CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

T-Spoon: Tightly Secure 2-Round Multi-Signatures with Key Aggregation

IACR CRYPTO 2025

Renas Bacho, Benedikt Wagner

Multi-Signatures

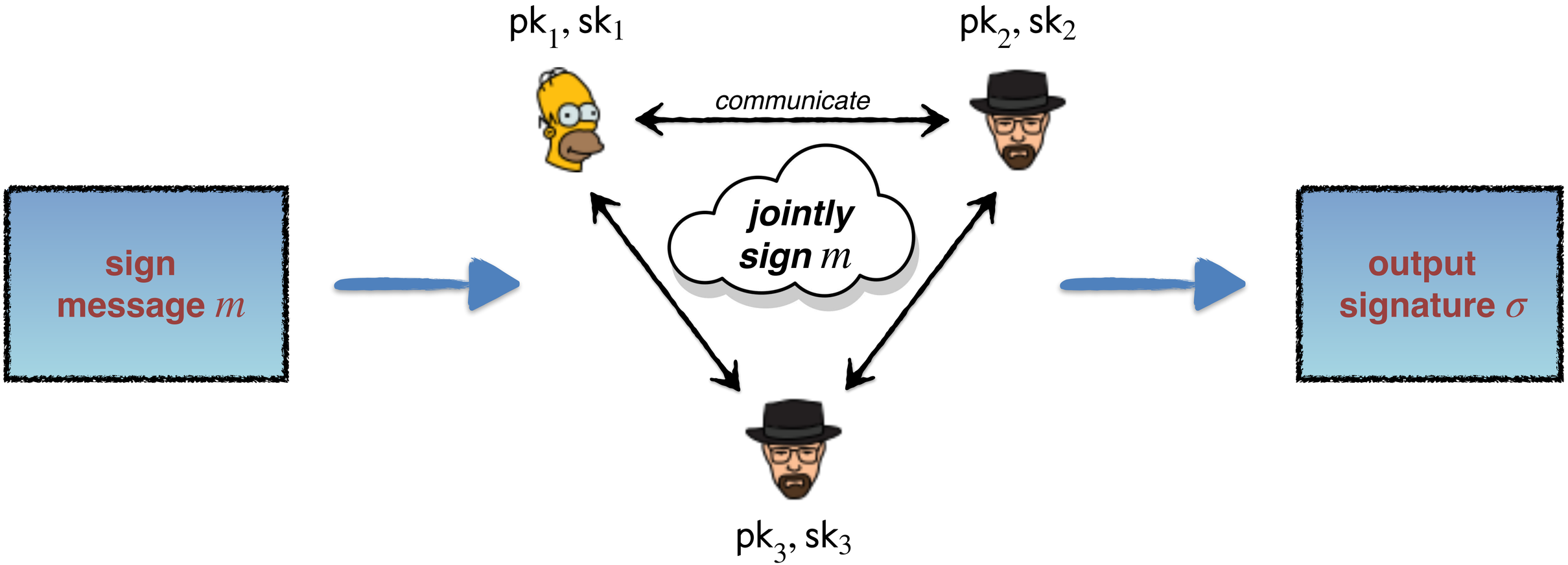
pk_1, sk_1

pk_2, sk_2

sign message m

pk_3, sk_3

Multi-Signatures



Multi-Signatures

Multi-Signatures

