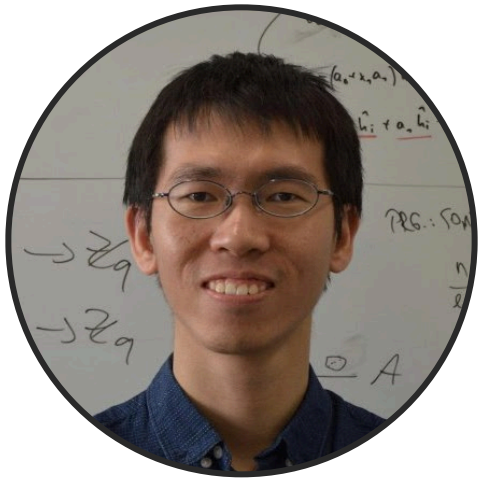
# Chopsticks:
## Fork-Free Two-Round Multi-Signatures from Non-Interactive Assumptions




Jiaxin Pan

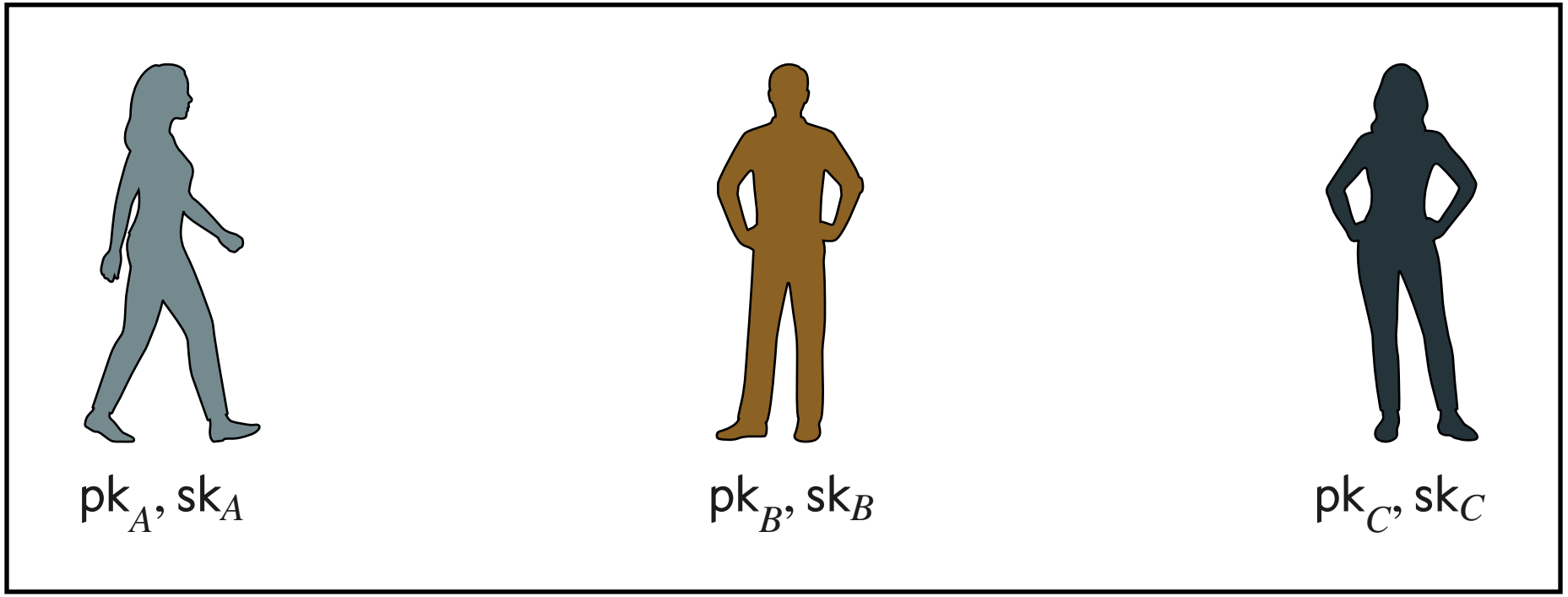
NTNU

**Benedikt Wagner**

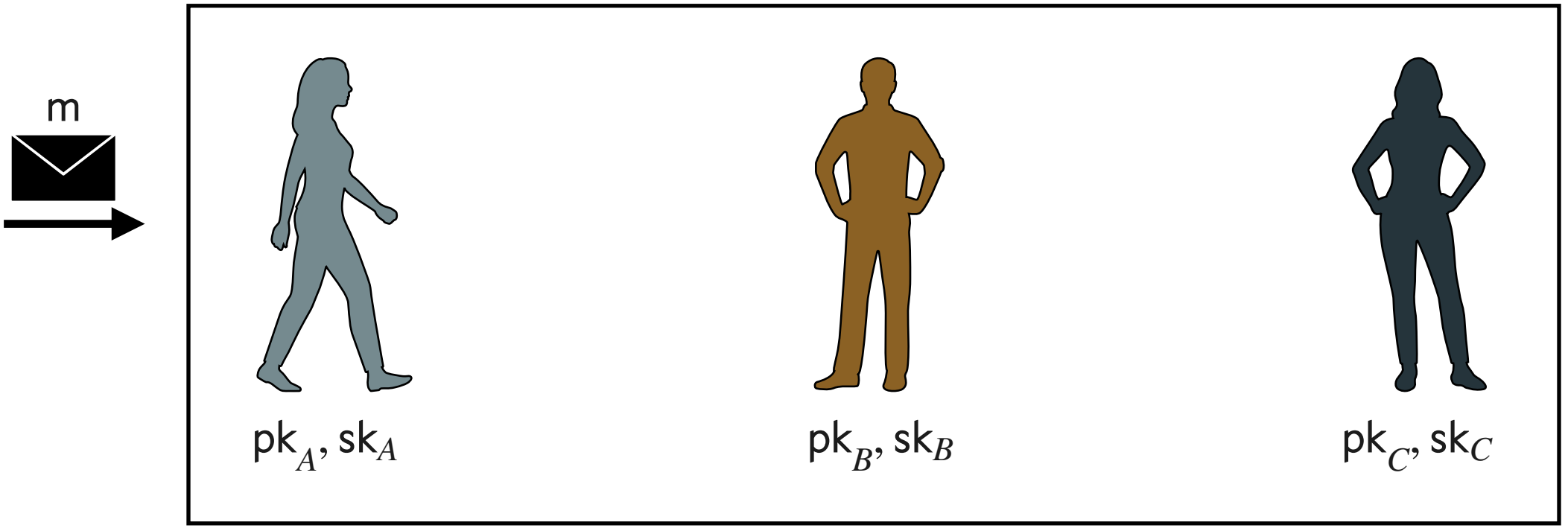
CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY


