

Gargos: Threshold Schnorr Signature Scheme



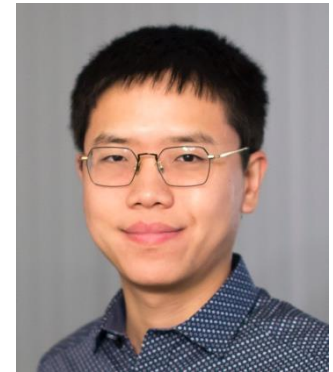
Renas Bacho



Sourav Das



Julian Loss



Ling Ren

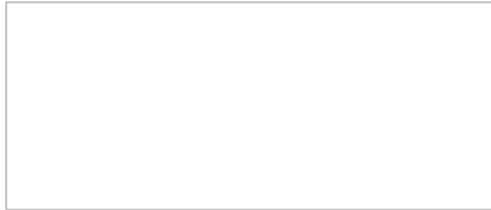


souravdas1547@gmail.com

Schnorr Signatures

Schnorr Signatures

Key Generation



Schnorr Signatures

Key Generation

$$\text{sk} := s \leftarrow \mathbb{Z}_p$$

Schnorr Signatures

Key Generation

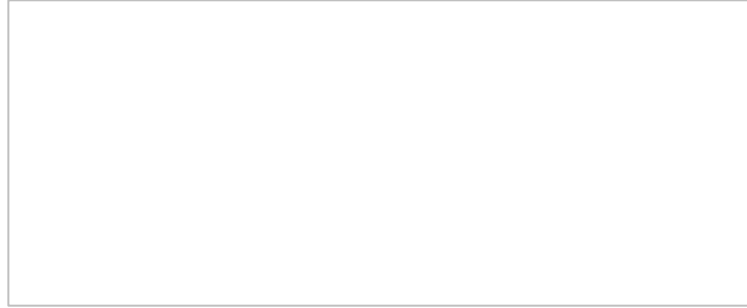
$$\begin{aligned} \text{sk} &:= s \leftarrow \mathbb{Z}_p \\ \text{pk} &:= g^s \end{aligned}$$

Schnorr Signatures

Key Generation

$$\begin{aligned} \text{sk} &:= s \leftarrow \mathbb{Z}_p \\ \text{pk} &:= g^s \end{aligned}$$

Signing



Schnorr Signatures

Key Generation

$$\begin{aligned} \text{sk} &:= s \leftarrow \mathbb{Z}_p \\ \text{pk} &:= g^s \end{aligned}$$

Signing

$$a \leftarrow \mathbb{Z}_p; A := g^a$$

Schnorr Signatures

Key Generation

$$\begin{aligned} \text{sk} &:= s \leftarrow \mathbb{Z}_p \\ \text{pk} &:= g^s \end{aligned}$$

Signing

$$\begin{aligned} a &\leftarrow \mathbb{Z}_p; A := g^a \\ c &:= H_s(A, \text{pk}, m) \end{aligned}$$

Schnorr Signatures

Key Generation

$$\begin{aligned} \text{sk} &:= s \leftarrow \mathbb{Z}_p \\ \text{pk} &:= g^s \end{aligned}$$

Signing

$$\begin{aligned} a &\leftarrow \mathbb{Z}_p; A := g^a \\ c &:= H_s(A, \text{pk}, m) \\ \sigma &:= (A, z = a + c \cdot s) \end{aligned}$$

Schnorr Signatures

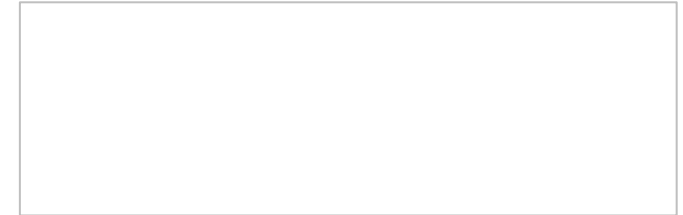
Key Generation

$$\begin{aligned} \text{sk} &:= s \leftarrow \mathbb{Z}_p \\ \text{pk} &:= g^s \end{aligned}$$

Signing

$$\begin{aligned} a &\leftarrow \mathbb{Z}_p; A := g^a \\ c &:= H_s(A, \text{pk}, m) \\ \sigma &:= (A, z = a + c \cdot s) \end{aligned}$$

Verify



Schnorr Signatures

Key Generation

$$\begin{aligned} \text{sk} &:= s \leftarrow \mathbb{Z}_p \\ \text{pk} &:= g^s \end{aligned}$$

Signing

$$\begin{aligned} a &\leftarrow \mathbb{Z}_p; A := g^a \\ c &:= H_s(A, \text{pk}, m) \\ \sigma &:= (A, z = a + c \cdot s) \end{aligned}$$

Verify

$$c' := H_s(A, \text{pk}, m)$$

Schnorr Signatures

Key Generation

$$\begin{aligned} \text{sk} &:= s \leftarrow \mathbb{Z}_p \\ \text{pk} &:= g^s \end{aligned}$$

Signing

$$\begin{aligned} a &\leftarrow \mathbb{Z}_p; A := g^a \\ c &:= H_s(A, \text{pk}, m) \\ \sigma &:= (A, z = a + c \cdot s) \end{aligned}$$

Verify

$$\begin{aligned} c' &:= H_s(A, \text{pk}, m) \\ g^z &= A \cdot \text{pk}^{c'} \end{aligned}$$

Schnorr Signatures

Key Generation

$$\begin{aligned} \text{sk} &:= s \leftarrow \mathbb{Z}_p \\ \text{pk} &:= g^s \end{aligned}$$

Signing

$$\begin{aligned} a &\leftarrow \mathbb{Z}_p; A := g^a \\ c &:= H_s(A, \text{pk}, m) \\ \sigma &:= (A, z = a + c \cdot s) \end{aligned}$$

Verify

$$\begin{aligned} c' &:= H_s(A, \text{pk}, m) \\ g^z &= A \cdot \text{pk}^{c'} \end{aligned}$$

Hardness of discrete logarithm (DL) in the Random Oracle model (ROM)

Schnorr Signatures

Key Generation

$$\begin{aligned} \text{sk} &:= s \leftarrow \mathbb{Z}_p \\ \text{pk} &:= g^s \end{aligned}$$

Signing

$$\begin{aligned} a &\leftarrow \mathbb{Z}_p; A := g^a \\ c &:= H_s(A, \text{pk}, m) \\ \sigma &:= (A, z = a + c \cdot s) \end{aligned}$$

Verify

$$\begin{aligned} c' &:= H_s(A, \text{pk}, m) \\ g^z &= A \cdot \text{pk}^{c'} \end{aligned}$$

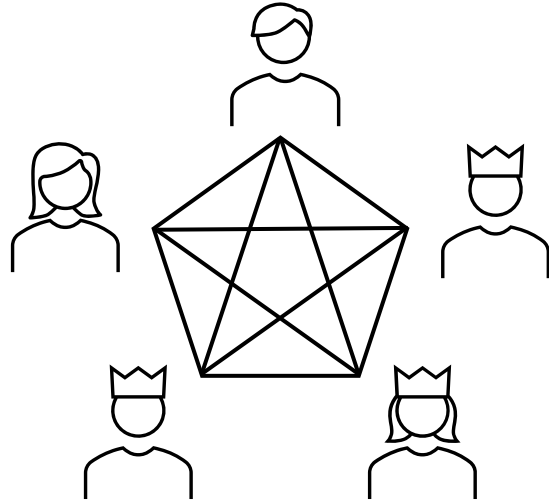
Hardness of discrete logarithm (DL) in the Random Oracle model (ROM)

