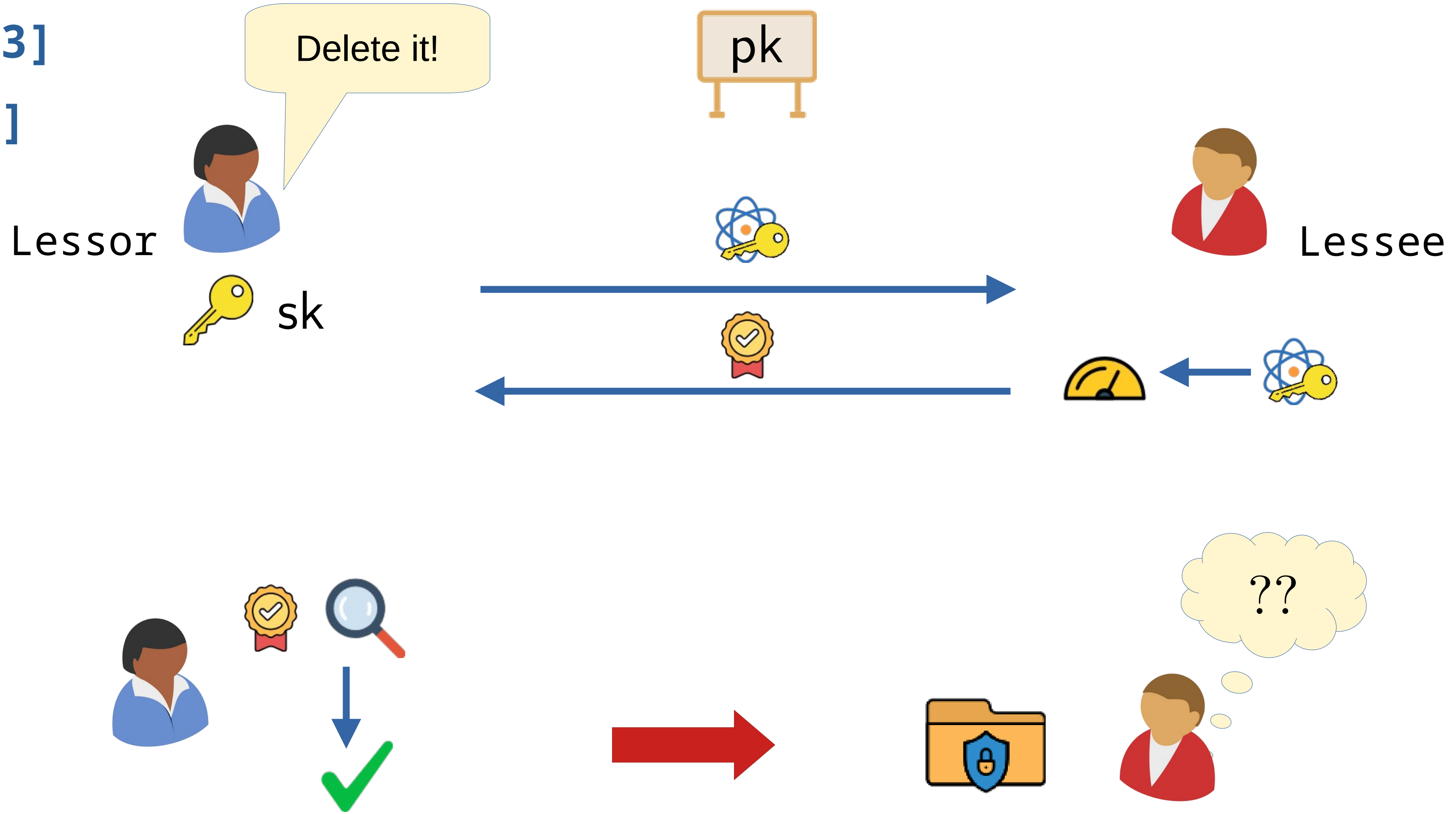
[APV23]



PKE with Secure Key Leasing

[AKN+23]

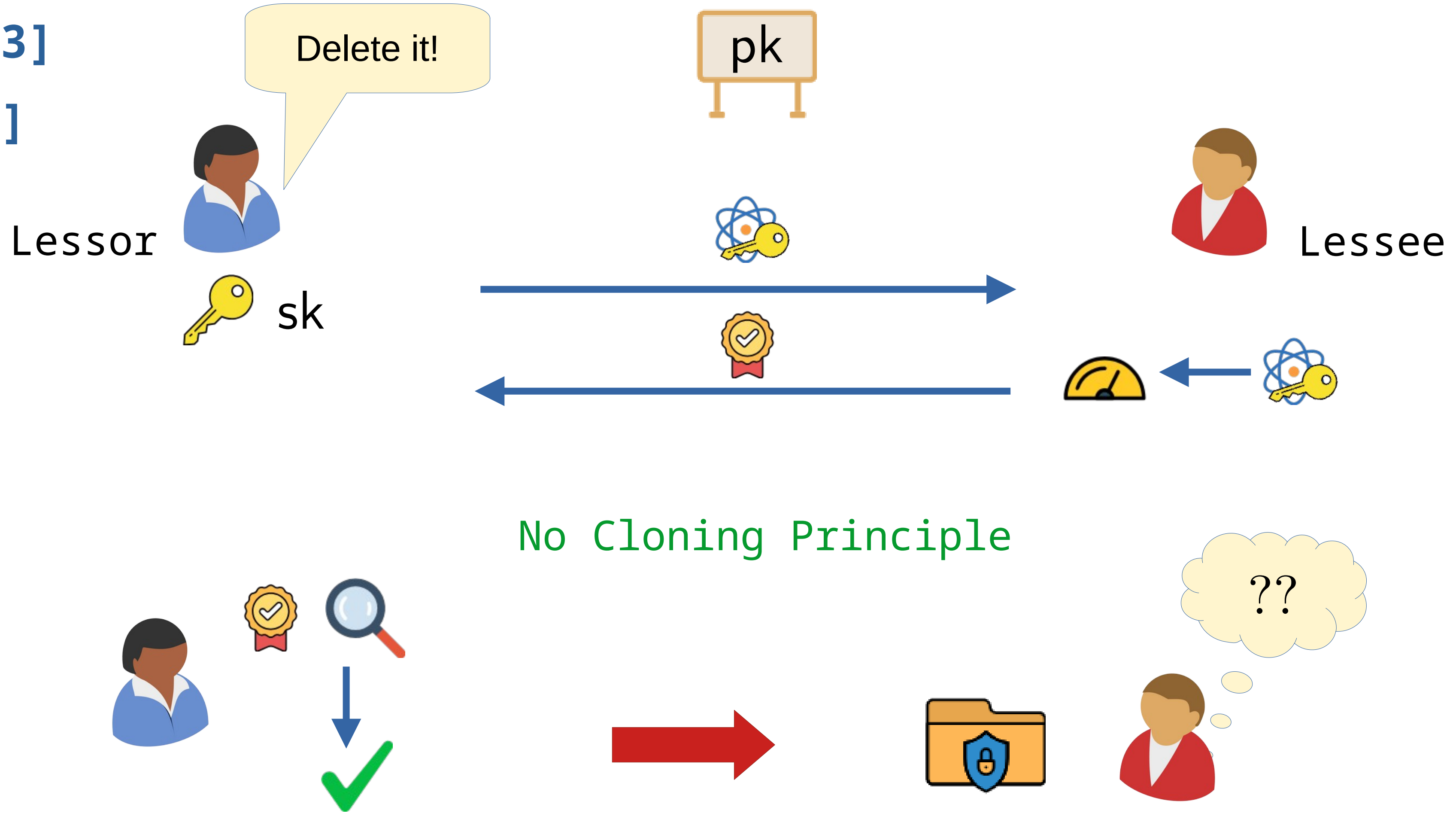
[APV23]



PKE with Secure Key Leasing

[AKN+23]

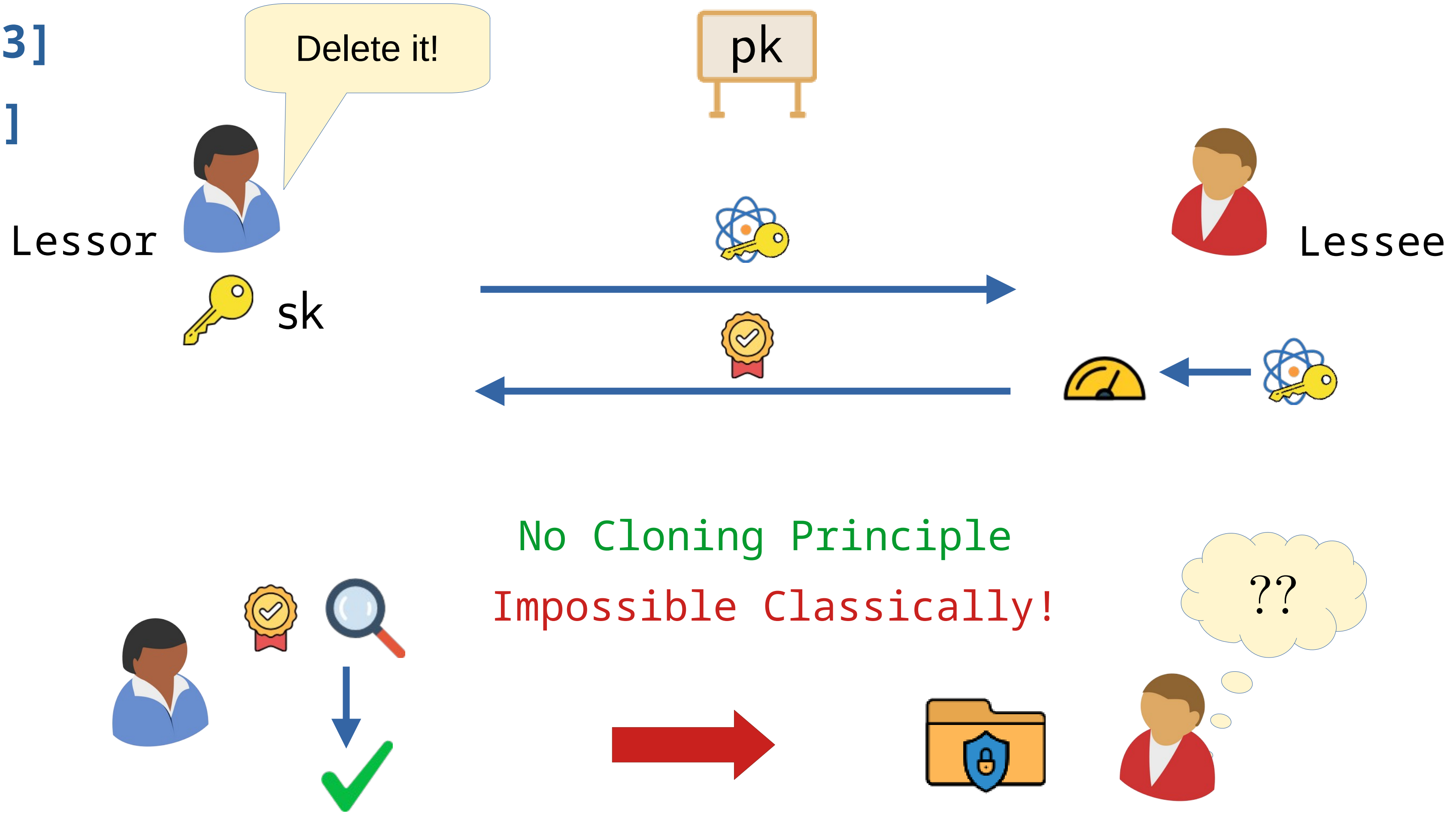
[APV23]



PKE with Secure Key Leasing

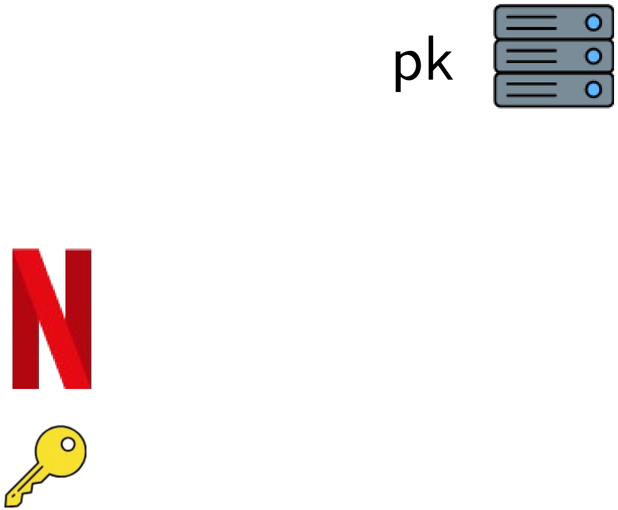
[AKN+23]

[APV23]