# Multi-Signatures

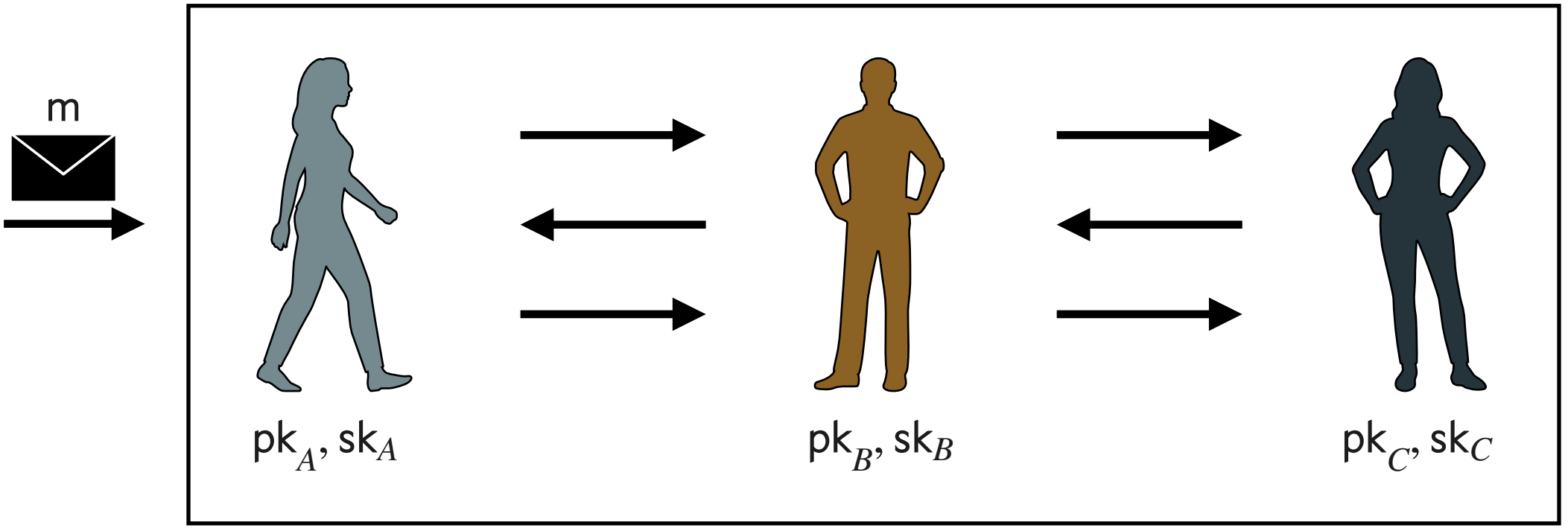
# Multi-Signatures



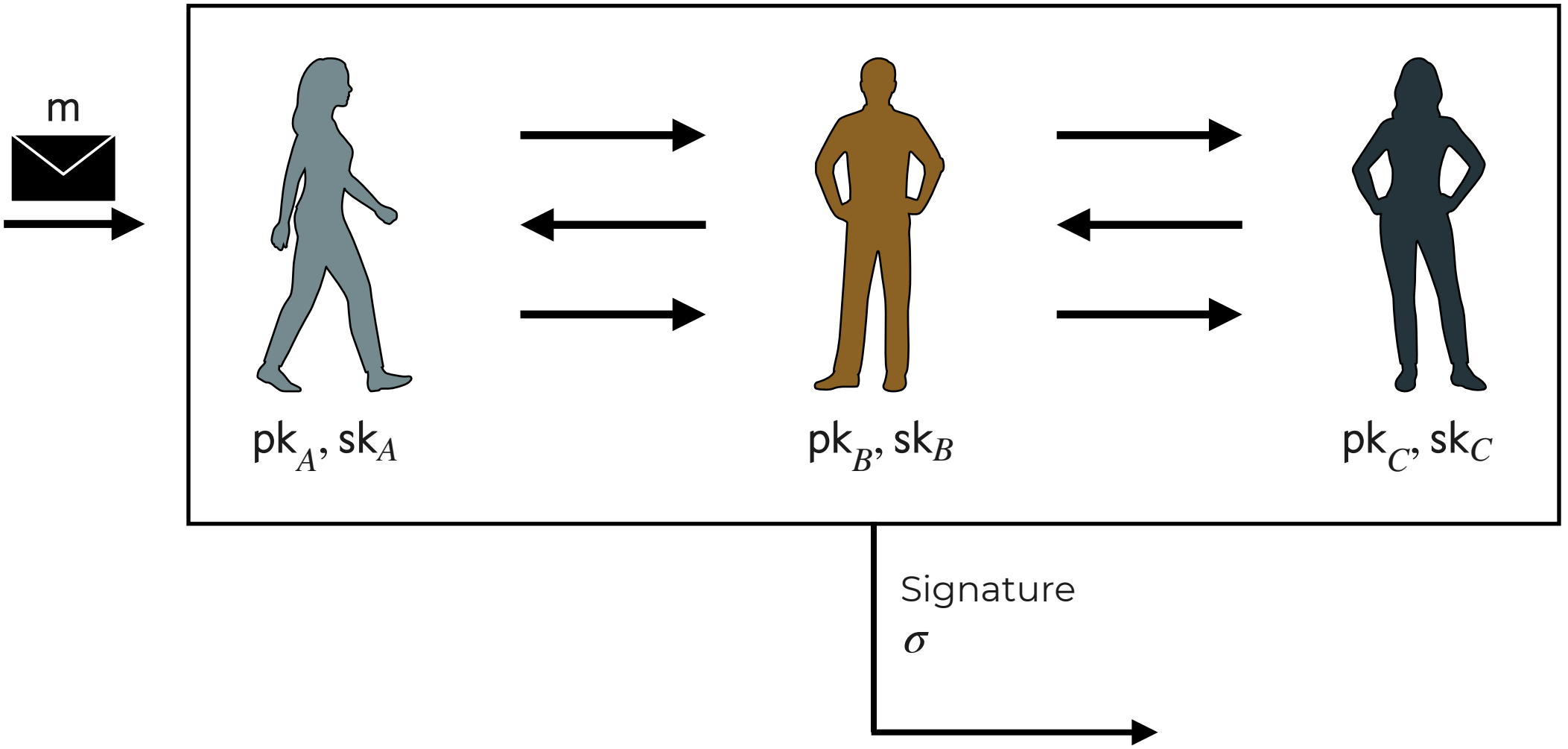
# Multi-Signatures



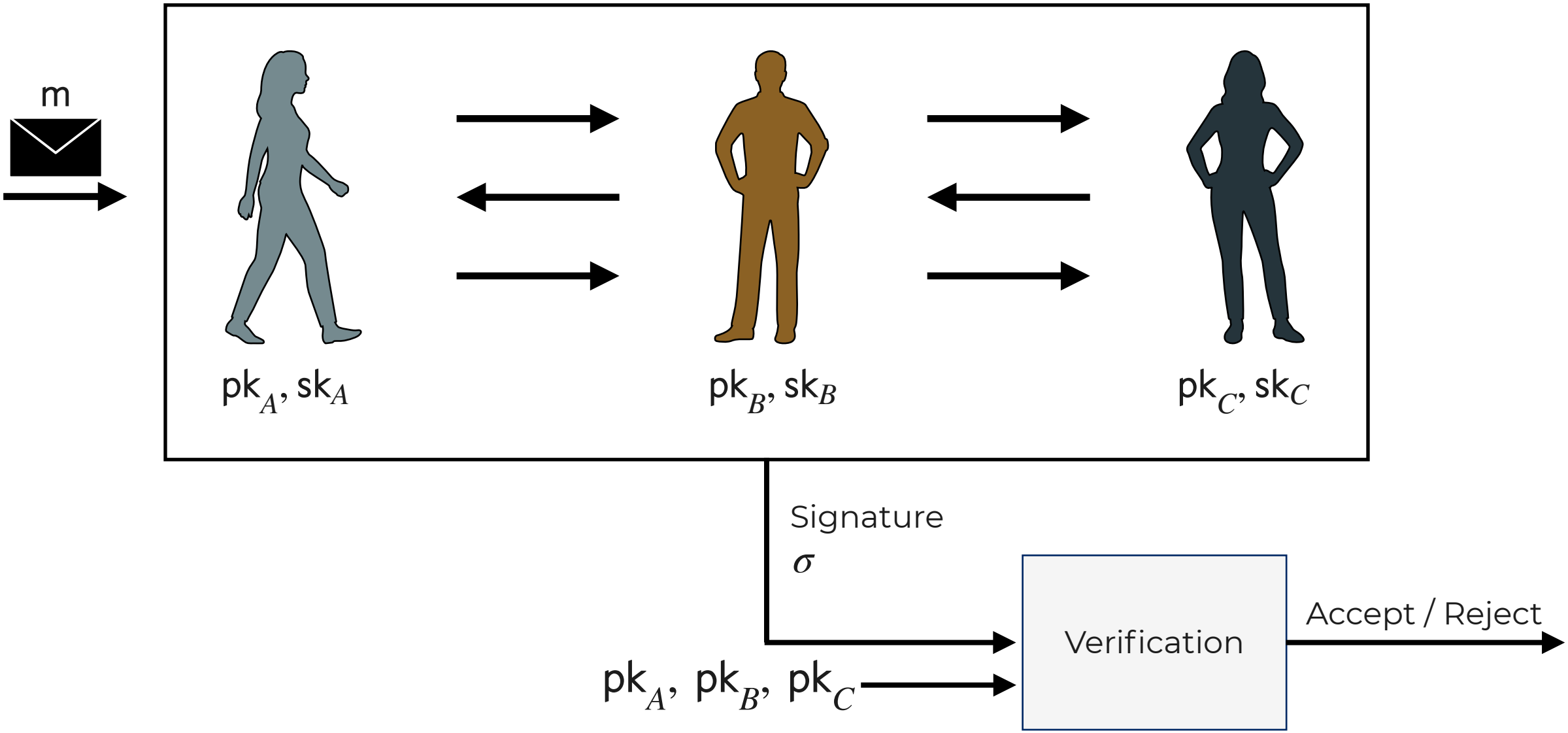
# Multi-Signatures



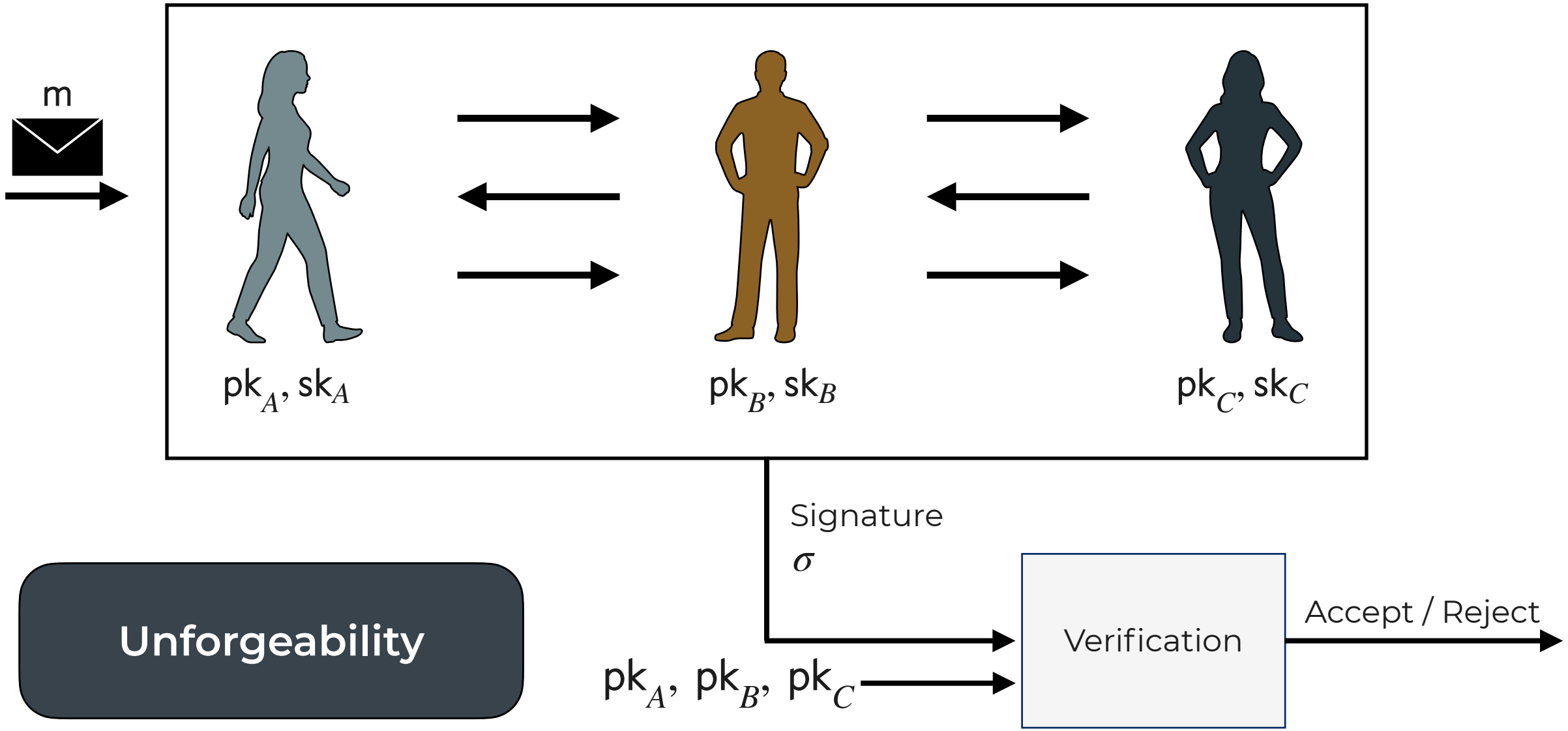
# Multi-Signatures



# Multi-Signatures



# Multi-Signatures




**Unforgeability**

# Multi-Signatures - Objectives

## Efficiency

## Functionality

## Security

# Multi-Signatures - Objectives

**Efficiency**

Signature Size

**Functionality**

**Security**

# Multi-Signatures - Objectives

**Efficiency**

- Signature Size
- Communication
- Round Complexity
- Computation

**Functionality**

**Security**

# Multi-Signatures - Objectives

**Efficiency**

- Signature Size
- Communication
- Round Complexity
- Computation

**Functionality**

- Key Aggregation

**Security**

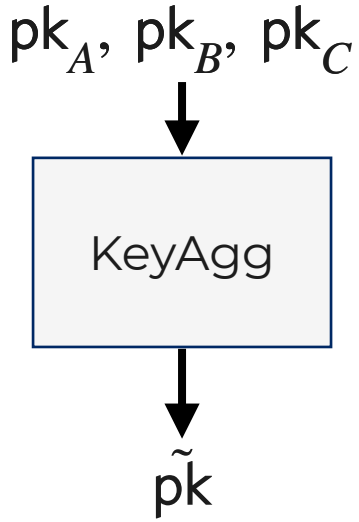
