

Updatable Policy-Compliant Signatures

Christian Badertscher

IOHK

Monosij Maitra

IIT Kharagpur

Christian Matt

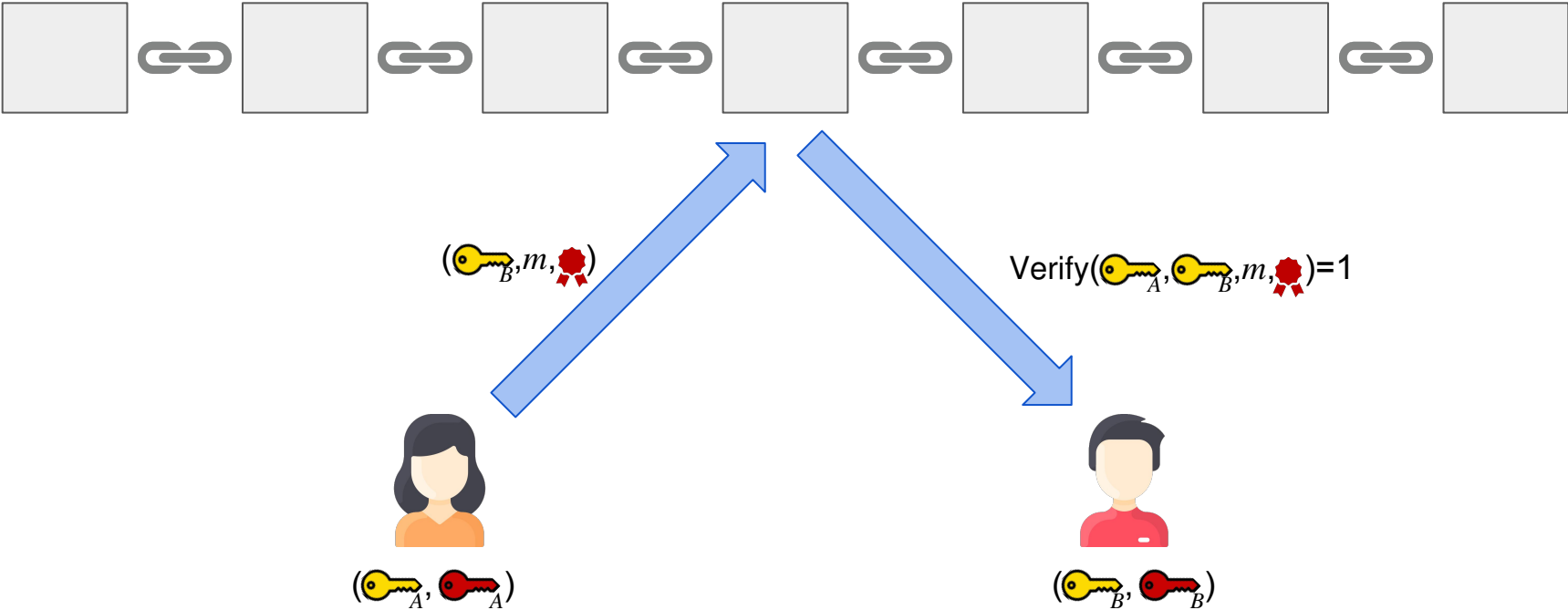
Primev

Hendrik Waldner

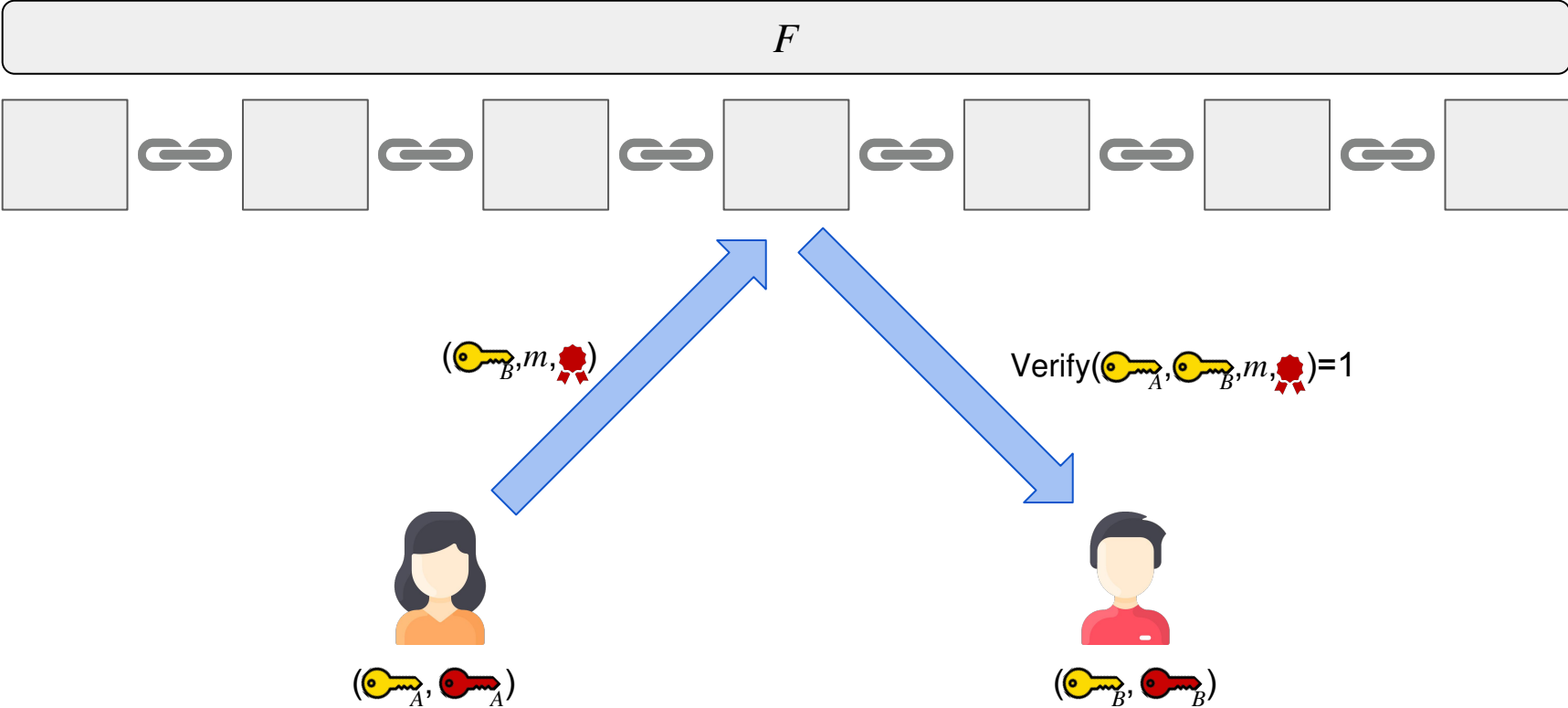
UMD

Motivation

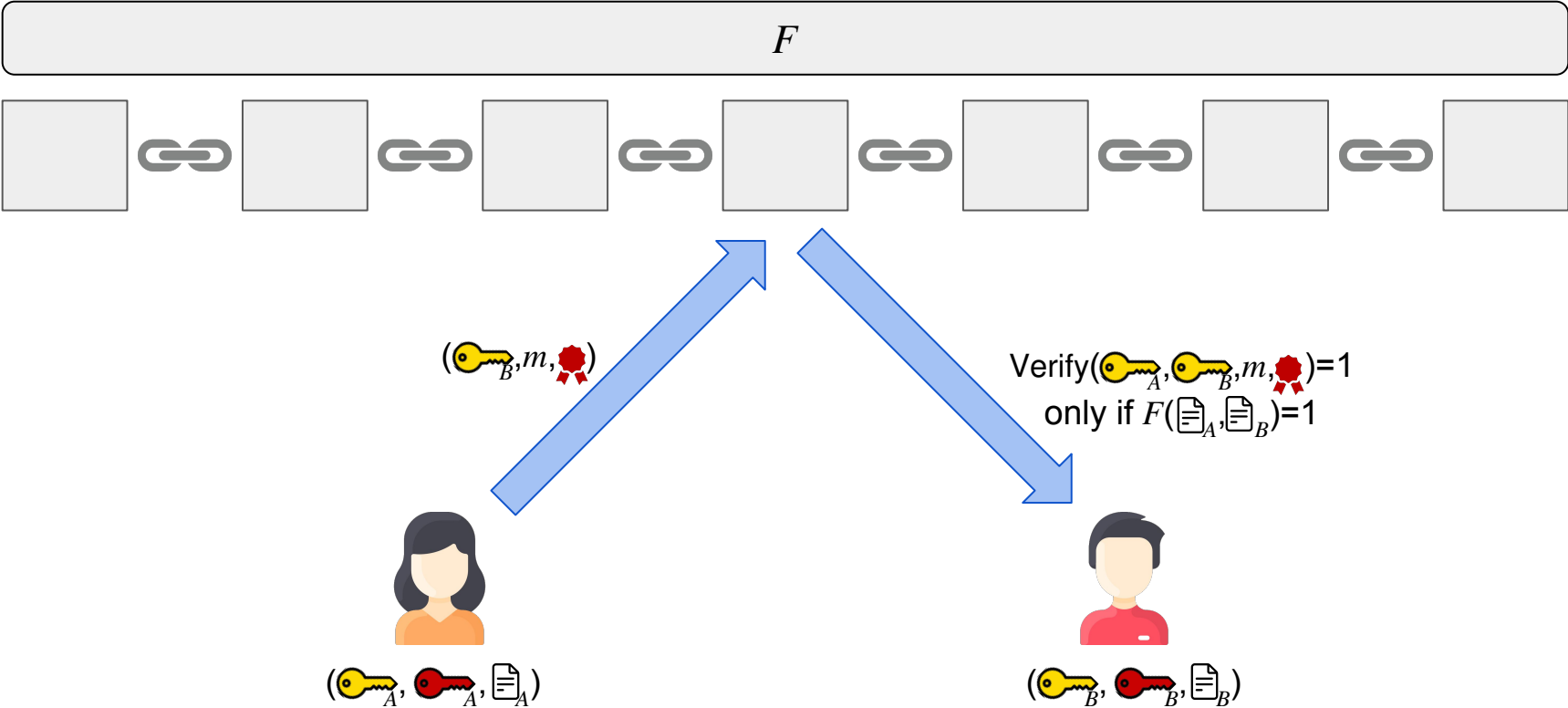
Motivation



Motivation

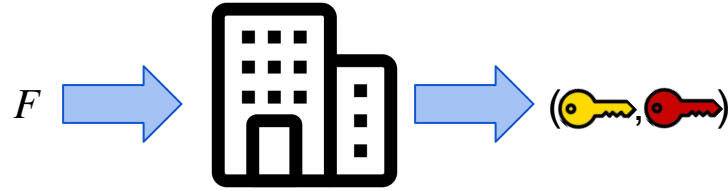


Motivation

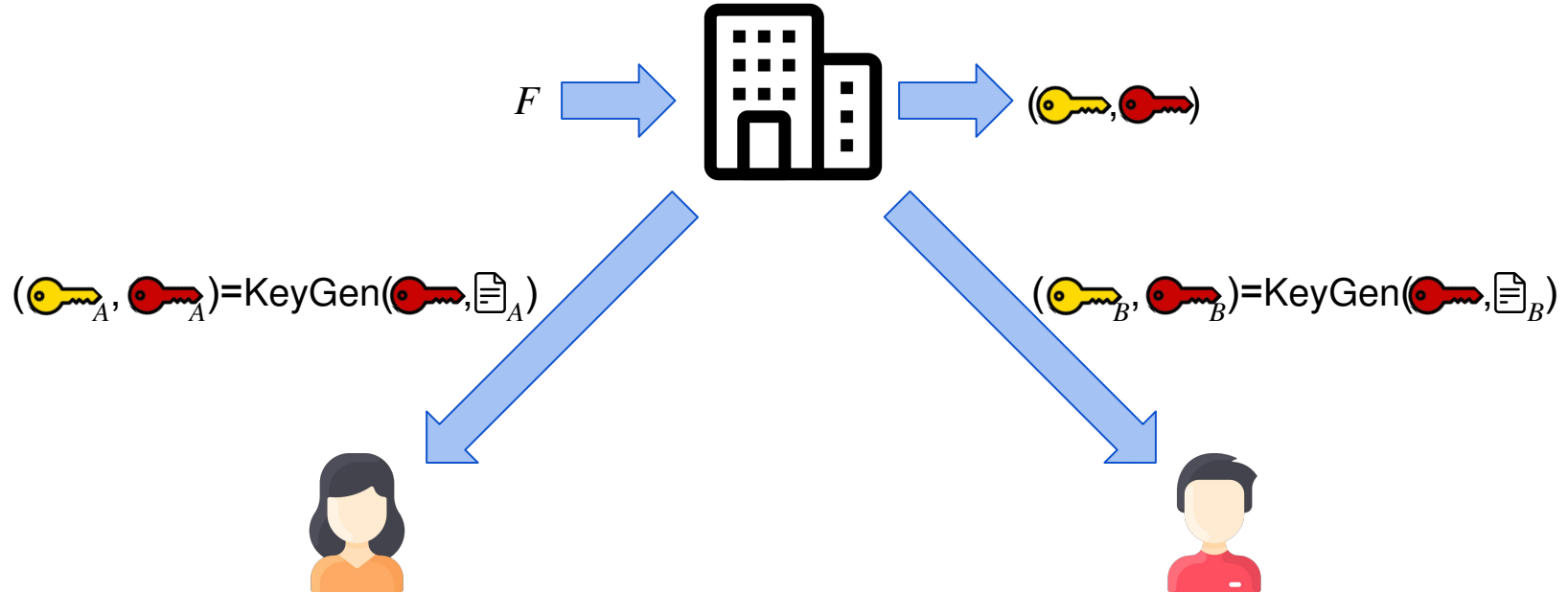


Policy-Compliant Signatures [BMW21]

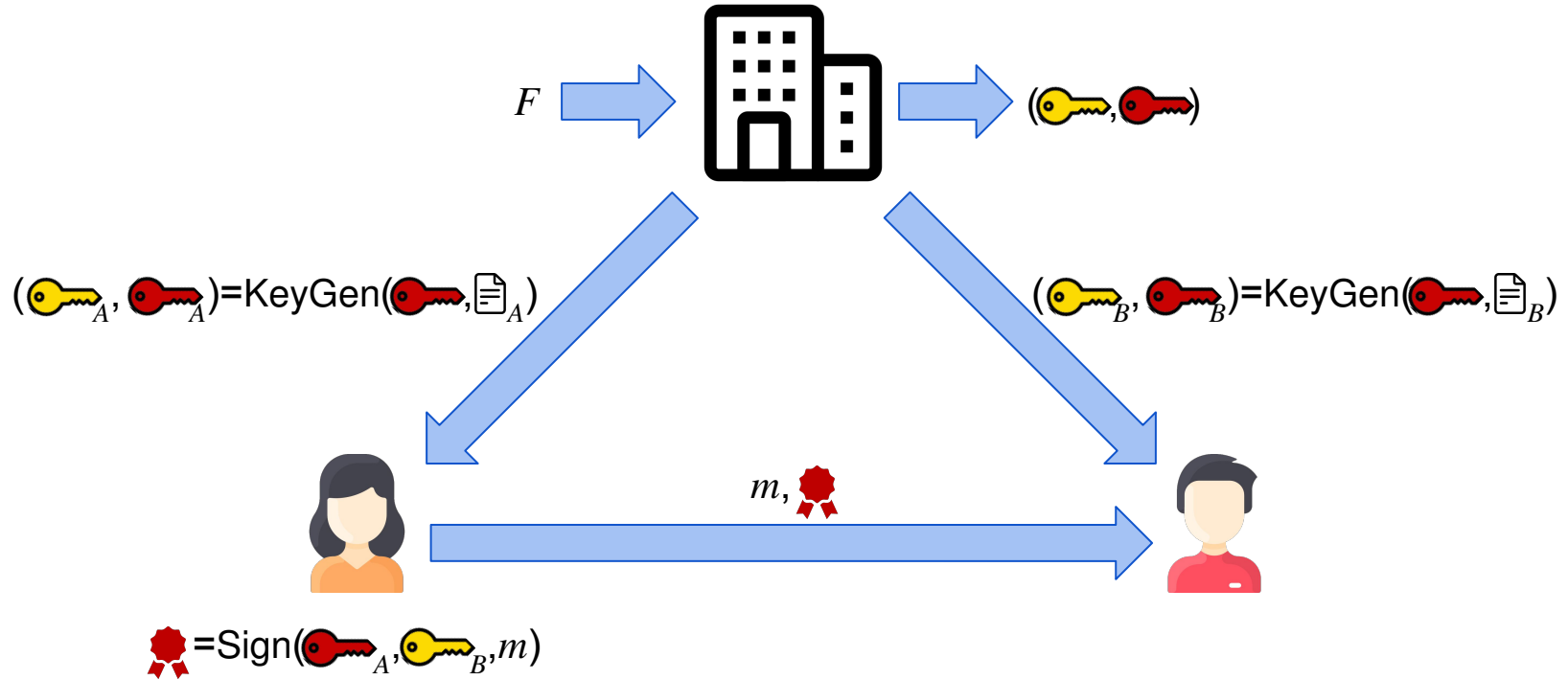
Policy-Compliant Signatures [BMW21]