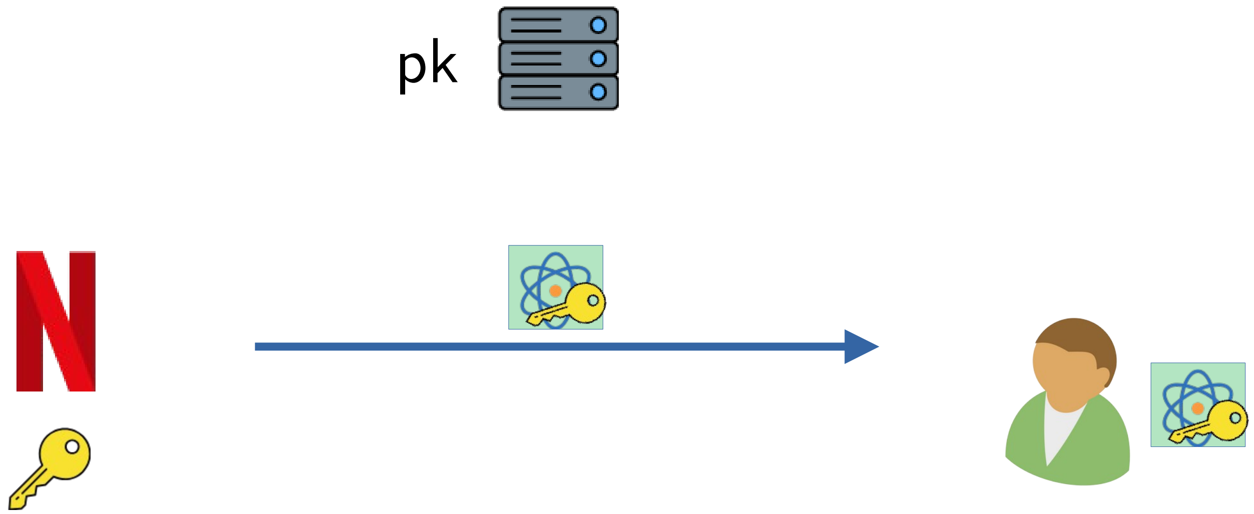


Collusion-Resistance

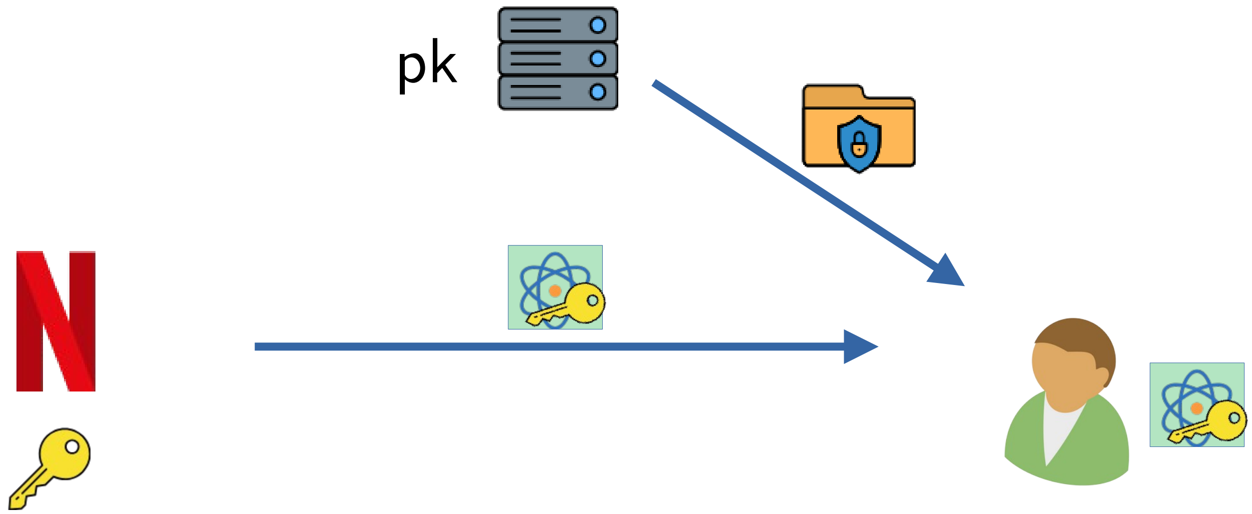
Collusion-Resistance



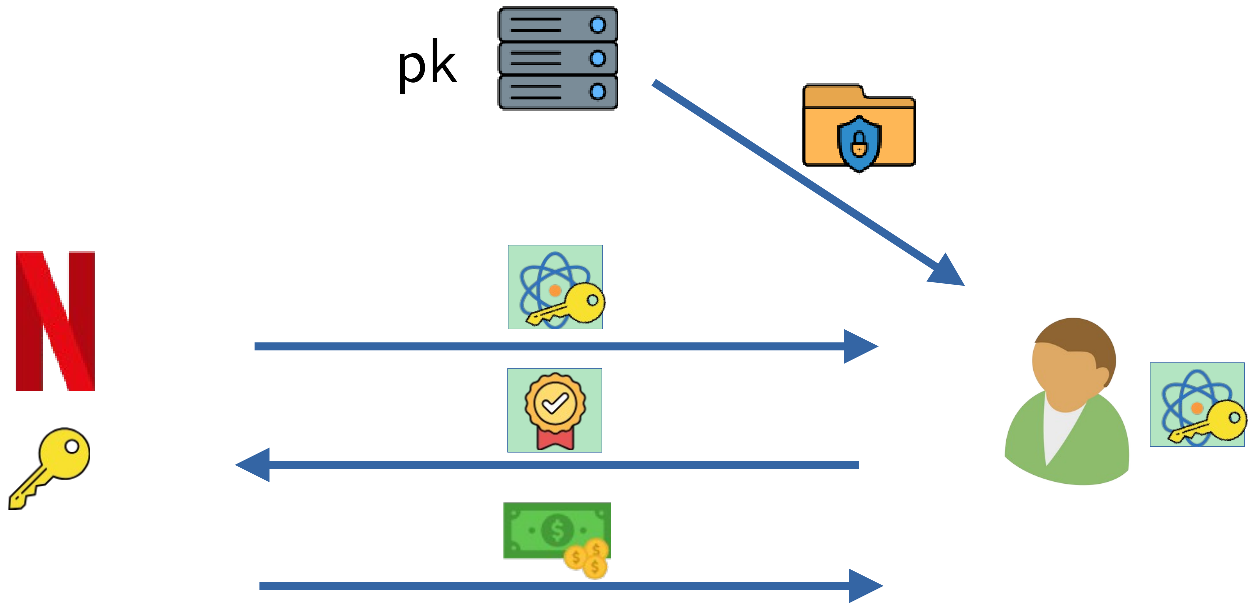
Collusion-Resistance



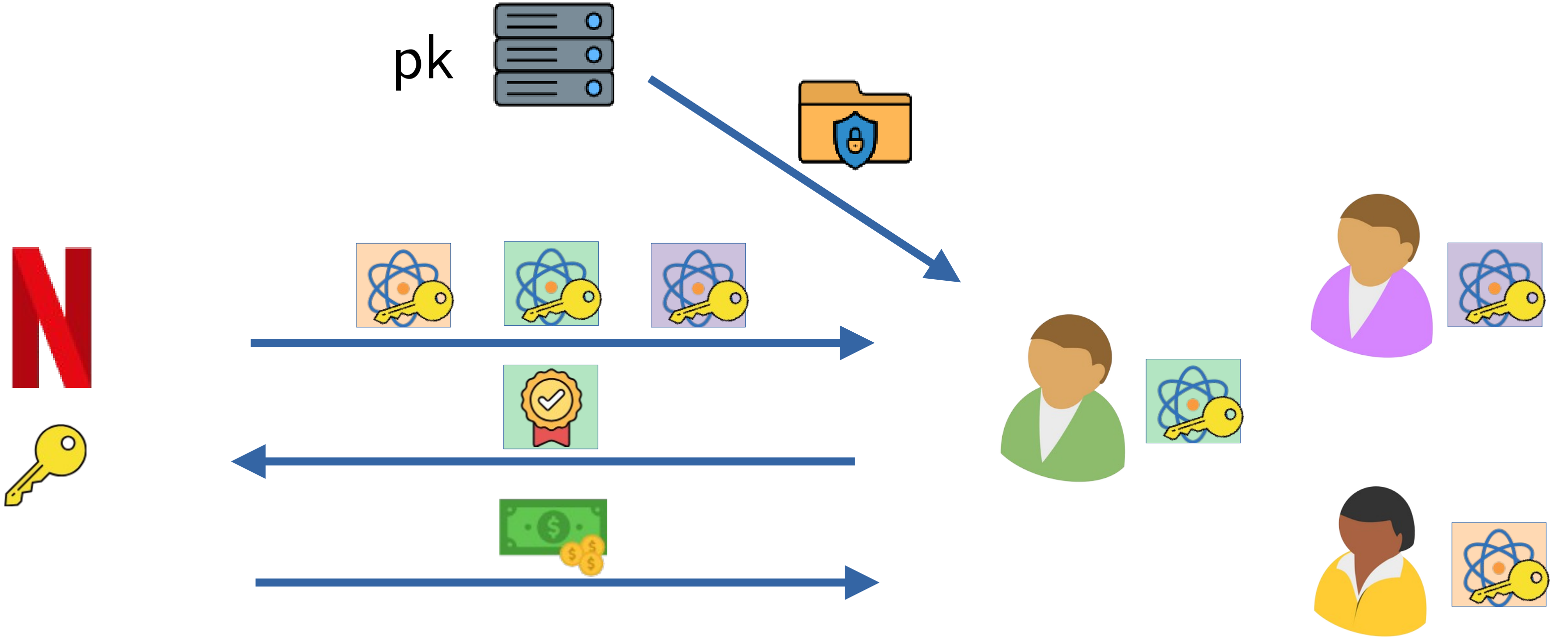
Collusion-Resistance



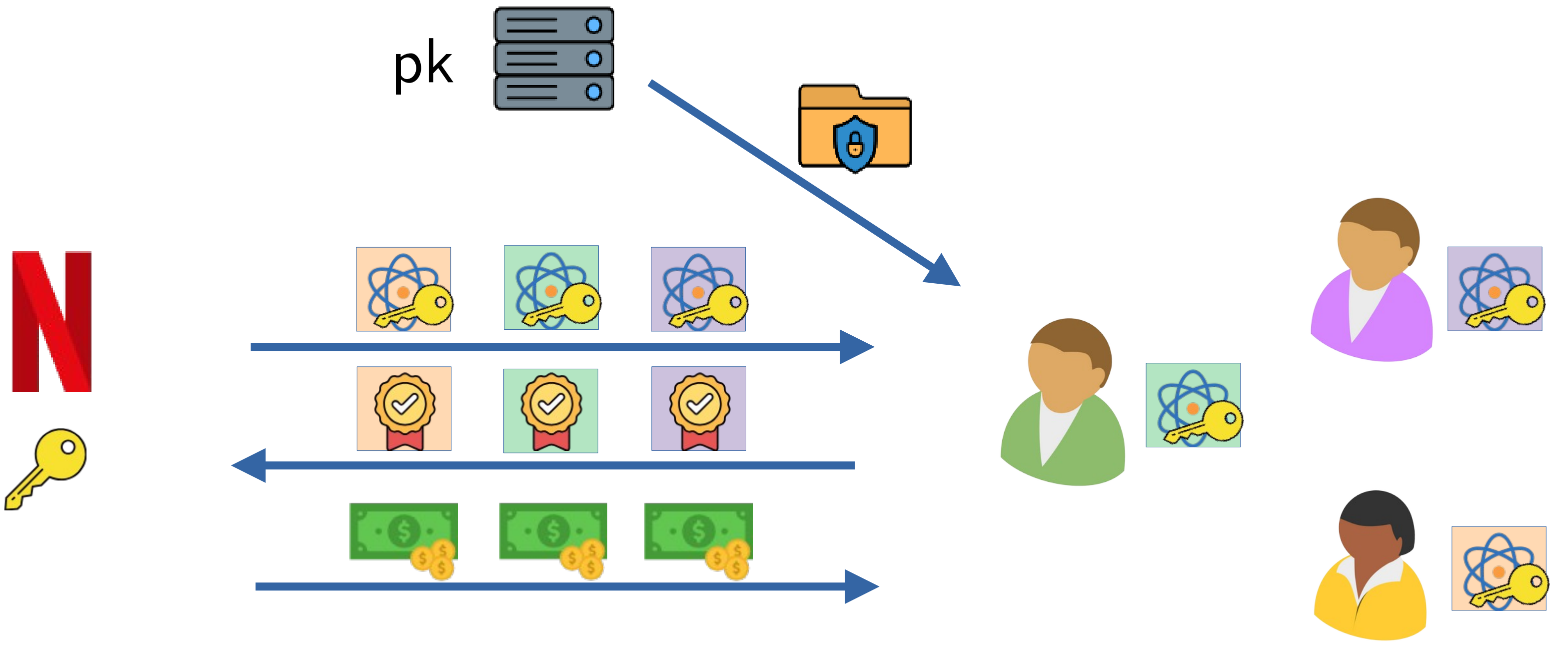
Collusion-Resistance



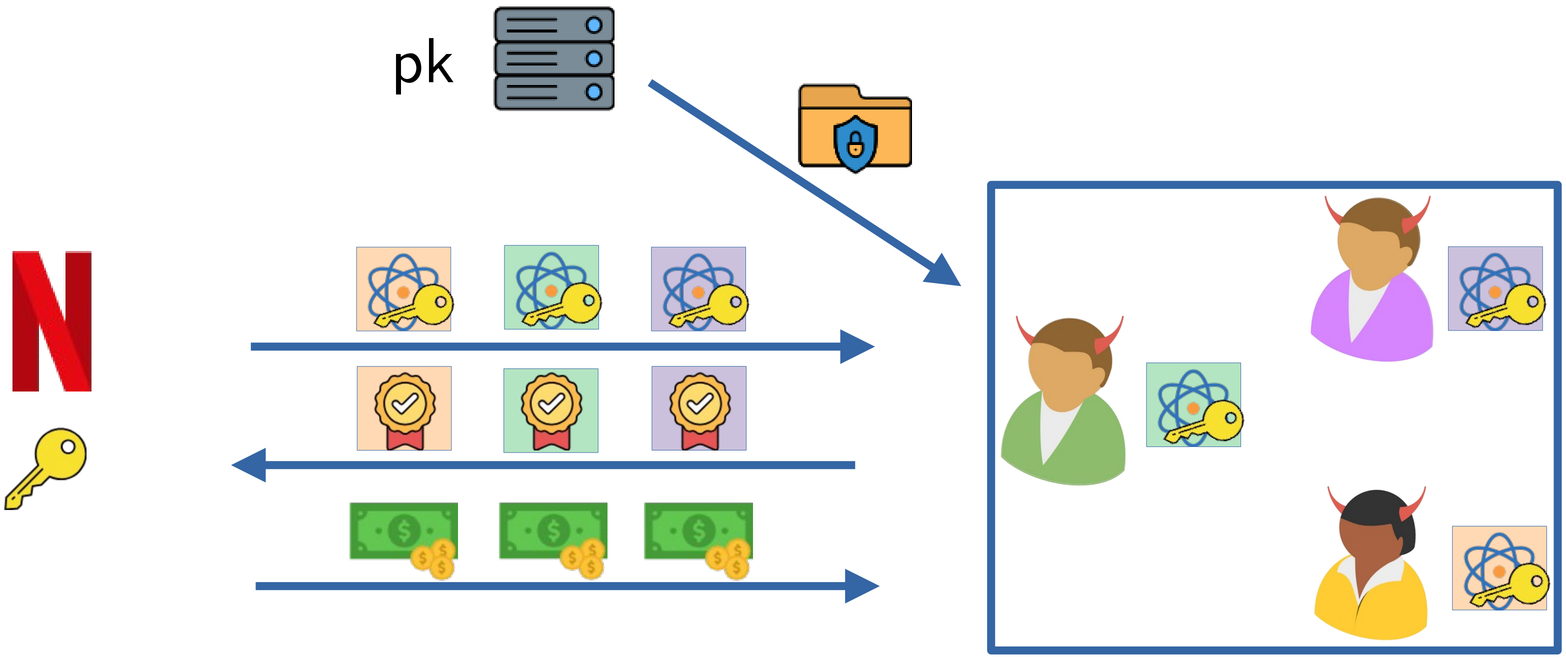
Collusion-Resistance



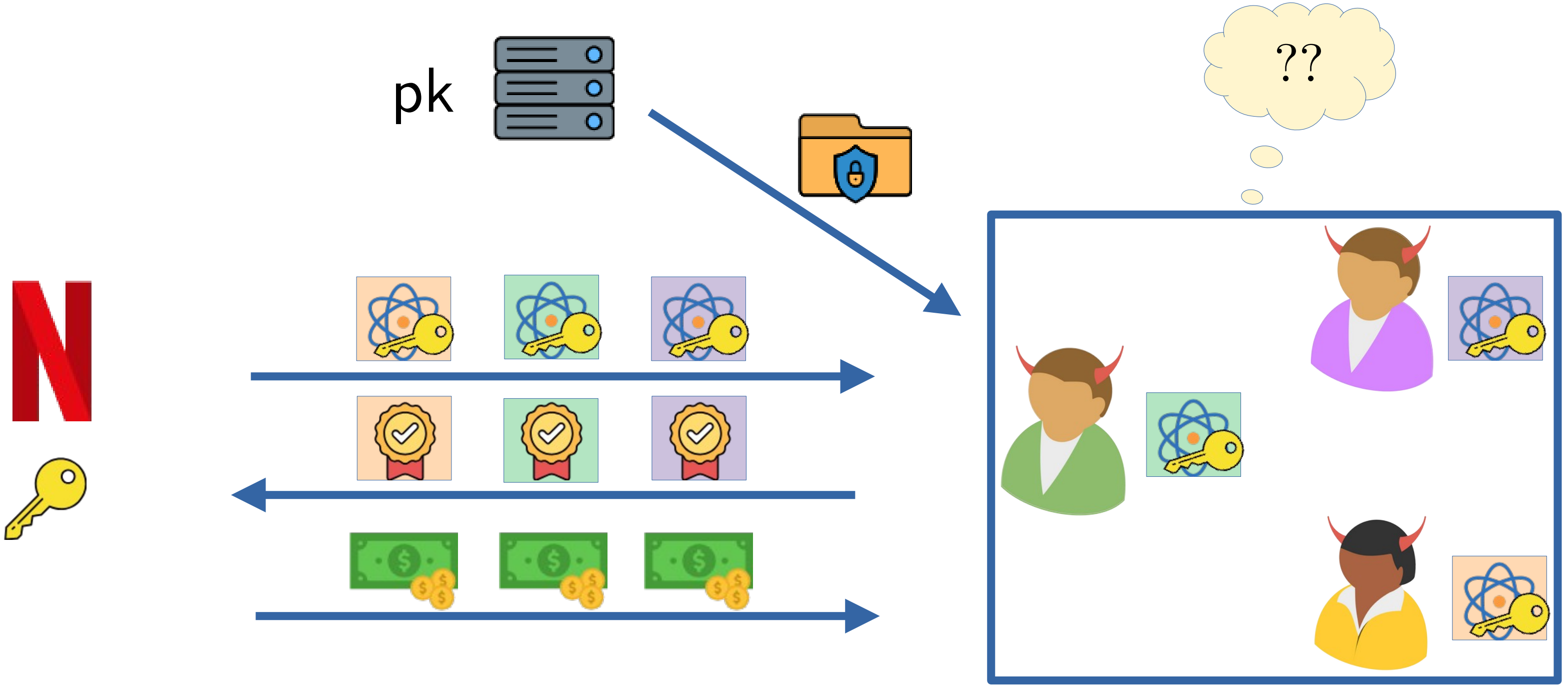
Collusion-Resistance



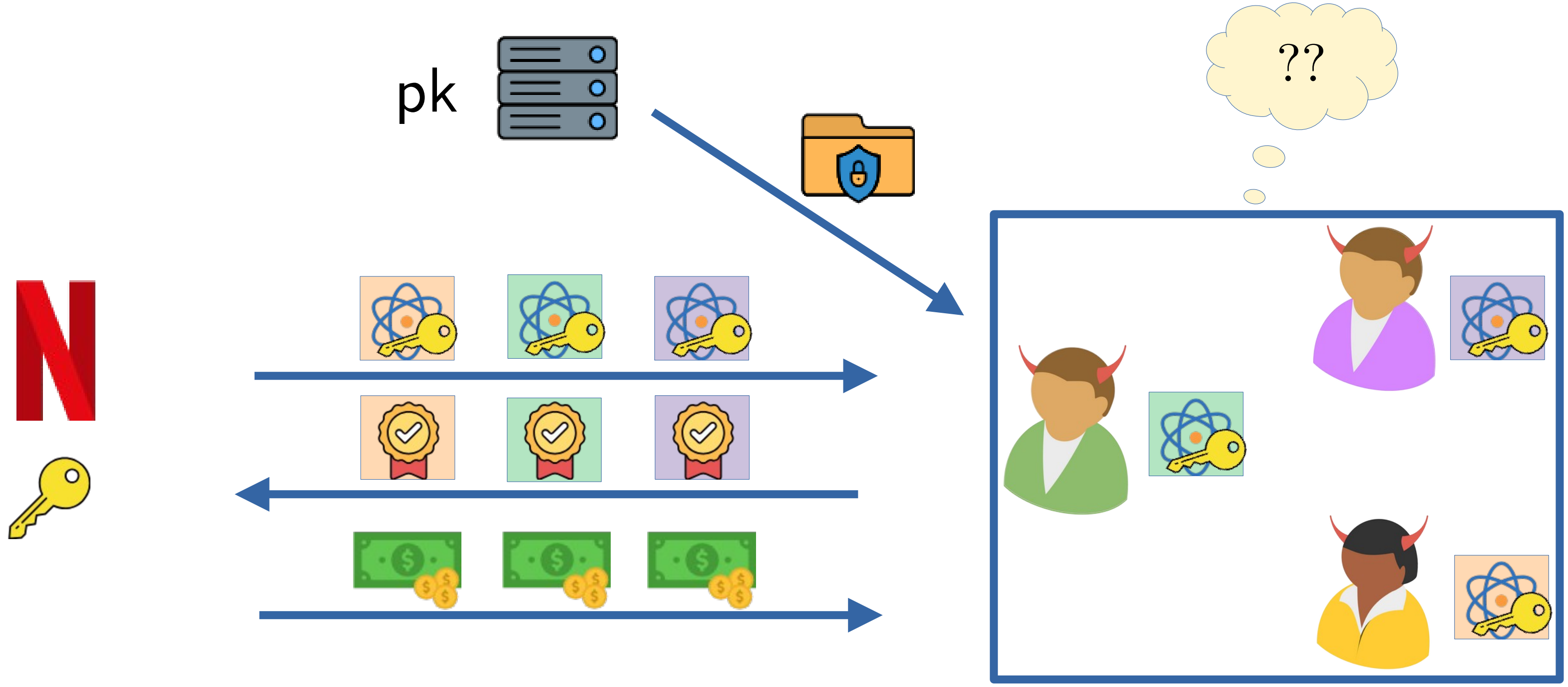
Collusion-Resistance



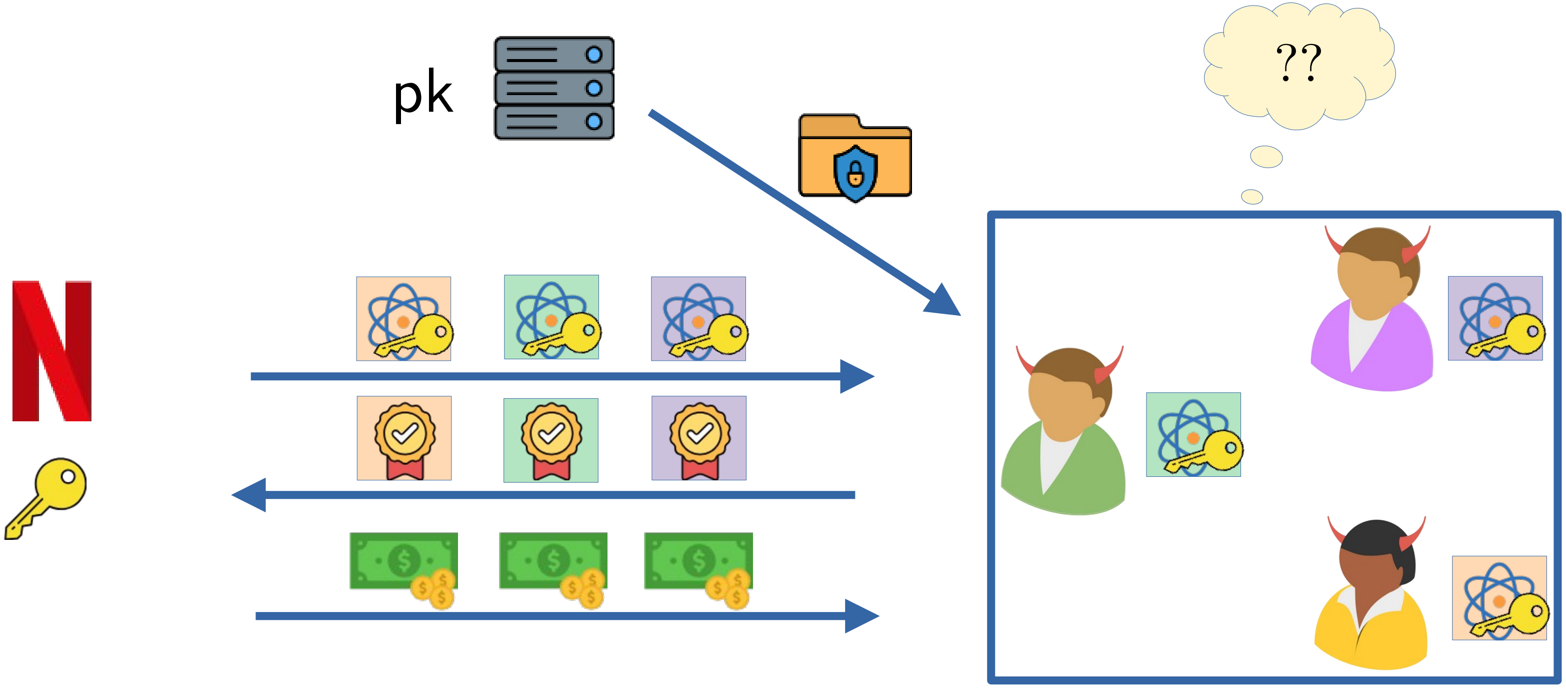
Collusion-Resistance



Collusion-Resistance



Collusion-Resistance



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

Quantum Copy Protection

Quantum Copy Protection

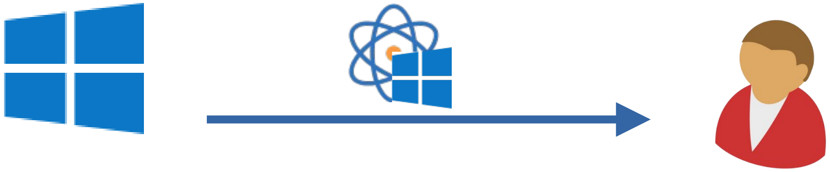
[Aar09] Copy Protection

Quantum Copy Protection

[Aar09] Copy Protection

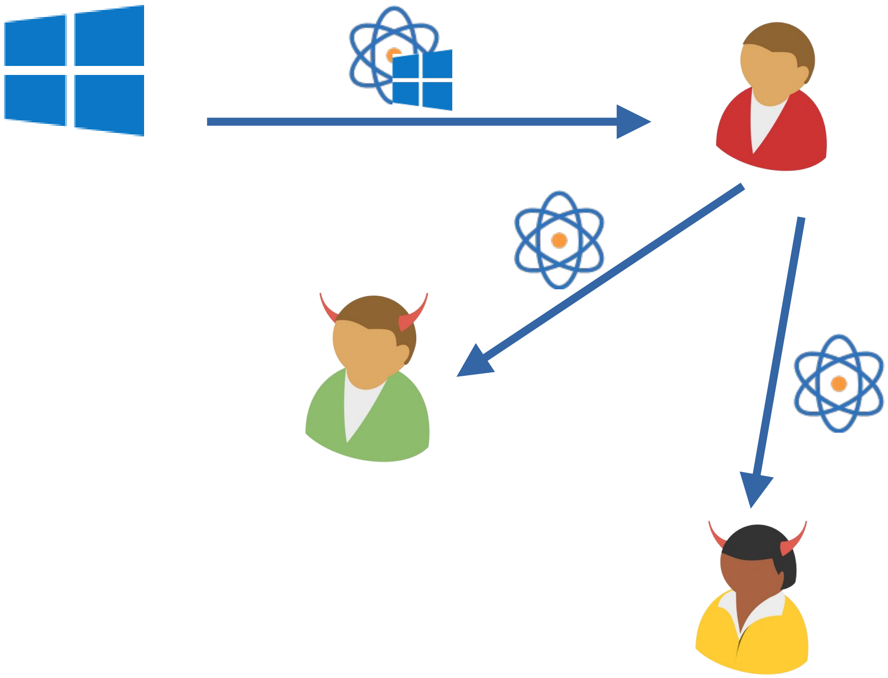
Quantum Copy Protection

[Aar09] <u>Copy Protection</u>



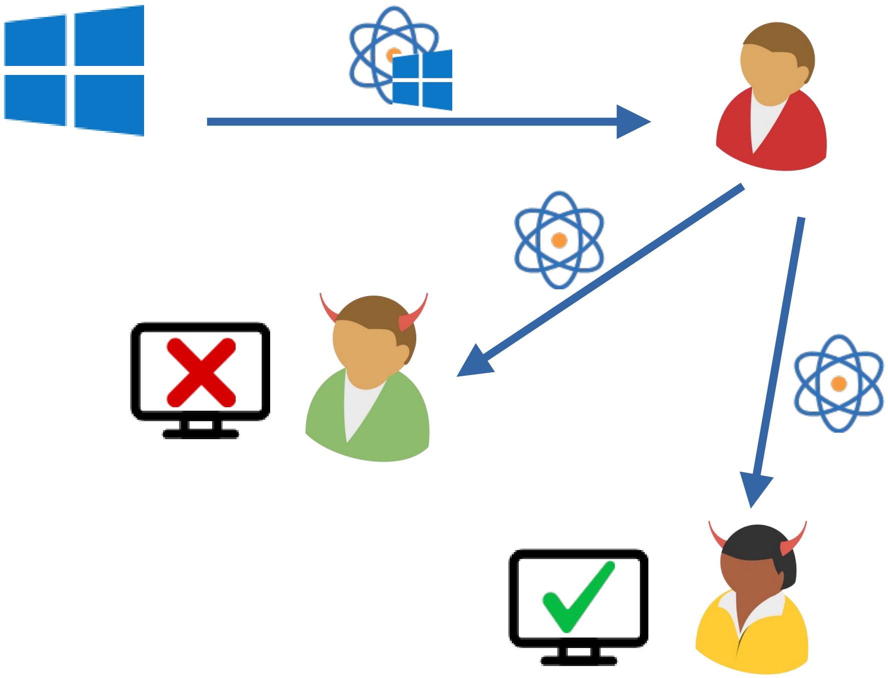
Quantum Copy Protection

[Aar09] Copy Protection



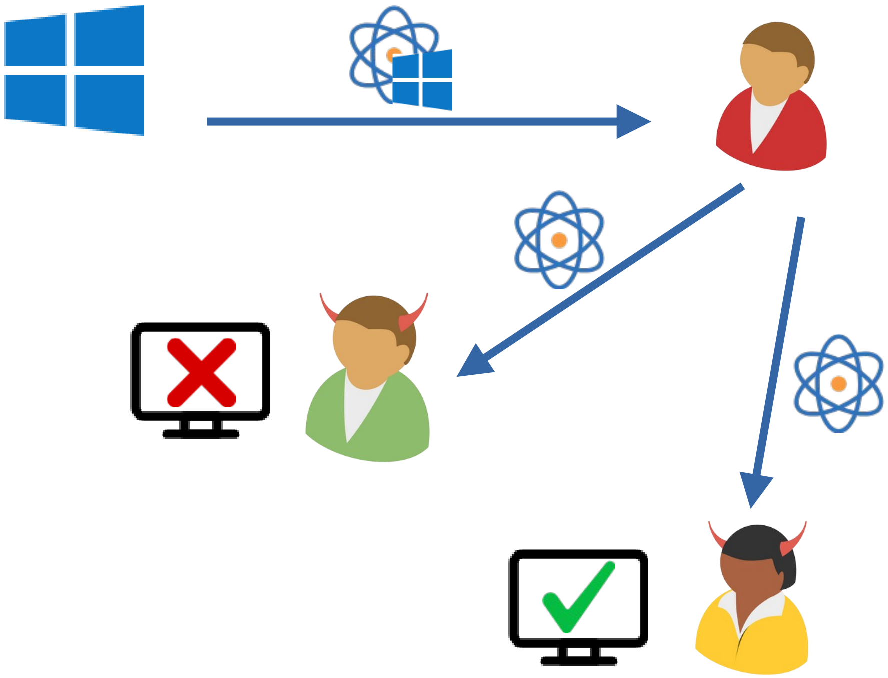
Quantum Copy Protection

[Aar09] Copy Protection



Quantum Copy Protection

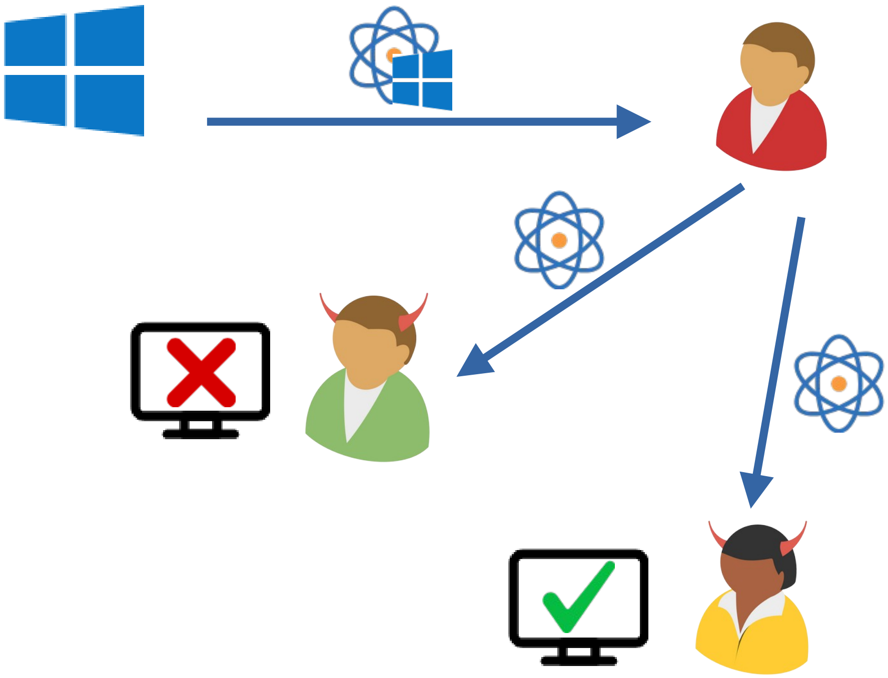
[Aar09] Copy Protection



Impossible Classically!

Quantum Copy Protection

[Aar09] Copy Protection

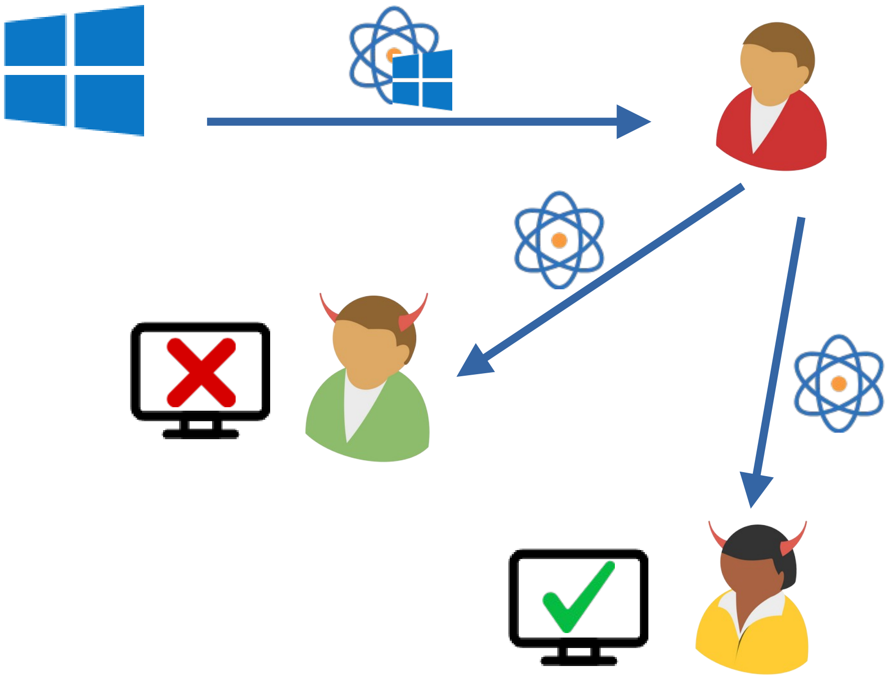


Impossible Classically!

- Implies* Secure Key Leasing

Quantum Copy Protection

[Aar09] Copy Protection

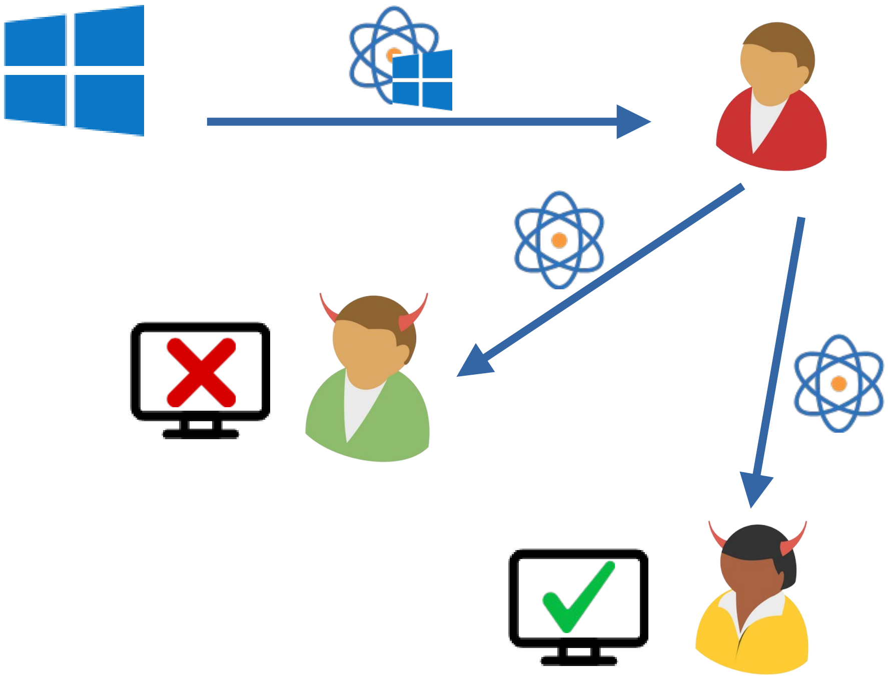


Impossible Classically!