# Multi-Signatures - Objectives

**Efficiency**

- Signature Size
- Communication
- Round Complexity
- Computation

**Functionality**

- Key Aggregation




**Security**

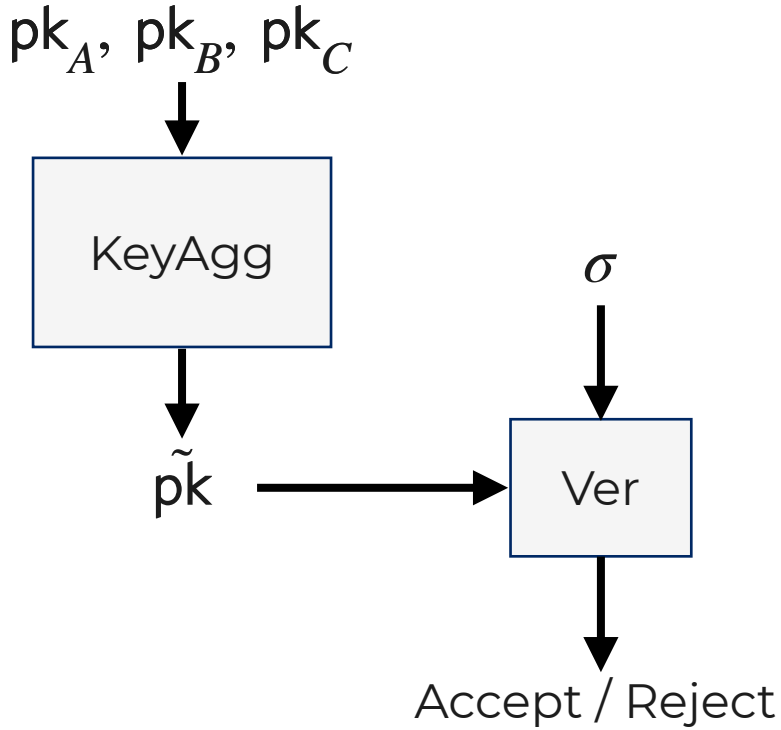
# Multi-Signatures - Objectives

**Efficiency**

- Signature Size
- Communication
- Round Complexity
- Computation

**Functionality**

- Key Aggregation




**Security**

# Multi-Signatures - Objectives

**Efficiency**

- Signature Size
- Communication
- Round Complexity
- Computation

**Functionality**

- Key Aggregation
- Preprocessing

**Security**

# Multi-Signatures - Objectives

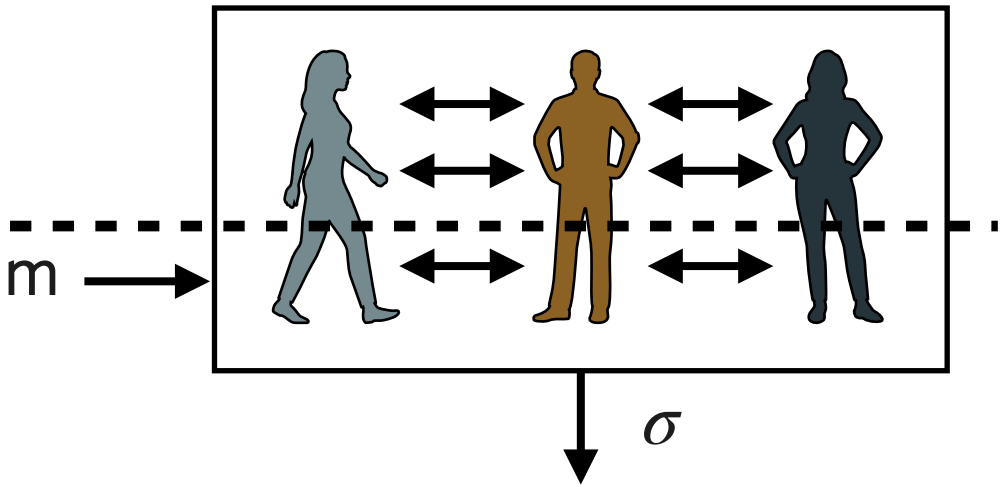
**Efficiency**

- Signature Size
- Communication
- Round Complexity
- Computation

**Functionality**

- Key Aggregation
- Preprocessing

**Security**



# Multi-Signatures - Objectives

**Efficiency**

- Signature Size
