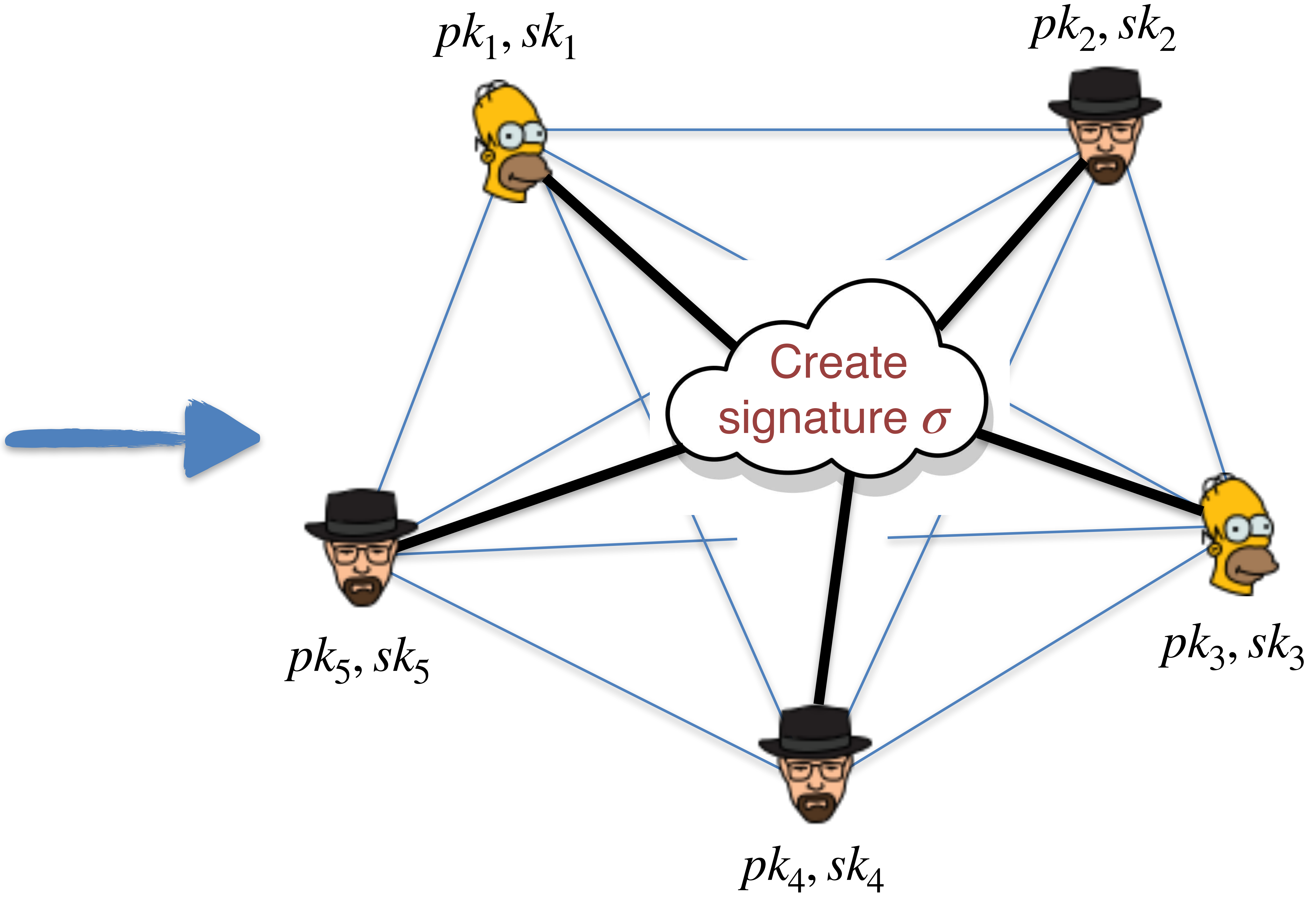
Tightly Secure Non-Interactive BLS Multi-Signatures