1. Fast verification
2. Pairing free
3. NIST compatibility
4. Blockchain adoption

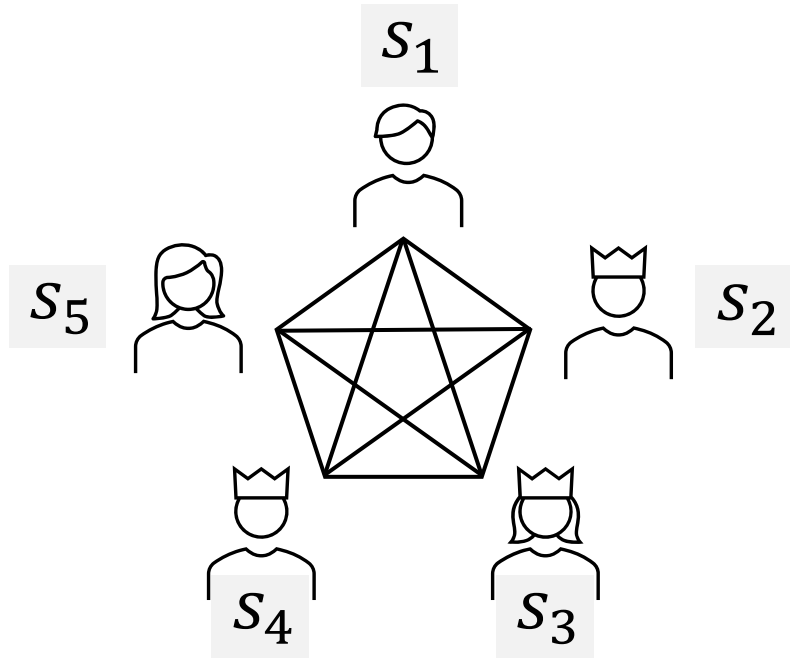


Threshold Schnorr Signatures

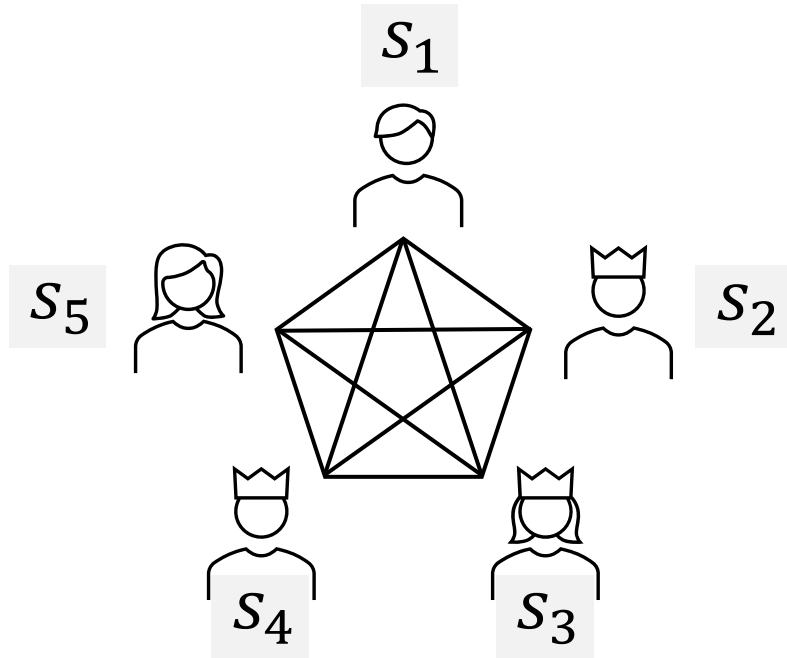
Threshold Schnorr Signatures



Threshold Schnorr Signatures

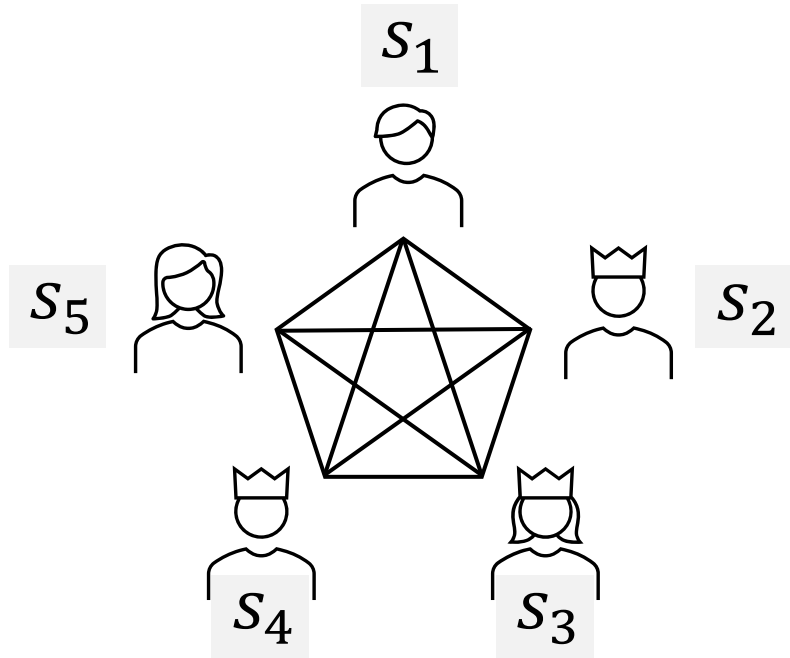


Threshold Schnorr Signatures



$\{s_1, \dots, s_n\} \leftarrow (n, t)$ -
Share(s)

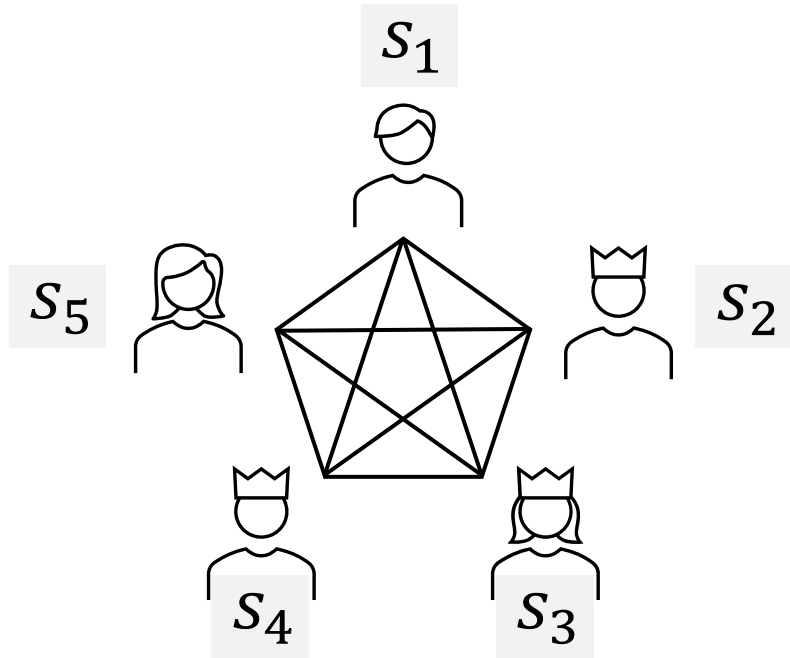
Threshold Schnorr Signatures



$\{s_1, \dots, s_n\} \leftarrow (n, t)$ -
Share(s)

