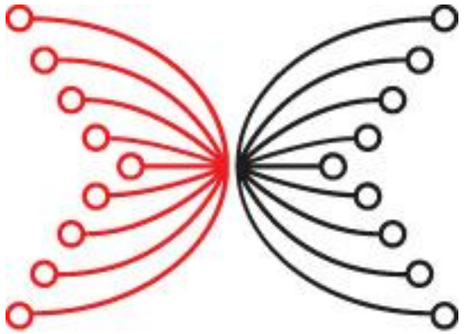
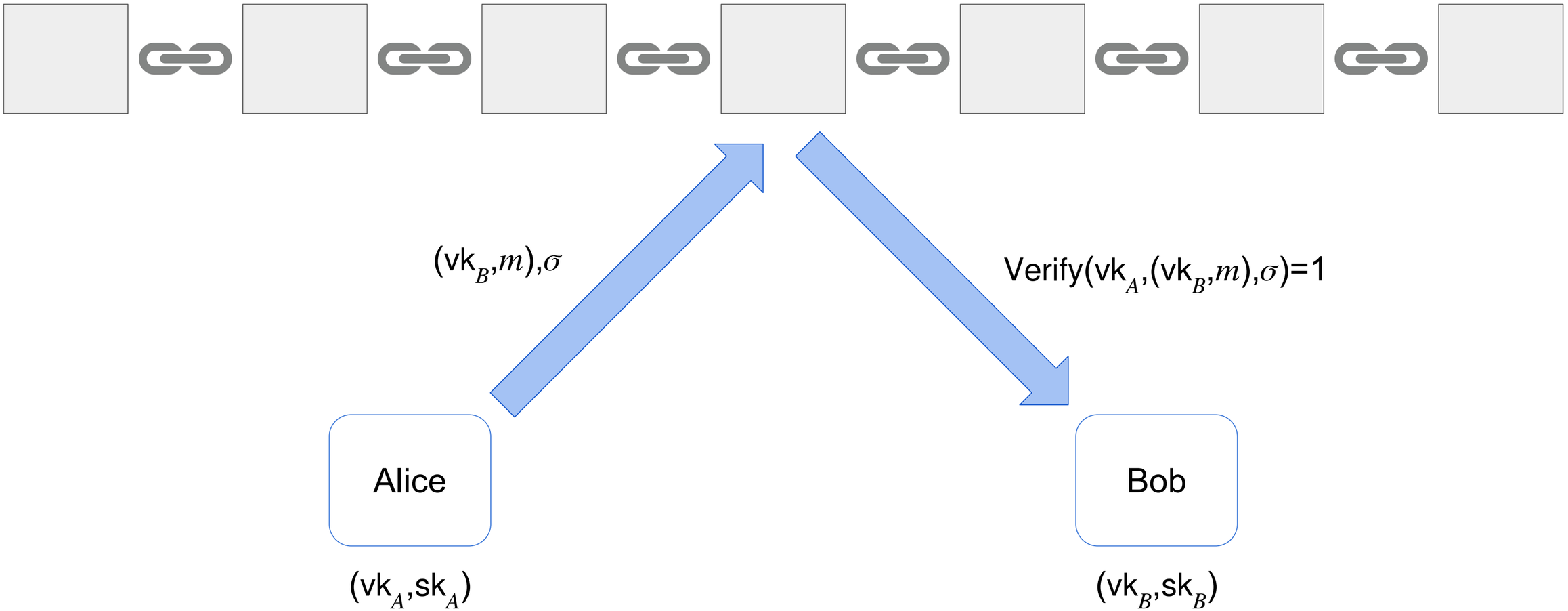
Policy-Compliant Signatures

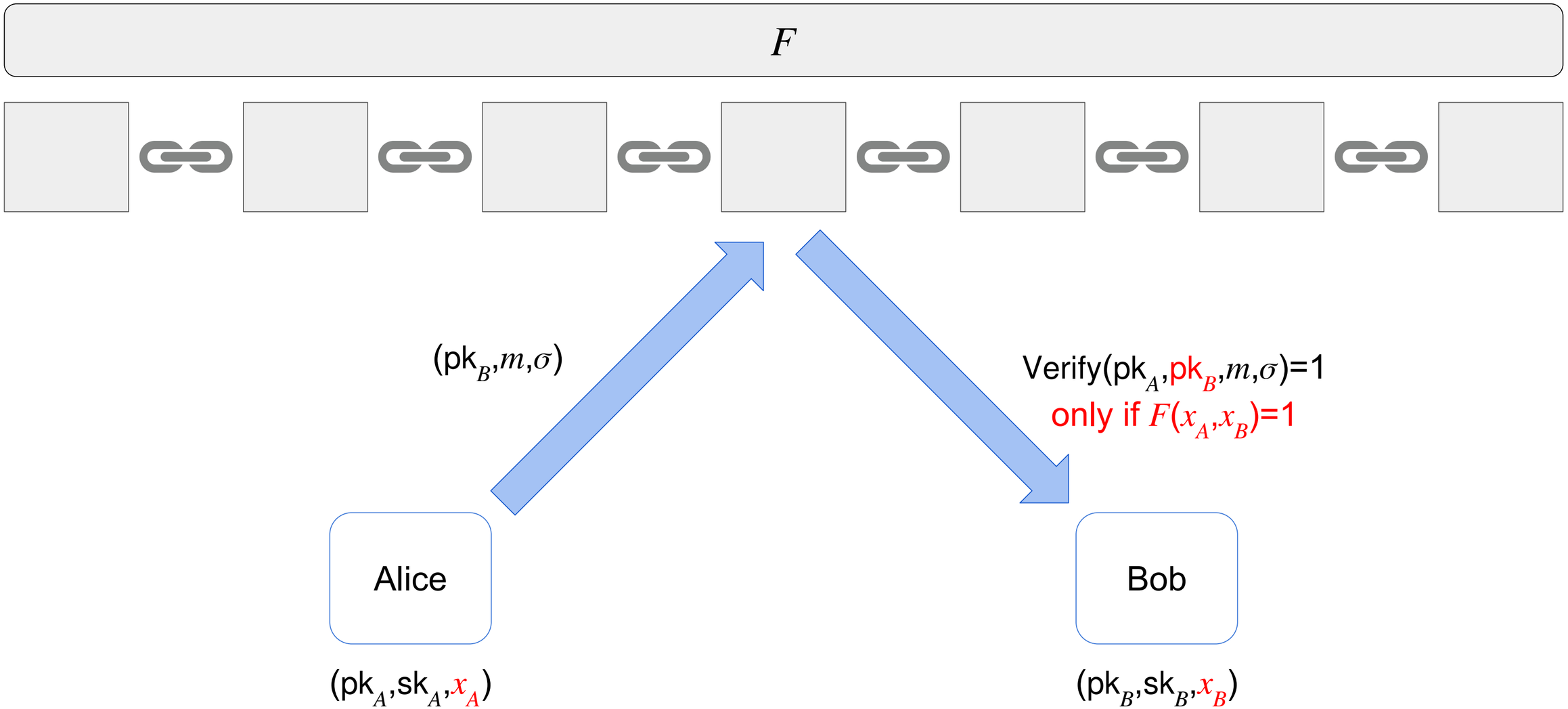
Christian Badertscher, Christian Matt,
Hendrik Waldner