- Implies* Secure Key Leasing
- In SKL, adversary may copy, but won’t pass verification.

Quantum Copy Protection

[Aar09] Copy Protection

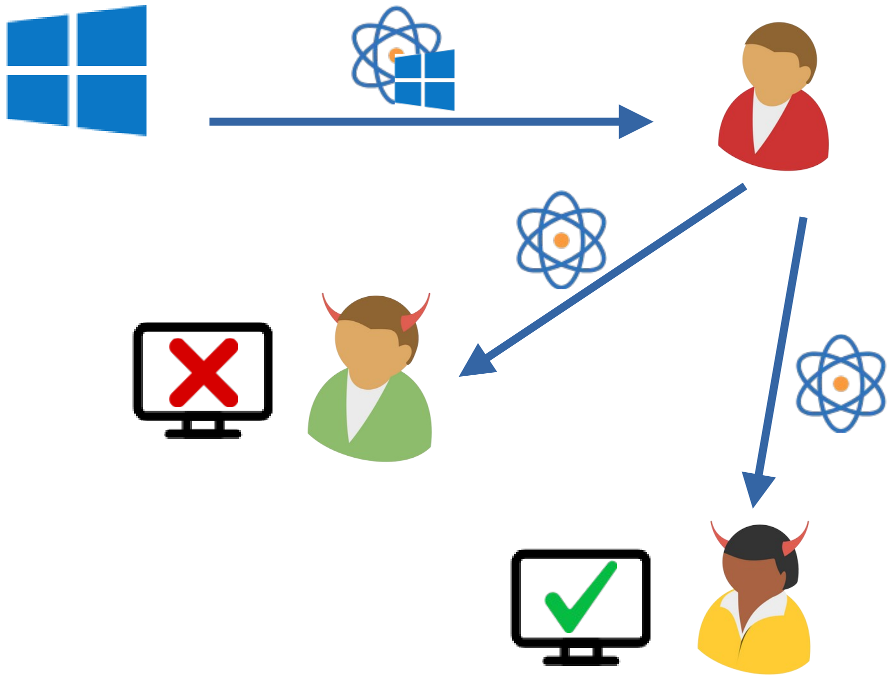


Impossible Classically!

- Implies* Secure Key Leasing
- In SKL, adversary may copy, but won’t pass verification.
- Collusion-resistant Constructions **[LLQZ22]**, **[ÇG24]**

Quantum Copy Protection

[Aar09] Copy Protection



Impossible Classically!

- Implies* Secure Key Leasing
- In SKL, adversary may copy, but won’t pass verification.
- Collusion-resistant Constructions **[LLQZ22]**, **[ÇG24]**
- Constructions rely on iO.

Prior Work

Prior Work

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

- Various PKE-SKL Constructions
- Standard Assumptions

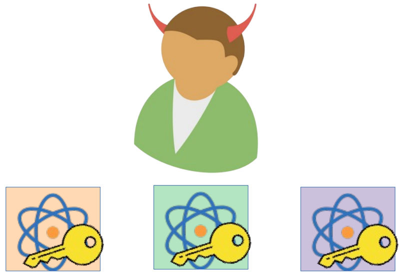
Prior Work

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

- Various PKE-SKL Constructions
- Standard Assumptions

Completely Broken with Collusions

Prior Work



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

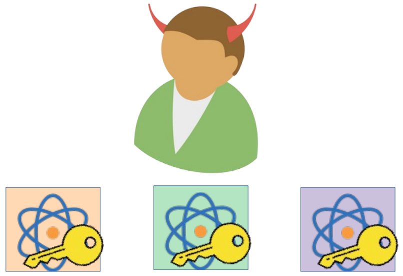
- Various PKE-SKL Constructions
- Standard Assumptions

⚠ Completely Broken with Collusions

Prior Work

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

- Various PKE-SKL Constructions
- Standard Assumptions



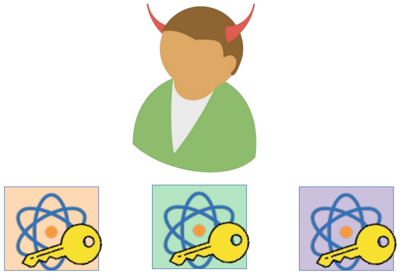
1) Correlate keys before deletion

Completely Broken with Collusions

Prior Work

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

- Various PKE-SKL Constructions
- Standard Assumptions

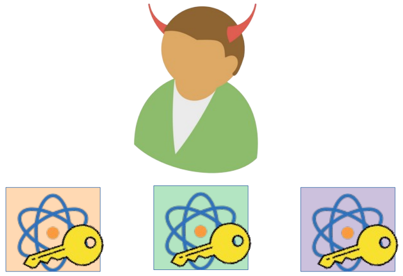


Completely Broken with Collusions

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

Prior Work

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



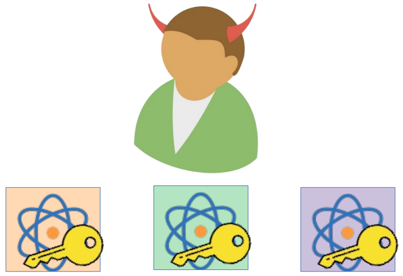
- Various PKE-SKL Constructions
- Standard Assumptions

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]:



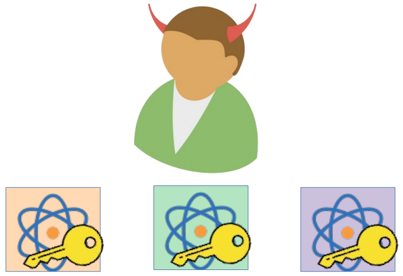
- Various PKE-SKL Constructions
- Standard Assumptions

⚠ 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

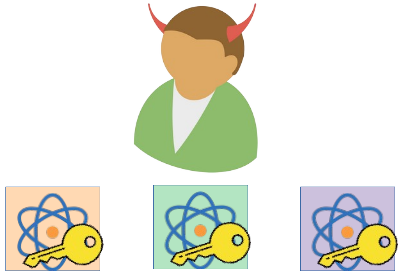
Completely Broken with Collusions

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

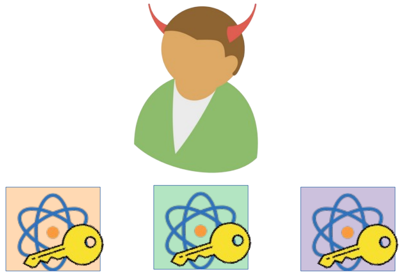
Challenging Setting.
Provable-Security even more so!

[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

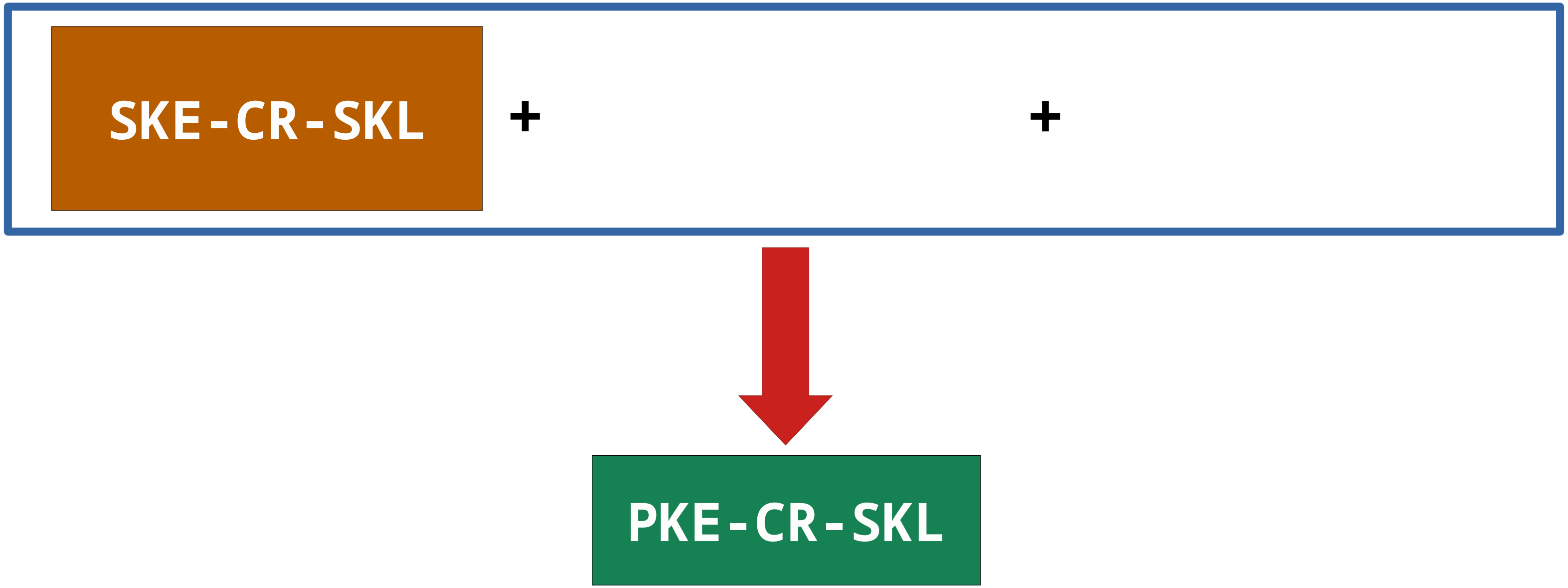
[KNP25]

+ +

PKE-CR-SKL

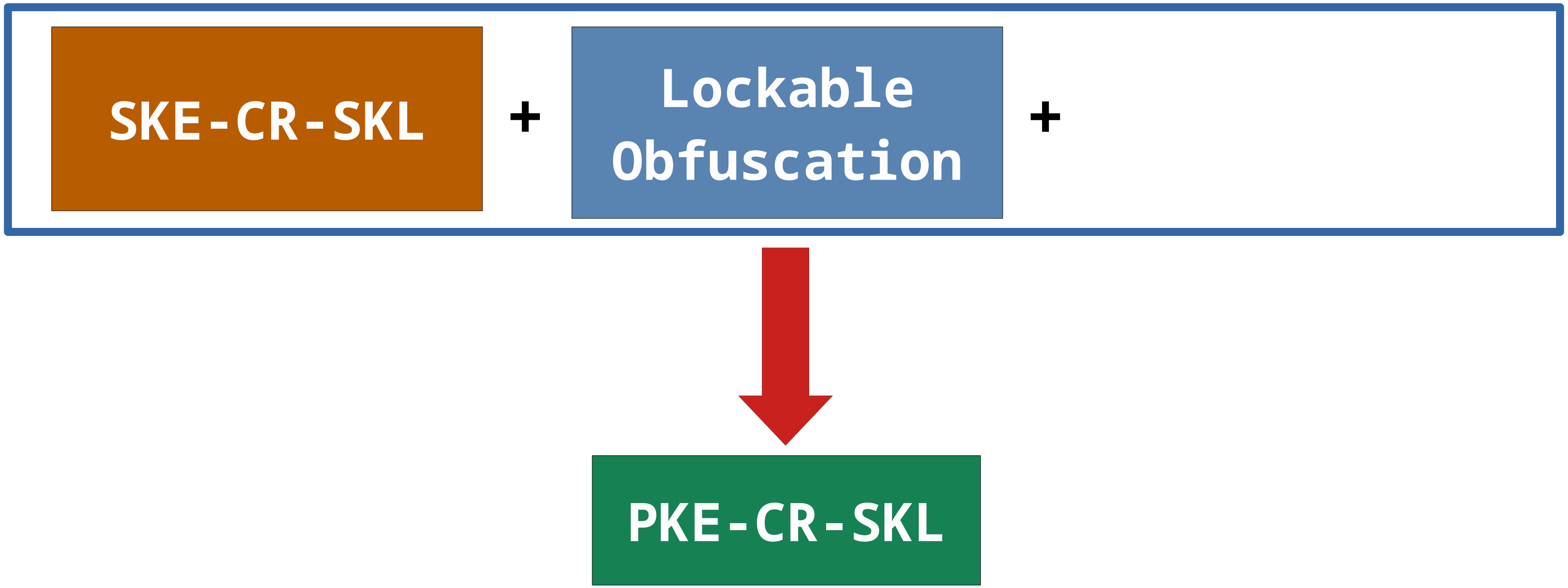
Main Result

[KNP25]



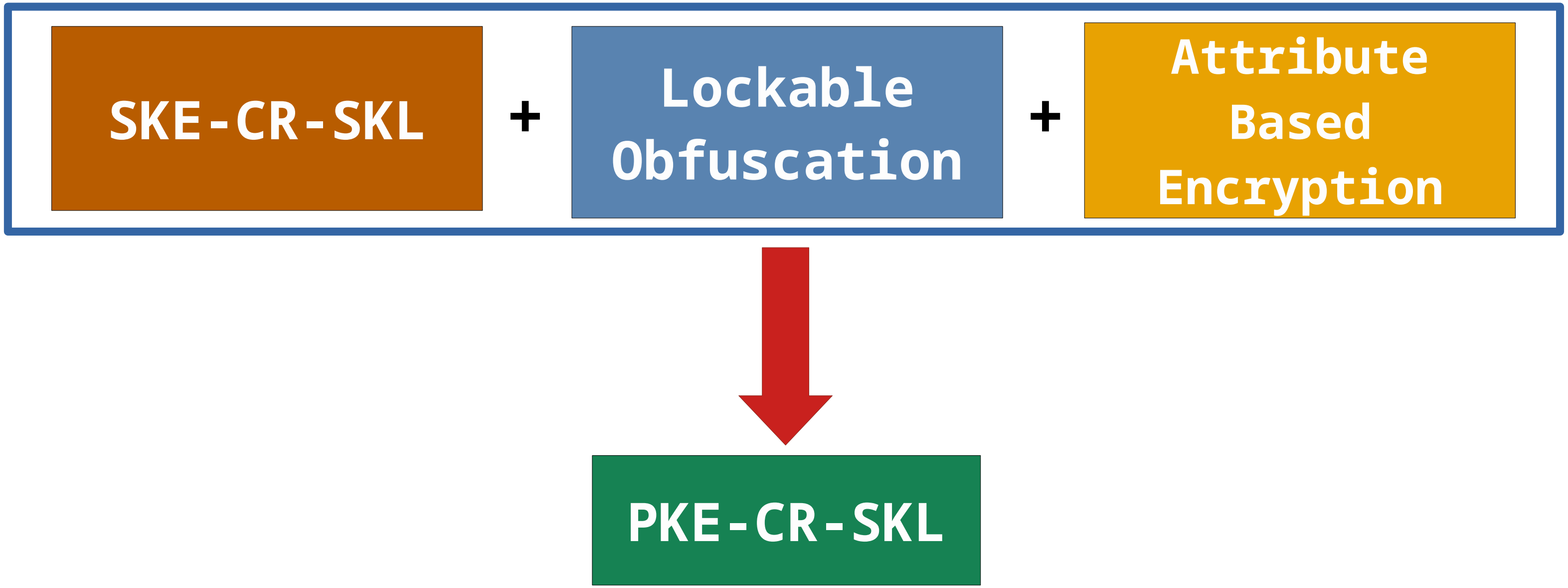
Main Result

[KNP25]



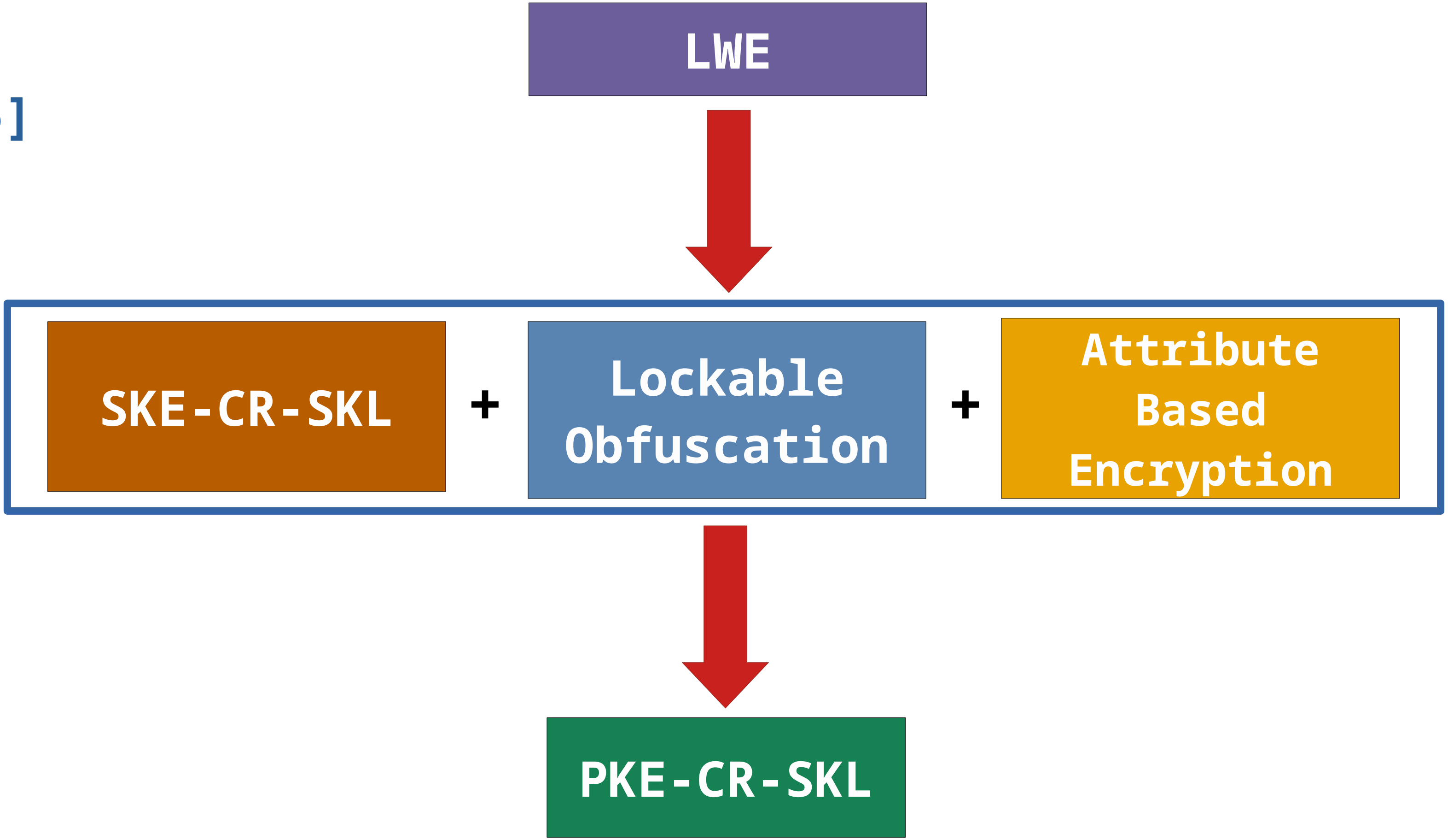
Main Result

[KNP25]

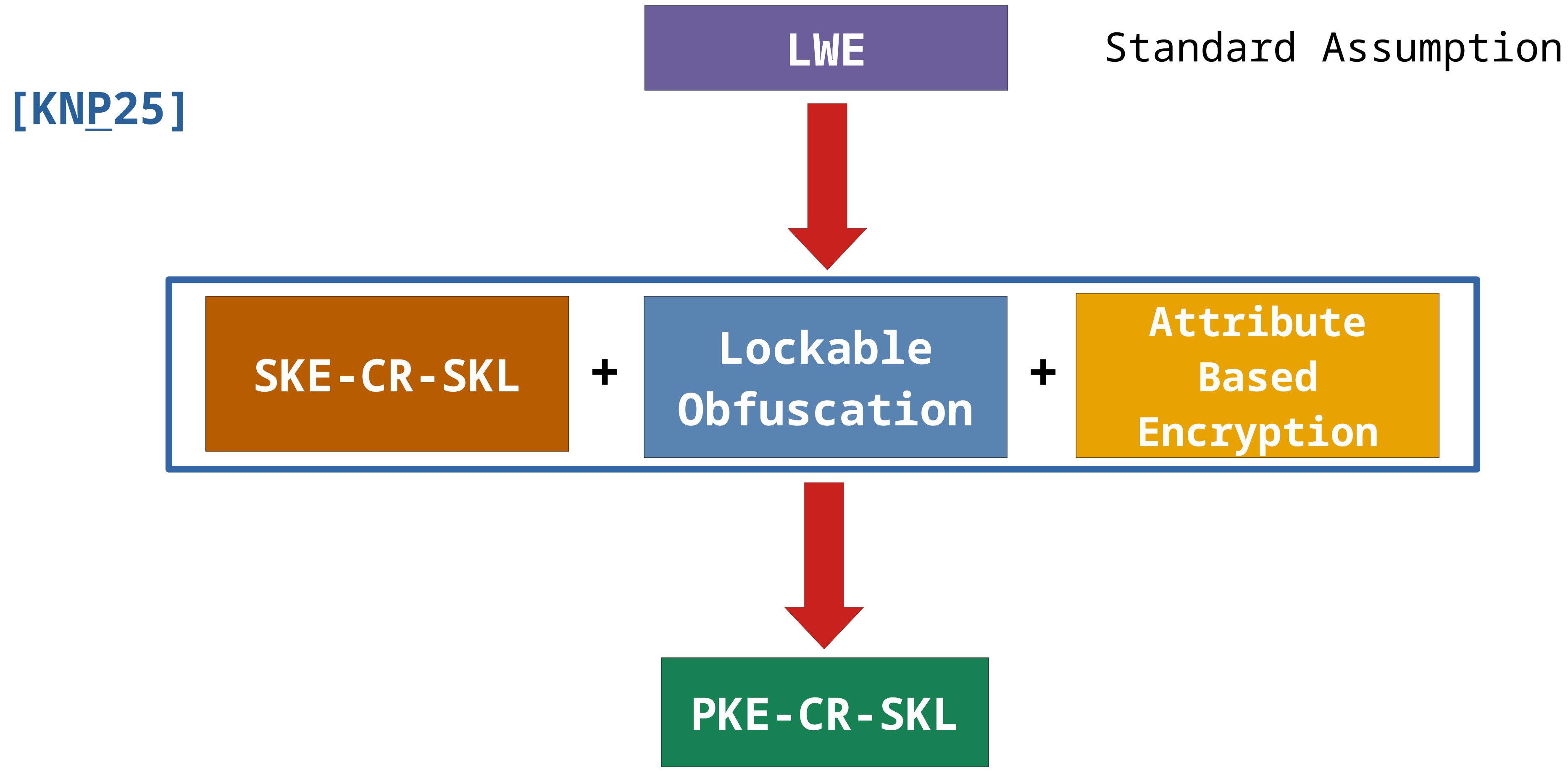


Main Result

[KNP25]

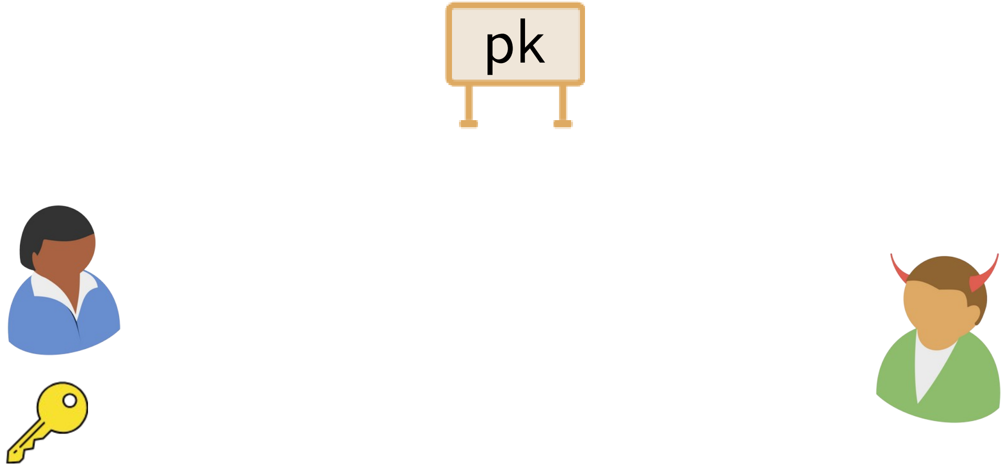


Main Result

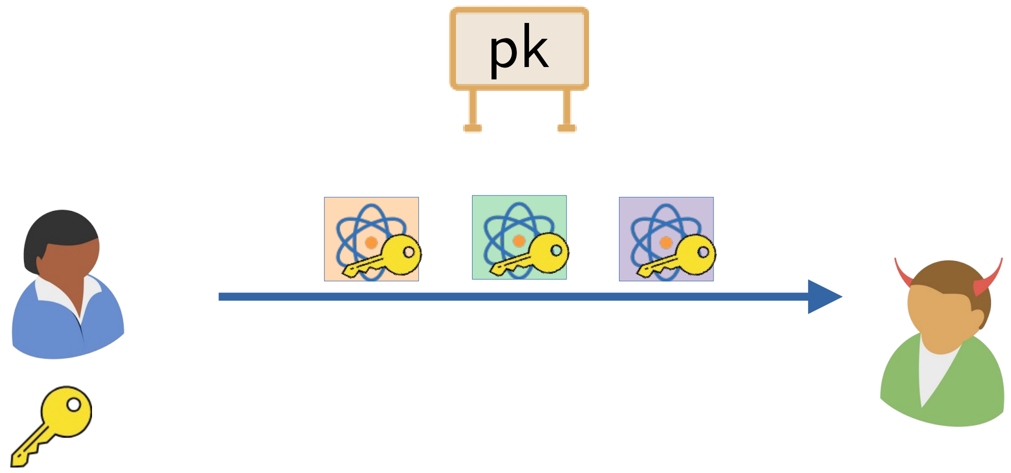

LWE
Standard Assumption
[KNP25]
SKE-CR-SKL
+
Lockable Obfuscation
+
Attribute Based Encryption
PKE-CR-SKL