$$\text{pk} := g^s$$

Threshold Schnorr Signatures

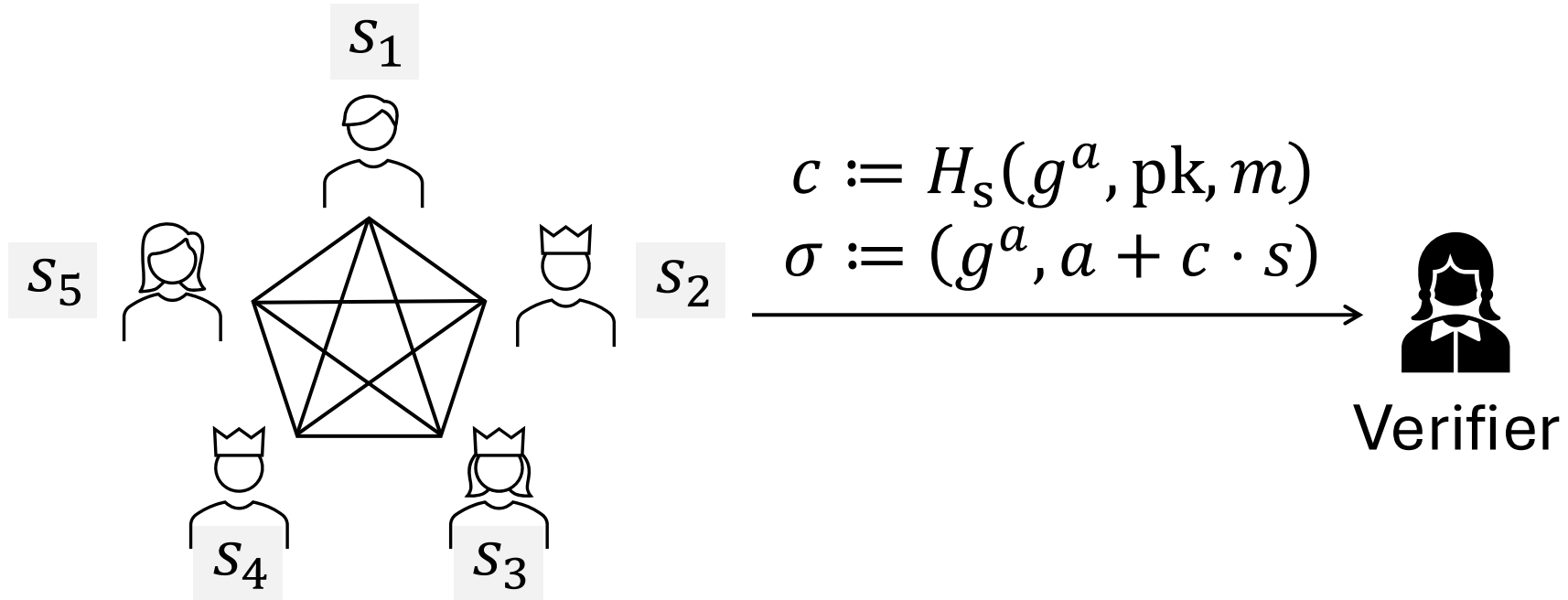


$\{s_1, \dots, s_n\} \leftarrow (n, t)$ -
Share(s)

$$\text{pk} := g^s$$

$$\text{tpk} := \{g^{s_1}, \dots, g^{s_n}\}$$

Threshold Schnorr Signatures

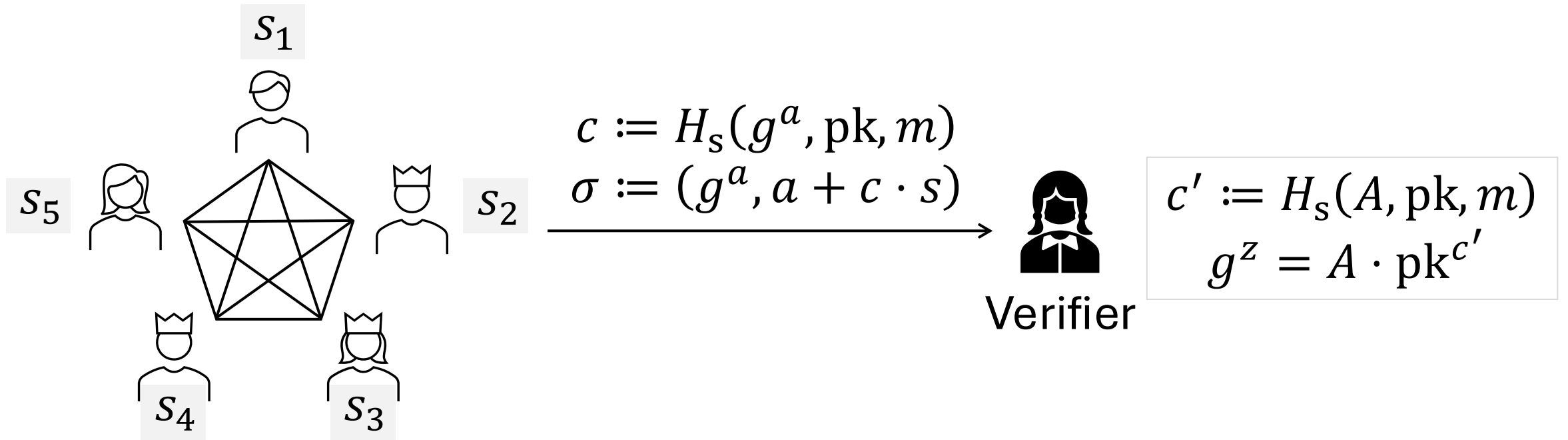


$\{s_1, \dots, s_n\} \leftarrow (n, t)$ -
Share(s)

$$pk := g^s$$

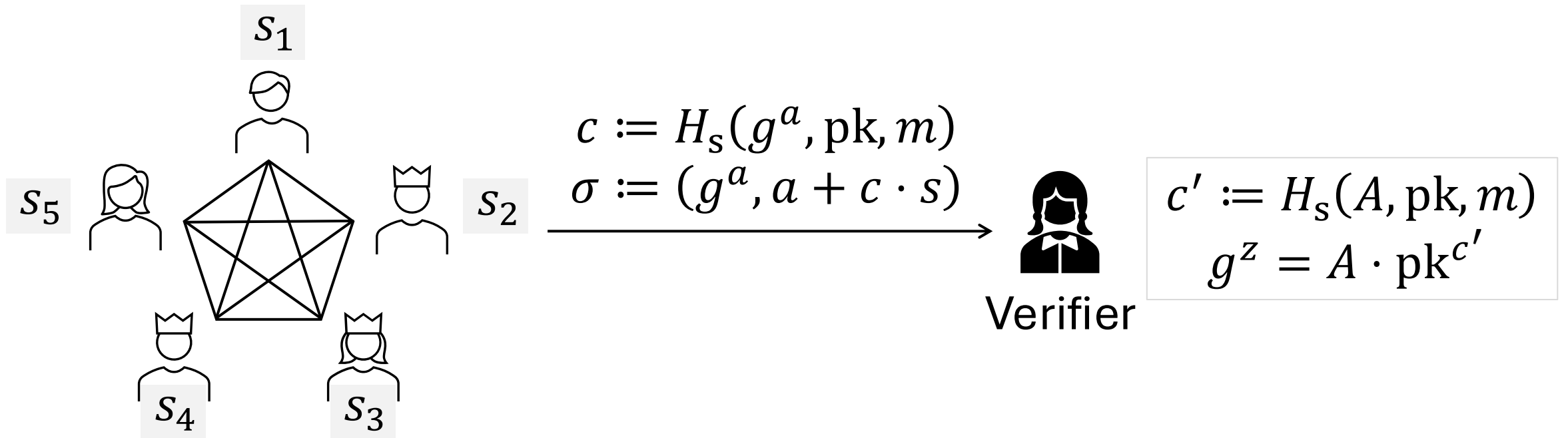
$$tpk := \{g^{s_1}, \dots, g^{s_n}\}$$

Threshold Schnorr Signatures



$$\{s_1, \dots, s_n\} \leftarrow (n, t)\text{-Share}(s)$$
$$pk := g^s$$
$$tpk := \{g^{s_1}, \dots, g^{s_n}\}$$