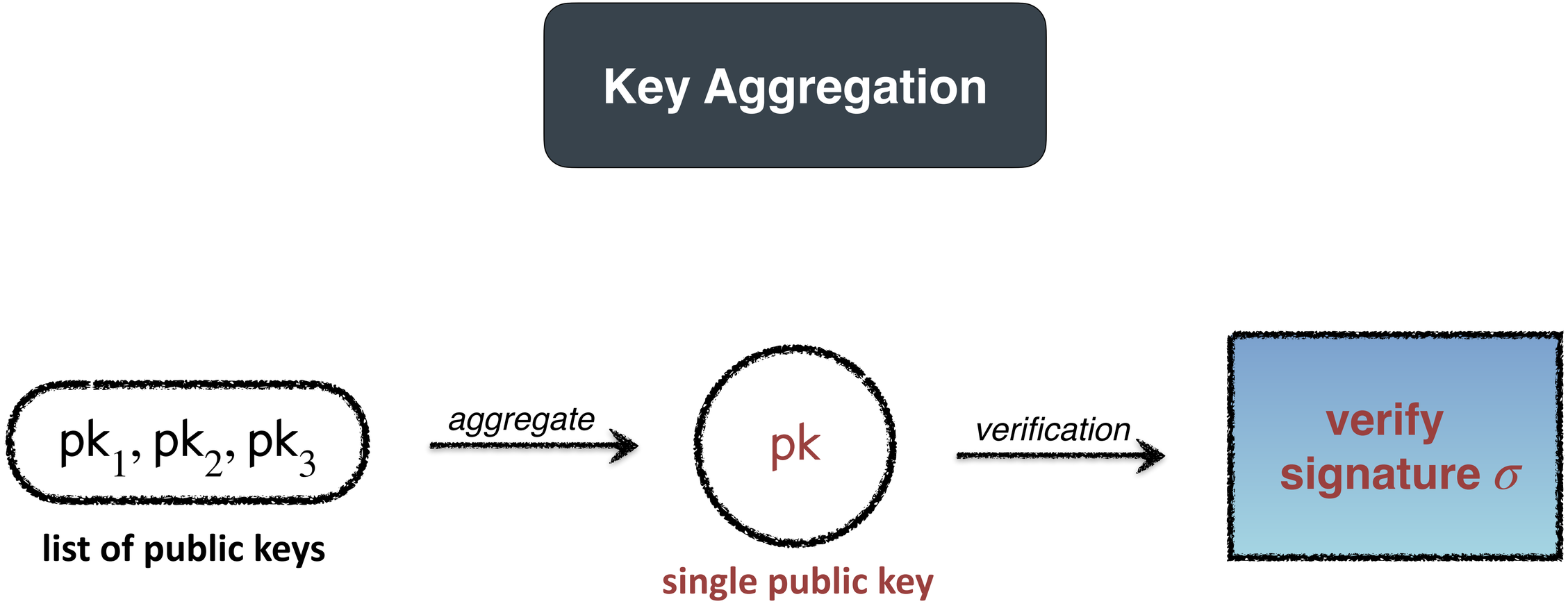
pk_1, pk_2, pk_3

list of public keys

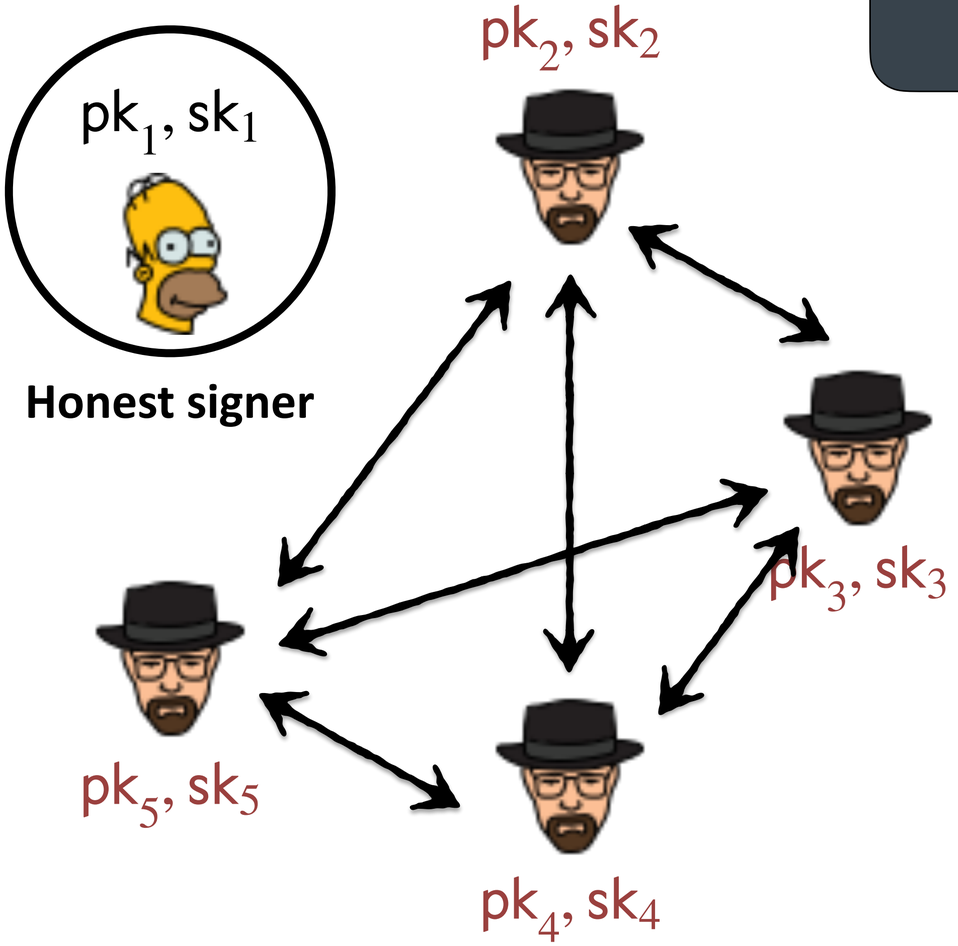
verification →

verify signature σ

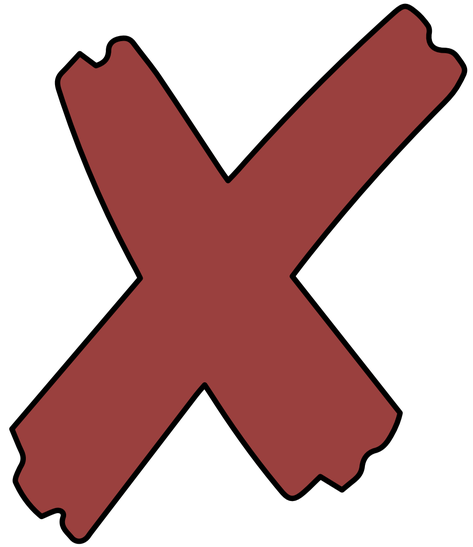
Multi-Signatures



Multi-Signatures

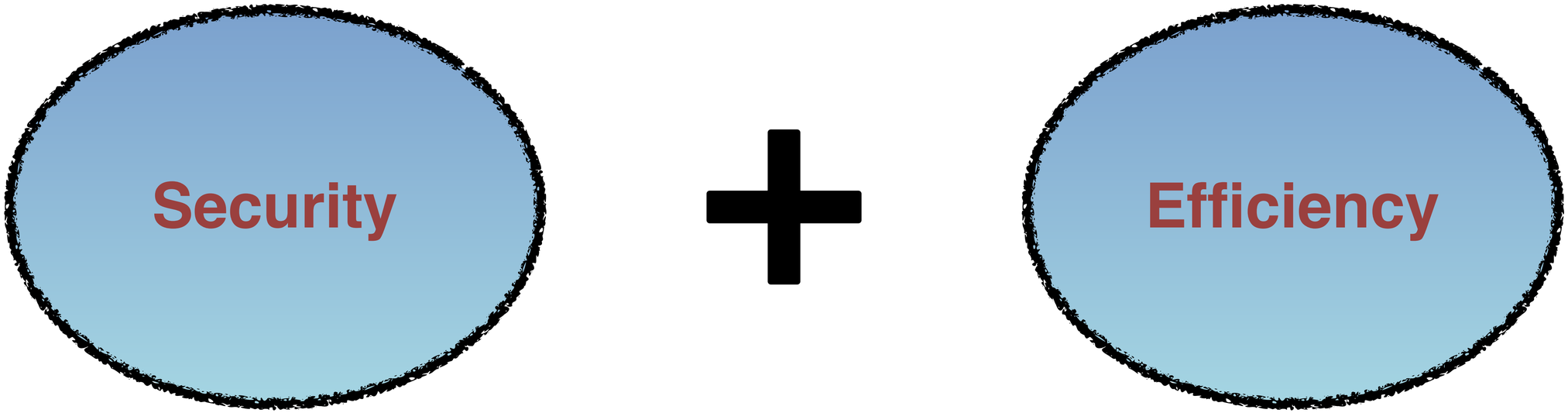


Security: Unforgeability

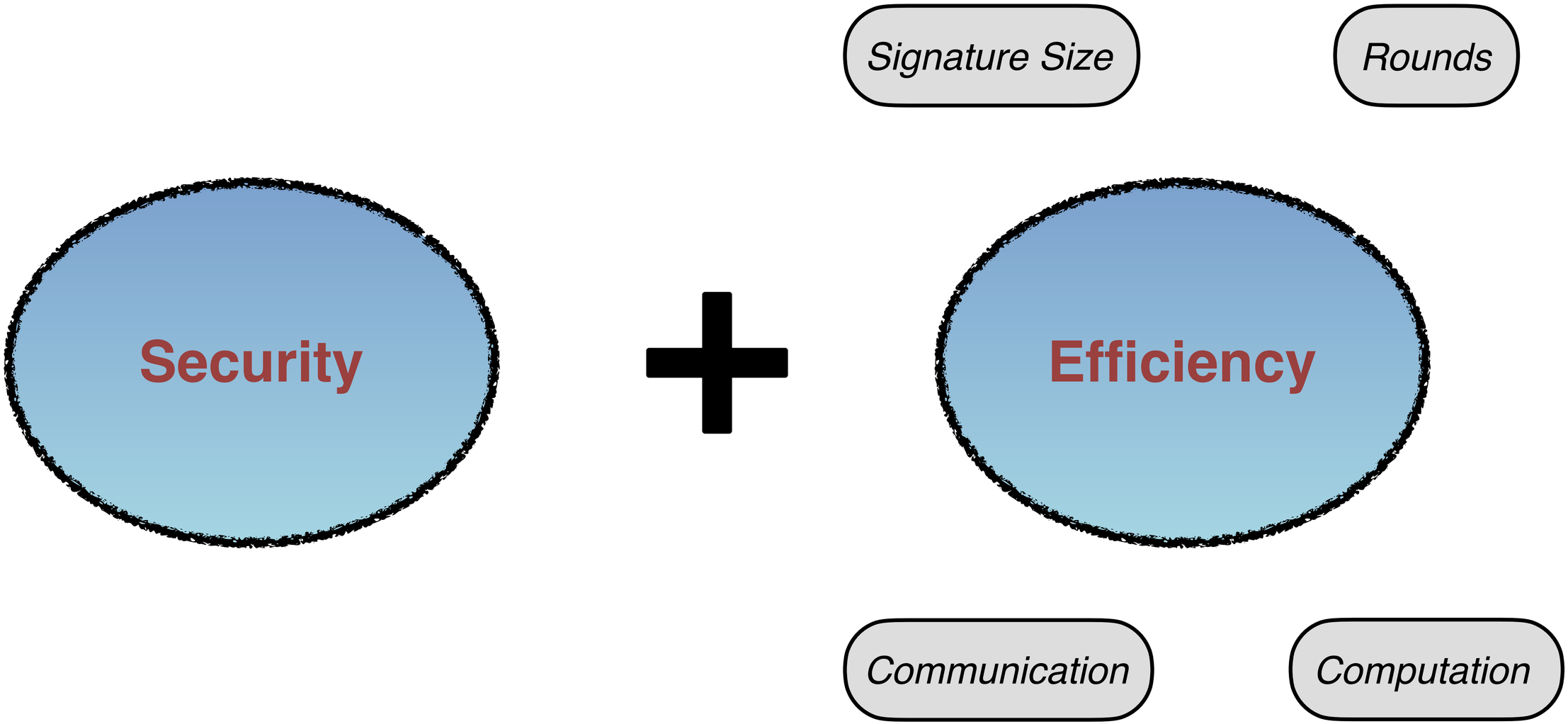


Can not forge signatures !