ASIACRYPT 2024

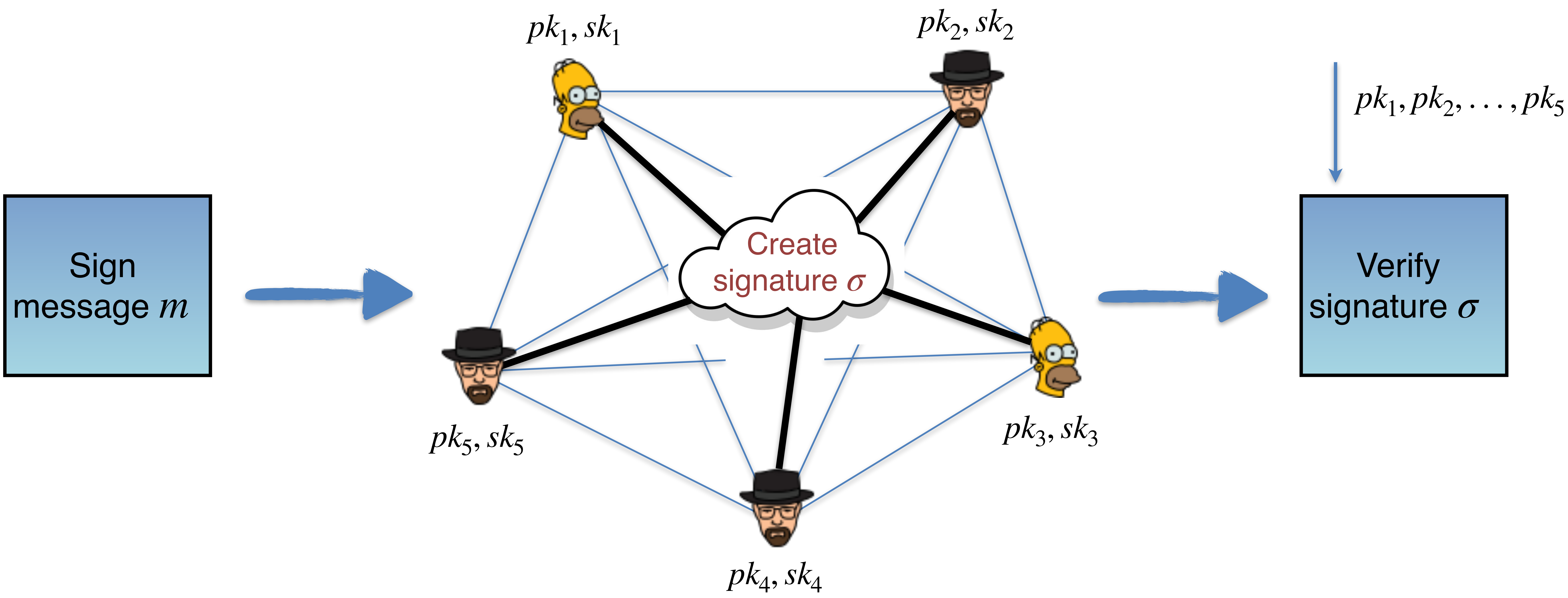
Renas Bacho, Benedikt Wagner

Multi-Signatures

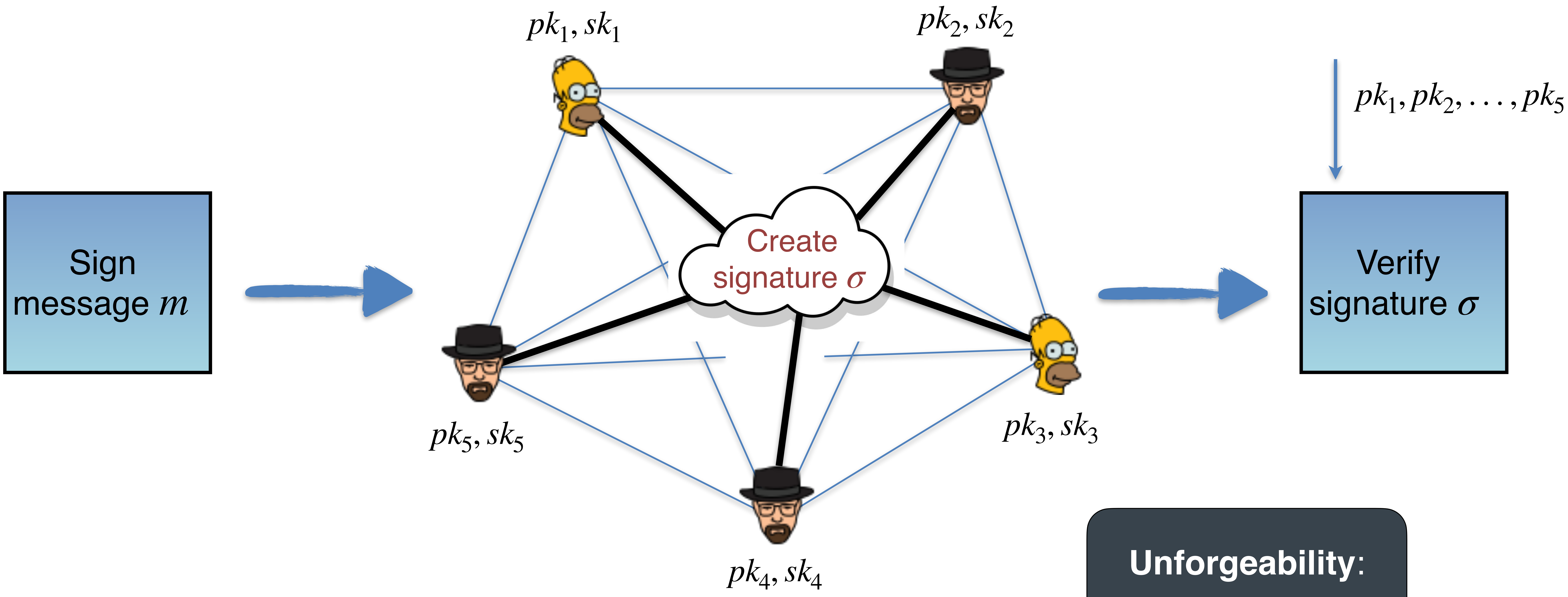
Sign message m



Multi-Signatures



Multi-Signatures



Unforgeability:

All signers need to participate

Goal: Best of both Worlds

Security

Efficiency

Goal: Best of both Worlds

Small Signature

Efficiency

Non-Interactive

Goal: Best of both Worlds

Small Signature

Efficiency

Non-Interactive

Tight Security

$\epsilon_{adv} \leq L \cdot \epsilon_{red}$

Security

Standard Assumption

Example: BLS Multi-Signatures

- n parties $P_1, \ldots, P_n$ want to sign message $m \in \{0,1\}^*$

pk_1, sk_1 

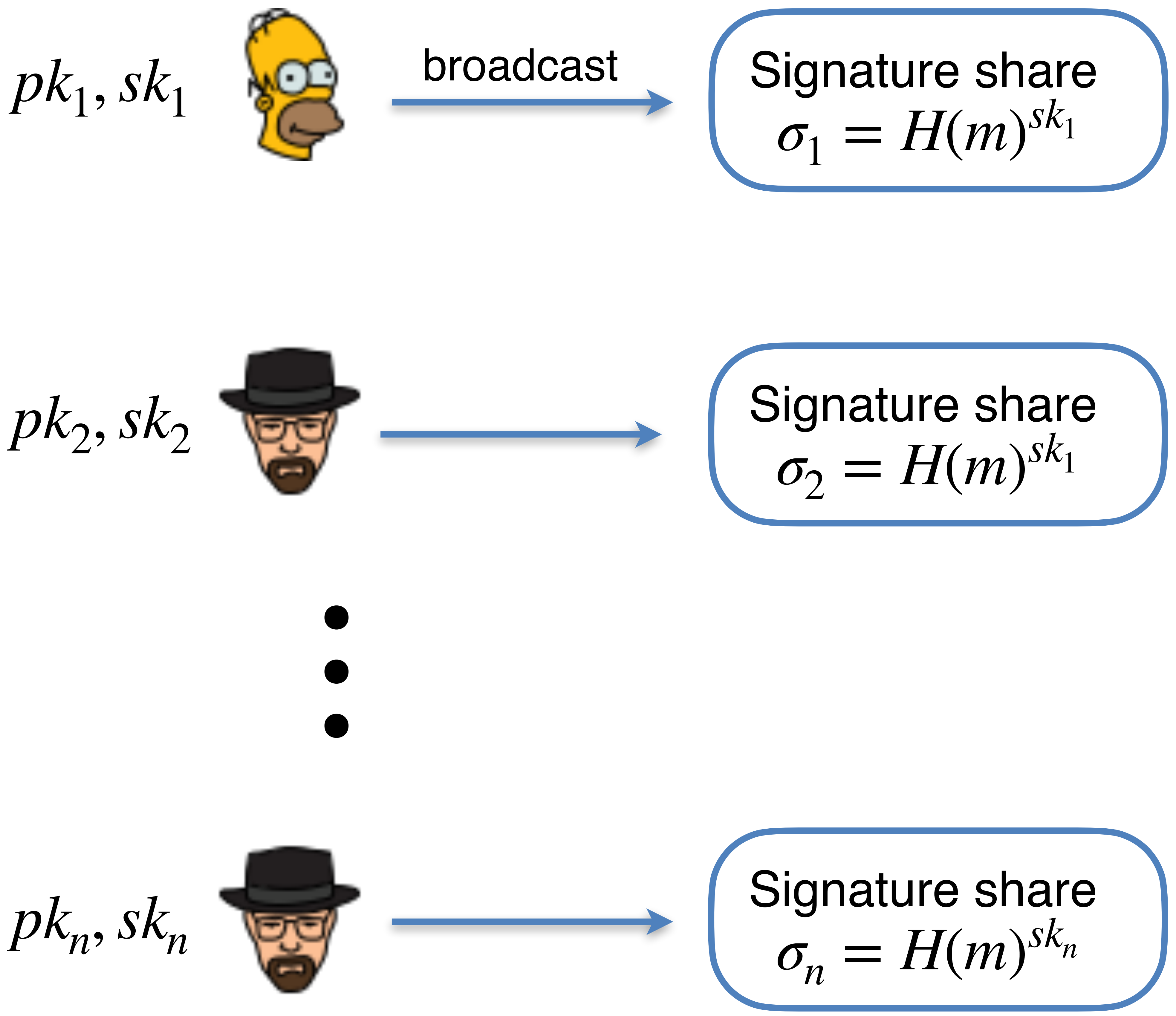
pk_2, sk_2 

$\vdots$

pk_n, sk_n 

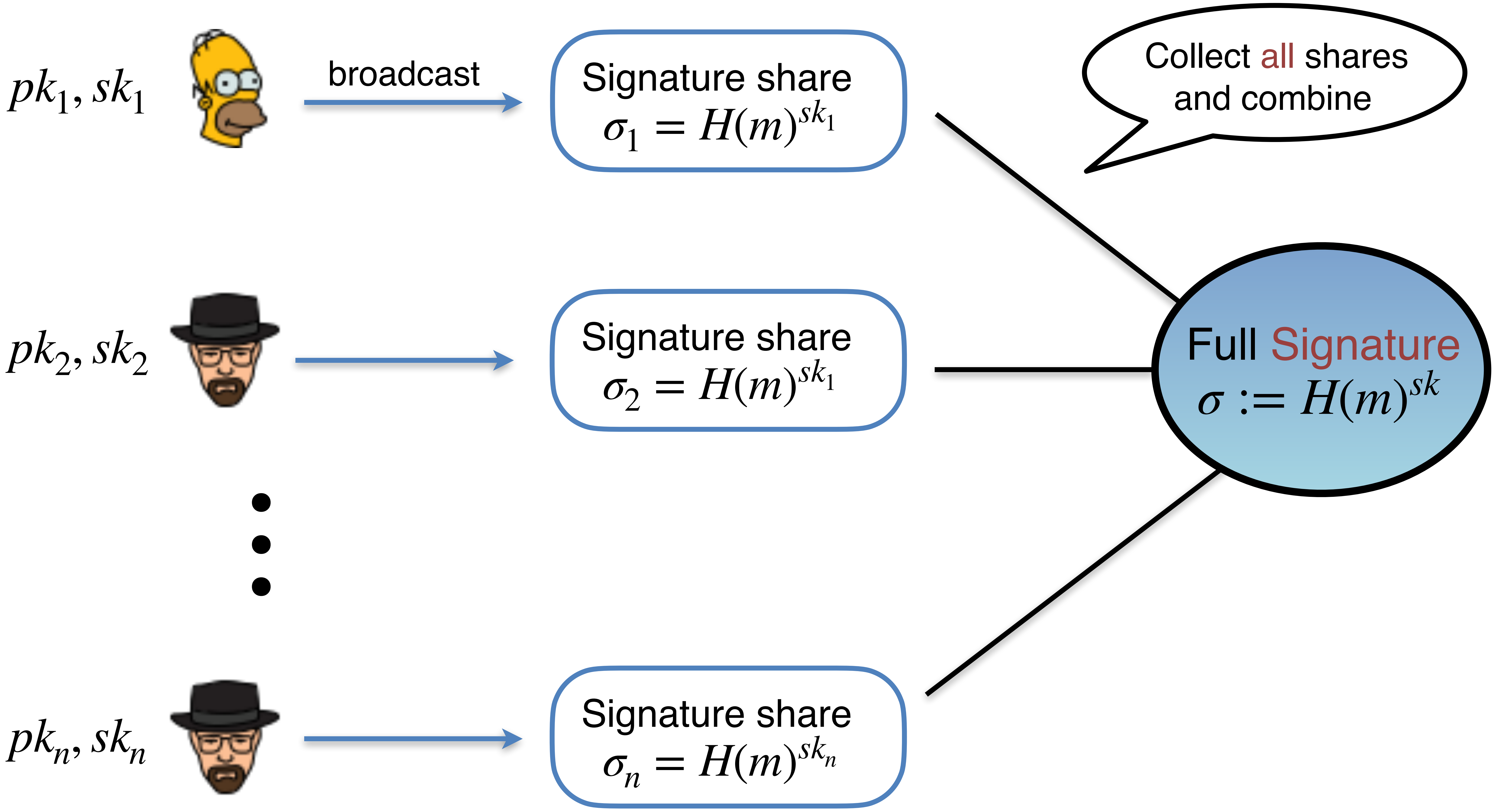
Example: BLS Multi-Signatures

- n parties $P_1, \ldots, P_n$ want to sign message $m \in \{0,1\}^*$



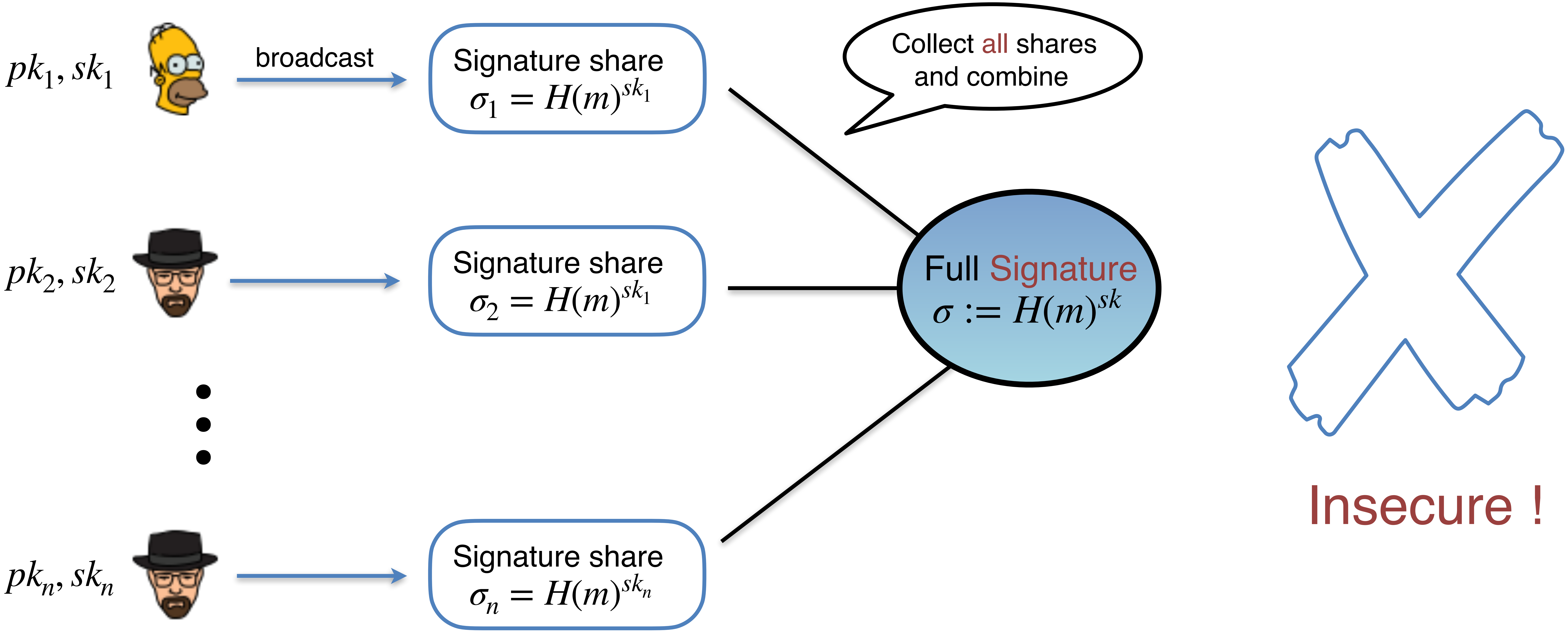
Example: BLS Multi-Signatures

- n parties $P_1, \ldots, P_n$ want to sign message $m \in \{0,1\}^*$



Example: BLS Multi-Signatures

- n parties $P_1, \ldots, P_n$ want to sign message $m \in \{0,1\}^*$



Insecure !

Example: BLS Multi-Signatures

pk_1, sk_1 

- Sample $r \leftarrow \mathbb{Z}_p$
- $pk_2 = pk_1^{-1} \cdot g^r$

Example: BLS Multi-Signatures

pk_1, sk_1

Signature share
$\sigma_1 = H(m)^{sk_1}$

Signature share
$\sigma_2 = \sigma_1^{-1} \cdot H(m)^r$

- Sample $r \leftarrow \mathbb{Z}_p$
- $pk_2 = pk_1^{-1} \cdot g^r$

Example: BLS Multi-Signatures

pk_1, sk_1 

Signature share
$\sigma_1 = H(m)^{sk_1}$

Combine

Full Signature
$\sigma := H(m)^r$

Signature share
$\sigma_2 = \sigma_1^{-1} \cdot H(m)^r$

- Sample $r \leftarrow \mathbb{Z}_p$
- $pk_2 = pk_1^{-1} \cdot g^r$

Example: BLS Multi-Signatures

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

pk_1, sk_1 

Signature share
$\sigma_1 = H(m)^{sk_1}$

Combine

Full Signature
$\sigma := H(m)^r$

Forging is easy !

Rogue-Key Attack

Signature share
$\sigma_2 = \sigma_1^{-1} \cdot H(m)^r$

- Sample $r \leftarrow \mathbb{Z}_p$
- $pk_2 = pk_1^{-1} \cdot g^r$

Common Solutions

- Knowledge of secret key (KOSK) assumption [Boldyreva, PKC '03]
- Rerandomization of keys $pk_i \mapsto pk_i^{a_i}$ for random $a_i \in \mathbb{Z}_p$ [Bellare-Neven, CCS '06]
- Proof of knowledge of secret key as $\pi_i := H(pk_i)^{sk_i}$ [Ristenpart-Yilek, EC '07]

Common Solutions

- Knowledge of secret key (KOSK) assumption [Boldyreva, PKC ’03]
- Rerandomization of keys $pk_i \mapsto pk_i^{a_i}$ for random $a_i \in \mathbb{Z}_p$ [Bellare-Neven, CCS ‘06]
- Proof of knowledge of secret key as $\pi_i := H(pk_i)^{sk_i}$ [Ristenpart-Yilek, EC ‘07]

Non-Interactive + CDH

Common Solutions

- Knowledge of secret key (KOSK) assumption [Boldyreva, PKC '03]
- Rerandomization of keys $pk_i \mapsto pk_i^{a_i}$ for random $a_i \in \mathbb{Z}_p$ [Bellare-Neven, CCS '06]
- Proof of knowledge of secret key as $\pi_i := H(pk_i)^{sk_i}$ [Ristenpart-Yilek, EC '07]

