Updatable Policy-Compliant Signatures

Christian Badertscher

IOHK

Monosij Maitra

IIT Kharagpur

Christian Matt

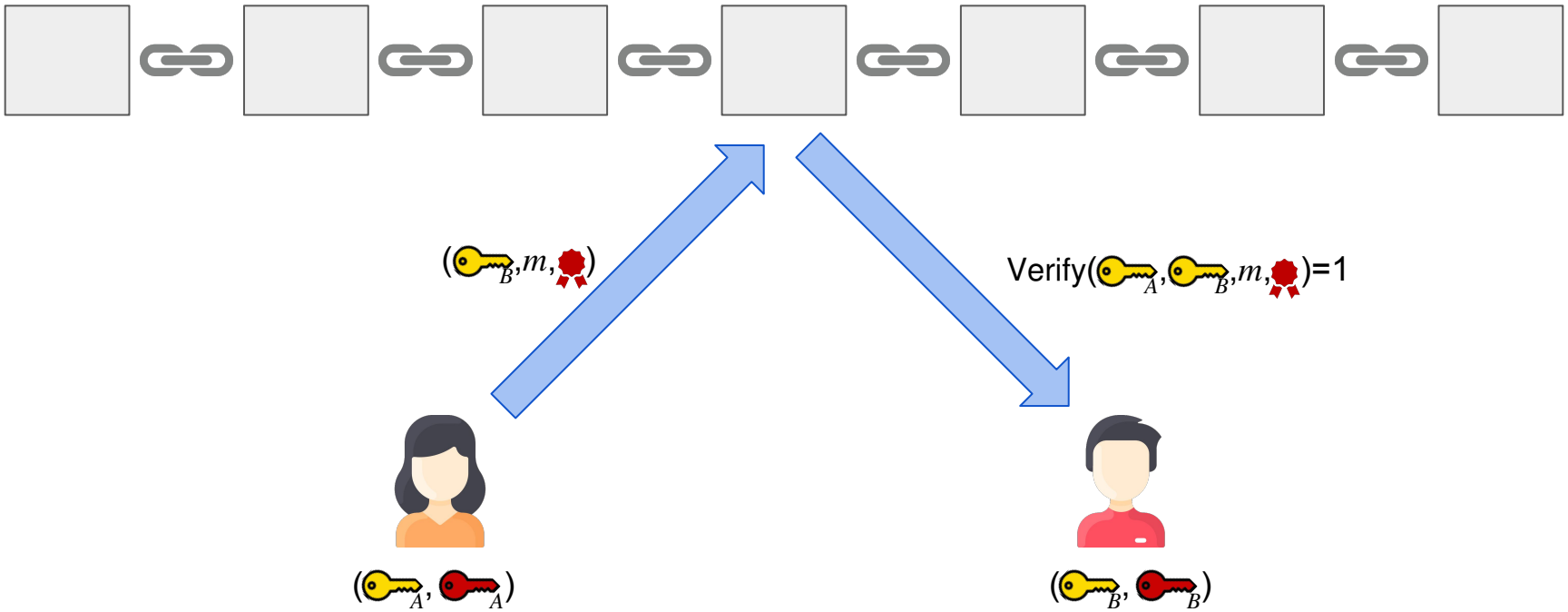
Primev

Hendrik Waldner

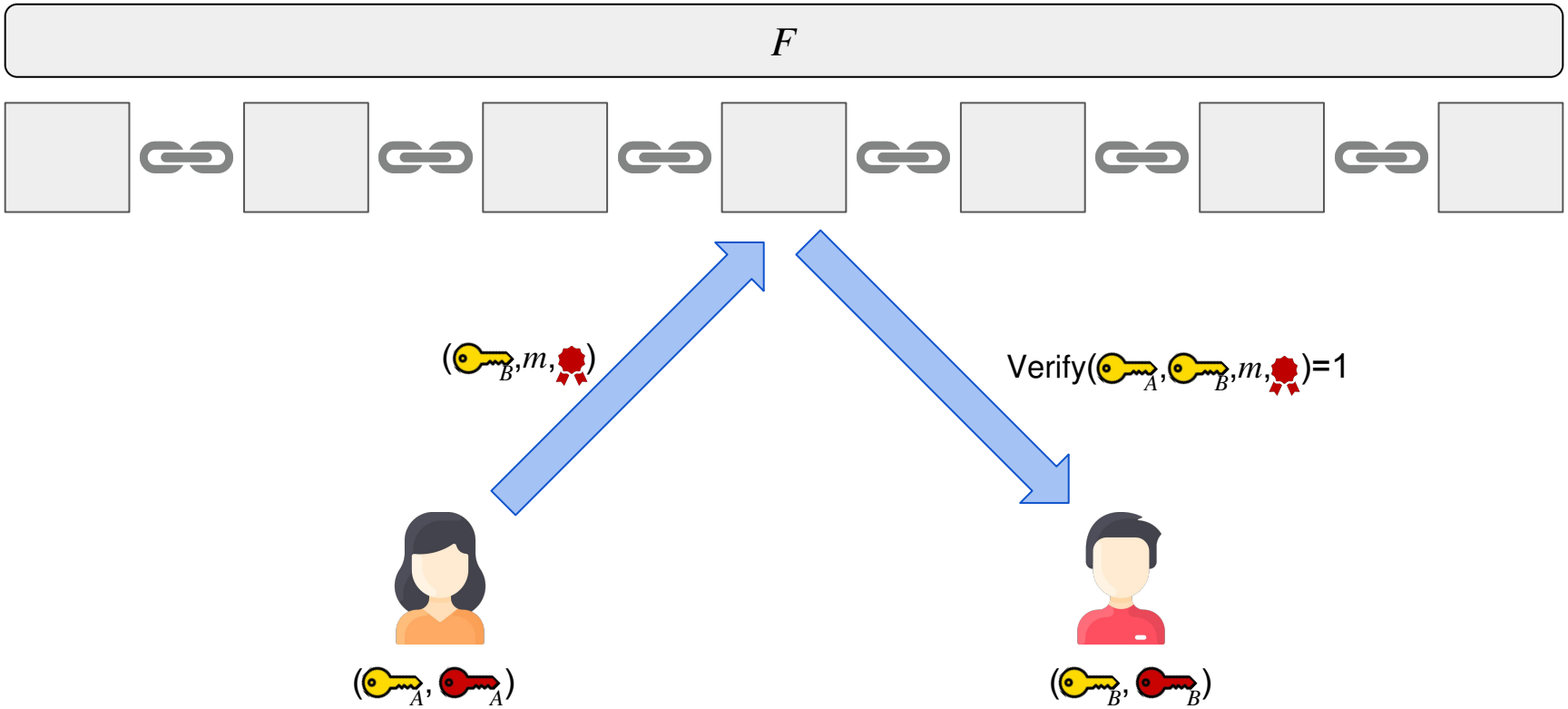
UMD

Motivation

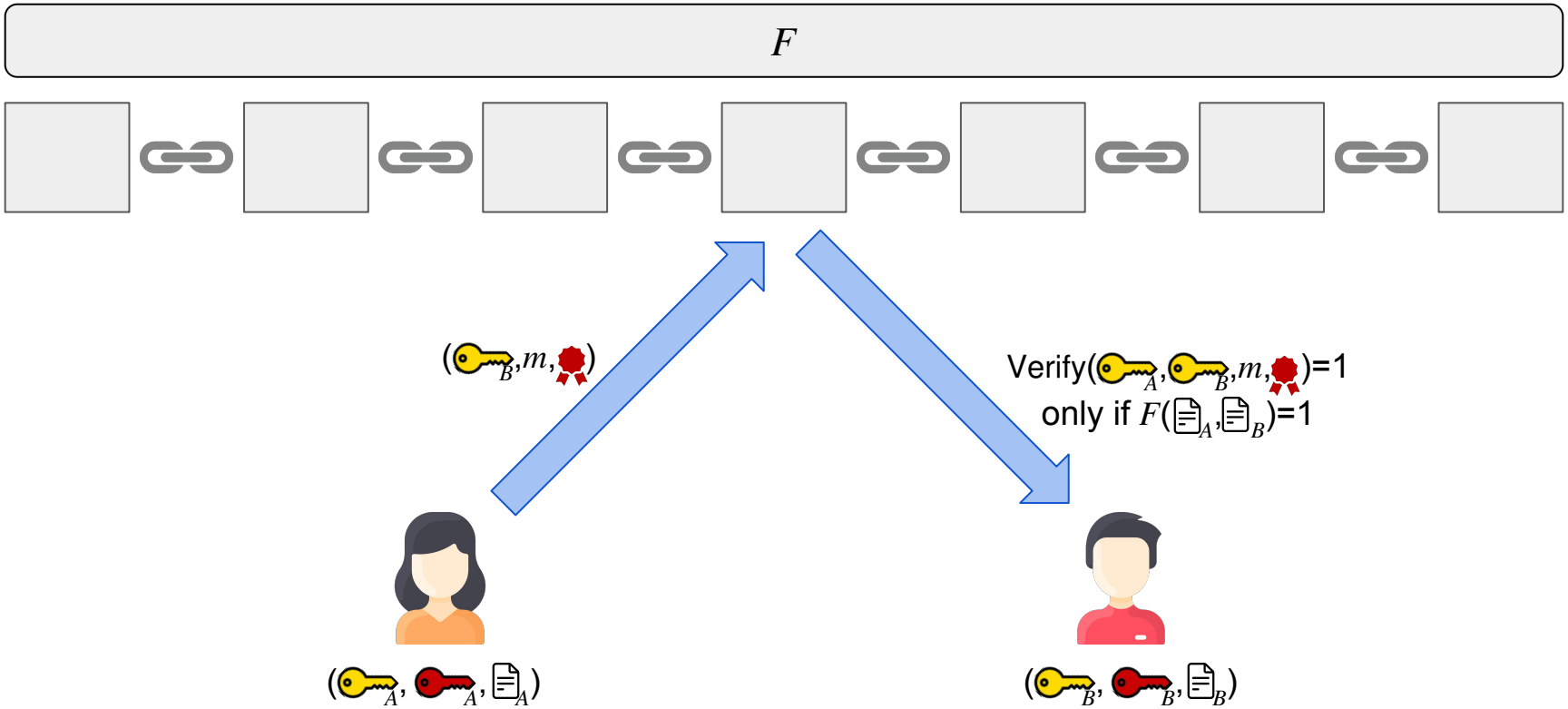
Motivation



Motivation

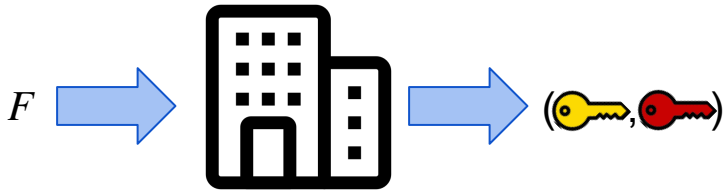


Motivation

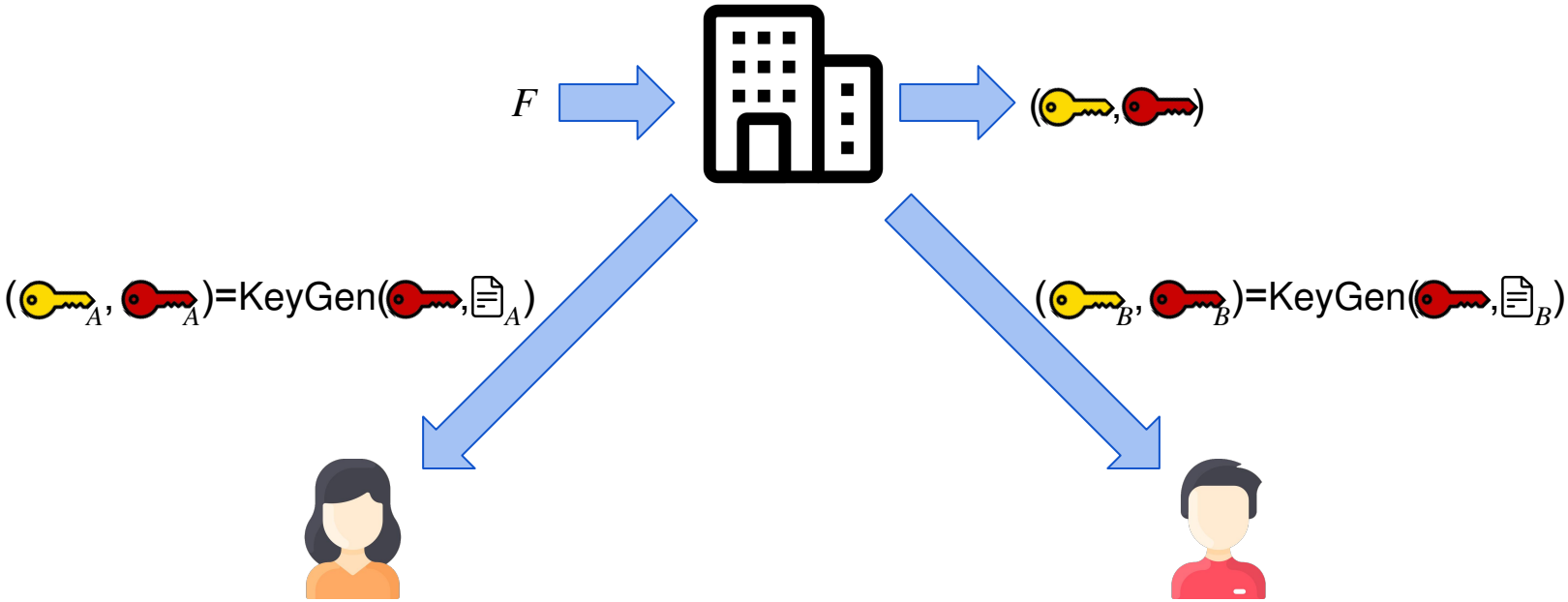


Policy-Compliant Signatures [BMW21]

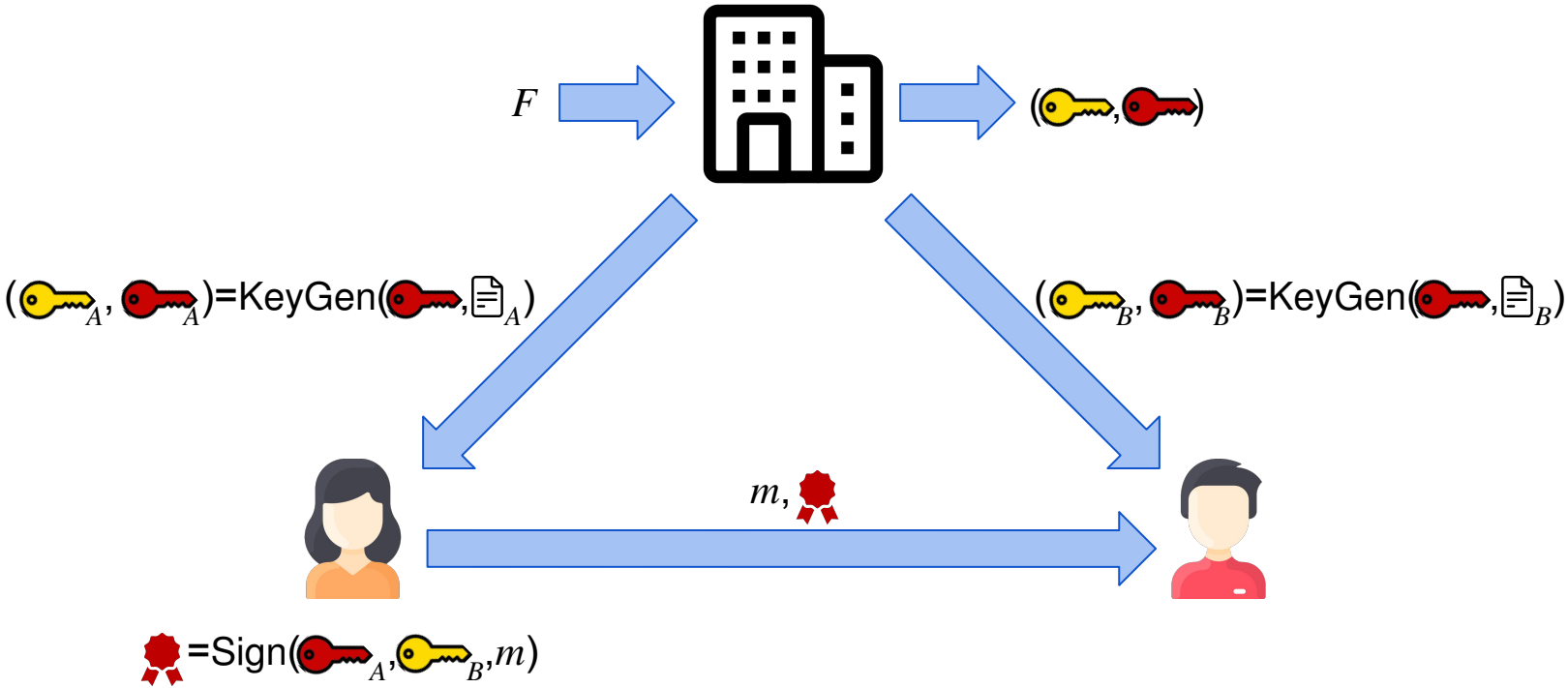
Policy-Compliant Signatures [BMW21]