PKE-CR-SKL and SKE-CR-SKL

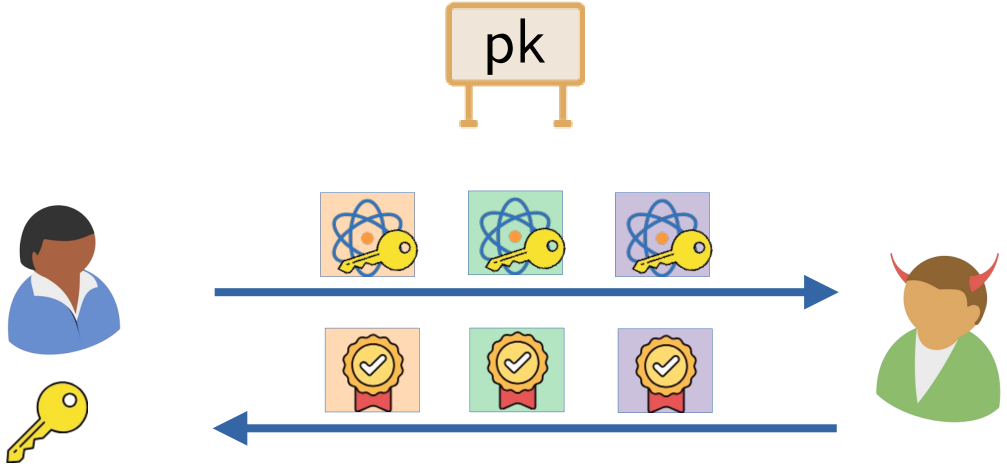
PKE-CR-SKL and SKE-CR-SKL



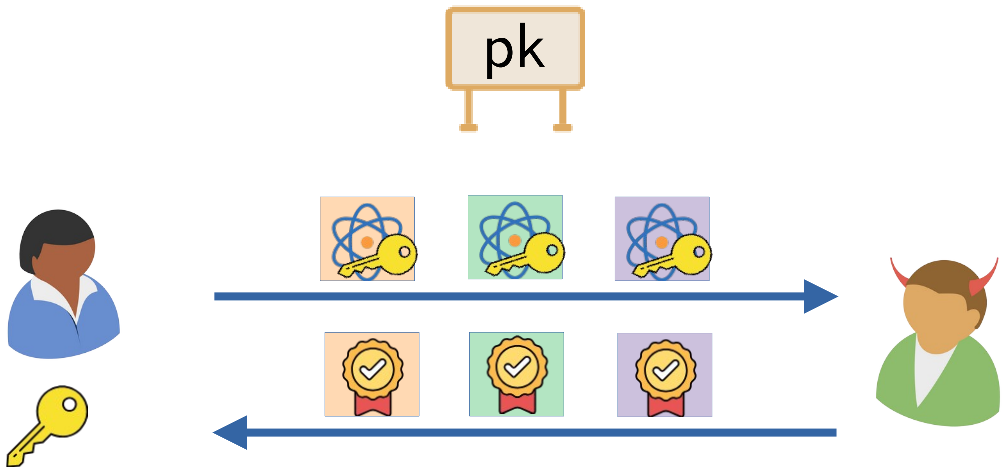
PKE-CR-SKL and SKE-CR-SKL

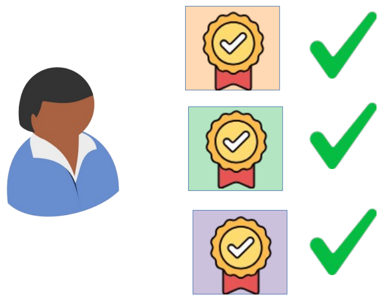


PKE-CR-SKL and SKE-CR-SKL

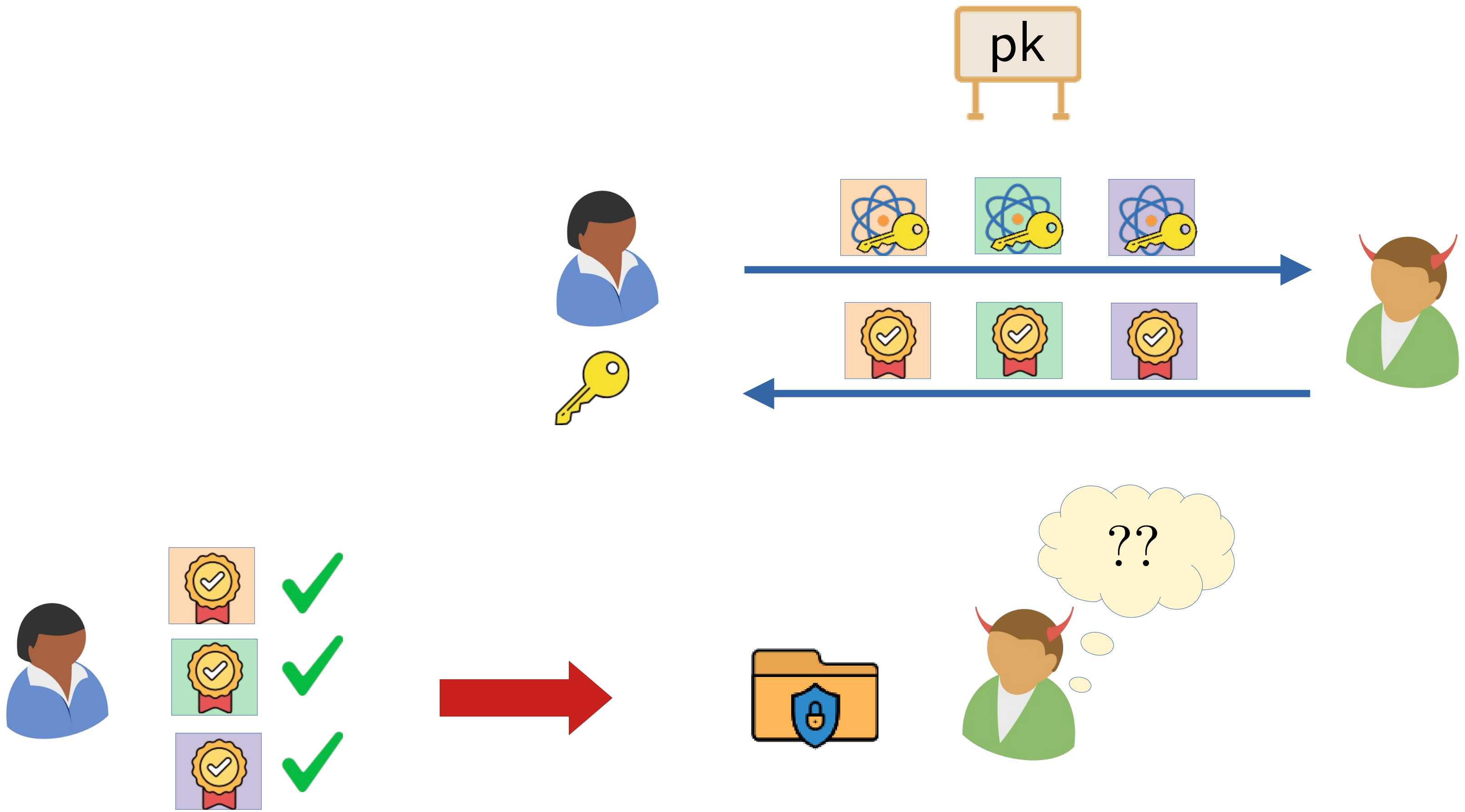


PKE-CR-SKL and SKE-CR-SKL



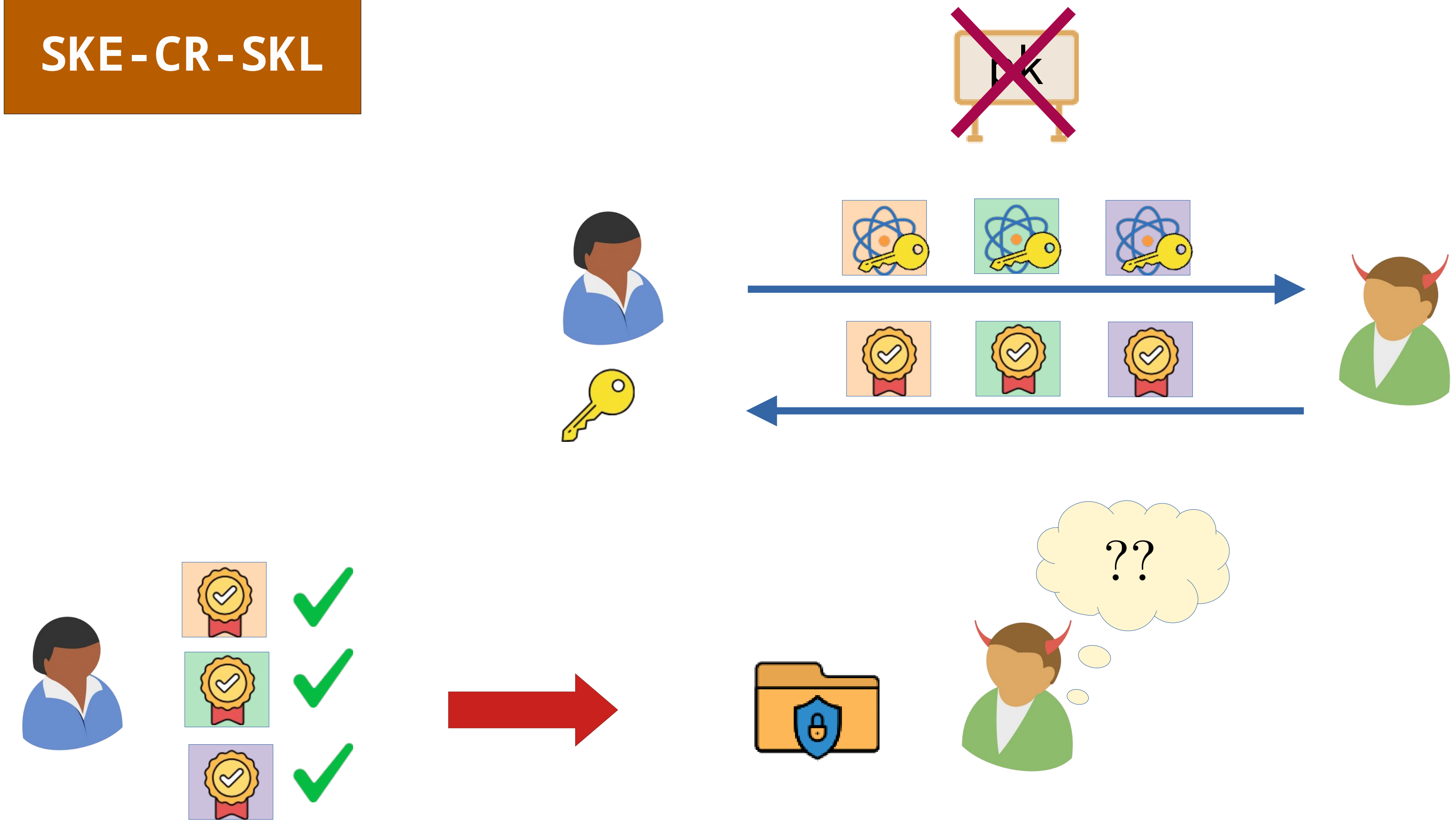


PKE-CR-SKL and SKE-CR-SKL



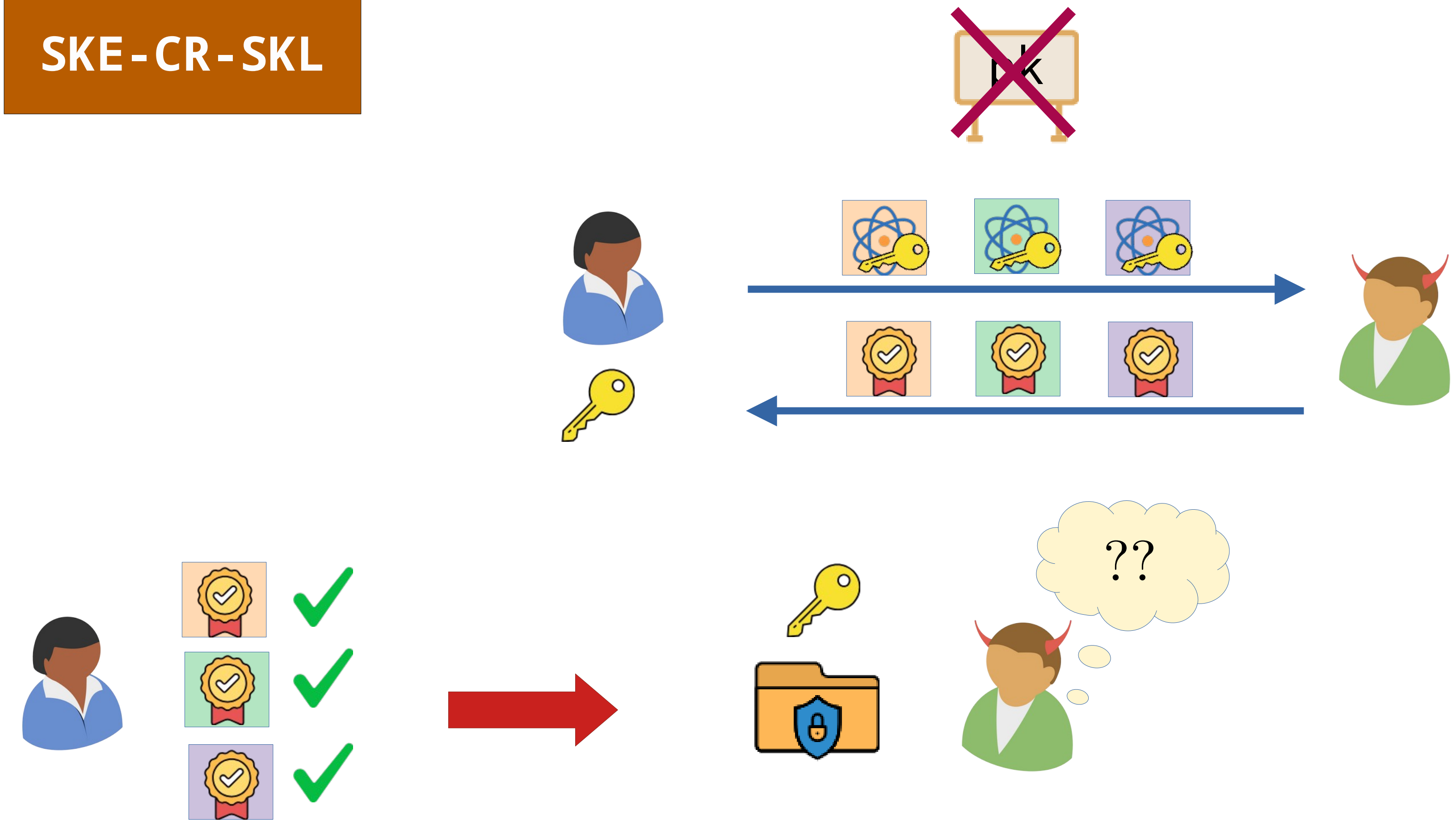
PKE-CR-SKL and SKE-CR-SKL

SKE-CR-SKL



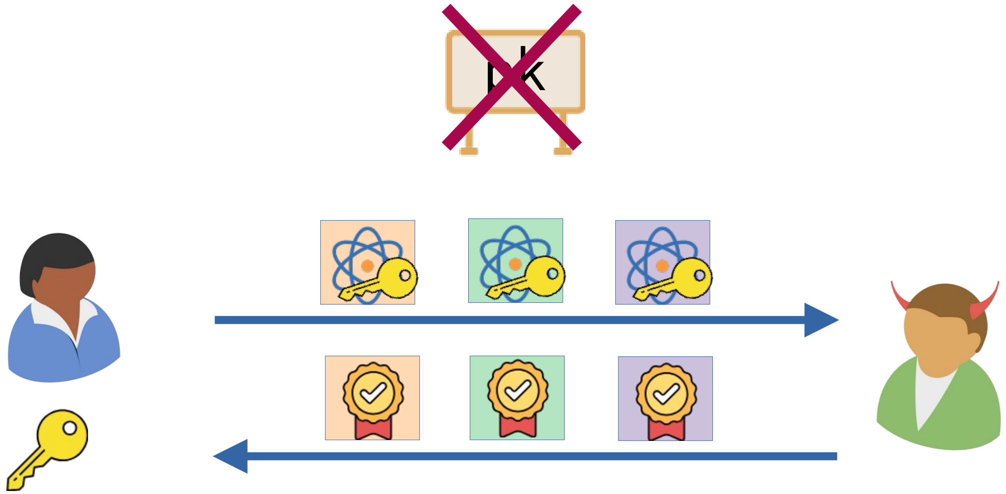
PKE-CR-SKL and SKE-CR-SKL

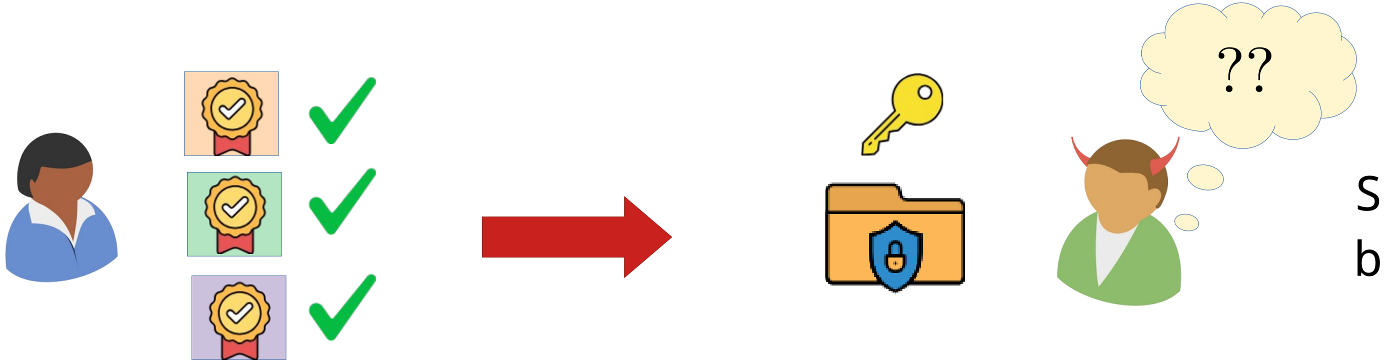
SKE-CR-SKL



PKE-CR-SKL and SKE-CR-SKL

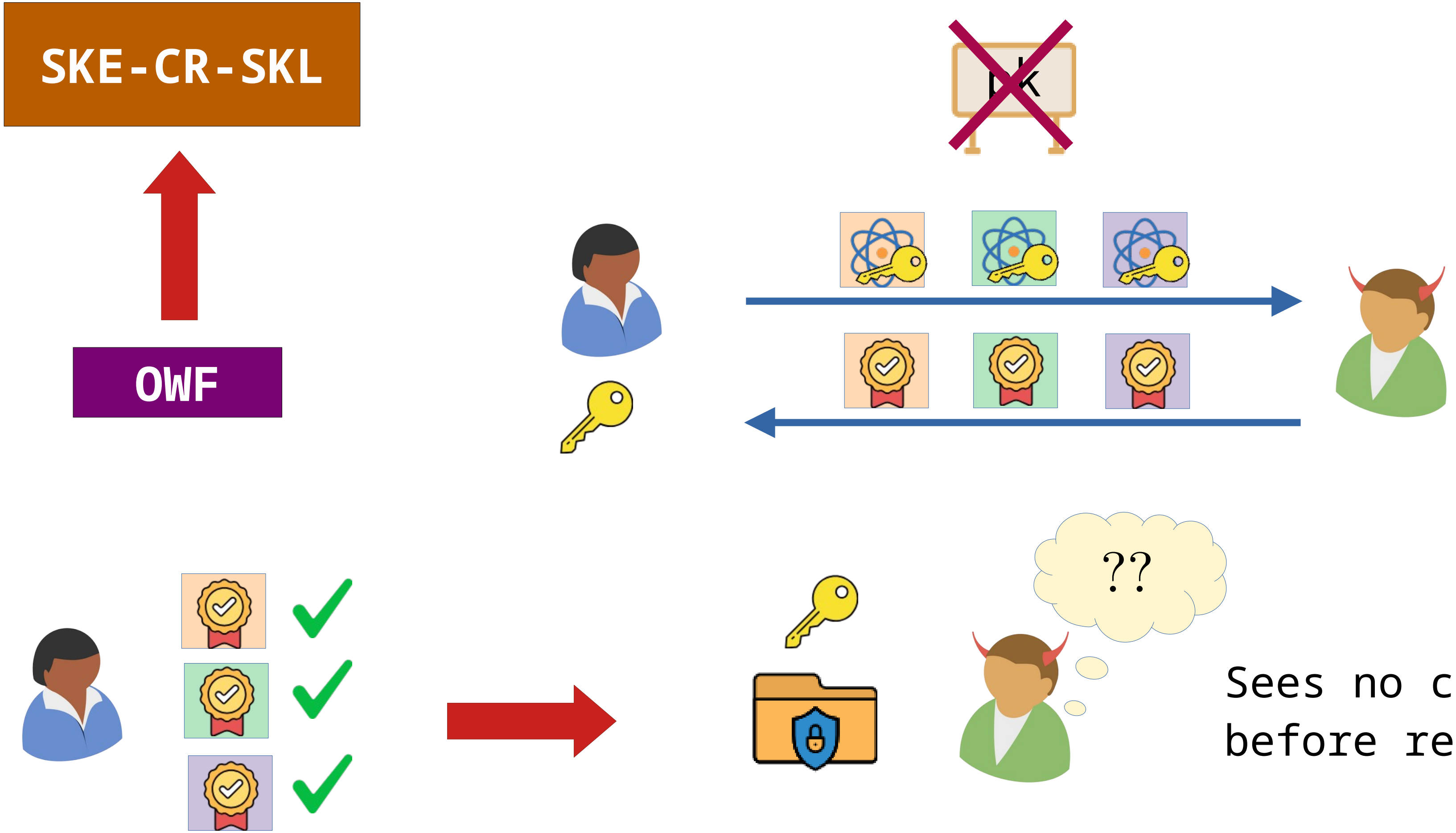
SKE-CR-SKL





Sees no ciphertexts before returning!

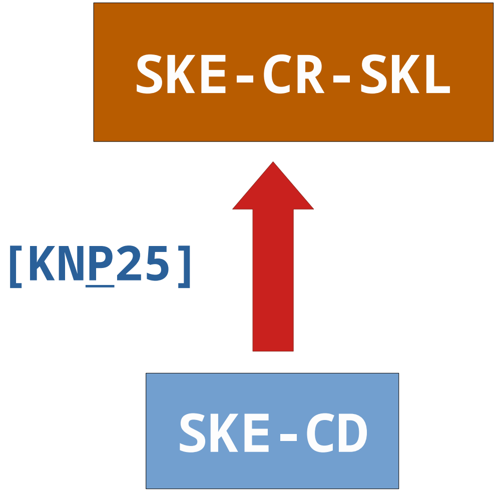
PKE-CR-SKL and SKE-CR-SKL



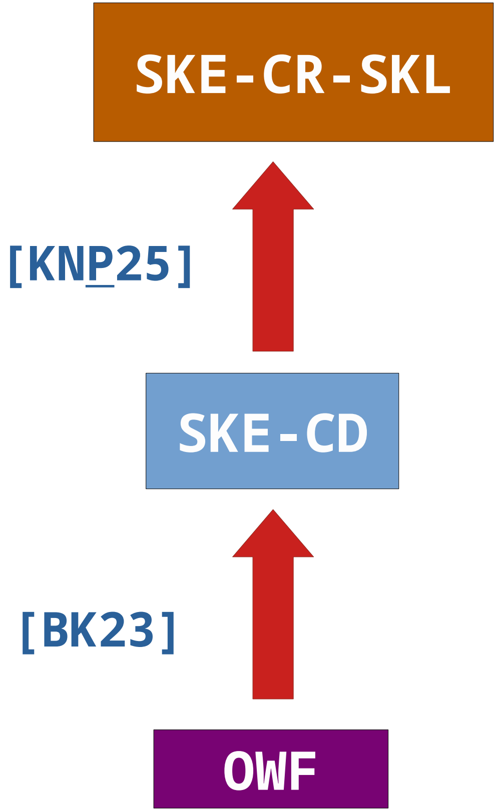
Sees no ciphertexts before returning!