- Communication
- Round Complexity
- Computation

**Functionality**

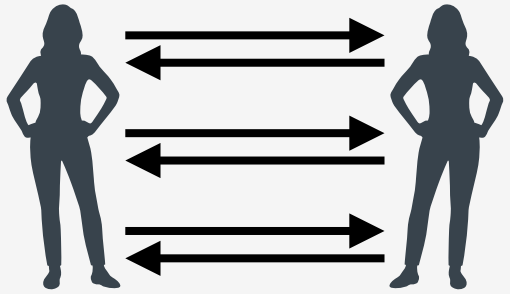
- Key Aggregation
- Preprocessing

**Security**

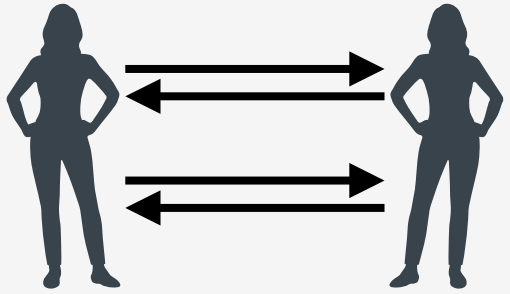
- Assumptions
- Security Loss

# State-of-the-Art

## 3 Rounds



## 2 Rounds

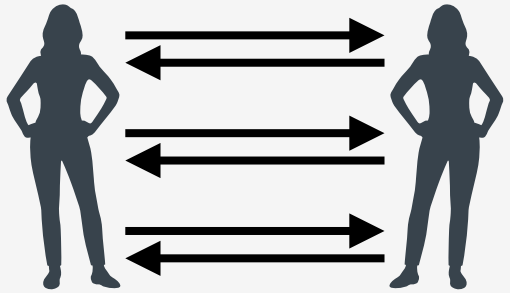




BN [CCS 06, BN], Musig [Asiacrypt 18, BDN, and DCC 19, MPS+], Musig-T [IJNC 21, FH], Musig2 [Crypto 21, NRS], HBMS [Asiacrypt 21, BD]

# State-of-the-Art

**3 Rounds**

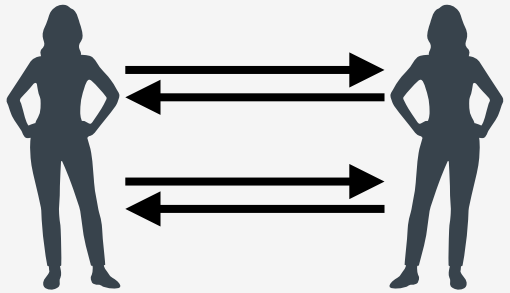


**BN**

DLOG

$$\epsilon^2 \leq Q_H \epsilon'$$

**2 Rounds**

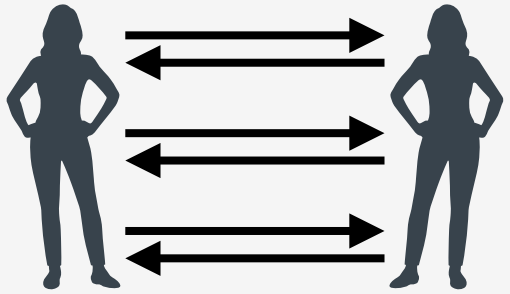




BN [CCS 06, BN], Musig [Asiacrypt 18, BDN, and DCC 19, MPS+], Musig-T [IJNC 21, FH], Musig2 [Crypto 21, NRS], HBMS [Asiacrypt 21, BD]

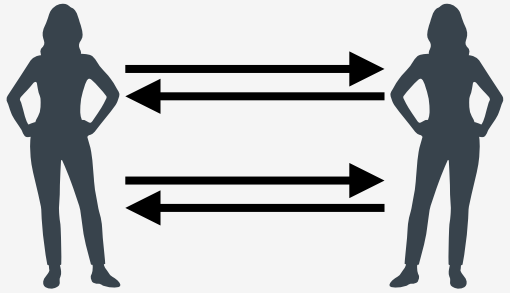
