Signatures Resilient to Uninvertible Leakage

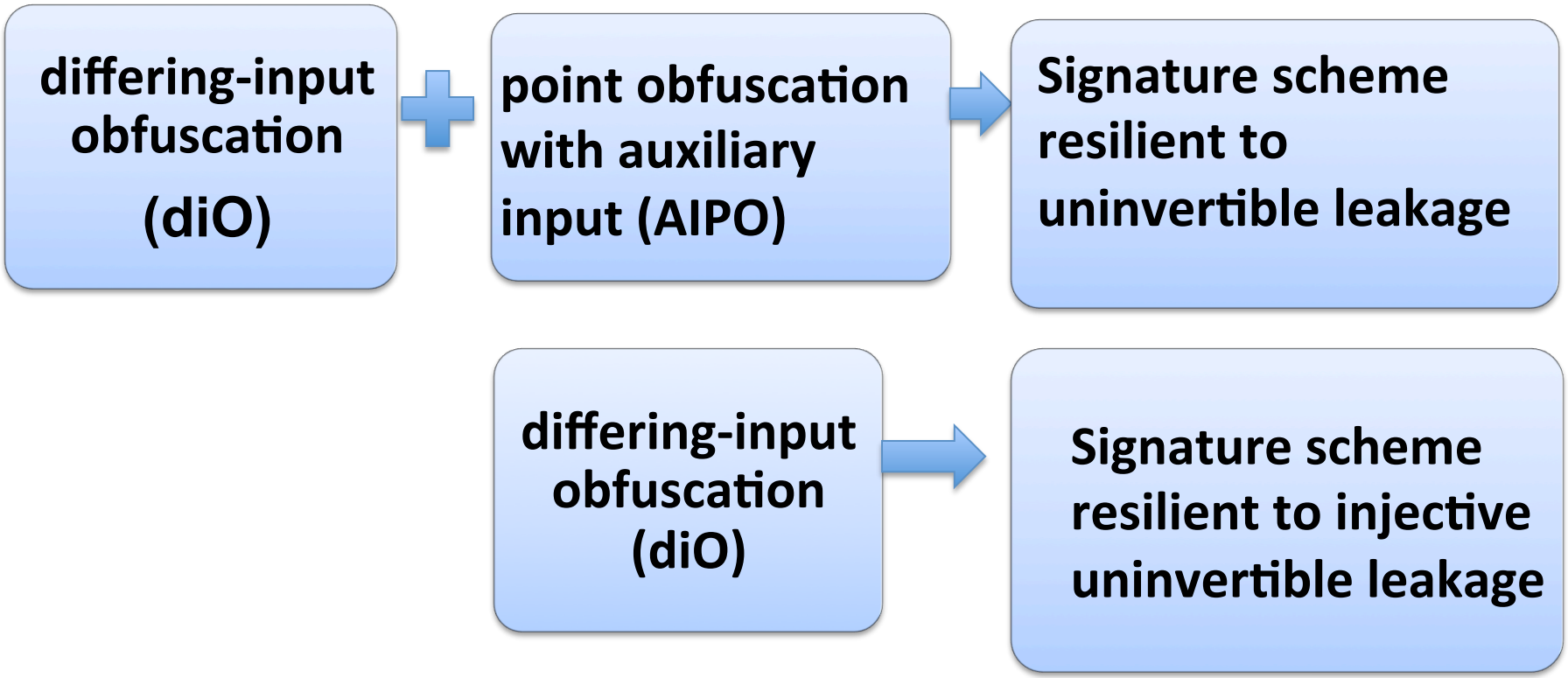
Yuyu Wang[1,2], Takahiro Matsuda[2],
Goichiro Hanaoka[2], and Keisuke Tanaka[1,3]

1 Tokyo Institute of Technology

2 AIST

3 JST CREST, Tokyo, Japan

Our work


differing-input obfuscation (diO)
point obfuscation with auxiliary input (AIPO)
Signature scheme resilient to uninvertible leakage
differing-input obfuscation (diO)
Signature scheme resilient to injective uninvertible leakage

Road map

- Background
- Our result
- Tools
- Our technique

Signatures

Signer

sk

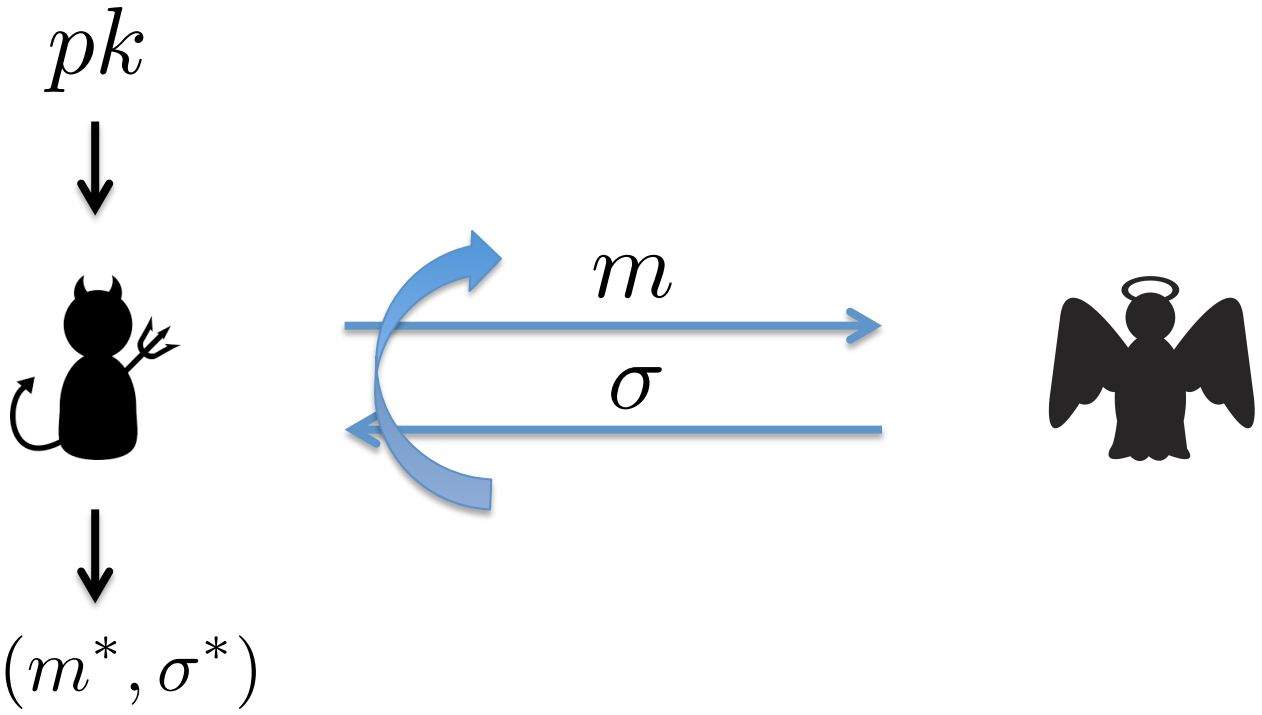
(m, σ)

Verifier

pk

$$\sigma \leftarrow \mathrm{Sign}_{sk}(m, r) \qquad \mathrm{Verify}_{pk}(m, \sigma) \stackrel{?}{=} 1$$

EUF-CMA security



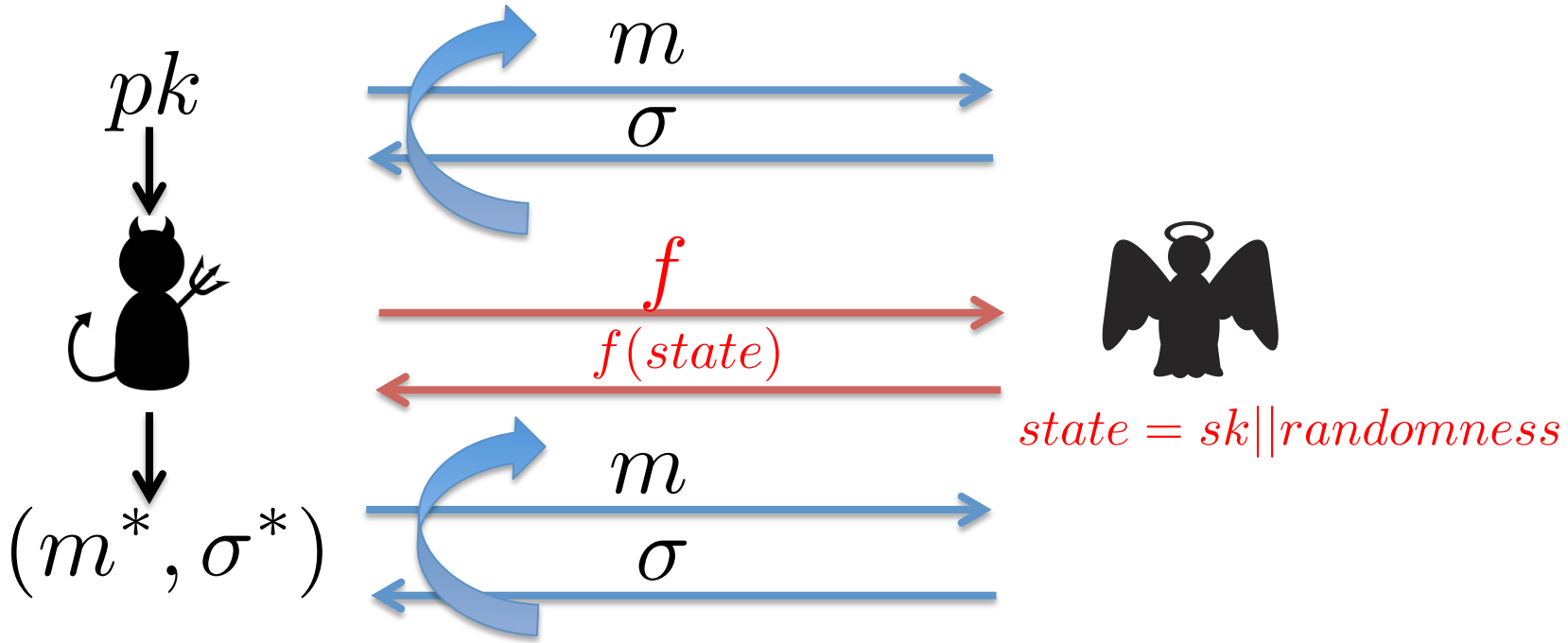
EUF-CMA security: if m* was not part of the queries, then the probability that the forgery is successful is negligible.