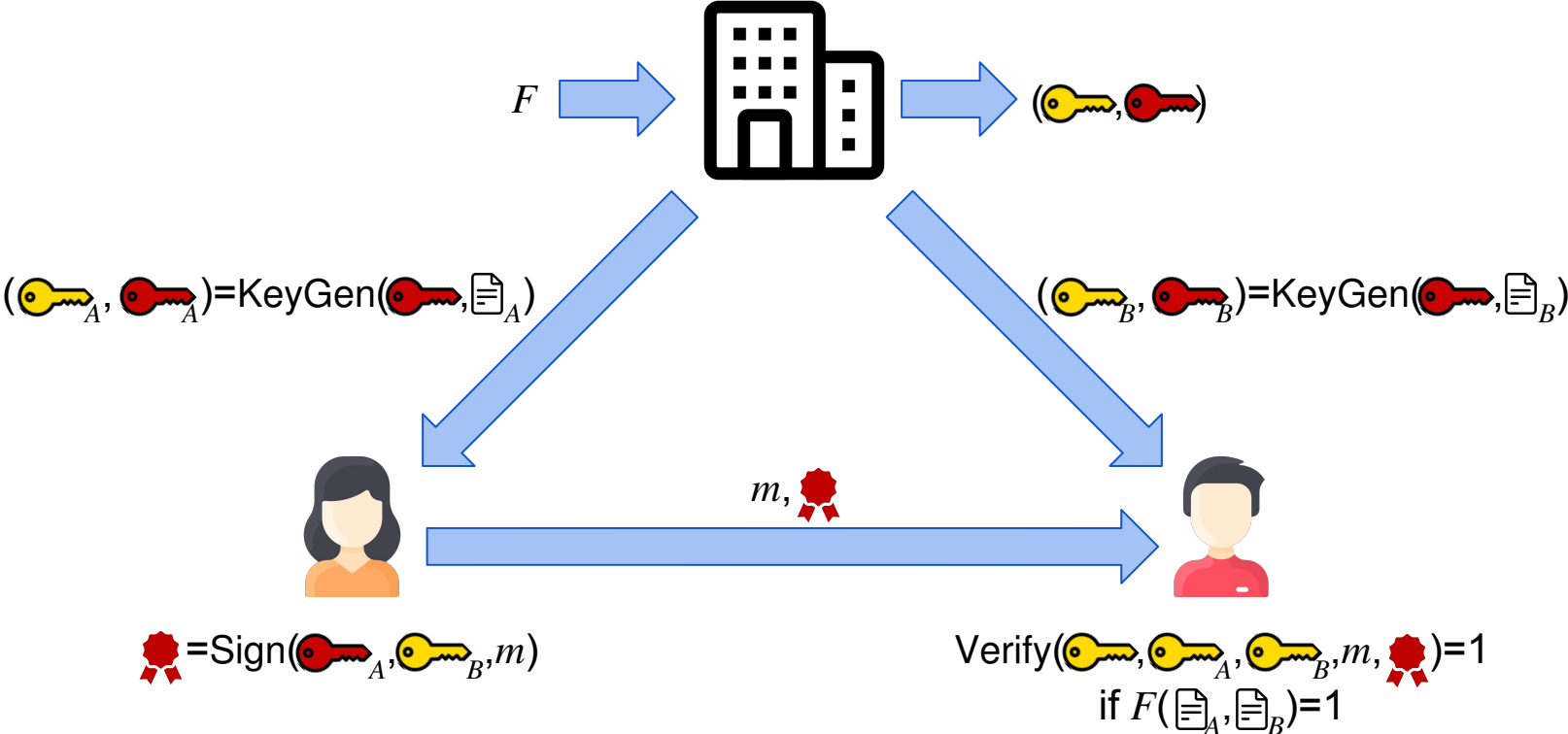
Policy-Compliant Signatures [BMW21]



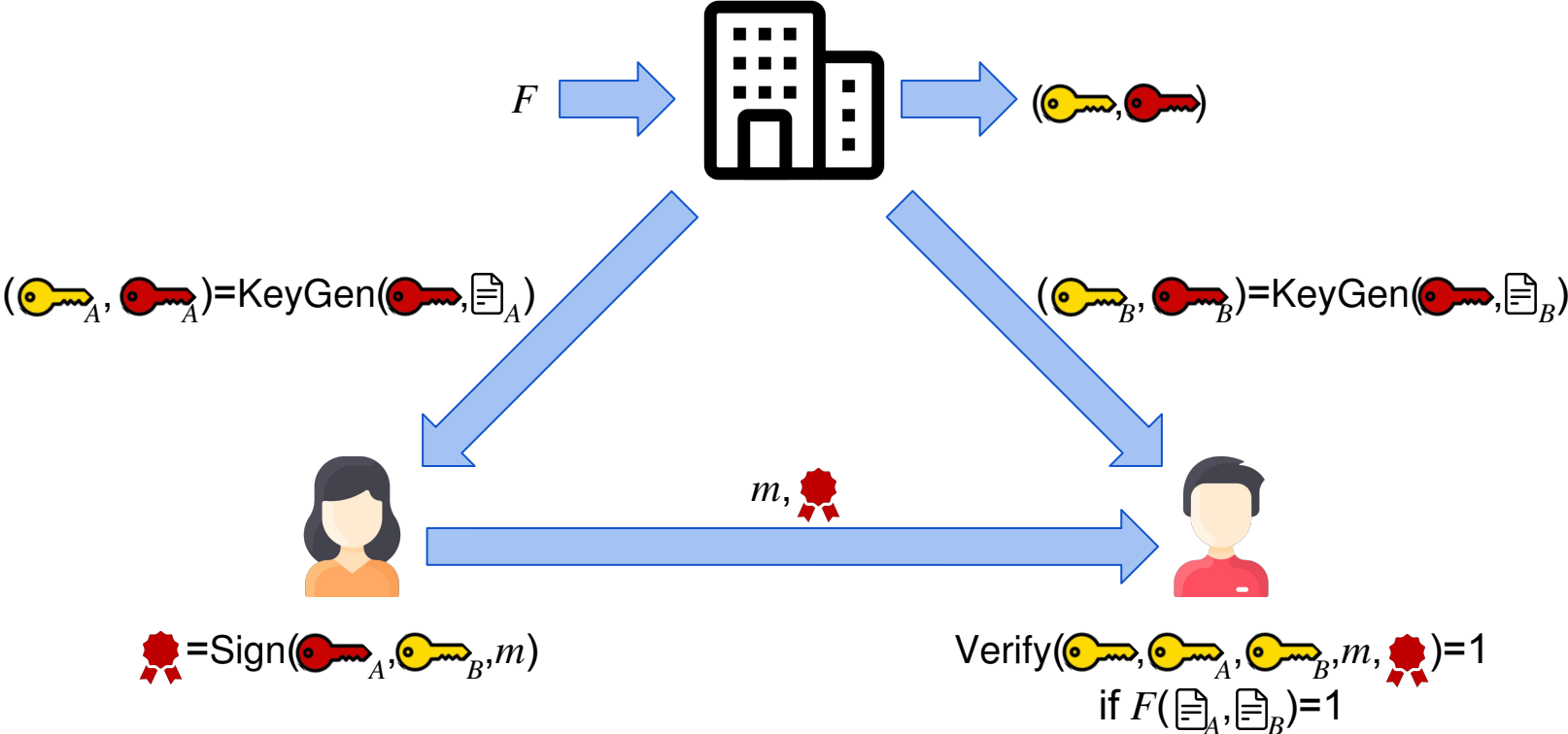
Policy-Compliant Signatures [BMW21]



Policy-Compliant Signatures [BMW21]

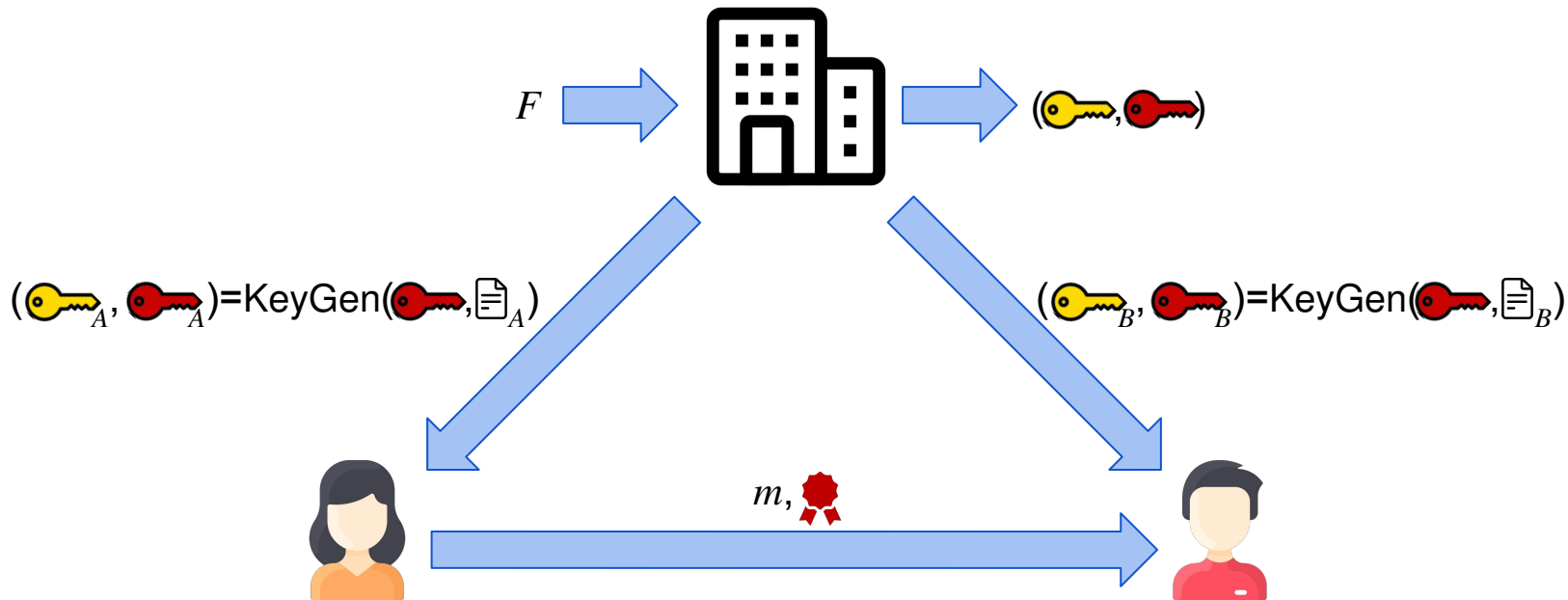


Policy-Compliant Signatures [BMW21]



Unforgeability and Attribute-Hiding

Policy-Compliant Signatures [BMW21]



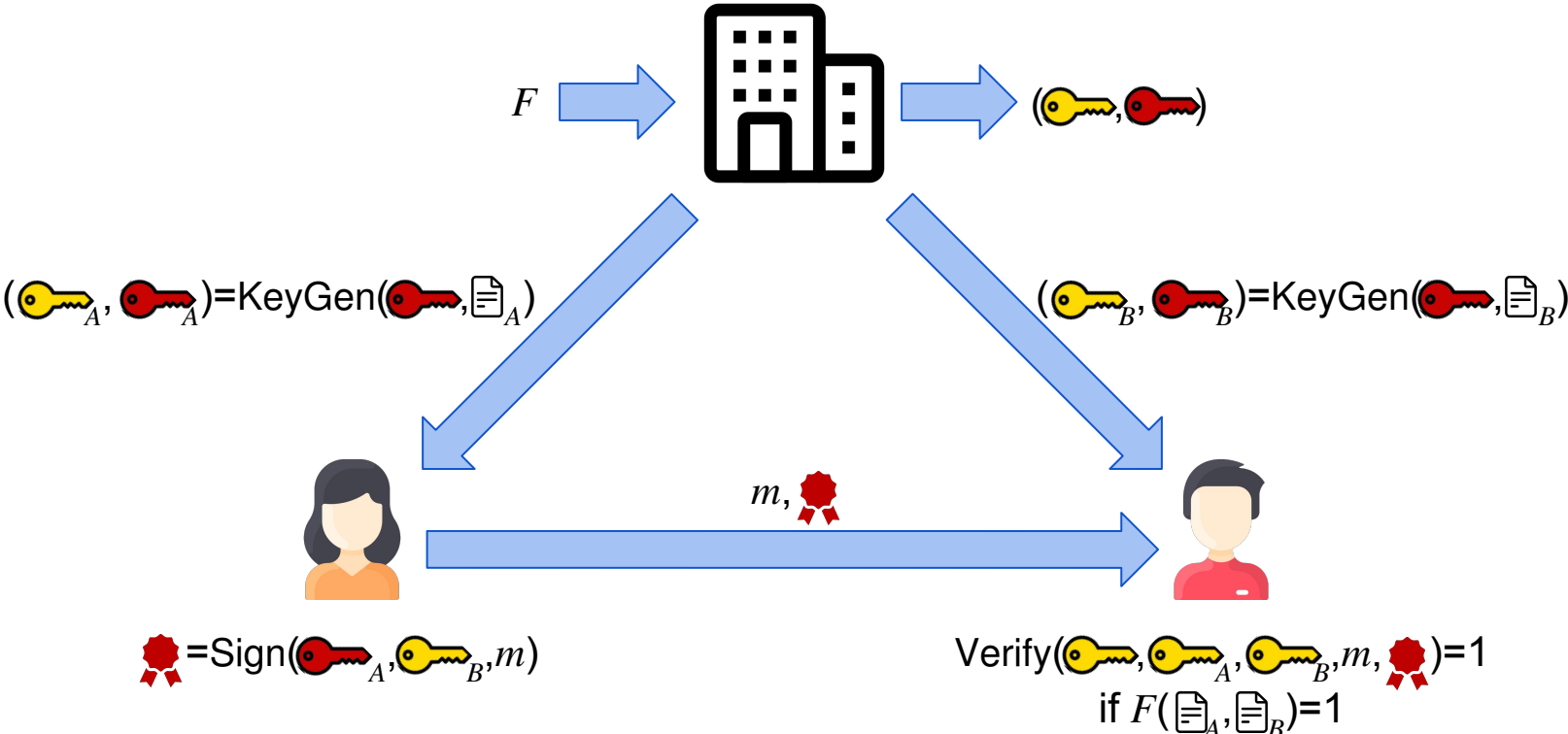
$[red\ seal] = Sign(red_key, doc)$

$key_A, key_B, m, [red\ seal] = 1, doc_B = 1$

What about updates?