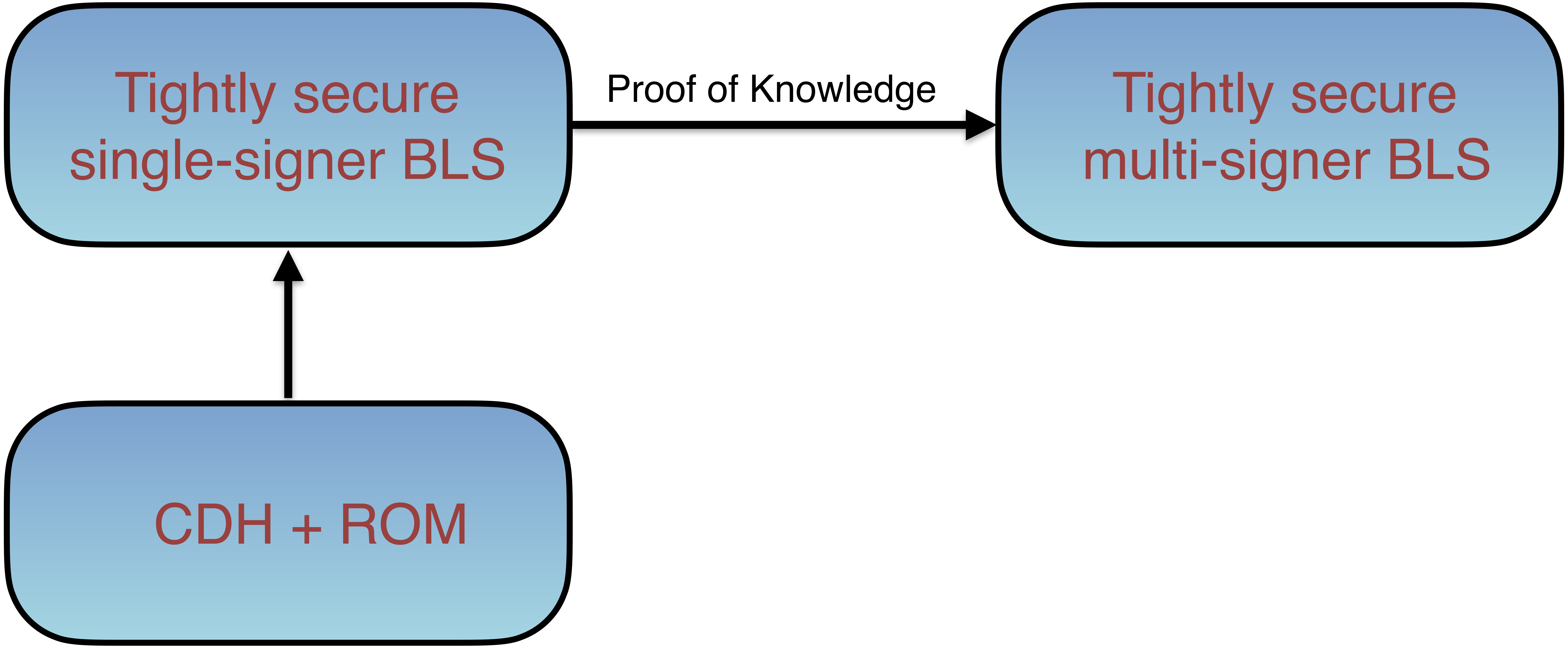
→ Non-Interactive + CDH

Still security loss of $O(Q_h)$ or worse !

What to do?

Can we design a tightly secure BLS multi-signature?

Our Results


Tightly secure single-signer BLS
Proof of Knowledge
Tightly secure multi-signer BLS
CDH + ROM

Comparison

Scheme	Assumption	Loss	Idealization
BLS [Bol03]	CDH	$\Theta(q_s)$	ROM
RY07 [RY07]	CDH	$\Theta(q_s)$	ROM
BDN18 [BDN18]	CDH	$\Theta(q_h^2/\epsilon)$	ROM
LOSSW06 [LOS$^+$06]	CDH	$\Theta(\ell q_s)$	KOSK
QX10 [QX10]	CDH	$\Theta(q_s^2 q_h/\epsilon)$	ROM
DGNW20 [DGNW20]	wBDHI	$\Theta(q_h)$	ROM
BNN07 [BNN07]	CDH	$\Theta(1)$	ROM
QLH12 [QLH12]	CDH	$\Theta(1)$	ROM
BLSMS_2	CDH	$\Theta(1)$	ROM

Table 1: Comparison of non-interactive multi-signature schemes in the pairing setting. We compare under which hardness assumption the scheme is proven secure, the asymptotic tightness loss of the security proof, and under which idealized model the scheme is proven secure. Here, we do not consider proofs in the algebraic group model (AGM). We denote the number of random oracle and signing queries by q_h and q_s, respectively, and the advantage of an adversary against the scheme by ϵ. For LOSSW06 [LOS$^+$06], ℓ denotes the bit-length of messages. Further, wBDHI denotes the weak bilinear Diffie-Hellman inversion assumption [BBG05], ROM denotes the random oracle model, and KOSK denotes the knowledge of secret key model [Bol03].

Comparison

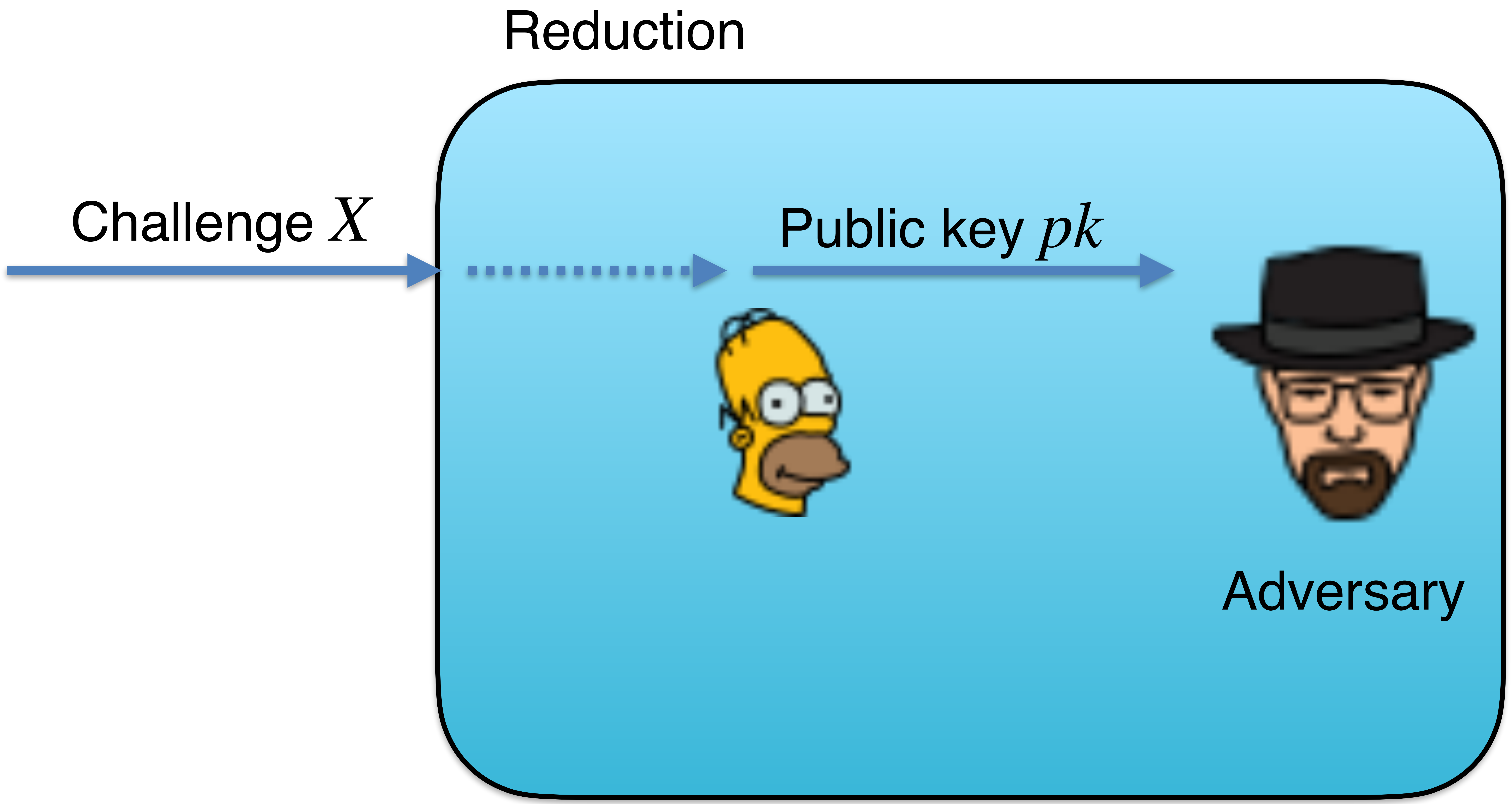
CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Scheme	Public Key	Sig Share	Signature	Cost (Sig)	Cost (Ver)
BLS [Bol03]	$1\langle\mathbb{G}\rangle$	$1\langle\mathbb{G}\rangle$	$1\langle\mathbb{G}\rangle$	$1\mathrm{ex}$	$2\mathrm{pr}$
RY07 [RY07]	$1\langle\mathbb{G}\rangle$	$1\langle\mathbb{G}\rangle$	$1\langle\mathbb{G}\rangle$	$1\mathrm{ex}$	$2\mathrm{pr}$
BDN18 [BDN18]	$1\langle\mathbb{G}\rangle$	$1\langle\mathbb{G}\rangle$	$1\langle\mathbb{G}\rangle$	$1\mathrm{ex}$	$2\mathrm{pr}$
LOSSW06 [LOS+06]	$1\langle\mathbb{G}_T\rangle$	$2\langle\mathbb{G}\rangle$	$2\langle\mathbb{G}\rangle$	$2\mathrm{ex} + 1\mathrm{ex}^\ell$	$2\mathrm{pr} + 1\mathrm{ex}^\ell$
QX10 [QX10]	$1\langle\mathbb{G}\rangle$	$1\langle\mathbb{G}\rangle$	$1\langle\mathbb{G}\rangle$	$1\mathrm{ex}$	$2\mathrm{pr} + 1\mathrm{ex}^{N+1}$
DGNW20 [DGNW20]	$1\langle\mathbb{G}\rangle$	$2\langle\mathbb{G}\rangle$	$2\langle\mathbb{G}\rangle$	$4\mathrm{ex}$	$3\mathrm{pr} + 1\mathrm{ex}$
BNN07 [BNN07]	$1\langle\mathbb{G}\rangle$	$1\langle\mathbb{G}\rangle + 1$	$1\langle\mathbb{G}\rangle + N$	$1\mathrm{ex}$	$(N+1)\mathrm{pr}$
QLH12 [QLH12]	$1\langle\mathbb{G}\rangle$	$2\langle\mathbb{G}\rangle + 1$	$4\langle\mathbb{G}\rangle$	$2\mathrm{ex}$	$4\mathrm{pr}$
BLSMS_2	$2\langle\mathbb{G}\rangle$	$1\langle\mathbb{G}\rangle + 1$	$1\langle\mathbb{G}\rangle + N$	$1\mathrm{ex}$	$2\mathrm{pr}$