The secret information is completely hidden

Side channel attack

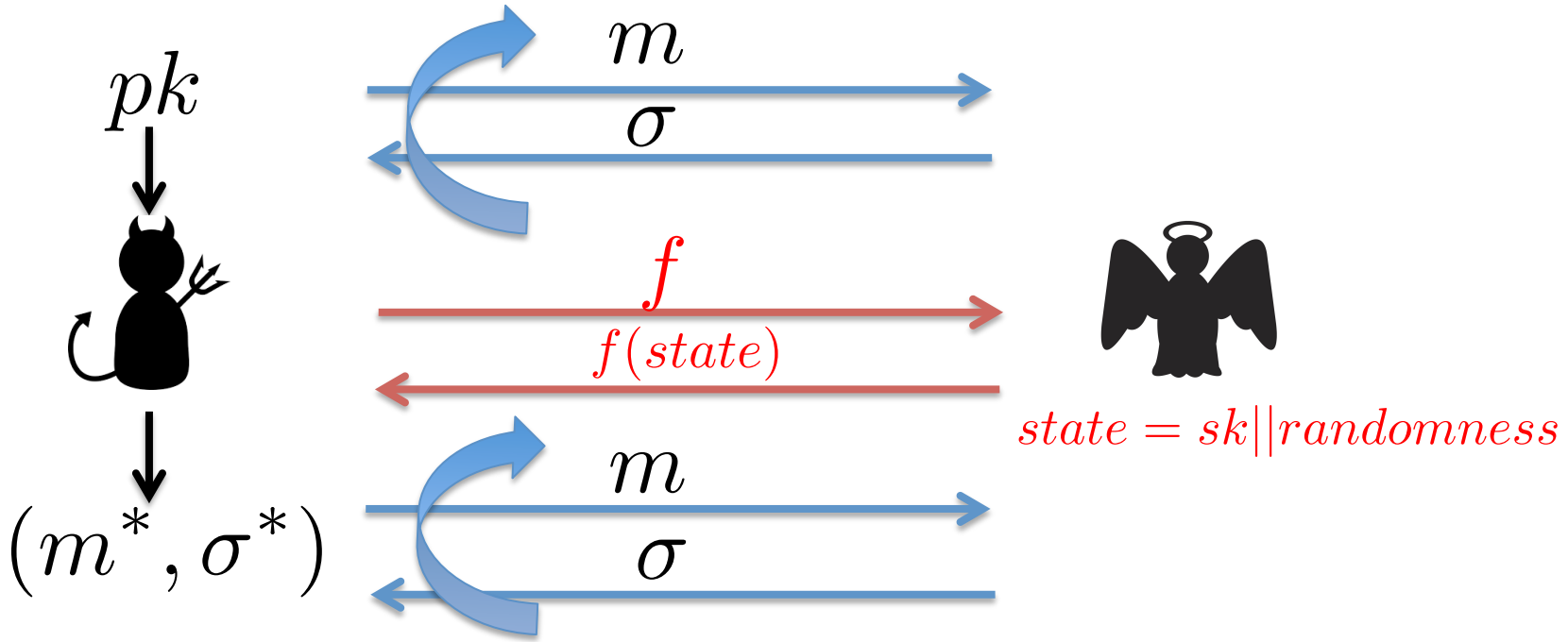
Secret information may be leaked via physical information from the device.

Leakage models

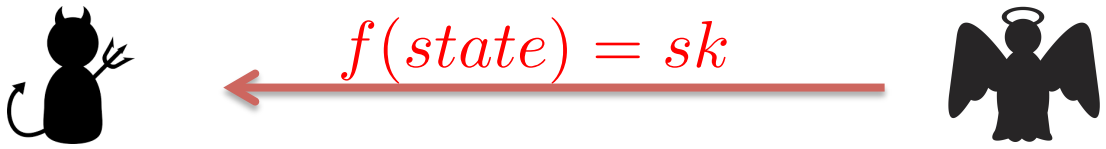


EUF-CMA security: if m* was not part of the queries, then the probability that the forgery is successful is negligible.

Leakage models



If f can be any function



Restriction on leakage functions

- Bounded leakage model, continual leakage model, noisy leakage model: part of the signing key is information-theoretically hidden in the presence of $f(state)$.

- Practical world: $f(state)$ typically information-theoretically determines $state$. [Standaert, Invited Talk, SKEW 2011]

Auxiliary input model [DKL09]

- Restriction on f: hard-to-invert, i.e., it is hard to computationally recover signing key from leakage.
- Trivial attack for signatures in this model:

$$f(\cdot) = sign(pk, \cdot, m^*)$$

$$f(sk) = sign(pk, sk, m^*) = \sigma^*$$

Successful forgery

More restrictions on f

- Auxiliary input model [FHNN12]:
  - f is exponentially hard-to invert, and may depend on the public parameters.
  - Full leakage is not considered.
- Selective auxiliary input model [YYH12]
  - f is independent of public parameters, but polynomially hard-to-invert.

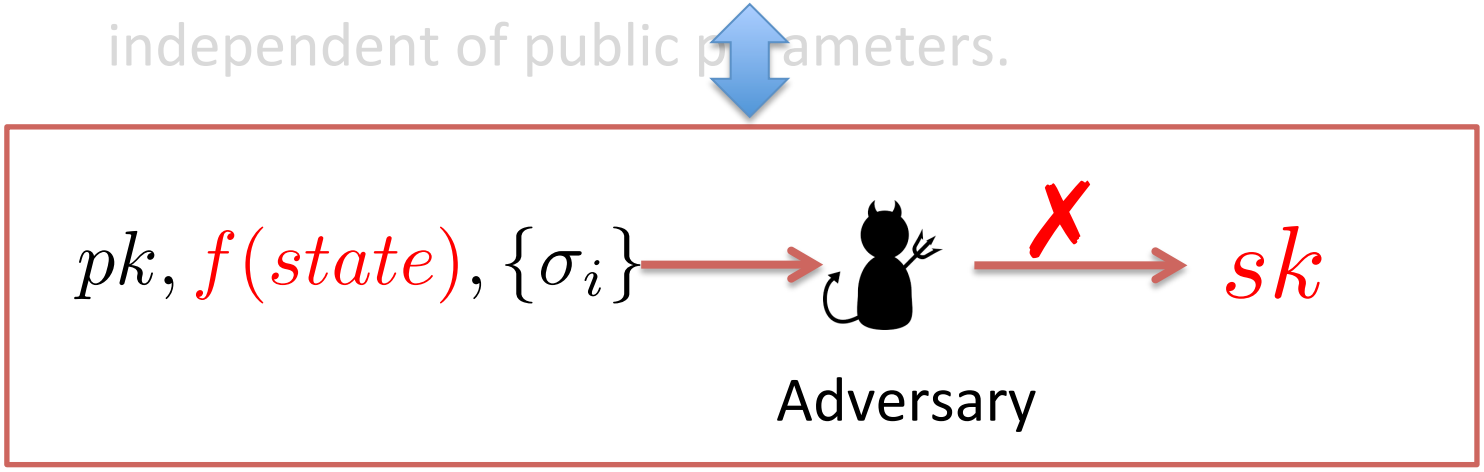
More restrictions on f

- Auxiliary input model [FHNN12]:
  - is exponentially hard-to invert, and may depend on the public parameters.
  - Full leakage is not considered.
- Selective auxiliary input model [YYH12]
  - f is independent of public parameters, but polynomially hard-to-invert