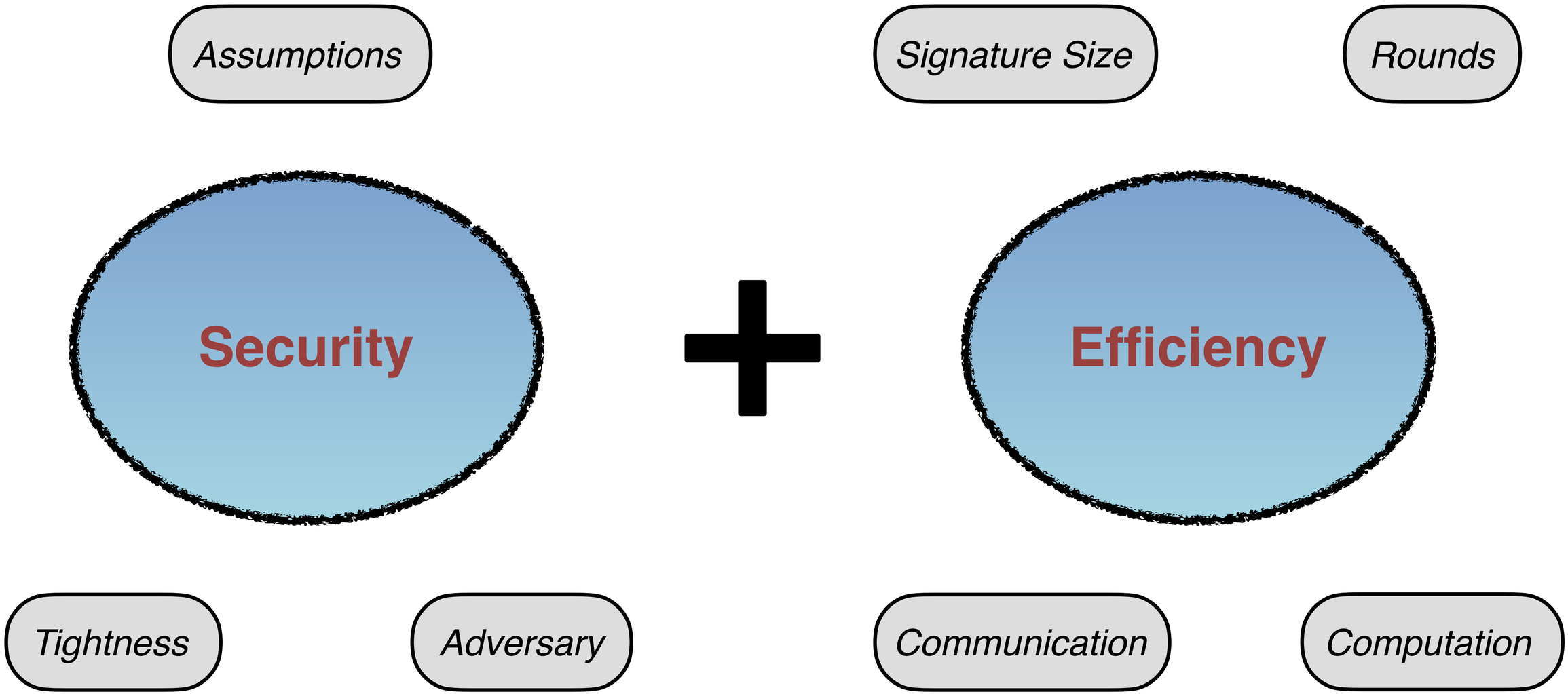
Objectives



Objectives


Signature Size
Rounds
Security
Efficiency
Communication
Computation

Objectives

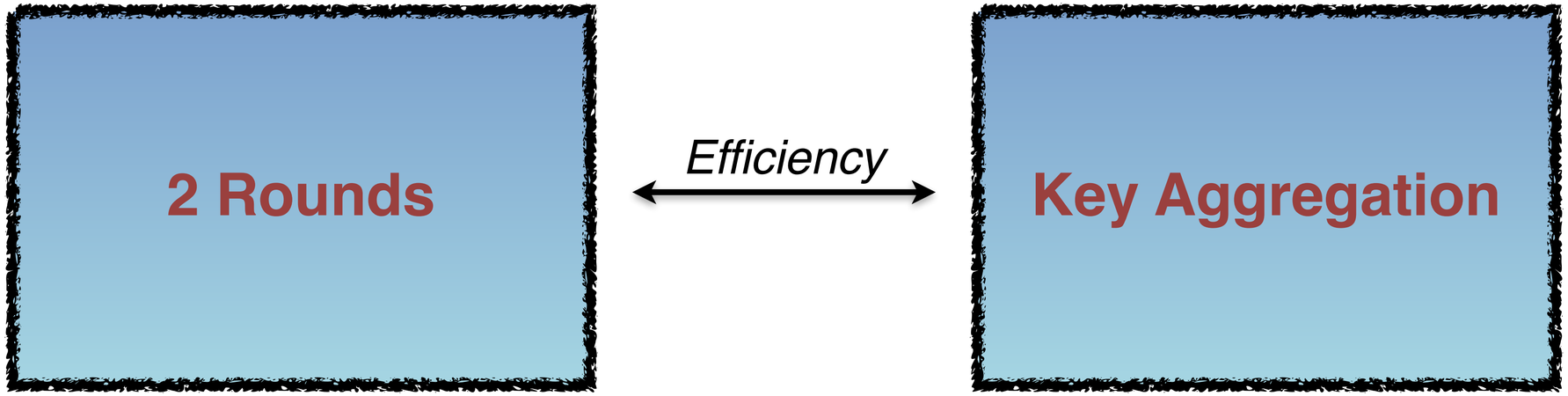

Assumptions
Signature Size
Rounds
Security
+
Efficiency
Tightness
Adversary
Communication
Computation

Objectives

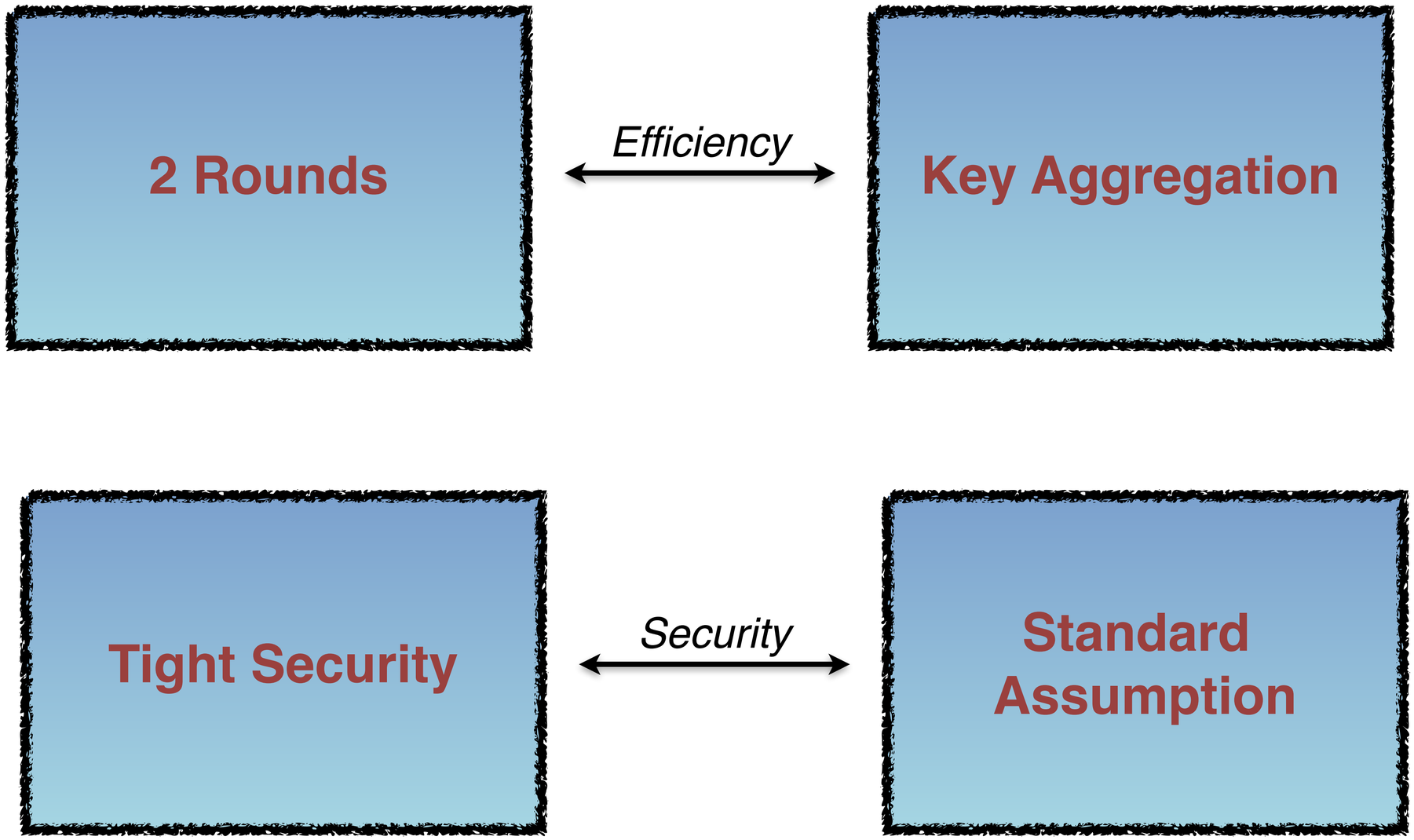
CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