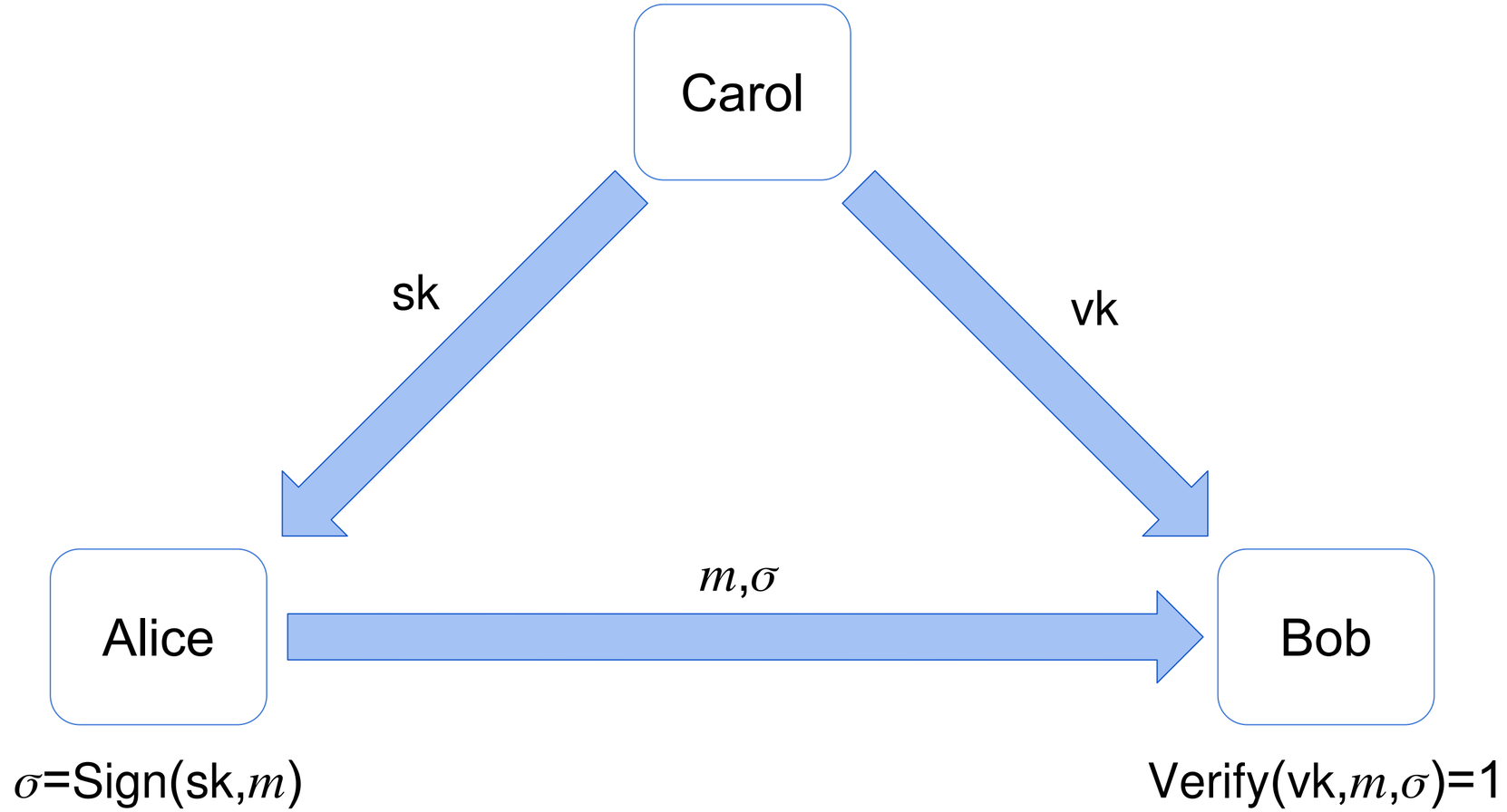
Motivation



Motivation

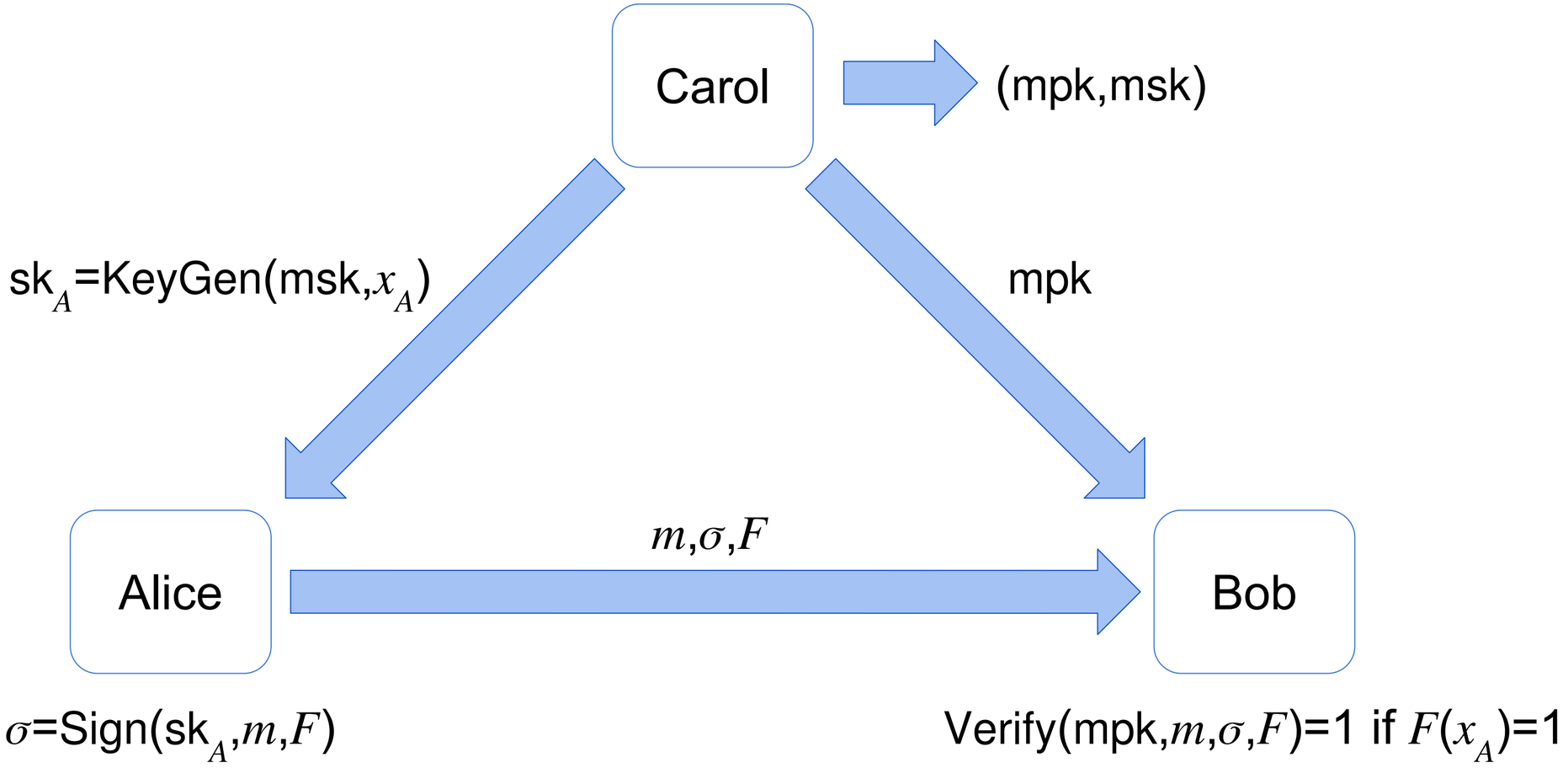

F
$(\mathrm{pk}_B, m, \sigma)$
$\mathrm{Verify}(\mathrm{pk}_A, \mathrm{pk}_B, m, \sigma)=1$
only if $F(x_A, x_B)=1$
Alice
Bob
$(\mathrm{pk}_A, \mathrm{sk}_A, x_A)$
$(\mathrm{pk}_B, \mathrm{sk}_B, x_B)$

Digital Signatures [DH76,RSA78]



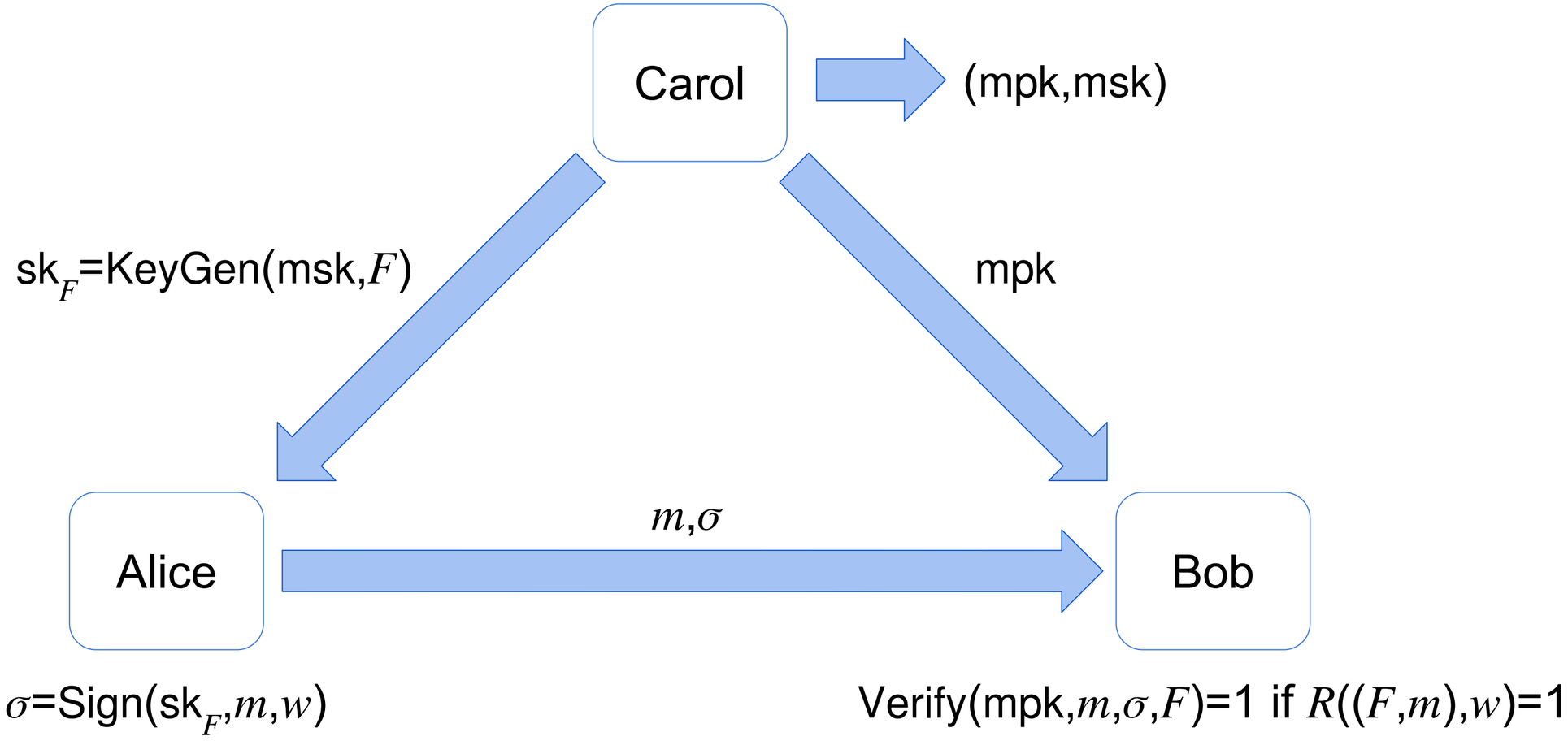
⇒ No Attributes

Attribute-Based Signatures [MPR11]



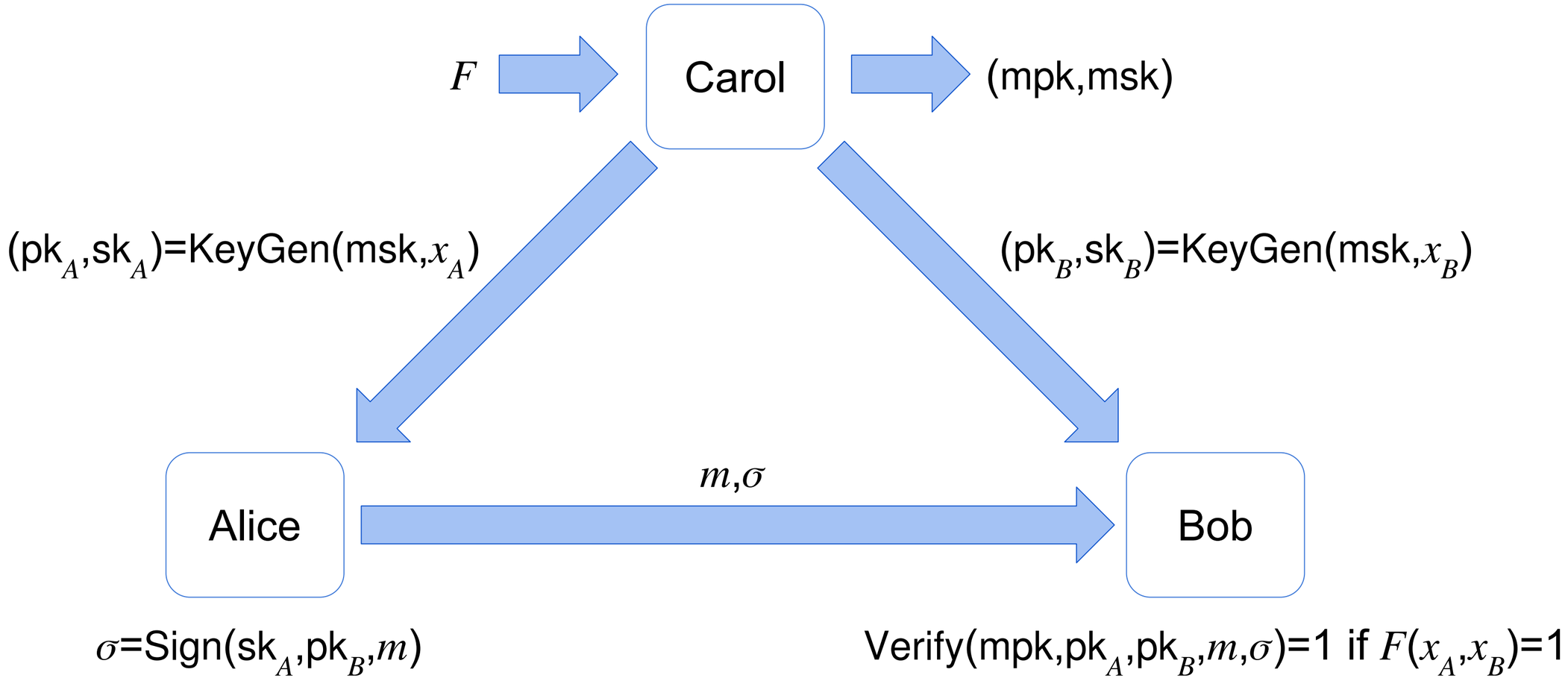
⇒ Only Sender Attributes are incorporated

Policy-Based Signatures [BF14]