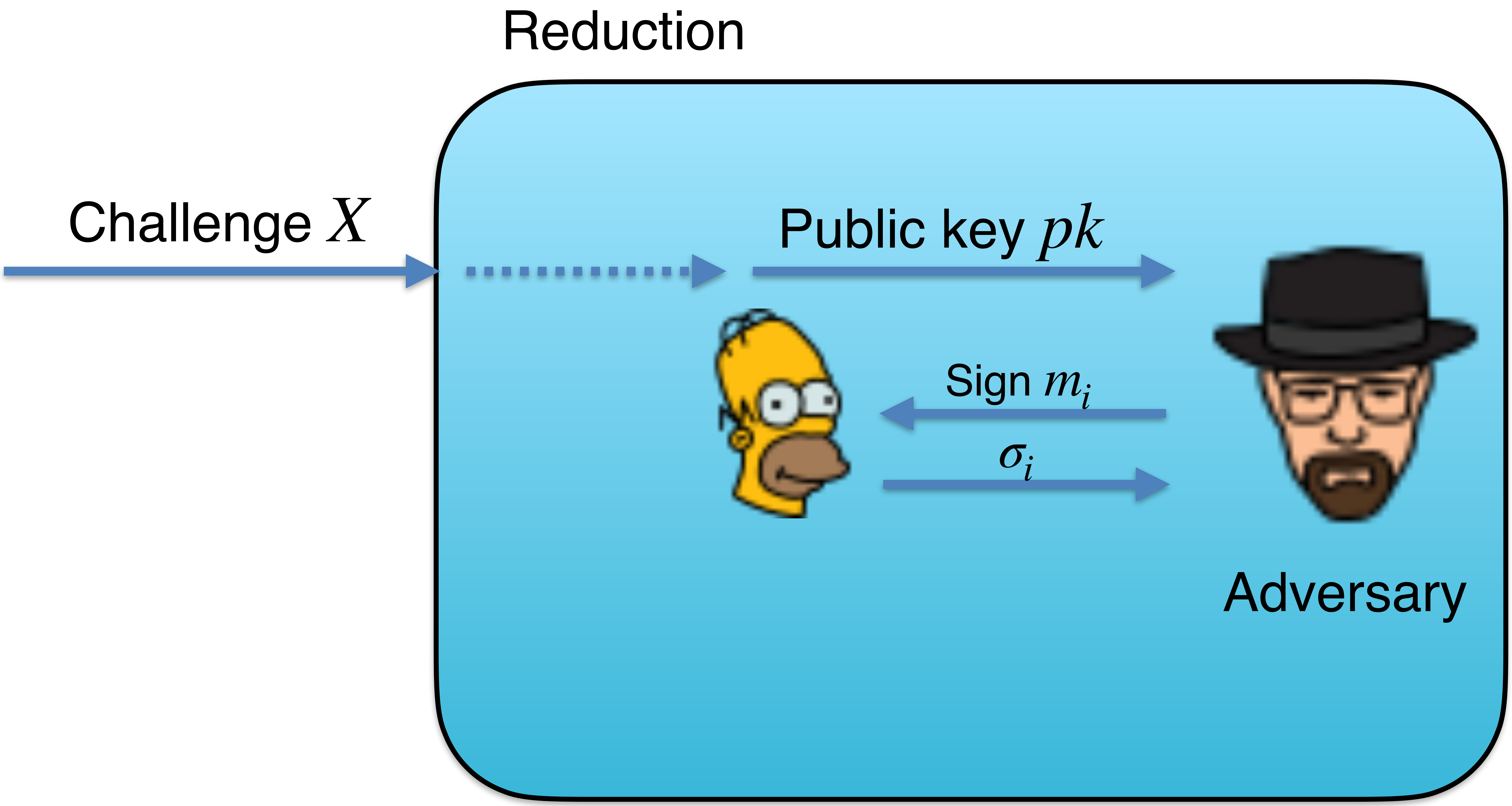
Table 2: Comparison of non-interactive multi-signature schemes in the pairing setting. We assume that all constructions are instantiated with a symmetric pairing $e\colon \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ and compare the size of a public key, signature share, the size of the signature, the computational cost per signer, and the computational cost for verification. We denote the size of a group element by $\langle\mathbb{G}\rangle$ (respectively $\langle\mathbb{G}_T\rangle$), the number of signers by N, and the number of exponentiations, pairings, and k-multi-exponentiations for $k \in \mathbb{N}$ by ex, pr, and ex^k, respectively. For LOSSW06 [LOS+06], ℓ denotes the bit-length of messages.