We concentrate on signatures in the latter model

More restrictions on f

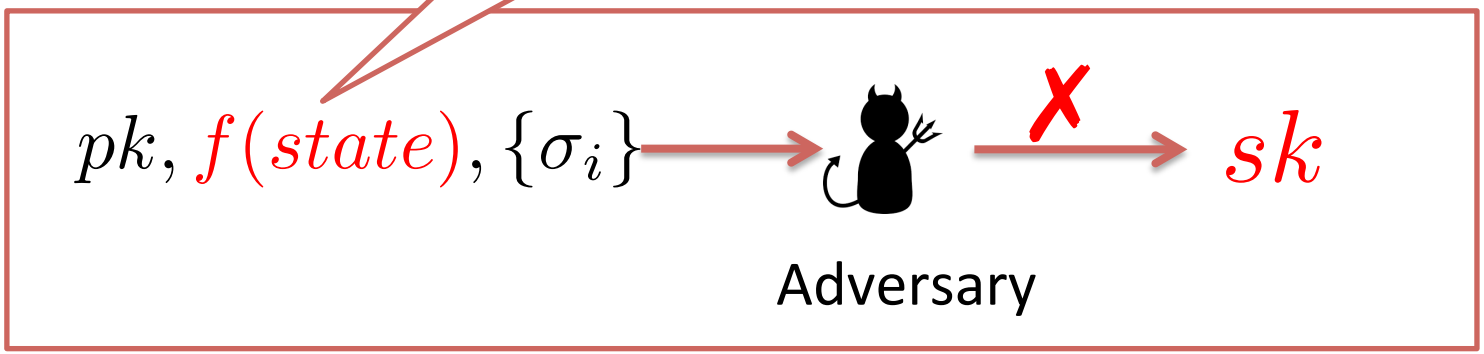
- Auxiliary input model [FHNN12]:
  - is exponentially hard-to invert, selectively chosen, and may depend on the public parameters.
- Selective auxiliary input model [YYH12]
  - is polynomial hard-to-invert, selectively chosen, but independent of public parameters.



More restrictions on f

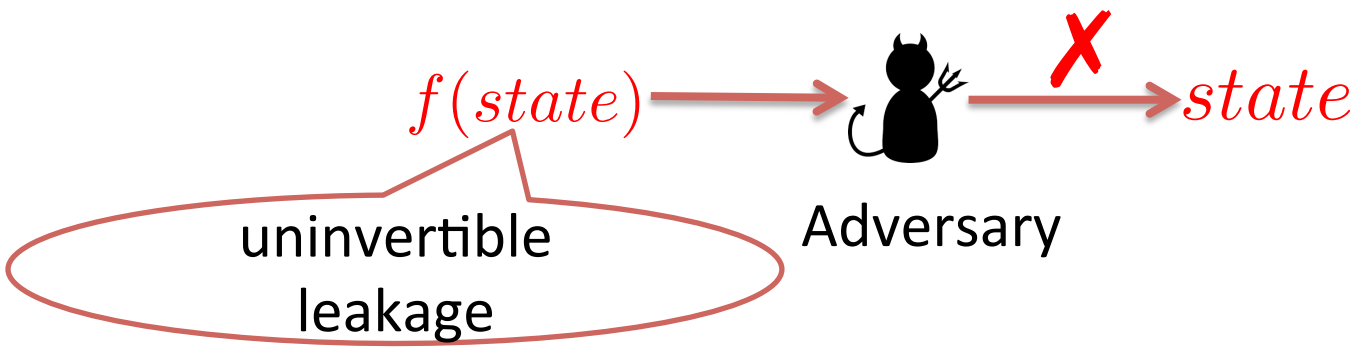
- Auxiliary input model [FHNN12]:
  - is exponentially hard-to invert, selectively chosen, and may depend on the public parameters.
- Selective a
  - is polynomial h invert, selectively chosen, but independent of ic parameters.

Can f be any uninvertible function?



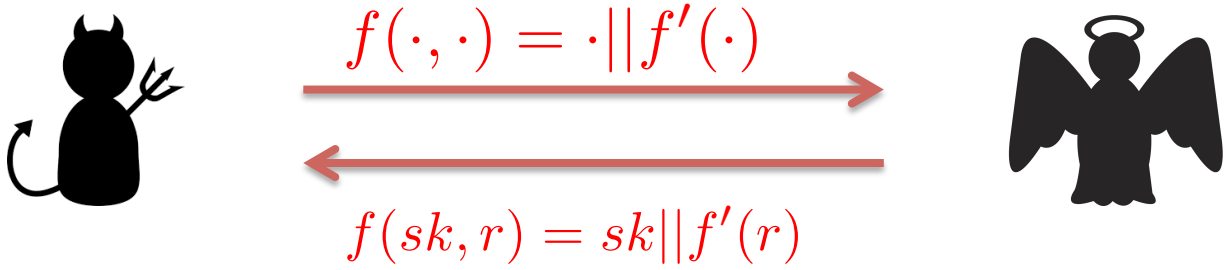
More restrictions on f

- Auxiliary input model [FHNN12]:
  - is exponentially hard-to invert, selectively chosen, and may depend on the public parameters.
- Selective auxiliary input model [YYH12]
  - is polynomial hard-to-invert, selectively chosen, but independent of public parameters.



Trivial attack by using uninvertible leakage

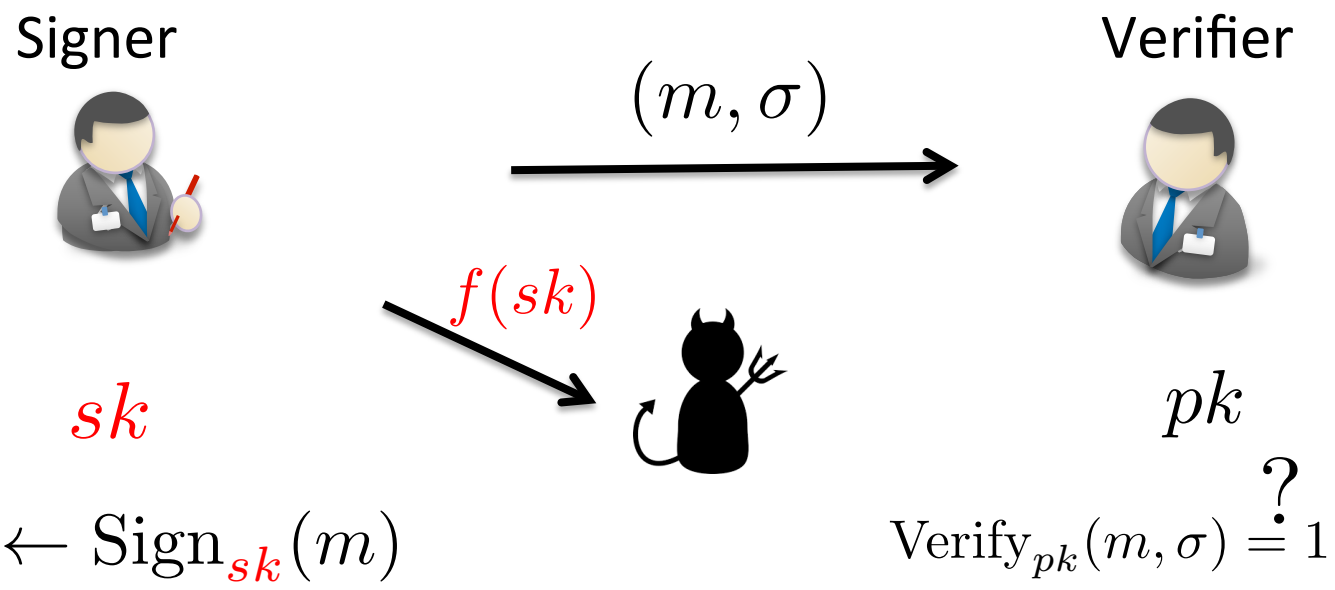
f':uninvertible



uninvertible leakage

How to avoid the trivial attack

- Deterministic signatures or signatures with public coin construction $\Rightarrow$ $state = sk$