This talk: Pairing-free, discrete logarithm setting

Our Goal



Our Goal


2 Rounds
Efficiency
Key Aggregation
Tight Security
Security
Standard Assumption

State-of-the-Art

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

3 Rounds

[BN ’06]
DDH
Tight

[MuSig ’19]
DLOG
Key Agg

[MuSig-T ’21]
DDH
Tight
Key Agg

2 Rounds

State-of-the-Art

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

3 Rounds

[BN ’06]
DDH
Tight

[MuSig ’19]
DLOG
Key Agg

[MuSig-T ’21]
DDH
Tight
Key Agg

2 Rounds

[MuSig2 ’21]
AOMDL
Key Agg

[TZ ’23]
DLOG
Key Agg

[Chopsticks ’23]
DDH
Tight/Key Agg

What should we do?

Can we design such a tightly secure 2-round MS?

Our Results

T-Spoon
Multi-Signature

Our Results

T-Spoon
Multi-Signature

2 Rounds ⟷ *Efficiency* ⟷ **Key Aggregation**

Tight Security ⟷ *Security* ⟷ **DDH Assumption**

Comparison

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

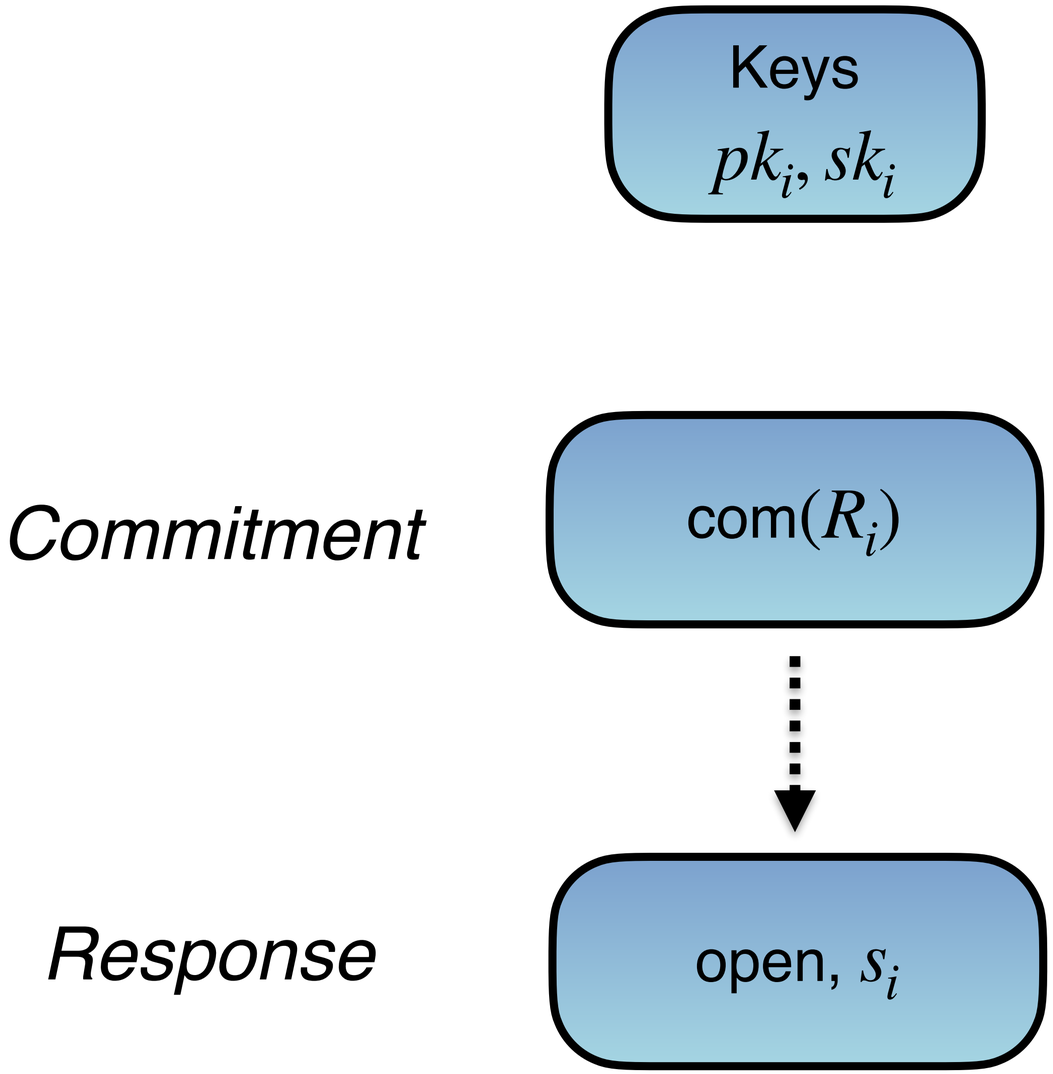
2-Round Multi-Signatures

Scheme	Key Agg	Assumption	Loss	Communication	Signature
Musig2 [NRS21]	✓	AOMDL	$\Theta(Q_H^3/\epsilon^3)$	$4\langle\mathbb{G}\rangle + 1\langle\mathbb{Z}_p\rangle$	$1\langle\mathbb{G}\rangle + 1\langle\mathbb{Z}_p\rangle$
HBMS [BD21]	✓	DLOG	$\Theta(Q_S^4 Q_H^3/\epsilon^3)$	$1\langle\mathbb{G}\rangle + 2\langle\mathbb{Z}_p\rangle$	$1\langle\mathbb{G}\rangle + 2\langle\mathbb{Z}_p\rangle$
TZ [TZ23]	✓	DLOG	$\Theta(Q_H^3/\epsilon^3)$	$4\langle\mathbb{G}\rangle + 2\langle\mathbb{Z}_p\rangle$	$1\langle\mathbb{G}\rangle + 2\langle\mathbb{Z}_p\rangle$
TSSHO [TSS+23]	✓	DDH	$\Theta(Q_S)$	$2\langle\mathbb{G}\rangle + 2\langle\mathbb{Z}_p\rangle$	$3\langle\mathbb{Z}_p\rangle$
Chopsticks I [PW23]	✓	DDH	$\Theta(Q_S)$	$3\langle\mathbb{G}\rangle + 2\langle\mathbb{Z}_p\rangle$	$3\langle\mathbb{G}\rangle + 4\langle\mathbb{Z}_p\rangle$
Toothpicks I [PW24]	✓	DDH	$\Theta(Q_S)$	$2\langle\mathbb{G}\rangle + 2\langle\mathbb{Z}_p\rangle$	$4\langle\mathbb{Z}_p\rangle$
Chopsticks II [PW23]	✗	DDH	$\Theta(1)$	$6\langle\mathbb{G}\rangle + 3\langle\mathbb{Z}_p\rangle$	$6\langle\mathbb{G}\rangle + 8\langle\mathbb{Z}_p\rangle + n$
Toothpicks II [PW24]	✗	DDH	$\Theta(1)$	$2\langle\mathbb{G}\rangle + 2\langle\mathbb{Z}_p\rangle$	$4\langle\mathbb{Z}_p\rangle + n$
T-Spoon (ours)	✓	DDH	$\Theta(1)$	$3\langle\mathbb{G}\rangle + 2\langle\mathbb{Z}_p\rangle$	$2\langle\mathbb{G}\rangle + 9\langle\mathbb{Z}_p\rangle$