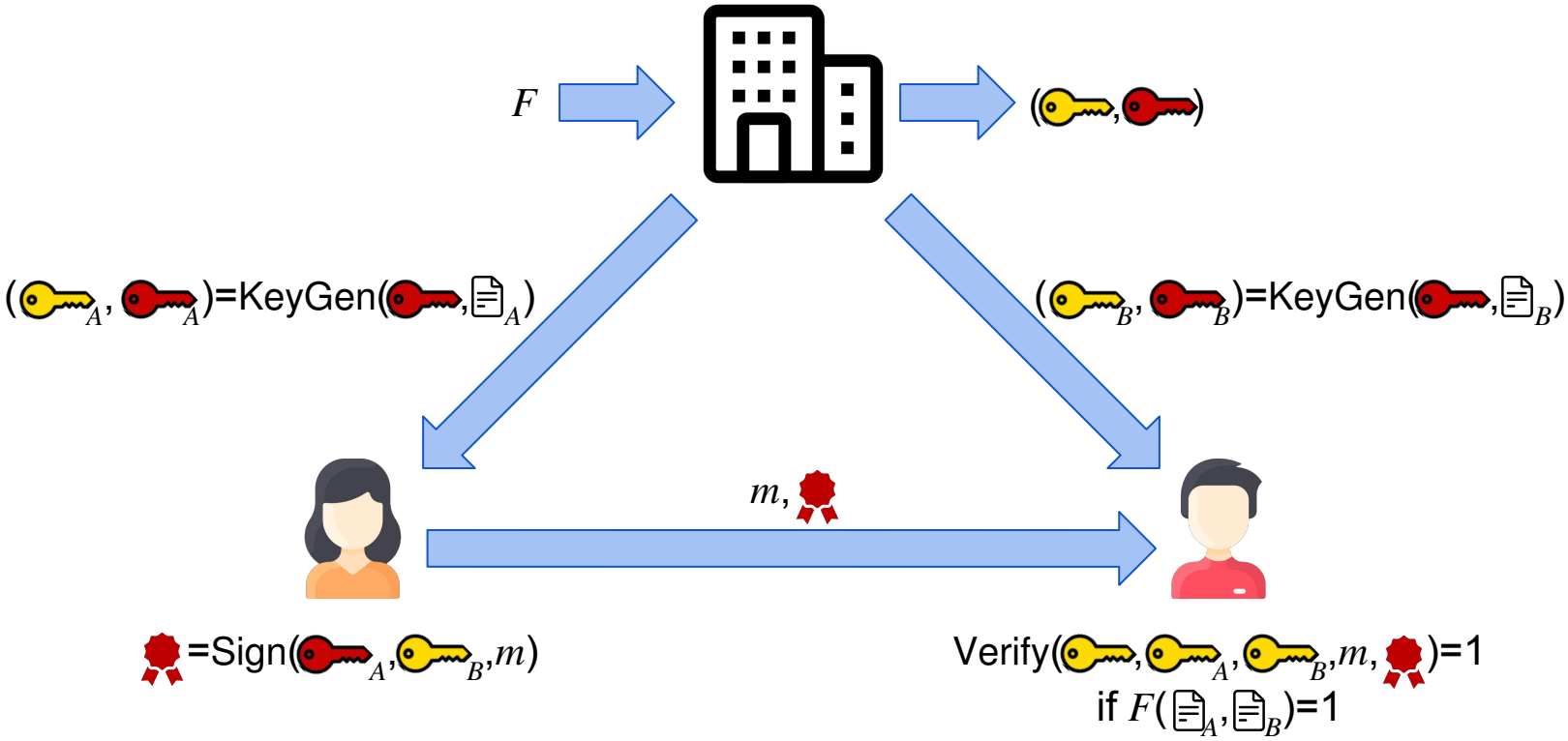
Policy-Compliant Signatures [BMW21]



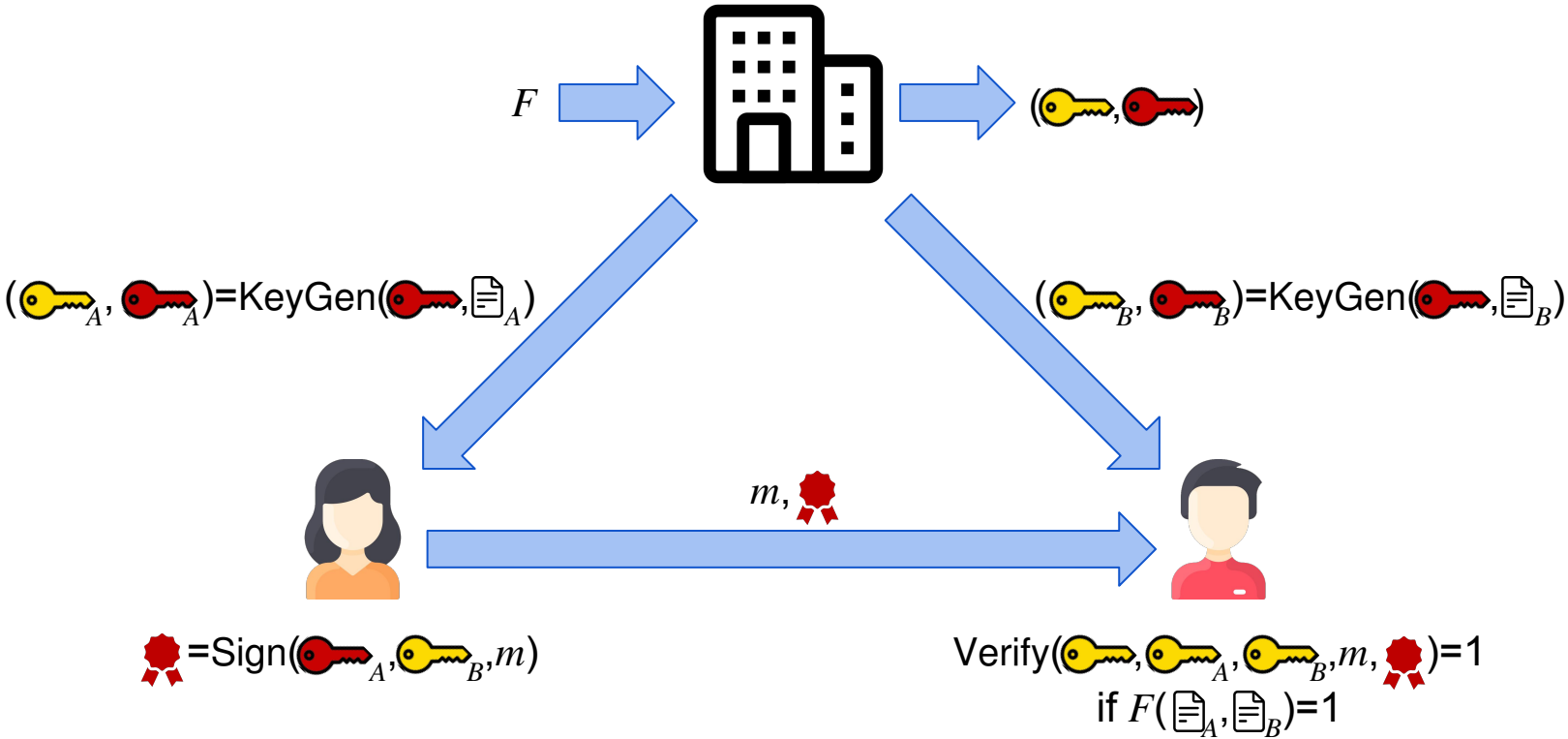
Policy-Compliant Signatures [BMW21]



Policy-Compliant Signatures [BMW21]

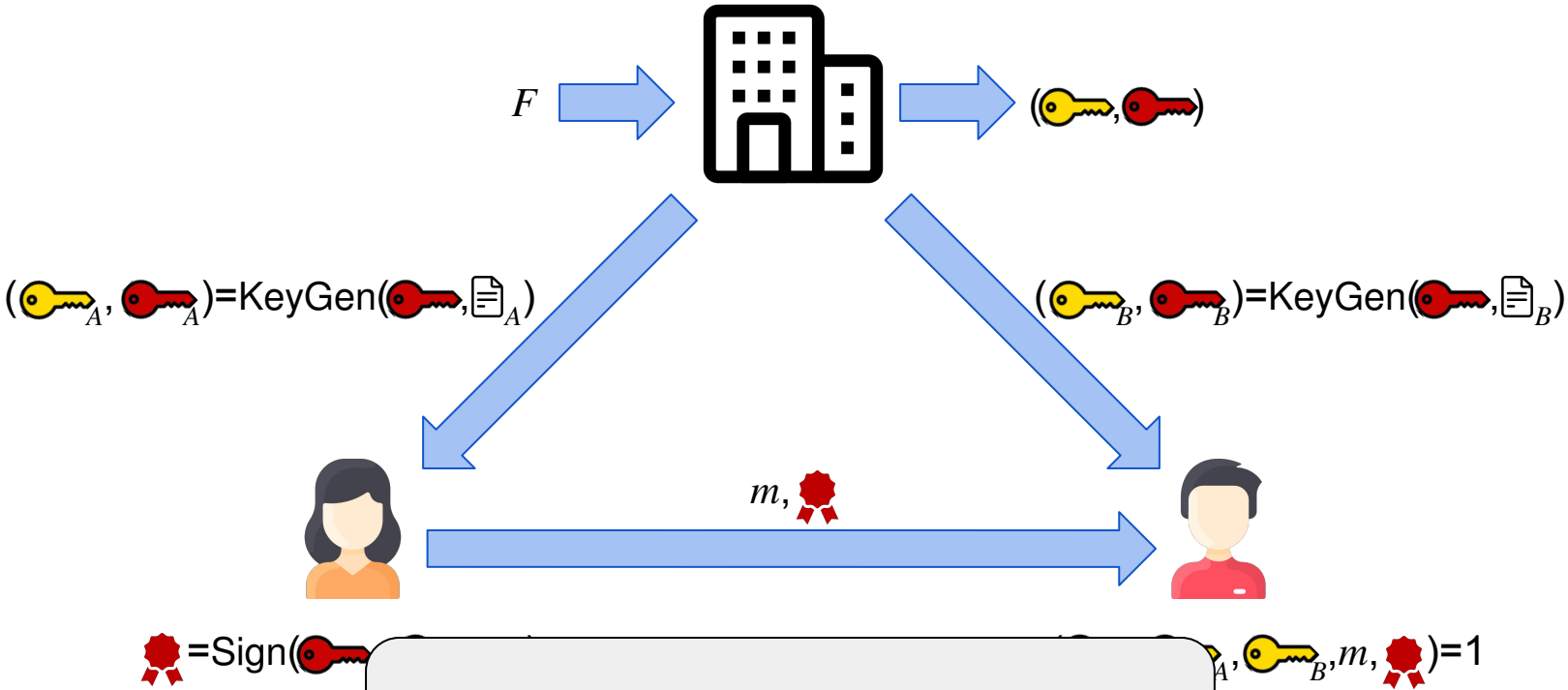


Policy-Compliant Signatures [BMW21]



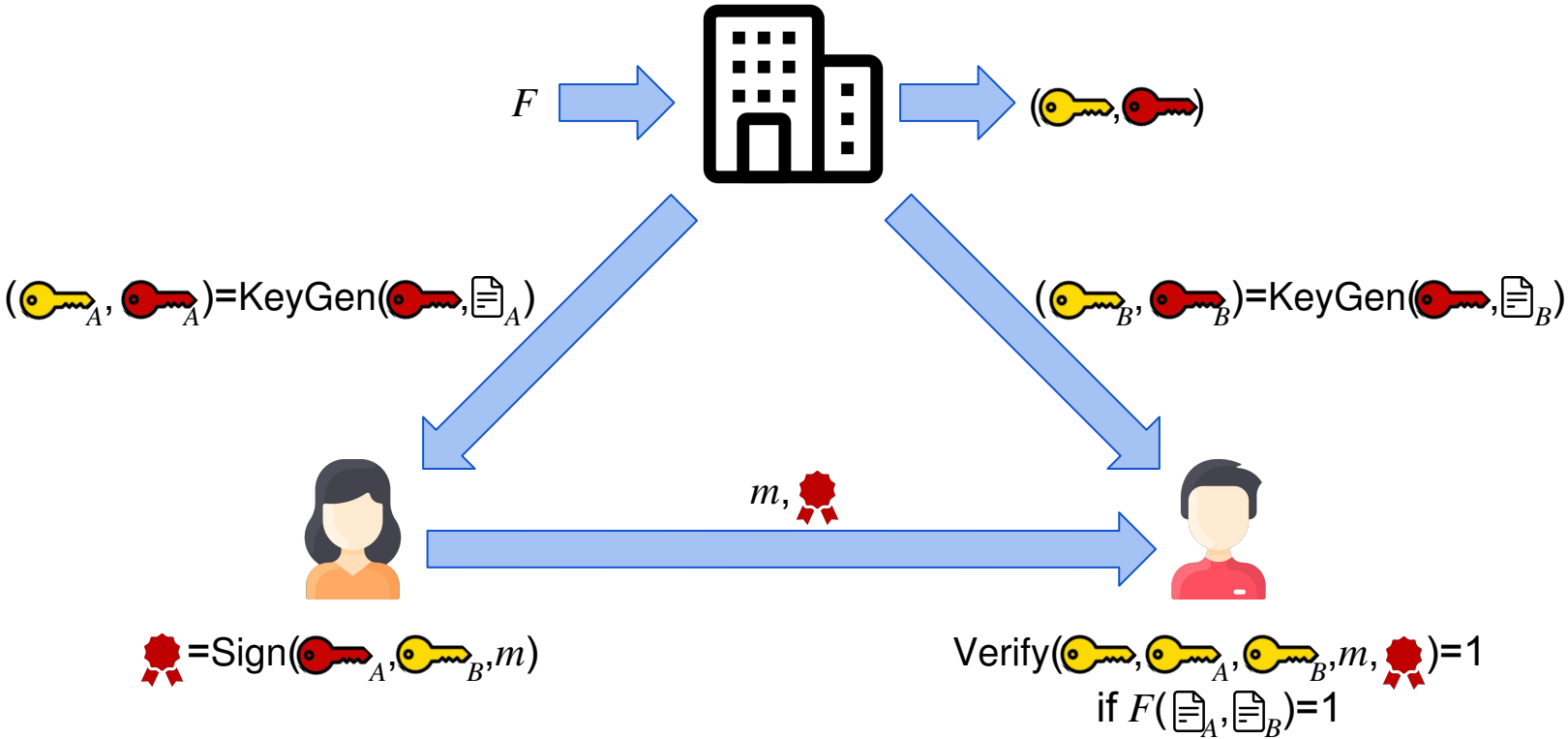
Unforgeability and Attribute-Hiding

Policy-Compliant Signatures [BMW21]