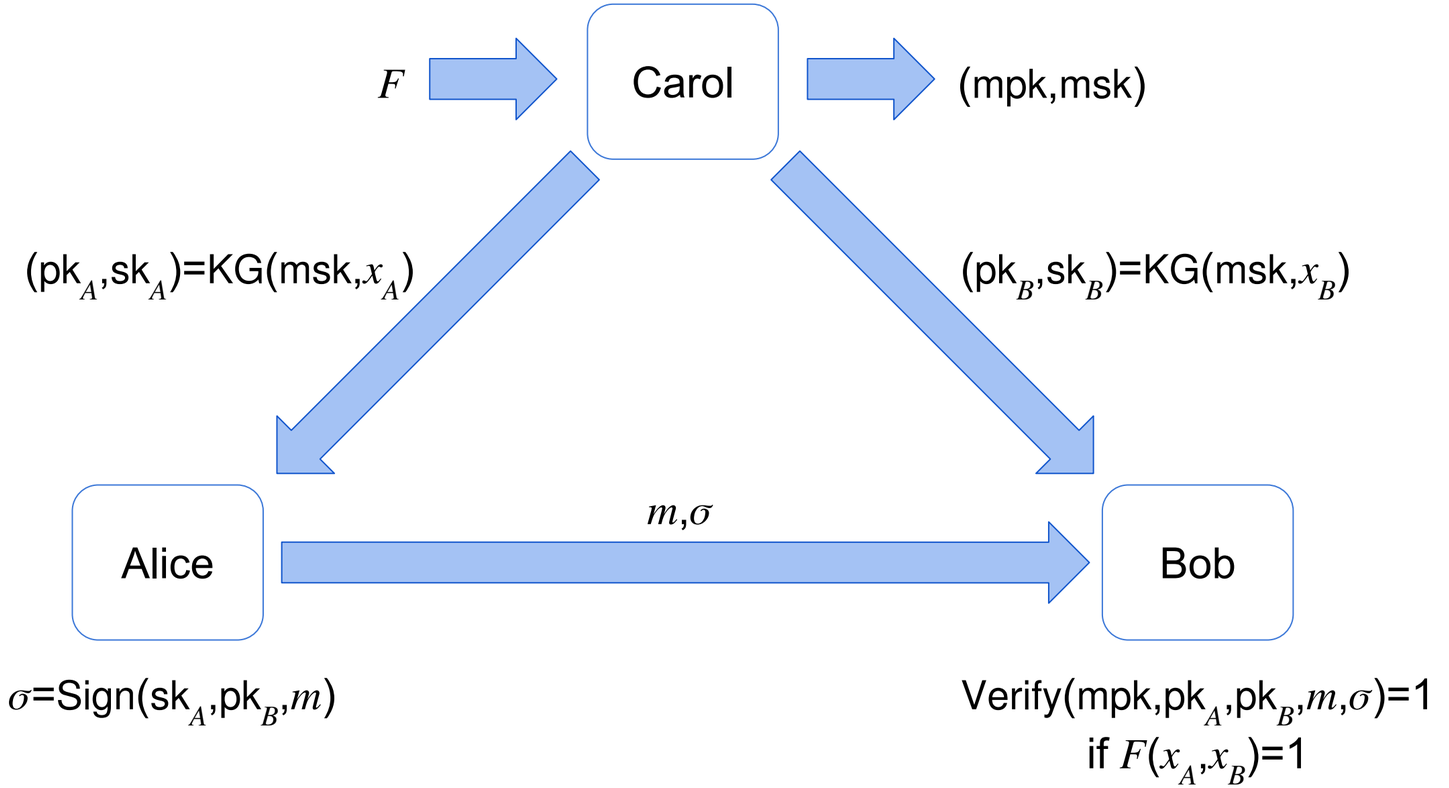
⇒ No Receiver Privacy

Policy-Compliant Signatures



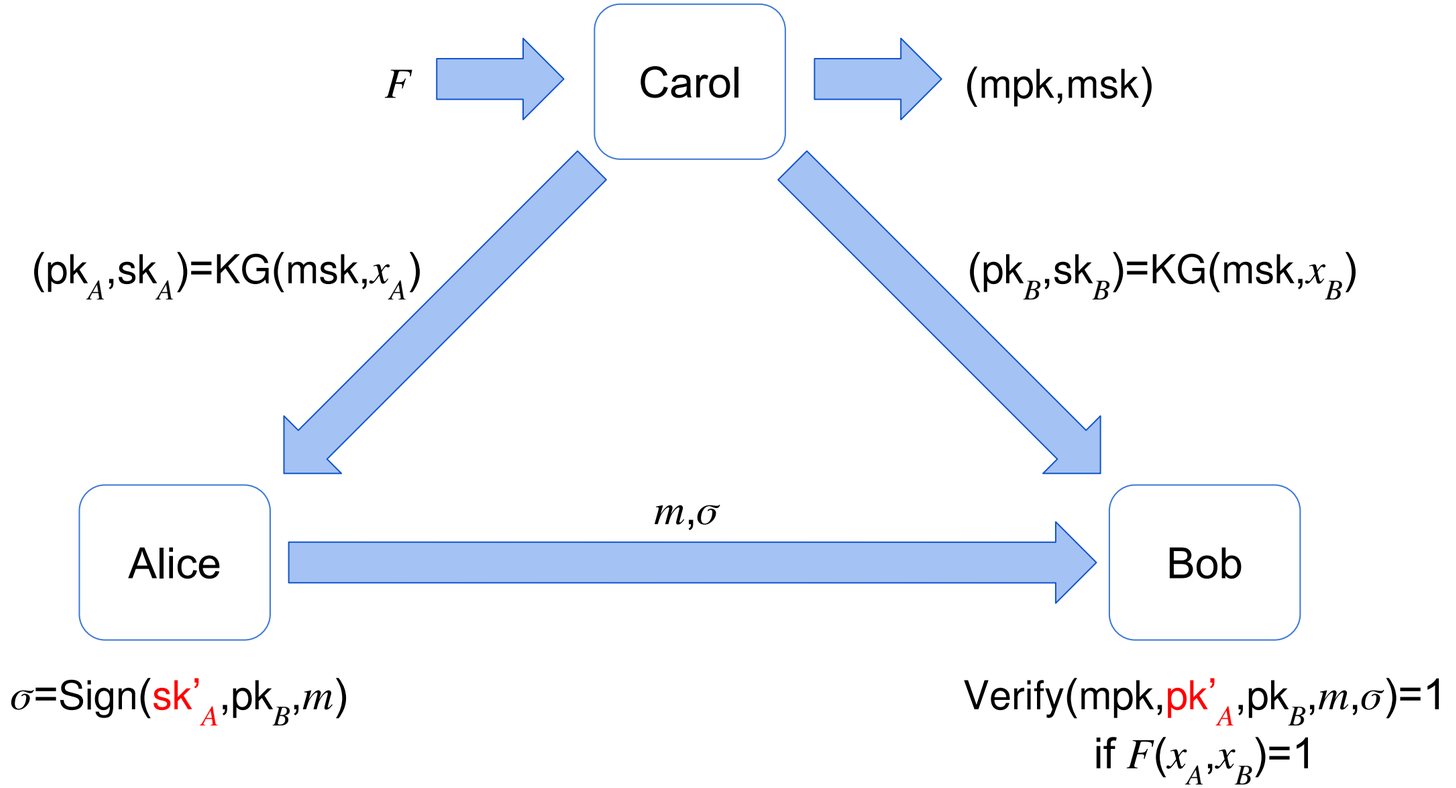
Unforgeability and Attribute-Hiding

Unforgeability



Unforgeability

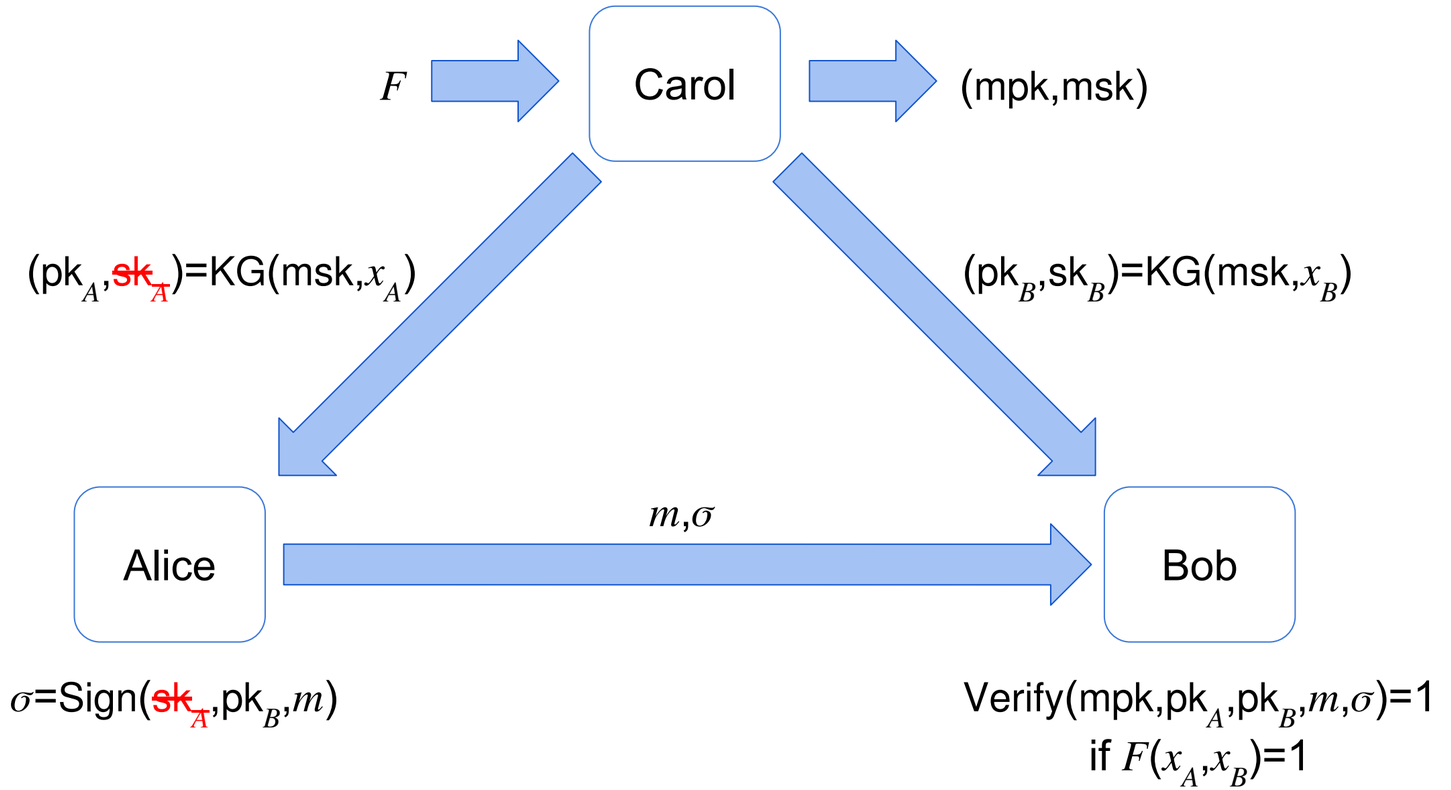
1. Key Generation Forgery



Unforgeability

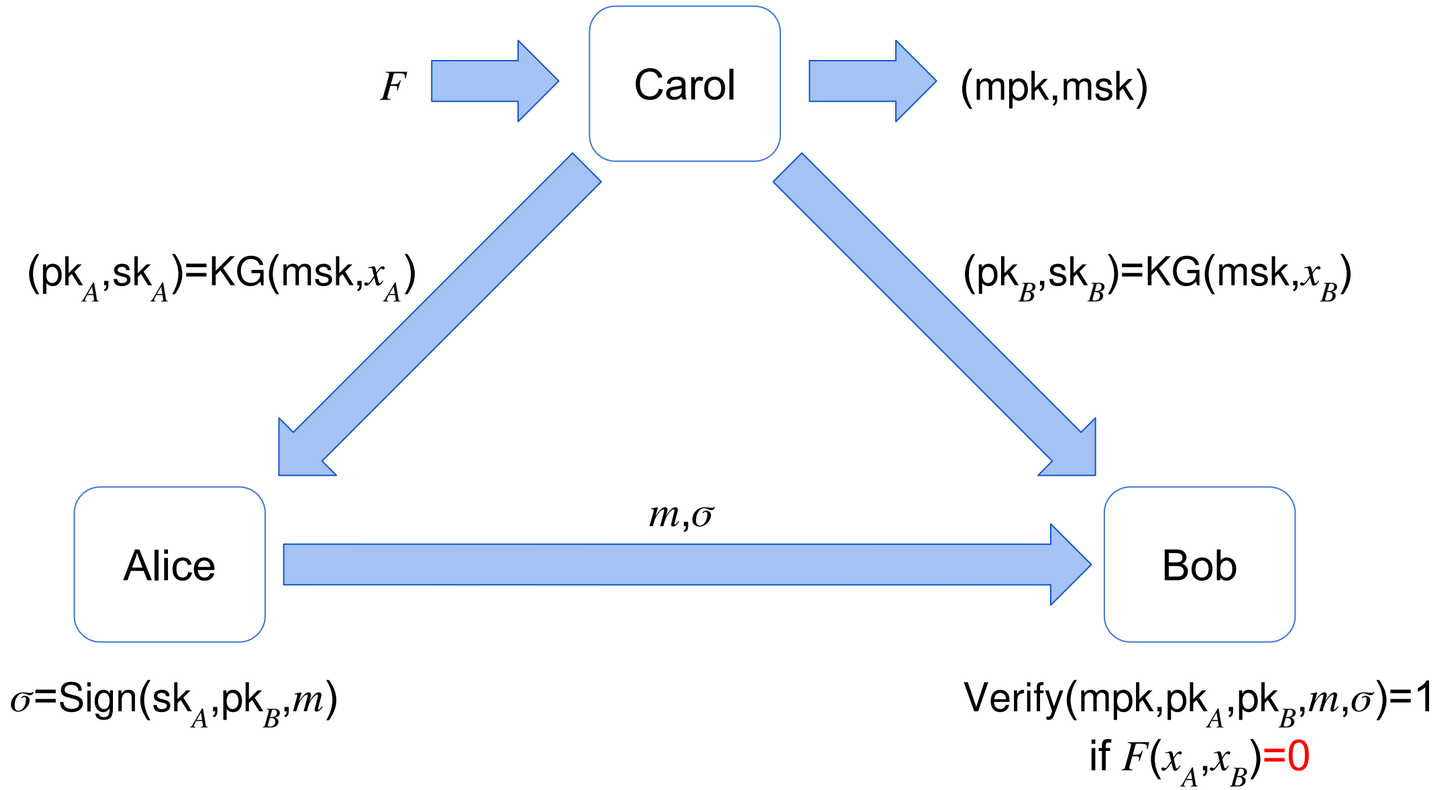
1. Key Generation Forgery

2. Signature Forgery



Unforgeability

1. Key Generation Forgery
2. Signature Forgery
3. Attribute Forgery



Unforgeability

KeyGen

x

pk

Corrupt

pk

sk

Sign

pk_S, pk_R, m

σ

pk, pk*, m*, σ*

Verify(mpk,pk,pk*,m*,σ*)=1 ∧

pk has not been queried to Cor ∨

$F(x,x^*)=0$ where x,x^* belong to pk,pk*

Attribute Hiding

1. Indistinguishability-Based

2. Simulation-Based

Attribute Hiding

1. Indistinguishability-Based

2. Simulation-Based

IND-Based Attribute Hiding

KeyGen

Corrupt

x_0=x_1

Sign

$F(x_0,y_0)$=$F(x_1,y_1)$

(x_0,x_1)