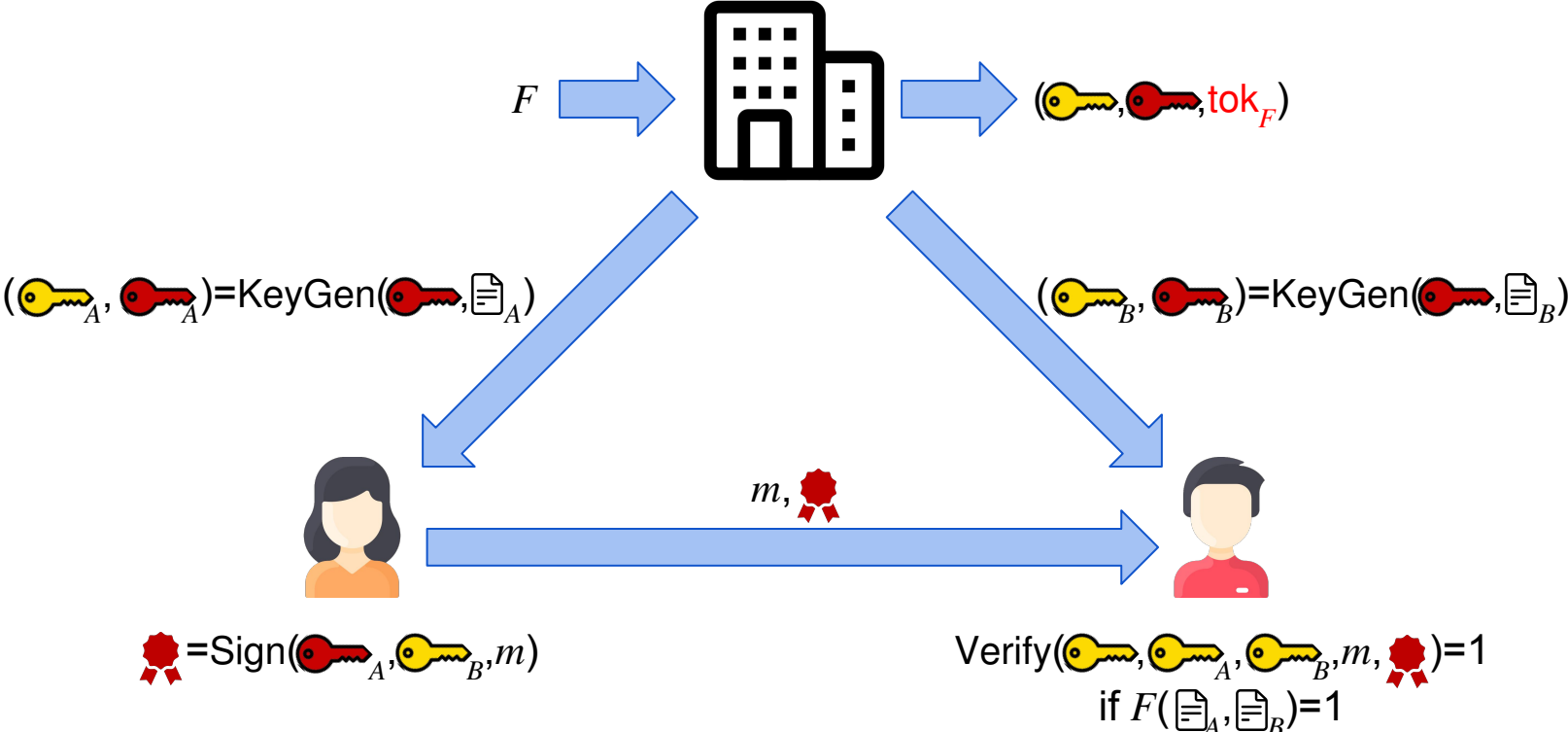
Unforgeability and

Updatable Policy-Compliant Signatures



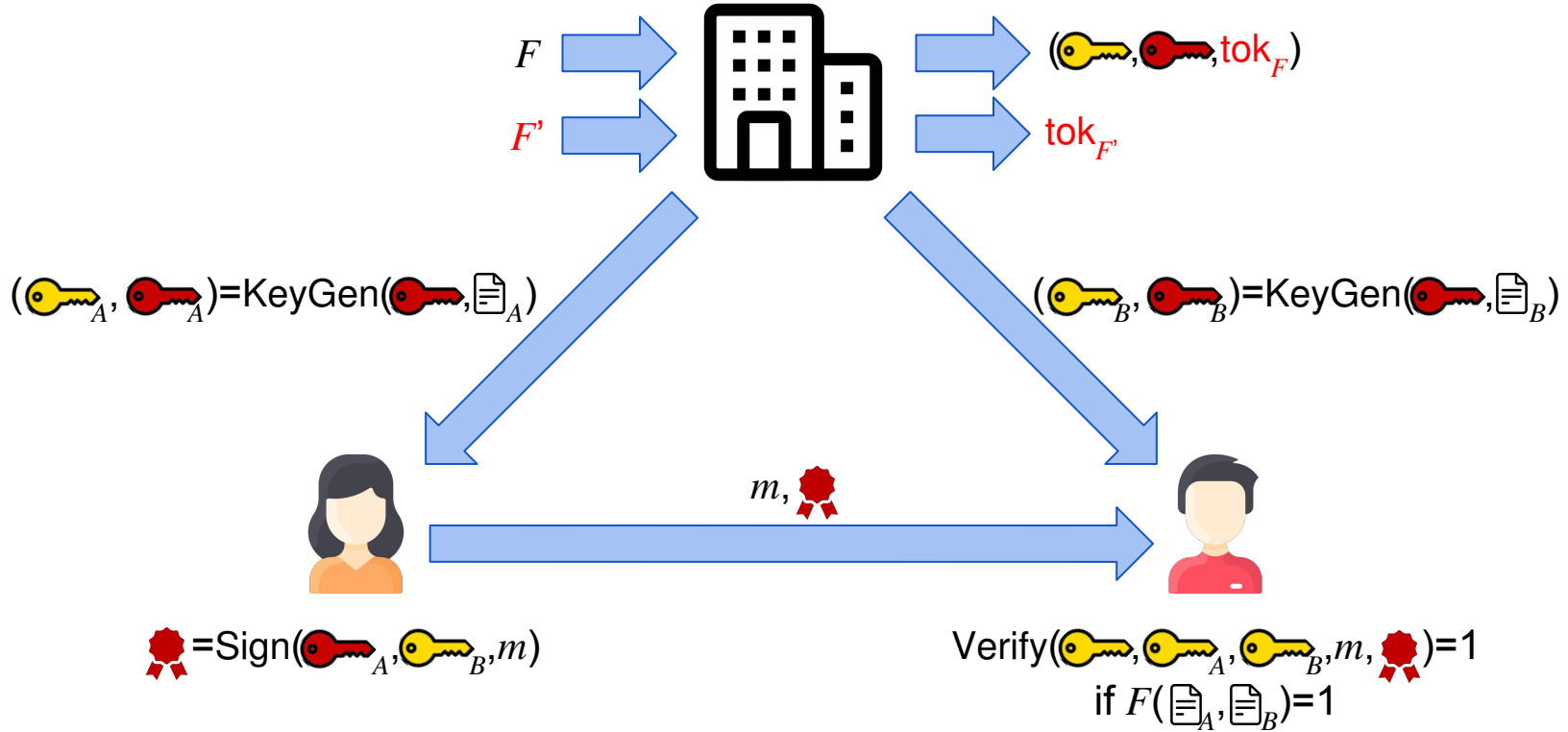
Unforgeability and Attribute-Hiding

Updatable Policy-Compliant Signatures



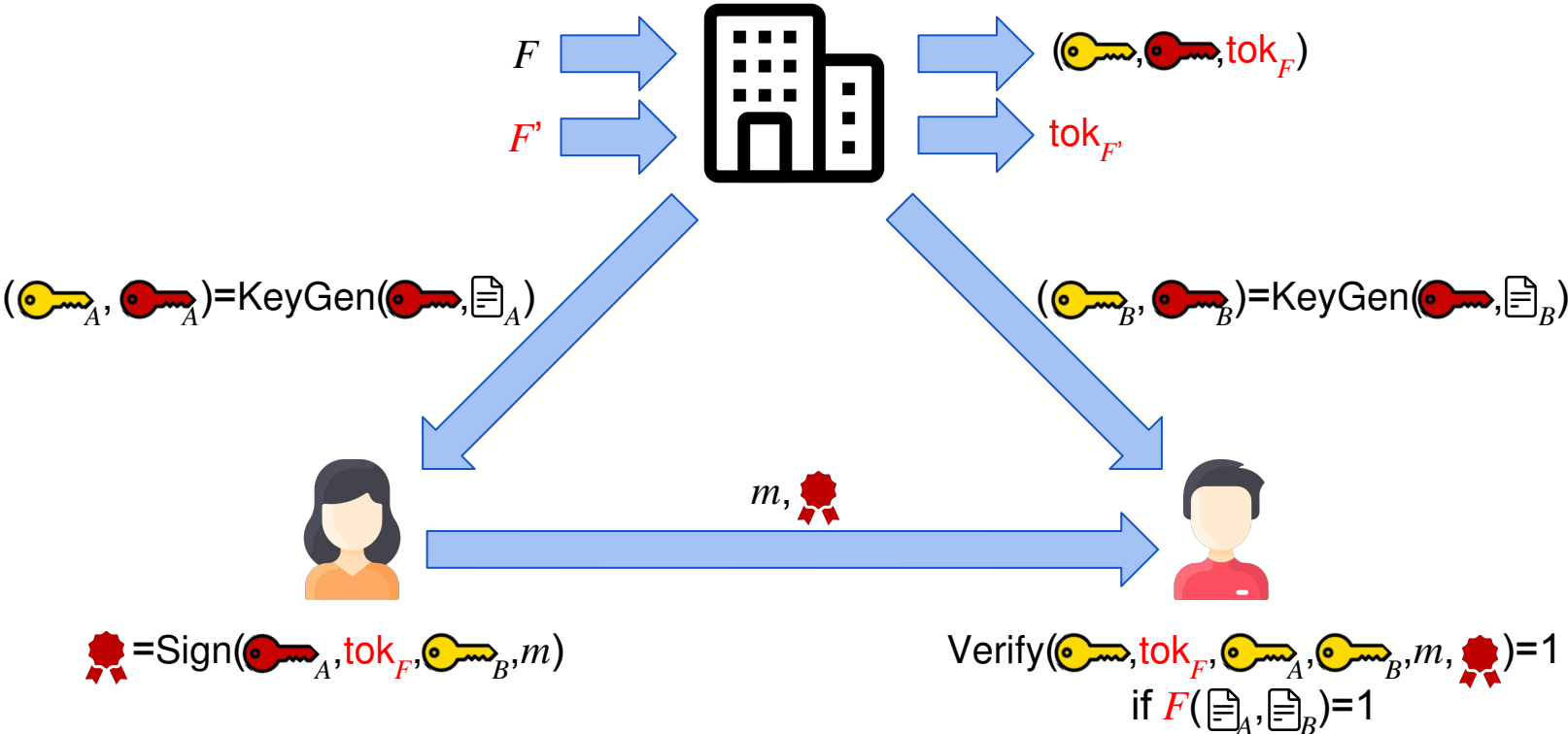
Unforgeability and Attribute-Hiding

Updatable Policy-Compliant Signatures



Unforgeability and Attribute-Hiding

Updatable Policy-Compliant Signatures

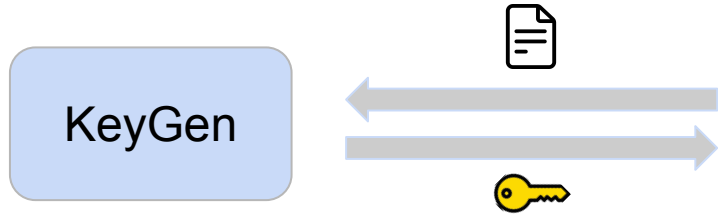


Unforgeability and Attribute-Hiding

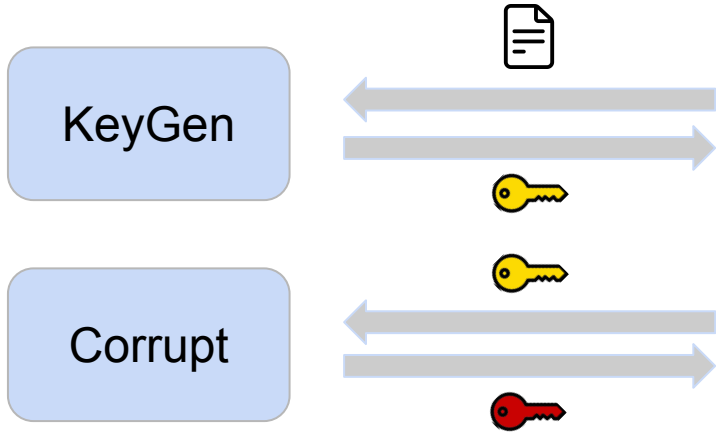
Unforgeability



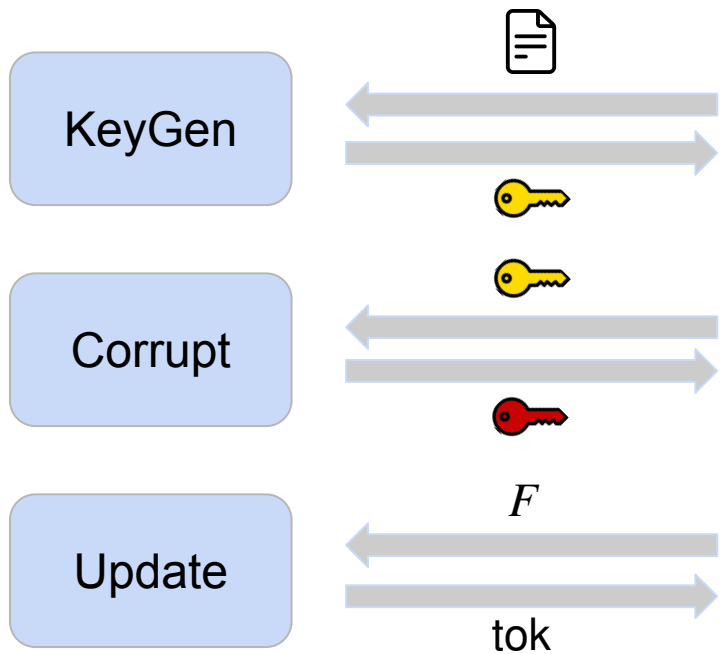
Unforgeability



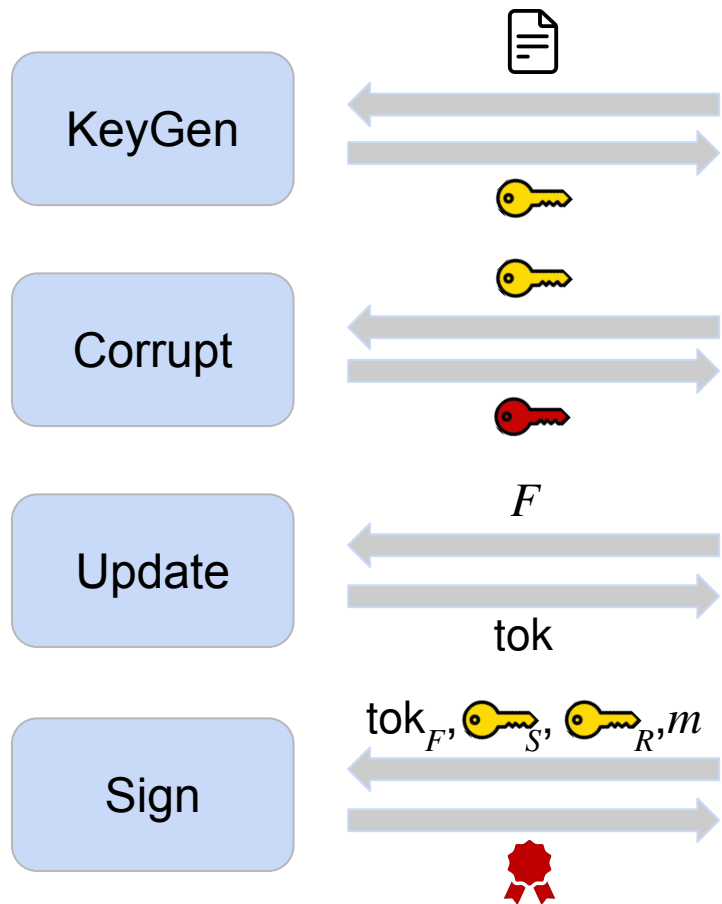
Unforgeability



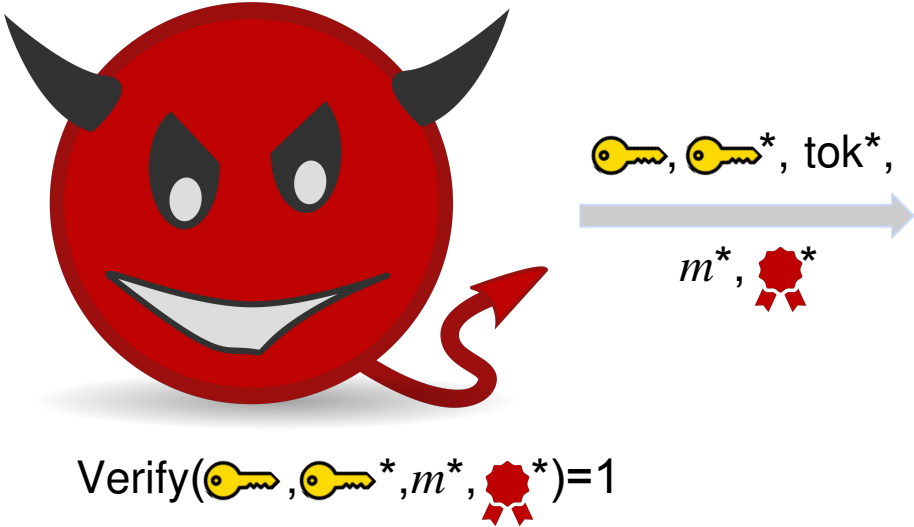
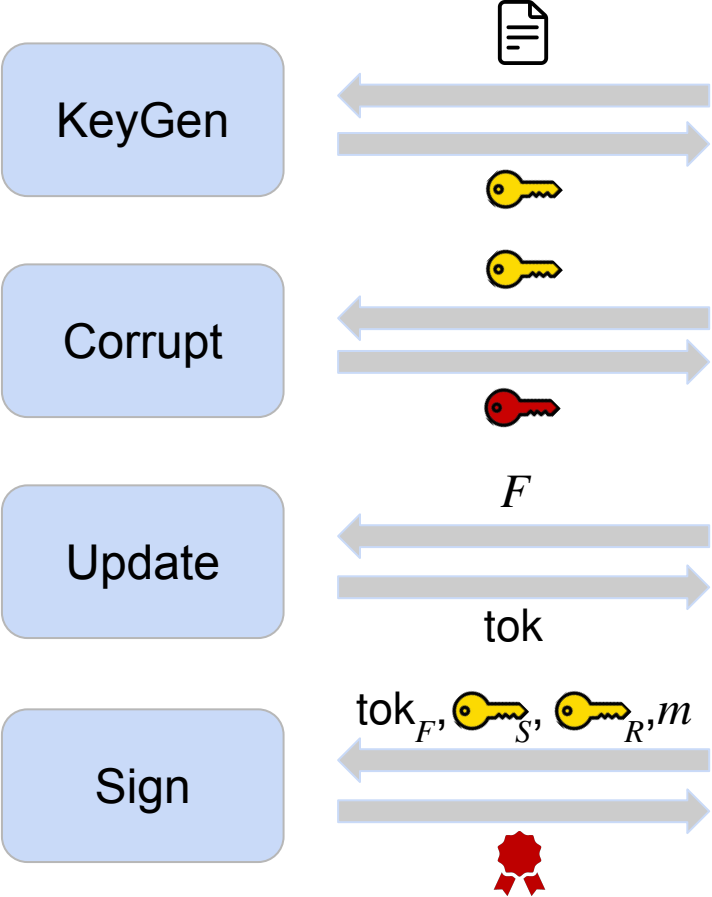
Unforgeability



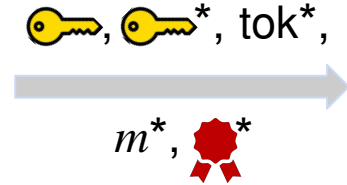
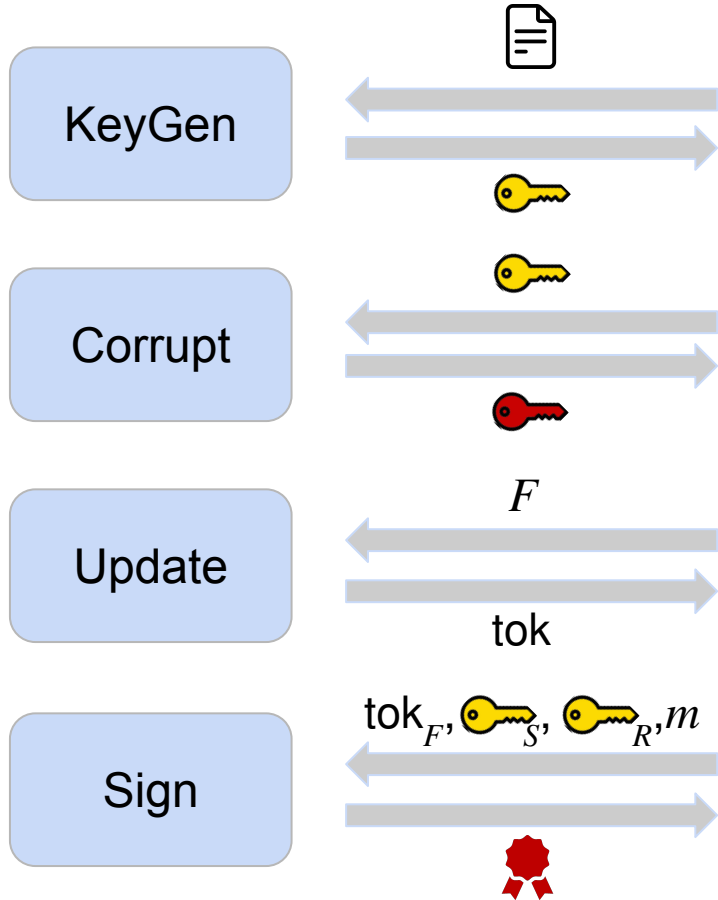
Unforgeability