Our Techniques

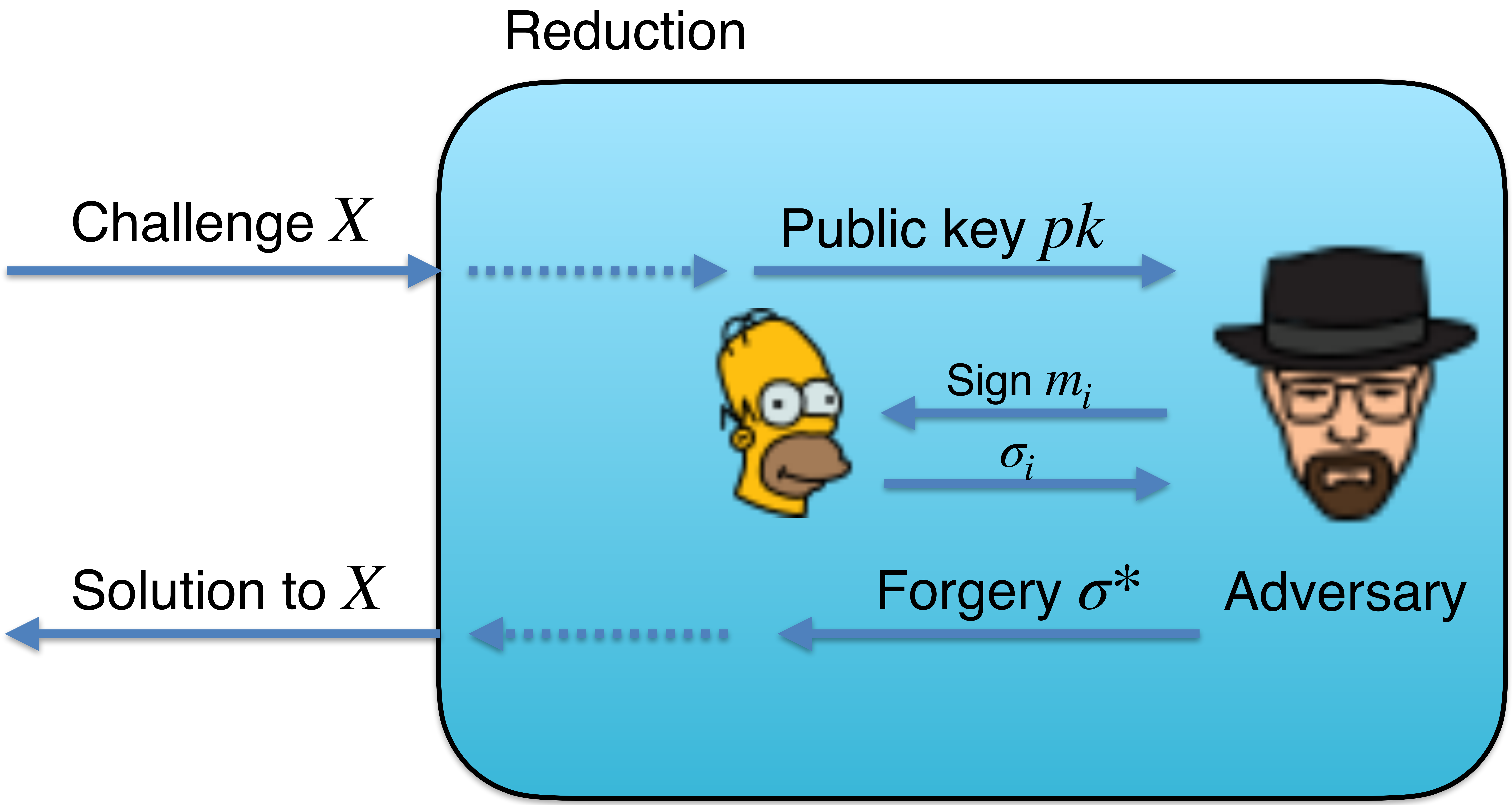
Proof Structure



Proof Structure



Proof Structure



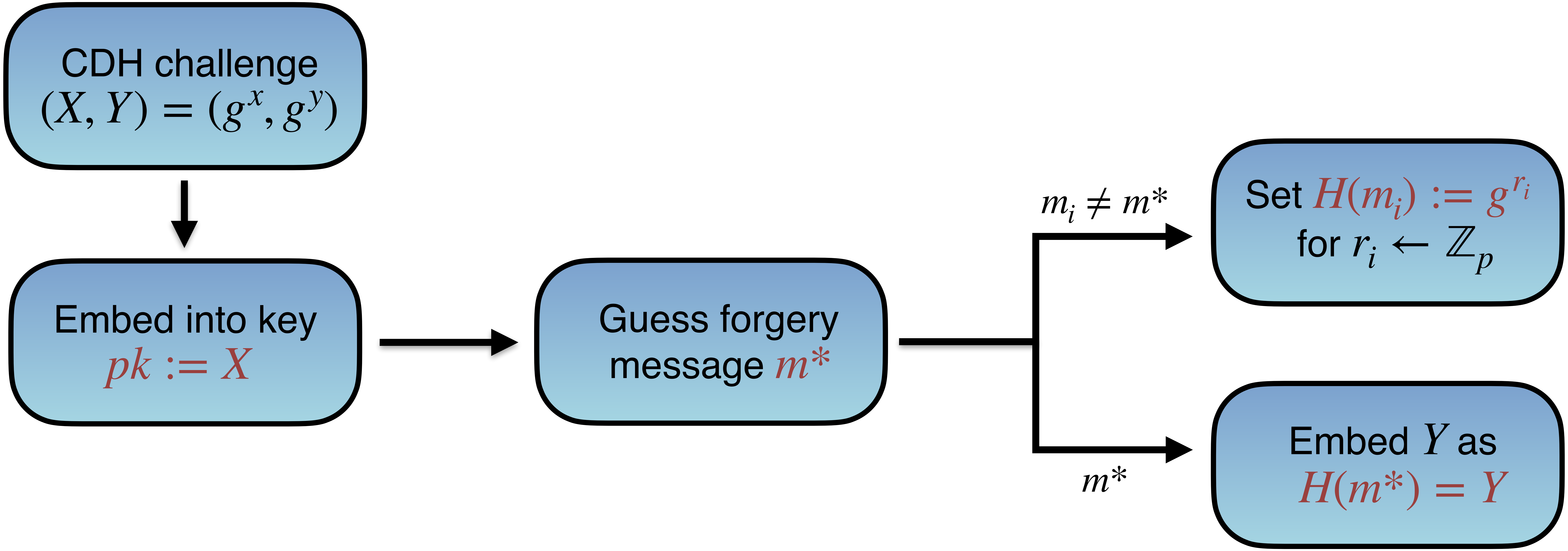
Proof Structure for BLS

CDH challenge
$(X, Y) = (g^x, g^y)$

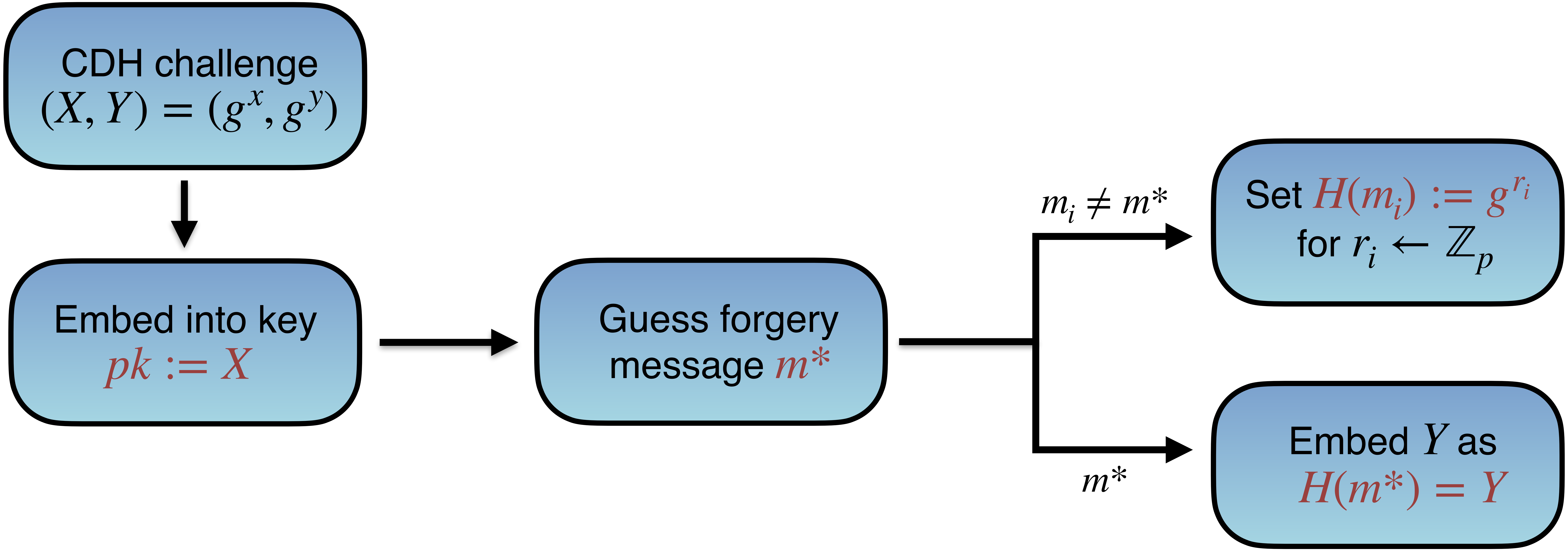
$\downarrow$

Embed into key
$pk := X$

Proof Structure for BLS

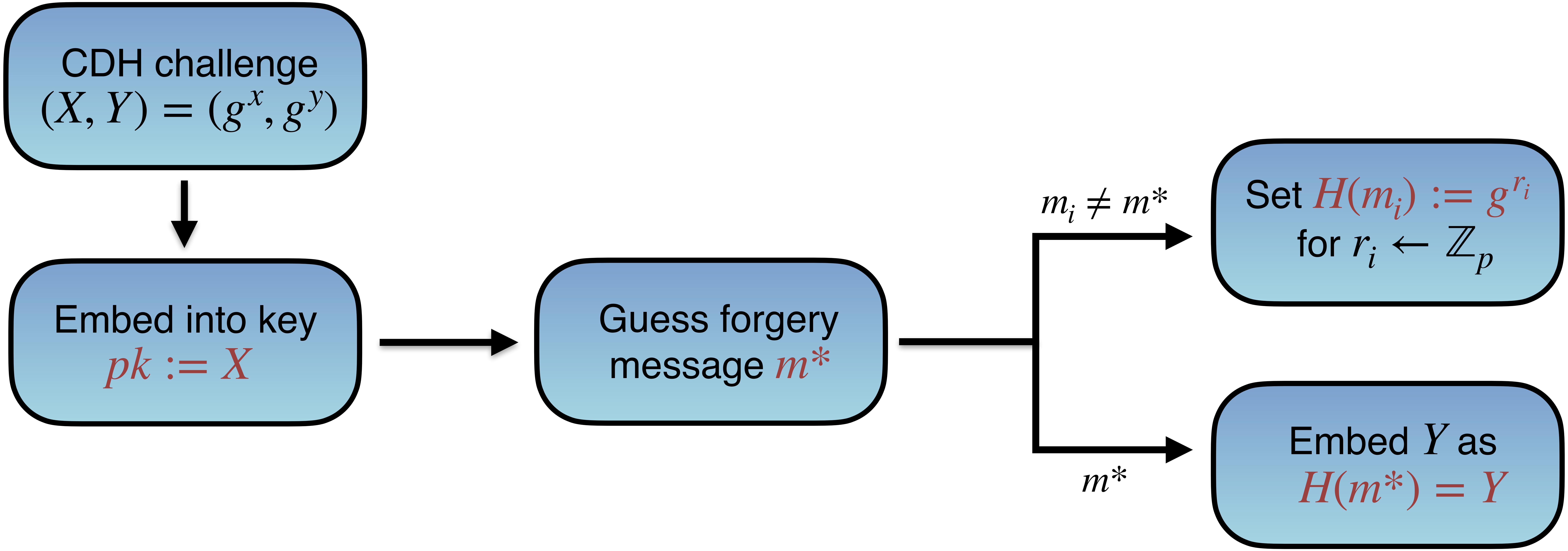


Proof Structure for BLS



→ Simulate signatures as $\sigma_i := X^{r_i}$

Proof Structure for BLS



Simulate signatures as $\sigma_i := X^{r_i}$