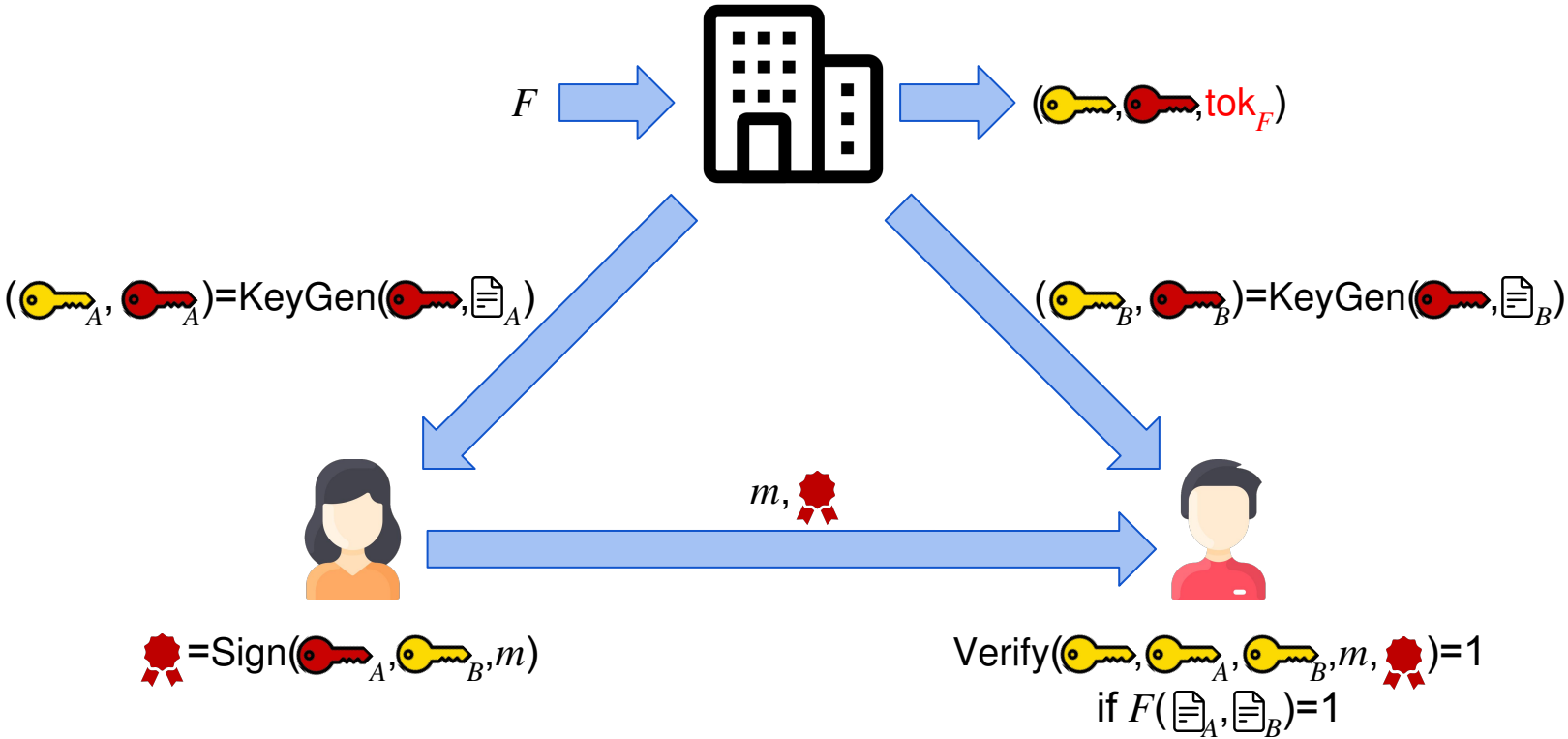
Unforgeability and

Updatable Policy-Compliant Signatures



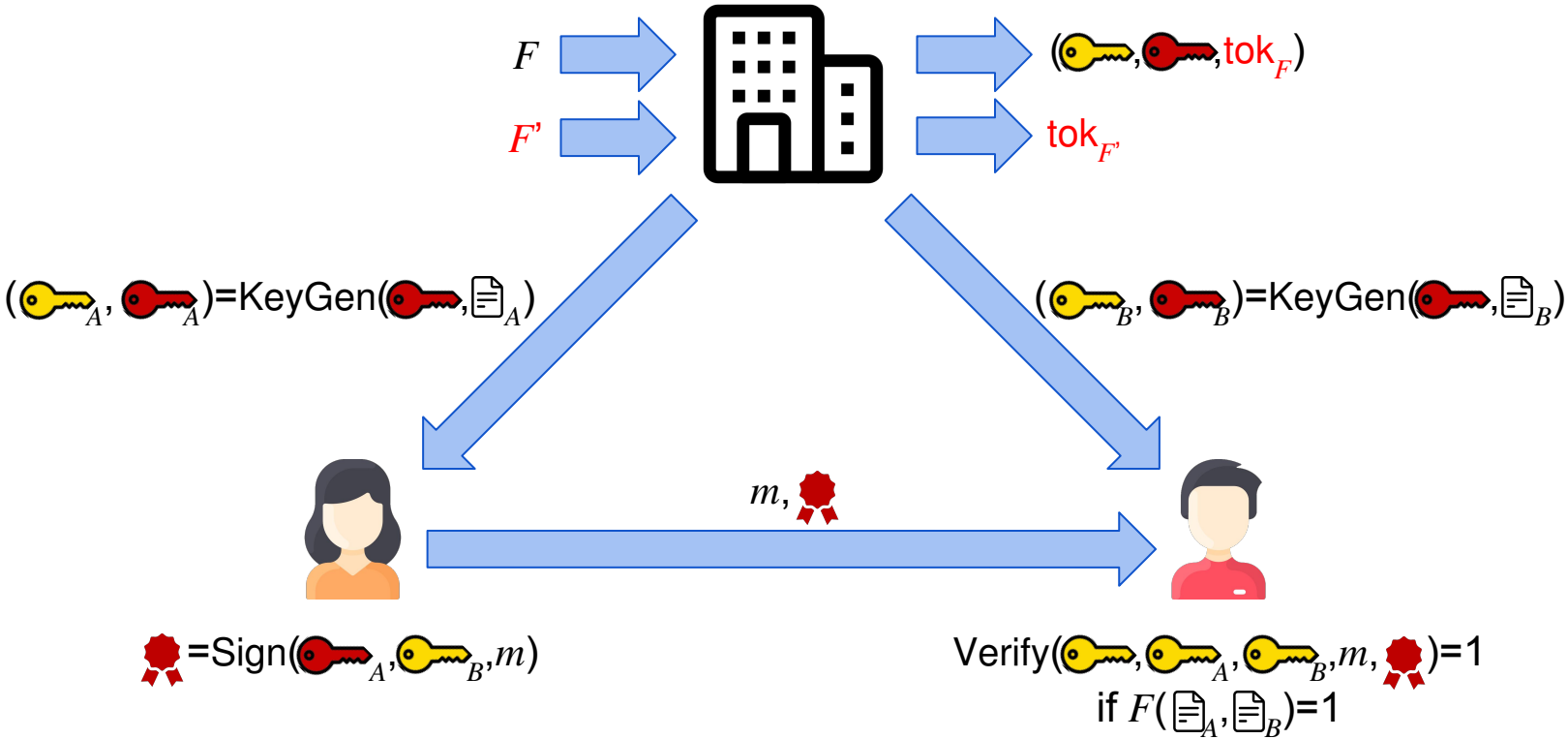
Unforgeability and Attribute-Hiding

Updatable Policy-Compliant Signatures



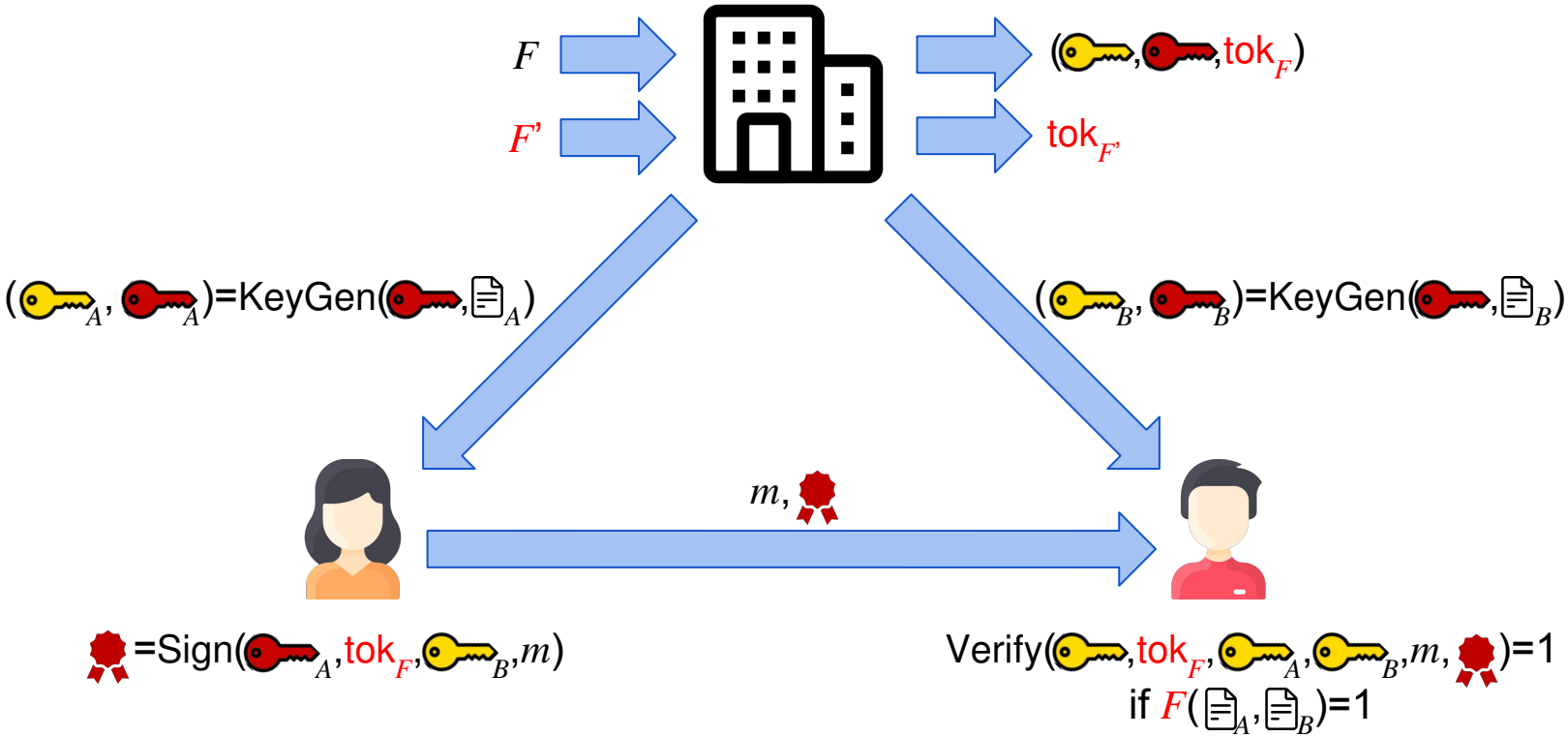
Unforgeability and Attribute-Hiding

Updatable Policy-Compliant Signatures



Unforgeability and Attribute-Hiding

Updatable Policy-Compliant Signatures

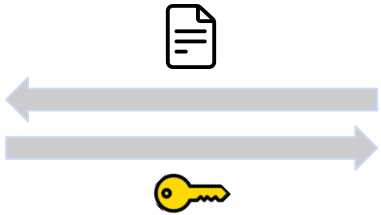


Unforgeability and Attribute-Hiding

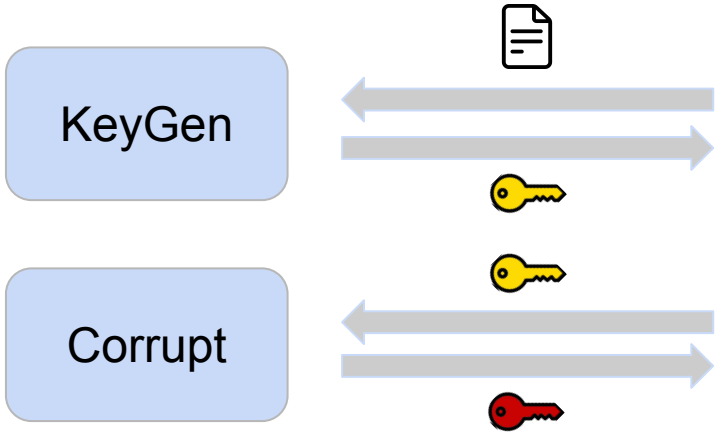
Unforgeability

Unforgeability

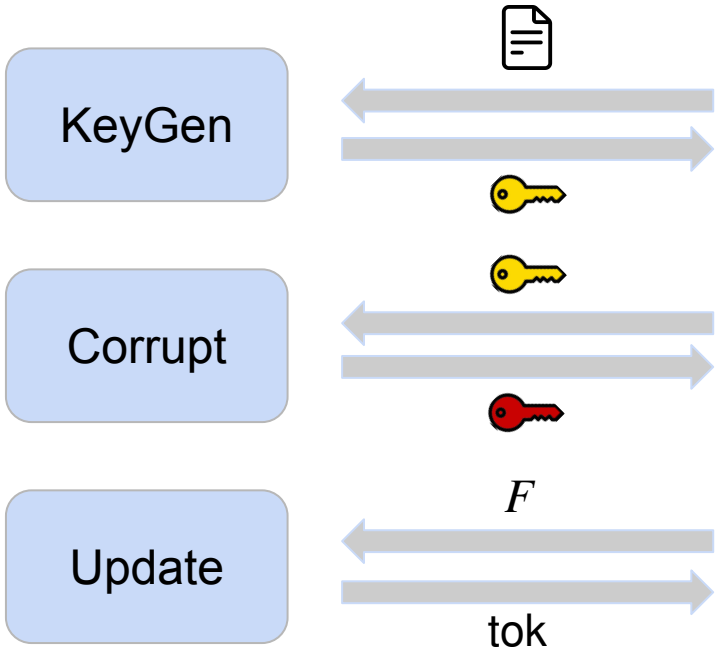
KeyGen



Unforgeability



Unforgeability



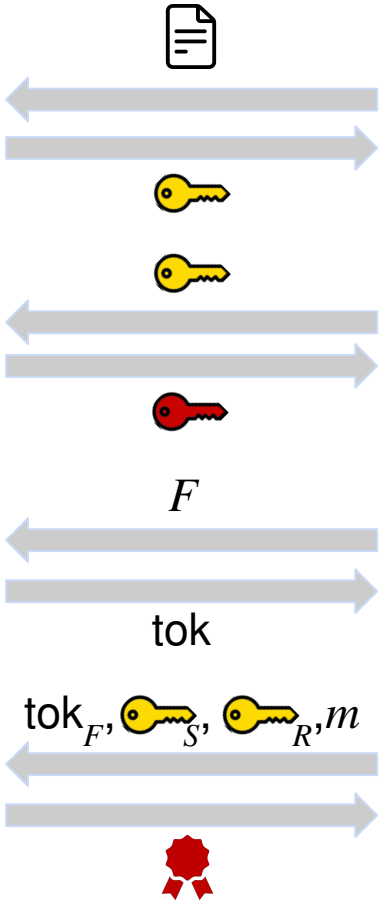
Unforgeability

KeyGen

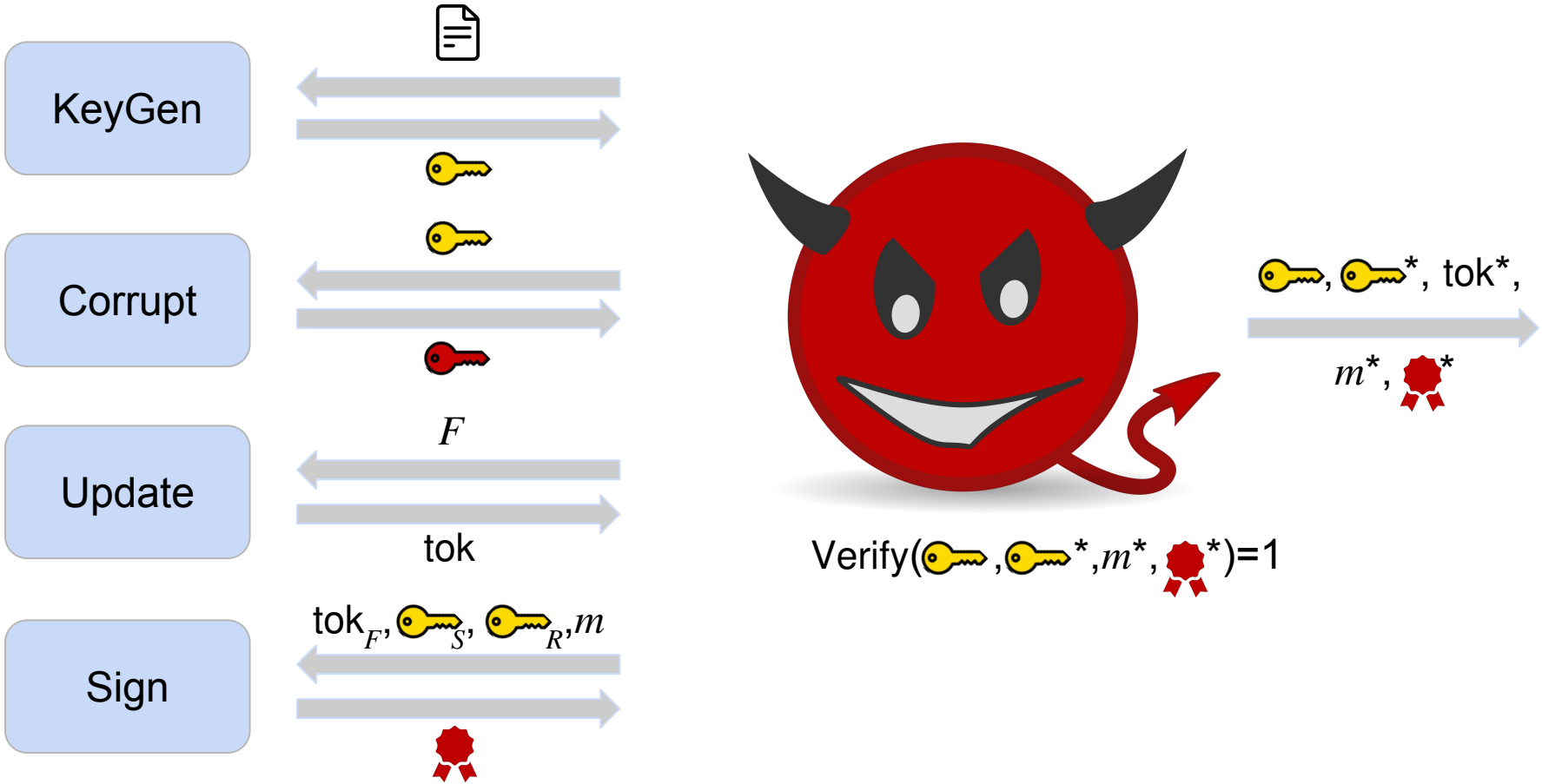