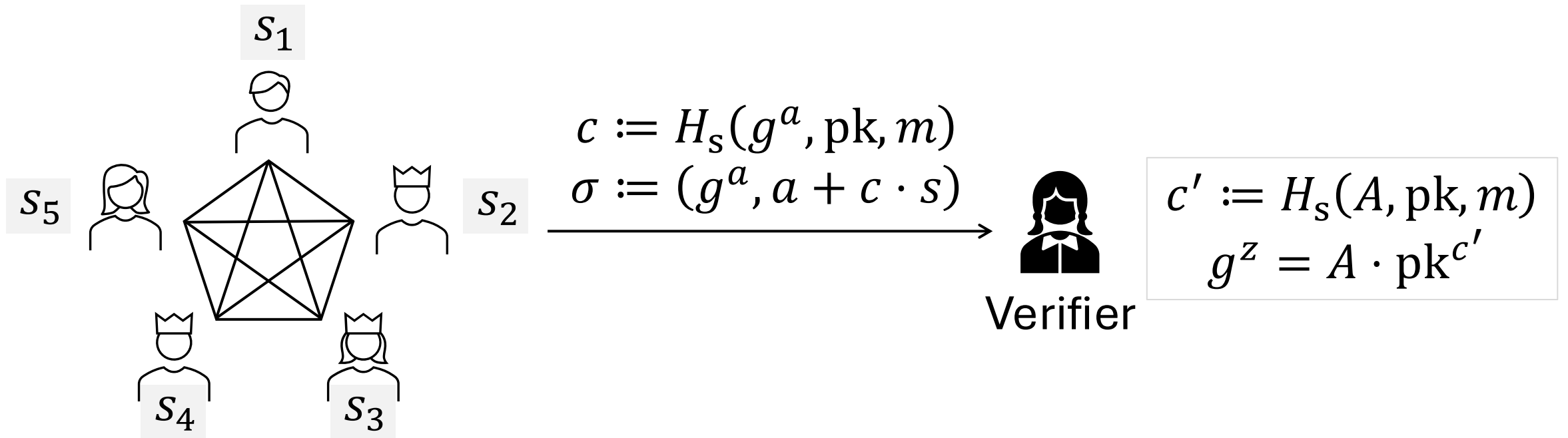
Threshold Schnorr Signatures



$$\{s_1, \dots, s_n\} \leftarrow (n, t)\text{-Share}(s)$$
$$pk := g^s$$
$$tpk := \{g^{s_1}, \dots, g^{s_n}\}$$

Unforgeable with $< t$ corruptions

Threshold Schnorr Signatures



$\{s_1, \dots, s_n\} \leftarrow (n, t)$ -
Share(s)

$$pk := g^s$$

$$tpk := \{g^{s_1}, \dots, g^{s_n}\}$$

Unforgeable with $< t$ corruptions

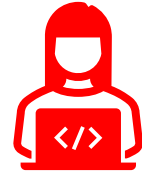
How to formalize this security?

Security of Threshold Signature (UF-CMA game)

Security of Threshold Signature (UF-CMA game)

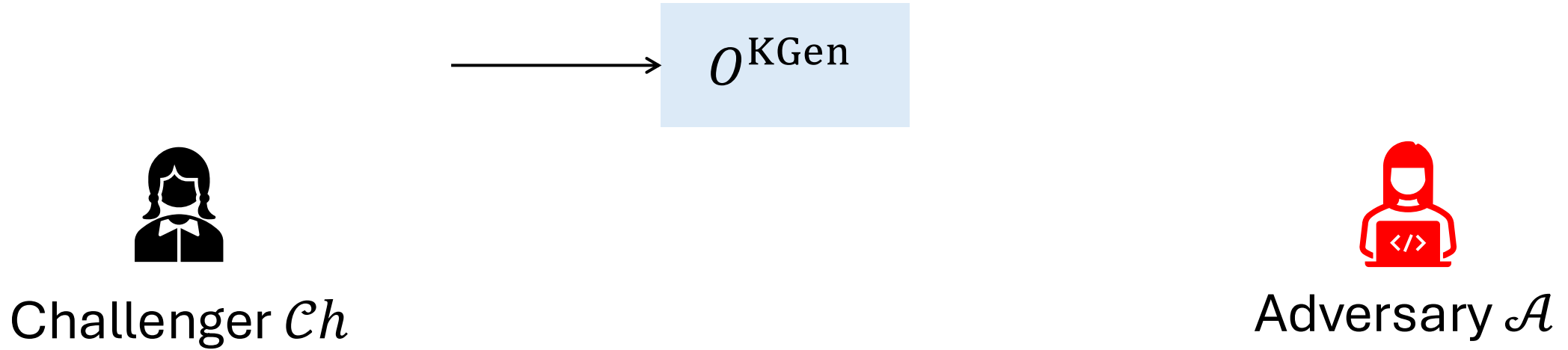


Challenger \mathcal{C}_h

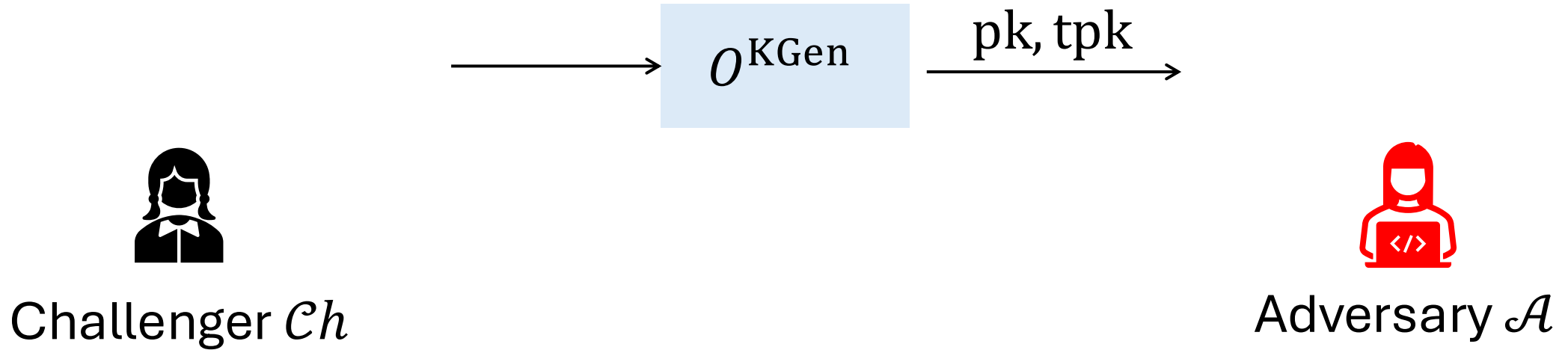


Adversary \mathcal{A}

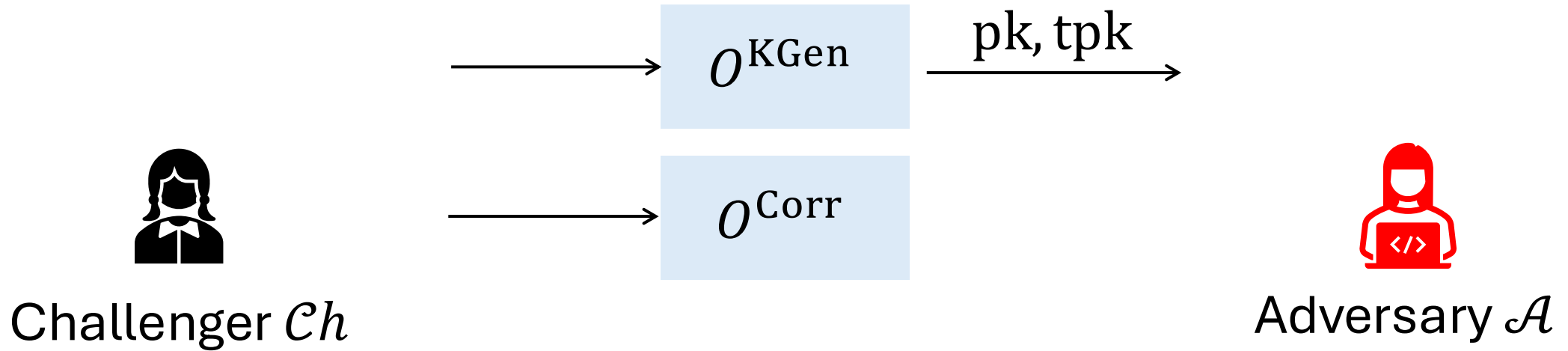
Security of Threshold Signature (UF-CMA game)