Unforgeability



Unforgeability

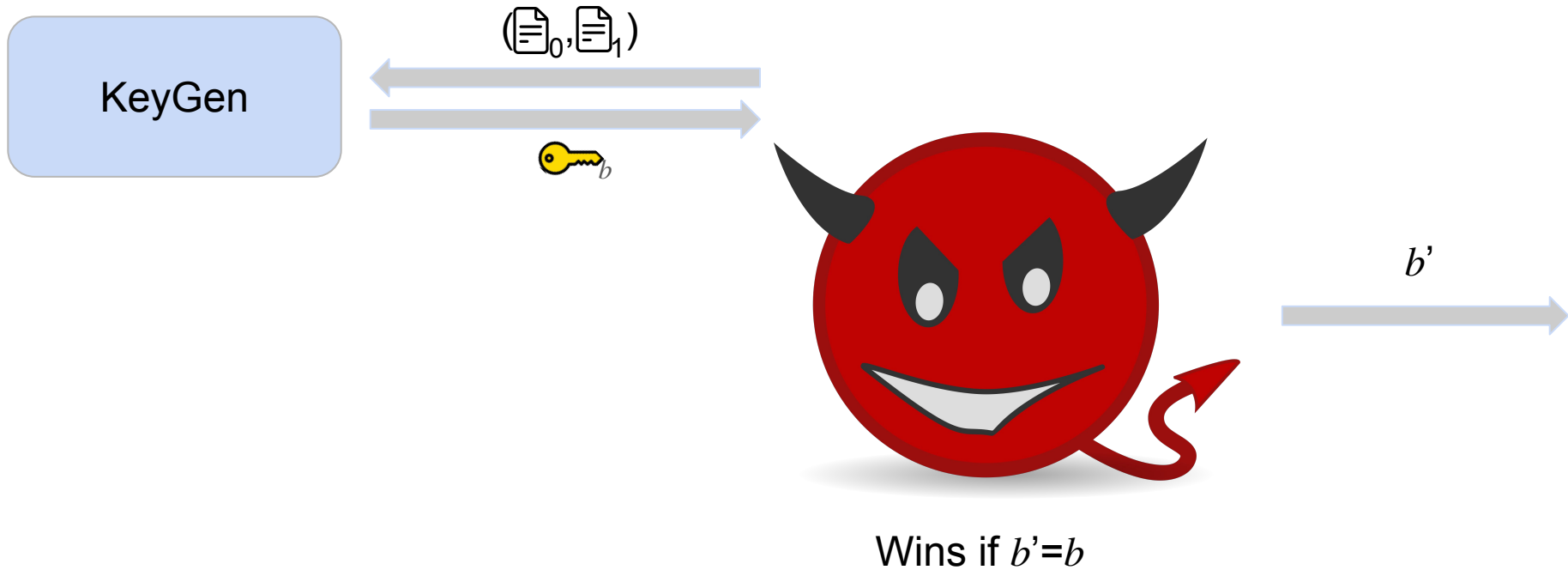


$Verify(\text{key}, \text{key}^*, m^*, \text{seal}^*) = 1 \wedge$
 (key has not been queried to Cor \vee
 $F(\text{doc}, \text{doc}^*) = 0 : \text{doc}, \text{doc}^*, F$ belong to $\text{key}, \text{key}^*, tok^* \vee$
 tok^* has not been output by Update)

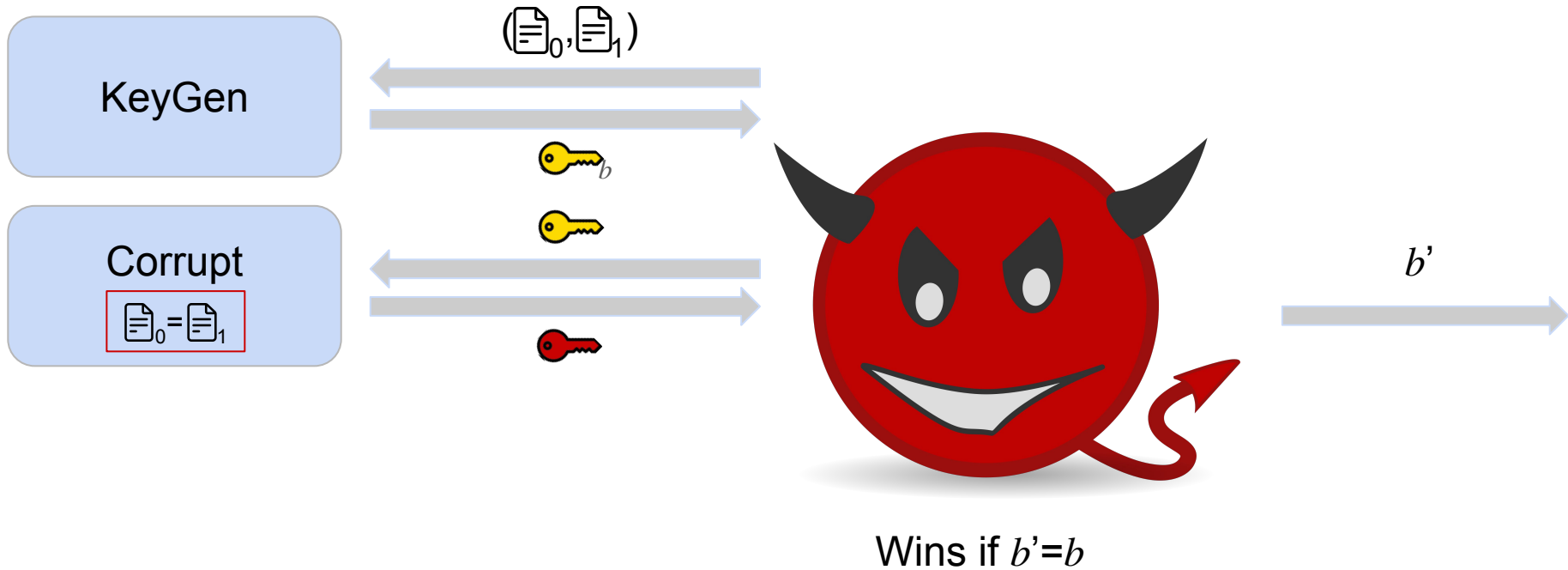
Attribute Hiding



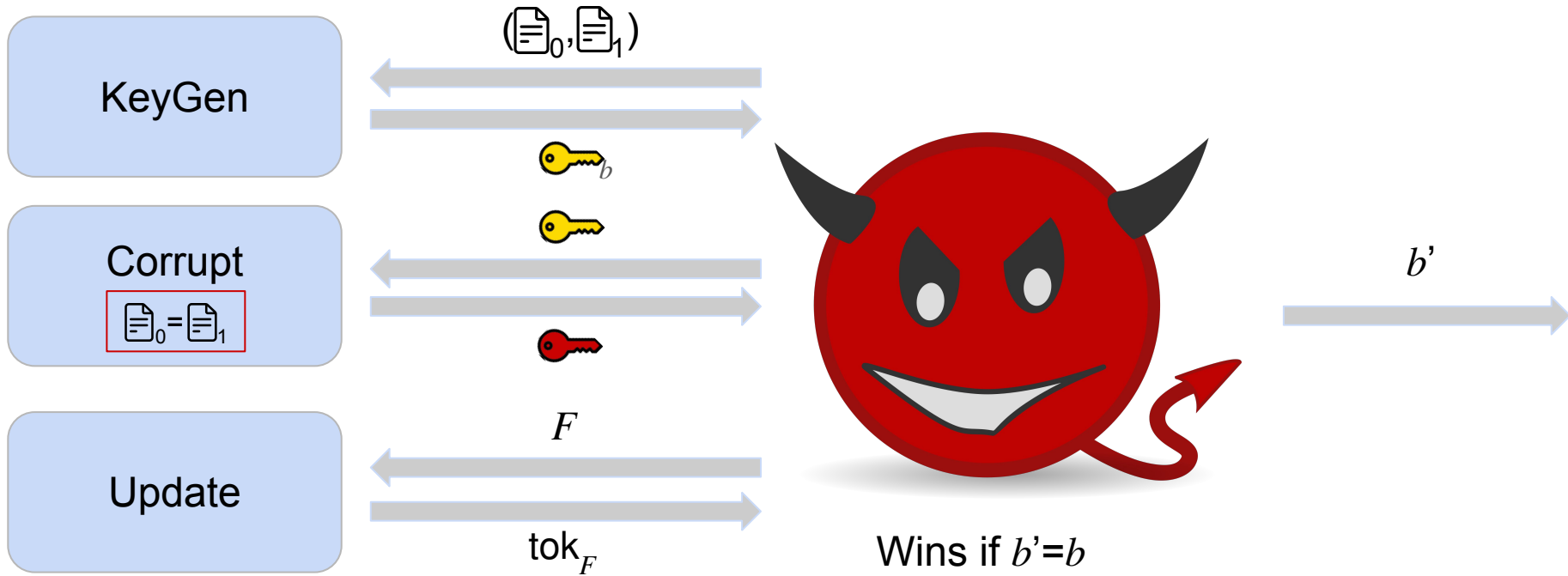
Attribute Hiding



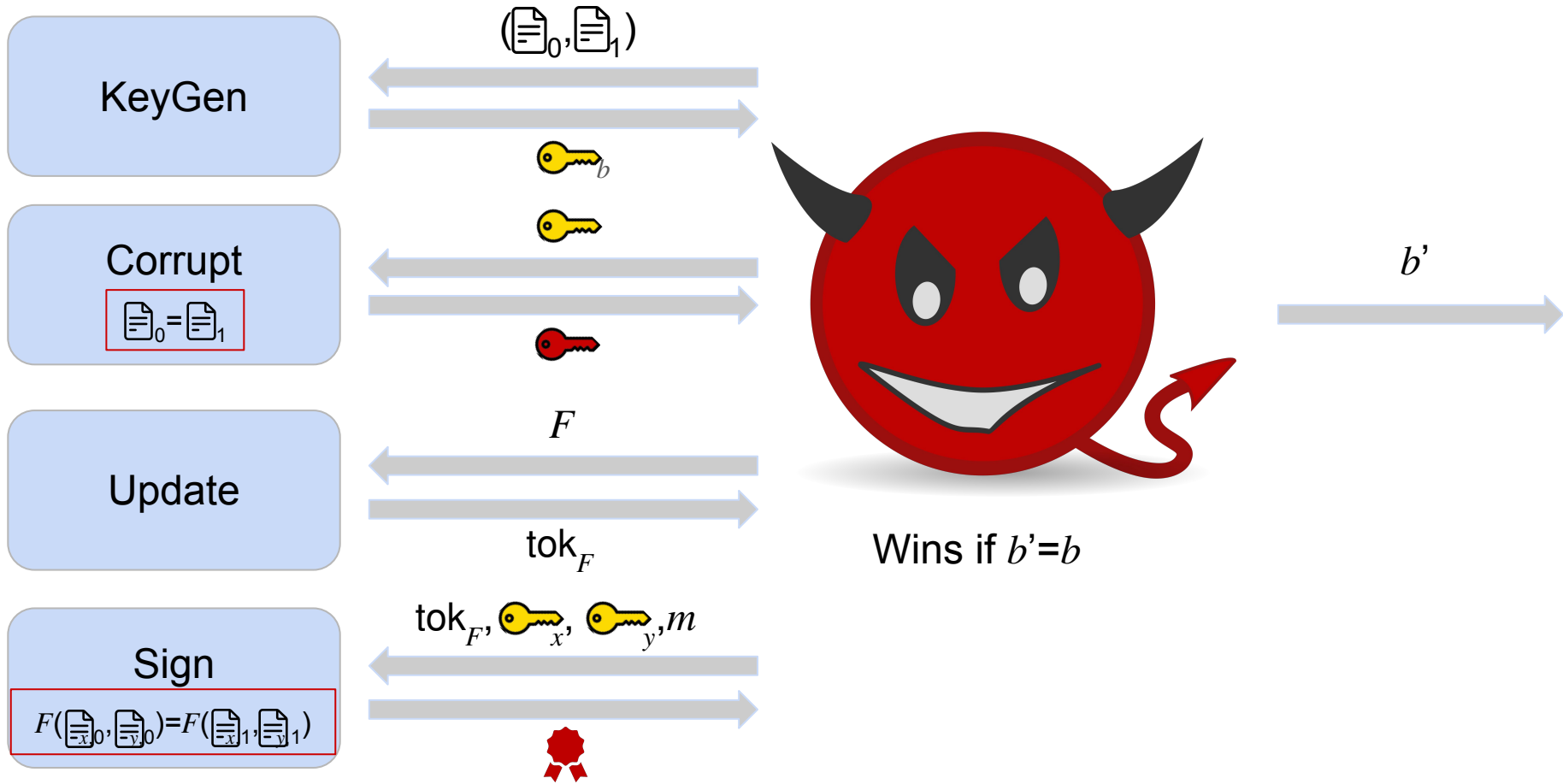
Attribute Hiding



Attribute Hiding

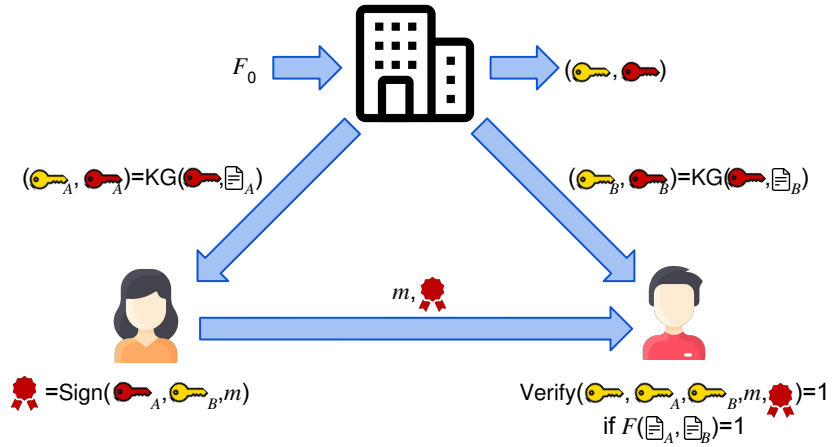


Attribute Hiding

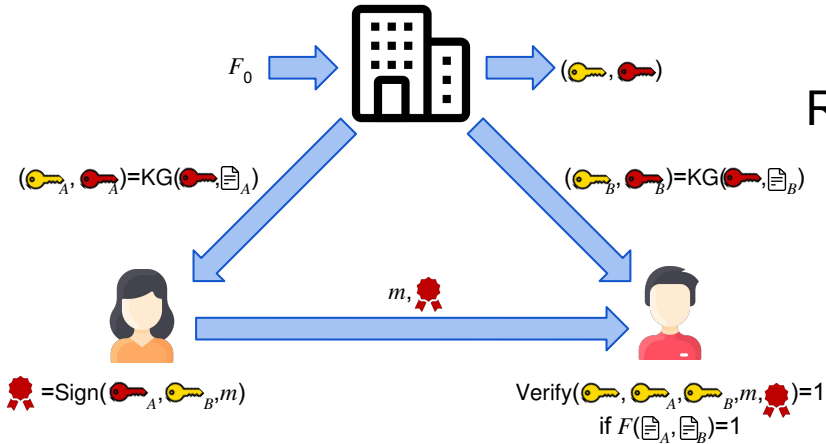


Naive Approach

Naive Approach



Naive Approach

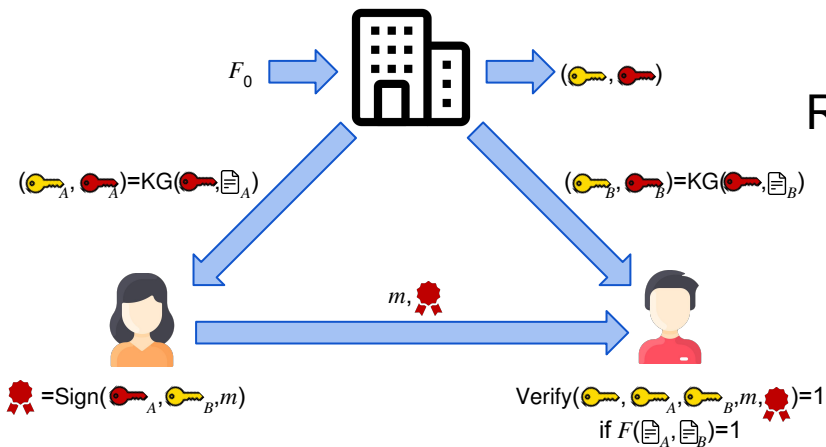


Rerun Setup



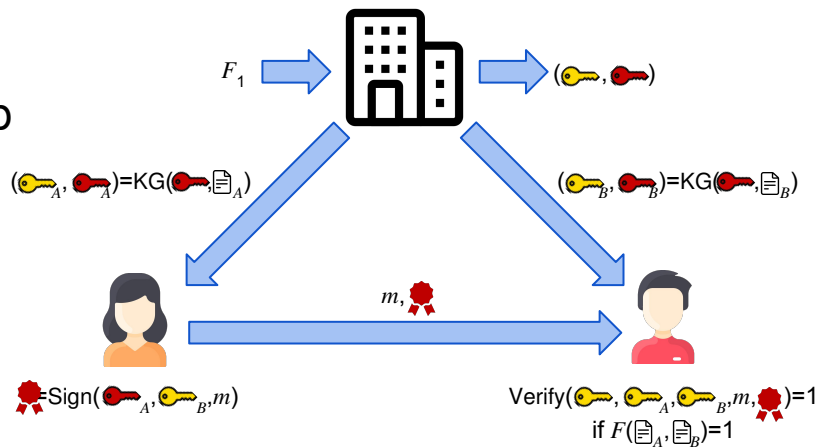
with F_1

Naive Approach

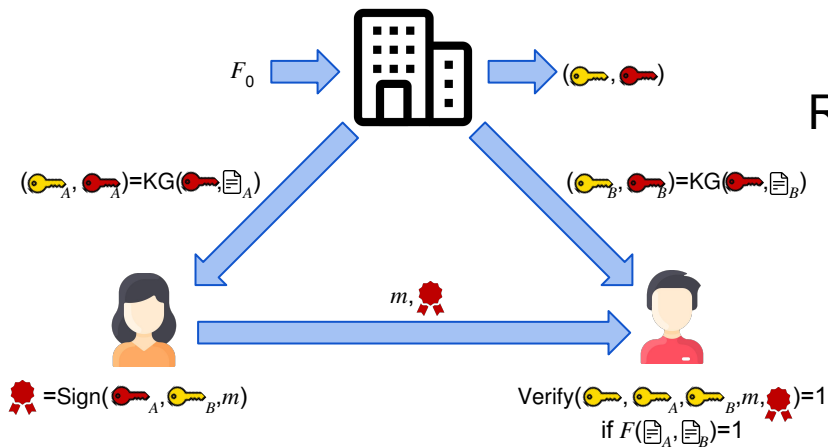


Rerun Setup

→
with F_1

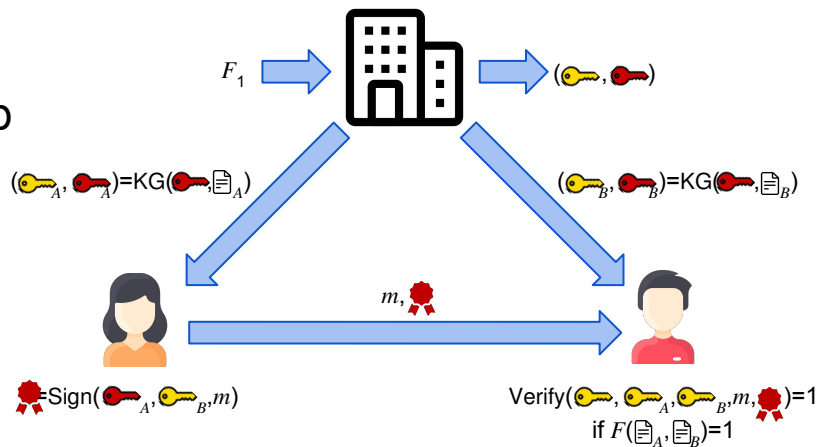


Naive Approach



Rerun Setup

→
with F_1



High communication complexity

Construction

Tools:

Construction

Tools:

1. Digital Signatures

Construction

Tools:

1. Digital Signatures
2. Non-Interactive Zero-Knowledge Proofs

Construction

Tools:

1. Digital Signatures
2. Non-Interactive Zero-Knowledge Proofs
3. Two-Input (Partially-Hiding) Predicate Encryption

Construction

Tools:

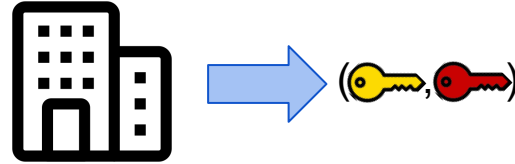
1. Digital Signatures

2. Non-Interactive Zero-Knowledge Proofs

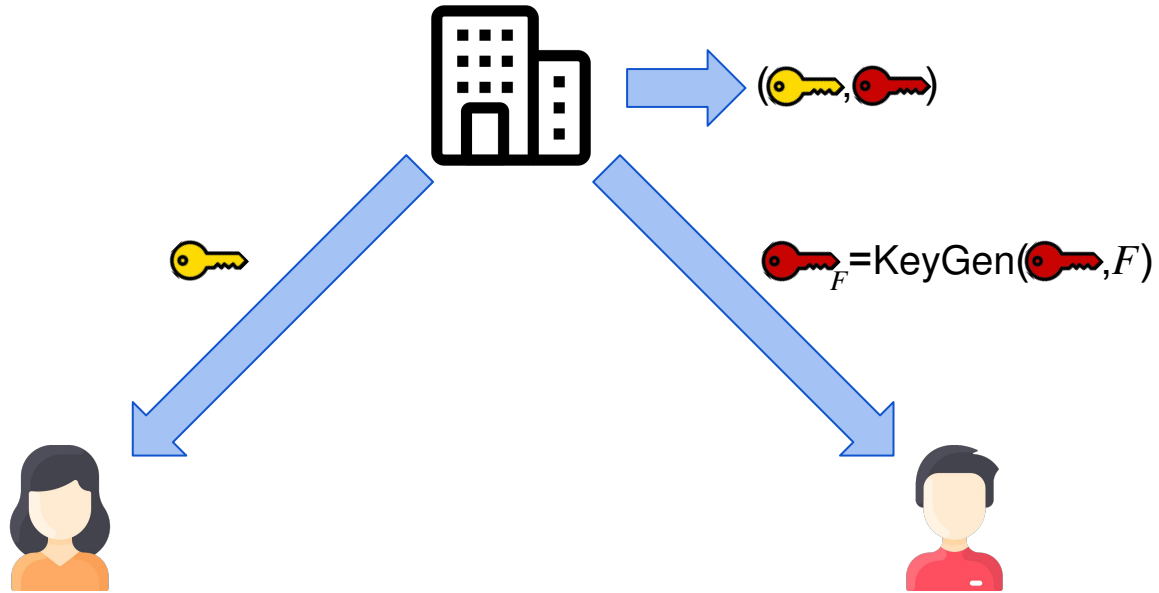
3. Two-Input (Partially-Hiding) Predicate Encryption

(Public-Key) Predicate Encryption [KSW07]

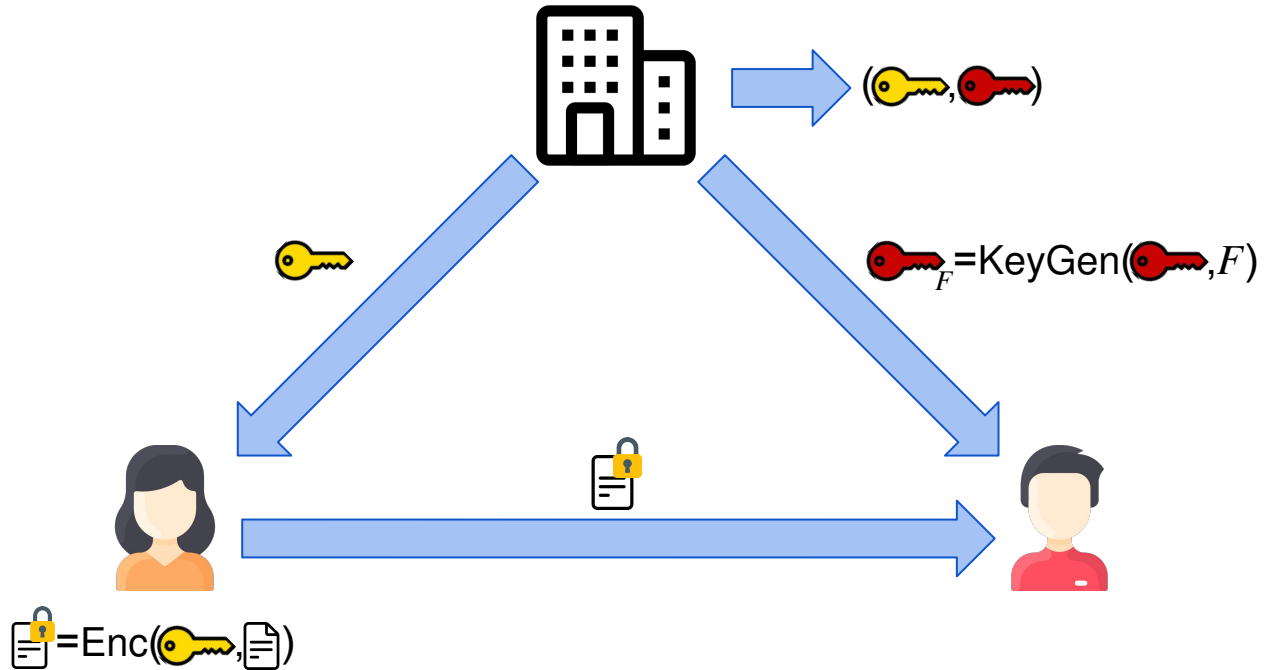
(Public-Key) Predicate Encryption [KSW07]



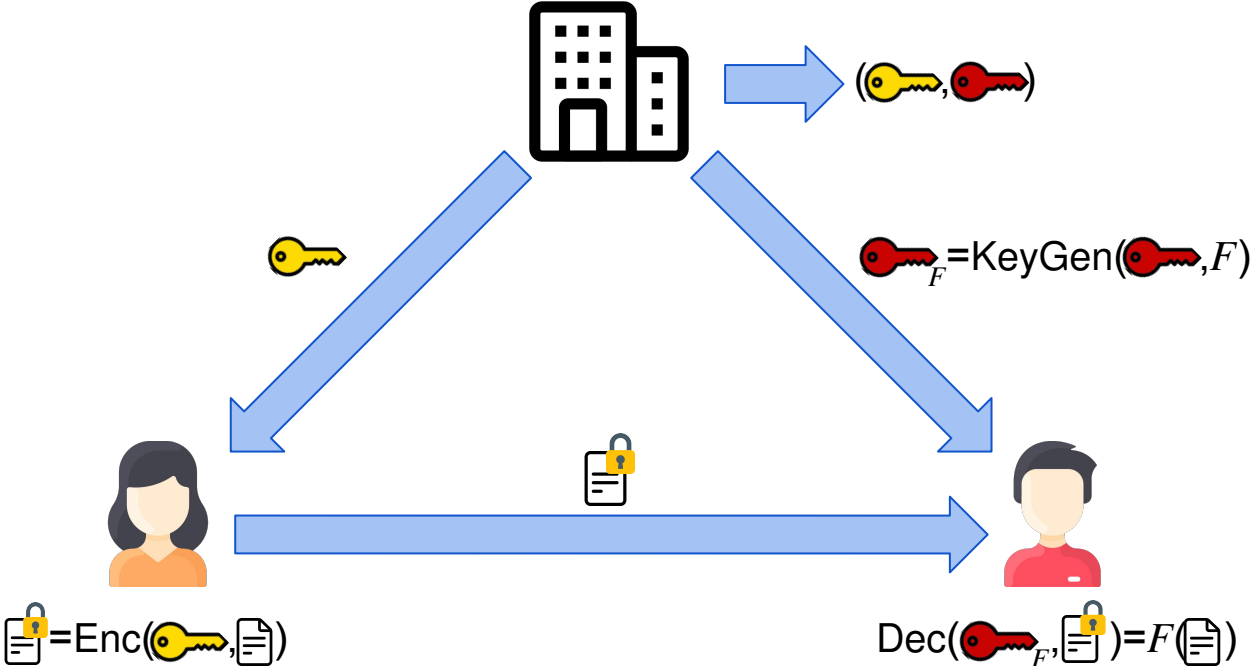
(Public-Key) Predicate Encryption [KSW07]



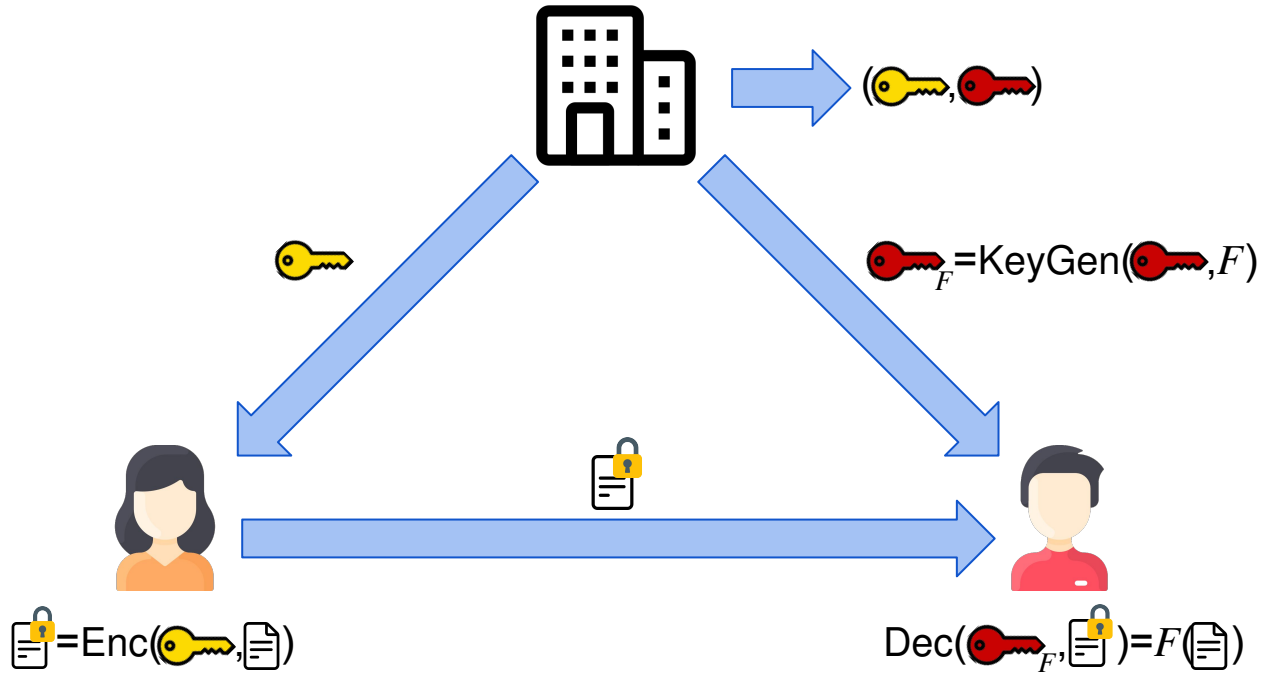
(Public-Key) Predicate Encryption [KSW07]



(Public-Key) Predicate Encryption [KSW07]

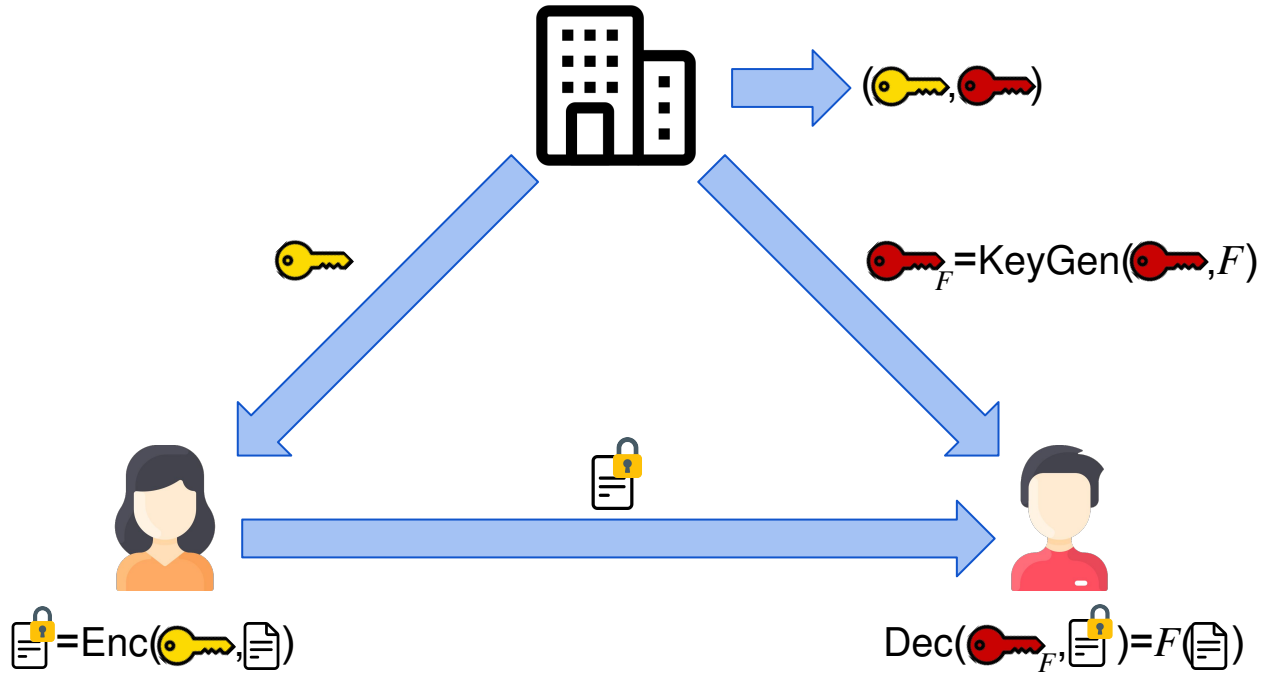


(Public-Key) Predicate Encryption [KSW07]



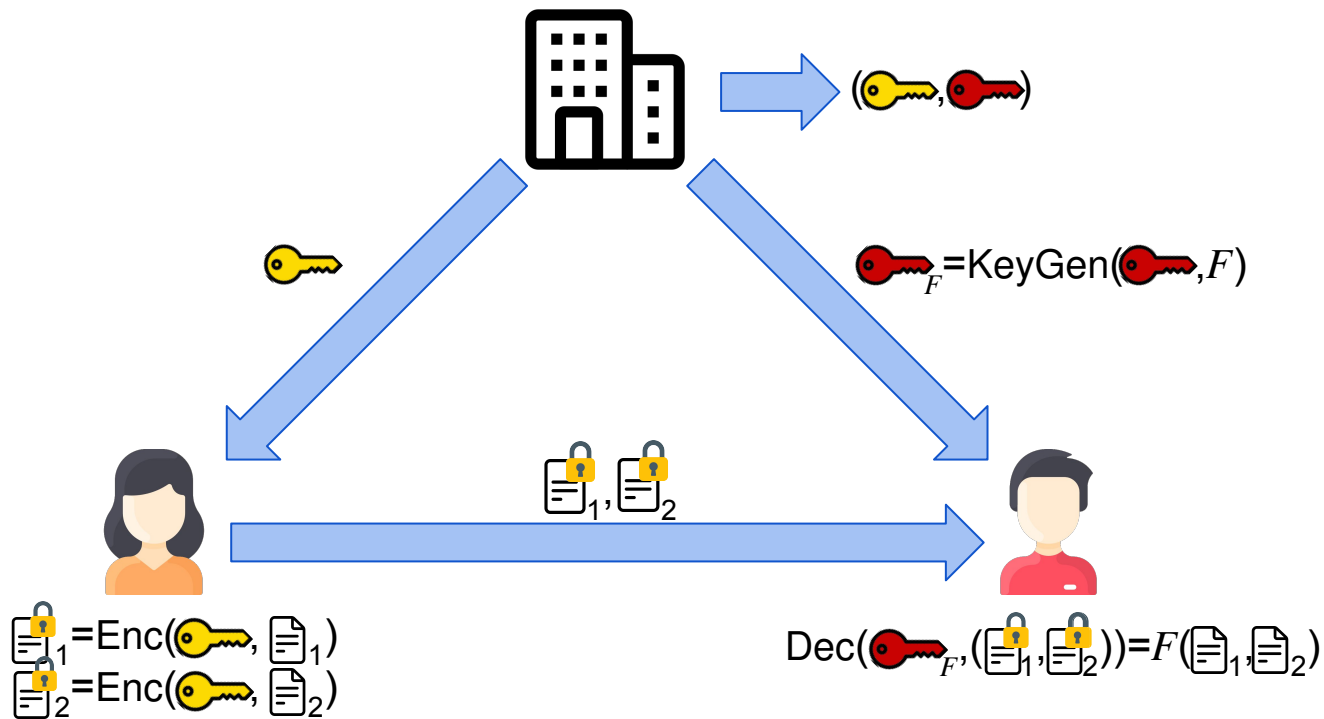
Attribute Hiding

Two-Input Predicate Encryption [GGG+14]