Corrupt

Update

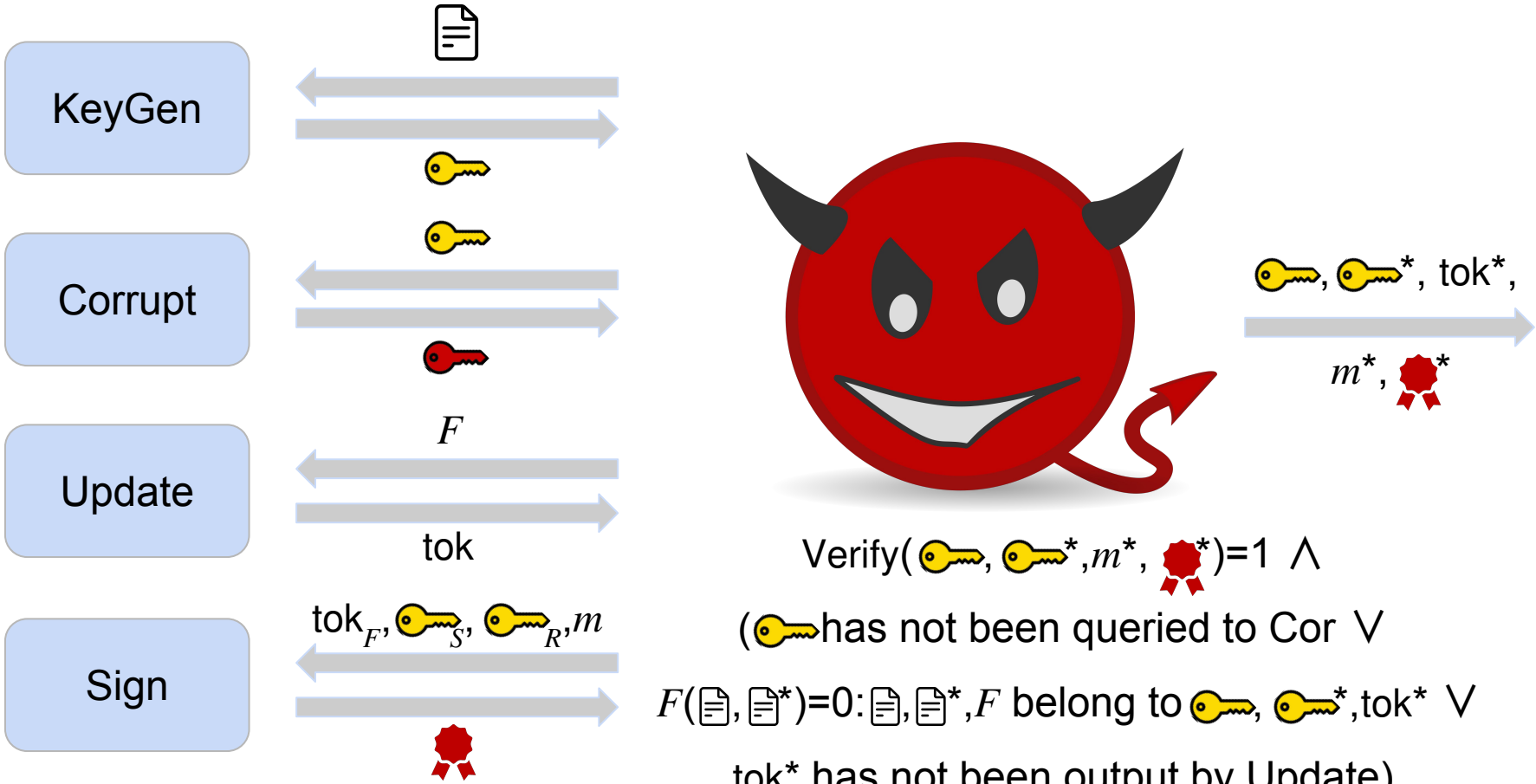
Sign



Unforgeability



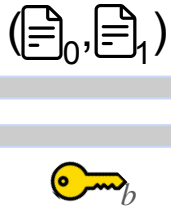
Unforgeability



Attribute Hiding

Attribute Hiding

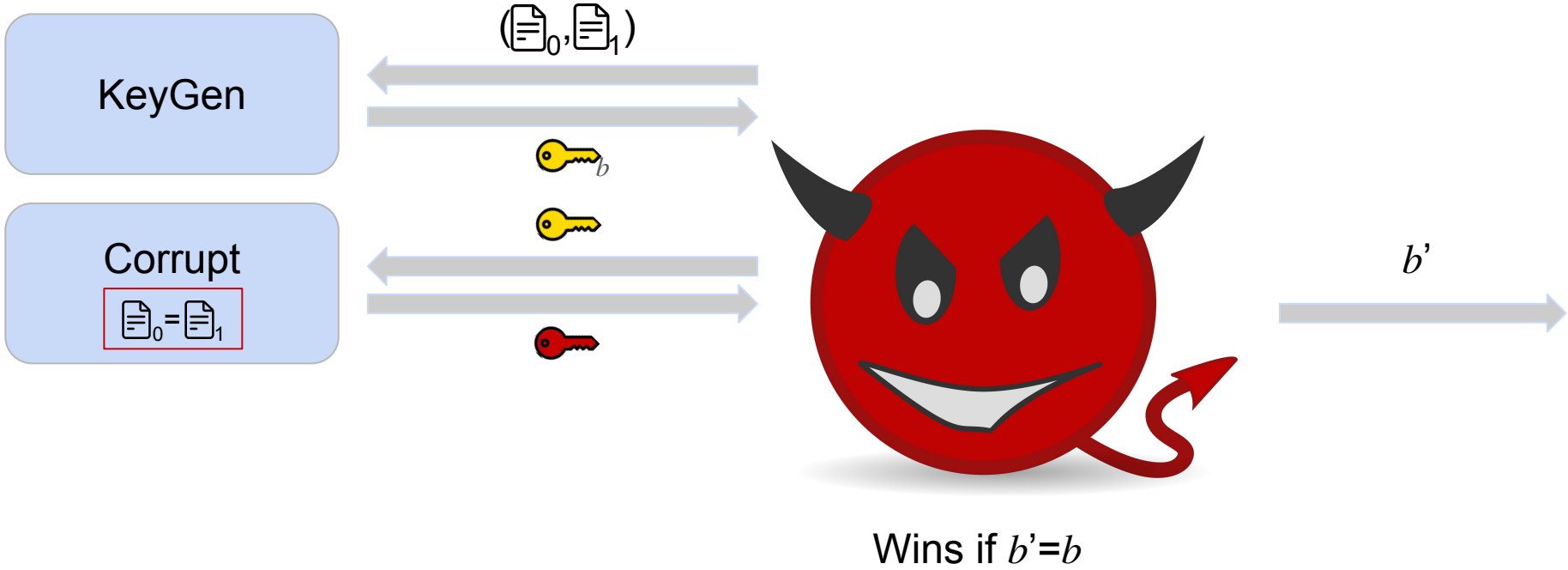
KeyGen



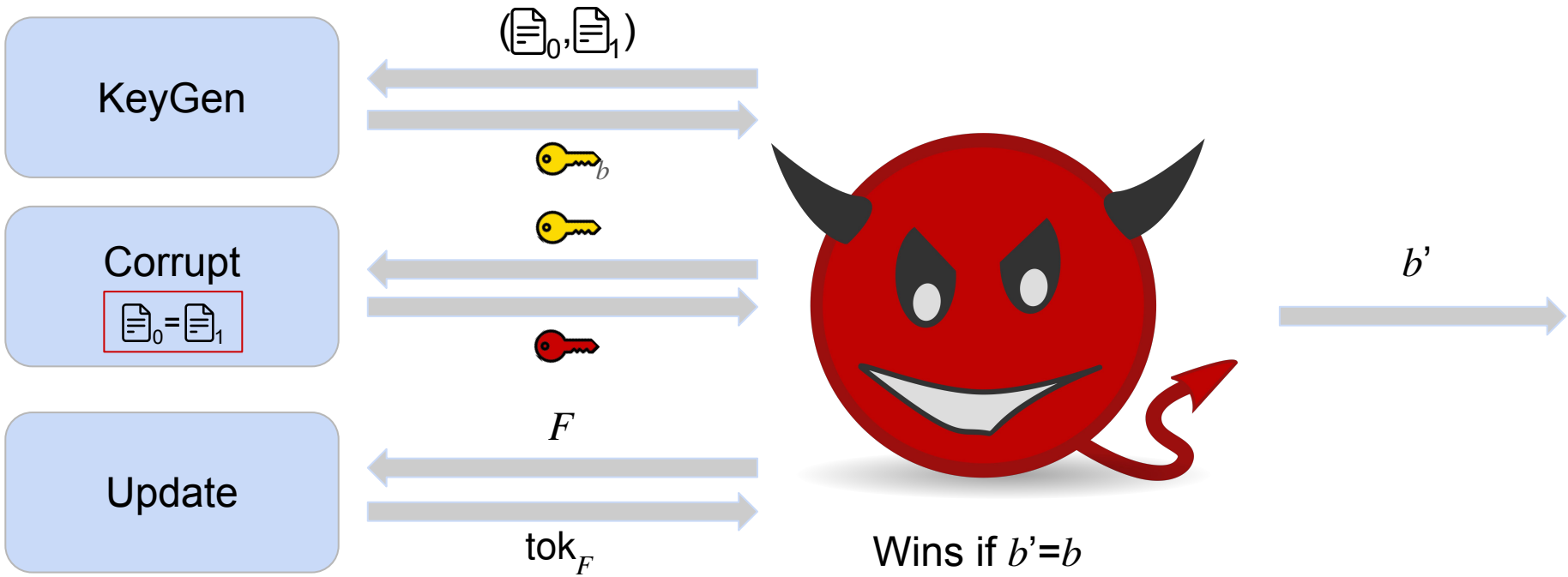
b’

Wins if b’=b

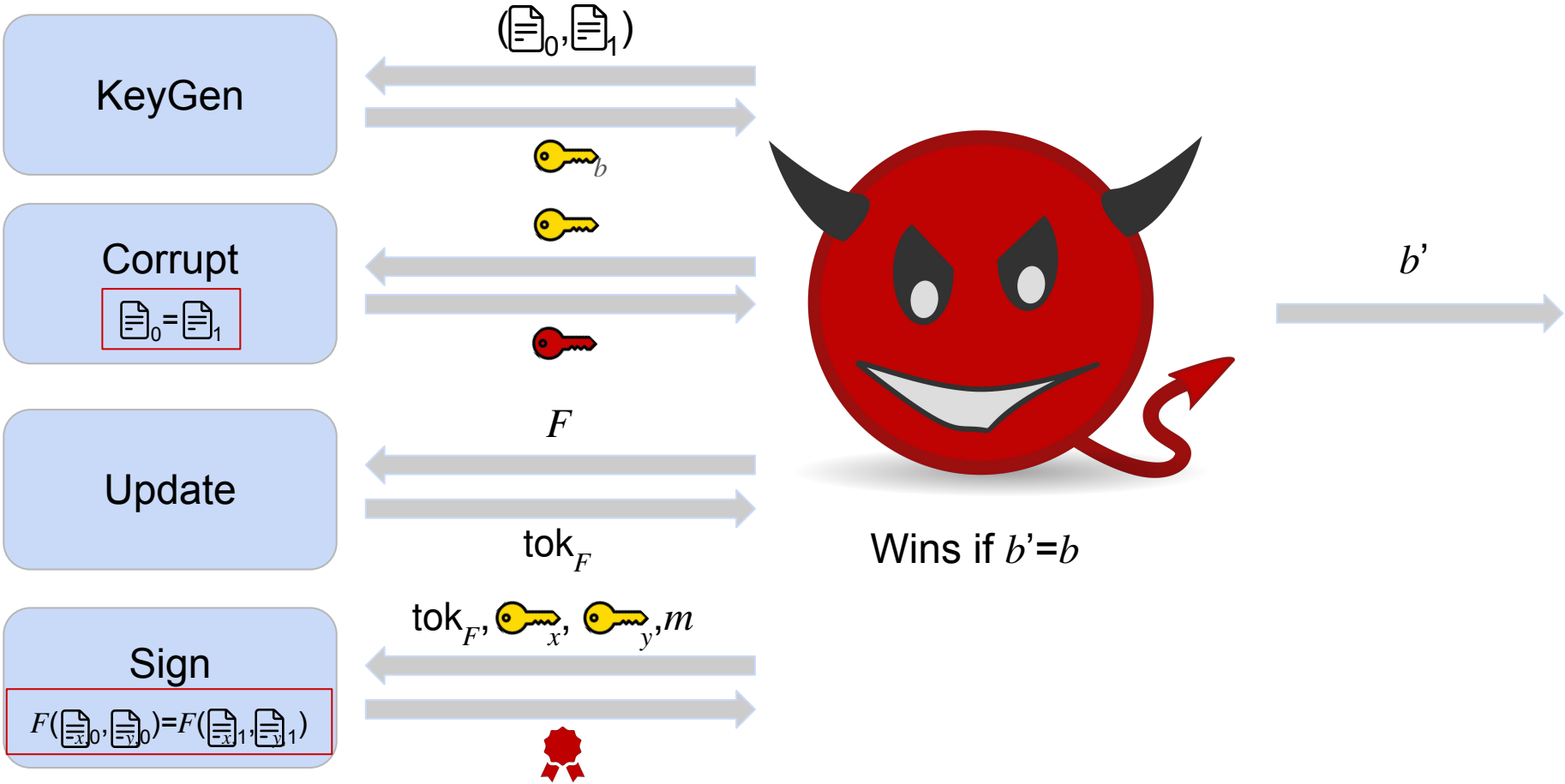
Attribute Hiding



Attribute Hiding

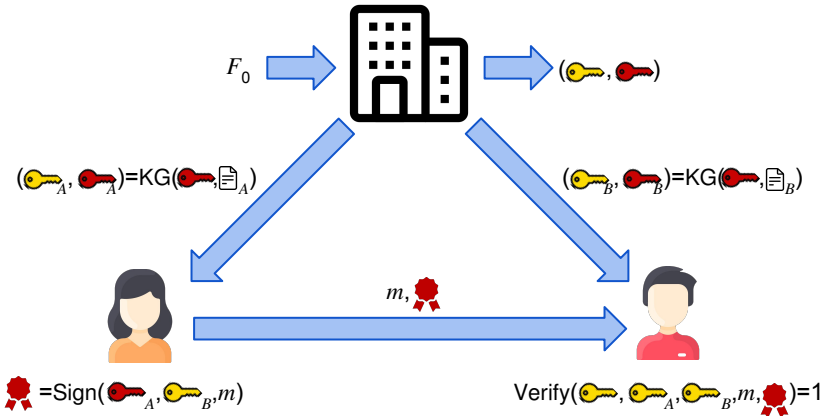


Attribute Hiding

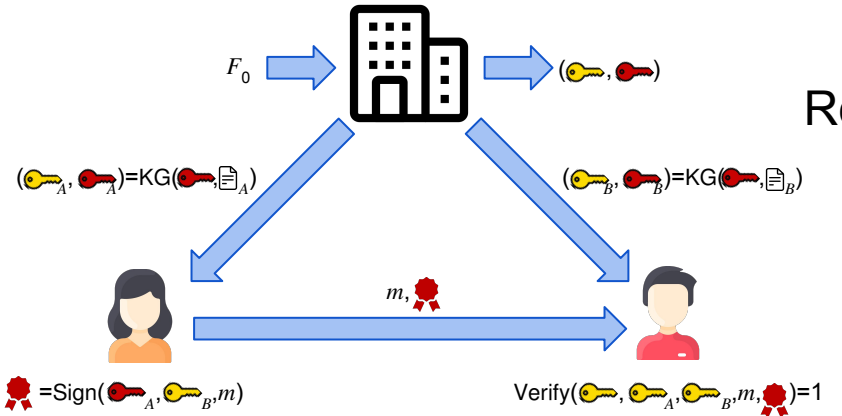


Naive Approach

Naive Approach



Naive Approach

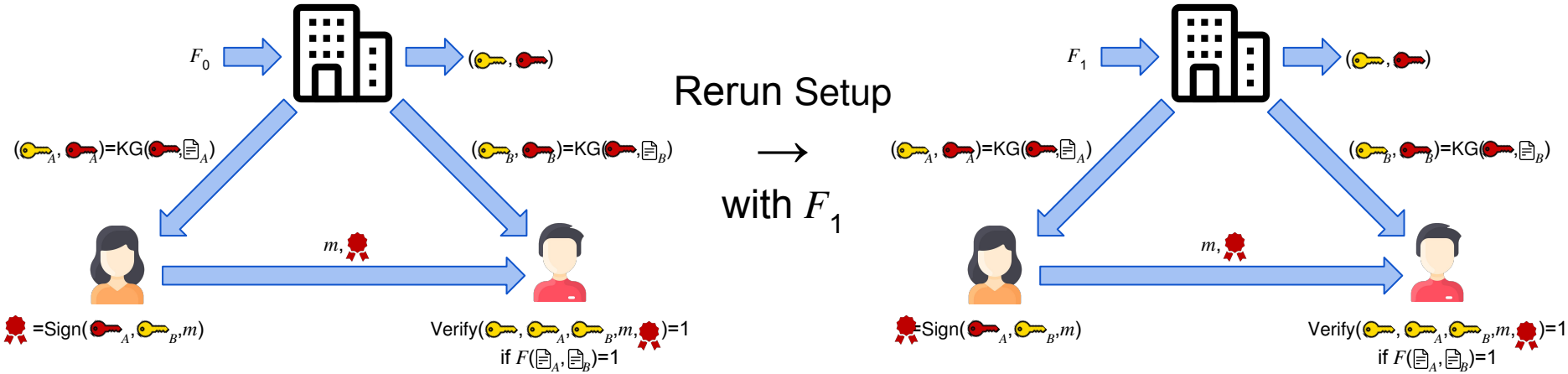


Rerun Setup

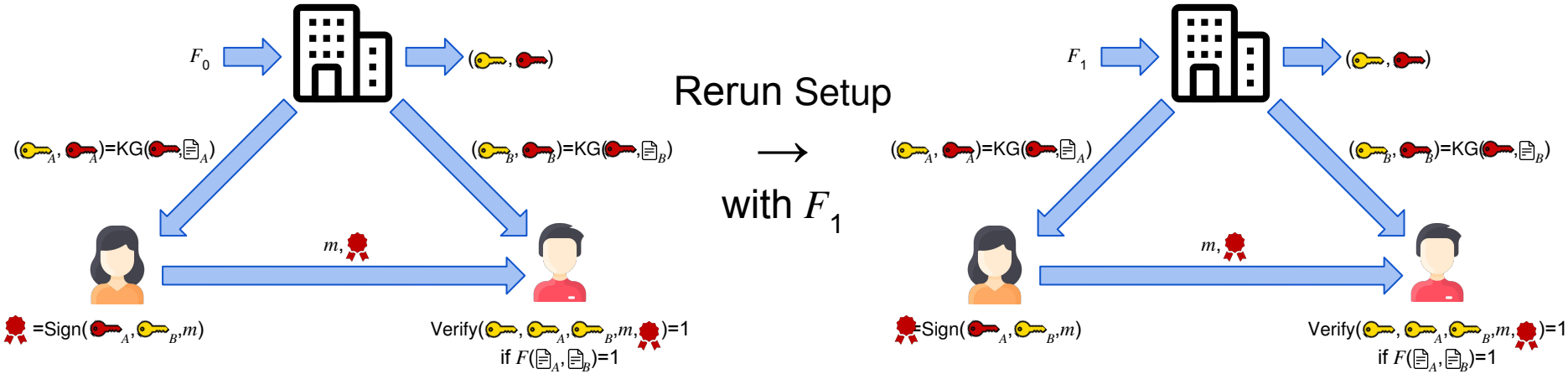
⟶

with F_1

Naive Approach



Naive Approach



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:

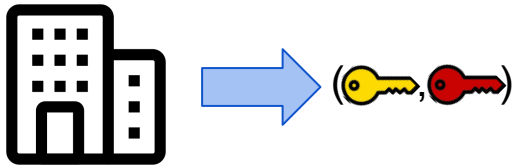
1. Digital Signatures

2. Non-Interactive Zero-Knowledge Proofs

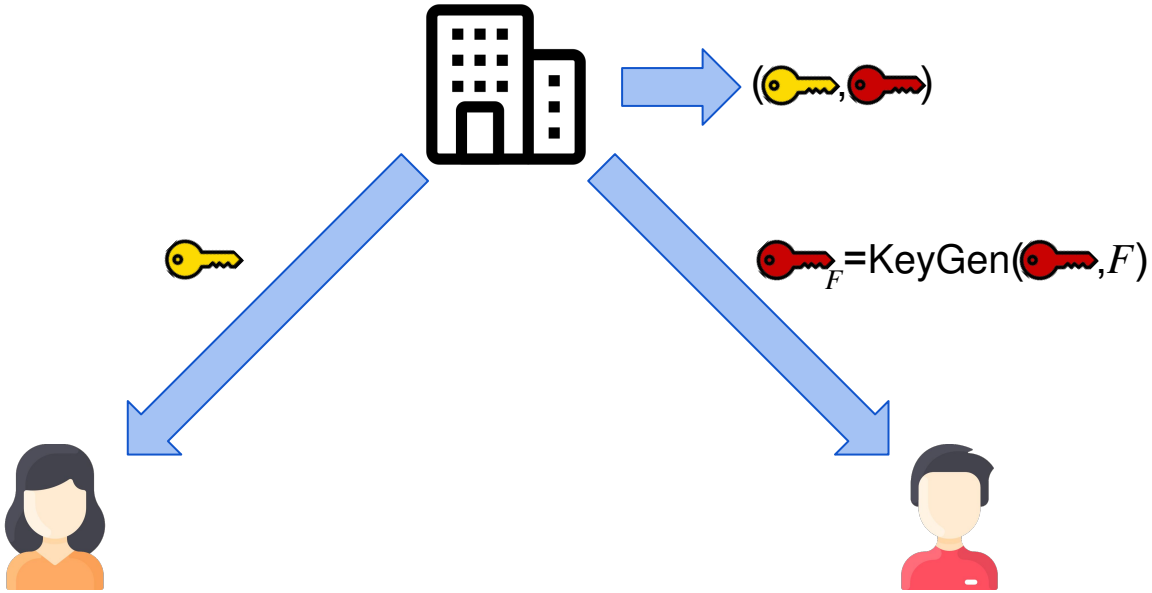
3. Two-Input (Partially-Hiding) Predicate Encryption

(Public-Key) Predicate Encryption [KSW07]

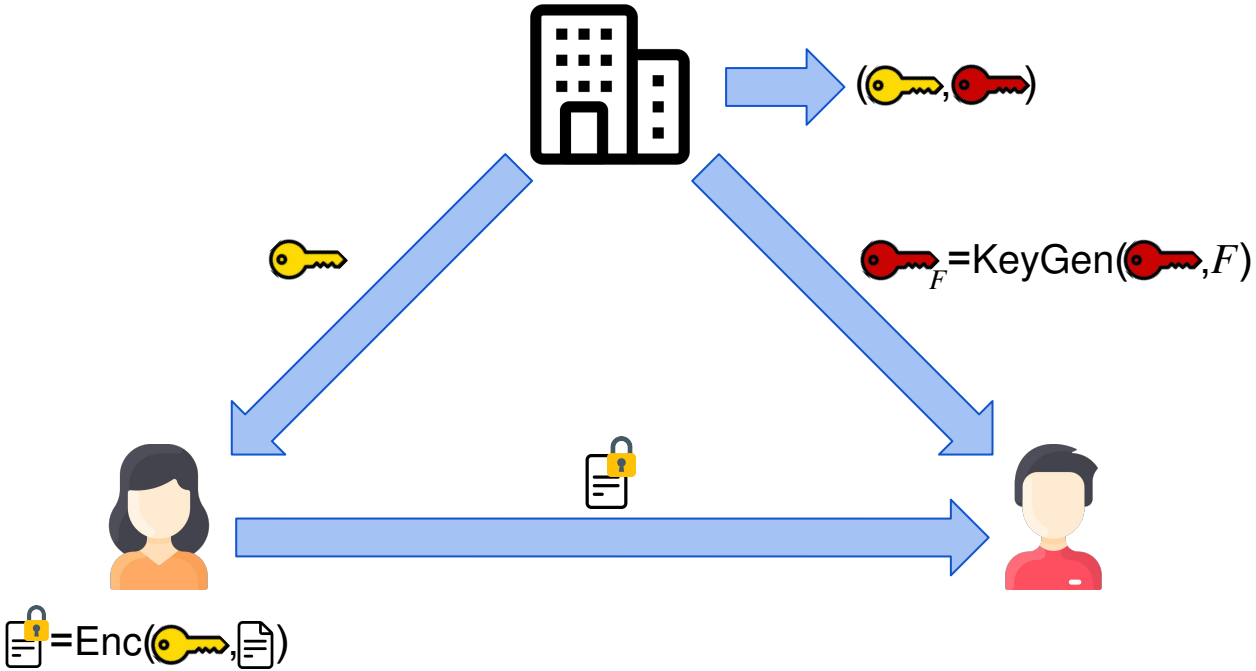
(Public-Key) Predicate Encryption [KSW07]



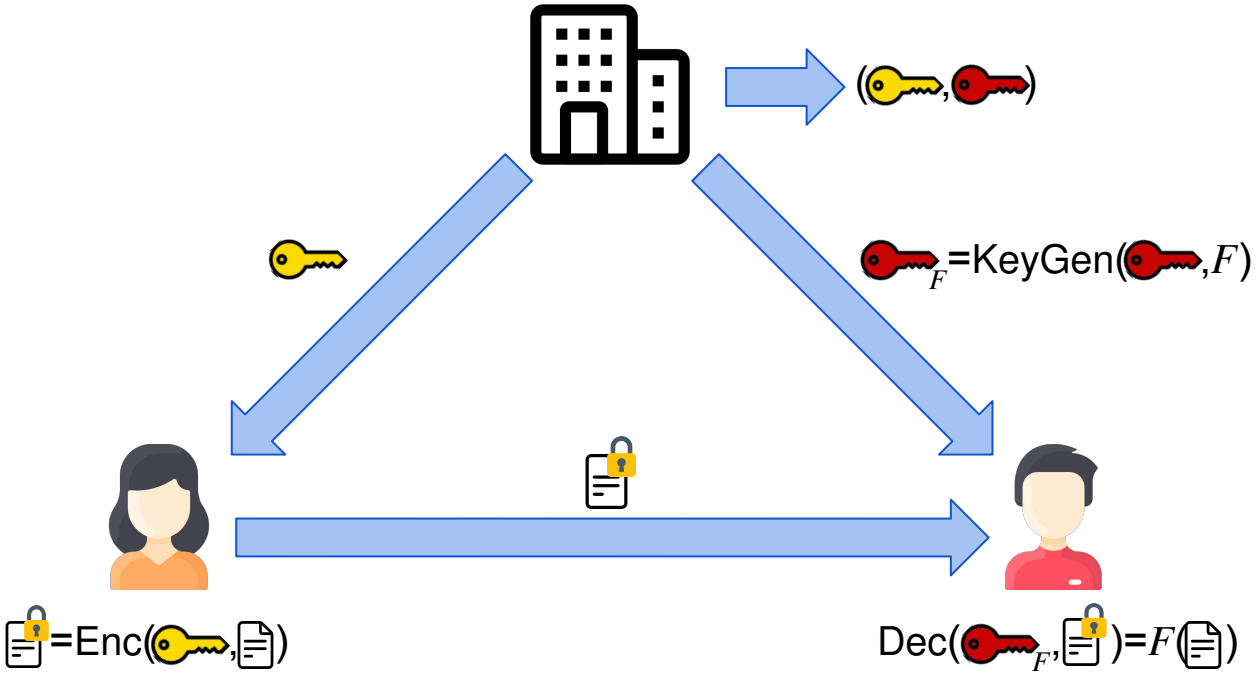
(Public-Key) Predicate Encryption [KSW07]



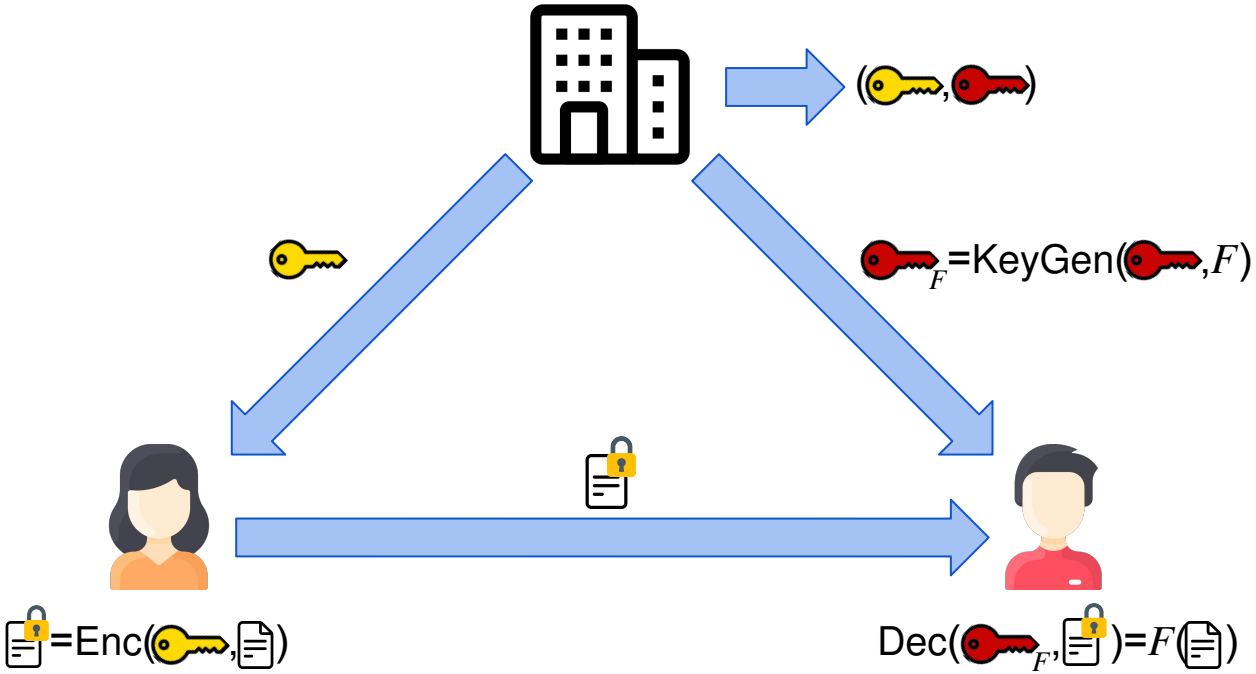
(Public-Key) Predicate Encryption [KSW07]



(Public-Key) Predicate Encryption [KSW07]

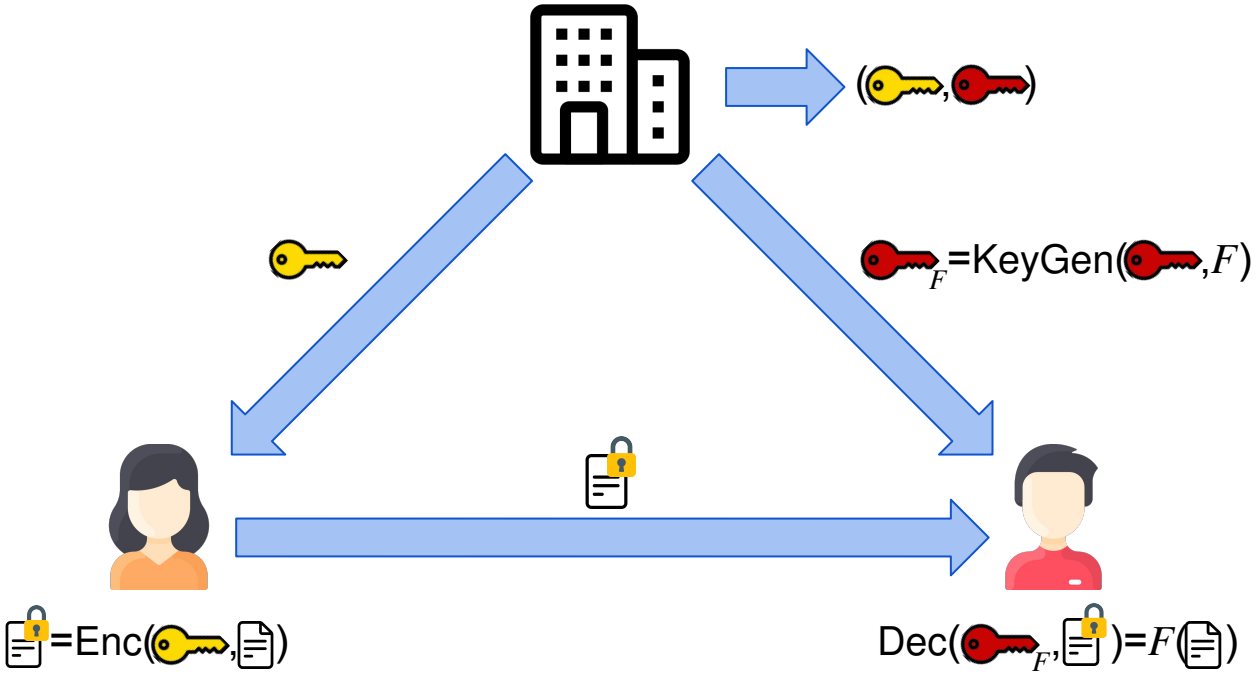


(Public-Key) Predicate Encryption [KSW07]



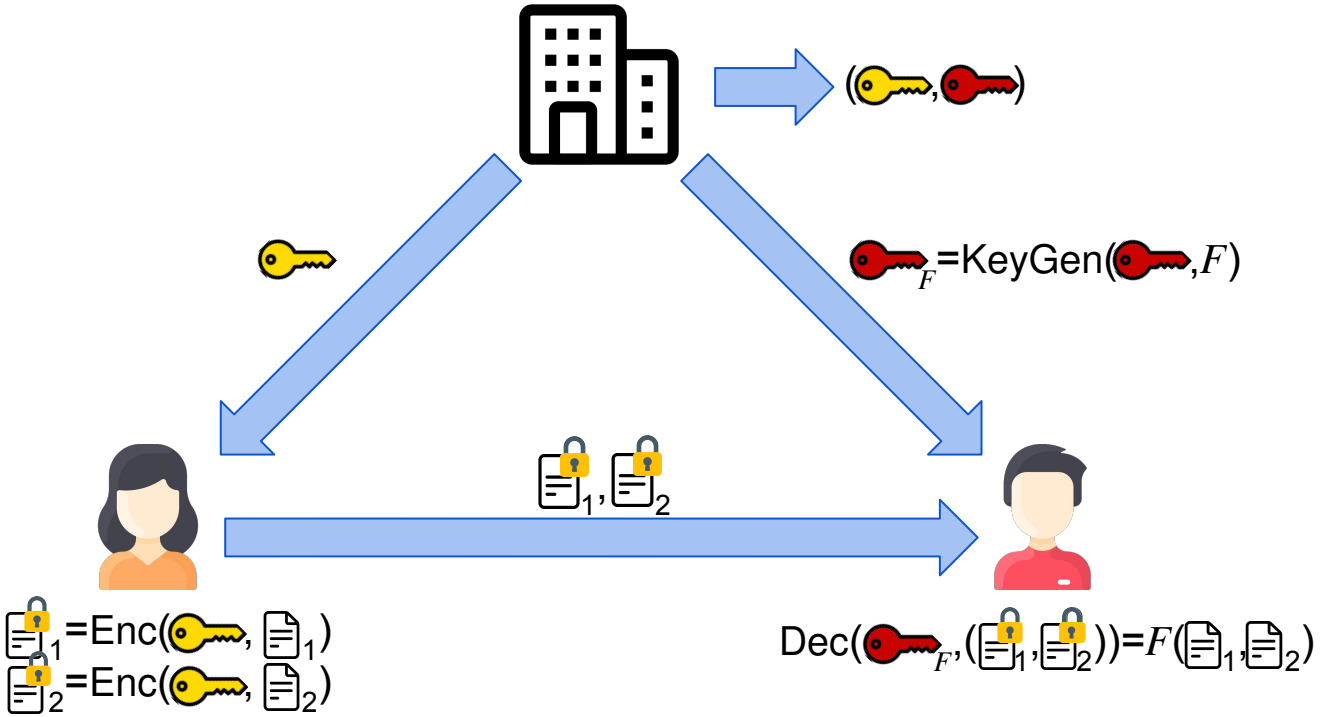
Attribute Hiding

Two-Input Predicate Encryption [GGG+14]



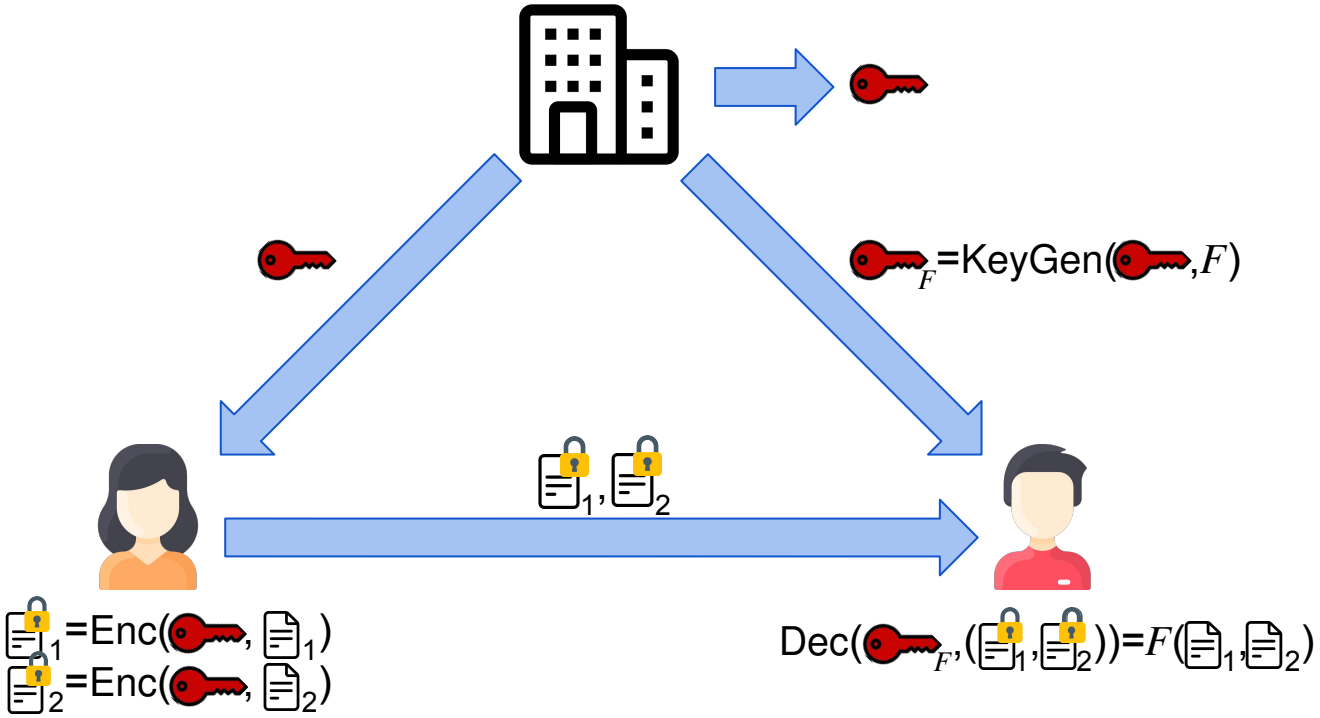
Attribute Hiding

Two-Input Predicate Encryption [GGG+14]