pk

pk

sk

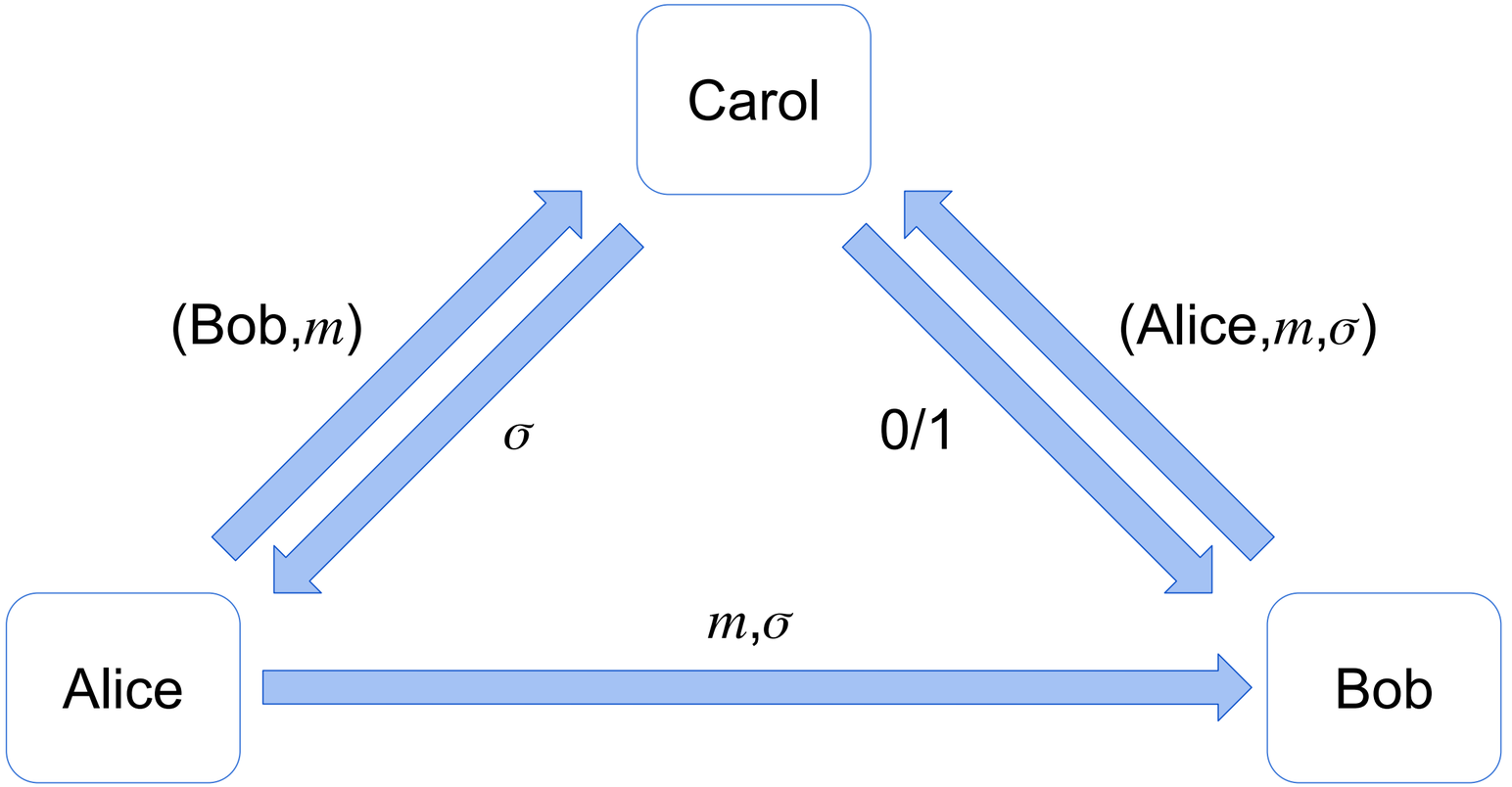
pk_x, pk_y, m

σ

b’

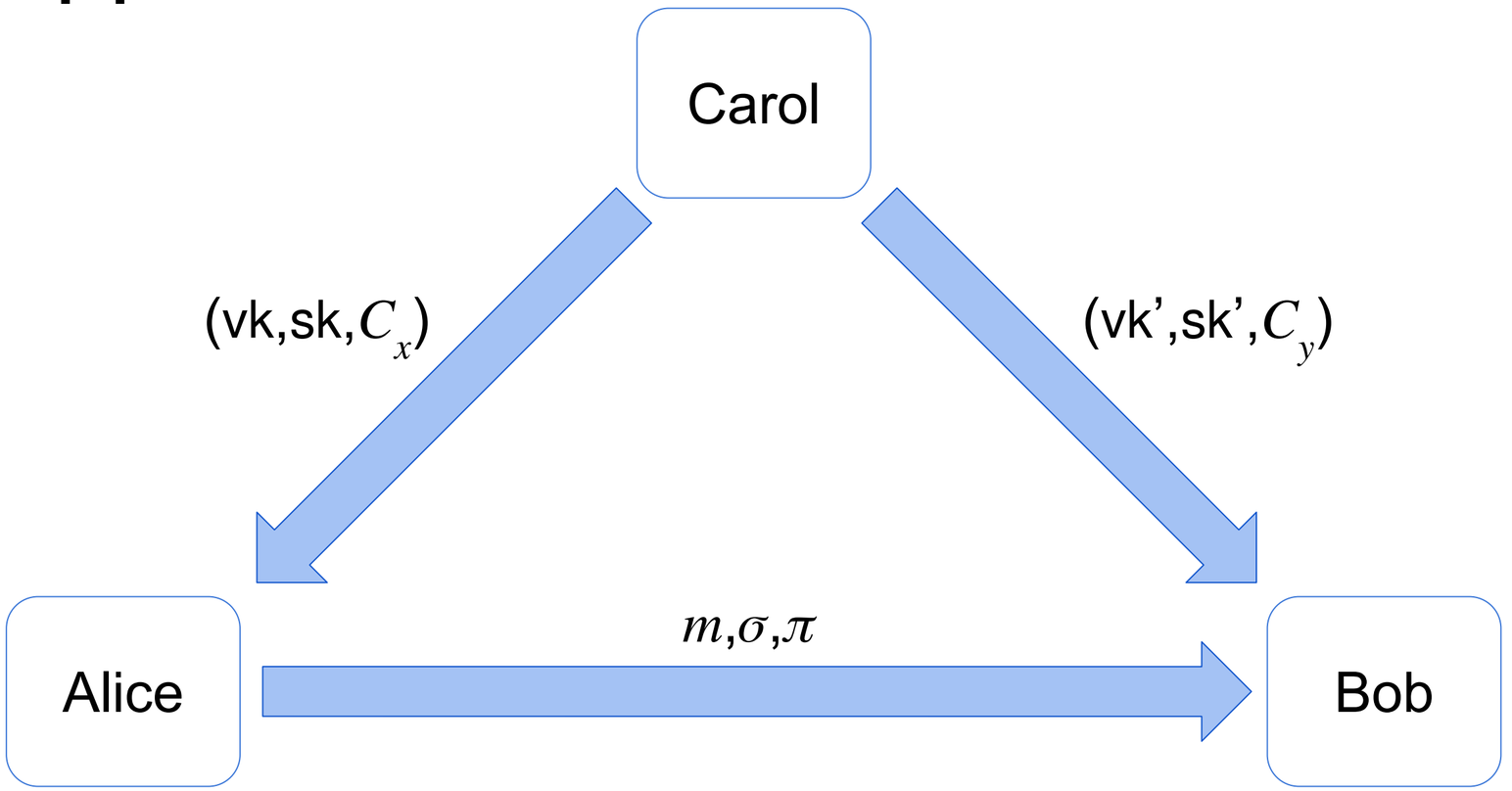
Wins if b’=b

First Approach



⇒ The Authority is needed for every Signature Generation and Verification

Second Approach



σ=Sign(sk,m)

π=Prove($F(x,y)$=1) w.r.t C_x,C_y, vk and vk'

Verify(vk,m,σ)=1

Verify(π)=1

⇒ No Attribute Privacy

Construction

Tools:

1. Digital Signatures

2. Non-Interactive Zero-Knowledge Proofs

3. Predicate Encryption

Construction

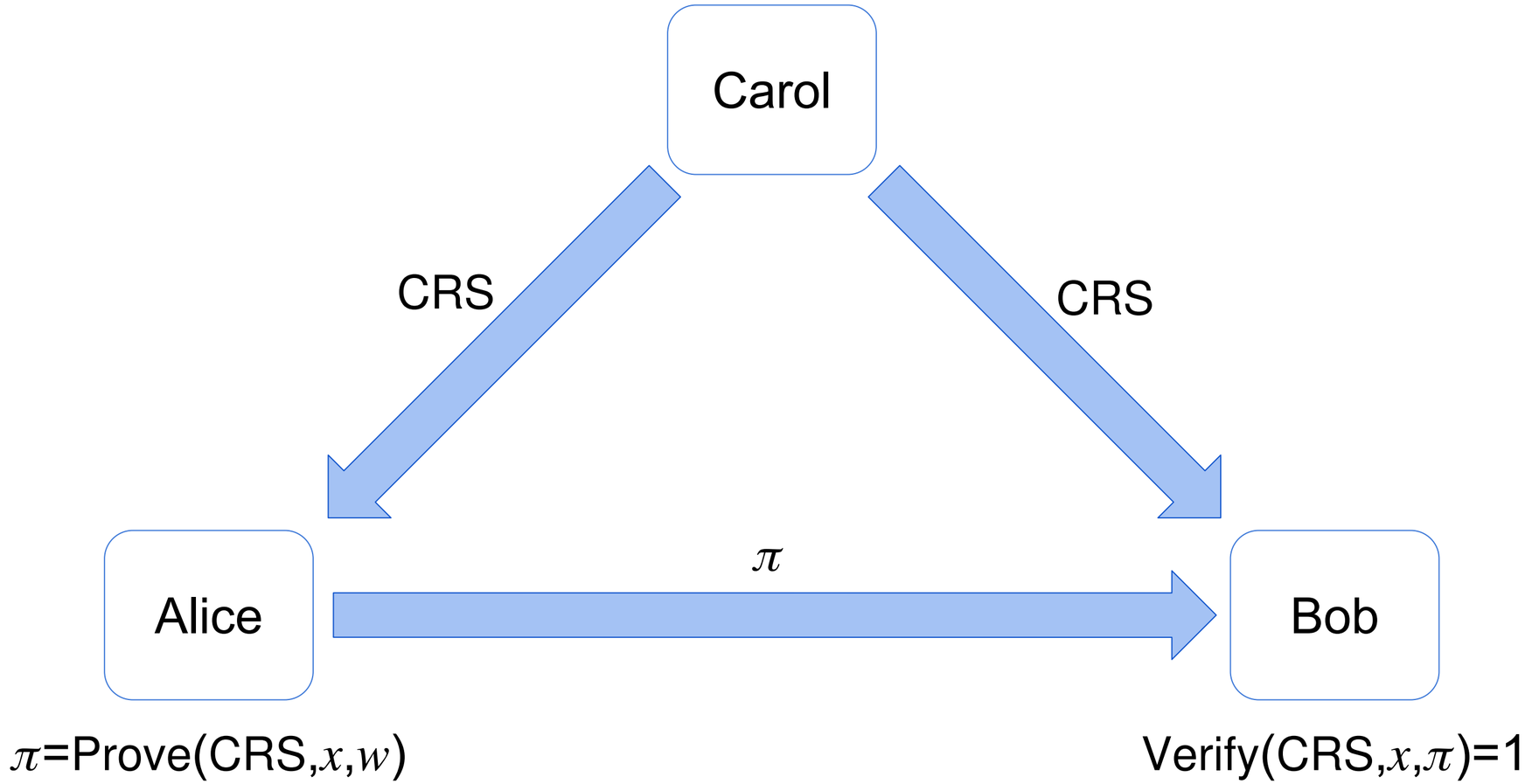
Tools:

1. Digital Signatures

2. Non-Interactive Zero-Knowledge Proofs

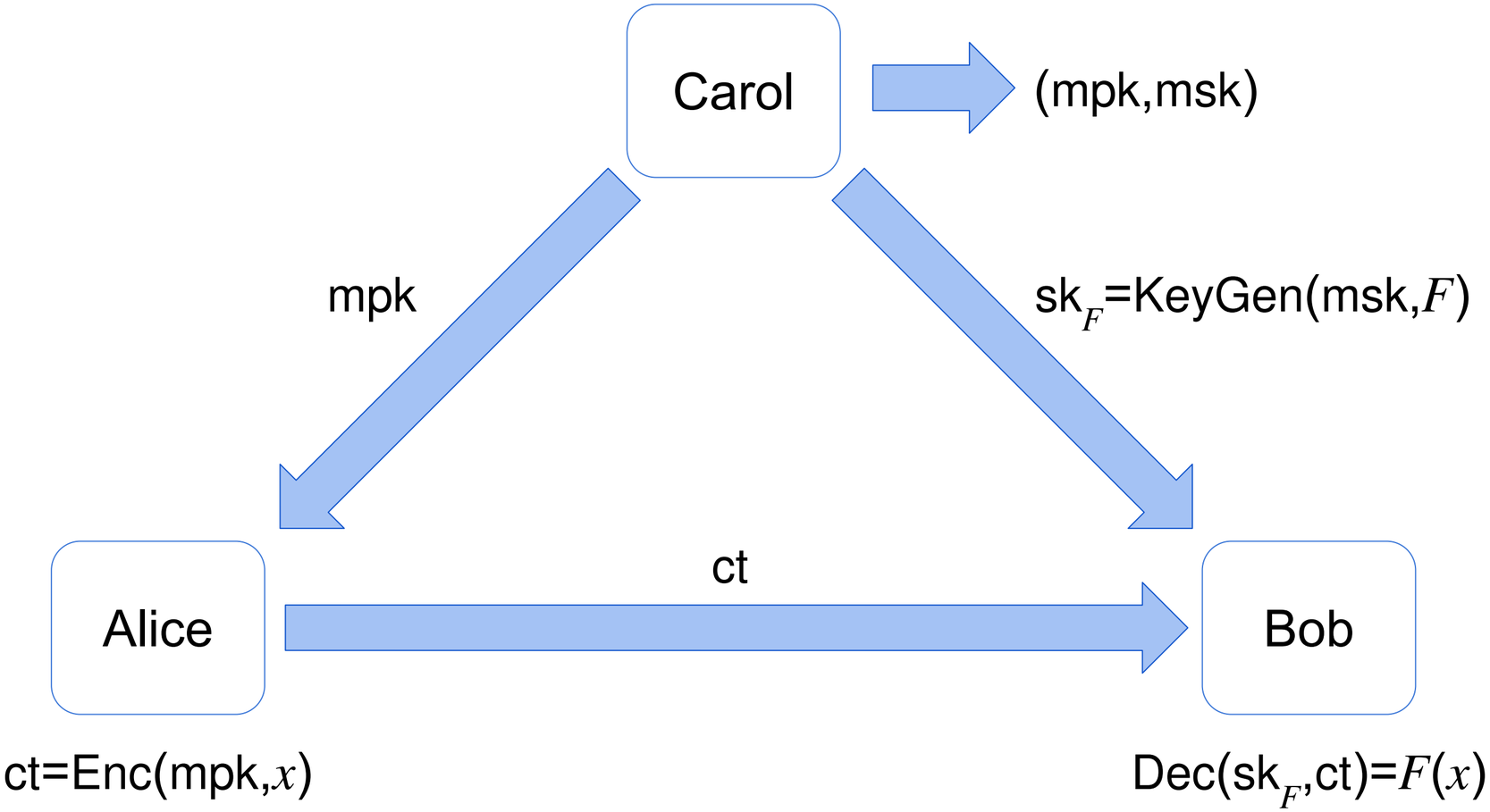
3. Predicate Encryption

Non-Interactive Zero-Knowledge Proofs [BFM88]