Constructing SKE-CR-SKL

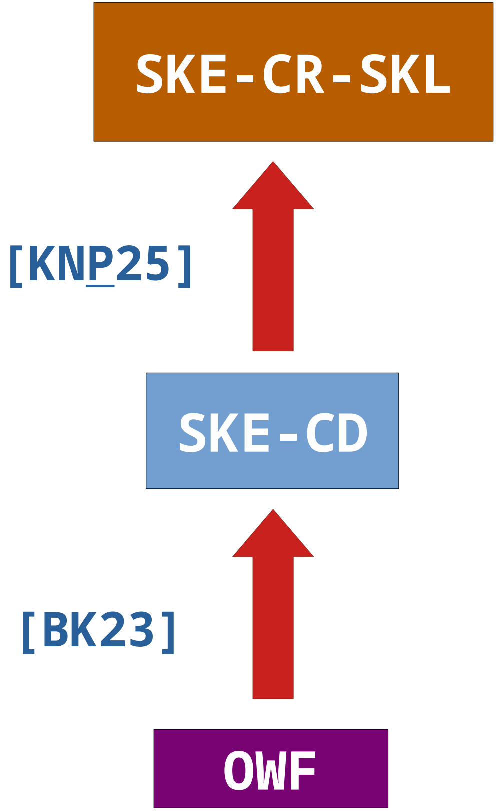
Constructing SKE-CR-SKL

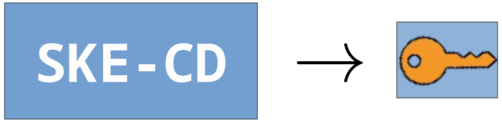


Constructing SKE-CR-SKL

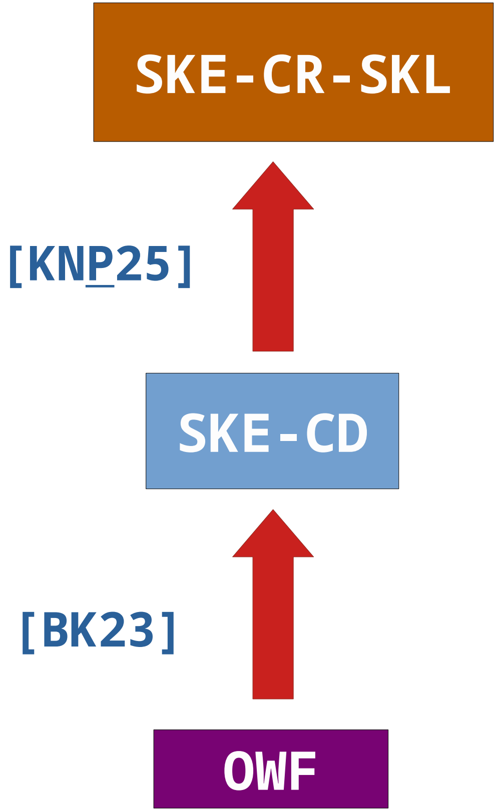


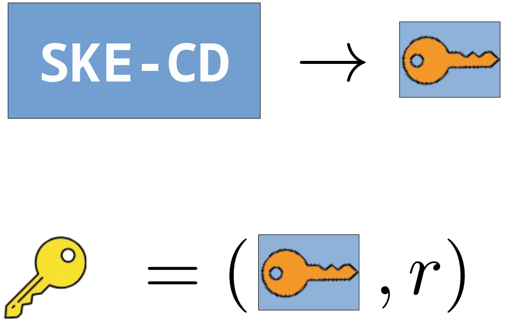
Constructing SKE-CR-SKL



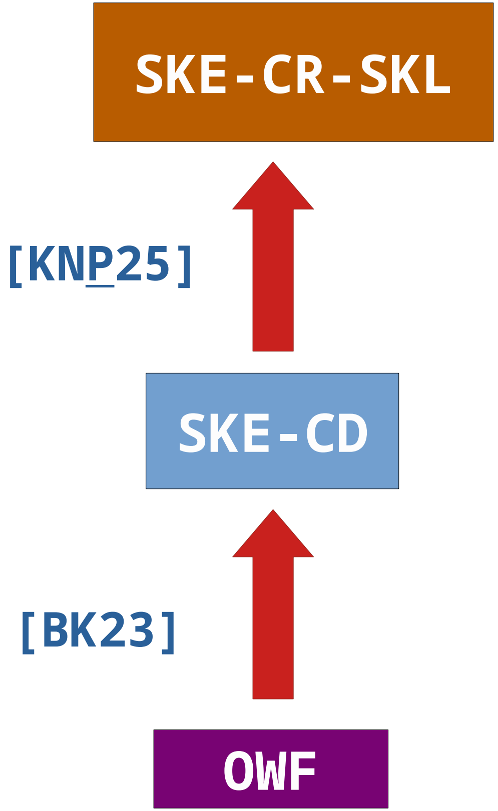


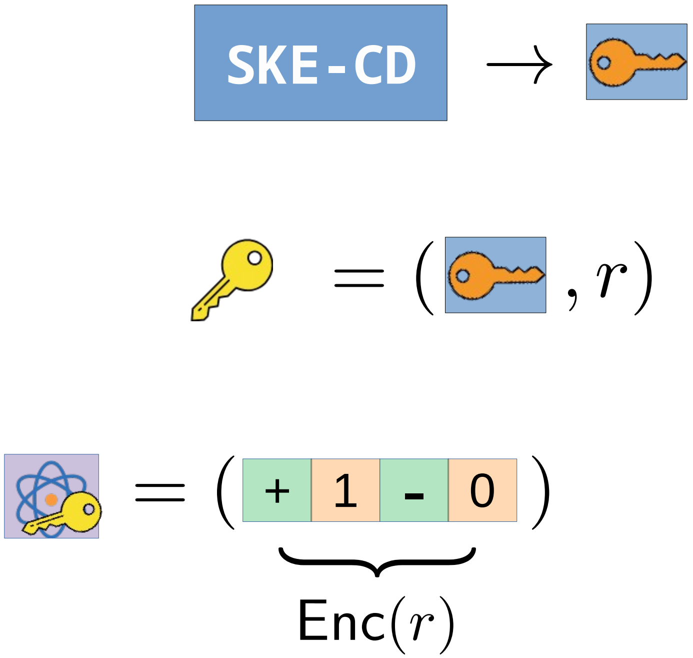
Constructing SKE-CR-SKL



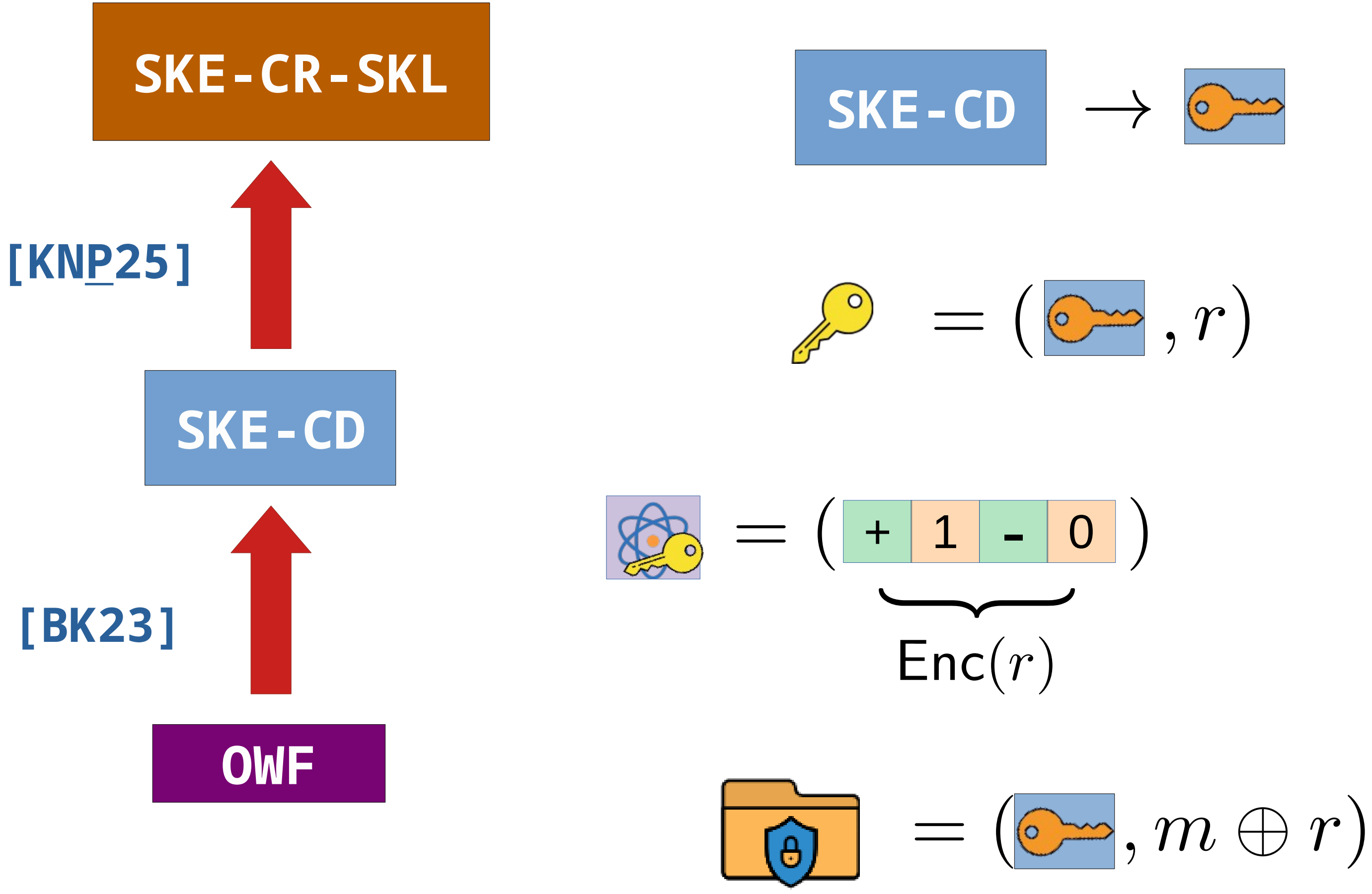


Constructing SKE-CR-SKL

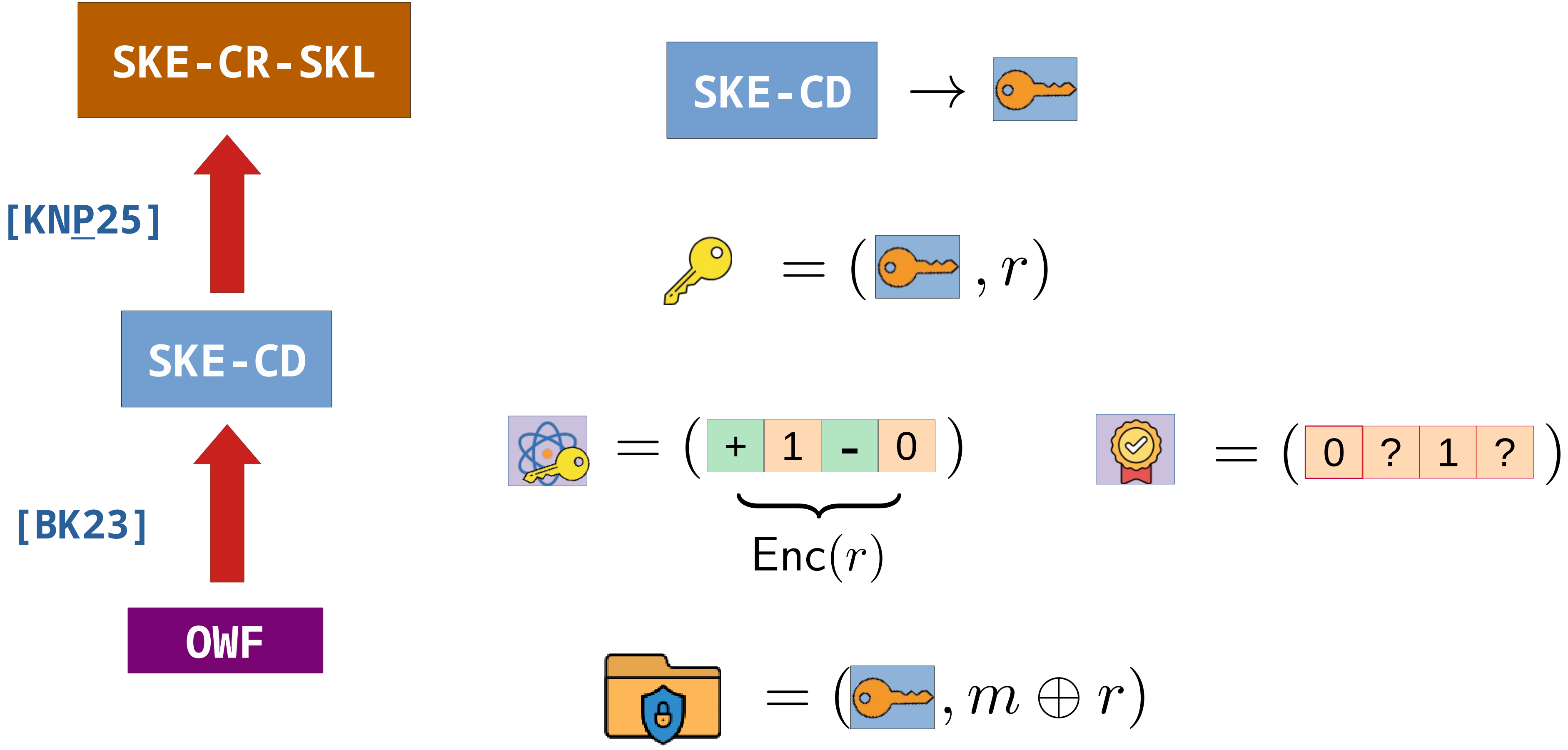




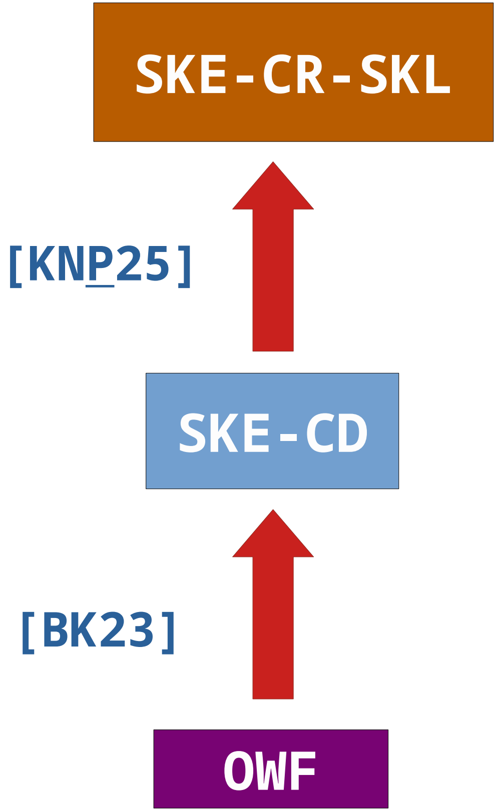
Constructing SKE-CR-SKL

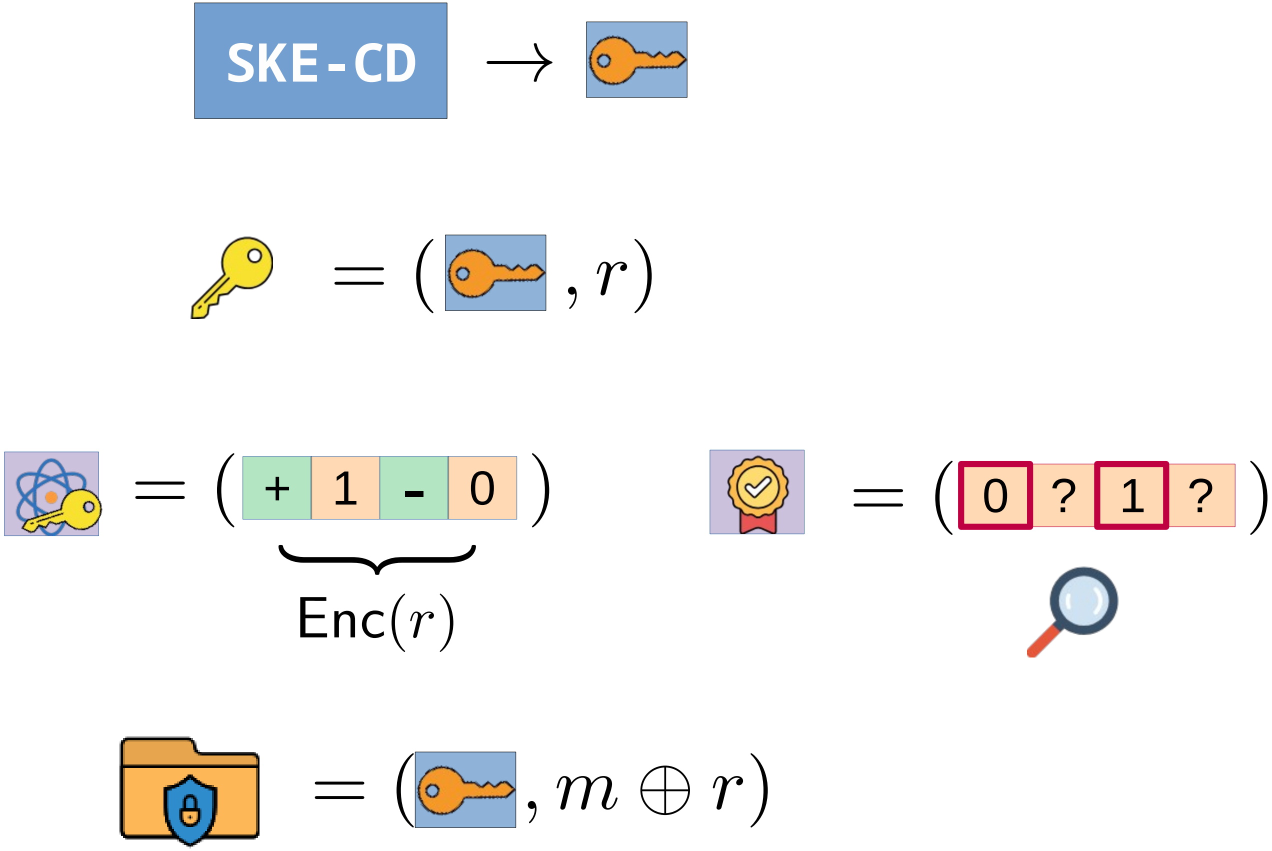


Constructing SKE-CR-SKL



Constructing SKE-CR-SKL





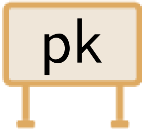
Building Block: ABE

Attribute Based Encryption

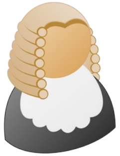
[GPS+06]

Building Block: ABE

Attribute Based Encryption



[GPS+06]

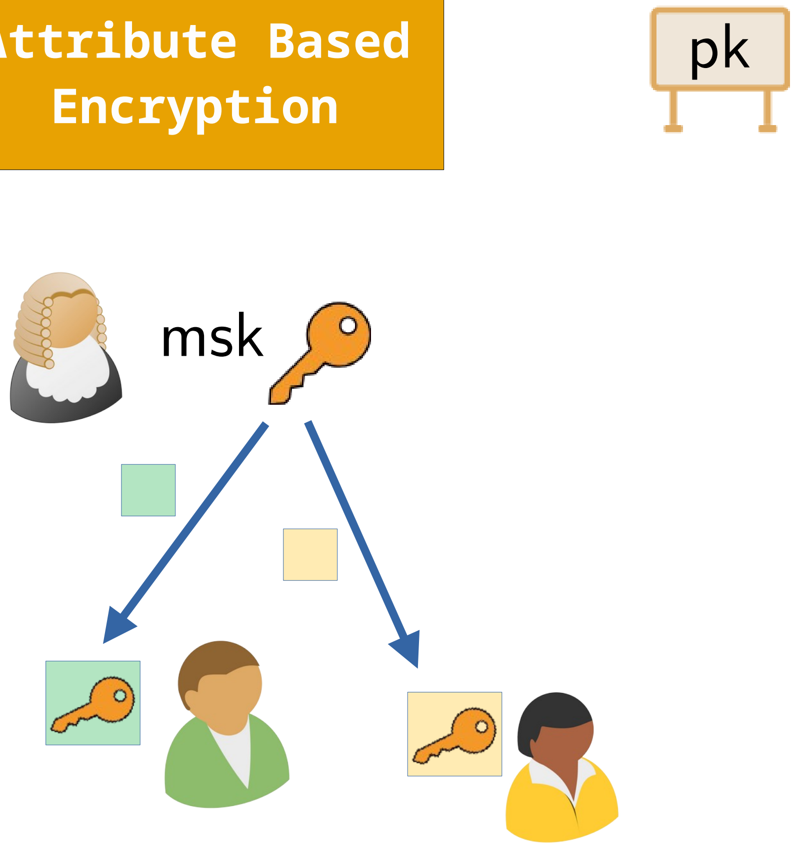


msk

Building Block: ABE

Attribute Based Encryption

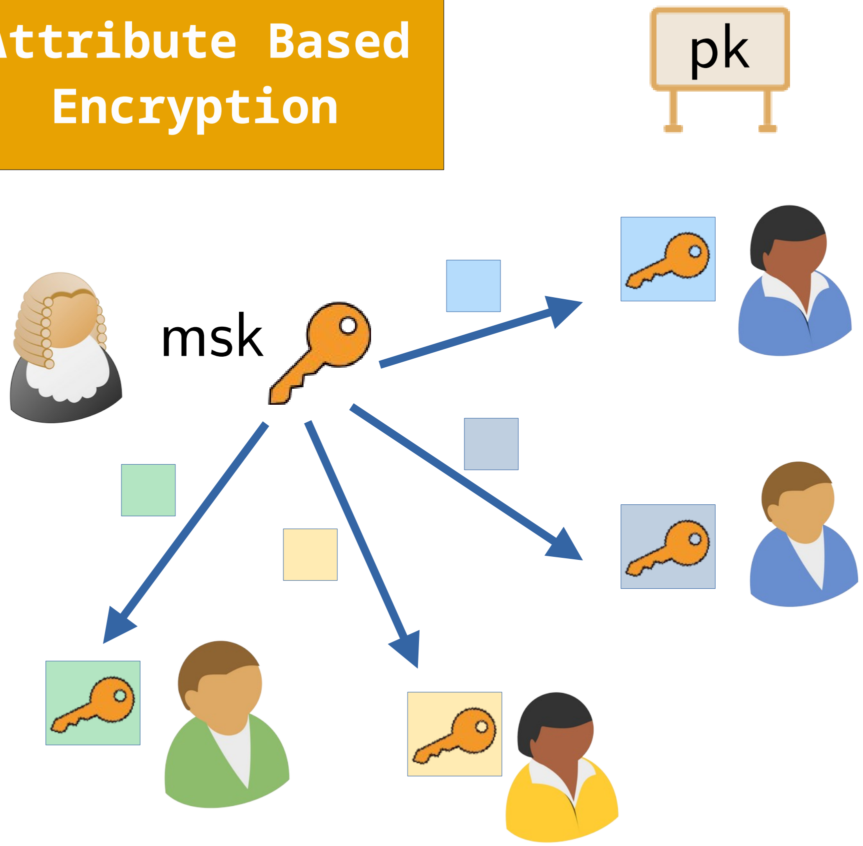
[GPS+06]



Building Block: ABE

Attribute Based Encryption

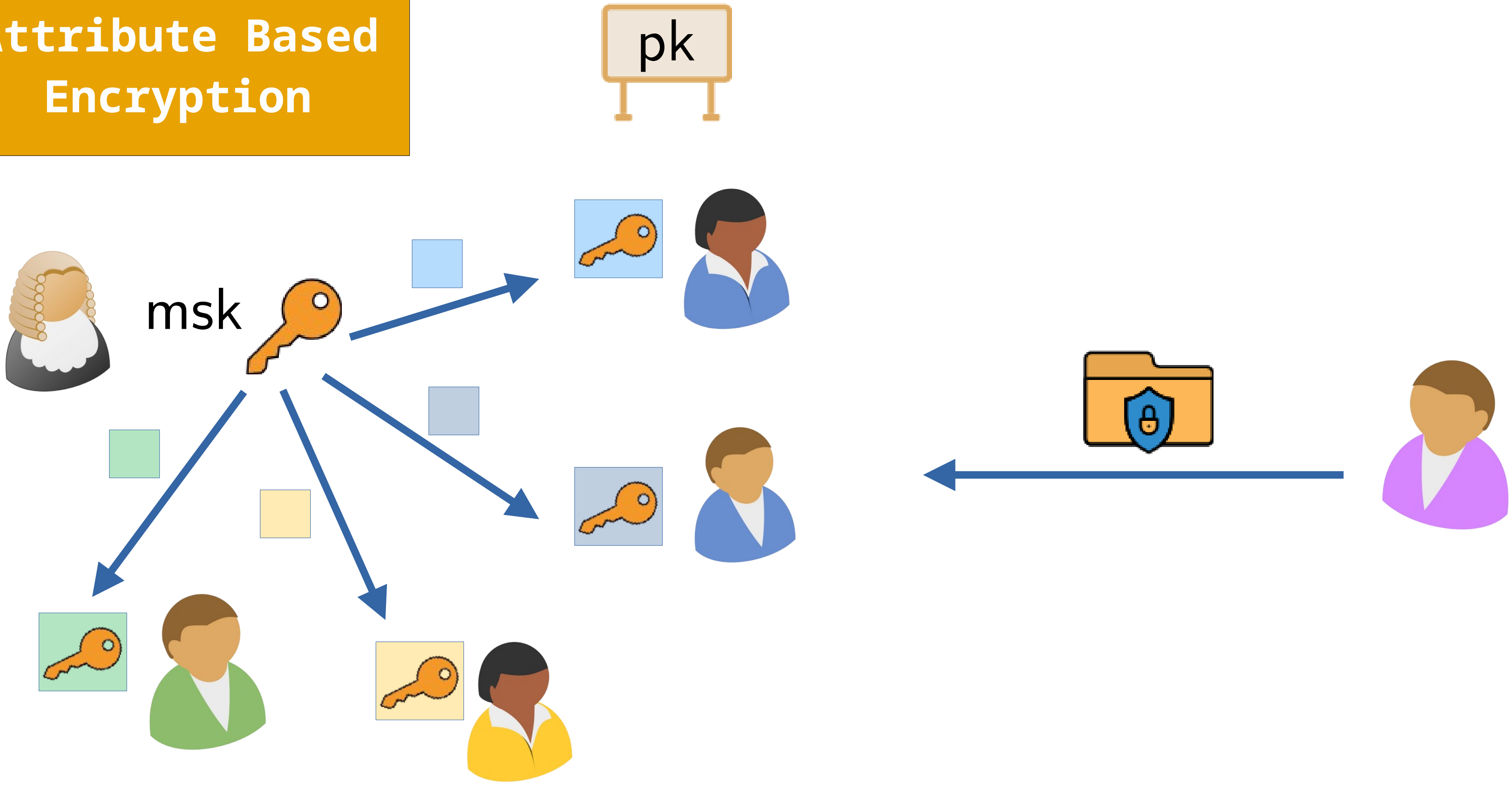
[GPS+06]