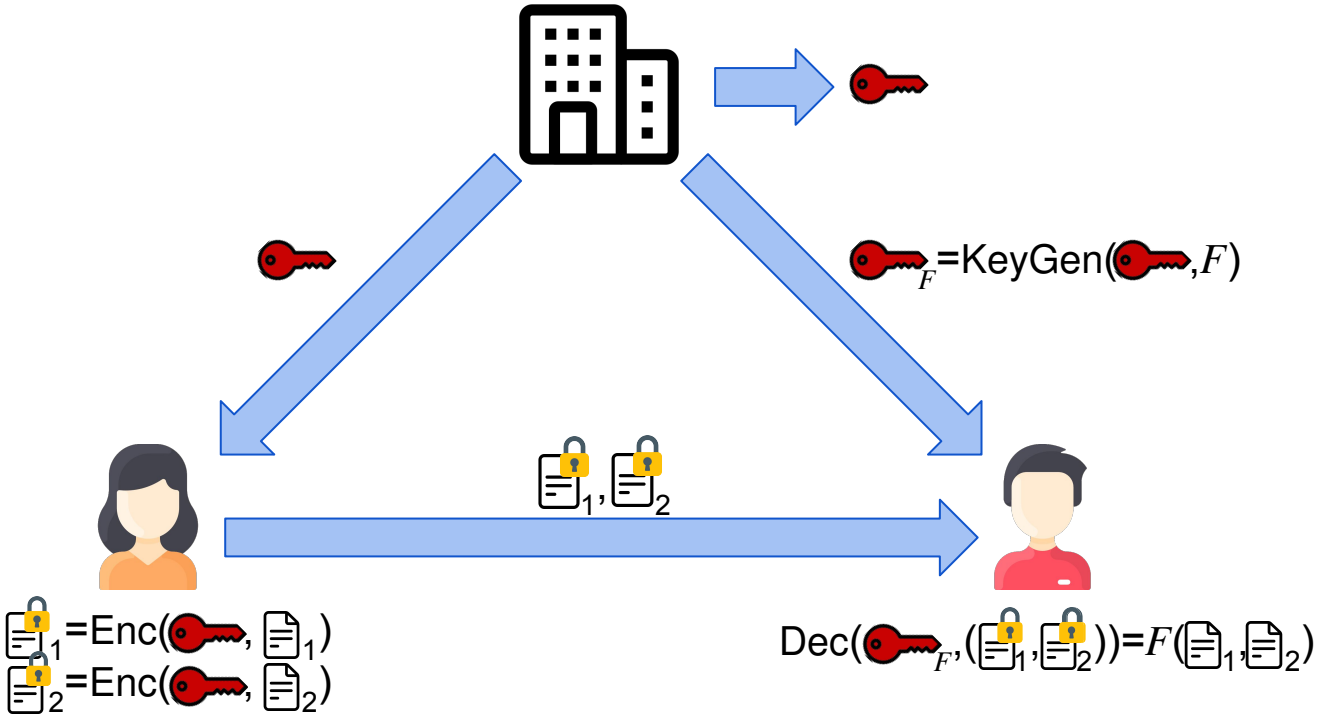
Attribute Hiding

Two-Input Predicate Encryption [GGG+14]



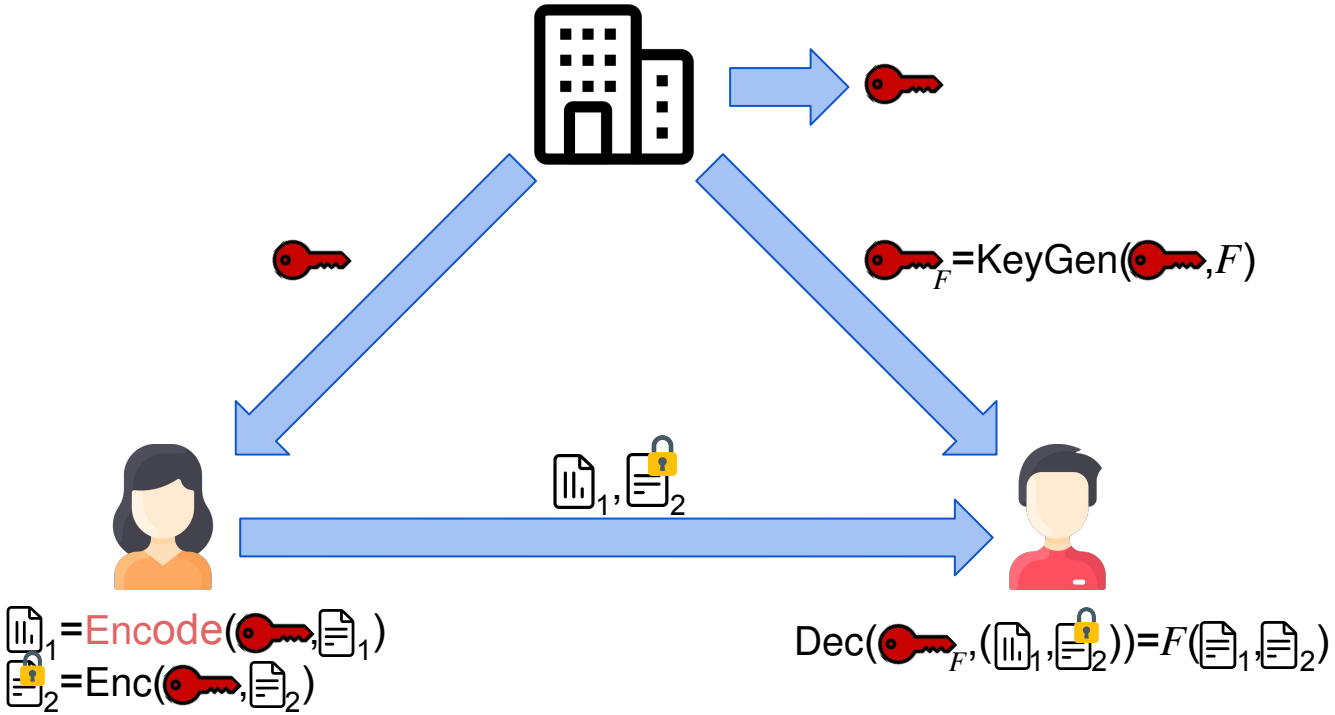
Attribute Hiding

Two-Input (Partially-Hiding) Predicate Encryption



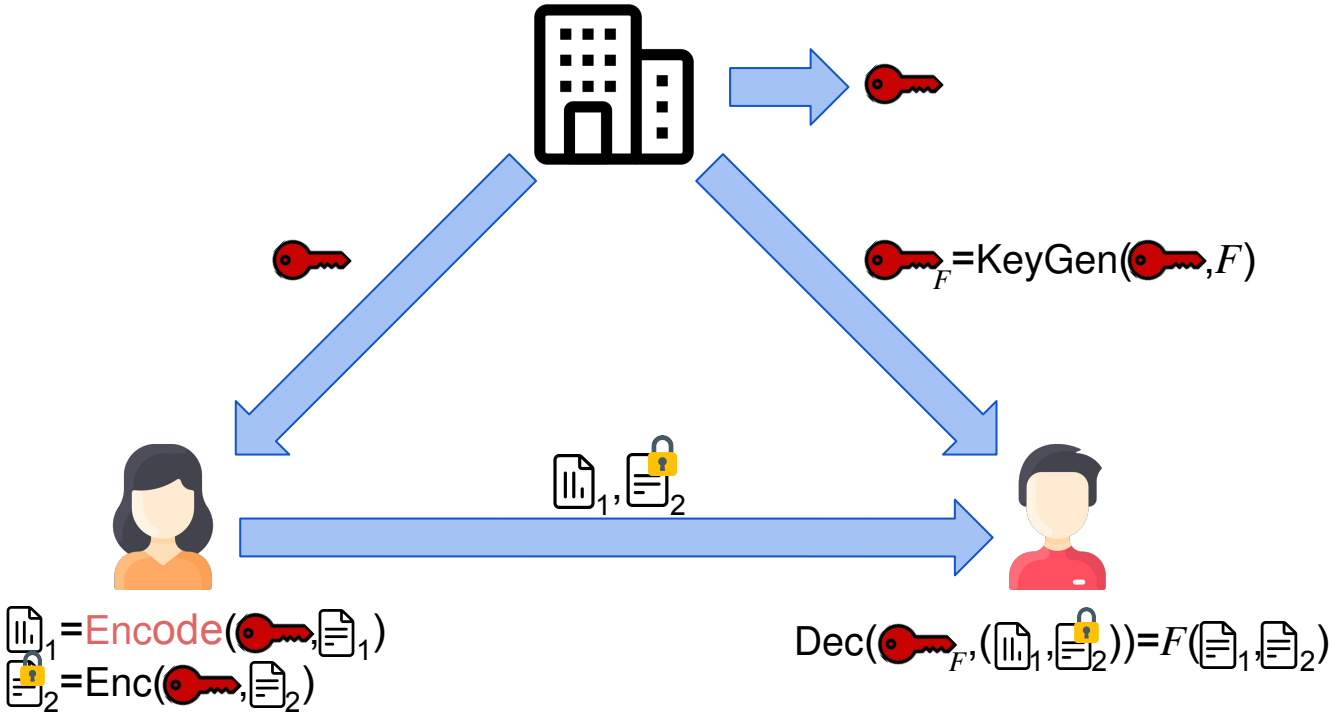
Attribute Hiding

Two-Input (Partially-Hiding) Predicate Encryption



Attribute Hiding

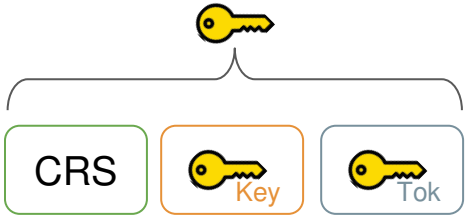
Two-Input (Partially-Hiding) Predicate Encryption