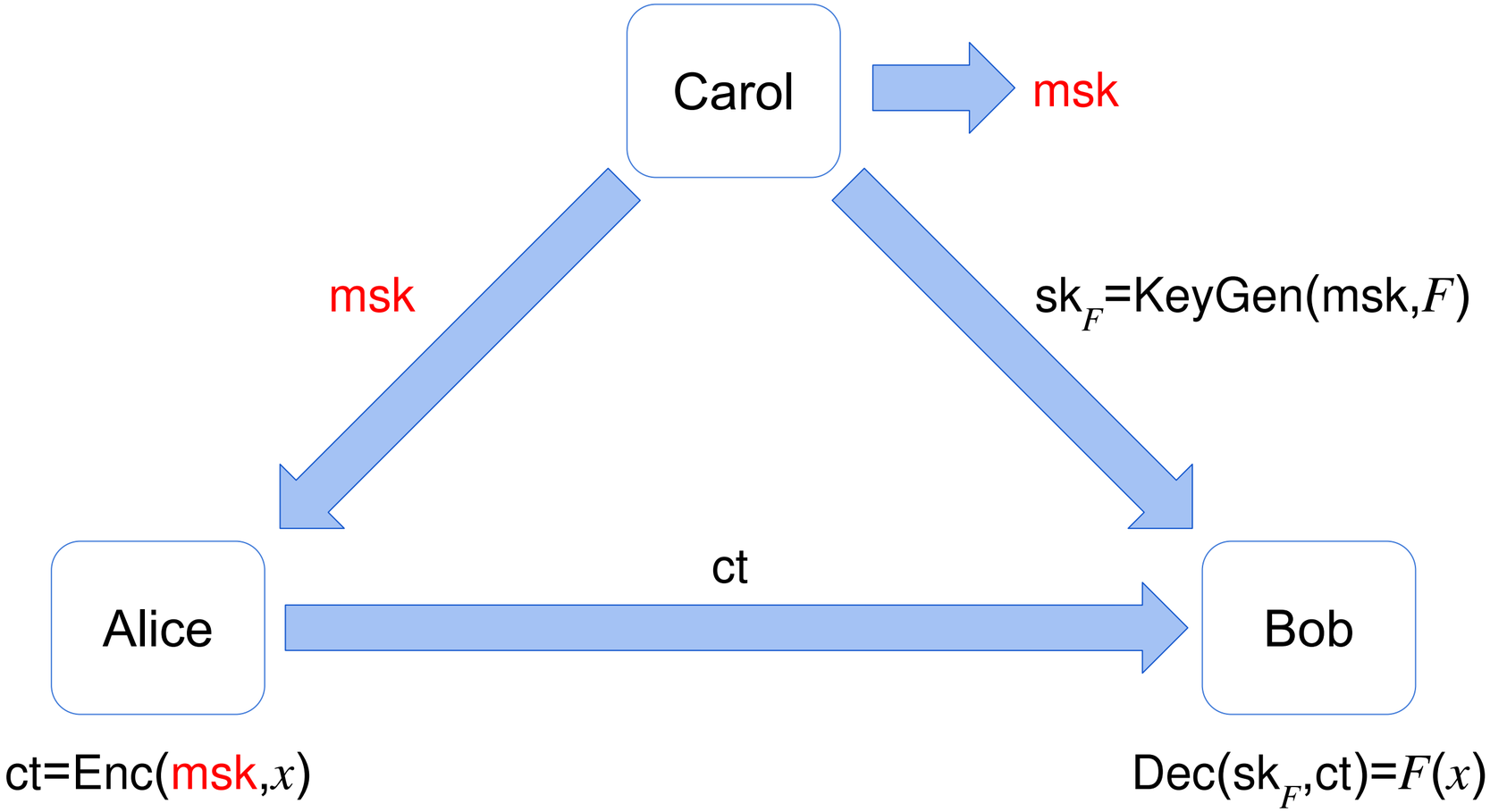
Soundness and Zero-Knowledge

Predicate Encryption [KSW07]



Attribute Hiding

Predicate Encryption [KSW07]



Attribute Hiding

Construction

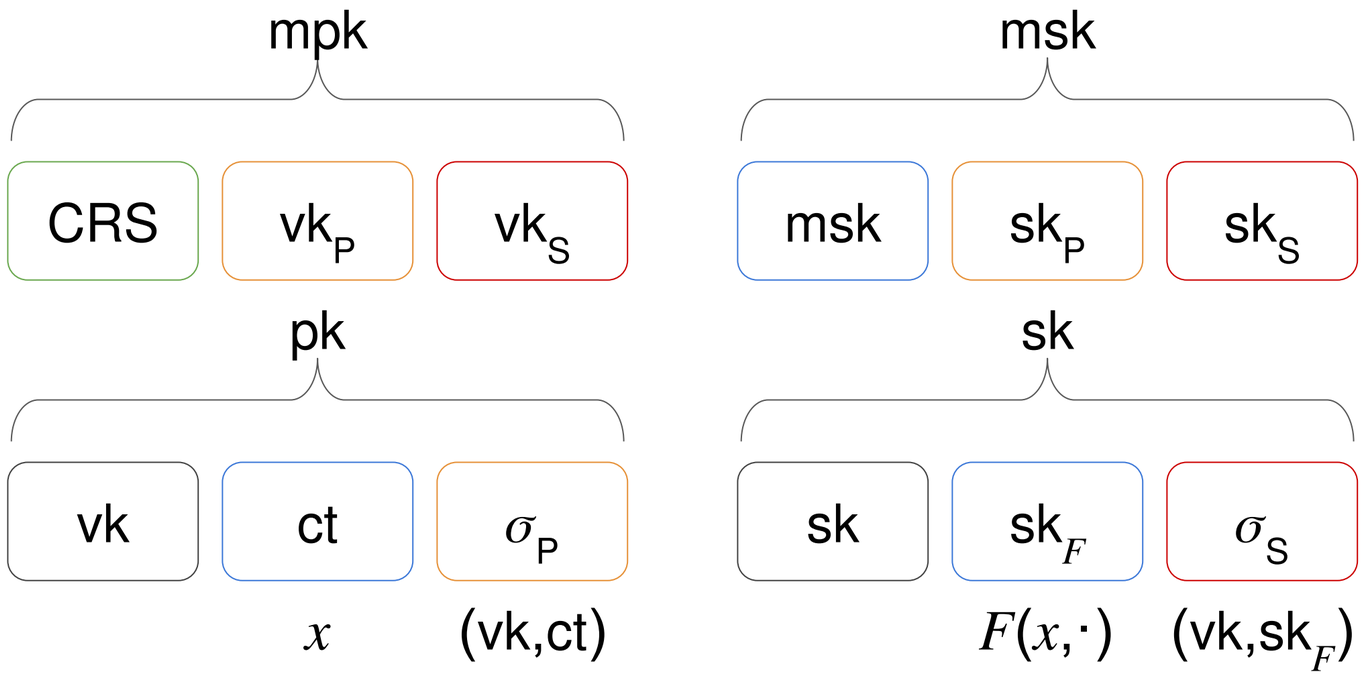
Idea:

- Use Ciphertexts to encrypt the attributes in the public key and the corresponding functional key as a component of the private key

- Generate a Signature by decrypting the ciphertext and proving that the decryption is equal to 1, i.e. the policy is fulfilled

Construction

Keys:



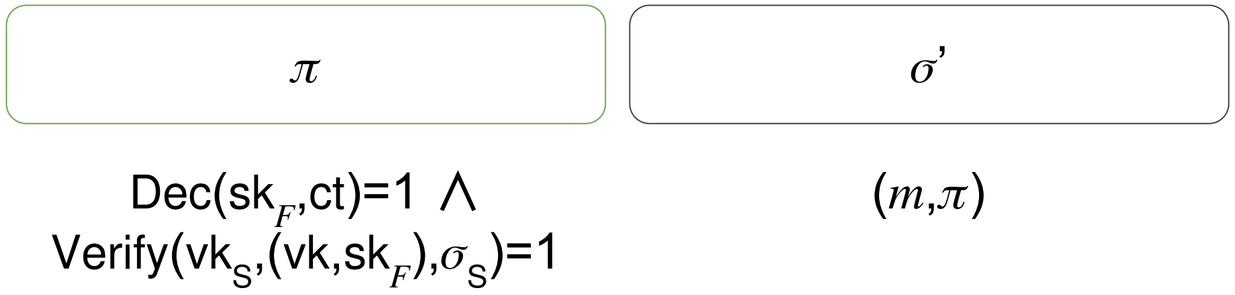
Signatures:

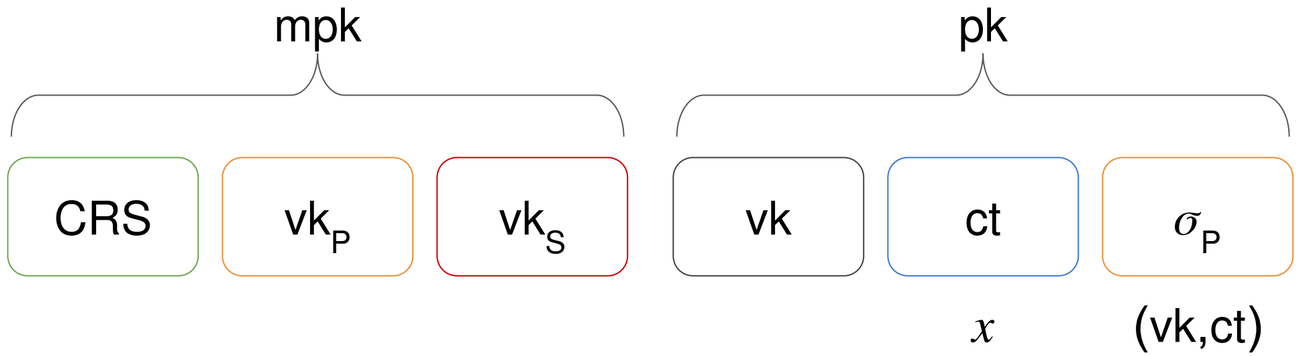
$Dec(sk_F,ct)=1 \wedge Verify(vk_S,(vk,sk_F),\sigma_S)=1$

(m,π)

Security

Unforgeability:

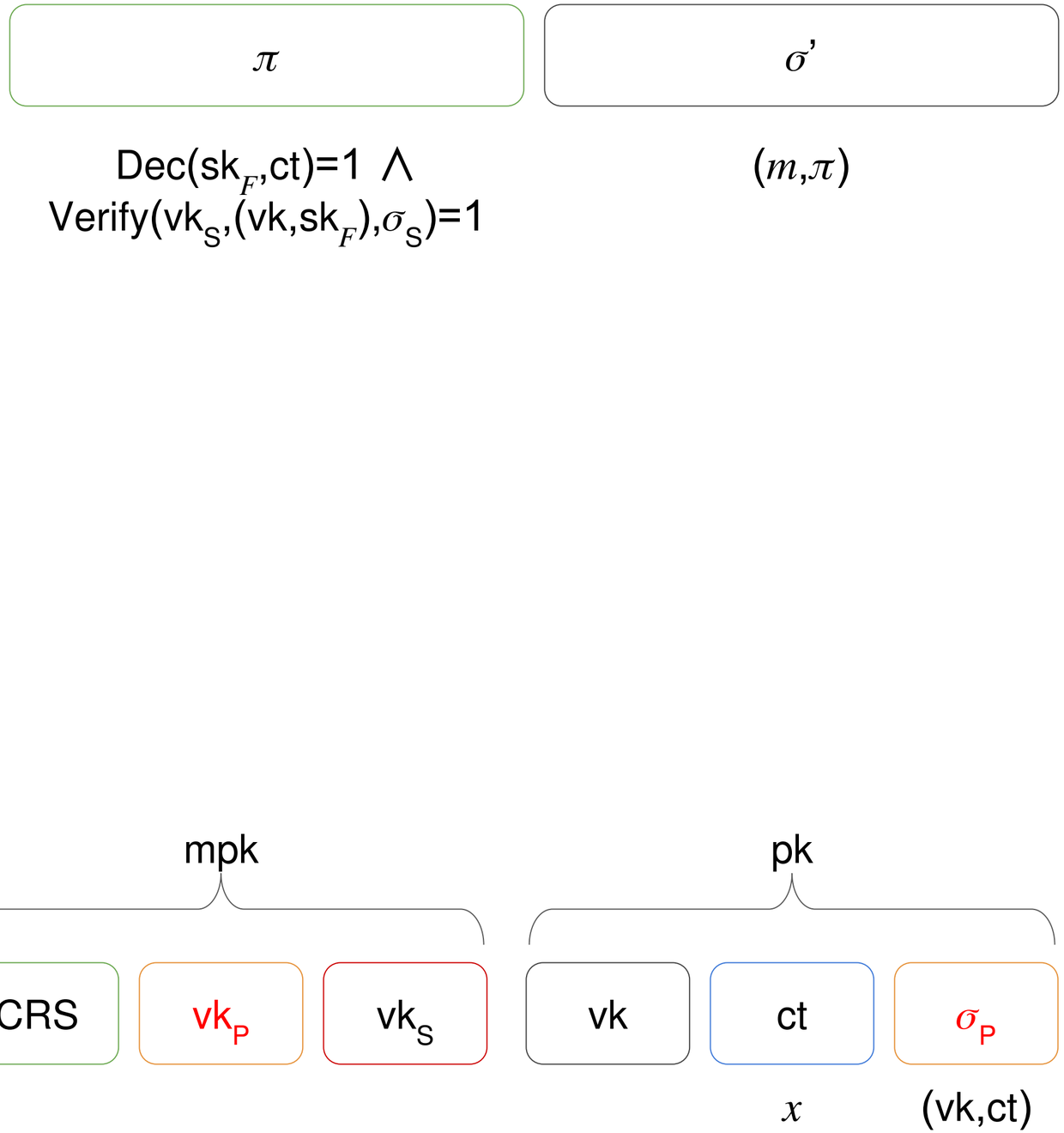




Security

Unforgeability:

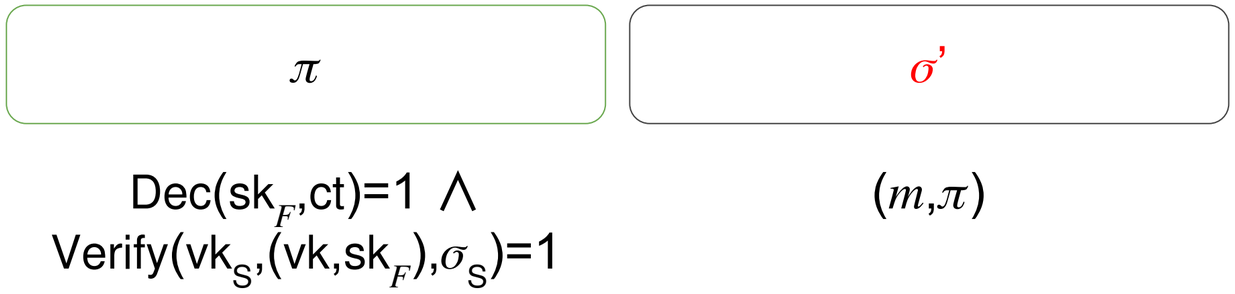
Signature Unforgeability

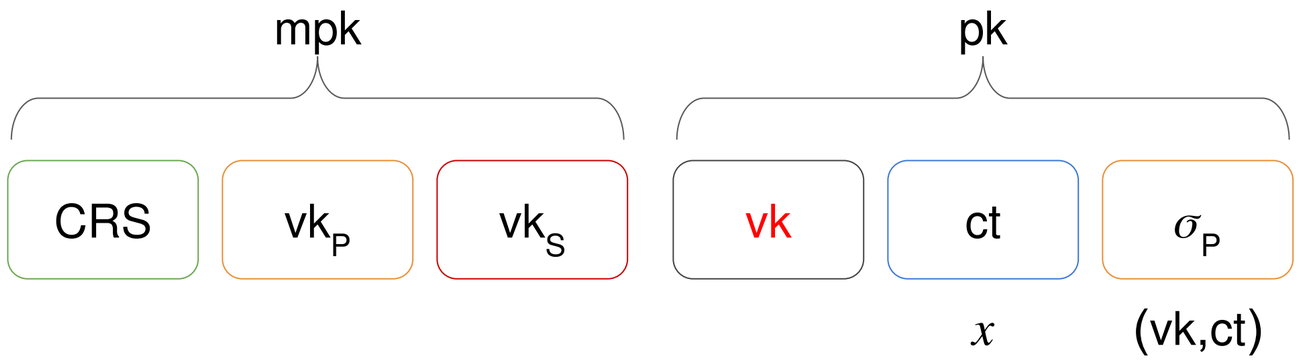


Security

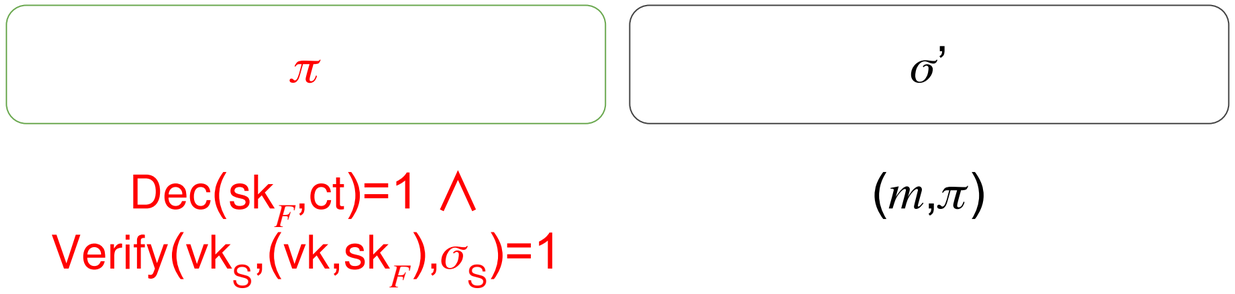
Unforgeability:

Signature Unforgeability (x2)



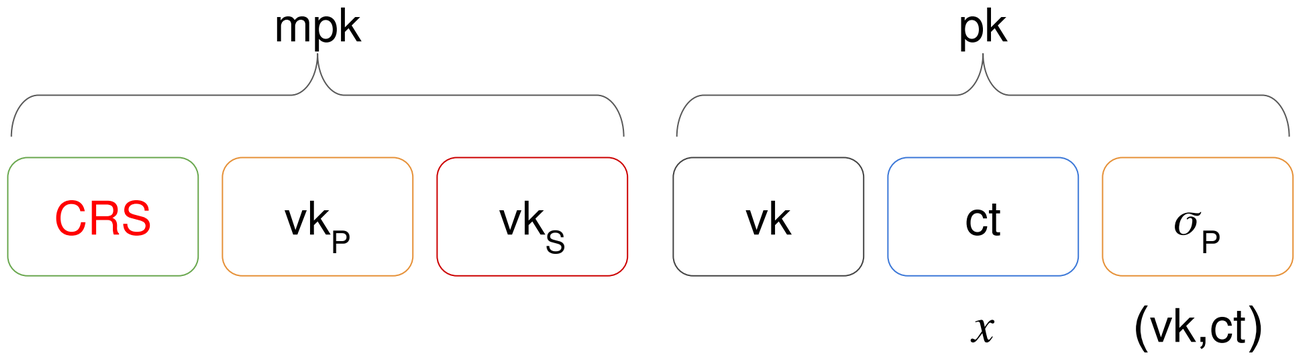


Security



Unforgeability:

Signature Unforgeability (x2) and Soundness of NIZK*

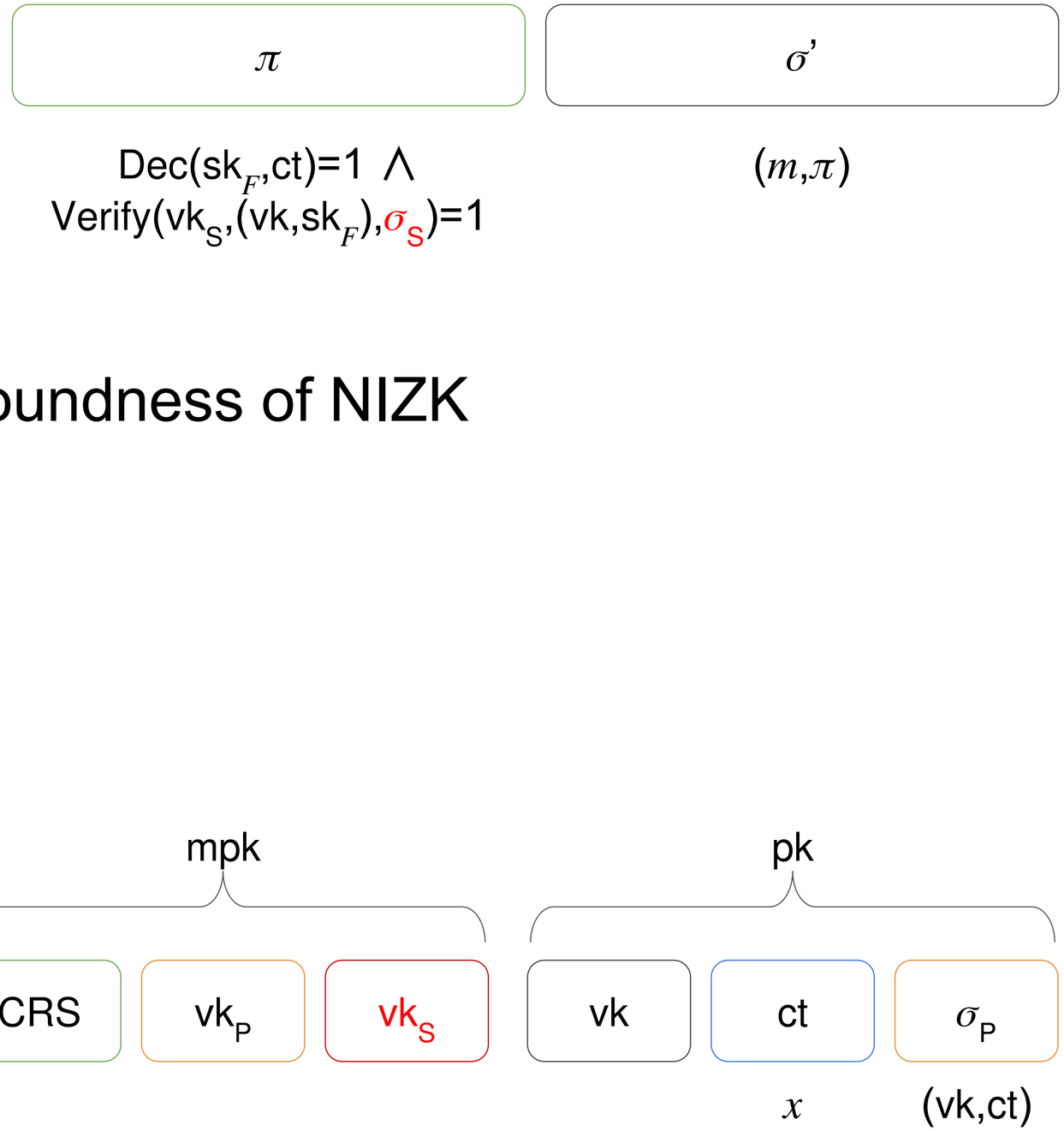


*We actually need Extractability here

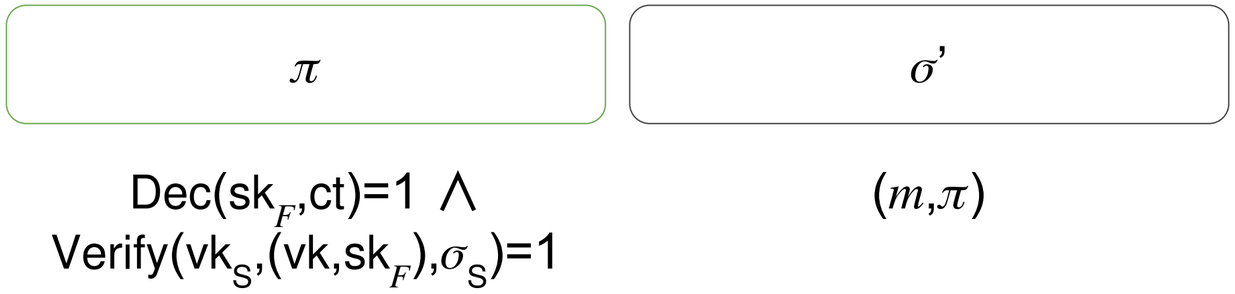
Security

Unforgeability:

Signature Unforgeability (x3) and Soundness of NIZK



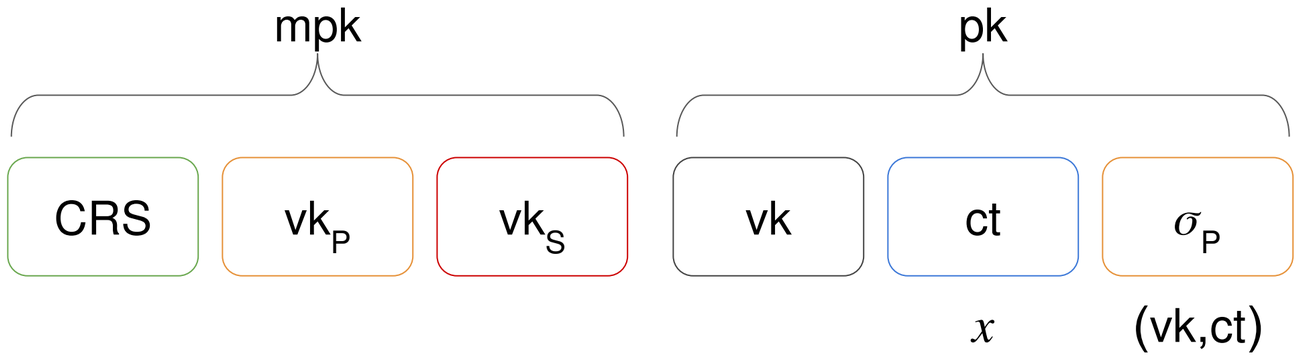
Security



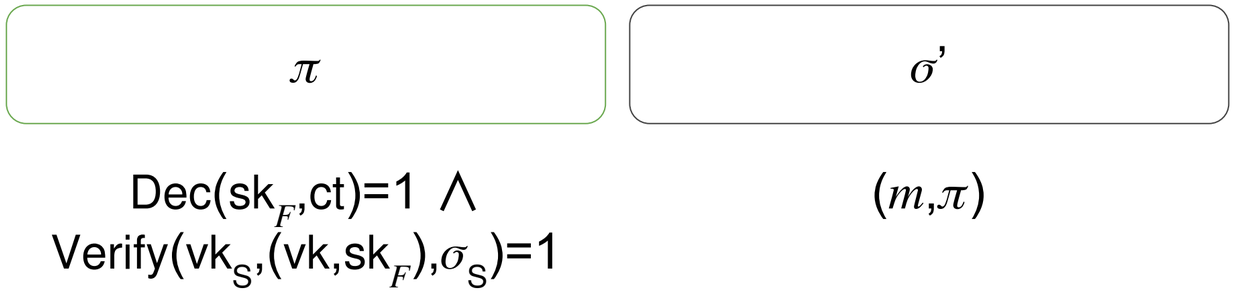
Unforgeability:

Signature Unforgeability (x3) and Soundness of NIZK

Attribute Hiding:



Security

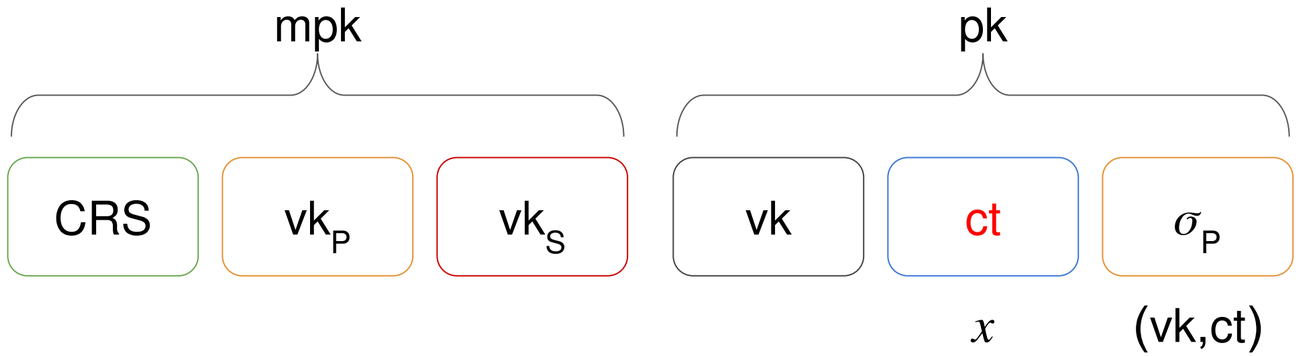


Unforgeability:

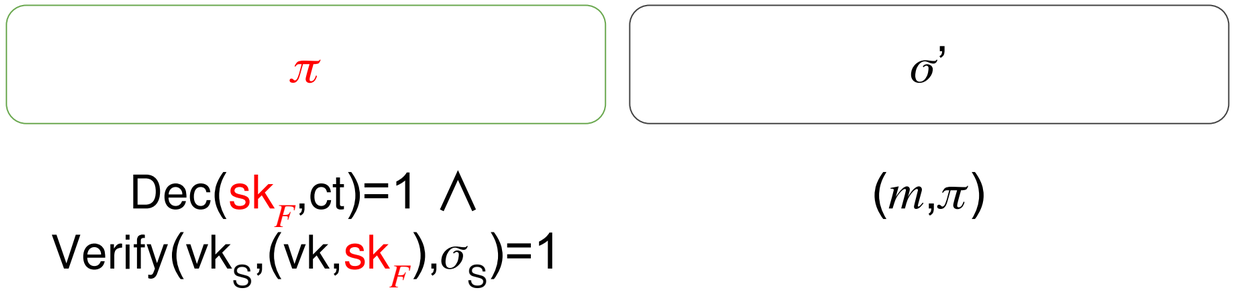
Signature Unforgeability (x3) and Soundness of NIZK

Attribute Hiding:

Attribute Hiding of PE



Security

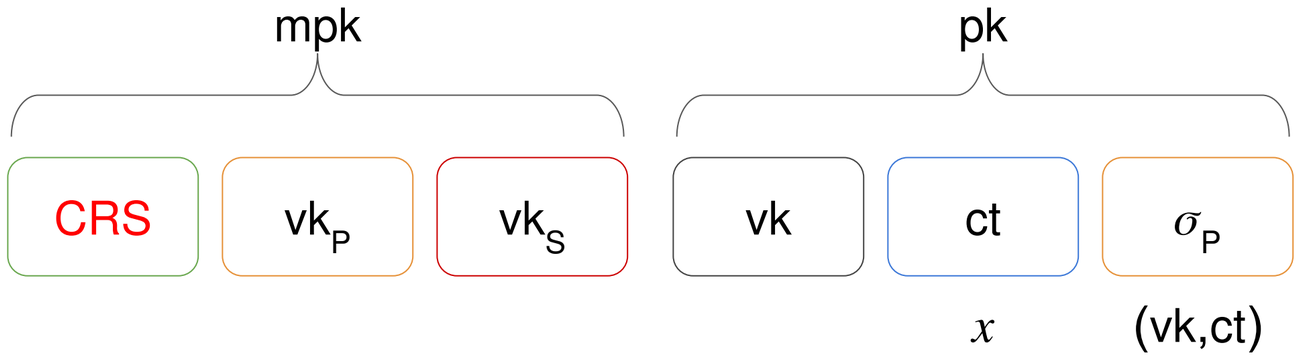


Unforgeability:

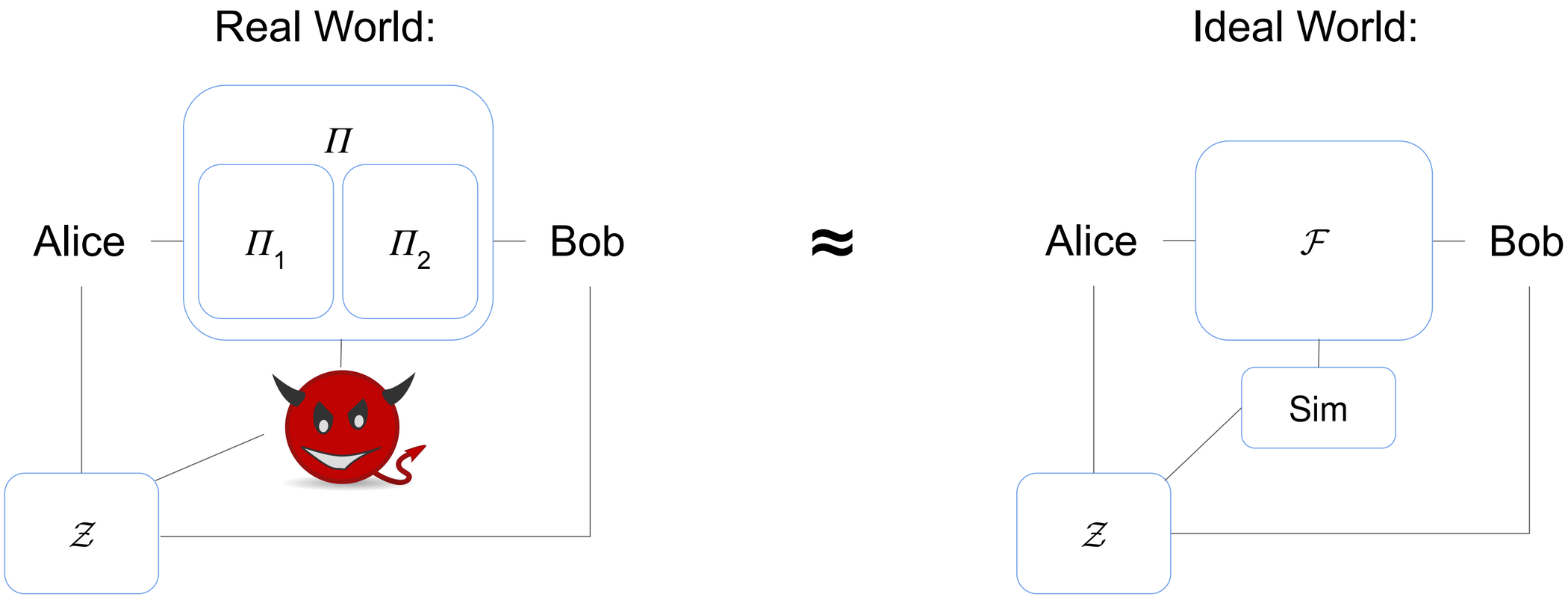
Signature Unforgeability (x3) and Soundness of NIZK

Attribute Hiding:

Attribute Hiding of PE and Zero-Knowledge Property of NIZK

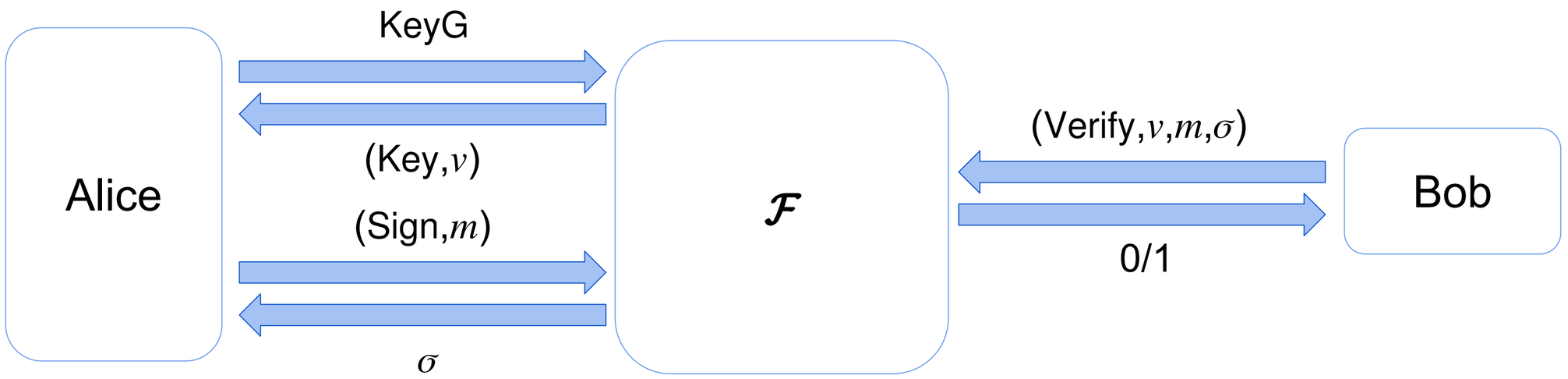


Universal Composability [Can01]

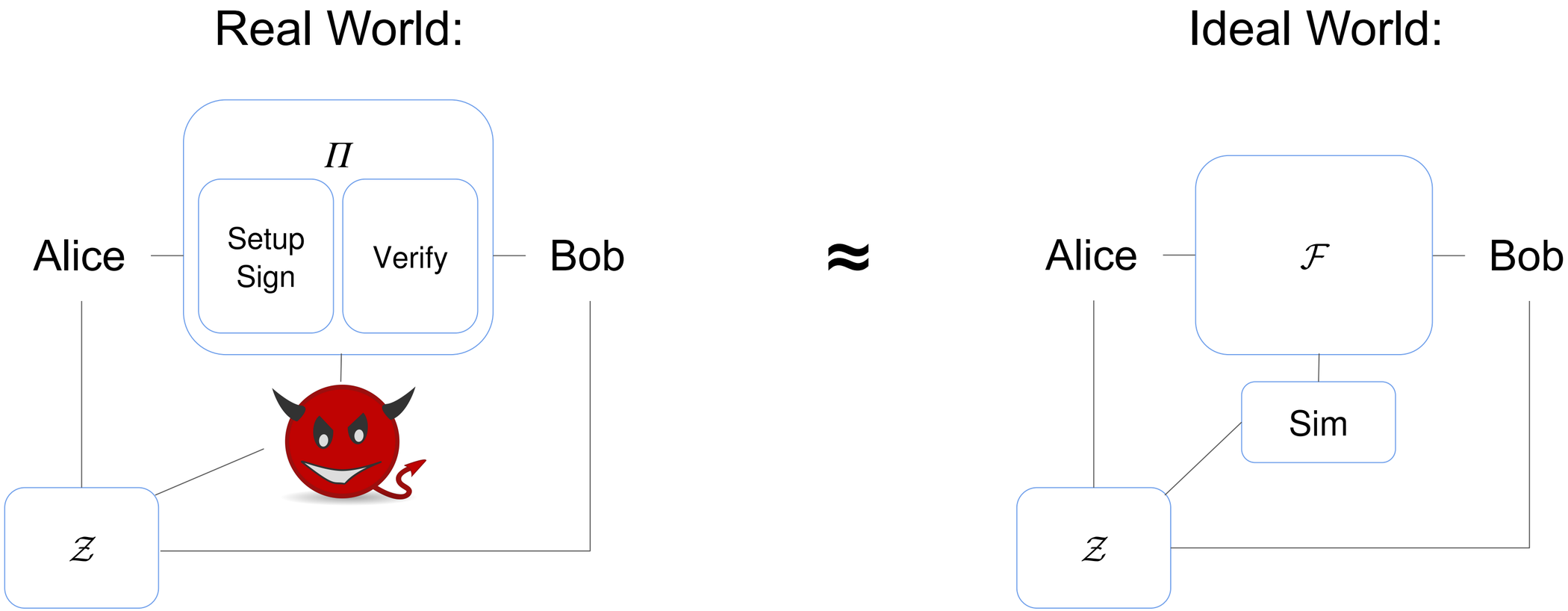


What is realized by a digital signature scheme?