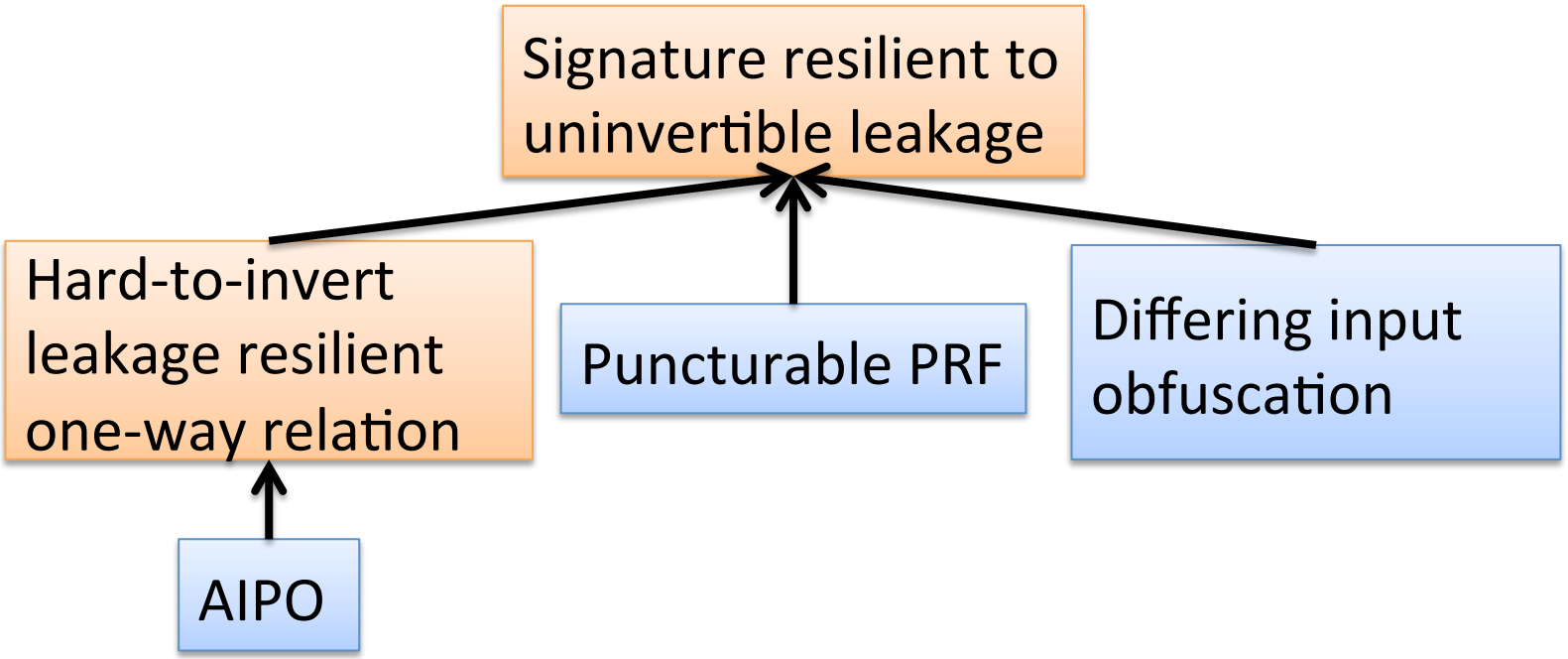


Road map

- Back ground
- Our result
- Tools
- Our technique

Our result

- The first signature scheme resilient to uninvertible leakage.
- The first leakage resilient (fully secure) signature scheme with public coin construction.



Comparison with previous works

	Leakage	**Hard-to-invert**	**Full leakage resiliency**	**Uninvertible leakage**
FHNN15	adaptive	exponential	✗	✗
YYH12	selective	polynomial	✓	✗
our work	selective	polynomial	✓	✓

About diO and AIPO

To achieve strong security, we make use of diO and AIPO.

- Differing input obfuscation (diO):
  - Negative results [GGHW14][BP15][BSW16].
  - However, there is no negative results, based on weak or standard assumptions, on diO for circuits yet.

- Point obfuscation with auxiliary input (AIPO)
  - Several candidates based on different assumptions [Can97][LPS04][BP12][BS16]

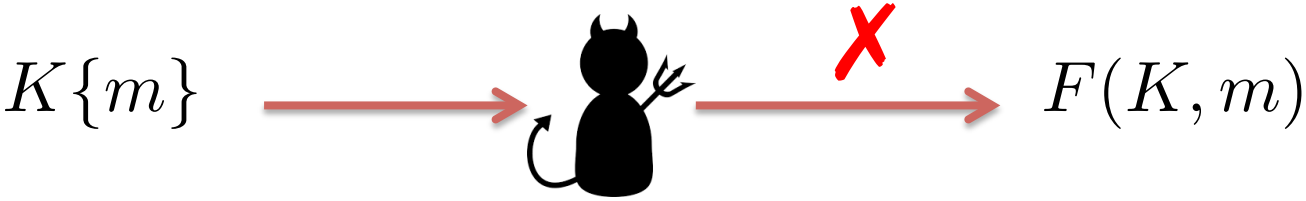
Road map

- Back ground
- Our result
- Tools
- Our technique

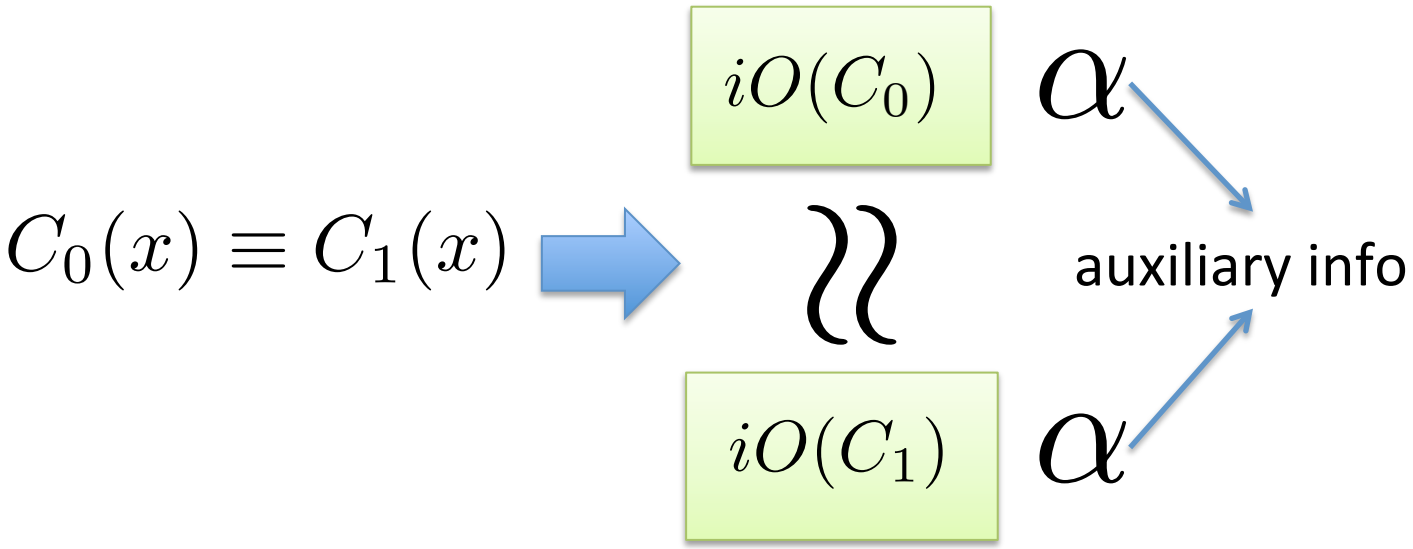
Puncturable PRF

$$K\{m\} = Puncture(K, m)$$

$$F(K\{m\}, x) = F(K, x) \qquad \text{for } x \neq m$$

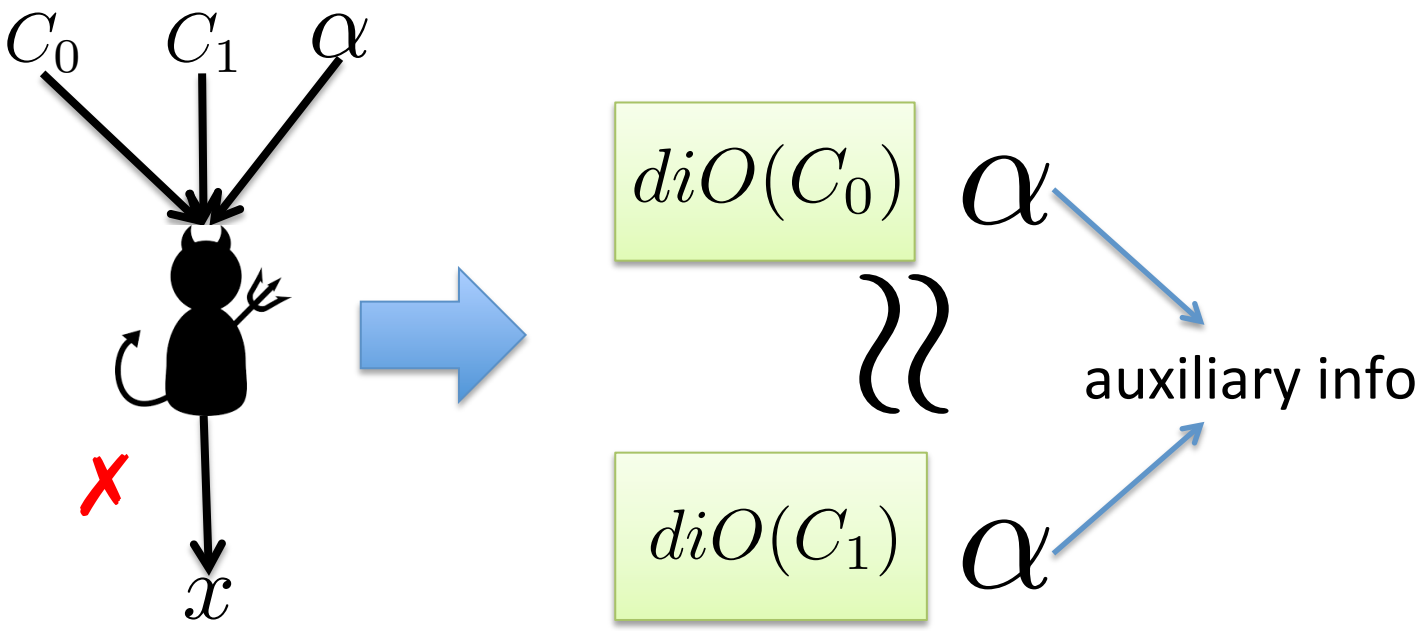


Indistinguishability obfuscation (iO)



Functionality preserving: the functionality of a circuit does not change after being obfuscated.