# State-of-the-Art

**3 Rounds**



| **BN** | **BN** |
|---|---|
| DLOG | DDH |
| $\epsilon^2 \leq Q_H \epsilon'$ | $\epsilon \leq \epsilon'$ |

**2 Rounds**

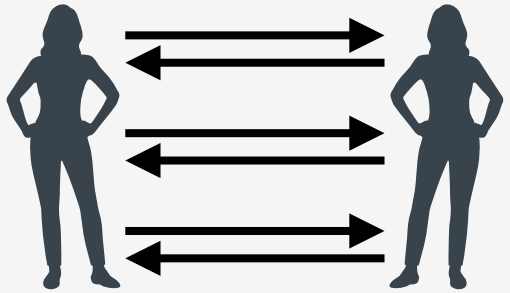




BN [CCS 06, BN], Musig [Asiacrypt 18, BDN, and DCC 19, MPS+], Musig-T [IJNC 21, FH], Musig2 [Crypto 21, NRS], HBMS [Asiacrypt 21, BD]

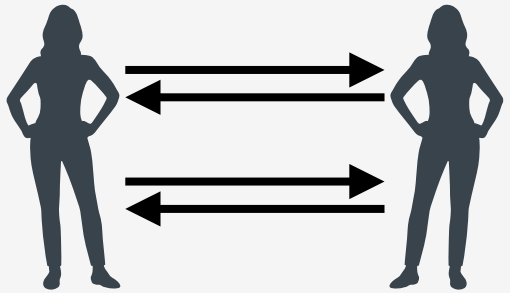
# State-of-the-Art

**3 Rounds**



| BN | BN | Musig | Musig-T |
|---|---|---|---|
| DLOG | DDH | DLOG | DDH |
| $\epsilon^2 \leq Q_H \epsilon'$ | $\epsilon \leq \epsilon'$ | $\epsilon^4 \leq Q_H^3 \epsilon'$ | $\epsilon \leq \epsilon'$ |
| | | KA | KA |

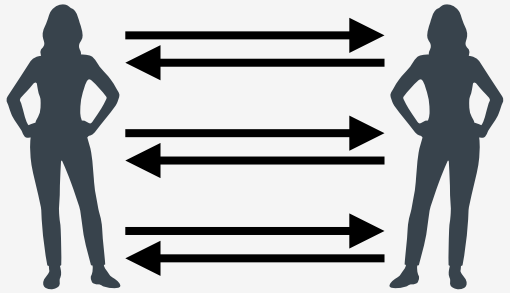
**2 Rounds**



4 BN [CCS 06, BN], Musig [Asiacrypt 18, BDN, and DCC 19, MPS+], Musig-T [IJNC 21, FH], Musig2 [Crypto 21, NRS], HBMS [Asiacrypt 21, BD]