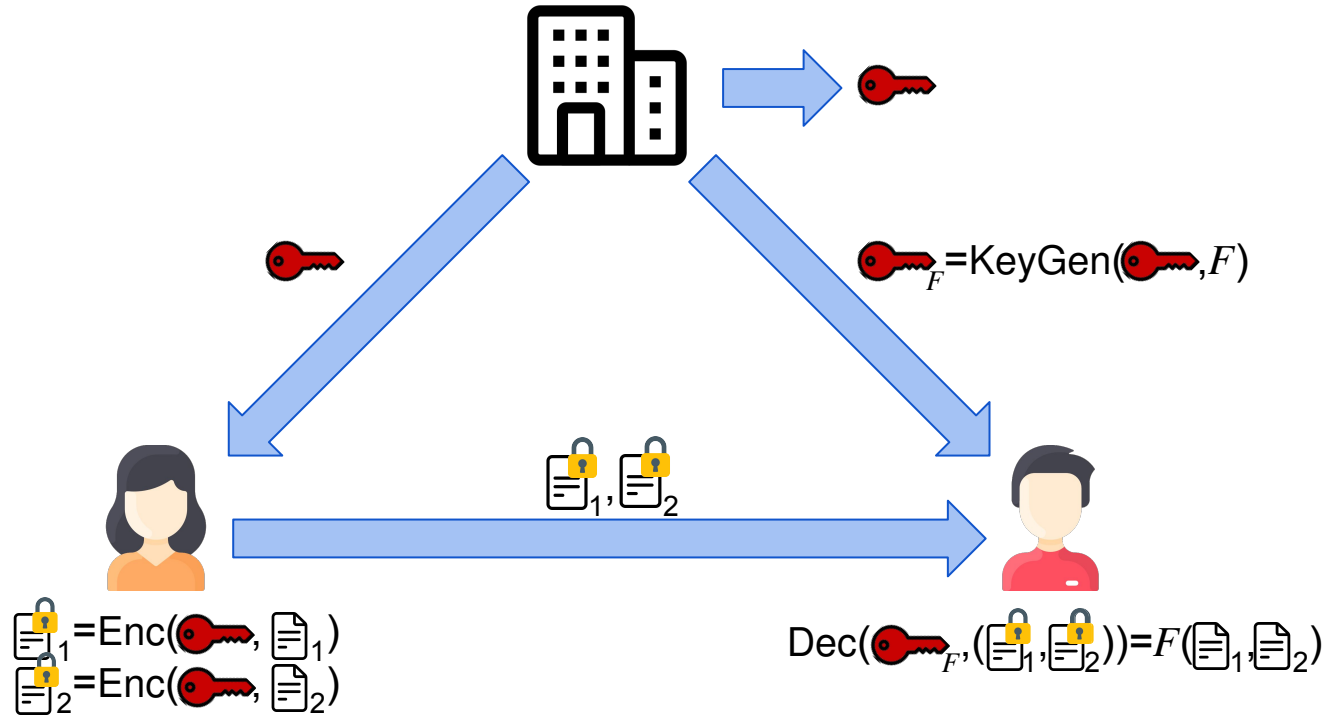
Attribute Hiding

Two-Input Predicate Encryption [GGG+14]



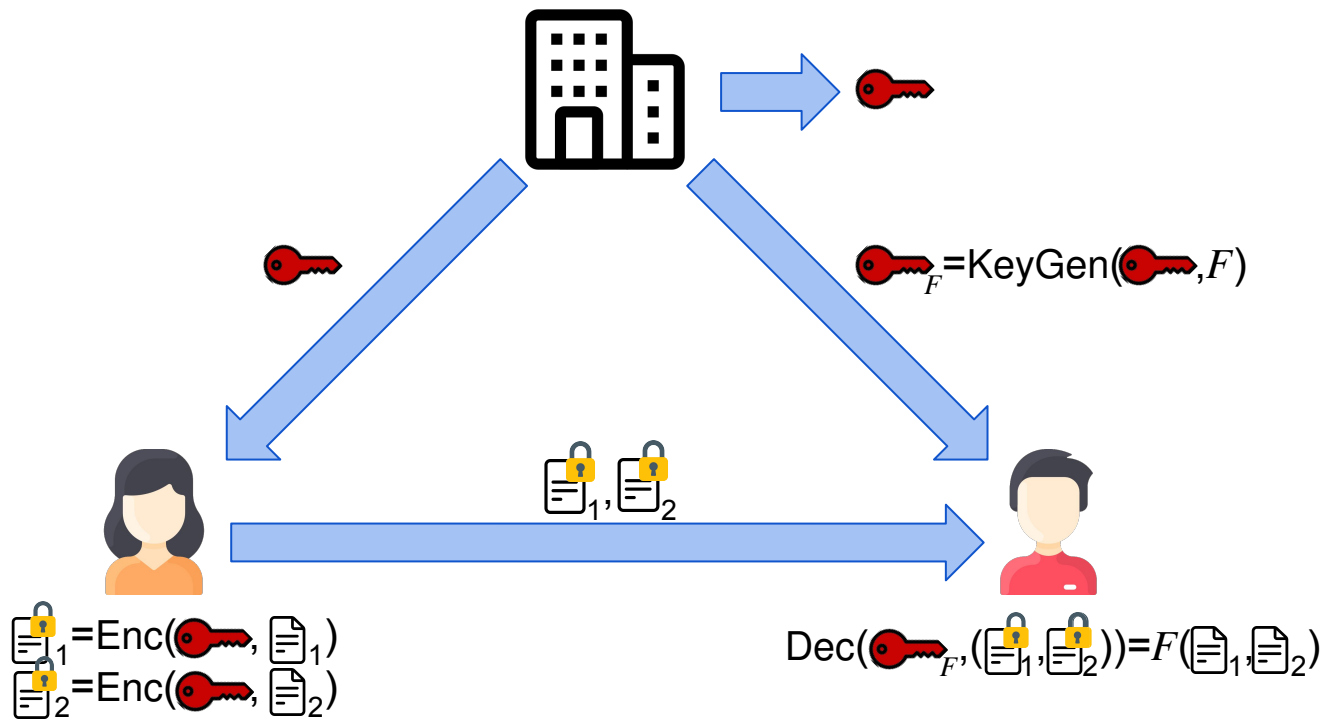
Attribute Hiding

Two-Input Predicate Encryption [GGG+14]



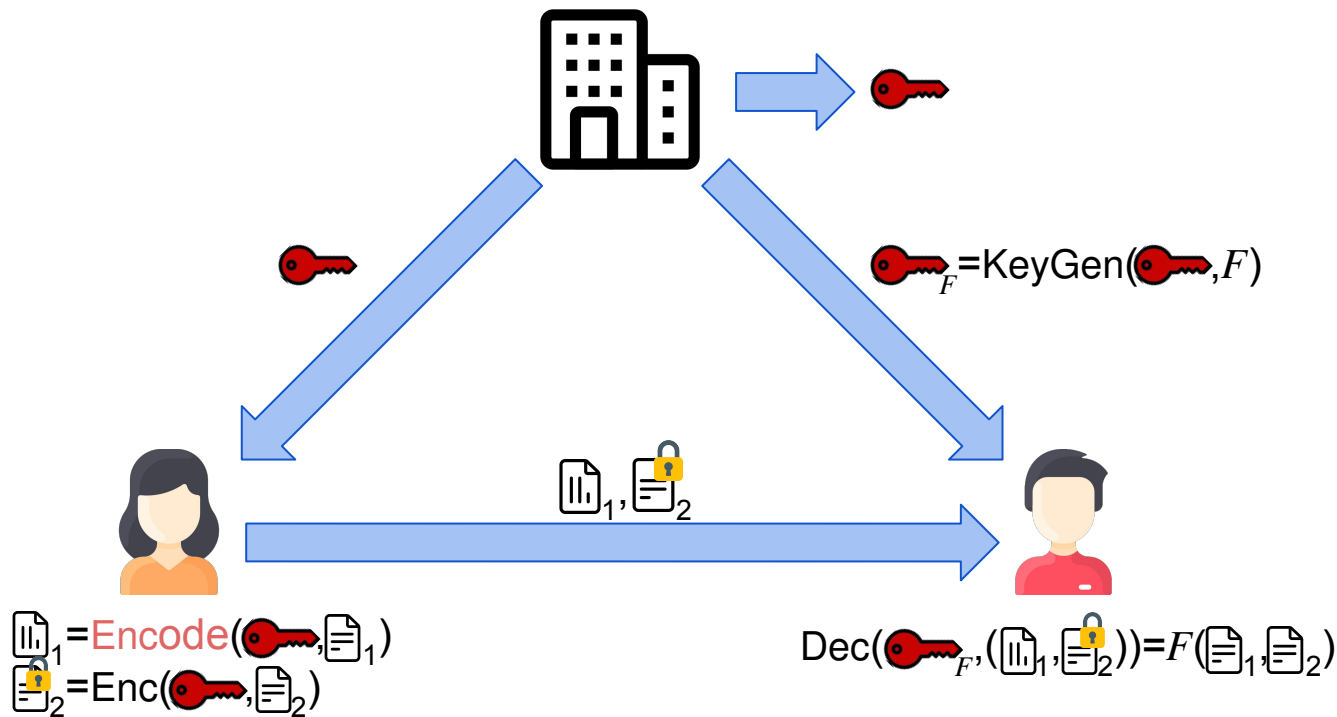
Attribute Hiding

Two-Input (Partially-Hiding) Predicate Encryption



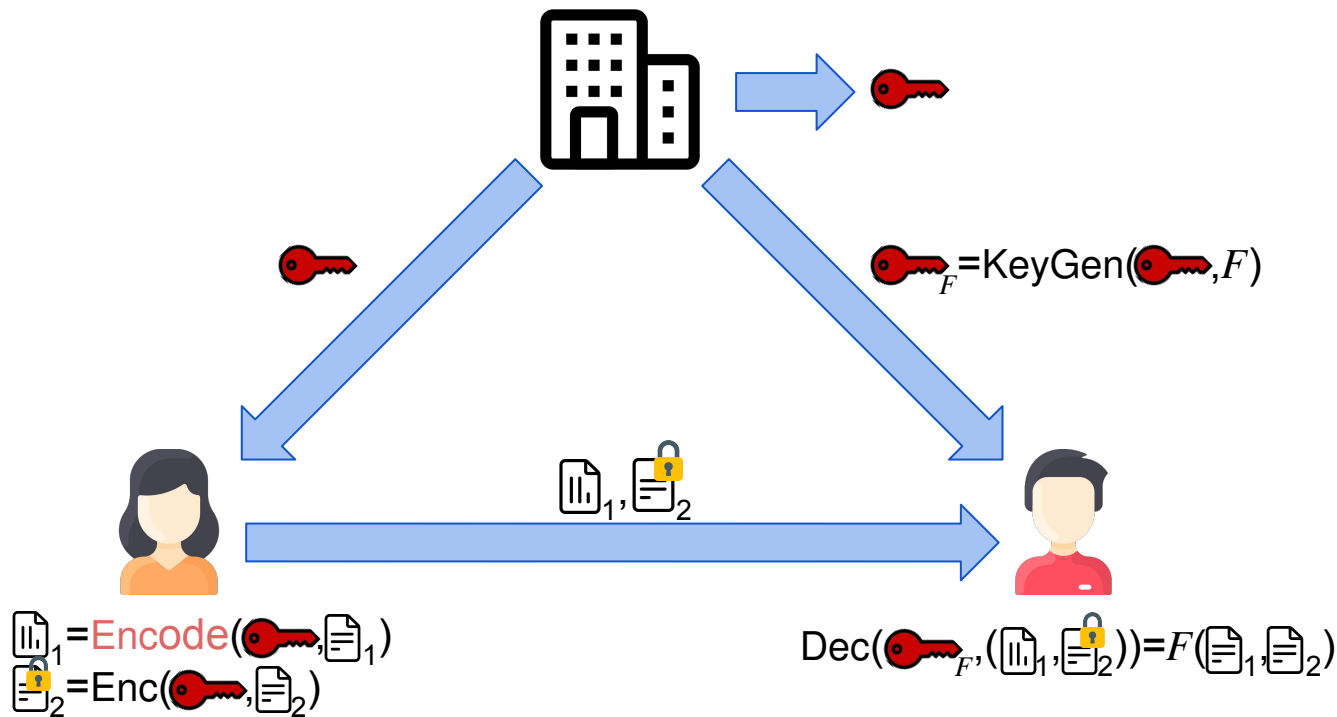
Attribute Hiding

Two-Input (Partially-Hiding) Predicate Encryption



Attribute Hiding

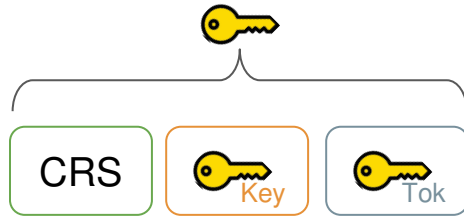
Two-Input (Partially-Hiding) Predicate Encryption



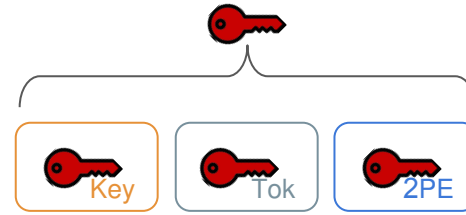
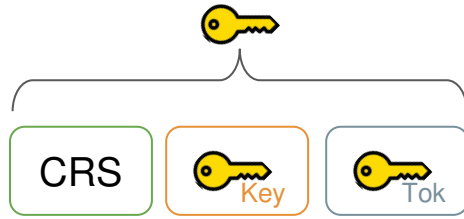
Attribute Hiding **only for second slot**

Construction

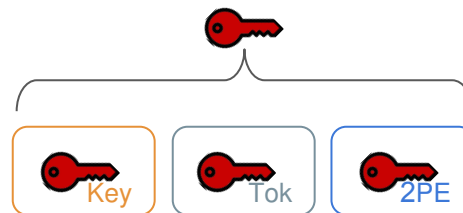
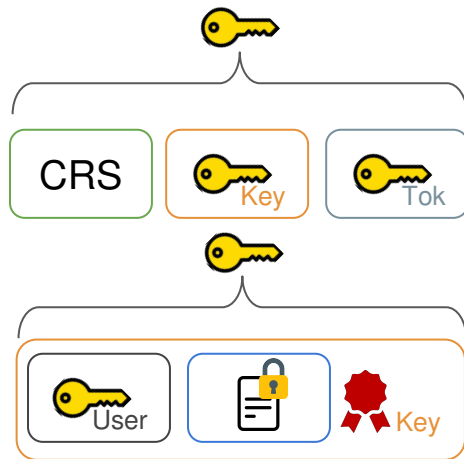
Construction



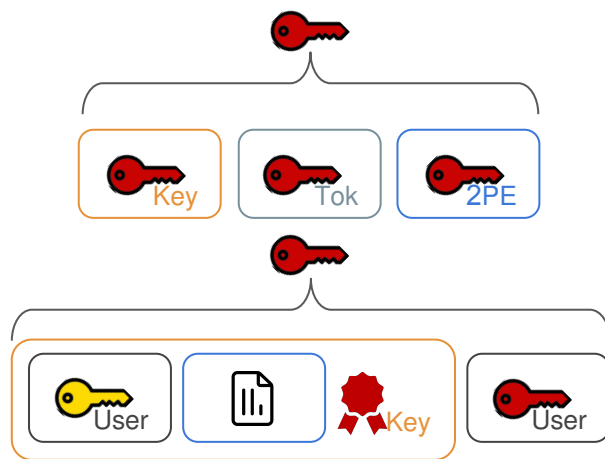
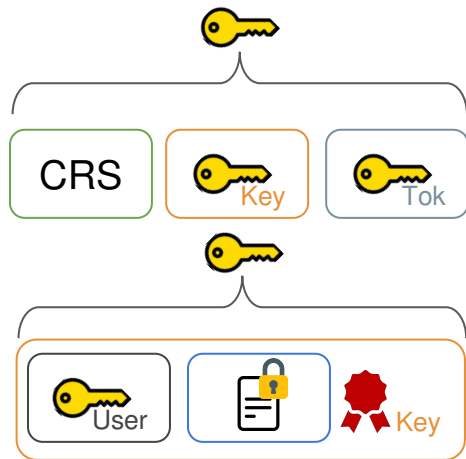
Construction



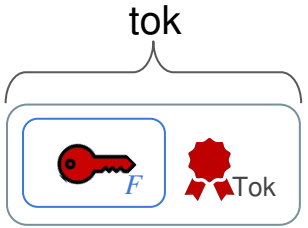
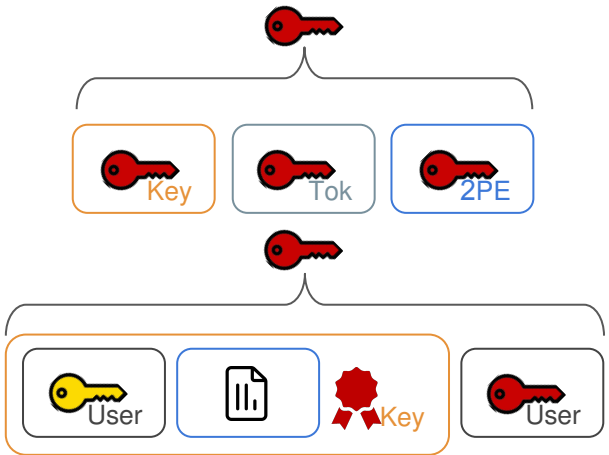
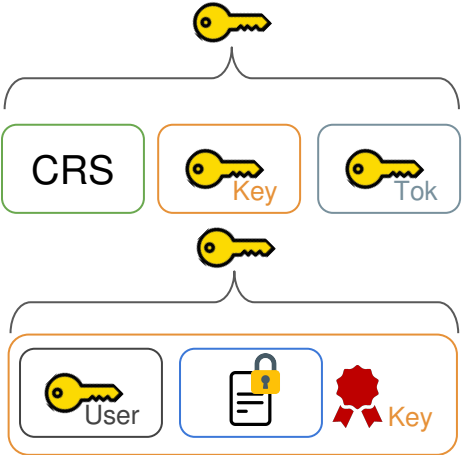
Construction