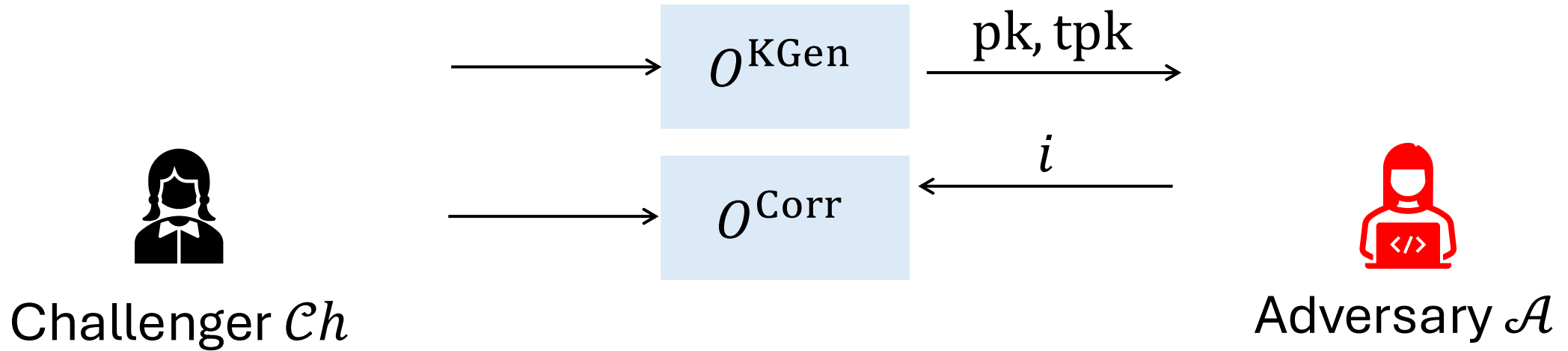
Security of Threshold Signature (UF-CMA game)



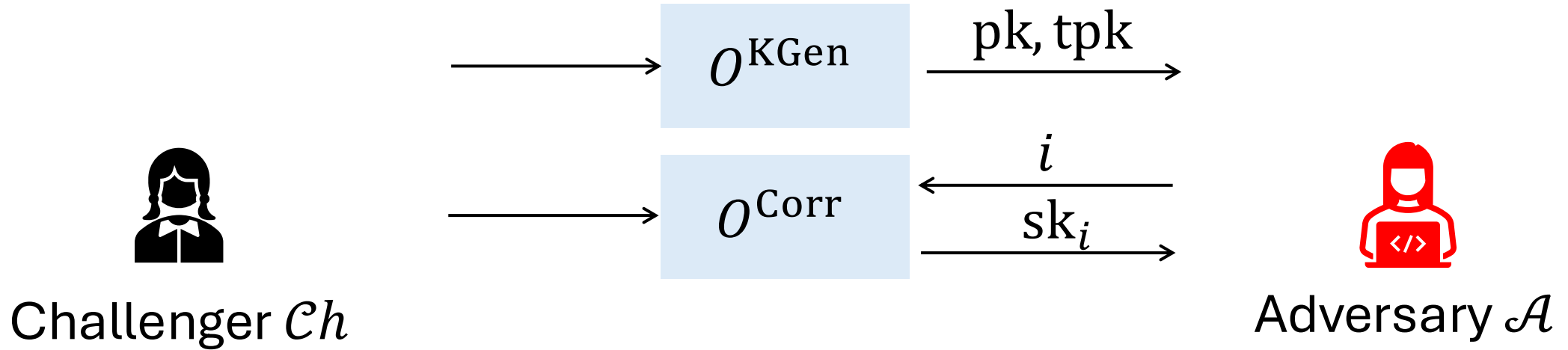
Security of Threshold Signature (UF-CMA game)



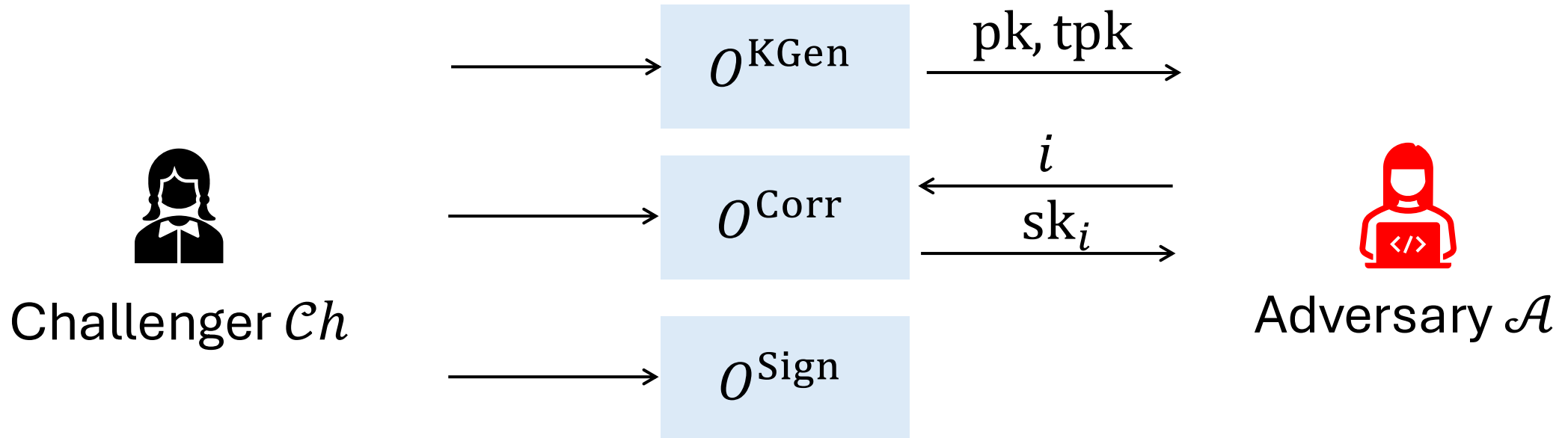
Security of Threshold Signature (UF-CMA game)



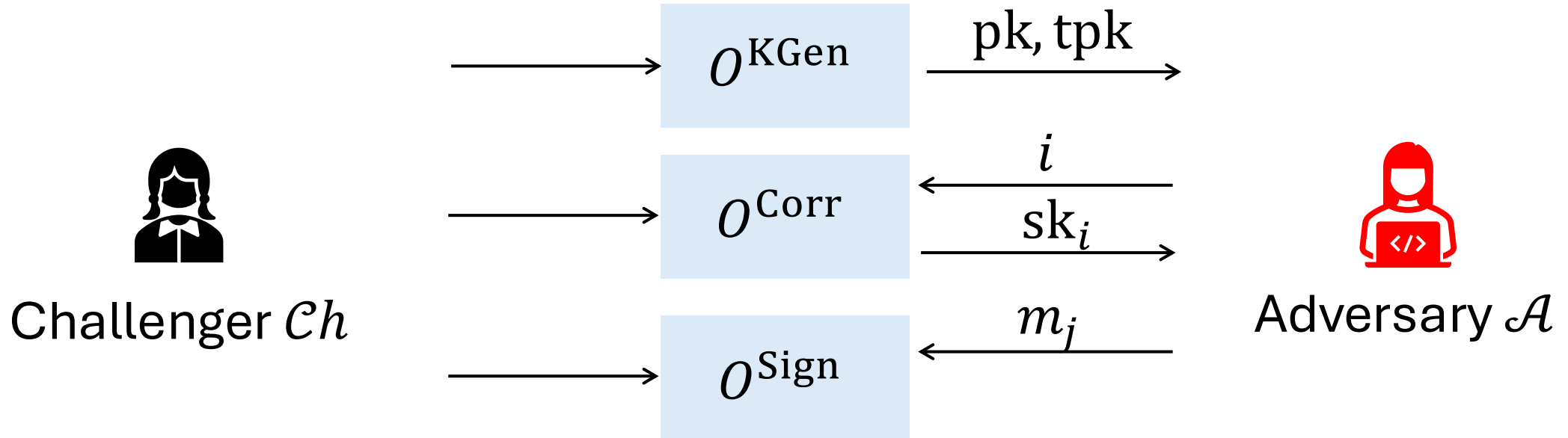
Security of Threshold Signature (UF-CMA game)