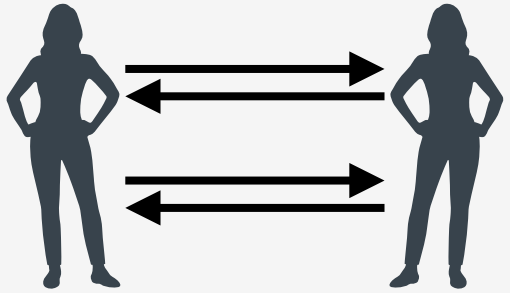
# State-of-the-Art

**3 Rounds**



| BN | BN | Musig | Musig-T |
|---|---|---|---|
| DLOG | DDH | DLOG | DDH |
| $\epsilon^2 \leq Q_H \epsilon'$ | $\epsilon \leq \epsilon'$ | $\epsilon^4 \leq Q_H^3 \epsilon'$ | $\epsilon \leq \epsilon'$ |
| | | KA | KA |

**2 Rounds**



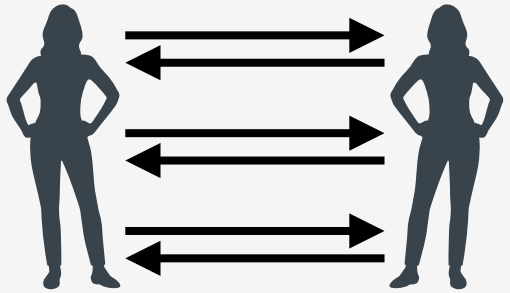
| Musig2 |
|---|
| OMDL |
| $\epsilon^4 \leq Q_H^3 \epsilon'$ |
| KA |



BN [CCS 06, BN], Musig [Asiacrypt 18, BDN, and DCC 19, MPS+], Musig-T [IJNC 21, FH], Musig2 [Crypto 21, NRS], HBMS [Asiacrypt 21, BD]

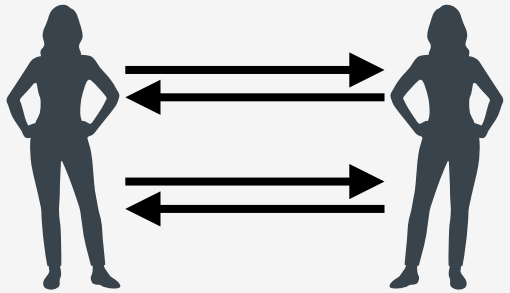
# State-of-the-Art

**3 Rounds**



| BN | BN | Musig | Musig-T |
|---|---|---|---|
| DLOG | DDH | DLOG | DDH |
| $\epsilon^2 \leq Q_H \epsilon'$ | $\epsilon \leq \epsilon'$ | $\epsilon^4 \leq Q_H^3 \epsilon'$ | $\epsilon \leq \epsilon'$ |
| | | KA | KA |

**2 Rounds**



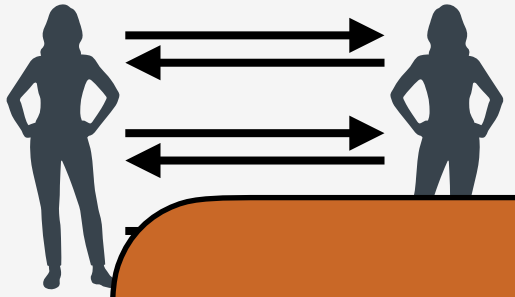
| Musig2 | HBMS |
|---|---|
| OMDL | DLOG |
| $\epsilon^4 \leq Q_H^3 \epsilon'$ | $\epsilon^4 \leq Q_S^4 Q_H^3 \epsilon'$ |
| KA | KA |



BN [CCS 06, BN], Musig [Asiacrypt 18, BDN, and DCC 19, MPS+], Musig-T [IJNC 21, FH], Musig2 [Crypto 21, NRS], HBMS [Asiacrypt 21, BD]

# State-of-the-Art

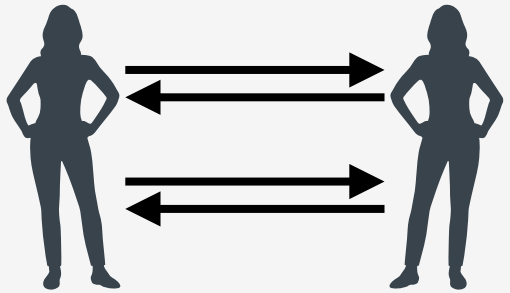
**3 Rounds**



| BN | BN | Musig | Musig-T |
|---|---|---|---|
| DLOG | DDH | DLOG | DDH |
| $\epsilon^2 \leq Q_H \epsilon'$ | $\epsilon \leq \epsilon'$ | $\epsilon^4 \leq Q_H^3 \epsilon'$ | $\epsilon \leq \epsilon'$ |

Is Rewinding Inherent for Two-round Schemes?

**2 Rou**



| OMDL | DLOG |
|---|---|
| $\epsilon^4 \leq Q_H^3 \epsilon'$ | $\epsilon^4 \leq Q_S^4 Q_H^3 \epsilon'$ |
| KA | KA |



BN [CCS 06, BN], Musig [Asiacrypt 18, BDN, and DCC 19, MPS+], Musig-T [IJNC 21, FH], Musig2 [Crypto 21, NRS], HBMS [Asiacrypt 21, BD]