Differing input obfuscation (diO)



s.t. $C_0(x) \neq C_1(x)$

Functionality preserving: the functionality of a circuit does not change after being obfuscated.

Road map

- Back ground
- Our result
- Tools
- Our technique

Deterministic signature (Sahai and Waters (STOC' 14))

sk K

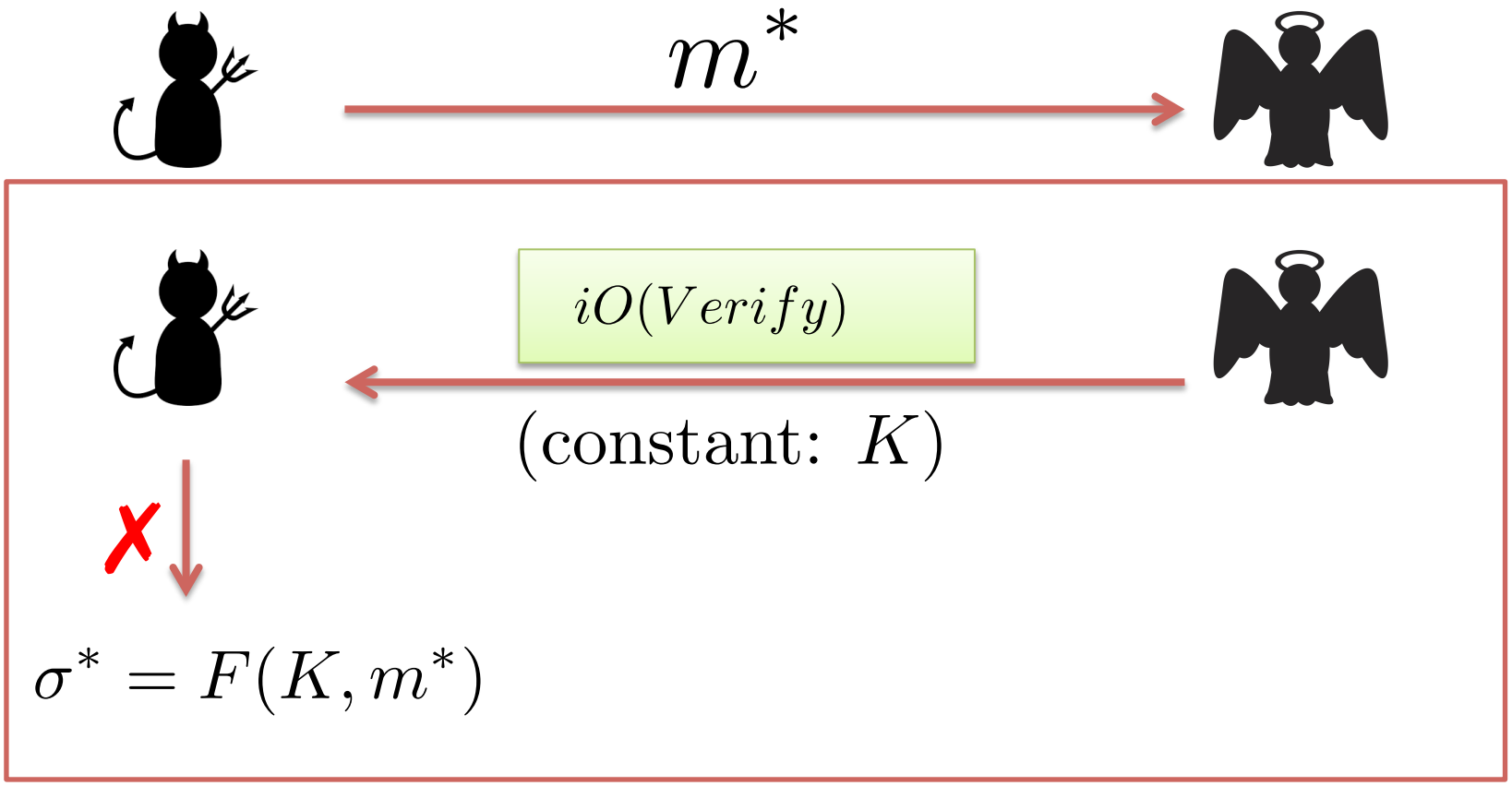
σ $\sigma = F(K, m)$

pk $iO(Verify)$

$Verify$

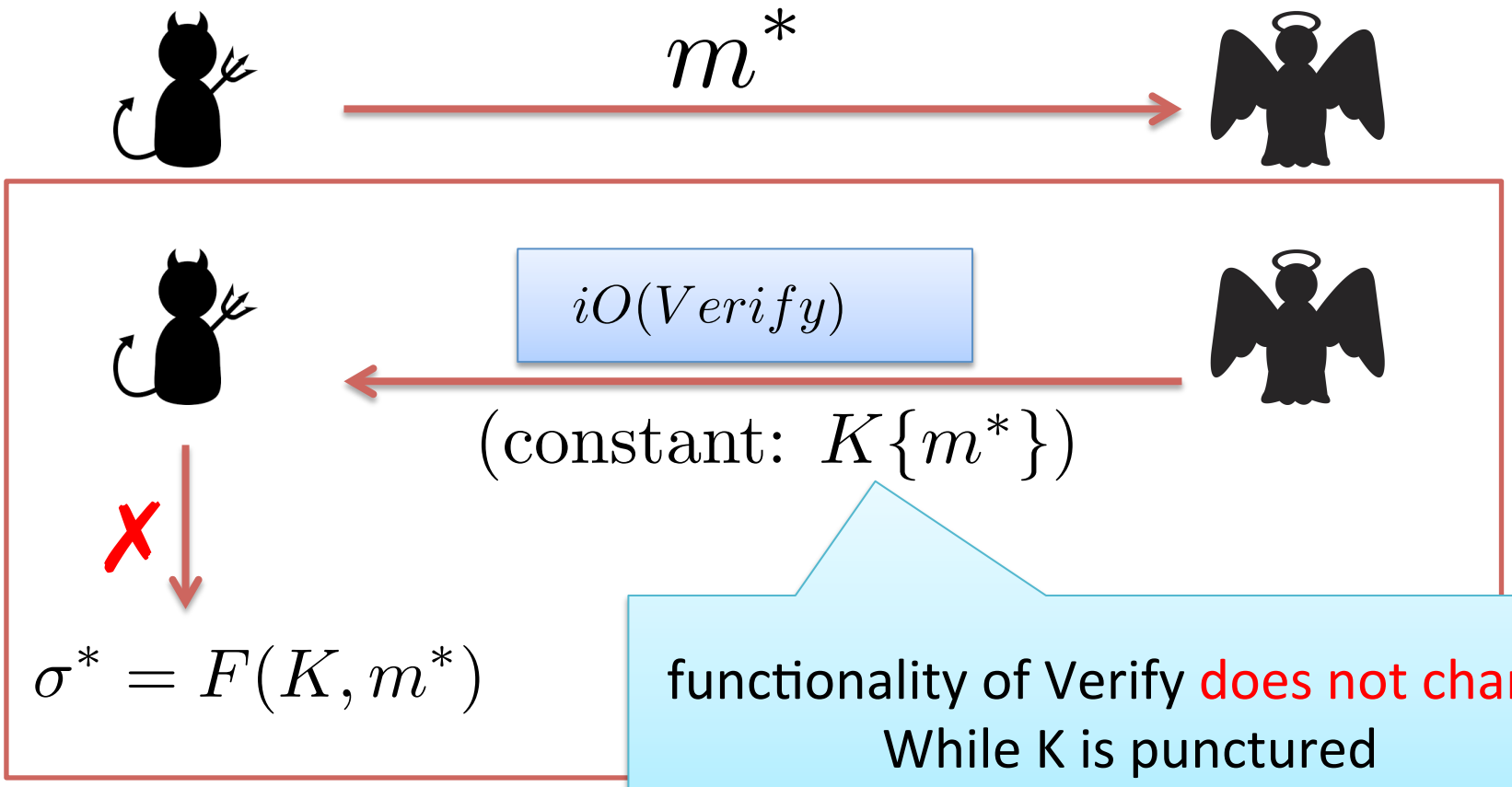
Input (m, σ)
Constant: K
Check if $F(K, m) = \sigma$

High-level idea (Sahai and Waters (STOC' 14))



Selective security

High-level idea (Sahai and Waters (STOC' 14))