Building Block: ABE

Attribute Based Encryption

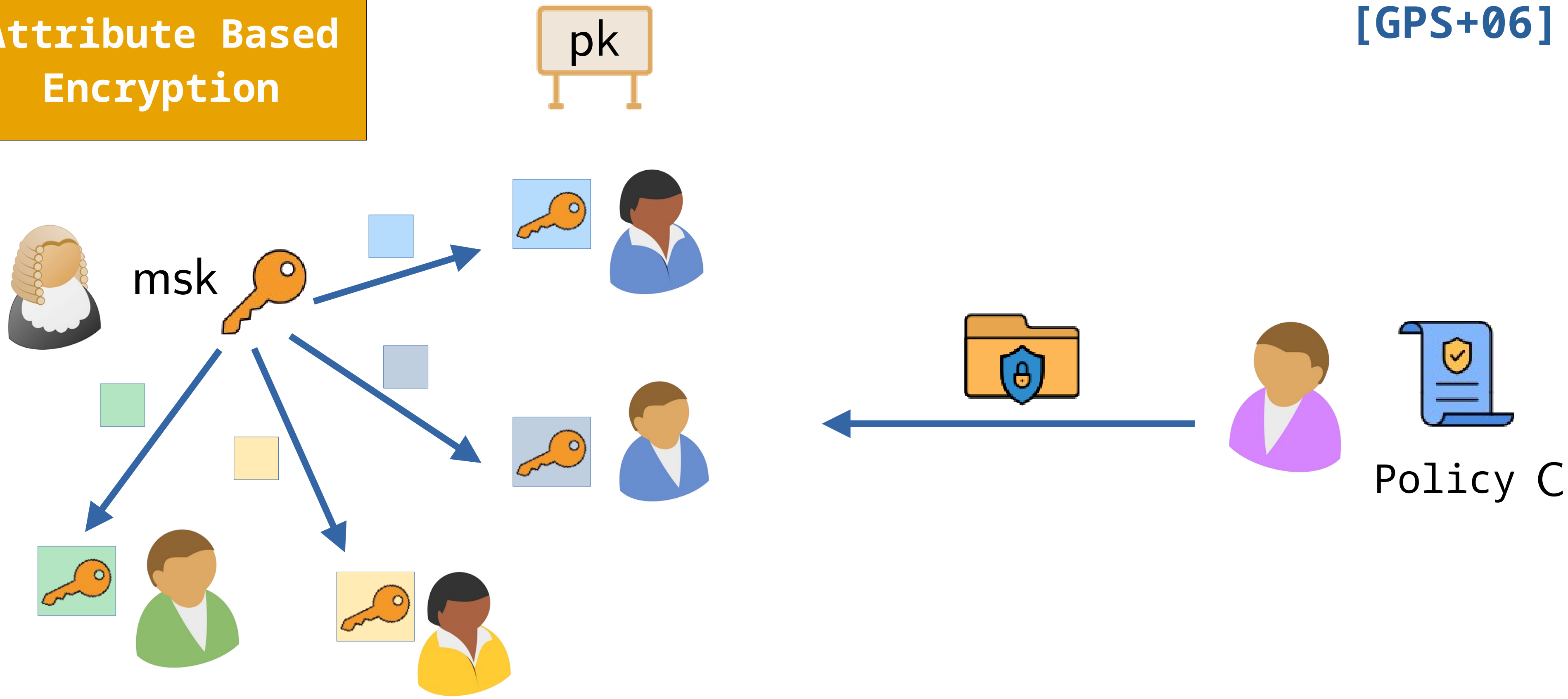
[GPS+06]



Building Block: ABE

Attribute Based Encryption

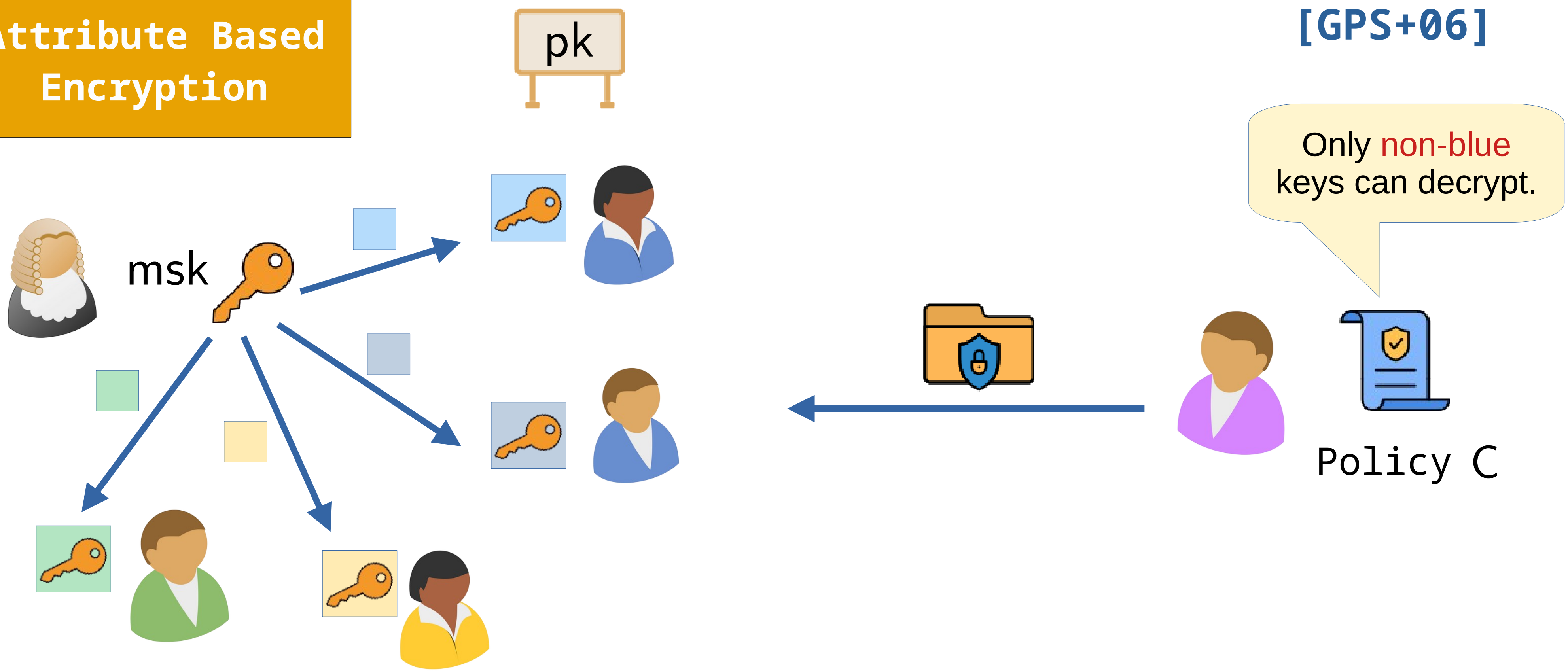
[GPS+06]



Building Block: ABE

Attribute Based Encryption

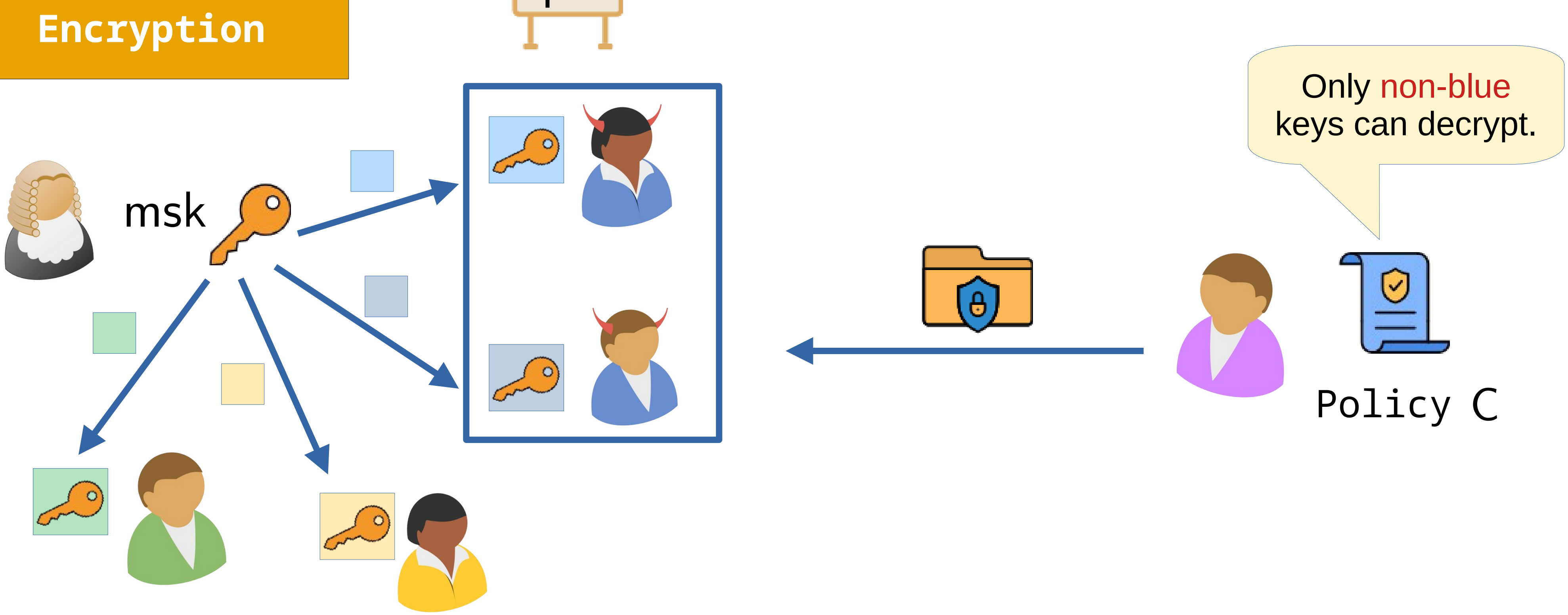
[GPS+06]



Building Block: ABE

Attribute Based Encryption

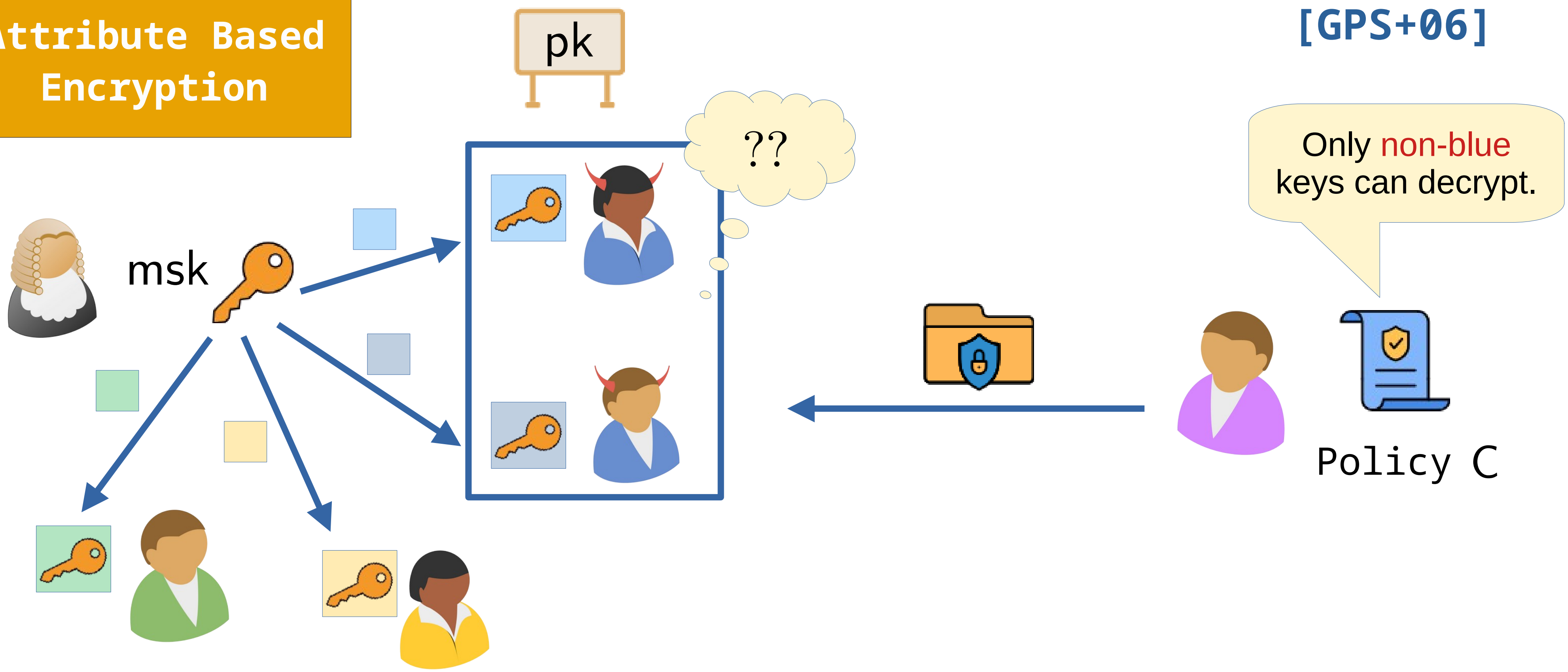
[GPS+06]



Building Block: ABE

Attribute Based Encryption

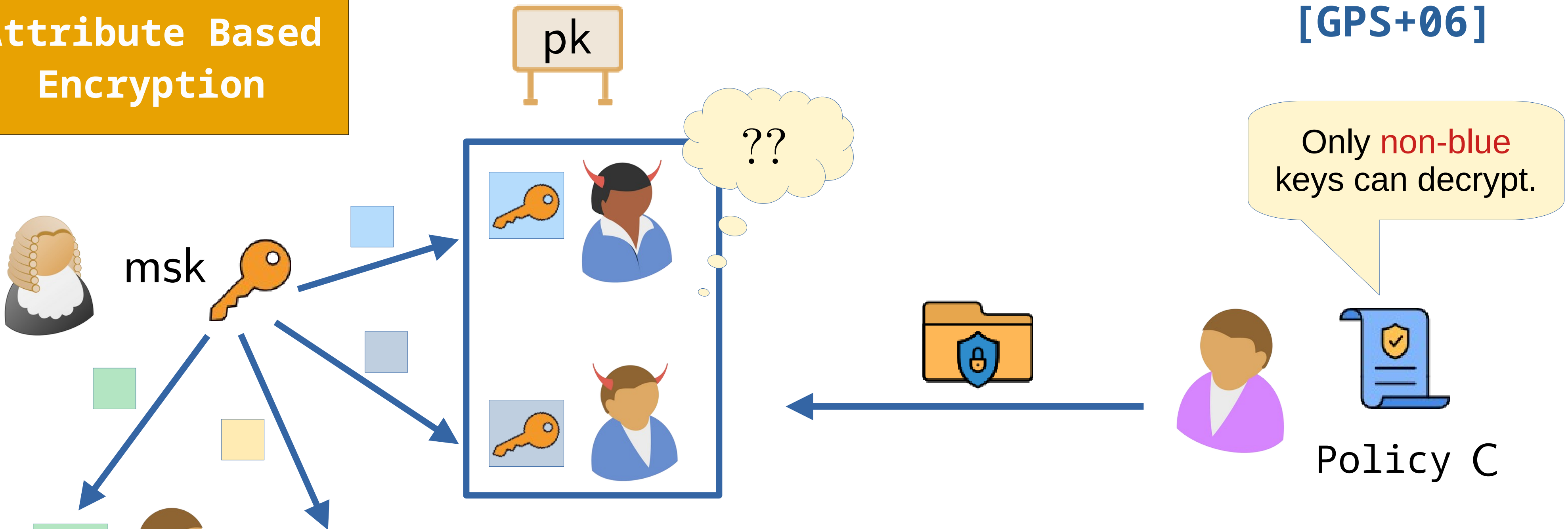
[GPS+06]



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

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

SKE-CR-SKL

Main Idea: Part I

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

SKE-CR-SKL

Classical Decryption Property

$$\mathsf{CDec}(\mathsf{ske.ct}, \square) = \mathsf{CDec}(\mathsf{ske.ct}, \square) = \ldots = \mathsf{CDec}(\mathsf{ske.ct}, \square) = \mathsf{m}$$

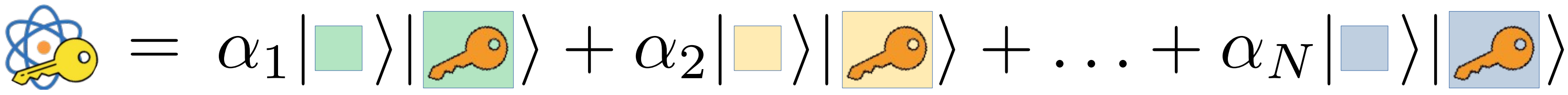
Main Idea: Part I

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

SKE-CR-SKL

Classical Decryption Property

$$\mathsf{CDec}(\mathsf{ske.ct}, \square) = \mathsf{CDec}(\mathsf{ske.ct}, \square) = \ldots = \mathsf{CDec}(\mathsf{ske.ct}, \square) = \mathsf{m}$$



PKE-CR-SKL

Main Idea: Part I

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

SKE-CR-SKL

Classical Decryption Property

$$\mathsf{CDec}(\mathsf{ske.ct}, \square) = \mathsf{CDec}(\mathsf{ske.ct}, \square) = \ldots = \mathsf{CDec}(\mathsf{ske.ct}, \square) = \mathsf{m}$$

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

PKE-CR-SKL

ABE Secret-Key

Main Idea: Part I

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

SKE-CR-SKL

Classical Decryption Property

$$\text{CDec}(\text{ske.ct}, \square) = \text{CDec}(\text{ske.ct}, \square) = \ldots = \text{CDec}(\text{ske.ct}, \square) = \text{m}$$

$$= \alpha_1|\square\rangle|\square\rangle + \alpha_2|\square\rangle|\square\rangle + \ldots + \alpha_N|\square\rangle\underbrace{|\square\rangle}_{\text{ABE Secret-Key}}$$

PKE-CR-SKL

Main Idea: Part I

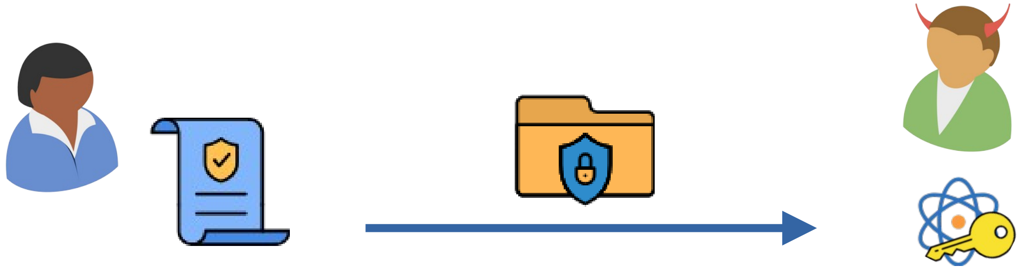
$\mathsf{ske.dk} = \alpha_1|\square\rangle + \alpha_2|\square\rangle + \ldots + \alpha_N|\square\rangle$ **SKE-CR-SKL**

Classical Decryption Property

$\mathsf{CDec}(\mathsf{ske.ct}, \square) = \mathsf{CDec}(\mathsf{ske.ct}, \square) = \ldots = \mathsf{CDec}(\mathsf{ske.ct}, \square) = \mathsf{m}$

 $= \alpha_1|\square\rangle|\square\rangle + \alpha_2|\square\rangle|\square\rangle + \ldots + \alpha_N|\square\rangle|\square\rangle$ **PKE-CR-SKL**

ABE Secret-Key



Main Idea: Part I

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

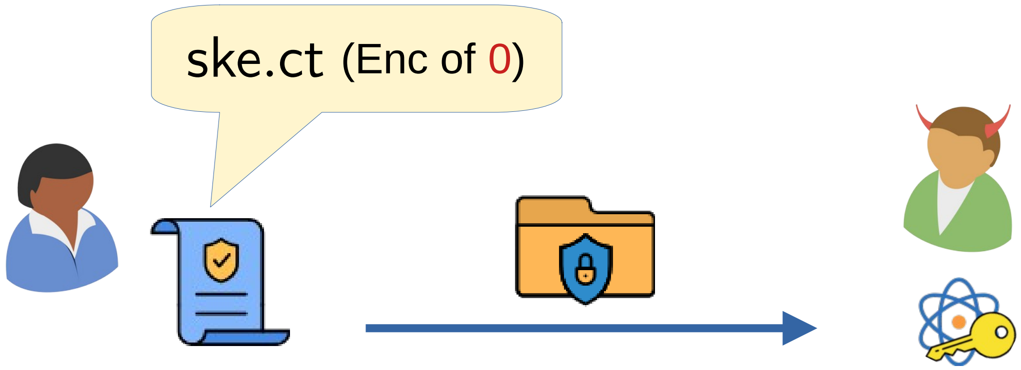
SKE-CR-SKL

<u>Classical Decryption Property</u>

$$\mathsf{CDec}(\mathsf{ske.ct}, \square) = \mathsf{CDec}(\mathsf{ske.ct}, \square) = \ldots = \mathsf{CDec}(\mathsf{ske.ct}, \square) = \mathsf{m}$$

$$= \alpha_1|\square\rangle|\square\rangle + \alpha_2|\square\rangle|\square\rangle + \ldots + \alpha_N|\square\rangle|\underbrace{\square}_{\text{ABE Secret-Key}}\rangle$$

PKE-CR-SKL



Main Idea: Part I

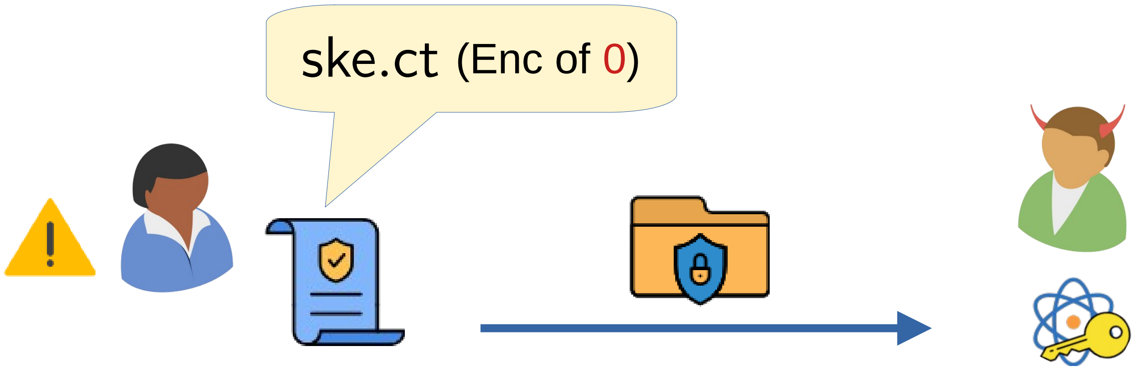
$\mathsf{ske.dk} = \alpha_1|\square\rangle + \alpha_2|\square\rangle + \ldots + \alpha_N|\square\rangle$ **SKE-CR-SKL**

<u>Classical Decryption Property</u>

$\mathsf{CDec}(\mathsf{ske.ct}, \square) = \mathsf{CDec}(\mathsf{ske.ct}, \square) = \ldots = \mathsf{CDec}(\mathsf{ske.ct}, \square) = \mathsf{m}$

 $= \alpha_1|\square\rangle|\square\rangle + \alpha_2|\square\rangle|\square\rangle + \ldots + \alpha_N|\square\rangle|\square\rangle$ **PKE-CR-SKL**

ABE Secret-Key



Main Idea: Part I

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

SKE-CR-SKL

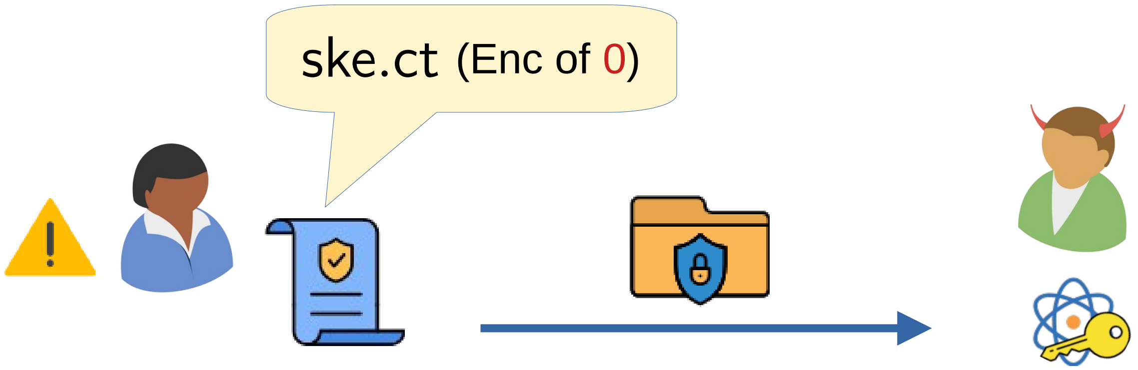
Classical Decryption Property

$$\mathsf{CDec}(\mathsf{ske.ct}, \square) = \mathsf{CDec}(\mathsf{ske.ct}, \square) = \ldots = \mathsf{CDec}(\mathsf{ske.ct}, \square) = \mathsf{m}$$

$$= \alpha_1|\square\rangle|\text{key}\rangle + \alpha_2|\square\rangle|\text{key}\rangle + \ldots + \alpha_N|\square\rangle|\text{key}\rangle$$

PKE-CR-SKL

ABE Secret-Key

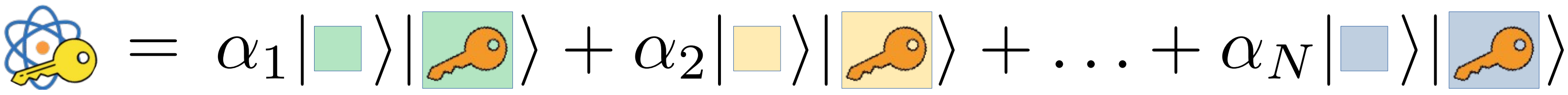


satisfies policy if:

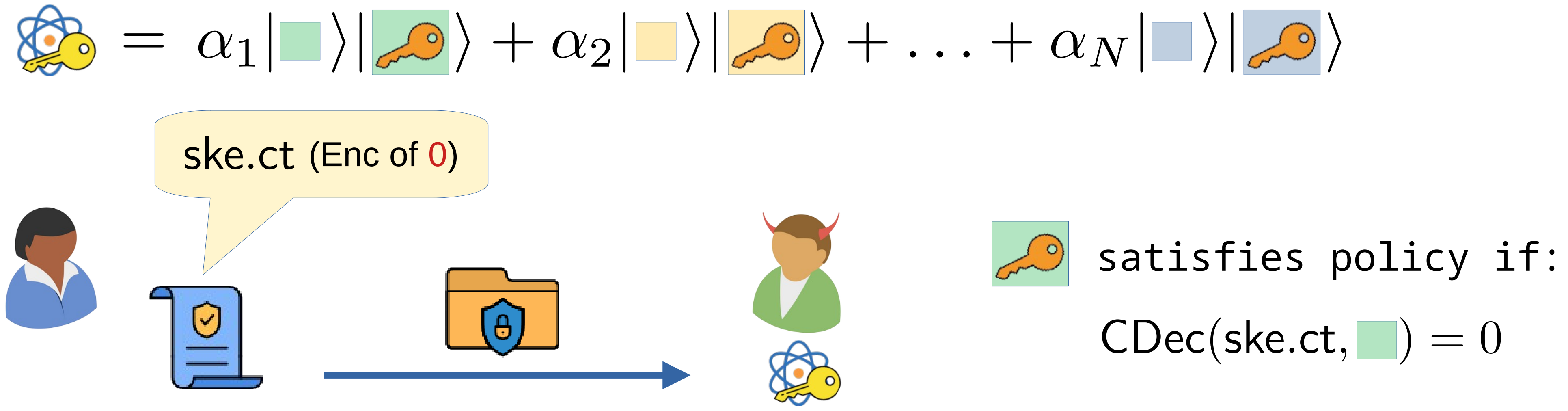
$$\mathsf{CDec}(\mathsf{ske.ct}, \square) = 0$$

Main Idea: Part II

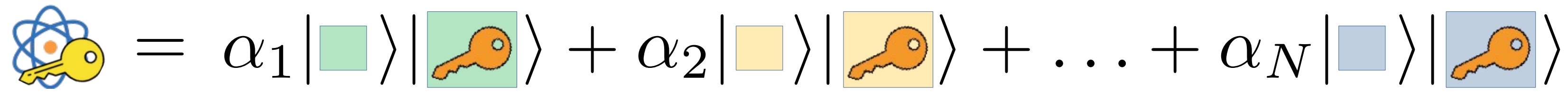
Main Idea: Part II

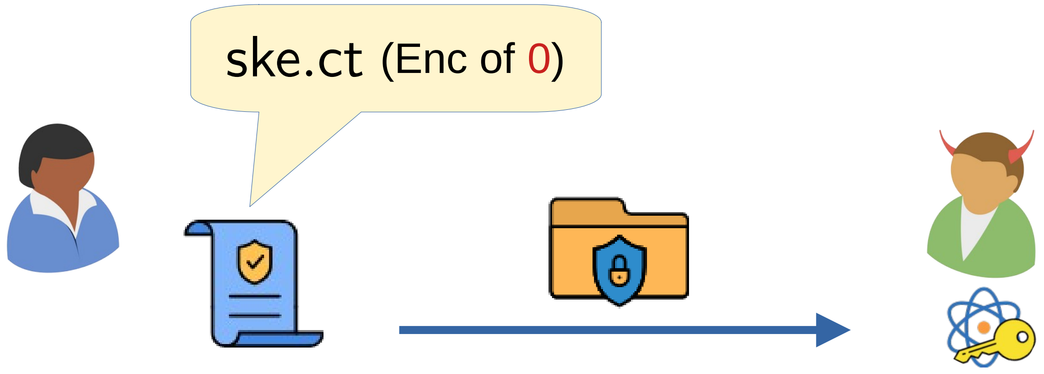


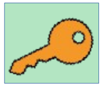
Main Idea: Part II



Main Idea: Part II

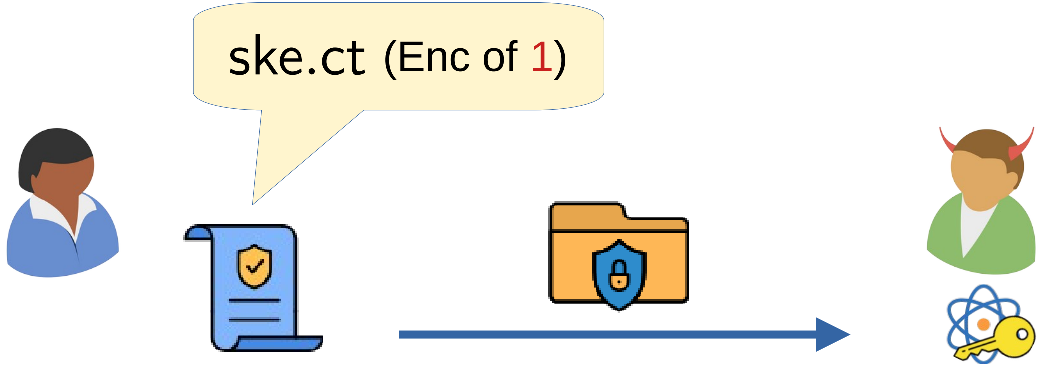




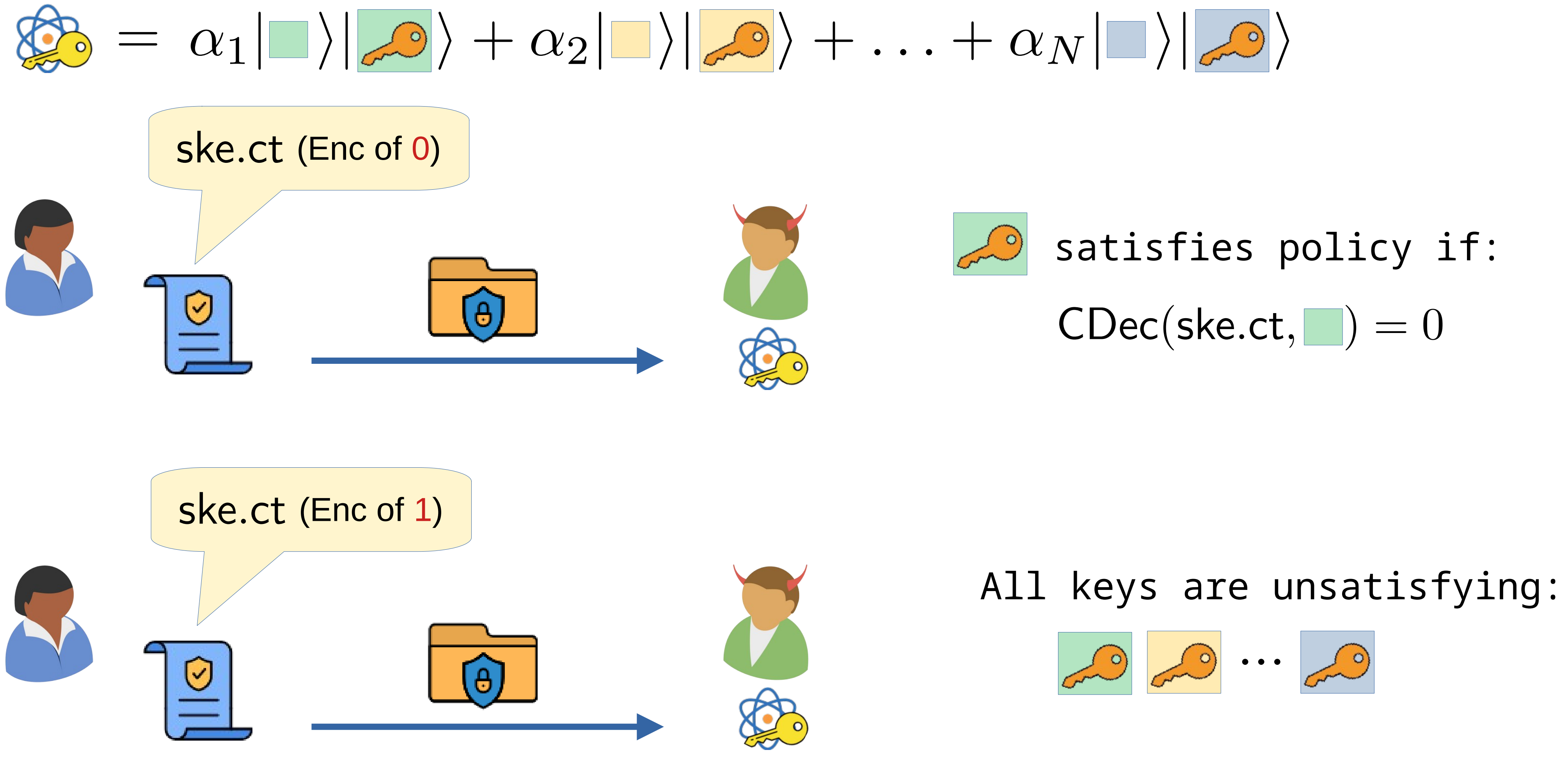


satisfies policy if:

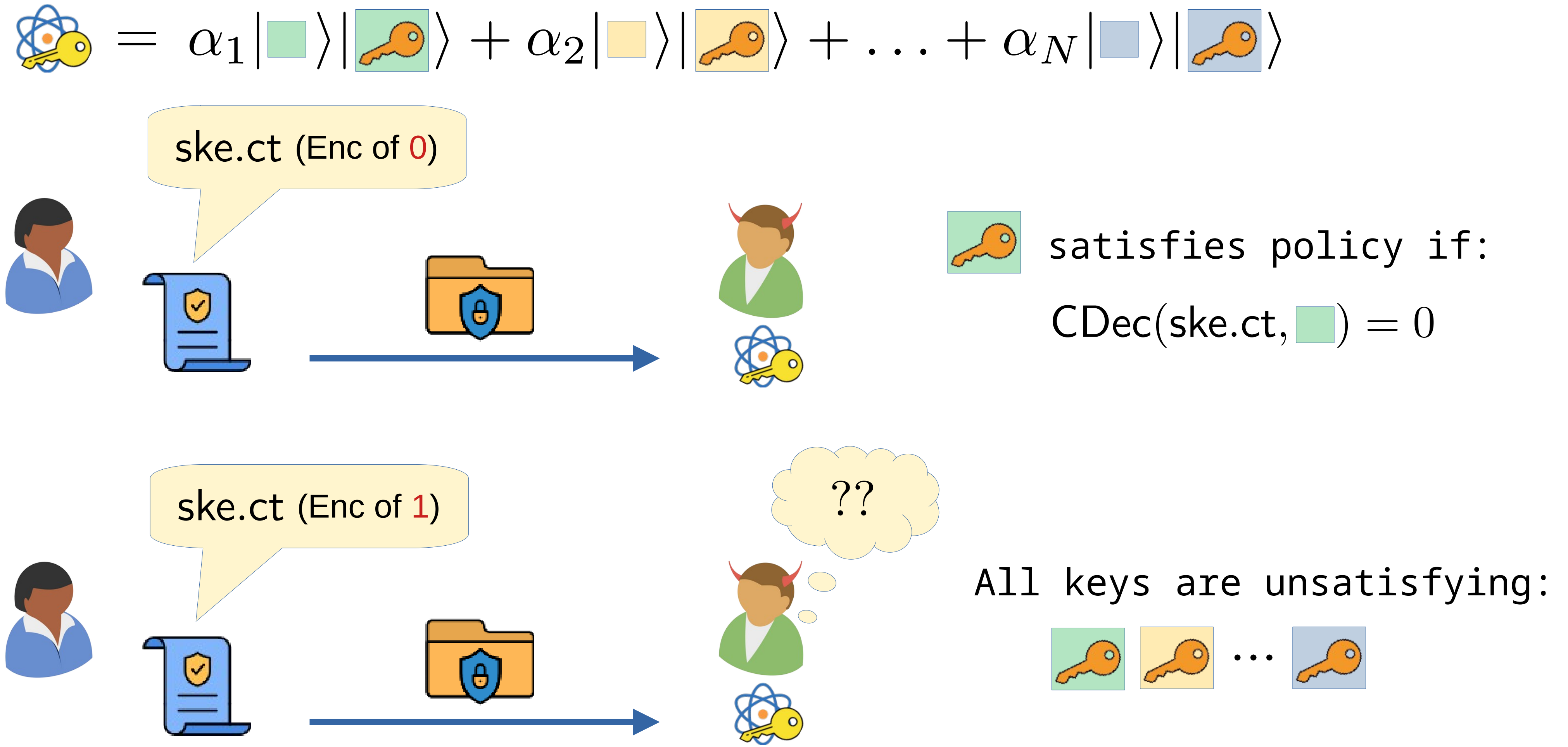
$\mathsf{CDec}(\mathsf{ske.ct}, \square) = 0$



Main Idea: Part II

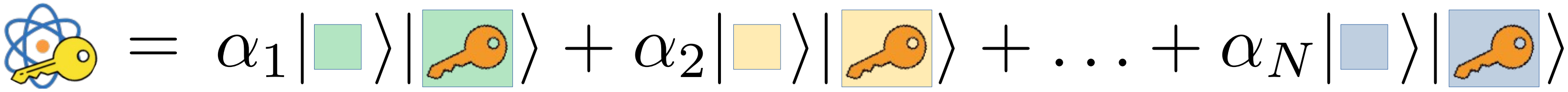


Main Idea: Part II

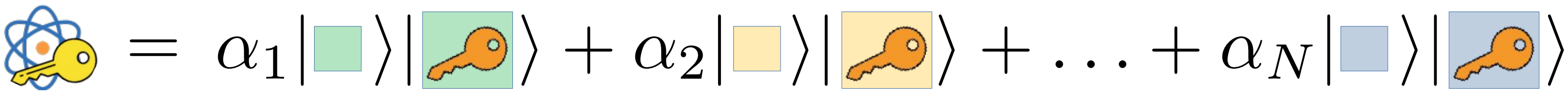


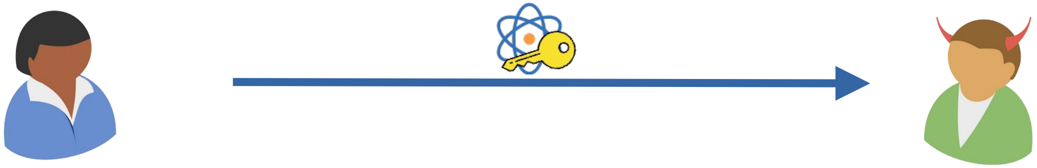
Main Idea: Part III

Main Idea: Part III

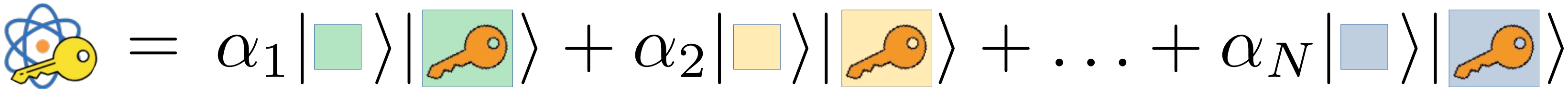


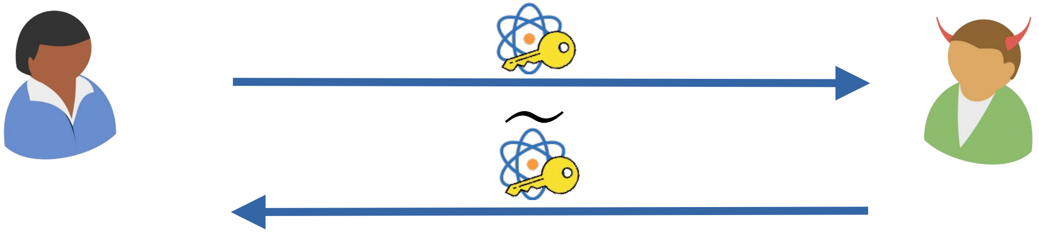
Main Idea: Part III



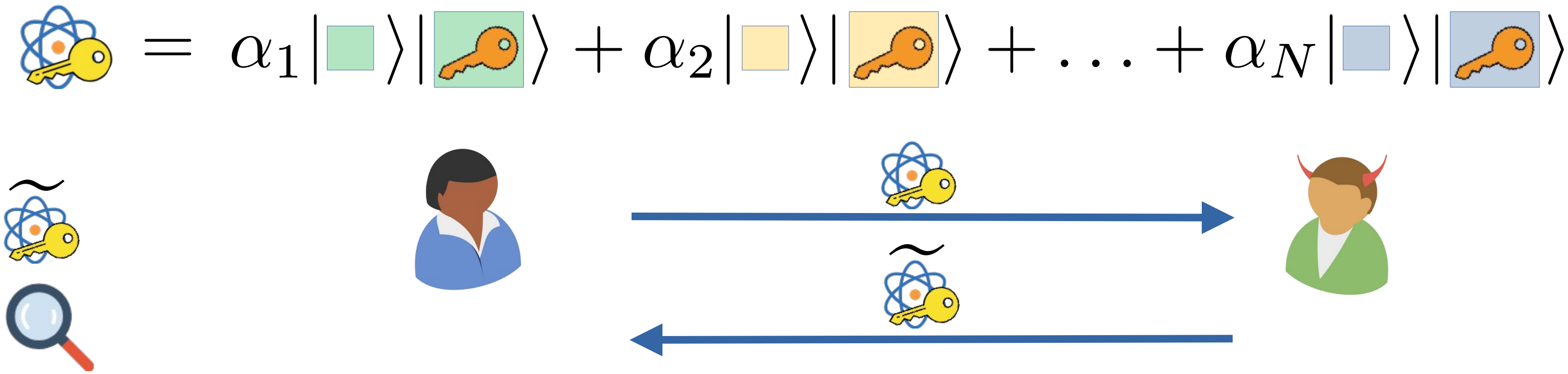


Main Idea: Part III

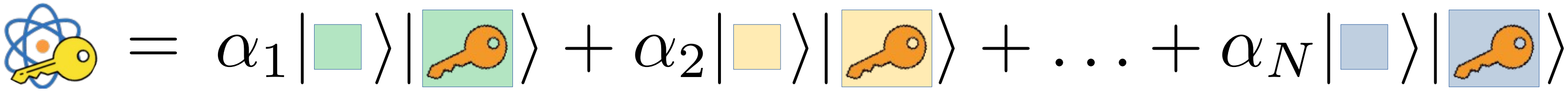


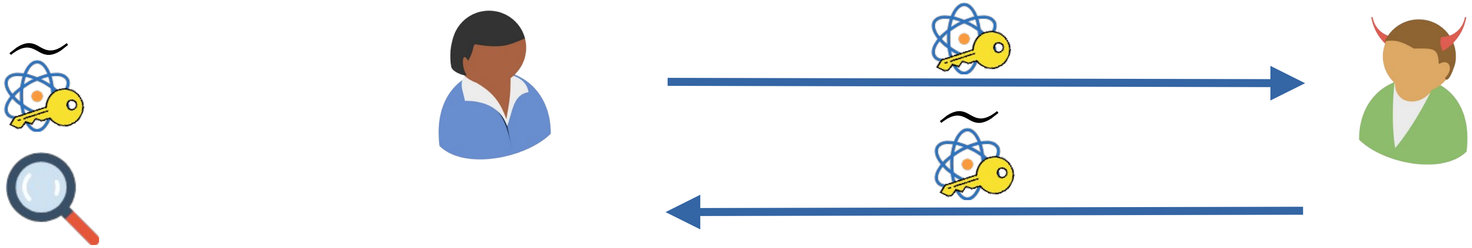


Main Idea: Part III

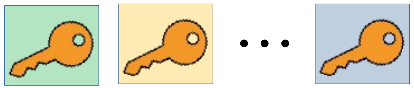


Main Idea: Part III

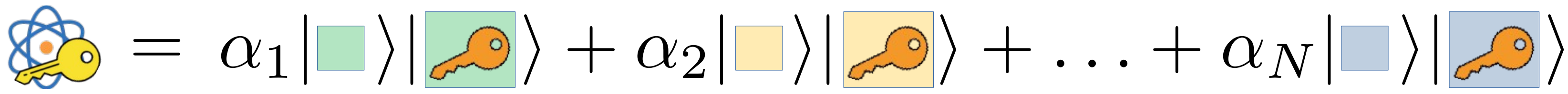


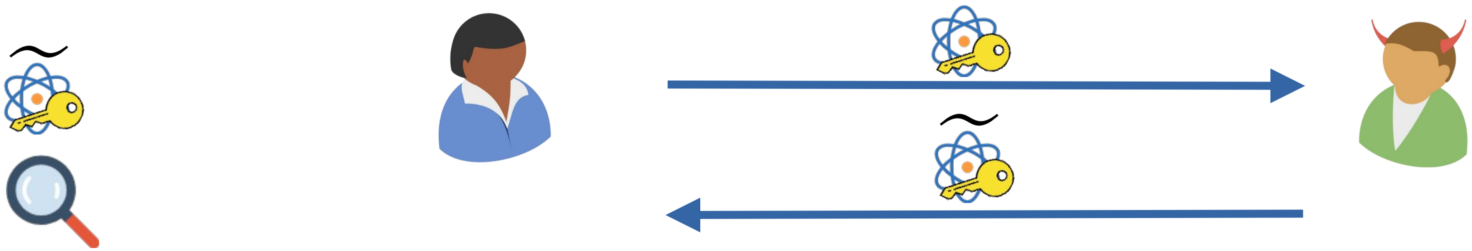


1. Uncompute ABE keys

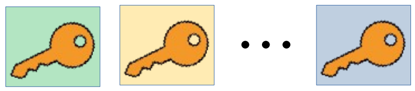


Main Idea: Part III



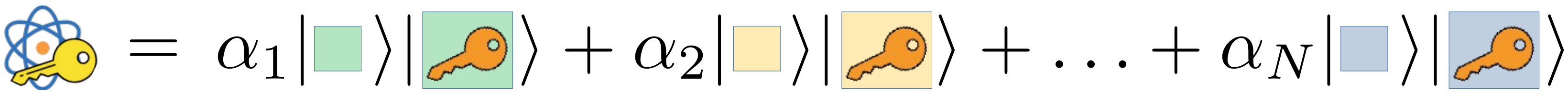


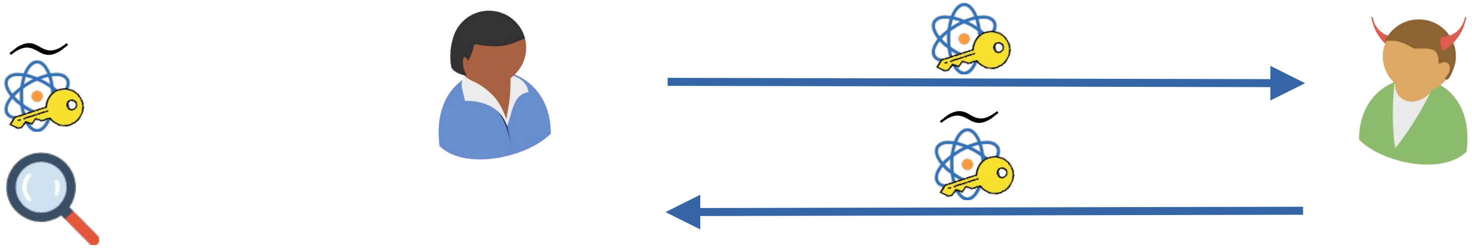
1. Uncompute ABE keys



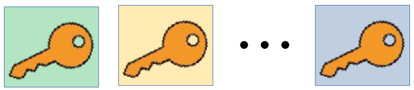
2. Verify $\mathsf{ske}.\widetilde{\mathsf{dk}}$.

Main Idea: Part III

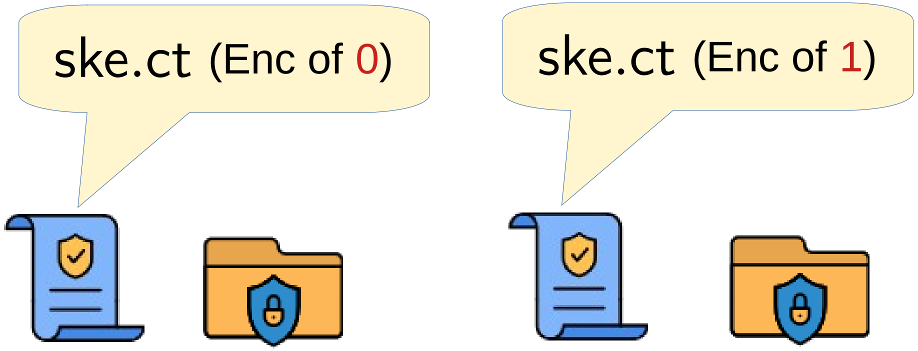




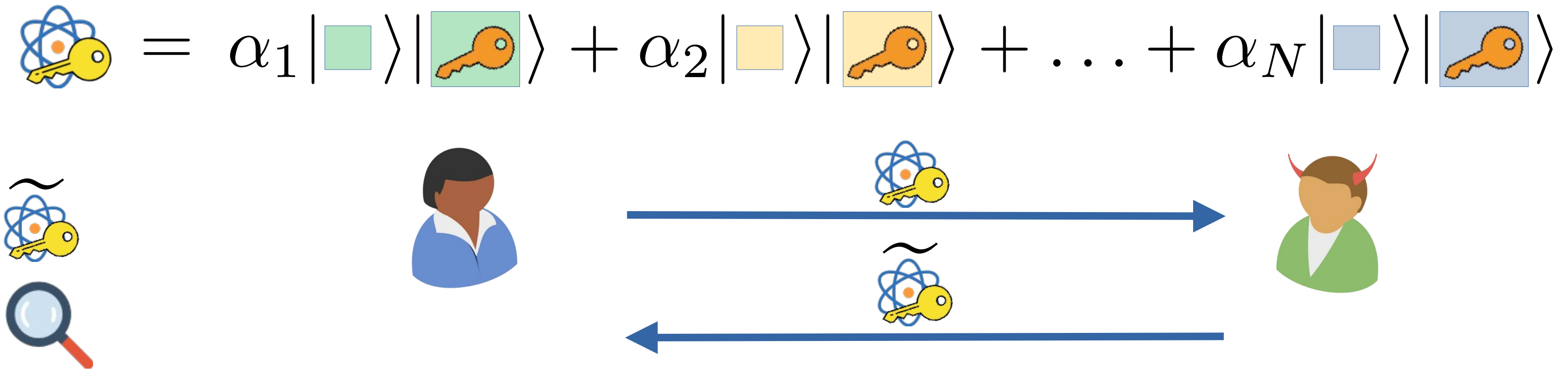
1. Uncompute ABE keys



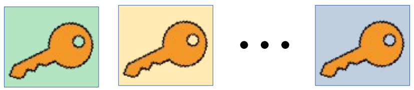
2. Verify ske.$\widetilde{\text{dk}}$.