Forgery gives CDH solution $\sigma^* = Y^x$

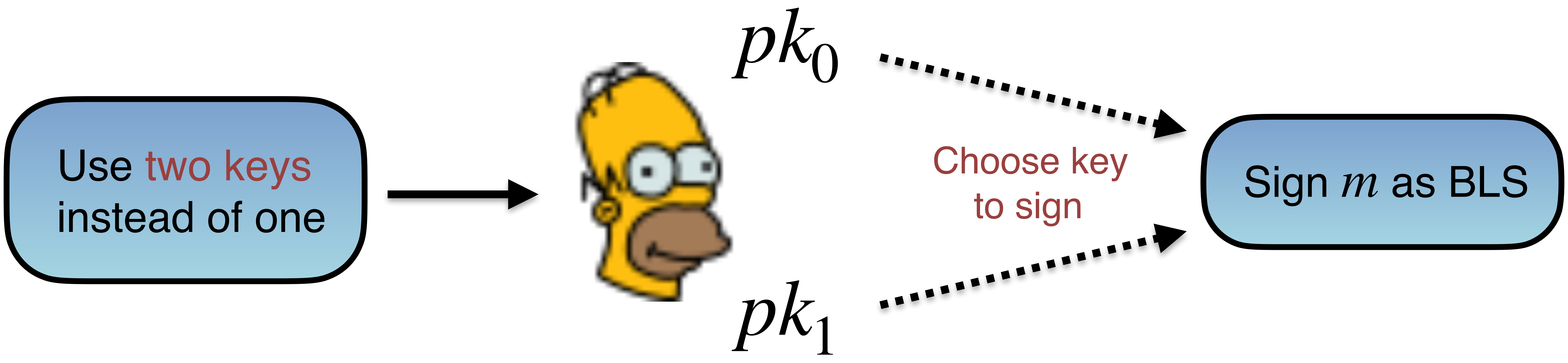
Our Construction

Use two keys instead of one

pk_0

pk_1

Our Construction



Our Construction

Use two keys instead of one

pk_0

pk_1

Choose key to sign

Sign m as BLS

Choose pk_0

Signature

$\sigma := H(m)^{sk_0}$

Our Construction

Use two keys instead of one

pk_0

pk_1

Choose key to sign

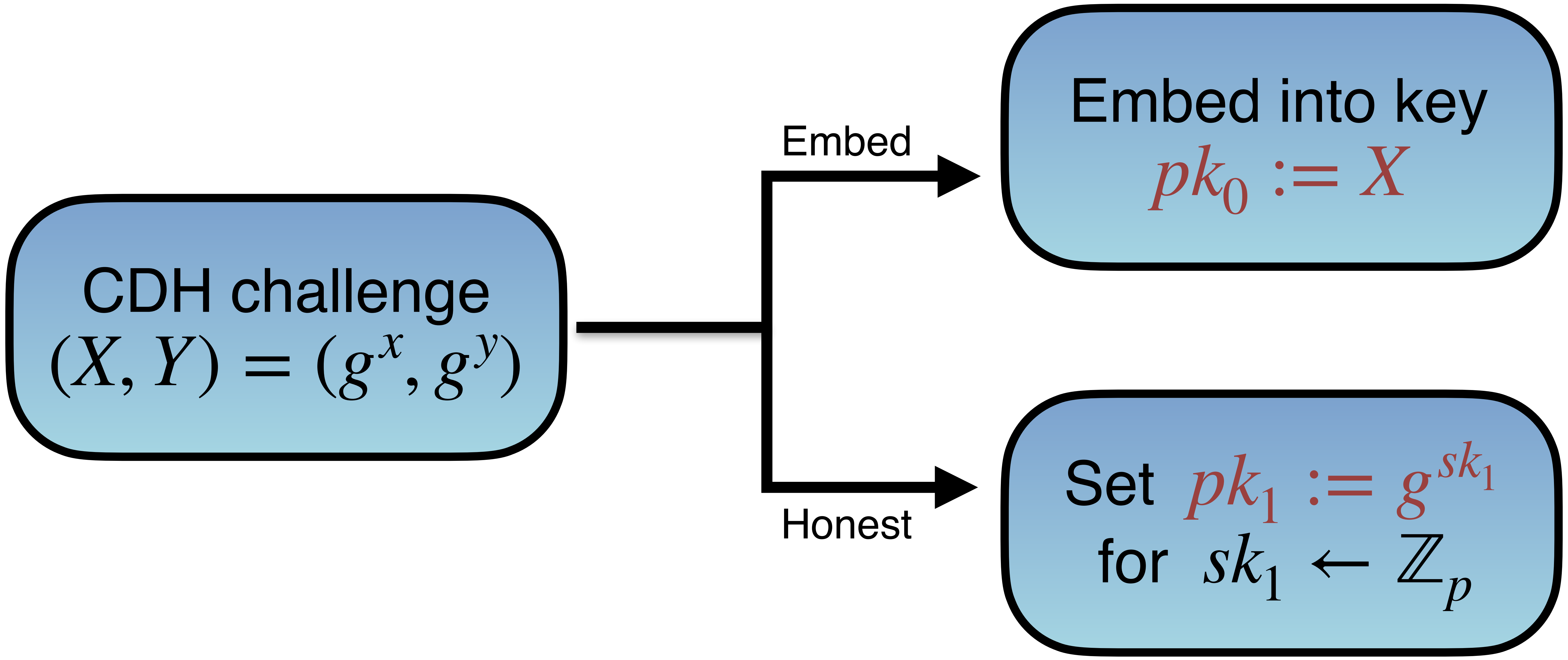
Sign m as BLS

Choose pk_0

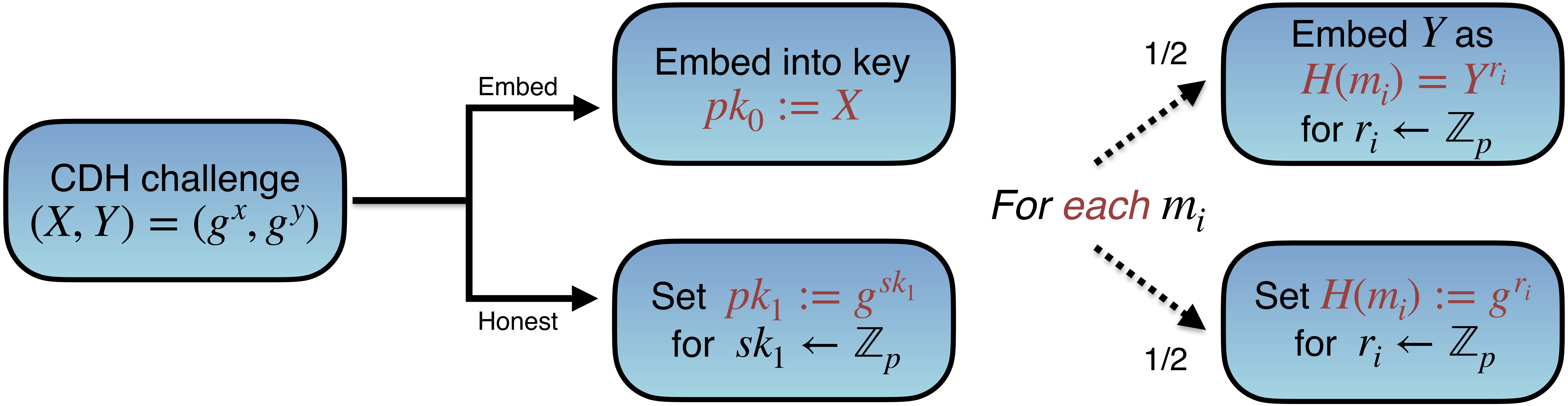
Signature
$\sigma := H(m)^{sk_0}$

How does that help?