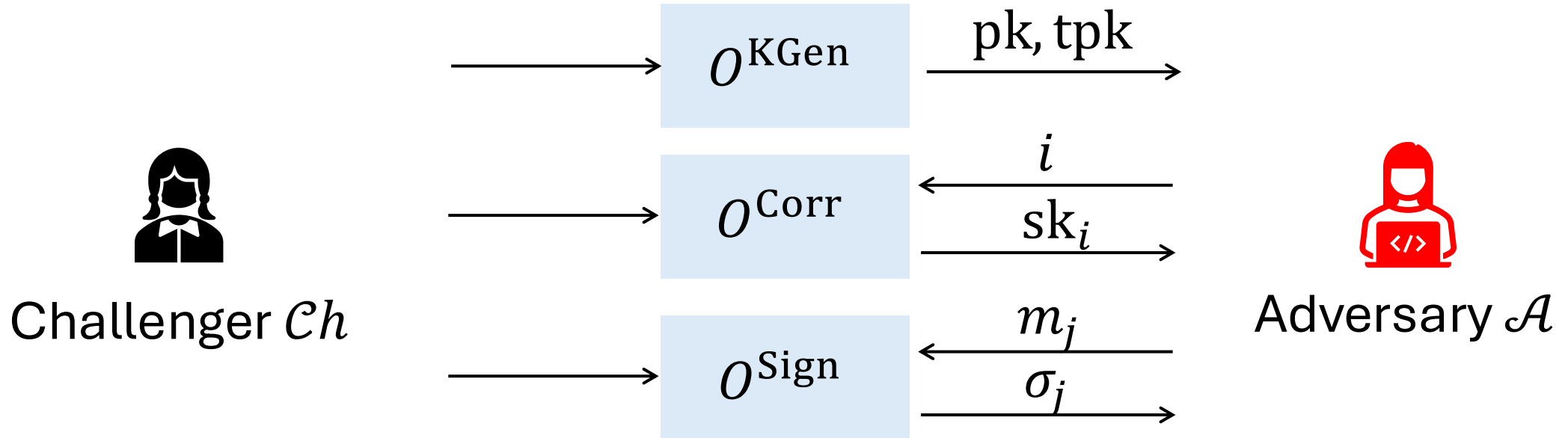
Security of Threshold Signature (UF-CMA game)



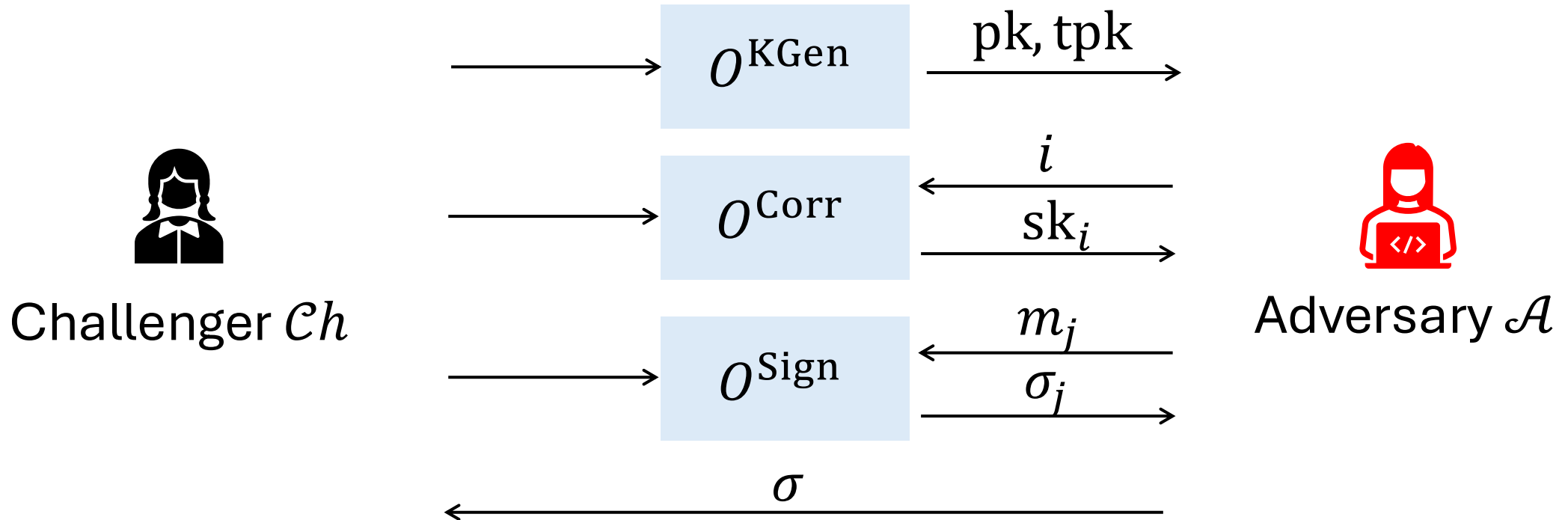
Security of Threshold Signature (UF-CMA game)



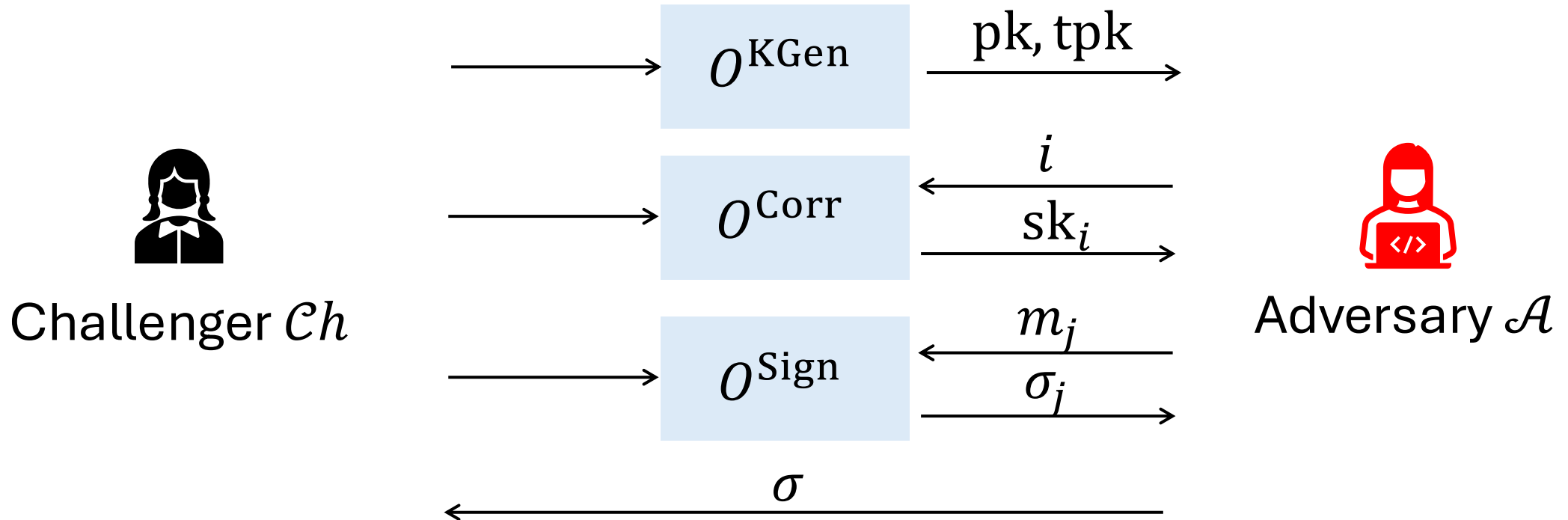
Security of Threshold Signature (UF-CMA game)



Security of Threshold Signature (UF-CMA game)