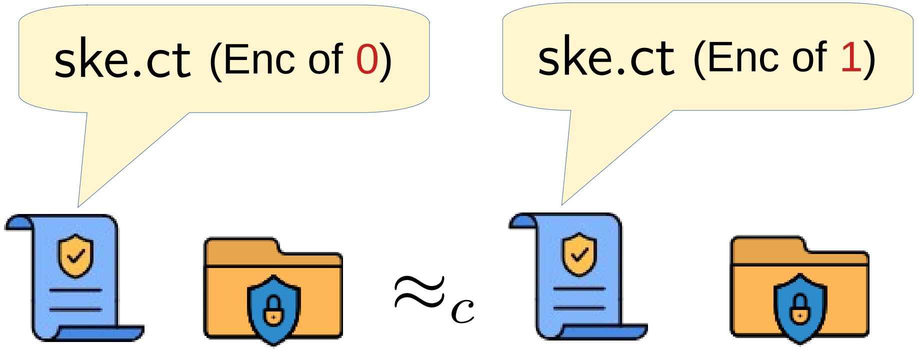
Main Idea: Part III



1. Uncompute ABE keys

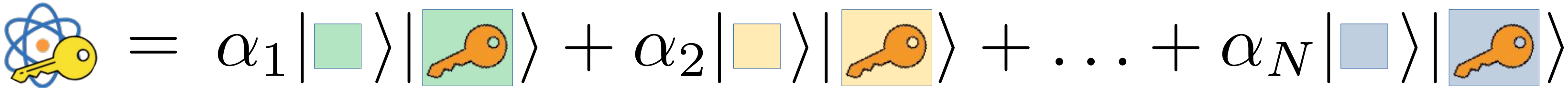


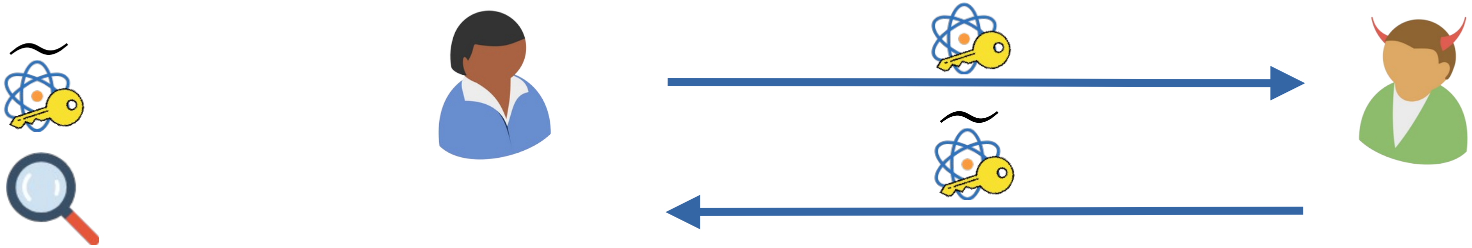
2. Verify $\widetilde{\text{ske.dk}}$.



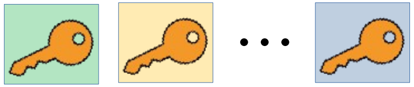
SKE-CR-SKL

Main Idea: Part III

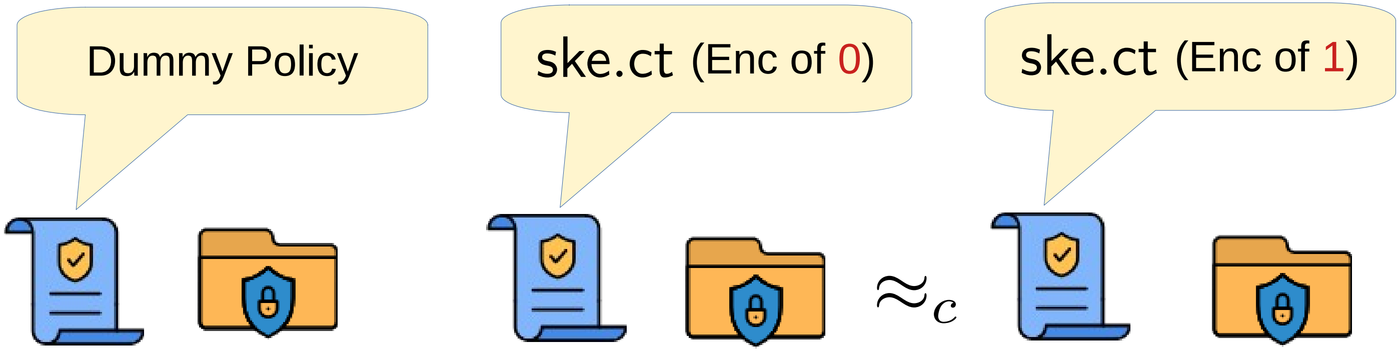




1. Uncompute ABE keys

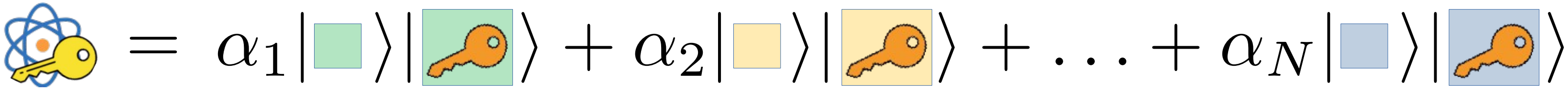


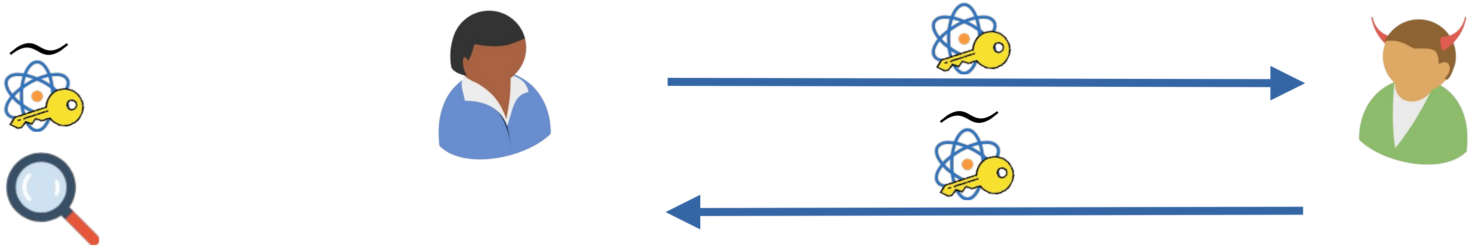
2. Verify $\widetilde{\text{ske.dk}}$.



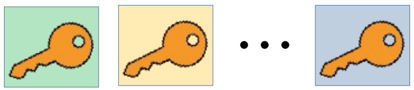
SKE-CR-SKL

Main Idea: Part III

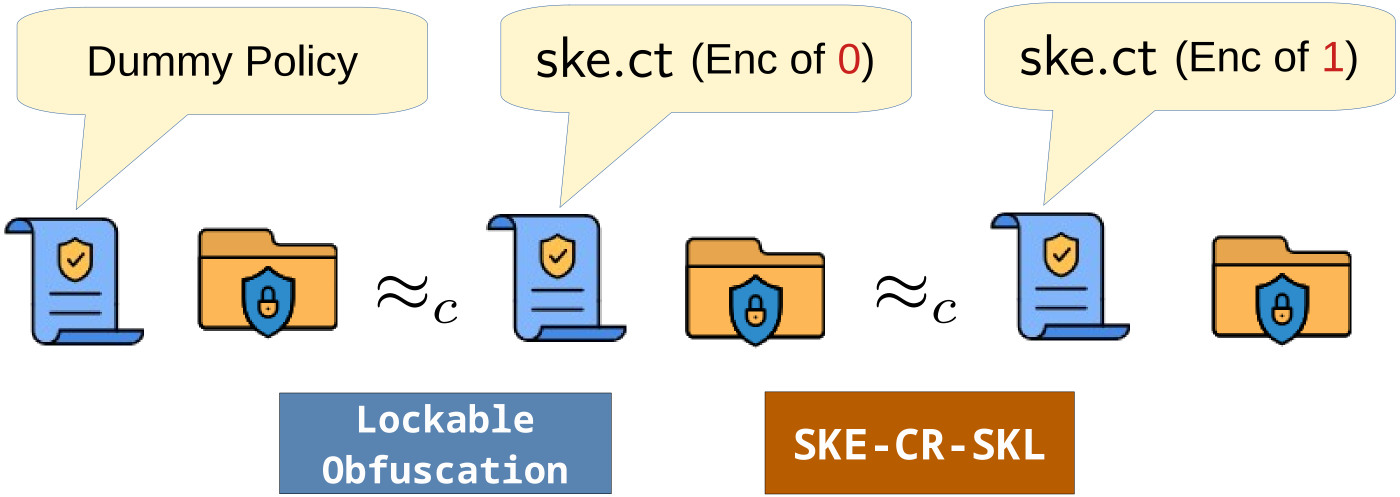




1. Uncompute ABE keys



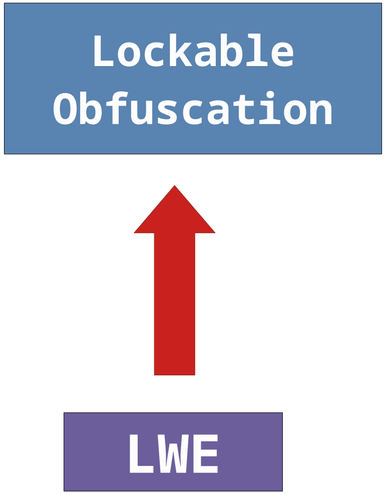
2. Verify $\widetilde{\text{ske.dk}}$.



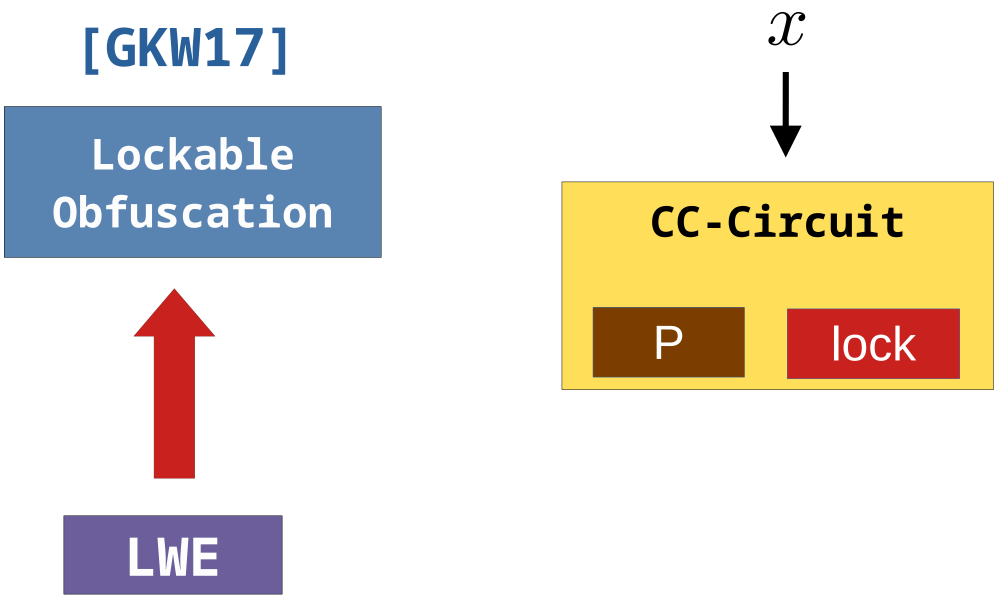
Main Idea: Part IV

Main Idea: Part IV

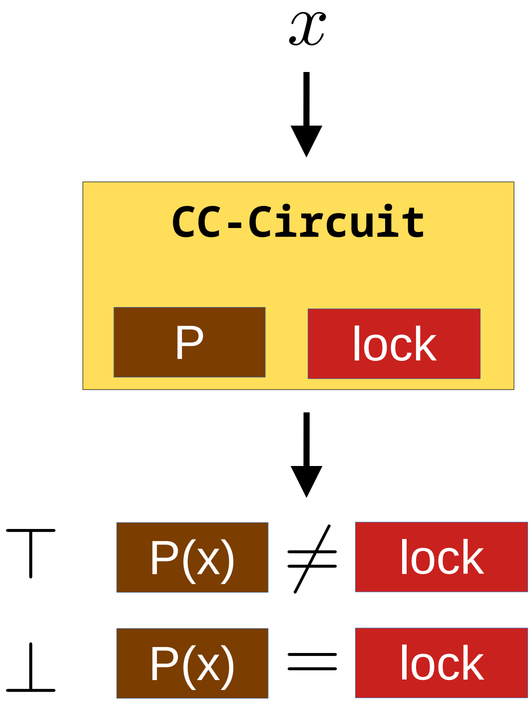
[GKW17]



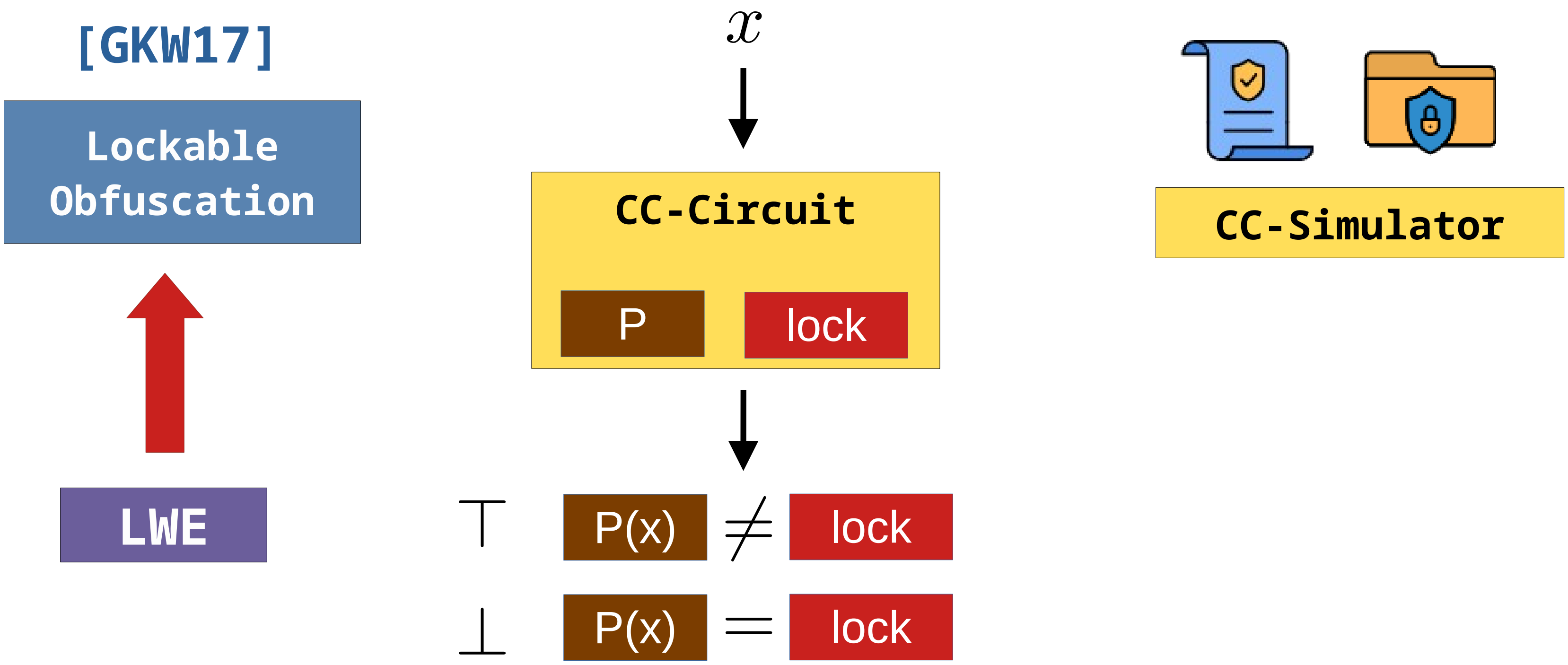
Main Idea: Part IV



Main Idea: Part IV



Main Idea: Part IV



Main Idea: Part IV

[GKW17]

Lockable Obfuscation

LWE

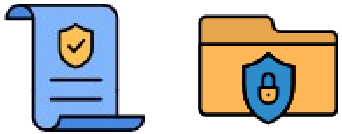
x

CC-Circuit

P lock

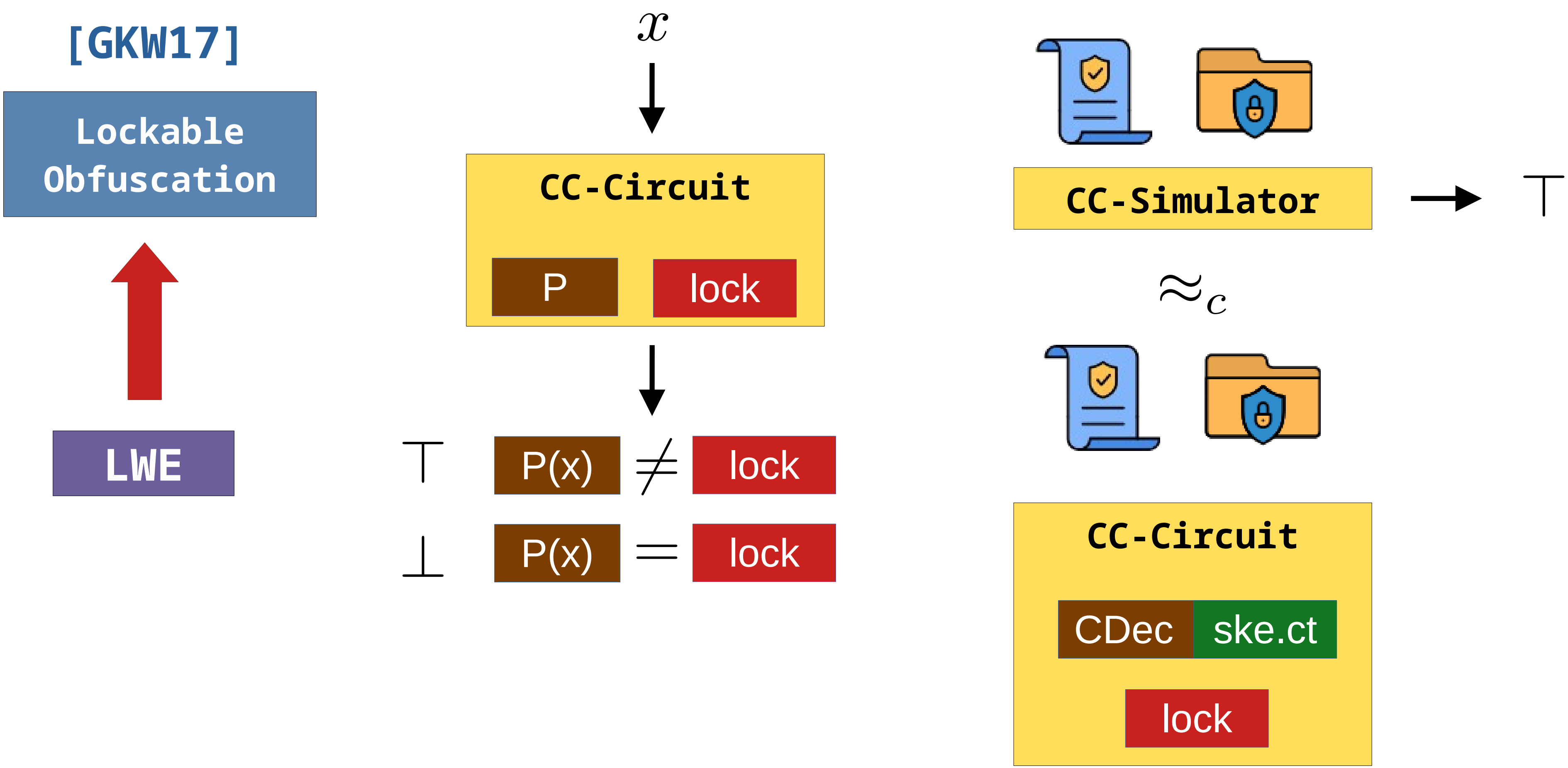
$\top$ P(x) $\neq$ lock

$\bot$ P(x) $=$ lock

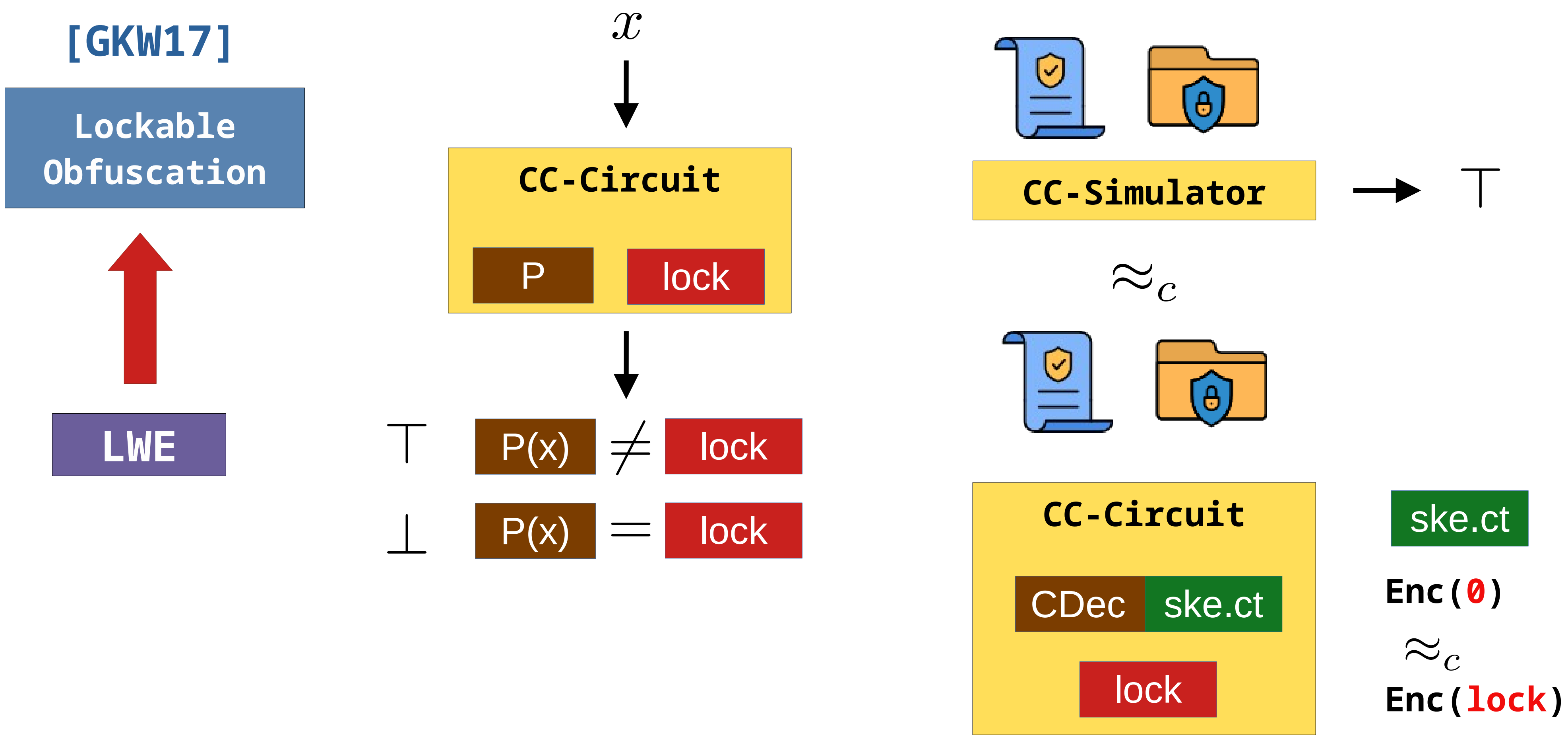


CC-Simulator $\rightarrow$ $\top$

Main Idea: Part IV



Main Idea: Part IV



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.

References

- **[Aar09]:** Aaronson, Scott. "Quantum copy-protection and quantum money." 2009 24th Annual IEEE Conference on Computational Complexity. IEEE, 2009.
- **[LLQZ22]:** Liu, Jiahui, et al. "Collusion resistant copy-protection for watermarkable functionalities." Theory of Cryptography Conference. Cham: Springer Nature Switzerland, 2022.
- **[ÇG24]:** Çakan, Alper, and Vipul Goyal. "Unclonable cryptography with unbounded collusions and impossibility of hyperefficient shadow tomography." Theory of Cryptography Conference. Cham: Springer Nature Switzerland, 2024.
- **[BK23]:** Bartusek, James, and Dakshita Khurana. "Cryptography with certified deletion." Annual International Cryptology Conference. Cham: Springer Nature Switzerland, 2023.
- **[GKW17]:** Goyal, Rishab, Venkata Koppula, and Brent Waters. "Lockable obfuscation." 2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS). IEEE, 2017.

Thank You!