Proof Idea

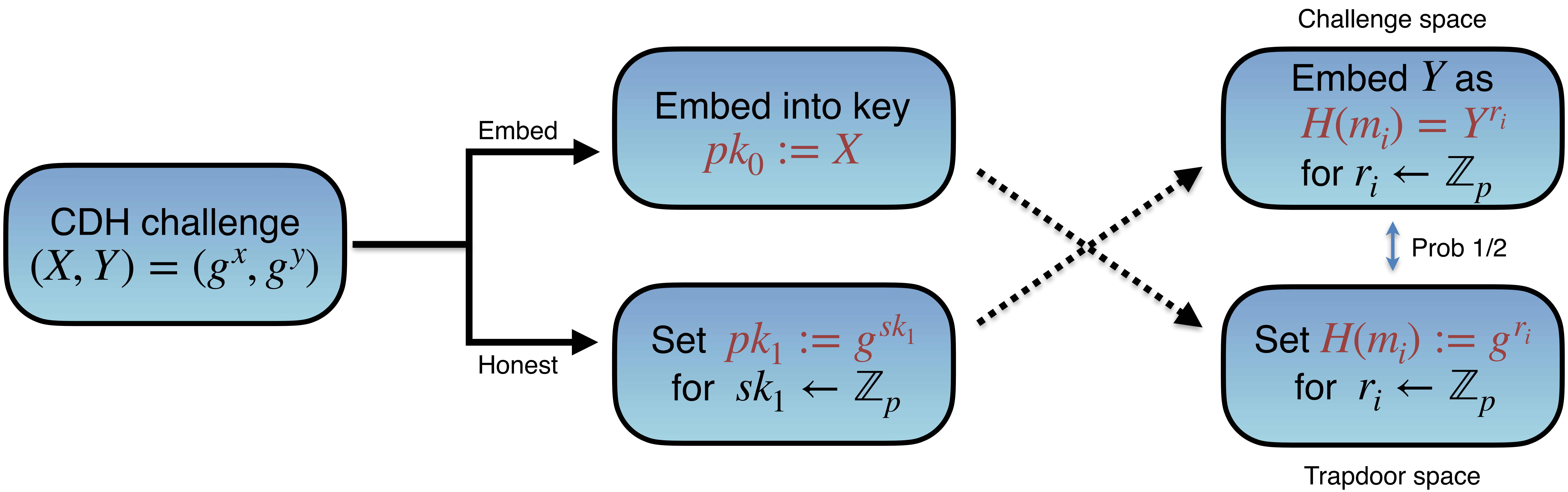

CDH challenge
$(X, Y) = (g^x, g^y)$
Embed
Honest
Embed into key
$pk_0 := X$
Set $pk_1 := g^{sk_1}$
for $sk_1 \leftarrow \mathbb{Z}_p$

Proof Idea



CDH challenge
$(X, Y) = (g^x, g^y)$
Embed
Honest
Embed into key
$pk_0 := X$
Set $pk_1 := g^{sk_1}$
for $sk_1 \leftarrow \mathbb{Z}_p$
For each m_i
1/2
1/2
Embed Y as
$H(m_i) = Y^{r_i}$
for $r_i \leftarrow \mathbb{Z}_p$
Set $H(m_i) := g^{r_i}$
for $r_i \leftarrow \mathbb{Z}_p$

Proof Idea



CDH challenge
$(X, Y) = (g^x, g^y)$
Embed
Honest
Embed into key
$pk_0 := X$
Set $pk_1 := g^{sk_1}$
for $sk_1 \leftarrow \mathbb{Z}_p$
Challenge space
Embed Y as
$H(m_i) = Y^{r_i}$
for $r_i \leftarrow \mathbb{Z}_p$
Prob 1/2
Set $H(m_i) := g^{r_i}$
for $r_i \leftarrow \mathbb{Z}_p$
Trapdoor space

Proof Idea

Simulate signatures m_i

$H(m_i) = Y^{r_i}$
for known r_i

$H(m_i) = g^{r_i}$
for known r_i

Proof Idea

Simulate signatures m_i

$H(m_i) = Y^{r_i}$
for known r_i

$\downarrow$

Choose honest
key pk_1

$H(m_i) = g^{r_i}$
for known r_i

$\downarrow$

Choose challenge
key $pk_0 = X$

Proof Idea

Simulate signatures m_i

$H(m_i) = Y^{r_i}$
for known r_i

Choose honest
key pk_1

→ Simulate as $\sigma_i := H(m_i)^{sk_1}$
(honest signing)

$H(m_i) = g^{r_i}$
for known r_i

Choose challenge
key $pk_0 = X$

→ Simulate as $\sigma_i := X^{r_i}$
(trapdoor signing)

Proof Idea

Forgery m^*

$H(m^*) = Y^{r^*}$
for known r^*

$H(m^*) = g^{r^*}$
for known r^*

Choose honest
key pk_1

Choose challenge
key $pk_0 = X$

Proof Idea

Forgery m^*

$H(m^*) = Y^{r^*}$
for known r^*

$H(m^*) = g^{r^*}$
for known r^*

Choose honest key pk_1

Choose challenge key $pk_0 = X$

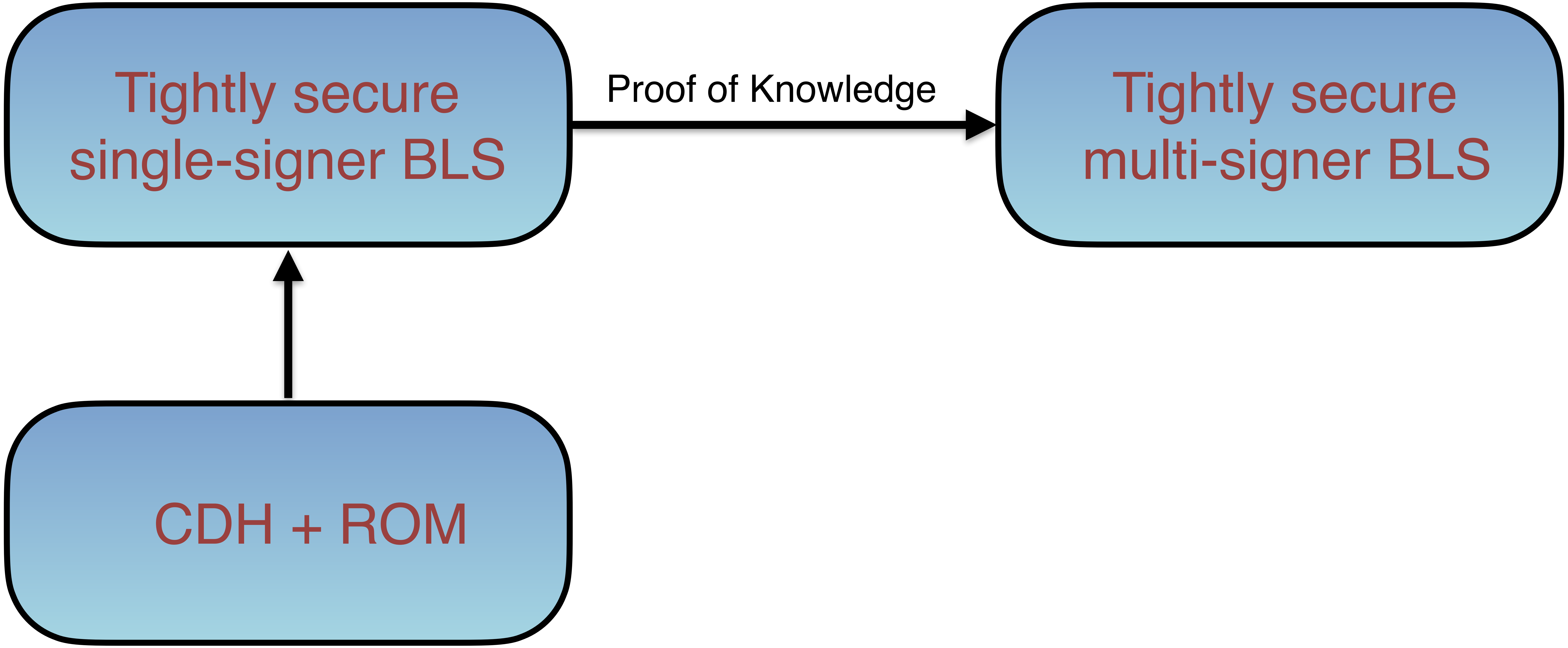
→ With prob 1/4 forgery gives CDH solution $(\sigma^*)^{1/r^*} = Y^x$!

CISPA

HELMHOLTZ CENTER FOR INFORMATION SECURITY

Questions?

Our Results


Tightly secure single-signer BLS
Proof of Knowledge
Tightly secure multi-signer BLS
CDH + ROM