Signature Functionality [Can03]

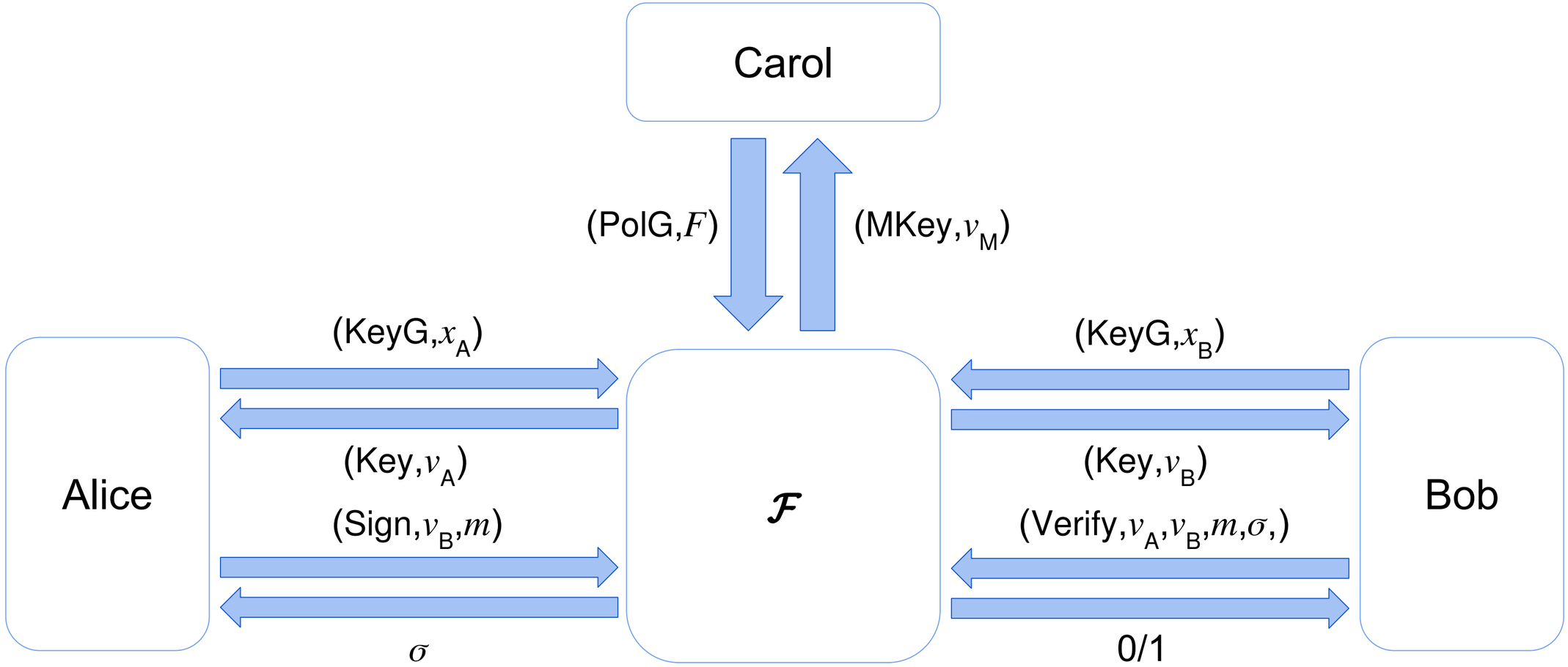


UC Realization



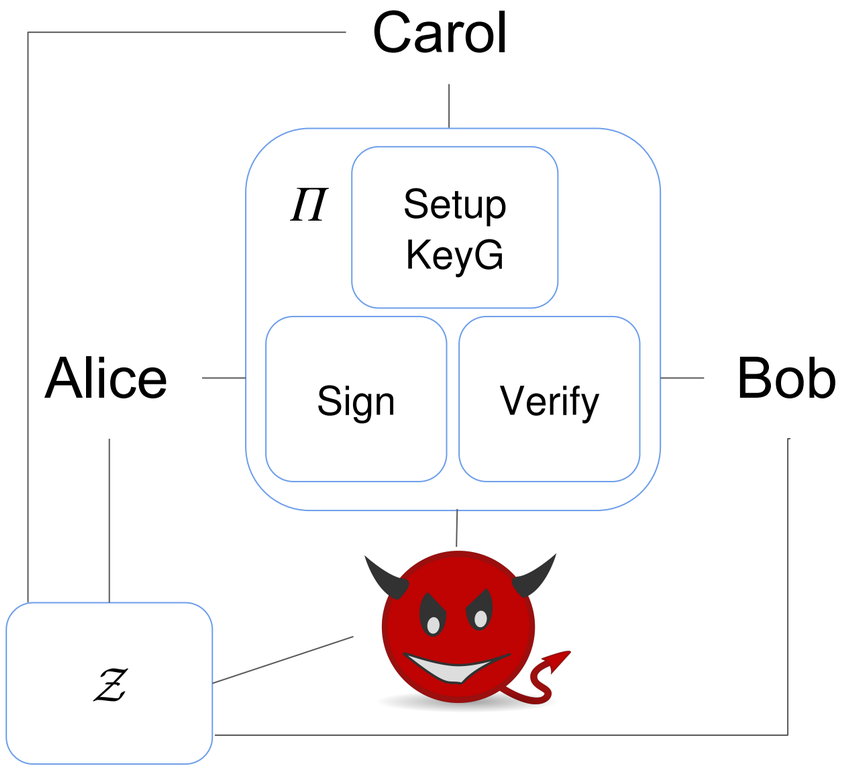
⇒ Extend this to the Policy-Compliance Setting

Policy-Compliant Signatures Functionality



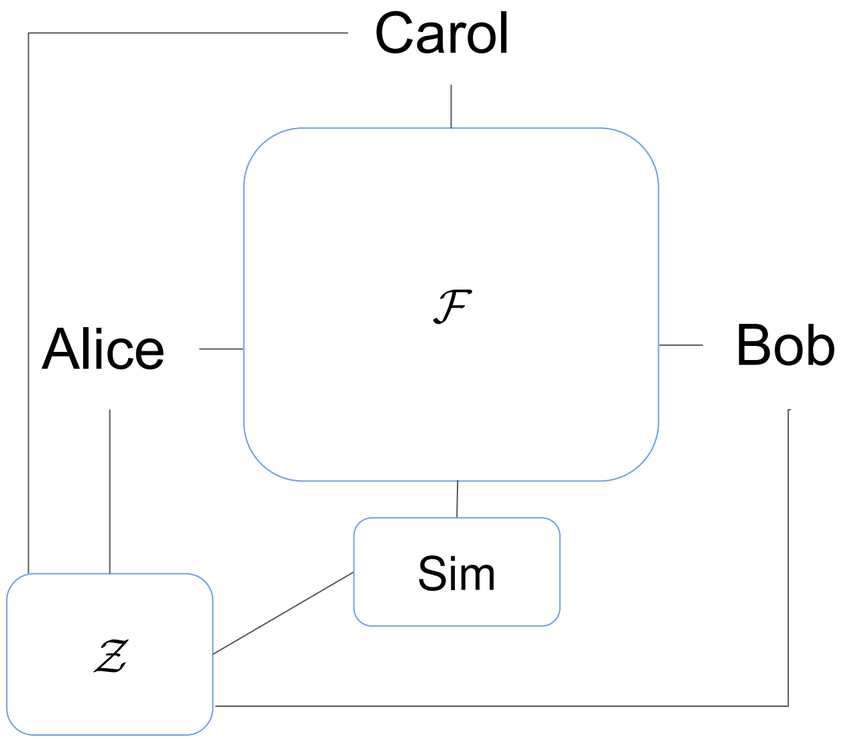
UC Realization

Real World:



$\approx$

Ideal World:



$\Rightarrow$ Requires stronger Attribute Hiding

SIM-Based Attribute Hiding

KeyGen

Corrupt

x_0=x_1

Sign

$F(x_0,y_0)$=$F(x_1,y_1)$

(x_0,x_1)

pk

pk

sk

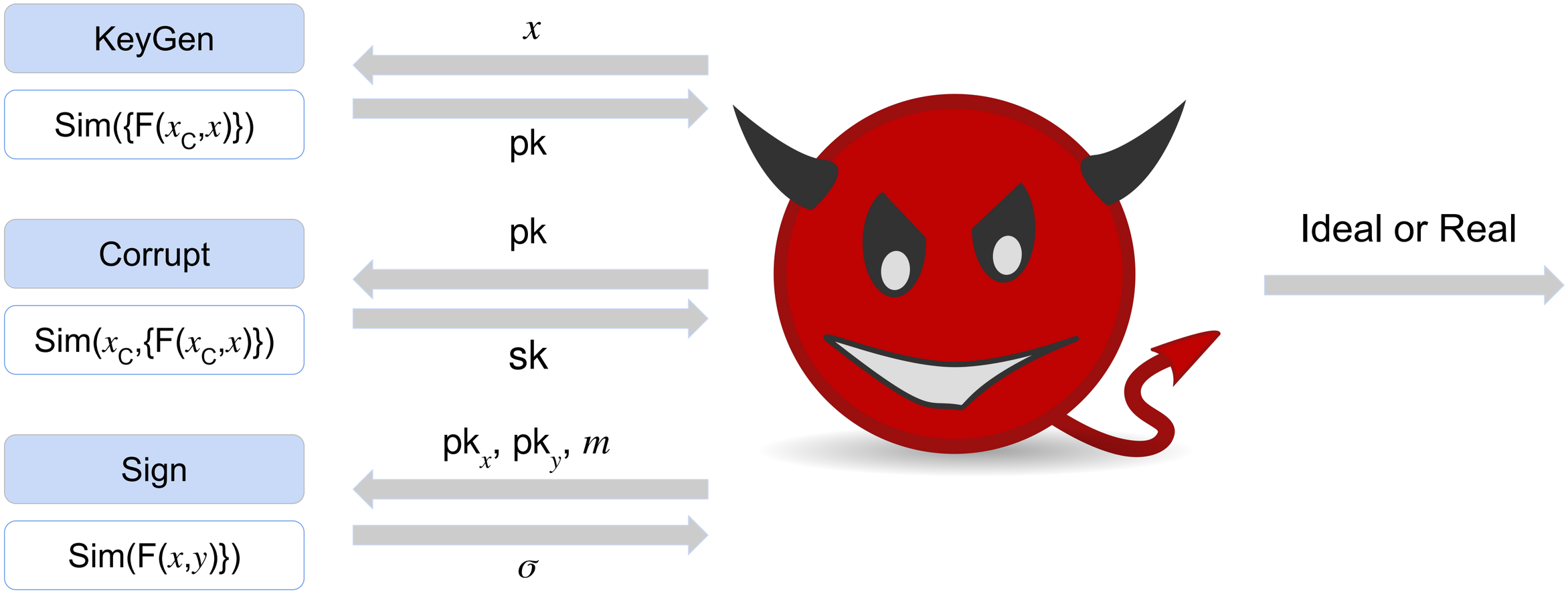
pk_x, pk_y, m

σ

b’

Wins if b’=b

SIM-Based Attribute Hiding



⇒ This is sufficient for the UC realization

Summary

1. Introduction of Policy-Compliant Signatures
    a. Unforgeability
    b. IND-Based Attribute Hiding
2. A Policy-Compliant Signature Scheme
3. UC Realization
    a. SIM-Based Attribute Hiding

Thank You

For Your Attention