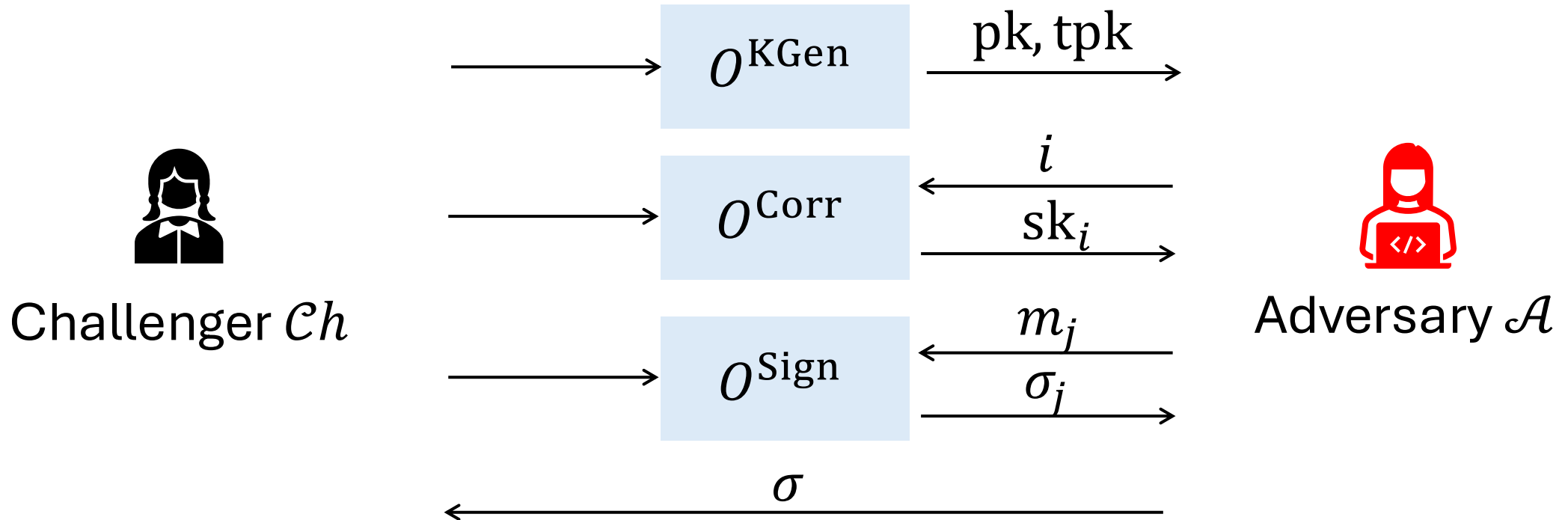


Security of Threshold Signature (UF-CMA game)



\mathcal{A} wins if it **forges** a signature while **invoking O^{Corr} less than t times**

Security of Threshold Signature (UF-CMA game)



\mathcal{A} wins if it **forges** a signature while **invoking O^{Corr} less than t times**

Corruption **timing** is critical!

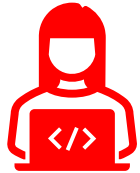
Static vs Adaptive Security

Static vs Adaptive Security



Static \mathcal{A}

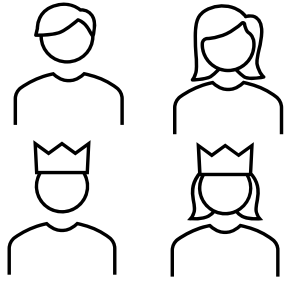
Static vs Adaptive Security



Static \mathcal{A}

Decide corrupt parties
before the protocol

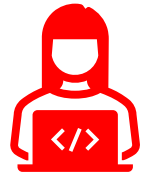
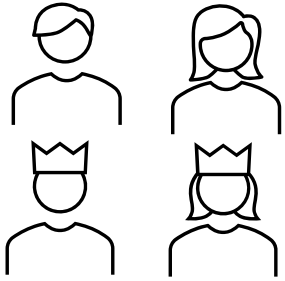
Static vs Adaptive Security



Static \mathcal{A}

Decide corrupt parties
before the protocol

Static vs Adaptive Security

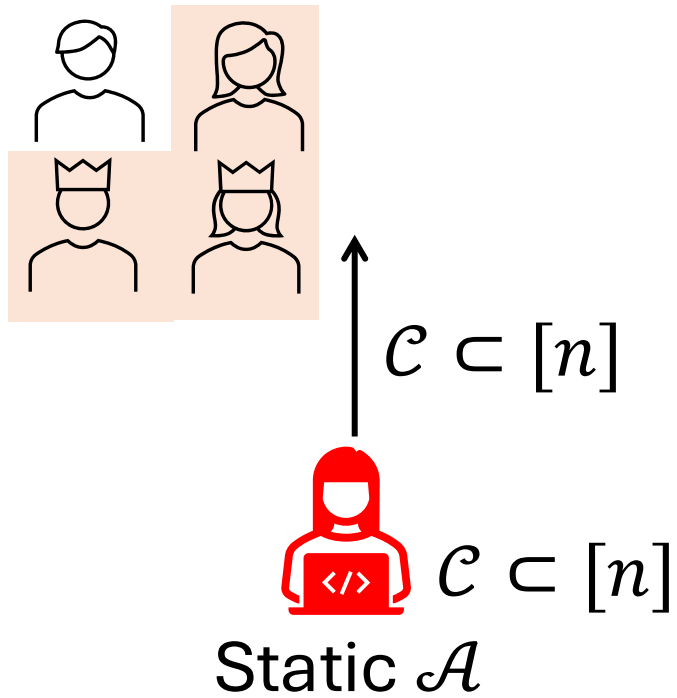


$\mathcal{C} \subset [n]$

Static \mathcal{A}

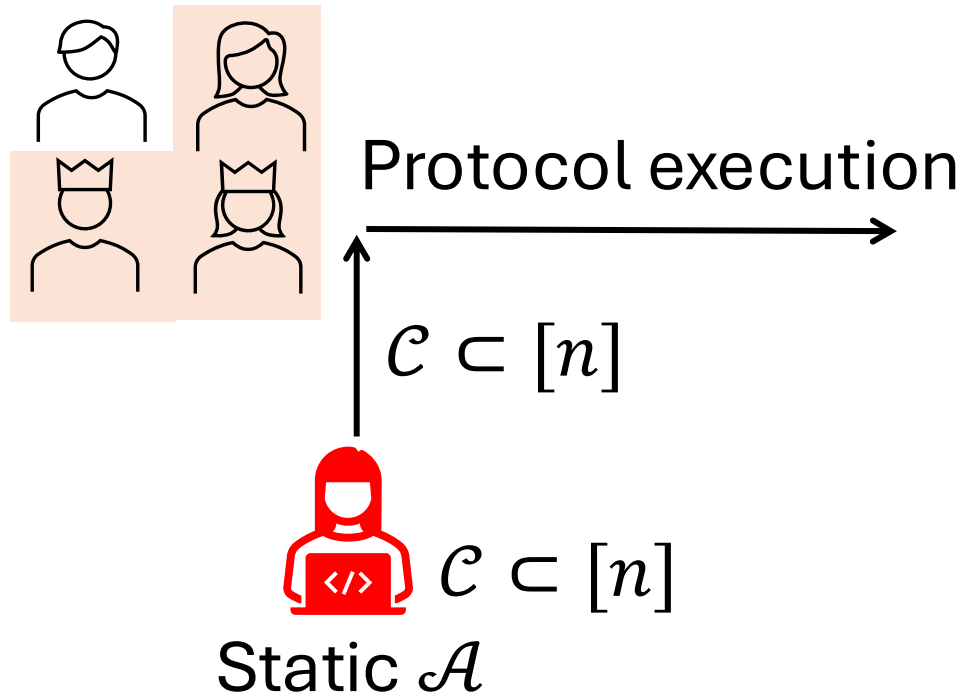
Decide corrupt parties
before the protocol