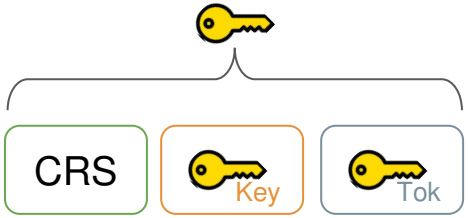
Attribute Hiding only for second slot

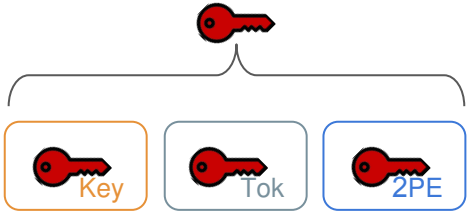
Construction

Construction

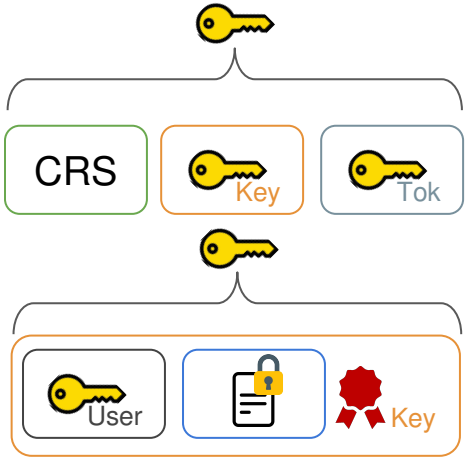


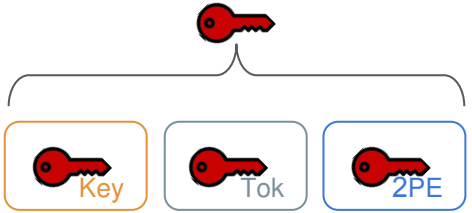
Construction



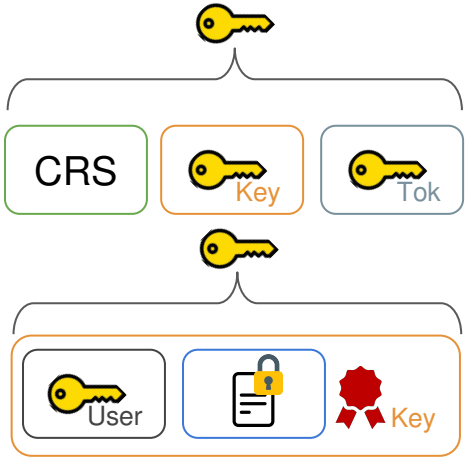


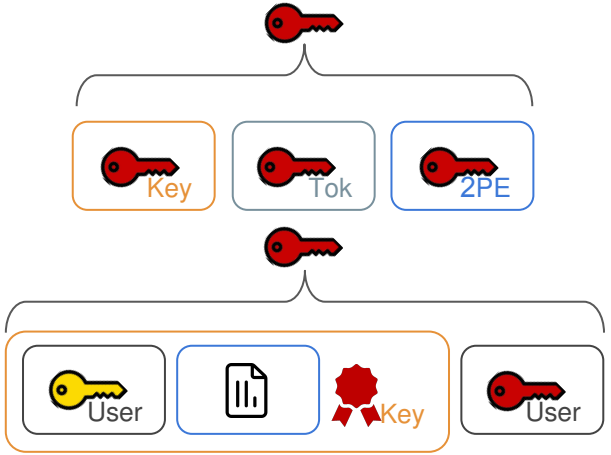
Construction



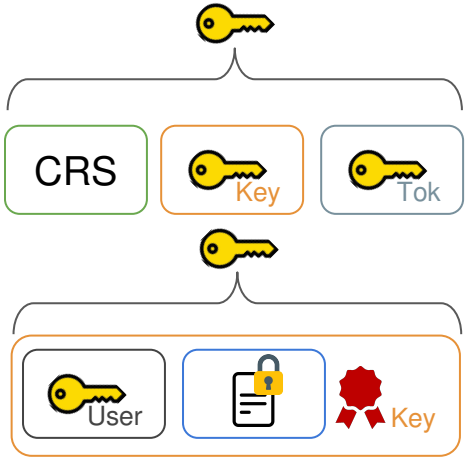


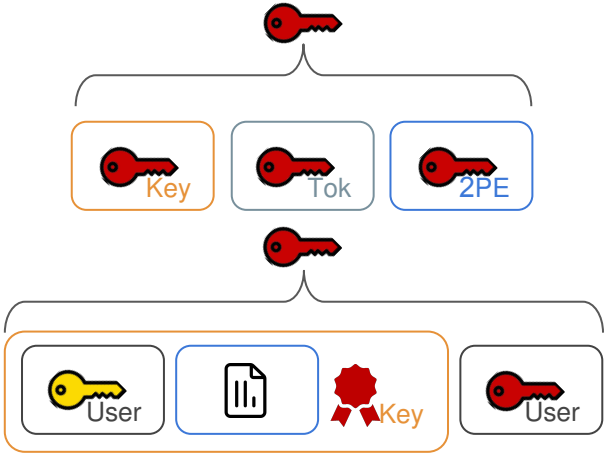
Construction

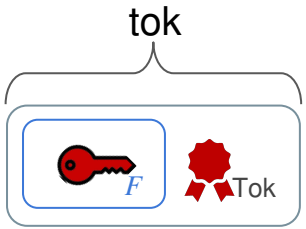




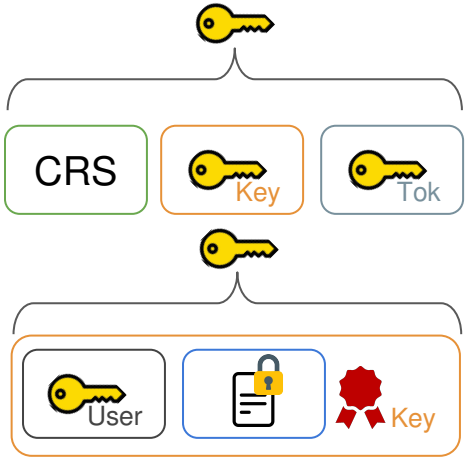
Construction

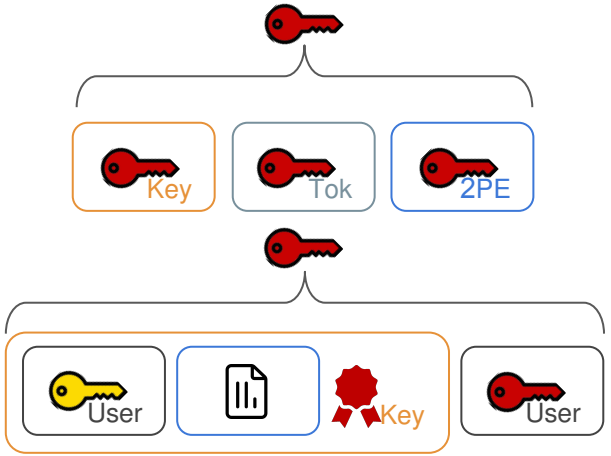


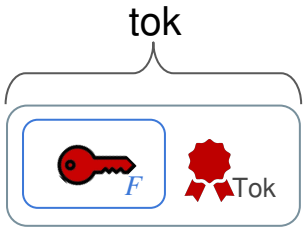


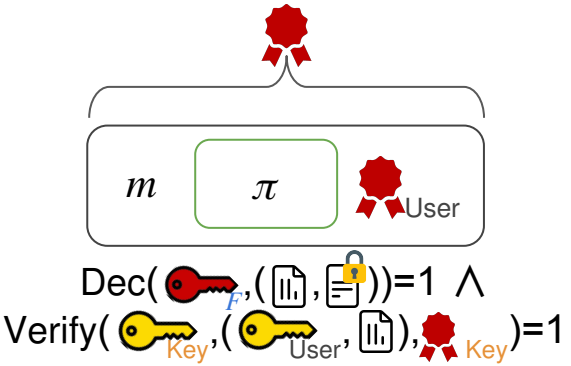


Construction

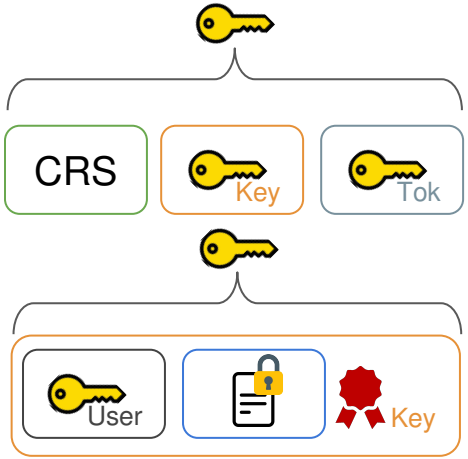


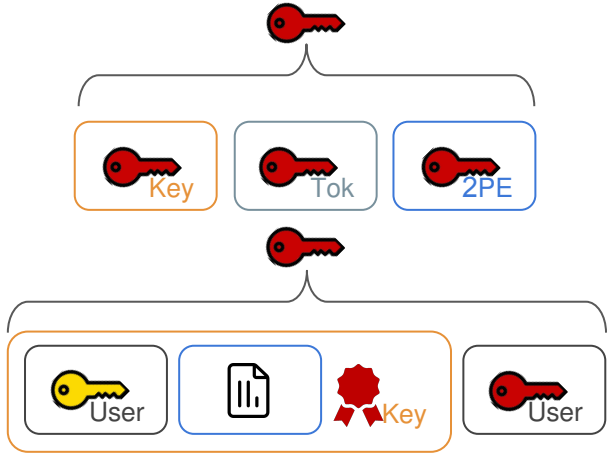


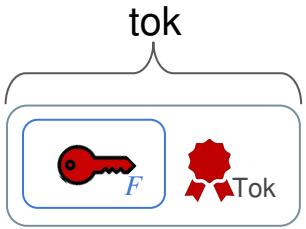


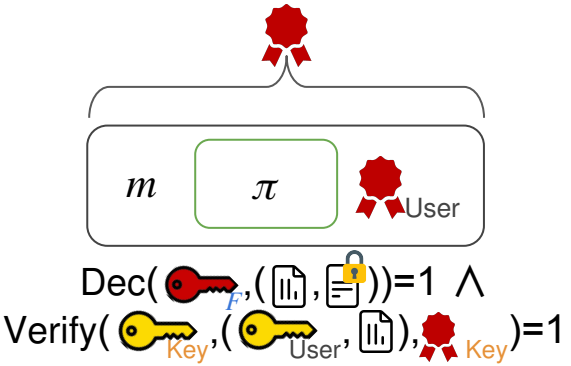


Construction









Done?

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

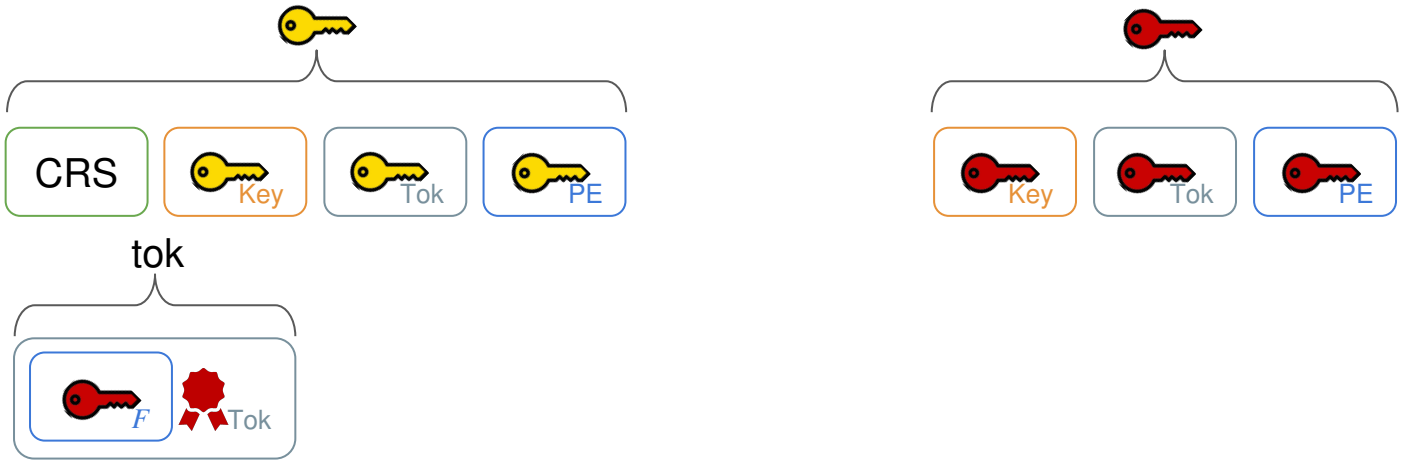
Can we realize UPCS without 2-PHPE?

⇒ No, since UPCS implies 2-PHPE

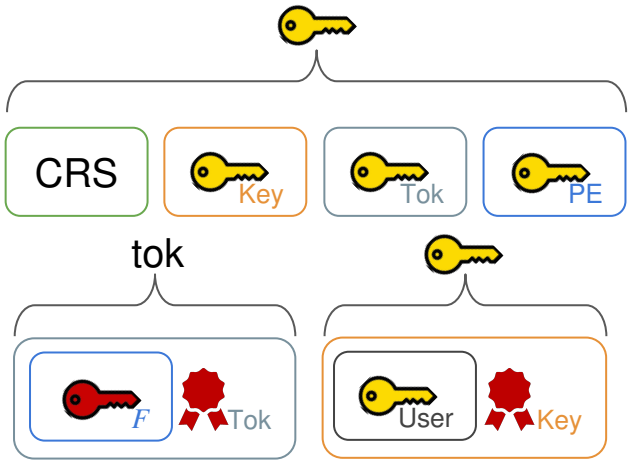
Solution: use interaction and PE for policy evaluation

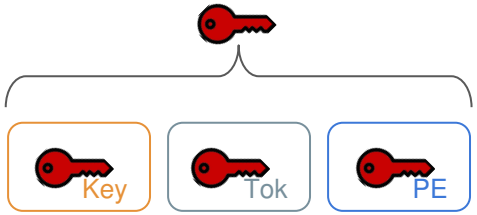
Interactive Updatable PCS

Interactive Updatable PCS

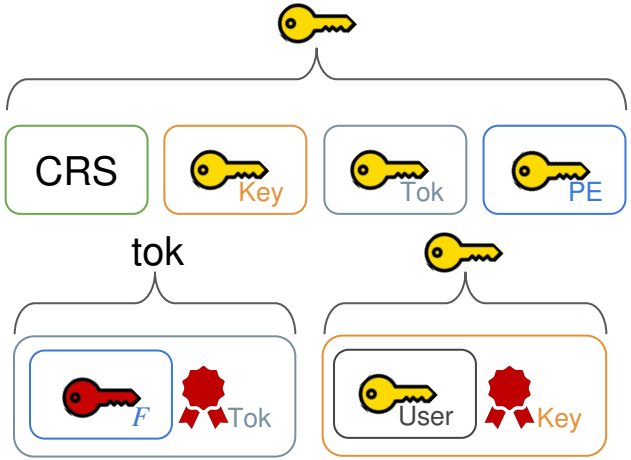


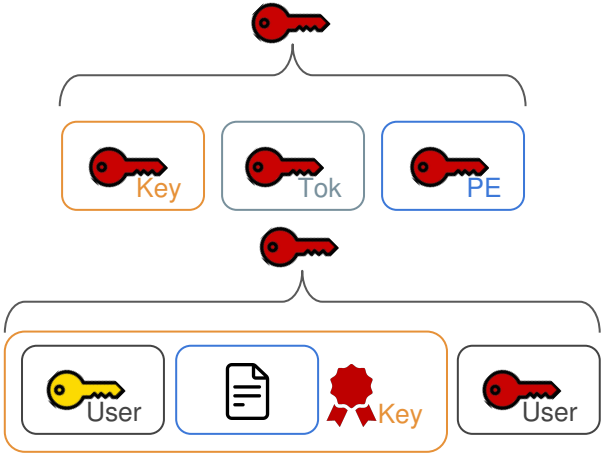
Interactive Updatable PCS



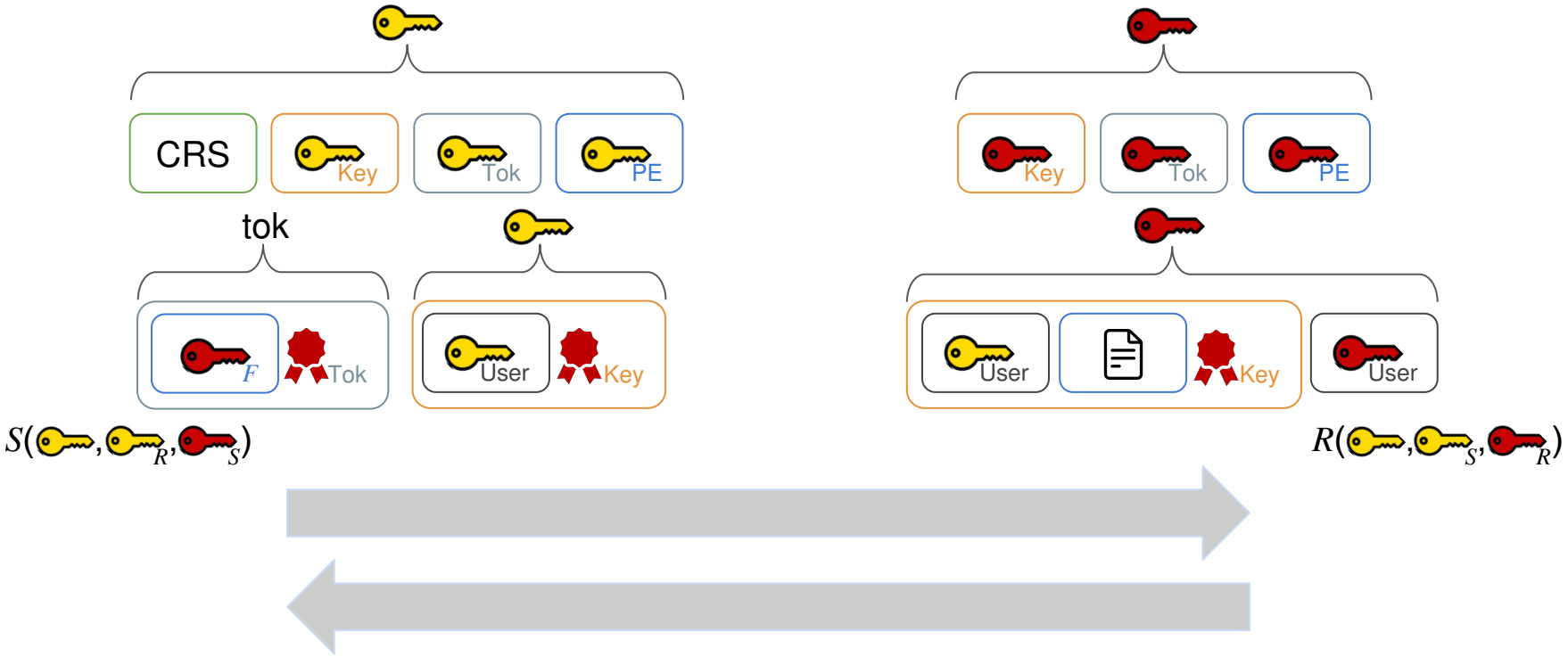


Interactive Updatable PCS

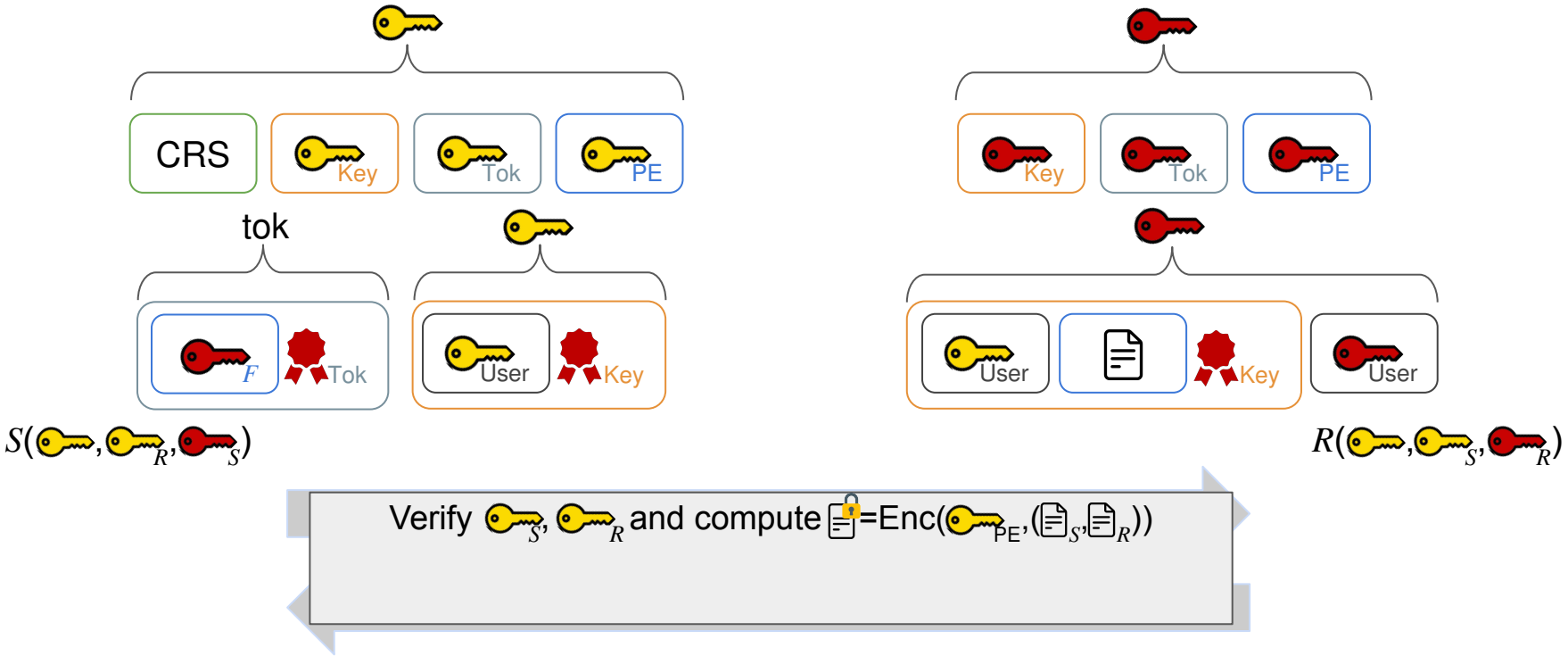




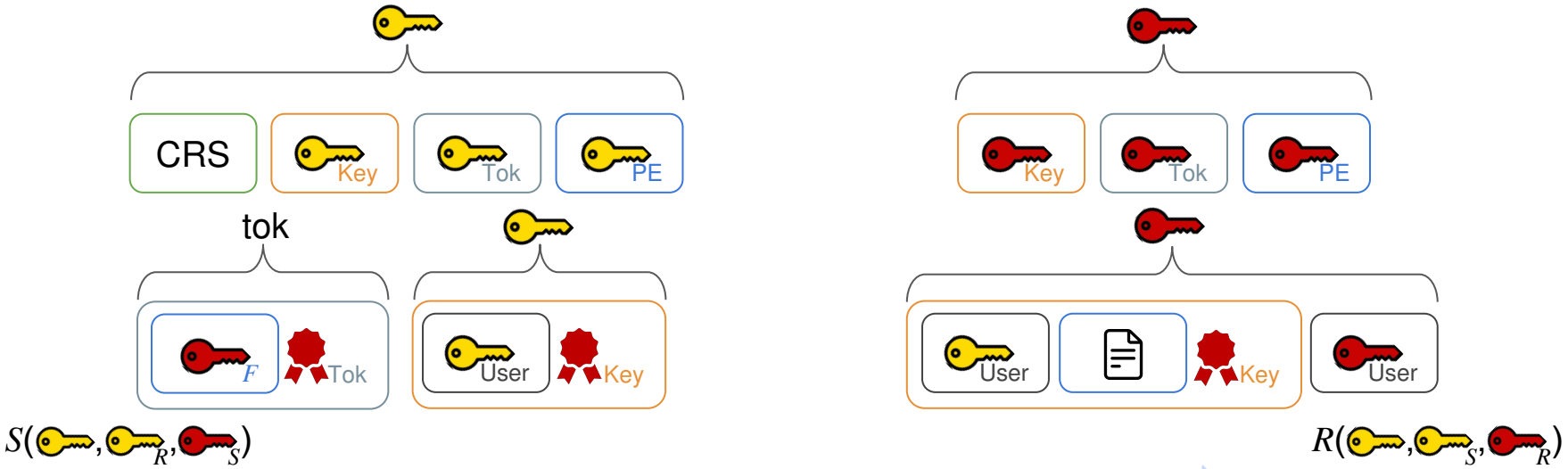
Interactive Updatable PCS



Interactive Updatable PCS



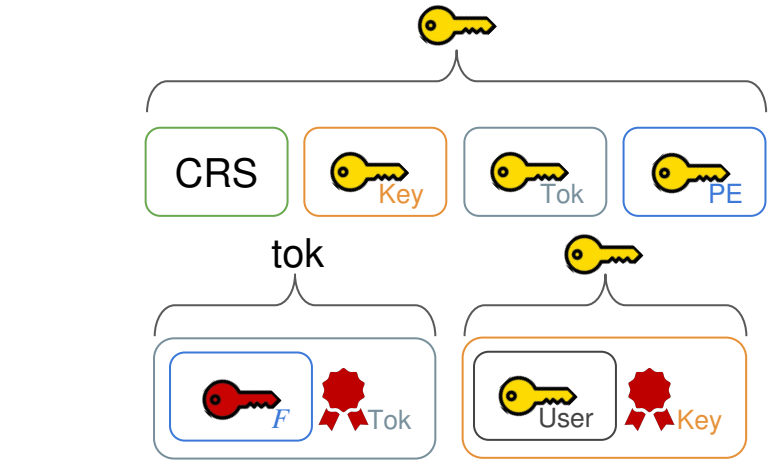
Interactive Updatable PCS

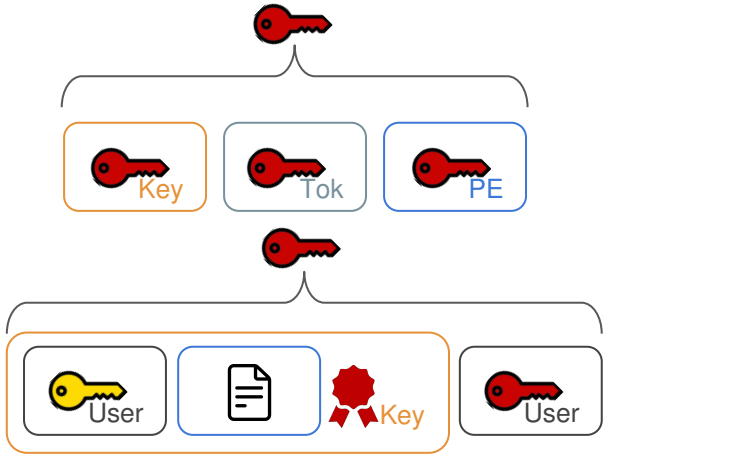


Verify key_S, key_R and compute $\text{ct}=\text{Enc}(\text{key}_{PE},(\text{doc}_S,\text{doc}_R))$