Selective security

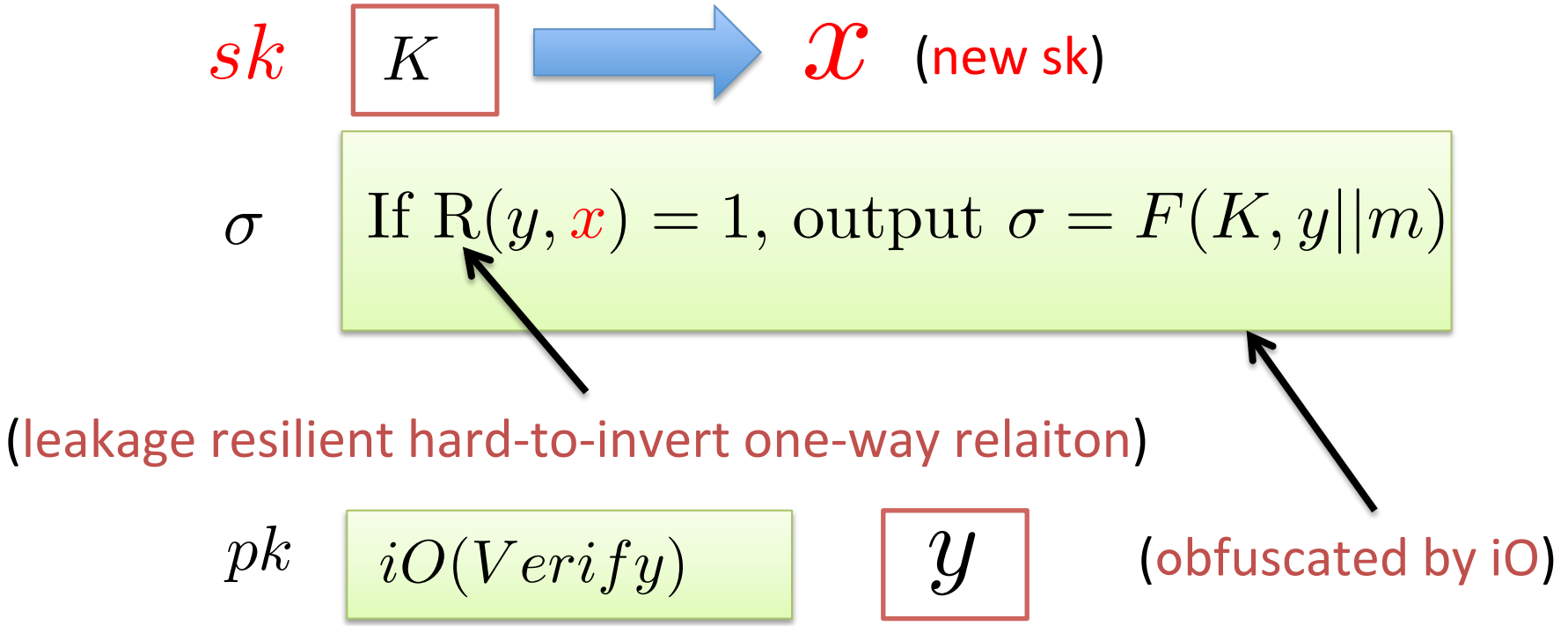
Our extension

sk K

σ $\sigma = F(K, m)$

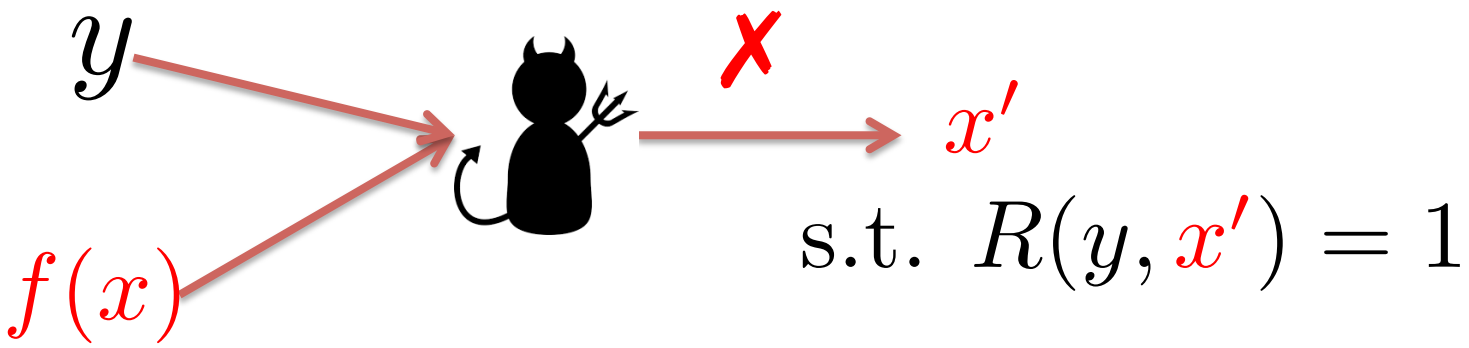
pk $iO(Verify)$

Our extension

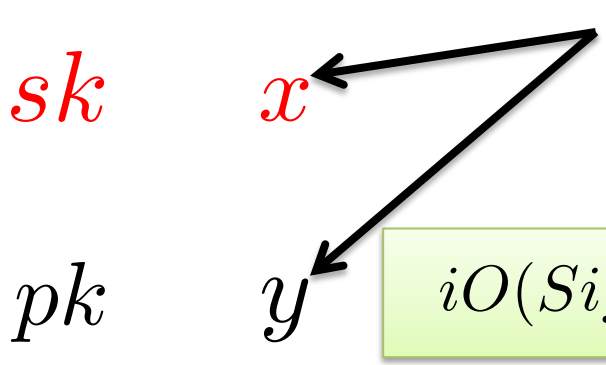


Hard-to-invert leakage resilient one-way relation (point obfuscation [BP12,BM14] based)

$$\mathrm{R}(y, x) = 1$$



Our scheme (selective secure)



Key pair of hard-to-invert leakage resilient one-way relation

$iO(Sign)$

$iO(Verify)$

input (y, x, m)

Constant: K

Check if $R(y, x) = 1$

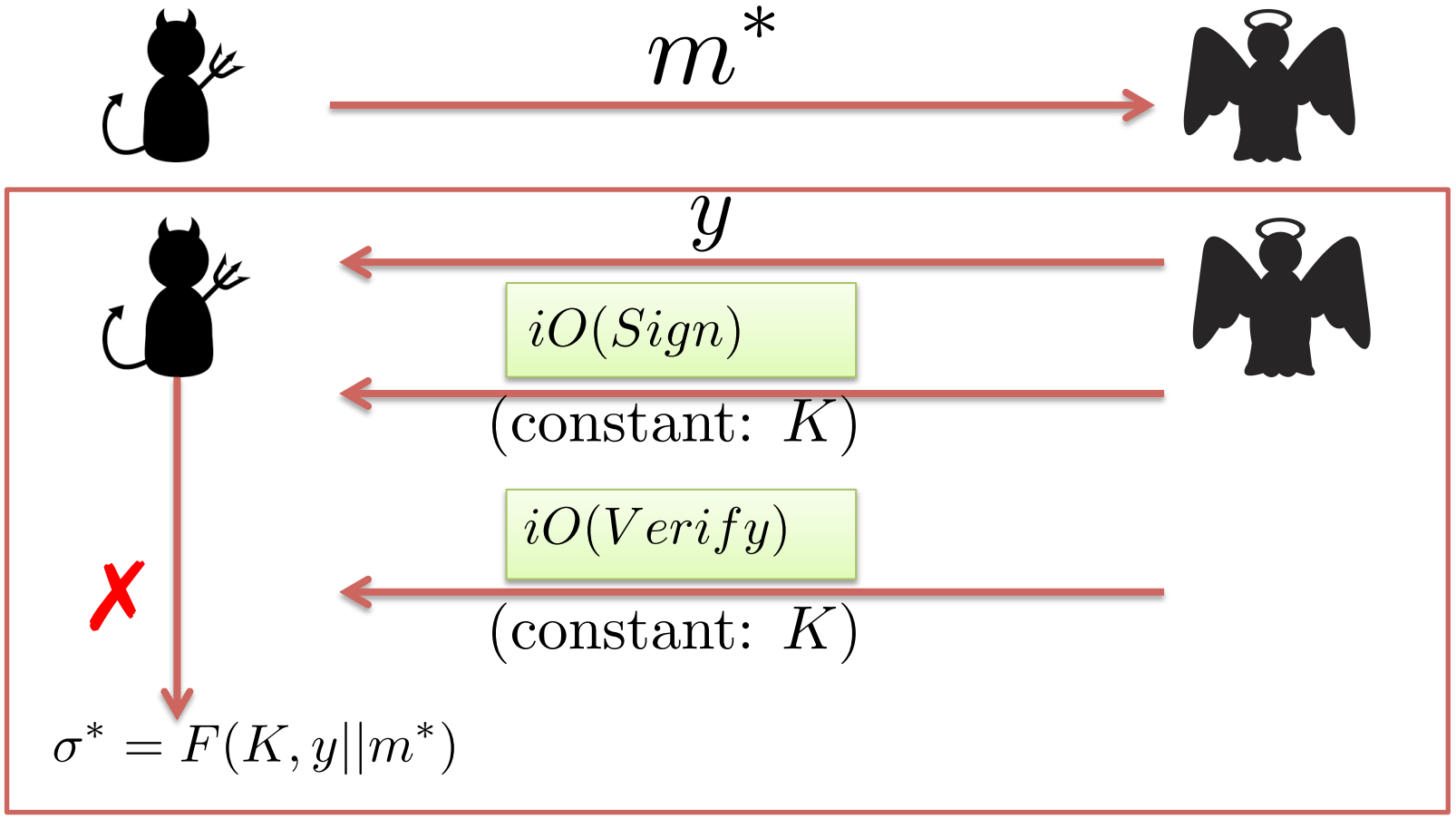
$\sigma = F(K, y||m)$

input (y, m, σ)