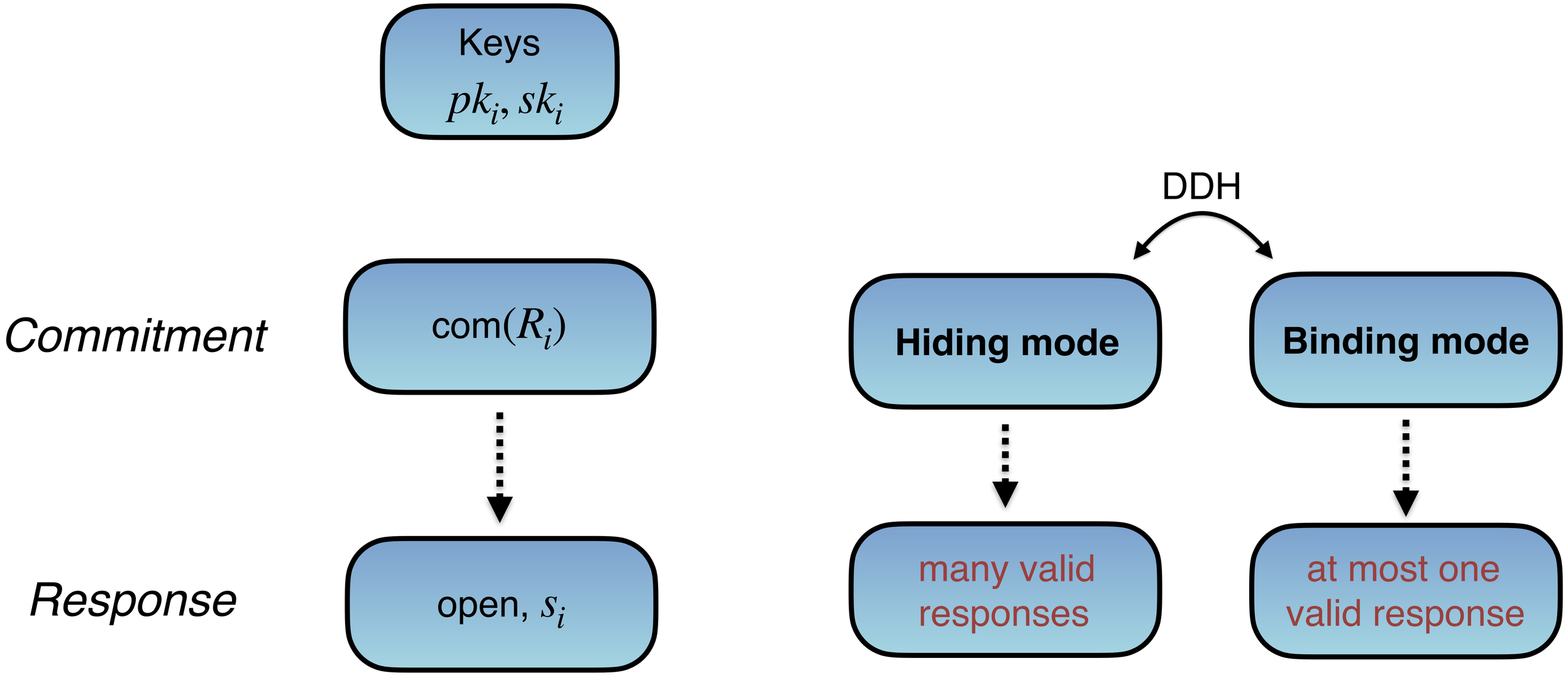
CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

Our Techniques

Starting Point: Chopsticks

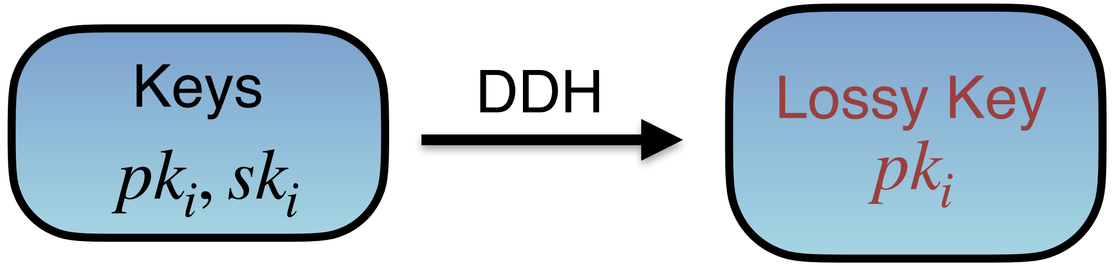


Starting Point: Chopsticks



Starting Point: Chopsticks

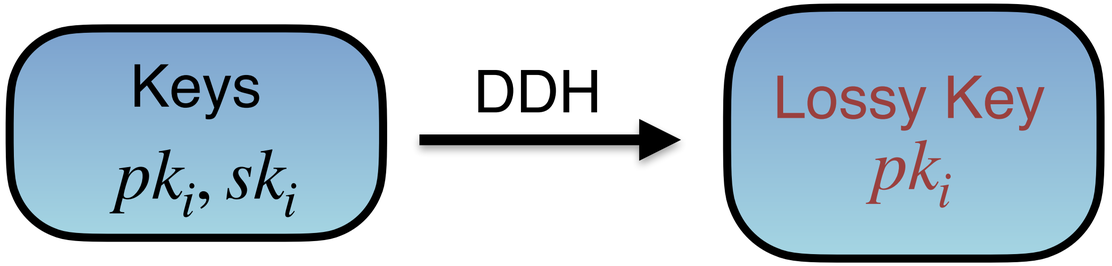
Reduction idea:



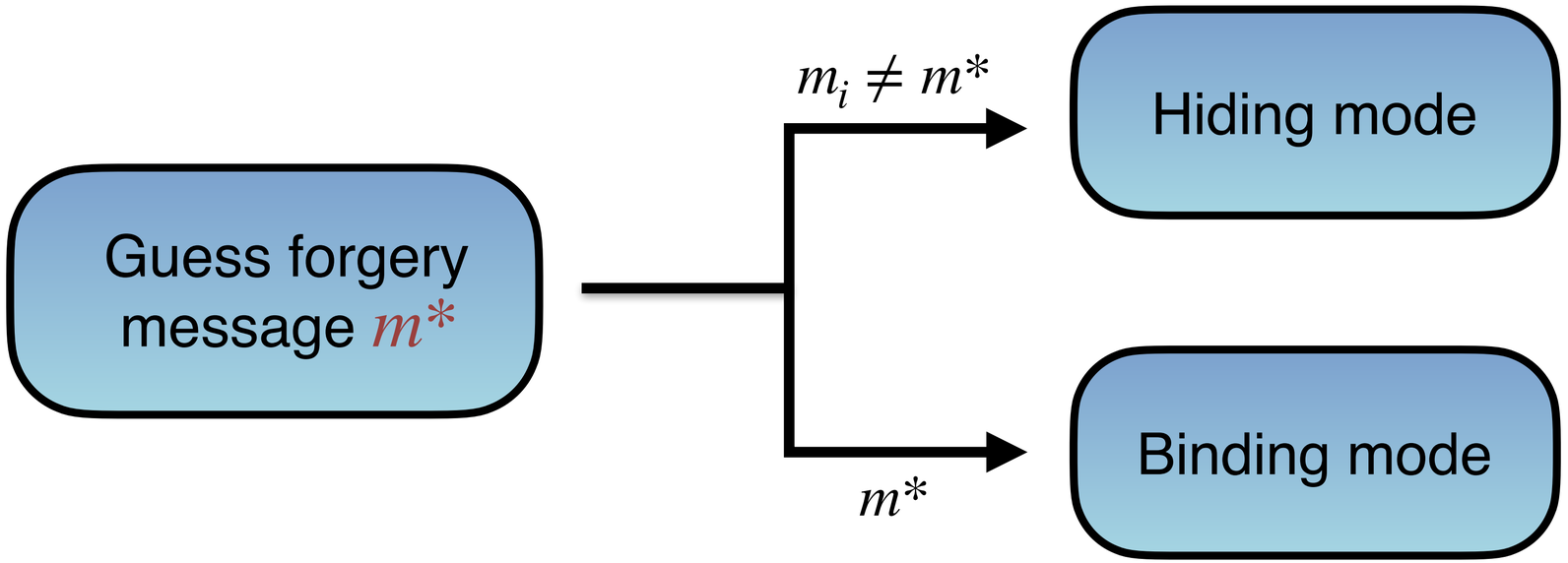
There is no secret key !