# Our Goals

# Our Goals

Round Complexity

*2 Rounds*

# Our Goals

Round Complexity

*2 Rounds*

Assumptions

*Non-Interactive, Well-Studied*

# Our Goals

Round Complexity

*2 Rounds*

Assumptions

*Non-Interactive, Well-Studied*

Security Loss

*Avoid Rewinding*
*Ideally: Tight*

# Our Results

Round Complexity

*2 Rounds*

Assumptions

*Non-Interactive, Well-Studied*

Security Loss

*Avoid Rewinding Ideally: Tight*

**Multi-Signature**

- 2 Rounds
- DDH Assumption
- $\epsilon \leq Q_S \epsilon'$
- Key Aggregation

**Multi-Signature**

- 2 Rounds
- DDH Assumption
- $\epsilon \leq \epsilon'$

# Technical Part

# What we know so Far

# What we know so Far

**Schnorr Identification**

$$R = F(r)$$

$$\longrightarrow$$

$$c$$

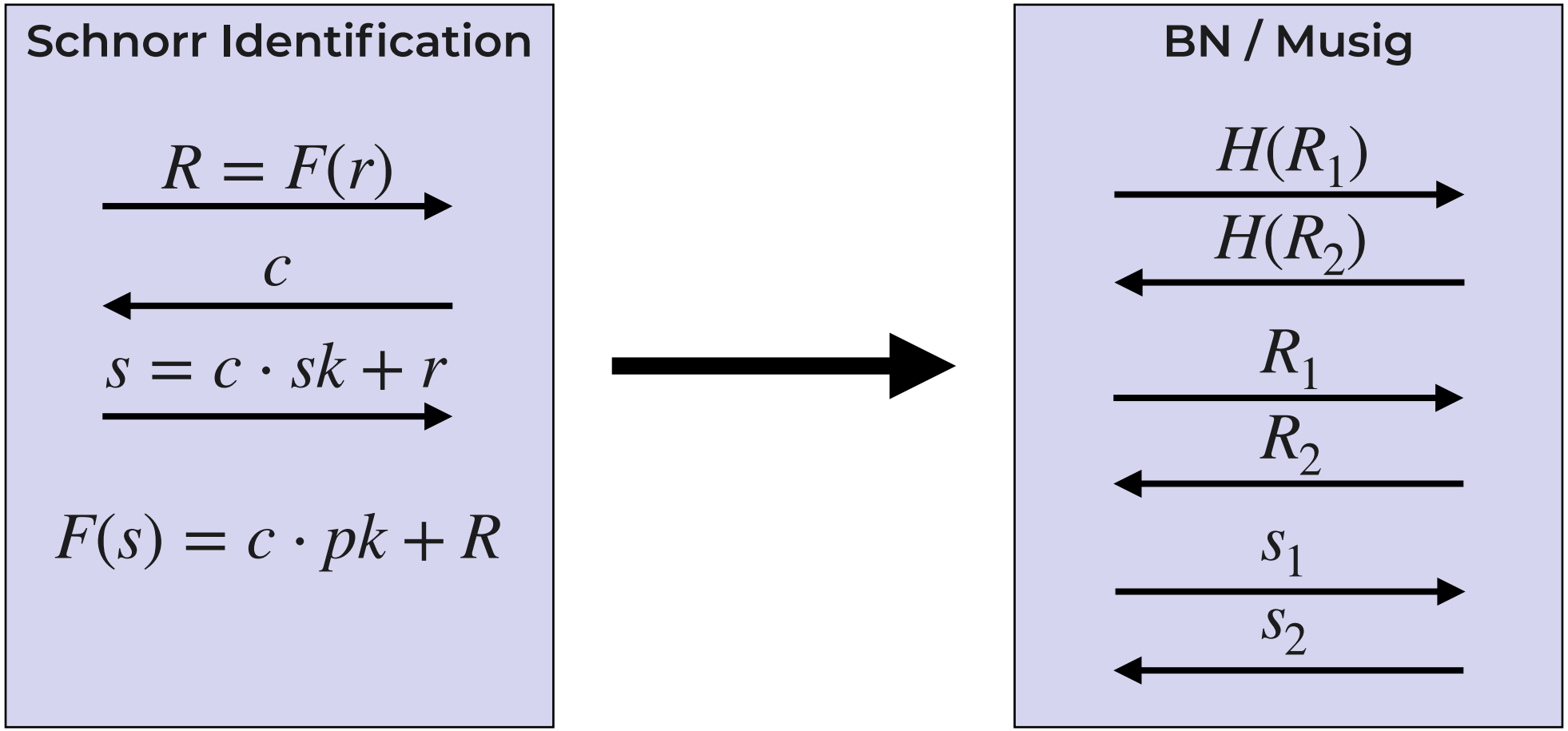
$$\longleftarrow$$

$$s = c \cdot sk + r$$

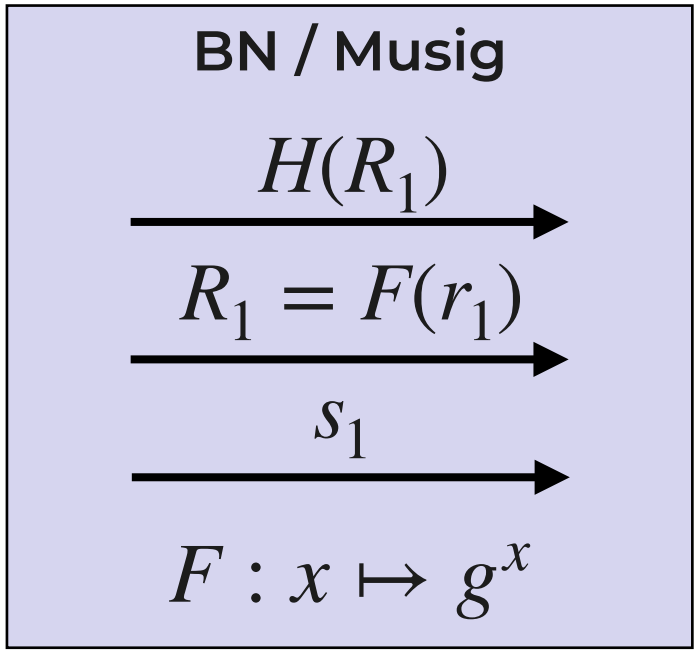
$$\longrightarrow$$

$$F(s) = c \cdot pk + R$$

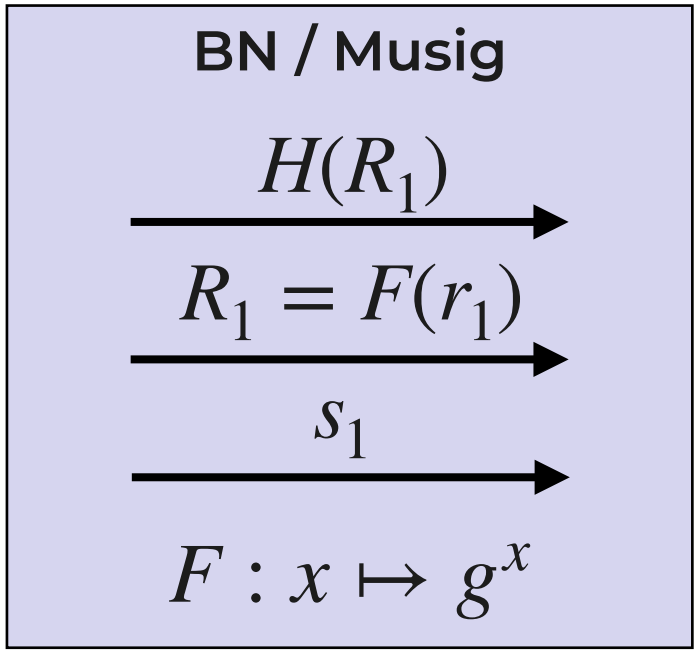
# What we know so Far



# What we know so Far

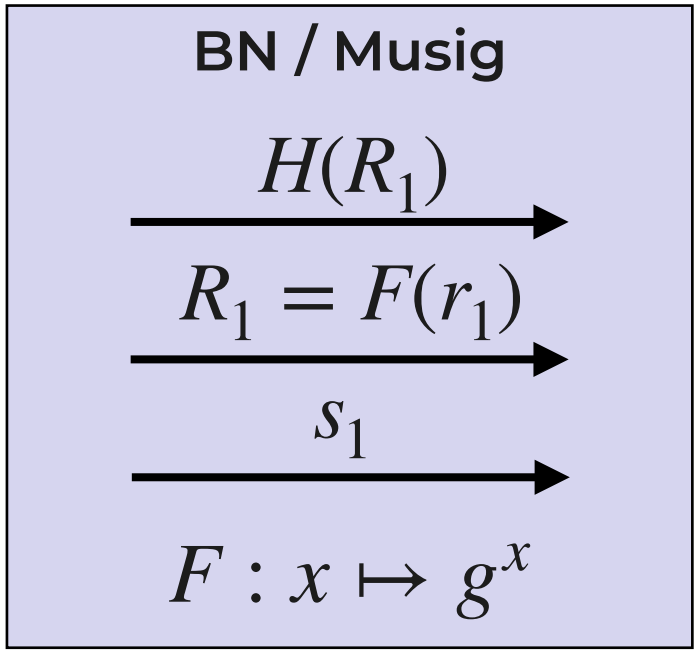


# What we know so Far




**Three Rounds**

# What we know so Far




**Three Rounds**

**Rewinding**

# What we know so Far

**BN / Musig**

$$\xrightarrow{H(R_1)}$$

$$\xrightarrow{R_1 = F(r_1)}$$

$$\xrightarrow{s_1}$$

$$F : x \mapsto g^x$$

Lossy Identification

**BN-Tight/Musig-Tight**

$$F : x \mapsto (g^x, h^x)$$

**Three Rounds**

**Rewinding**

[9] Lossy Identification [Eurocrypt 12, AFLT], DOTT [PKC 21, DOTT]

# What we know so Far

**BN / Musig**

$$\xrightarrow{H(R_1)}$$

$$\xrightarrow{R_1 = F(r_1)}$$

$$\xrightarrow{s_1}$$

$$F : x \mapsto g^x$$

**Three Rounds**

**Rewinding**

Lossy Identification

**BN-Tight/Musig-Tight**

$$F : x \mapsto (g^x, h^x)$$

**Three Rounds**



Lossy Identification [Eurocrypt 12, AFLT], DOTT [PKC 21, DOTT]

# What we know so Far

**BN / Musig**

$$H(R_1)$$

$$R_1 = F(r_1)$$

$$s_1$$

$$F : x \mapsto g^x$$

**Three Rounds**

**Rewinding**

Lossy Identification

Homomorphic
Trapdoor Commitment

**BN-Tight/Musig-Tight**

$$F : x \mapsto (g^x, h^x)$$

**Three Rounds**

**DOTT**

$$\mathrm{com}(R_1)$$

$$s_1,\ \mathrm{open}$$