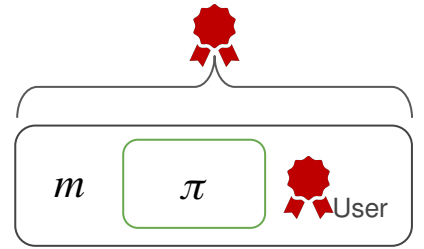
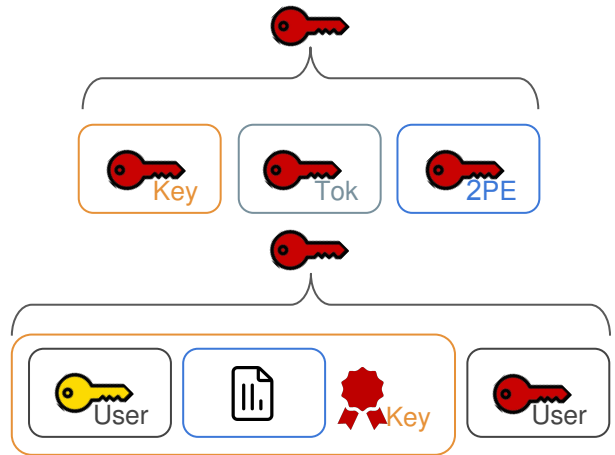
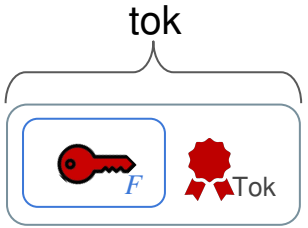
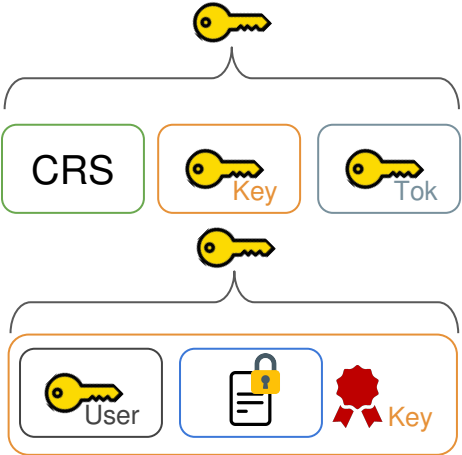
Construction



Construction



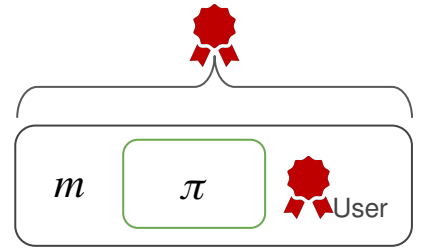
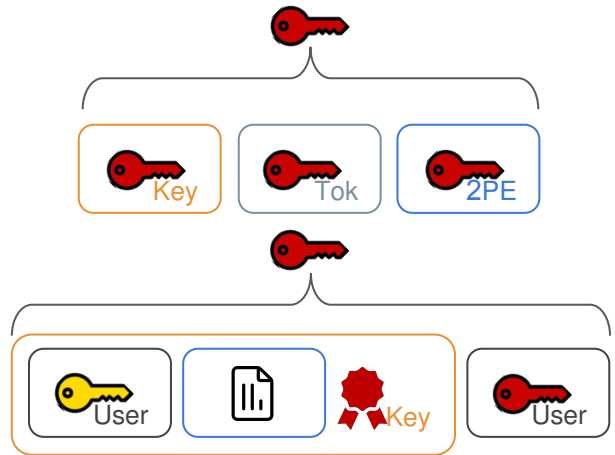
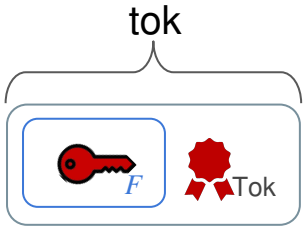
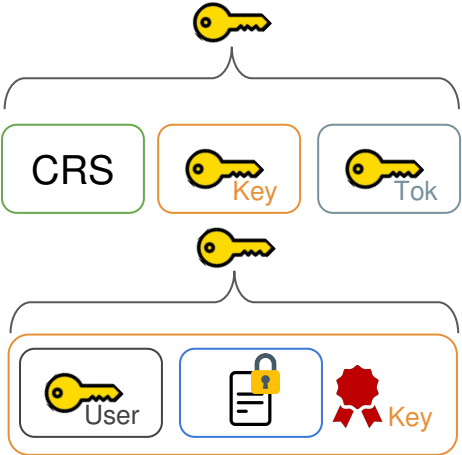
Construction



$$\text{Dec}(\text{red key}, (\text{document}, \text{locked document})) = 1 \wedge$$

$$\text{Verify}(\text{yellow key}, (\text{yellow key}, \text{document}, \text{red gear})) = 1$$

Construction



Done?

$$\text{Dec}(\text{red key}, (\text{document}, \text{locked document})) = 1 \wedge \text{Verify}(\text{yellow Key}, (\text{yellow User}, \text{document}, \text{red gear Key})) = 1$$

Non-Interactive Updatable PCS

No!

Non-Interactive Updatable PCS

No!

⇒ 2-PHPE currently only realizable from heavy assumptions

Non-Interactive Updatable PCS

No!

⇒ 2-PHPE currently only realizable from heavy assumptions

Can we realize UPCS without 2-PHPE?

Non-Interactive Updatable PCS

No!

⇒ 2-PHPE currently only realizable from heavy assumptions

Can we realize UPCS without 2-PHPE?

⇒ No, since UPCS implies 2-PHPE

Non-Interactive Updatable PCS

No!

⇒ 2-PHPE currently only realizable from heavy assumptions

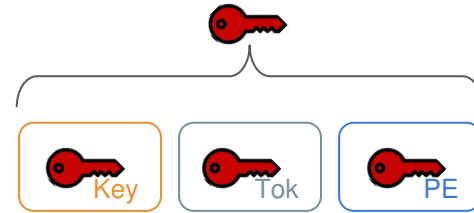
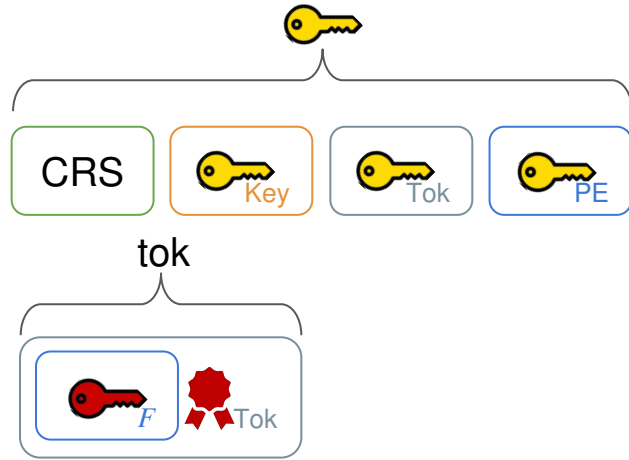
Can we realize UPCS without 2-PHPE?

⇒ No, since UPCS implies 2-PHPE

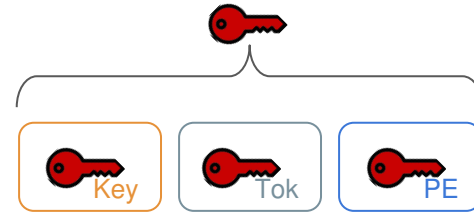
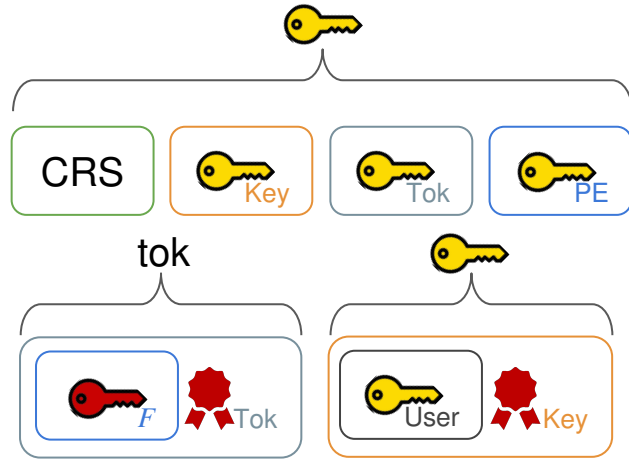
Solution: use interaction and PE for policy evaluation

Interactive Updatable PCS

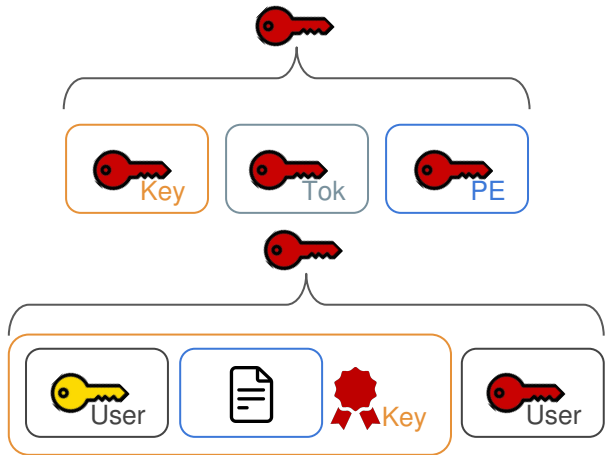
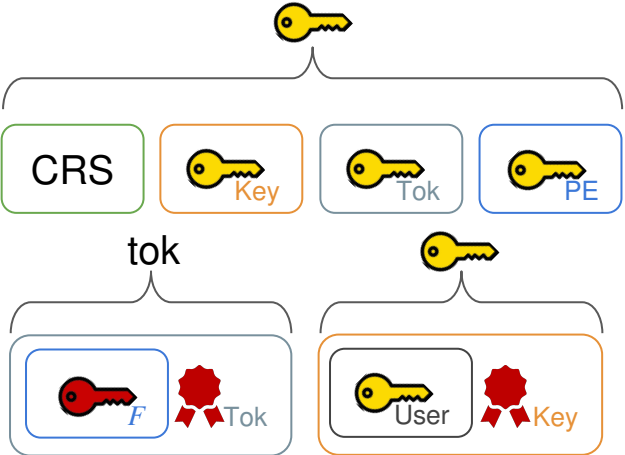
Interactive Updatable PCS



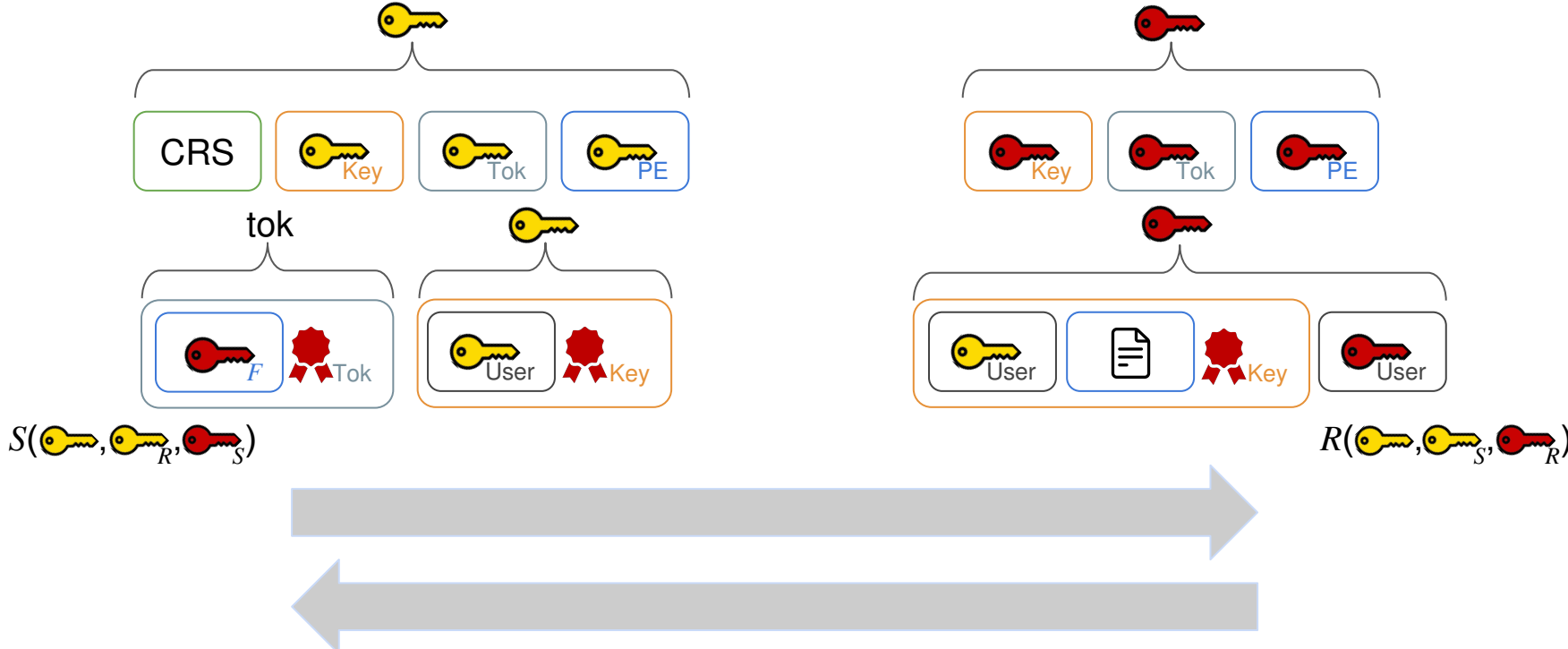
Interactive Updatable PCS



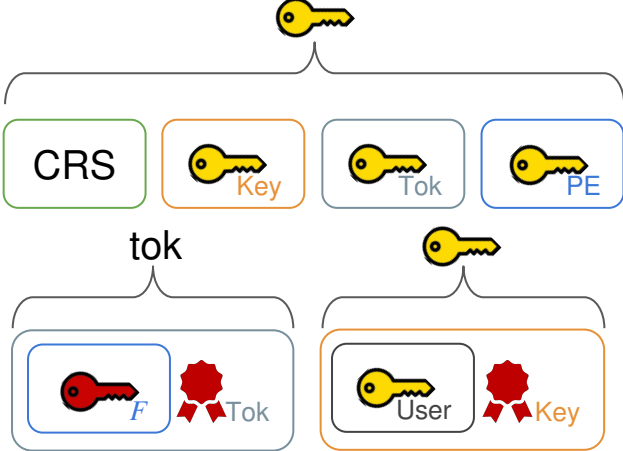
Interactive Updatable PCS



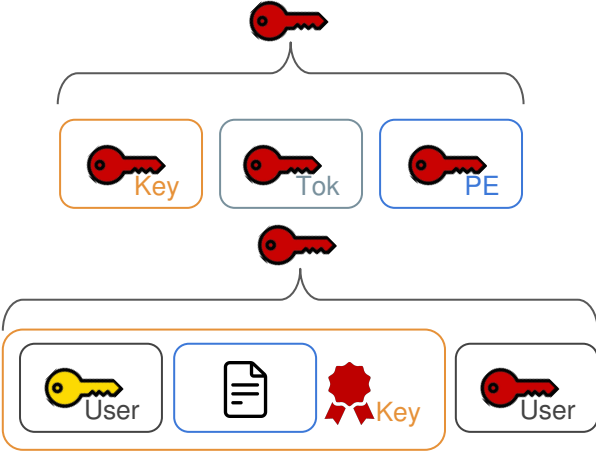
Interactive Updatable PCS



Interactive Updatable PCS



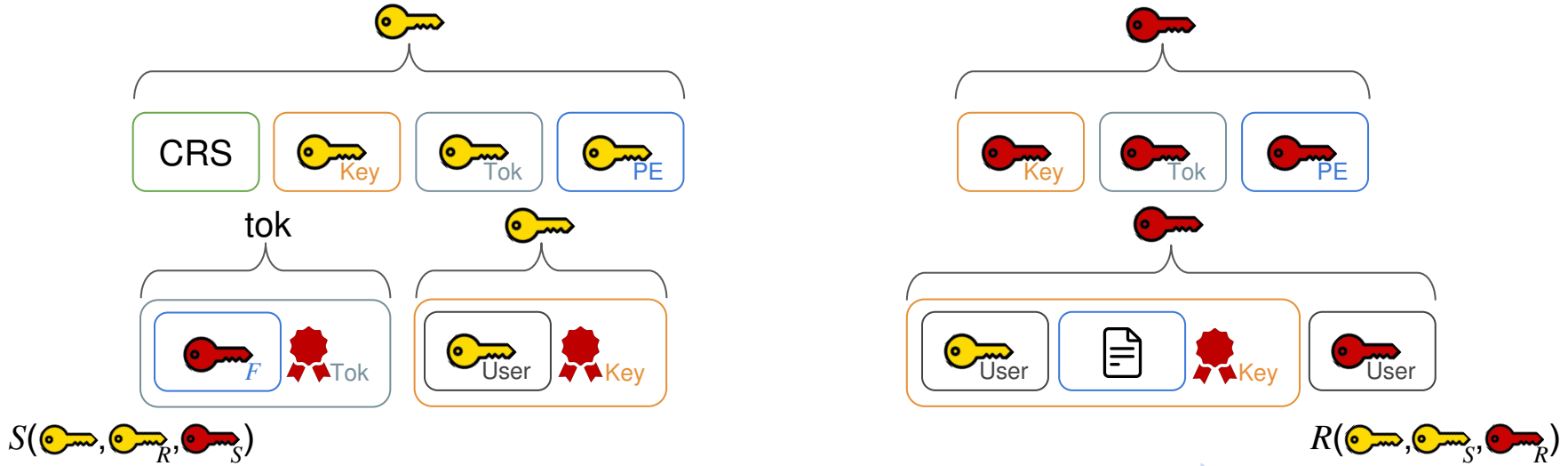
$S(\text{yellow key}, \text{yellow key}_R, \text{red key}_S)$



$R(\text{yellow key}, \text{yellow key}_S, \text{red key}_R)$

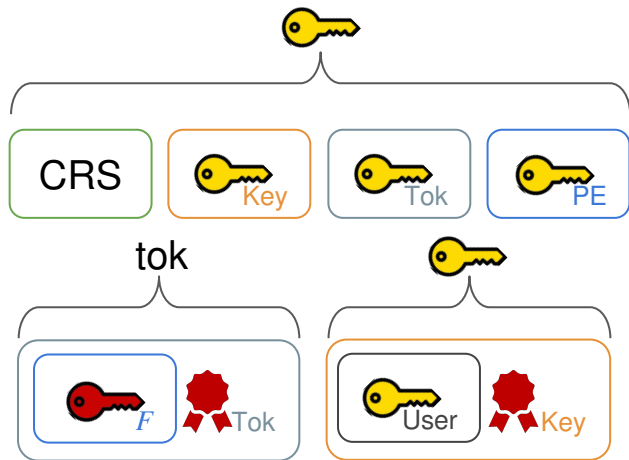
Verify $\text{yellow key}_S, \text{yellow key}_R$ and compute $\text{lock} = \text{Enc}(\text{yellow key}_{PE}, (\text{document}_S, \text{document}_R))$