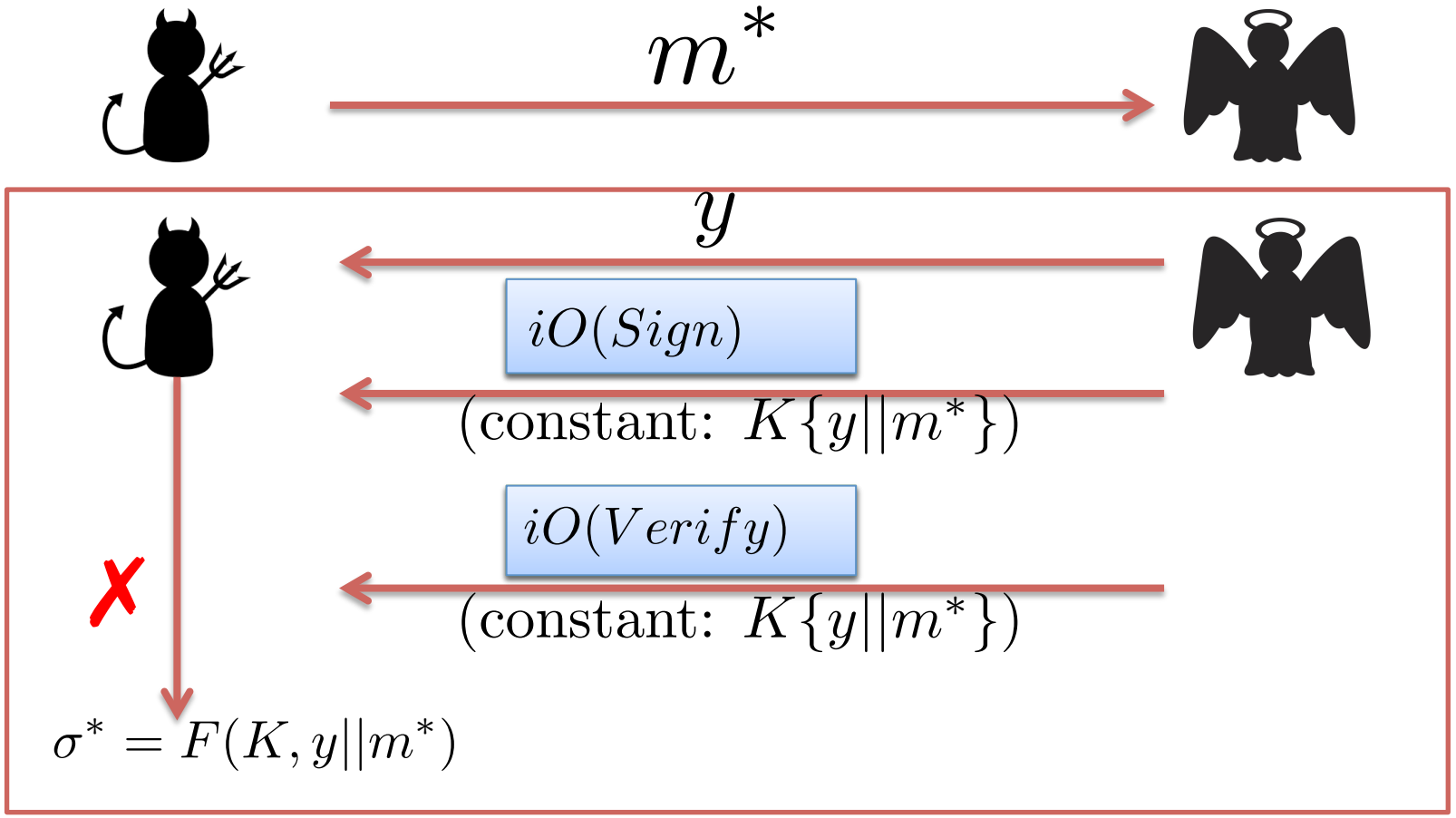
Constant: K

Check if $F(K, y||m) = \sigma$

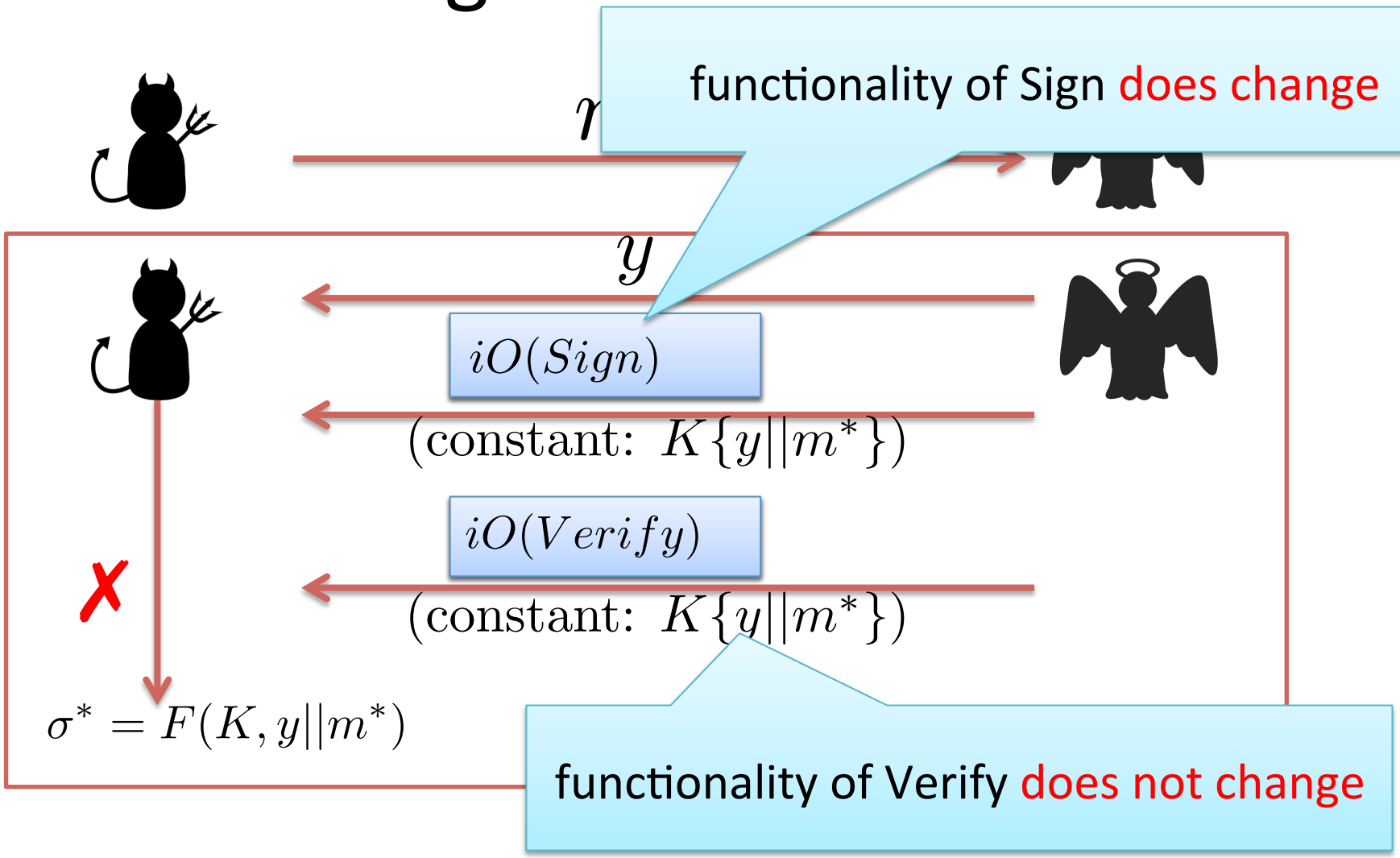
High-level idea



High-level idea

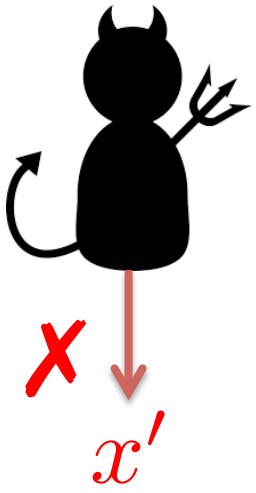


High-level idea



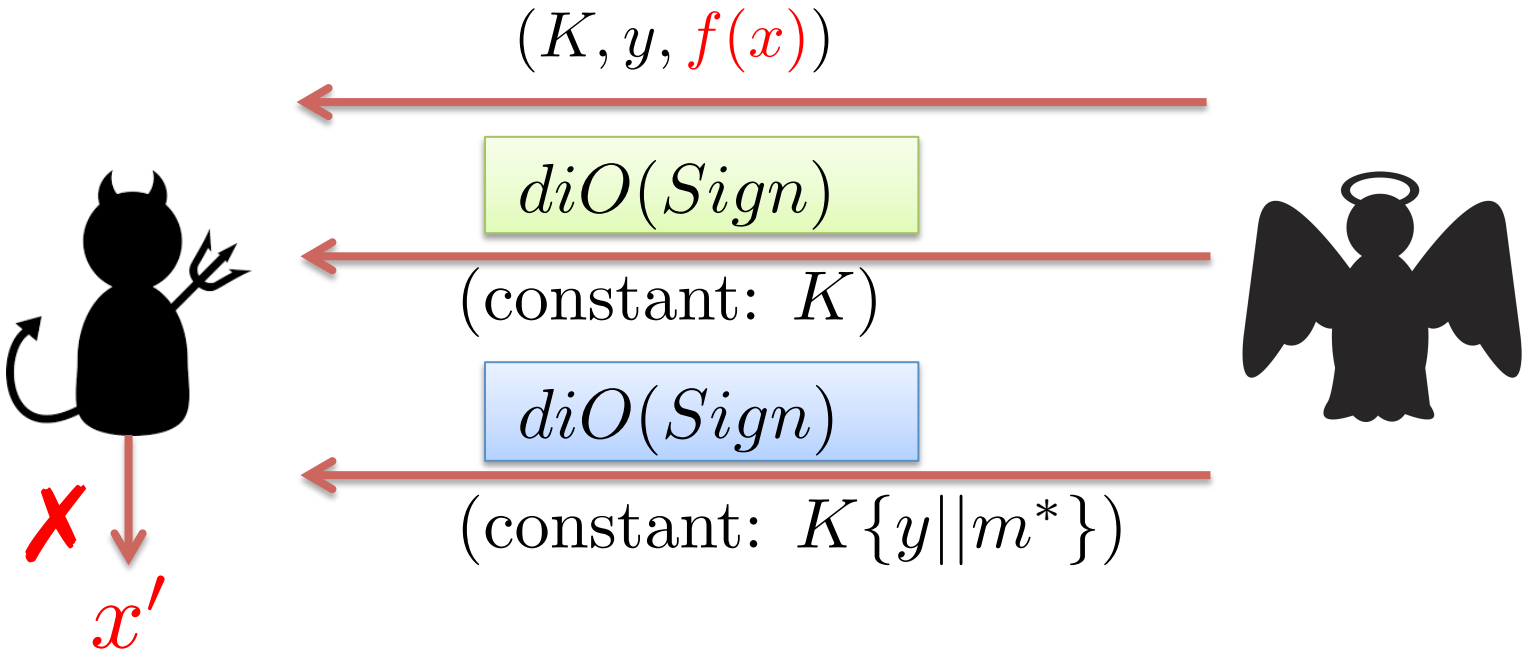
Why the view of adversary does not change if we use diO

$(y, f(x))$

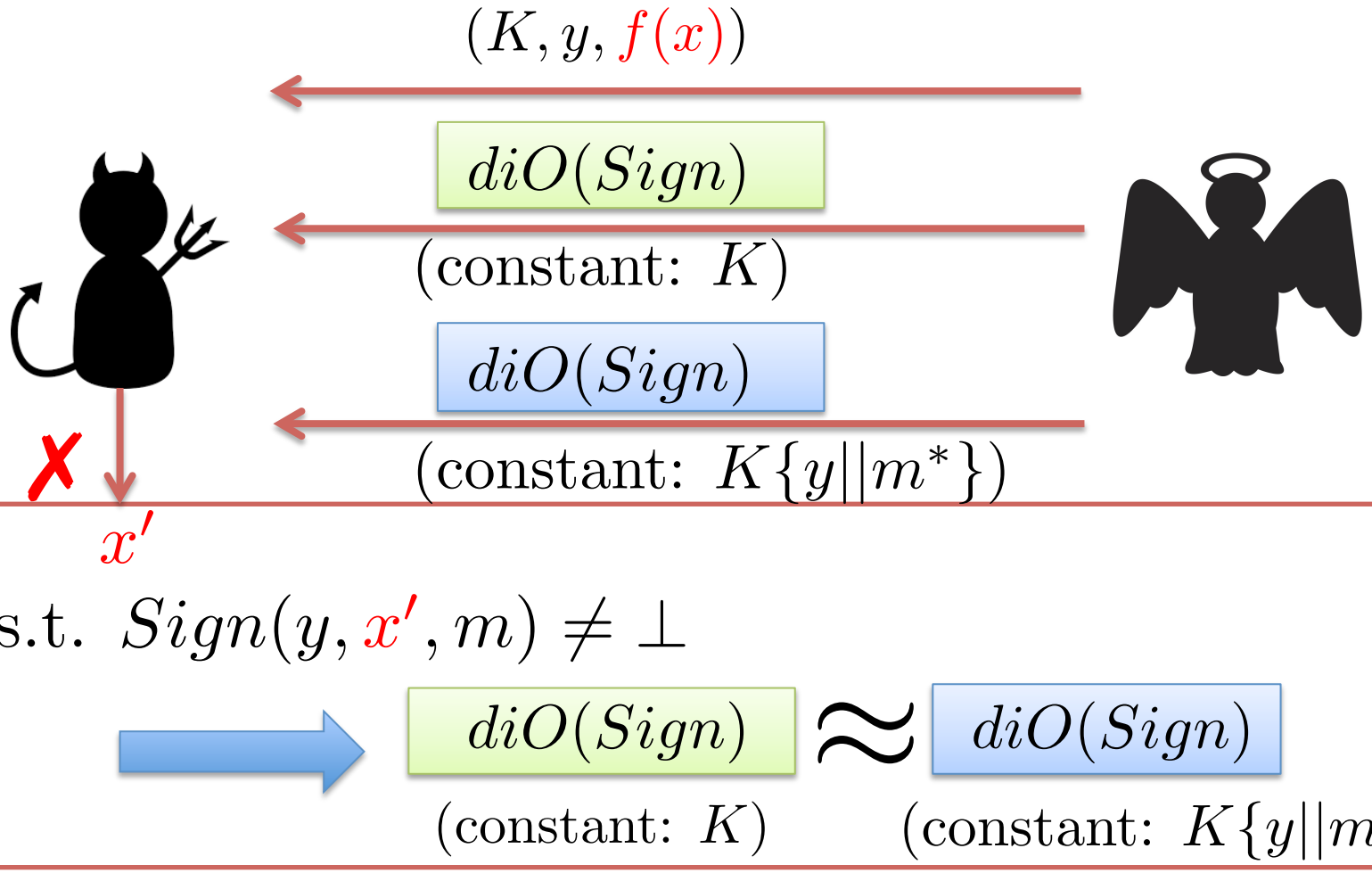


x'

Why the view of adversary does not change if we use diO



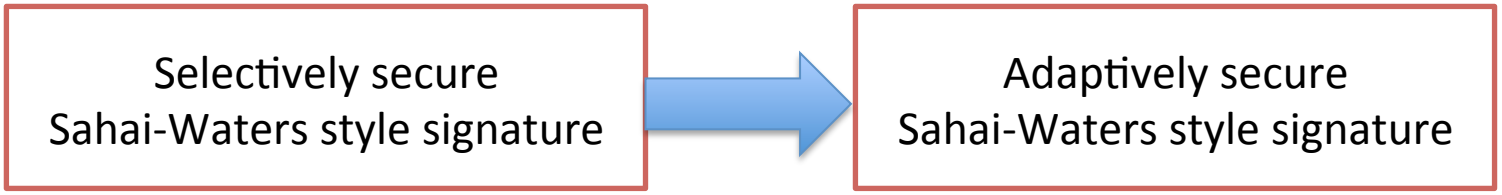
Why the view of adversary does not change if we use diO



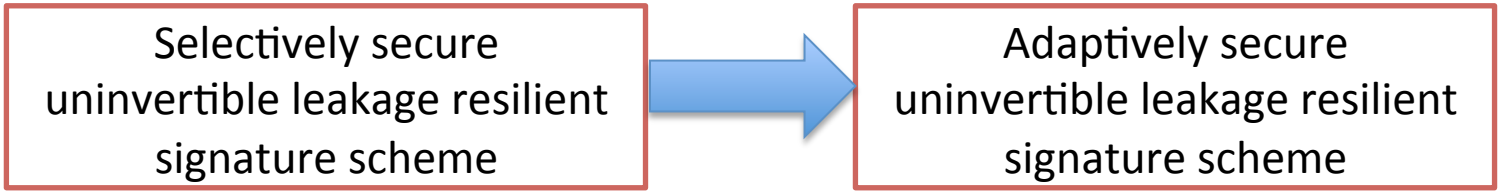
Adaptive security

Ramchen and Waters (ACM CCS' 14):

- Sahai–Waters style signature:



- Our scheme:



Signatures resilient to injective uninvertible leakage

- Building block: injective hard-to-invert leakage resilient one-way relation (based on iO).

- Based on : differing-input obfuscation.

- Without using point obfuscation.
- Why we buy this: information-theoretically determines the signing key.

Signatures resilient to injective uninvertible leakage

- Building block: injective hard-to-invert leakage resilient one-way relation (based on iO).

- Based on : differing-input obfuscation.

- Without using point obfuscation

- Why we buy this: $f(state)$ typically information-theoretically determines $state$.

Summary

- Signature resilient to uninvertible leakage
  - Based on: AIPO and diO.
- Signature resilient to injective uninvertible leakage
  - Based on : diO.

Open problem:

How to construct signatures resilient to uninvertible leakage without making use of diO, or even iO.