Lossy Identification [Eurocrypt 12, AFLT], DOTT [PKC 21, DOTT]

# What we know so Far

**BN / Musig**

$$H(R_1)$$

$$R_1 = F(r_1)$$

$$s_1$$

$$F : x \mapsto g^x$$

**Three Rounds**

**Rewinding**

Lossy Identification

Homomorphic
Trapdoor Commitment

**BN-Tight/Musig-Tight**

$$F : x \mapsto (g^x, h^x)$$

**Three Rounds**

**DOTT**

$$\mathrm{com}(R_1)$$

$$s_1,\ \mathrm{open}$$

**Rewinding**



Lossy Identification [Eurocrypt 12, AFLT], DOTT [PKC 21, DOTT]

# The Main Challenges

# The Main Challenges

## Challenge 1

Lossy ID Technique
+
Commitment Trick

# The Main Challenges

## Challenge 1

Lossy ID Technique
+
Commitment Trick

## Challenge 2

Commitment

- From DLOG or DDH
- Homomorphic over $\mathbb{G}^2$
- Equivocation Trapdoor

# The Main Challenges

## Challenge 1

Lossy ID Technique
+
Commitment Trick

## Challenge 2

Commitment

- From DLOG or DDH
- Homomorphic over $\mathbb{G}^2$
- Equivocation Trapdoor

Require Dual-Mode Commitment

# The Main Challenges

## Challenge 1

Lossy ID Technique
+
Commitment Trick

Require Dual-Mode Commitment

## Challenge 2

Commitment

- From DLOG or DDH
- Homomorphic over $\mathbb{G}^2$
- Equivocation Trapdoor

Require **Weak** Trapdoor

# Summary

# Summary and Open Problems

**Multi-Signature**

- 2 Rounds
- DDH Assumption
- $\epsilon \leq Q_S \epsilon'$
- Key Aggregation

**Multi-Signature**

- 2 Rounds
- DDH Assumption
- $\epsilon \leq \epsilon'$

# Summary and Open Problems

**Multi-Signature**

- 2 Rounds
- DDH Assumption
- $\epsilon \leq Q_S \epsilon'$
- Key Aggregation

**Multi-Signature**

- 2 Rounds
- DDH Assumption
- $\epsilon \leq \epsilon'$

Tight and Key Aggregation?

# Summary and Open Problems

**Multi-Signature**

- 2 Rounds
- DDH Assumption
- $\epsilon \leq Q_S \epsilon'$
- Key Aggregation

**Multi-Signature**

- 2 Rounds
- DDH Assumption
- $\epsilon \leq \epsilon'$

Tight and Key Aggregation?

Preprocessing?

# Summary and Open Problems

**Multi-Signature**

- 2 Rounds
- DDH Assumption
- $\epsilon \leq Q_S \epsilon'$
- Key Aggregation

**Multi-Signature**

- 2 Rounds
- DDH Assumption
- $\epsilon \leq \epsilon'$

Tight and Key Aggregation?

Preprocessing?

Other Assumptions? Lattices?