Starting Point: Chopsticks

Reduction idea:

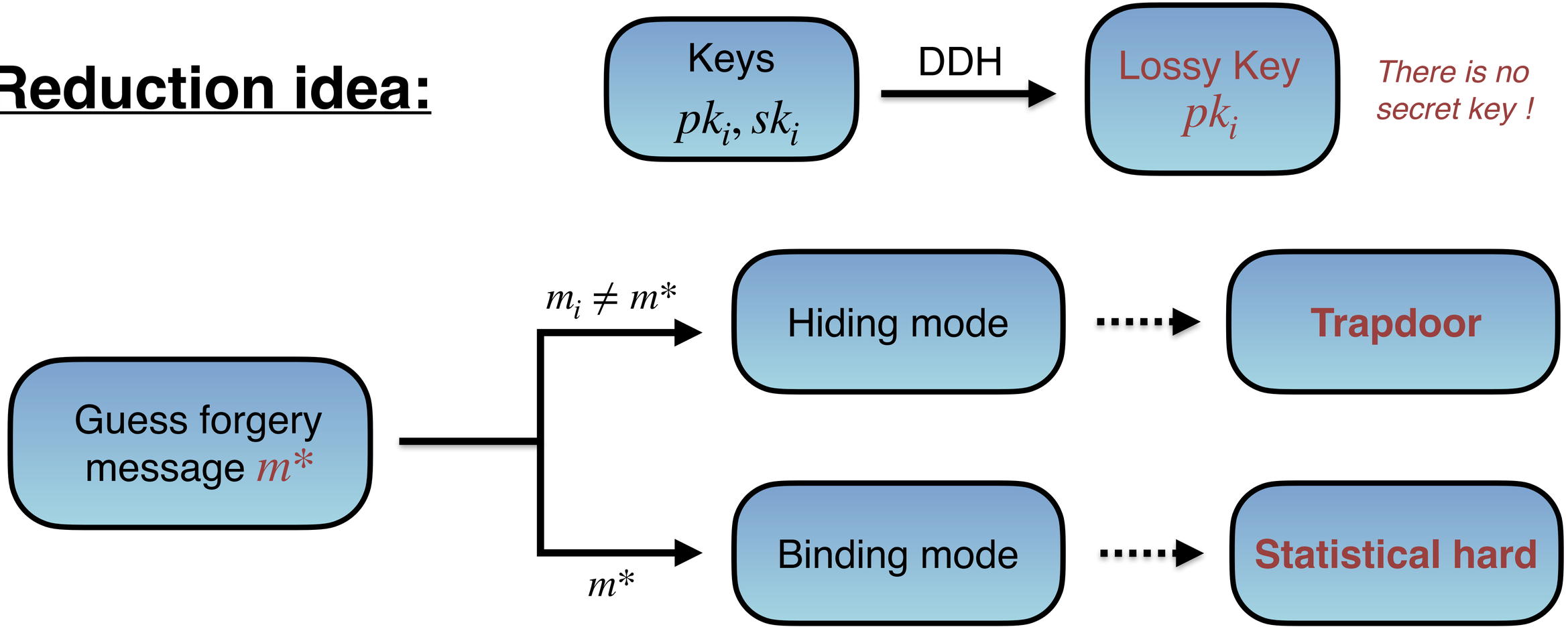


There is no secret key !



Starting Point: Chopsticks

Reduction idea:



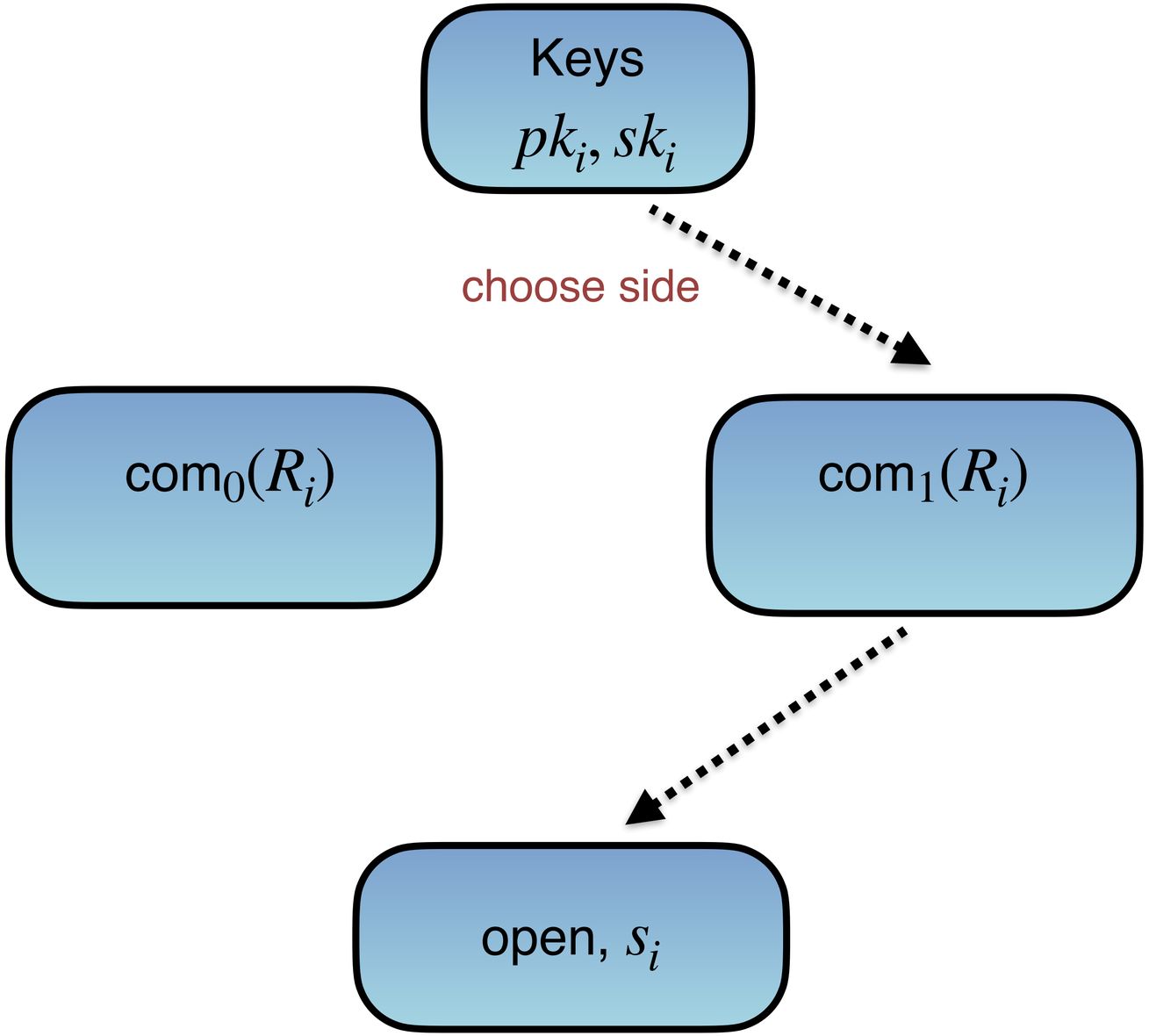
Guessing: security loss of $O(q_s)$!