Output ct and a proof π of the computation

Interactive Updatable PCS





$S(\,,\,_R,\,_S)$

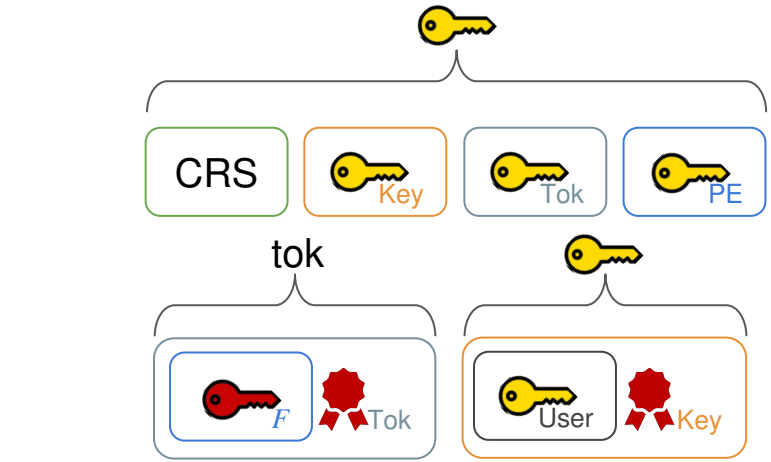
$R(\,,\,_S,\,_R)$

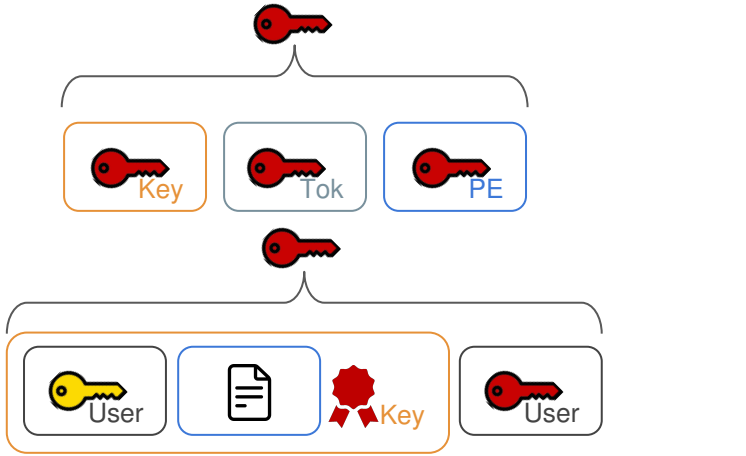
Verify $\,_S$, $\,_R$ and compute $\,$=Enc($\,_{PE}$,($\,_S$,$\,_R$))

Output $\,$ and a proof π of the computation

π':
Dec($\,_F$, $\,$)=1 $\wedge$
Verify(CRS,π)=1

Interactive Updatable PCS





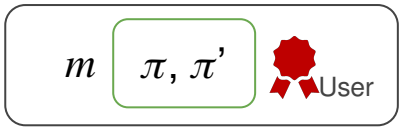
$S(\,,\,_R,\,_S)$

$R(\,,\,_S,\,_R)$

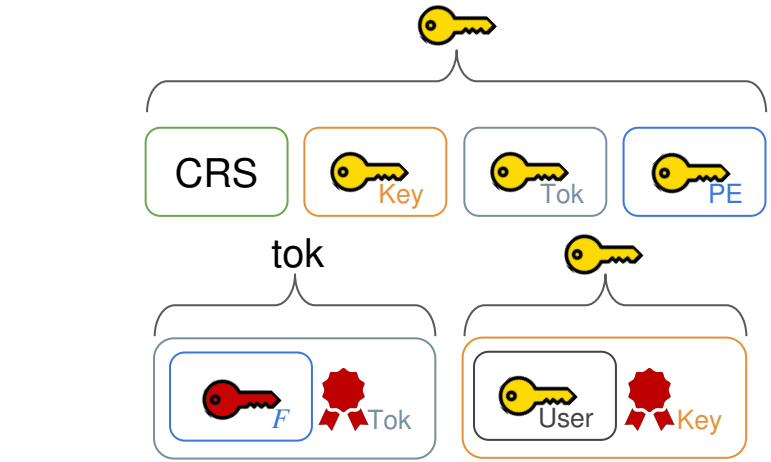
Verify $_S$, $_R$ and compute =Enc($_{PE}$,($_S$,$_R$))

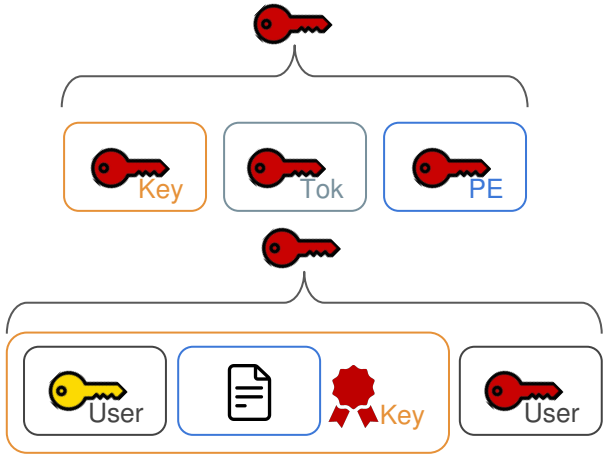
Output and a proof π of the computation

π':
Dec($_F$,)=1 $\wedge$
Verify(CRS,π)=1



Interactive Updatable PCS





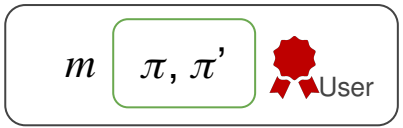
$S(\,,\,_R,\,_S)$

$R(\,,\,_S,\,_R)$

Verify $_S$, $_R$ and compute =Enc($_{PE}$,($_S$,$_R$))

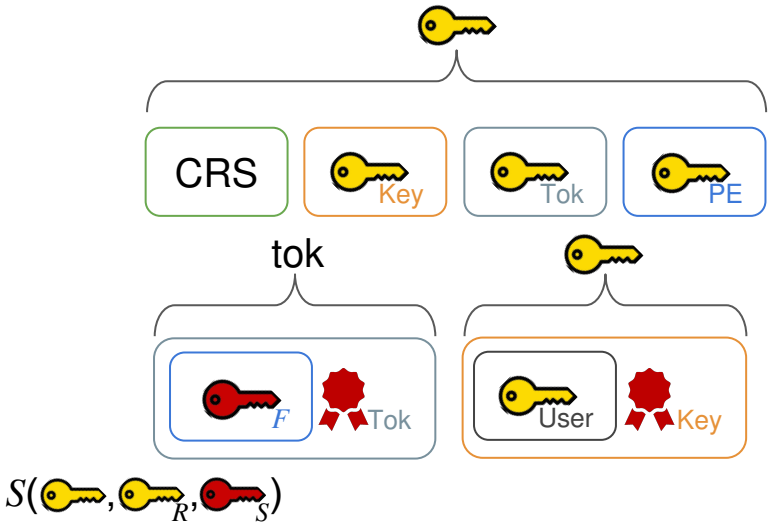
Output and a proof π of the computation

π':
Dec($_F$,)=1 $\wedge$
Verify(CRS,π)=1

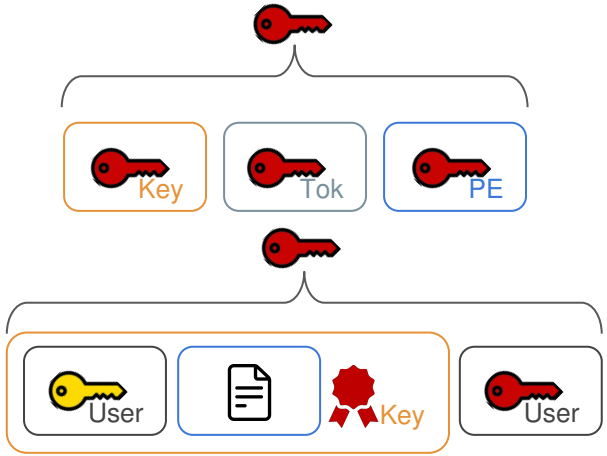


Requires recursion

Interactive Updatable PCS



$S(\,,\,_R,\,_S)$

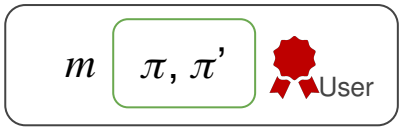


$R(\,,\,_S,\,_R)$

Verify $_S$, $_R$ and compute =Enc($_{PE}$,($_S$,$_R$))

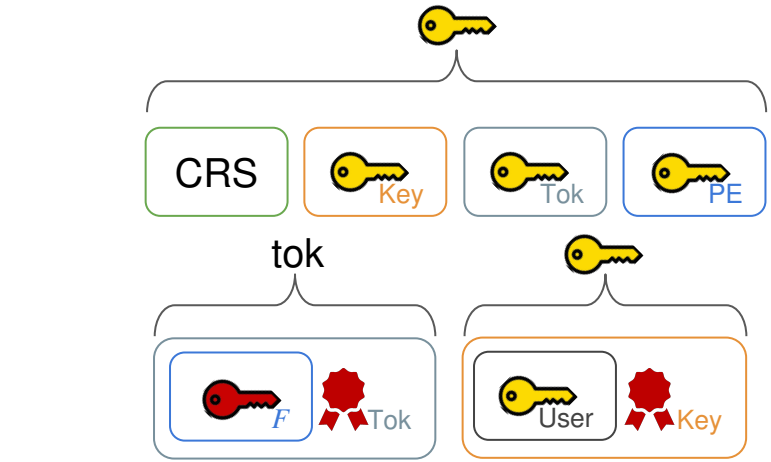
Output and a proof π of the computation

π':
Dec($_F$,)=1 ∧
Verify(CRS,π)=1

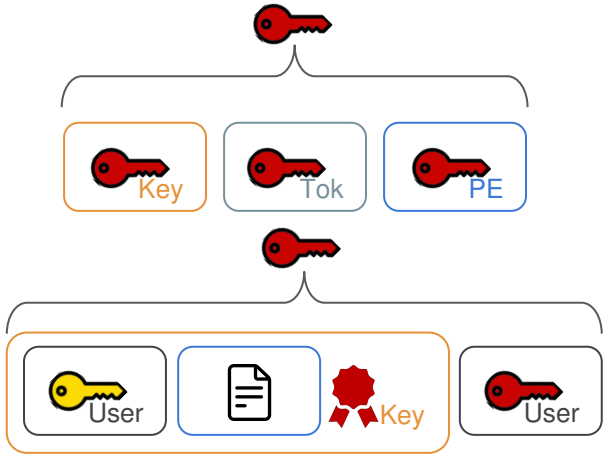


Requires recursion→Use commitments

Interactive Updatable PCS



$S(\,,\,_R,\,_S)$

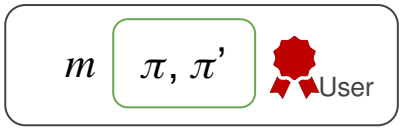


$R(\,,\,_S,\,_R)$

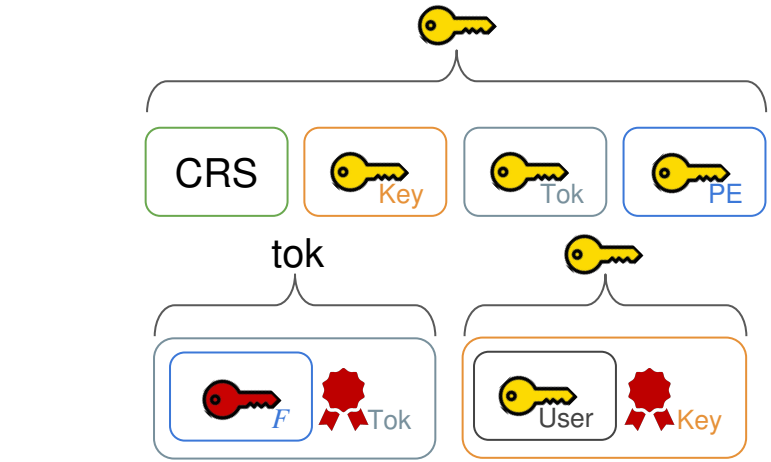
Verify $_S$, $_R$ compute =Enc($_{PE}$,($_S$,$_R$)) & c=Com(,r)

Output c, r, and a proof π of the computation

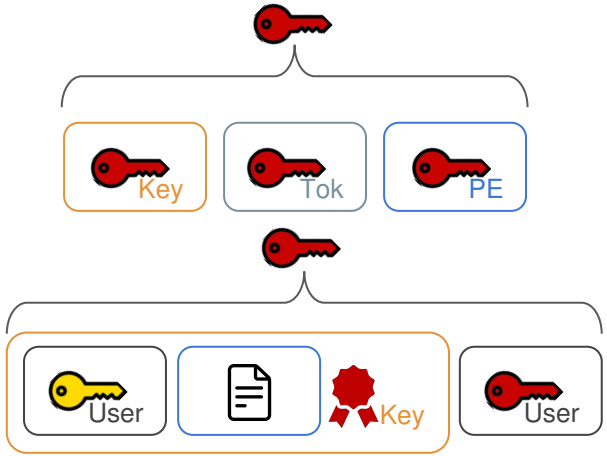
π':
Dec($_F$,)=1 ∧
Verify(CRS,π)=1



Interactive Updatable PCS



$S(\,,\,_R,\,_S)$



$R(\,,\,_S,\,_R)$

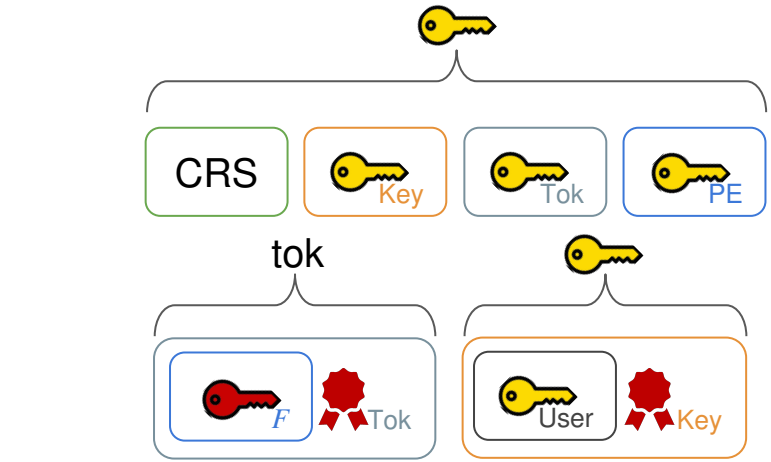
Verify $_S$, $_R$ compute =Enc($_{PE}$,($_S$,$_R$)) & c=Com(,r)

Output c, r, and a proof π of the computation

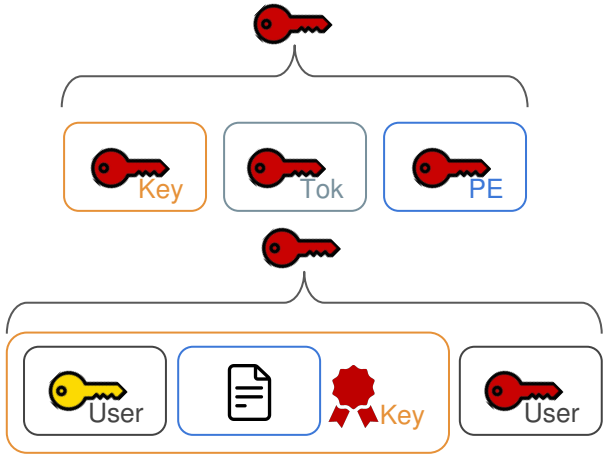
π':
Dec($_F$,)=1 $\wedge$
Com(,r)=c

m,c π, π' User

Interactive Updatable PCS



$S(\,,\,_R,\,_S)$



$R(\,,\,_S,\,_R)$

Verify $_S$, $_R$ compute =Enc($_{PE}$,($_S$,$_R$)) & c=Com(,r)

Output c, r, and a proof π of the computation

π':
Dec($_F$,)=1 $\wedge$
Com(,r)=c

m,c π, π' User

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?