Interactive Updatable PCS

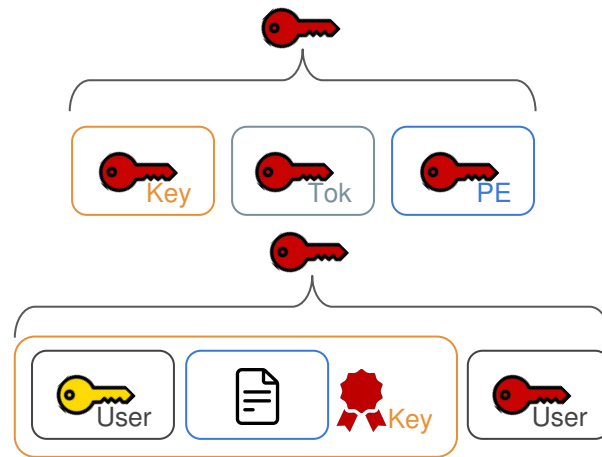


Verify $\text{yellow key}_S, \text{yellow key}_R$ and compute $\text{locked doc} = \text{Enc}(\text{yellow key}_{PE}, (\text{doc}_S, \text{doc}_R))$
 Output locked doc and a proof π of the computation

Interactive Updatable PCS



$S(\text{key}_S, \text{key}_R, \text{key}_S)$

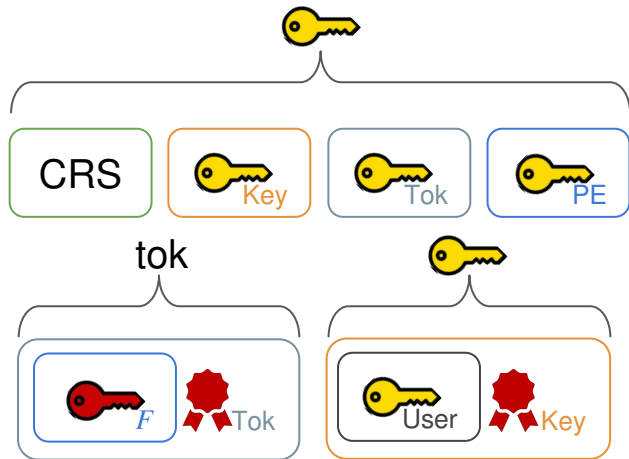


$R(\text{key}_S, \text{key}_S, \text{key}_R)$

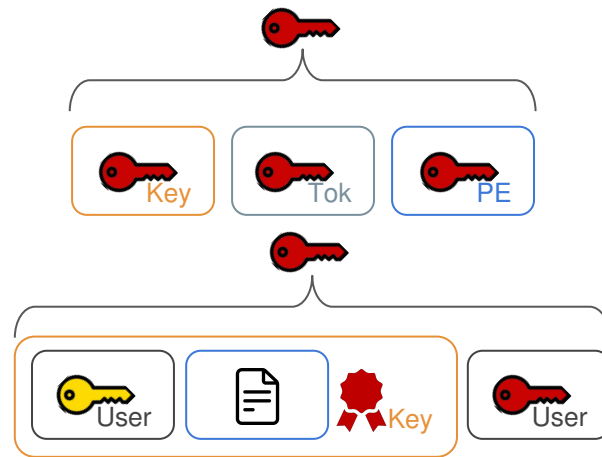
π' :
 $\text{Dec}(\text{key}_F, \text{msg}) = 1 \wedge$
 $\text{Verify}(\text{CRS}, \pi) = 1$

Verify $\text{key}_S, \text{key}_R$ and compute $\text{msg} = \text{Enc}(\text{key}_{PE}, (\text{msg}_S, \text{msg}_R))$
 Output msg and a proof π of the computation

Interactive Updatable PCS



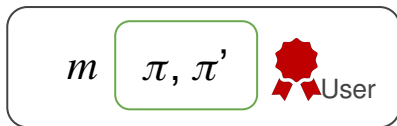
$$S(\text{key}, \text{key}_R, \text{key}_S)$$



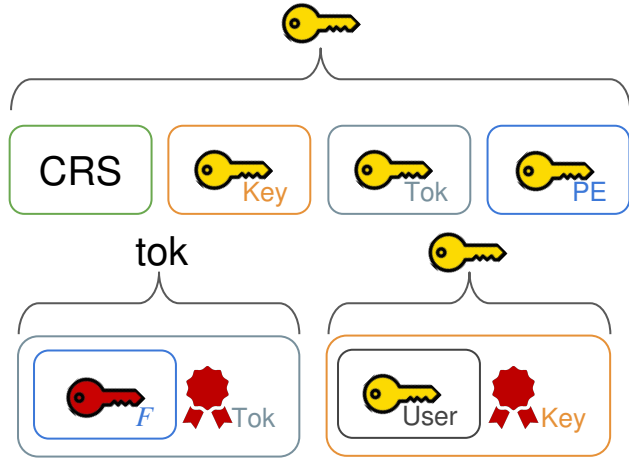
$$R(\text{key}, \text{key}_S, \text{key}_R)$$

$$\text{Dec}(\text{key}_F, \text{enc}) = 1 \wedge \text{Verify}(\text{CRS}, \pi) = 1$$

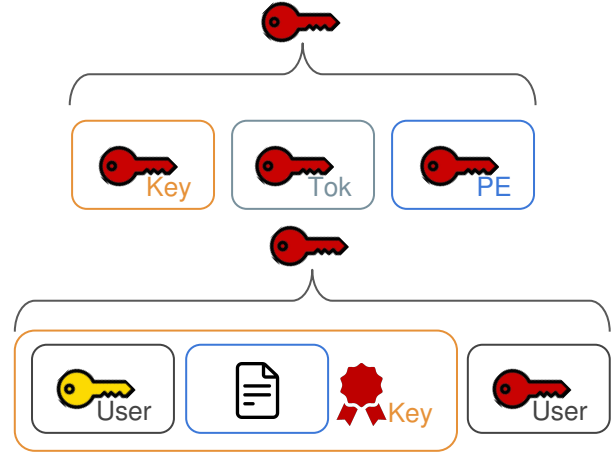
Verify $\text{key}_S, \text{key}_R$ and compute $\text{enc} = \text{Enc}(\text{key}_{PE}, (\text{doc}_S, \text{doc}_R))$
 Output enc and a proof π of the computation



Interactive Updatable PCS



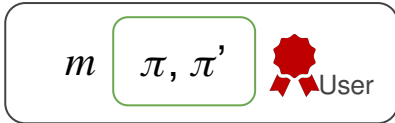
$S(\text{key}, \text{key}_R, \text{key}_S)$



$R(\text{key}, \text{key}_S, \text{key}_R)$

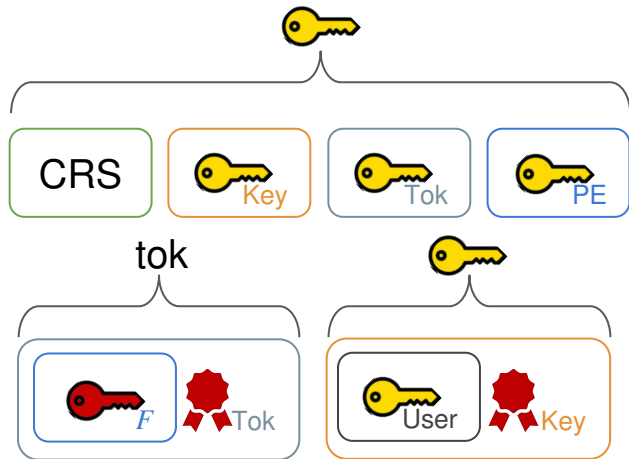
π' :
 $\text{Dec}(\text{key}_F, \text{msg}) = 1 \wedge$
 $\text{Verify}(\text{CRS}, \pi) = 1$

Verify $\text{key}_S, \text{key}_R$ and compute $\text{msg} = \text{Enc}(\text{key}_{PE}, (\text{msg}_S, \text{msg}_R))$
 Output msg and a proof π of the computation

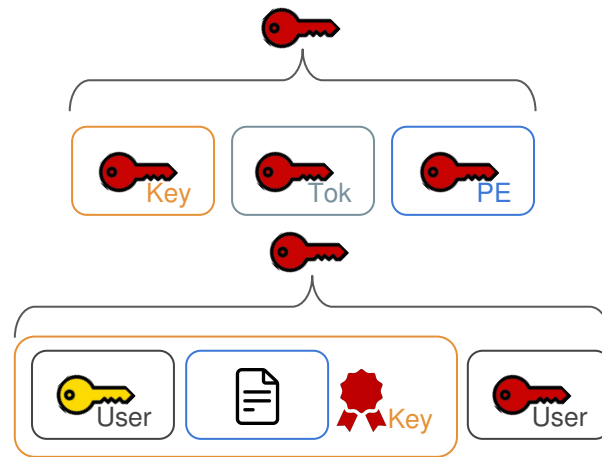


Requires recursion

Interactive Updatable PCS



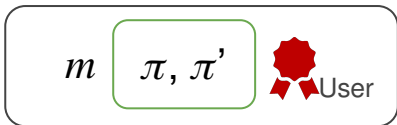
$$S(\text{key}_S, \text{key}_R, \text{key}_S)$$



$$R(\text{key}_S, \text{key}_S, \text{key}_R)$$

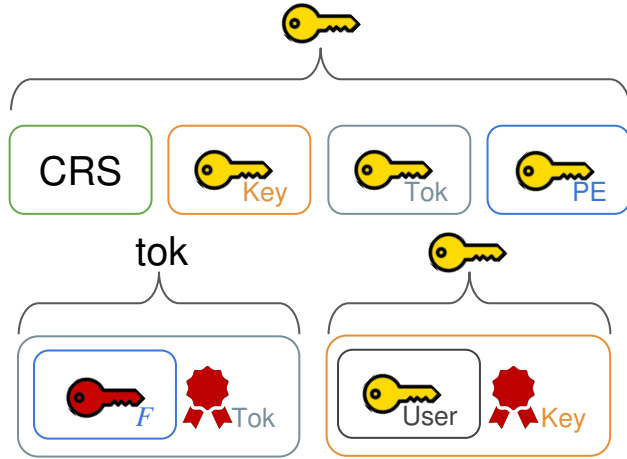
Verify $\text{key}_S, \text{key}_R$ and compute $\text{doc} = \text{Enc}(\text{key}_{PE}, (\text{doc}_S, \text{doc}_R))$
 Output doc and a proof π of the computation

$$\text{Dec}(\text{key}_F, \text{doc}) = 1 \wedge \text{Verify}(\text{CRS}, \pi) = 1$$

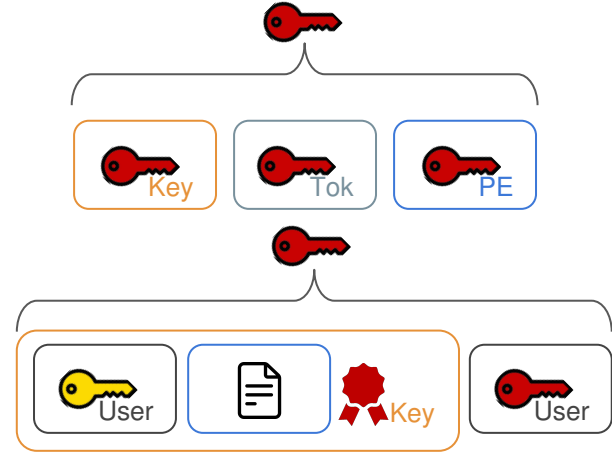


Requires recursion \rightarrow Use commitments

Interactive Updatable PCS



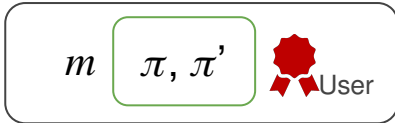
$S(\text{key}, \text{key}_R, \text{key}_S)$



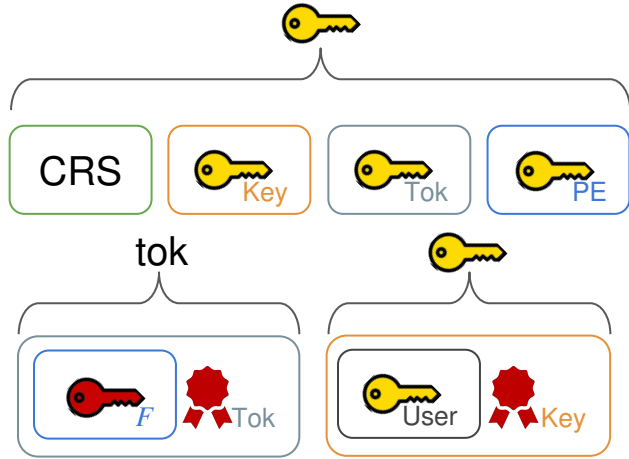
$R(\text{key}, \text{key}_S, \text{key}_R)$

Verify $\text{key}_S, \text{key}_R$ compute $\text{lock} = \text{Enc}(\text{key}_{PE}, (\text{doc}_S, \text{doc}_R))$ & $c = \text{Com}(\text{lock}, r)$
 Output c, r, lock and a proof π of the computation

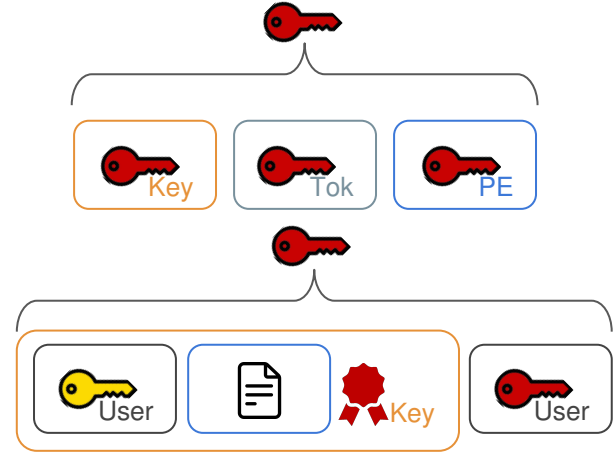
π' :
 $\text{Dec}(\text{key}_F, \text{lock}) = 1 \wedge$
 $\text{Verify}(\text{CRS}, \pi) = 1$



Interactive Updatable PCS



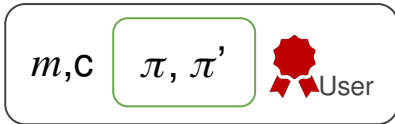
$S(\text{key}, \text{key}_R, \text{key}_S)$



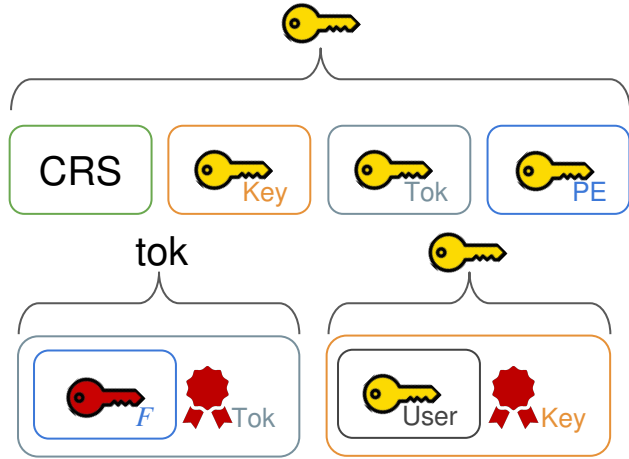
$R(\text{key}, \text{key}_S, \text{key}_R)$

Verify $\text{key}_S, \text{key}_R$ compute $\text{lock} = \text{Enc}(\text{key}_{PE}, (\text{doc}_S, \text{doc}_R))$ & $c = \text{Com}(\text{lock}, r)$
 Output c, r, lock and a proof π of the computation

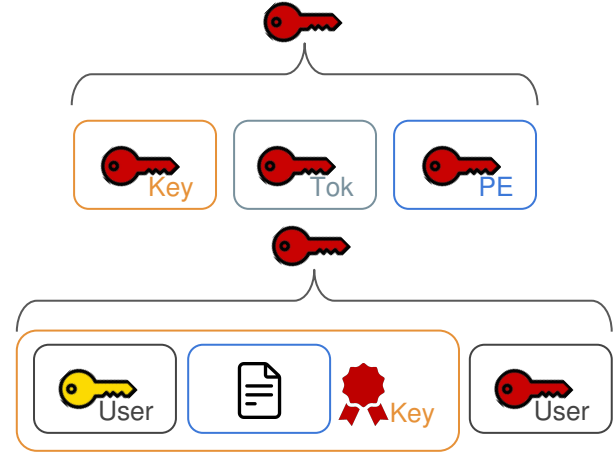
π' :
 $\text{Dec}(\text{key}_F, \text{lock}) = 1 \wedge$
 $\text{Com}(\text{lock}, r) = c$



Interactive Updatable PCS



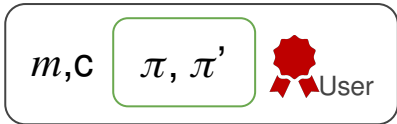
$S(\text{yellow key}, \text{yellow key}_R, \text{red key}_S)$



$R(\text{yellow key}, \text{yellow key}_S, \text{red key}_R)$

Verify $\text{yellow key}_S, \text{yellow key}_R$ compute $\text{lock} = \text{Enc}(\text{yellow key}_{PE}, (\text{document}_S, \text{document}_R))$ & $c = \text{Com}(\text{lock}, r)$
 Output c, r, lock and a proof π of the computation

π' :
 $\text{Dec}(\text{red key}_F, \text{lock}) = 1 \wedge$
 $\text{Com}(\text{lock}, r) = c$



Summary

1. Definition of Updatable Policy-Compliant Signatures

- Unforgeability
- Attribute Hiding

2. Non-Interactive Policy-Compliant Signature Scheme

- Two-Input (Partially-Hiding) Predicate Encryption \Leftrightarrow UPCS

3. Interactive Policy-Compliant Signature Scheme

Summary

1. Definition of Updatable Policy-Compliant Signatures

- Unforgeability
- Attribute Hiding

2. Non-Interactive Policy-Compliant Signature Scheme

- Two-Input (Partially-Hiding) Predicate Encryption \Leftrightarrow UPCS

3. Interactive Policy-Compliant Signature Scheme

Thanks! Questions?