Our Ideas

Construction

Commitment

Response

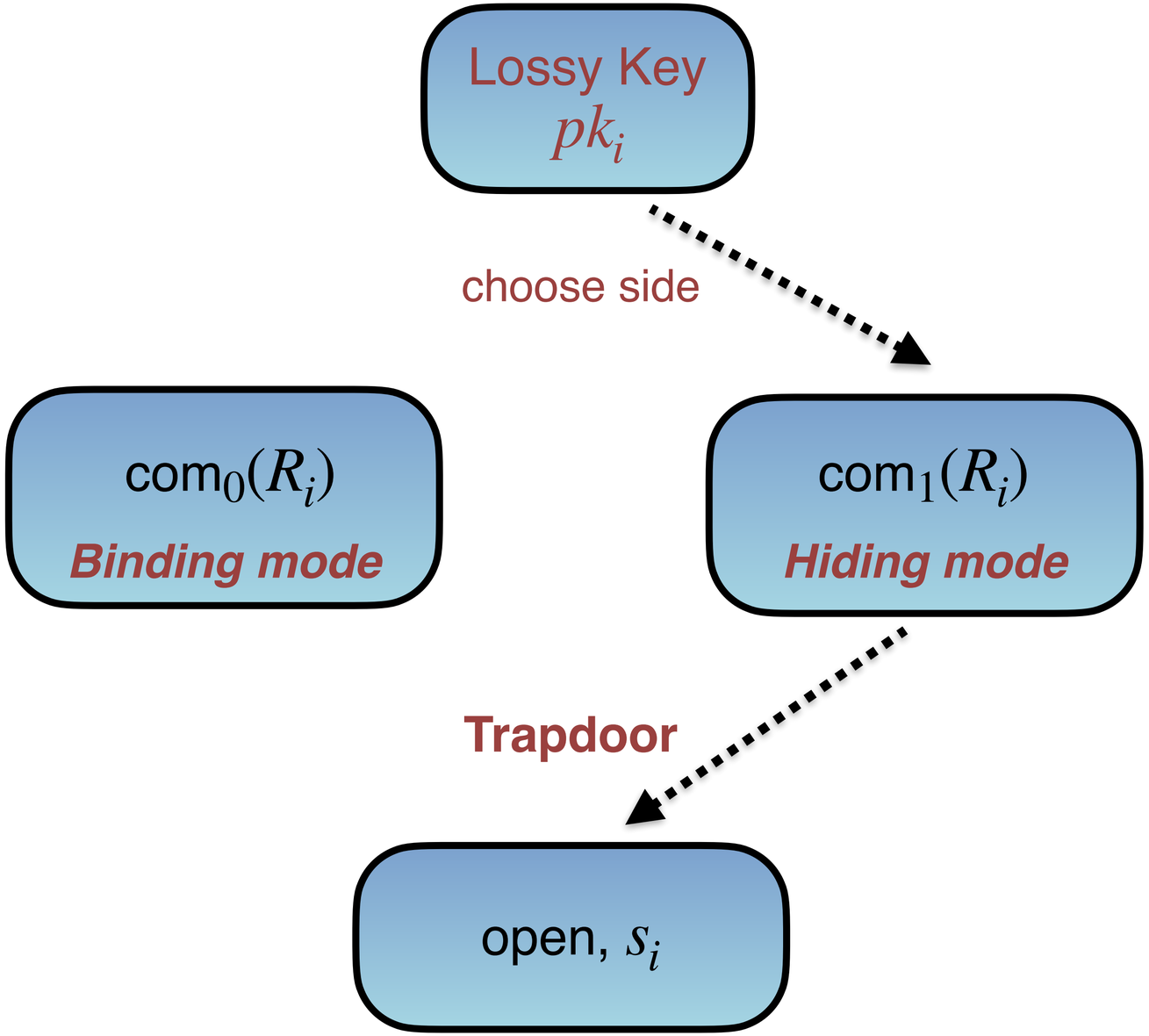


Our Ideas

Simulation

Commitment

Response

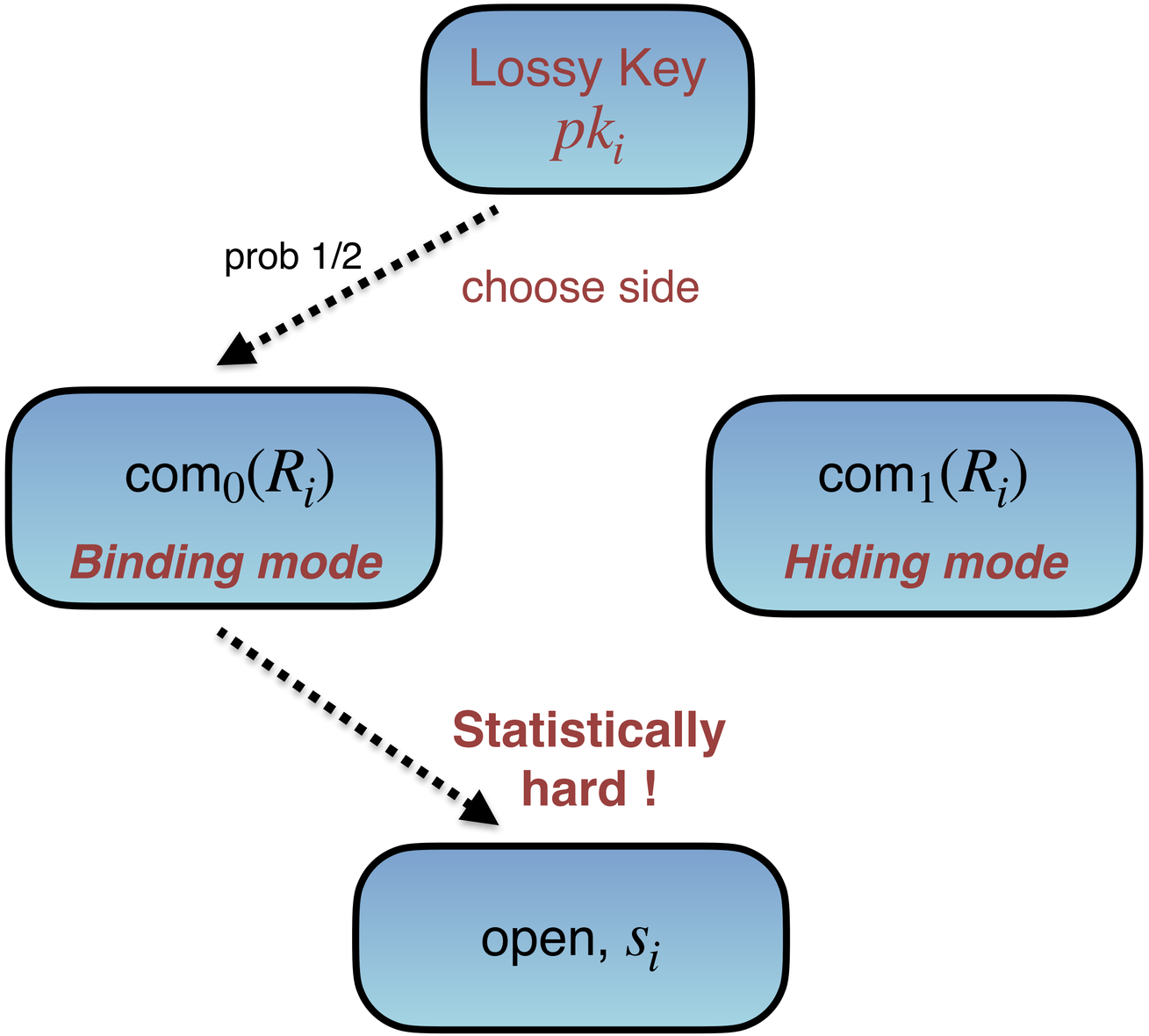


Our Ideas

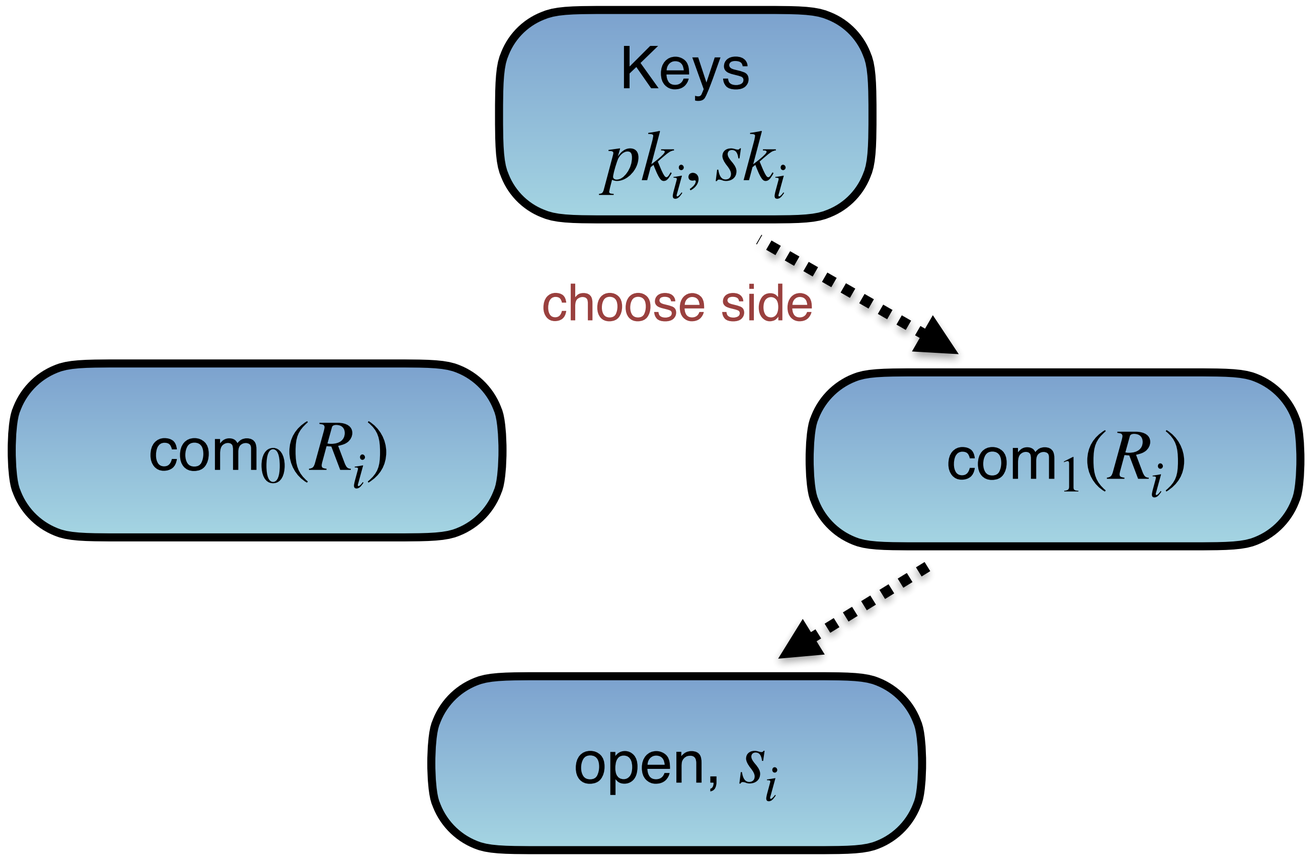
Forgery m^*

Commitment

Response

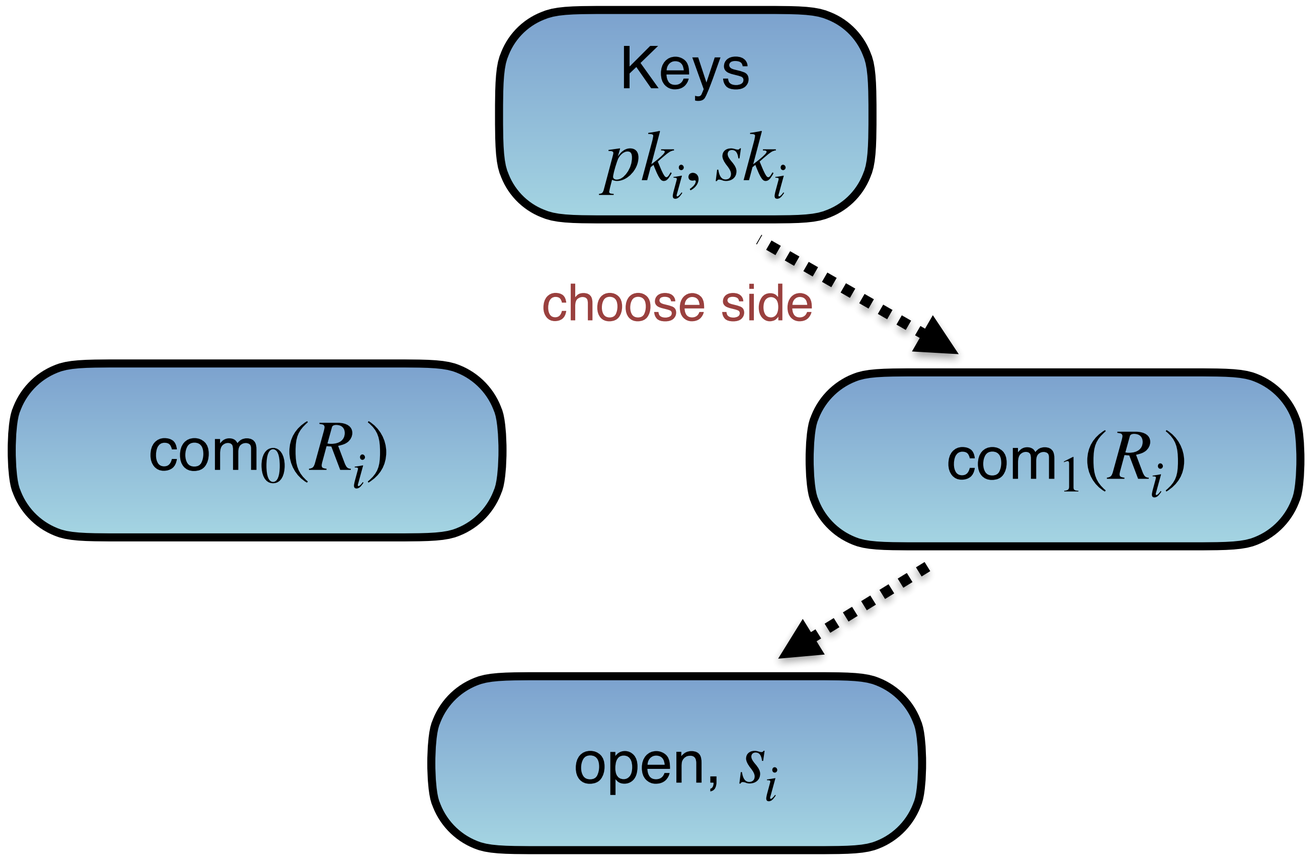


Our Ideas



How to aggregate different sides?

Our Ideas



How to aggregate different sides?

Signer partition technique !

CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

Questions?

Our Results

Multi-Signature

- **2 rounds**
- **Tightly secure**
- **DDH assumption**
- **Key aggregation**