Static vs Adaptive Security



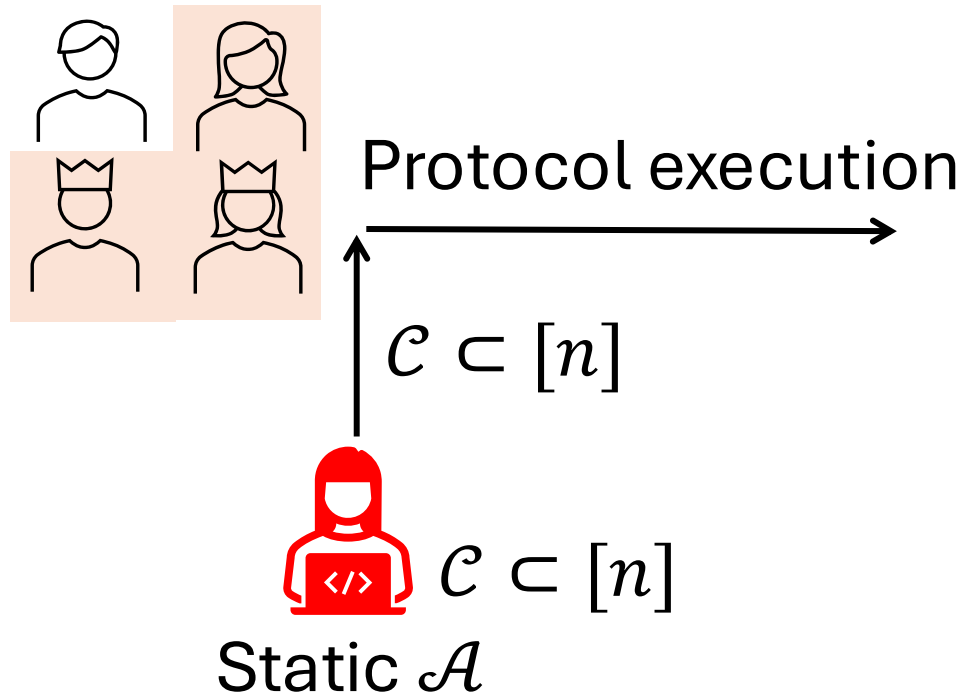
Decide corrupt parties
before the protocol

Static vs Adaptive Security



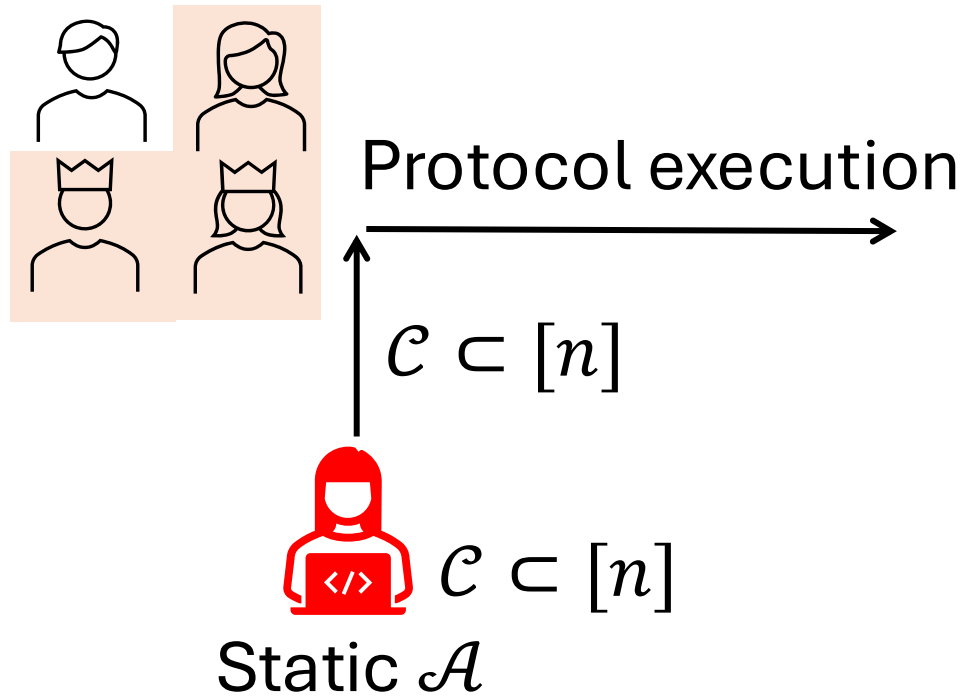
Decide corrupt parties
before the protocol

Static vs Adaptive Security



Decide corrupt parties
before the protocol

Static vs Adaptive Security



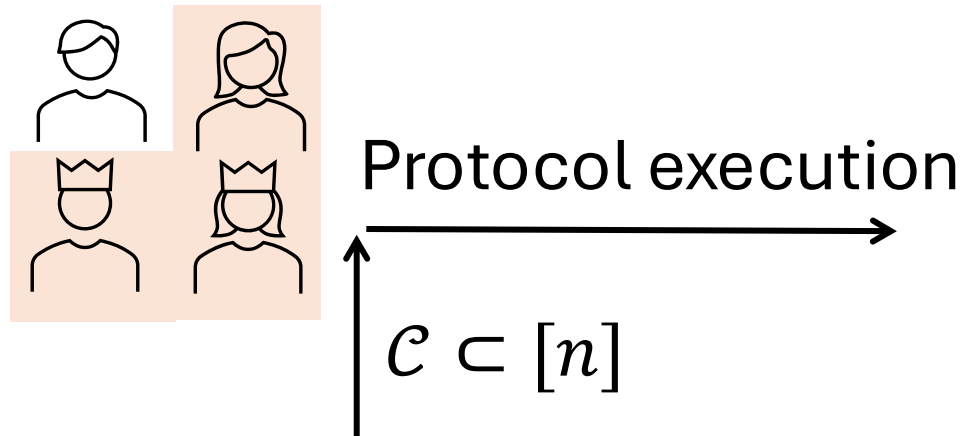
Decide corrupt parties
before the protocol



Adaptive \mathcal{A}

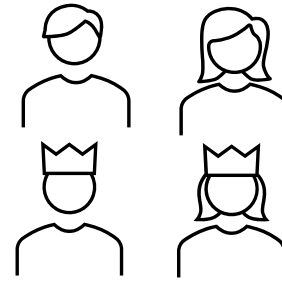
No timing restriction on
corruption decision

Static vs Adaptive Security



Static \mathcal{A}

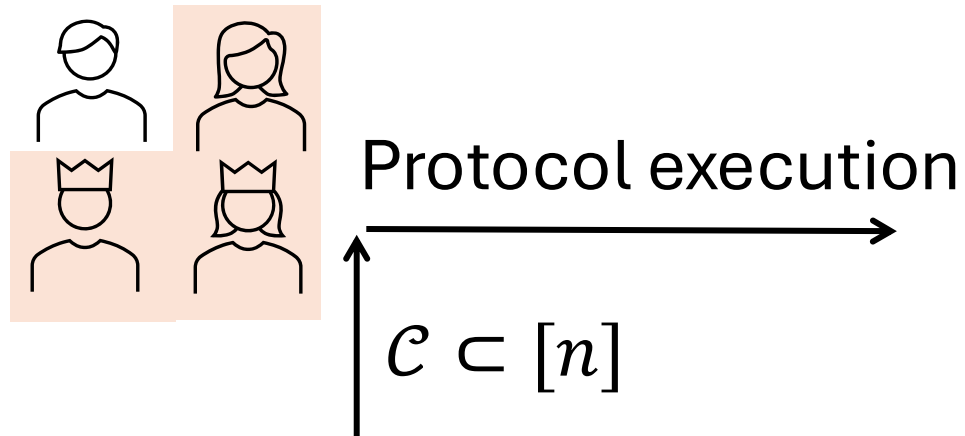
Decide corrupt parties
before the protocol



Adaptive \mathcal{A}

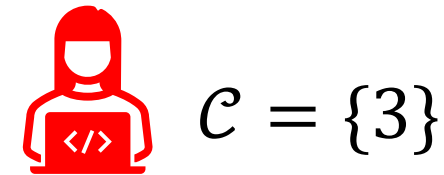
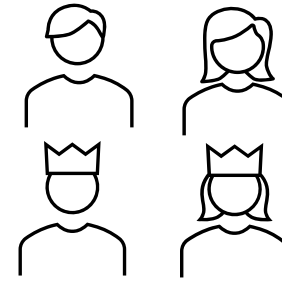
No timing restriction on
corruption decision

Static vs Adaptive Security



Static \mathcal{A}

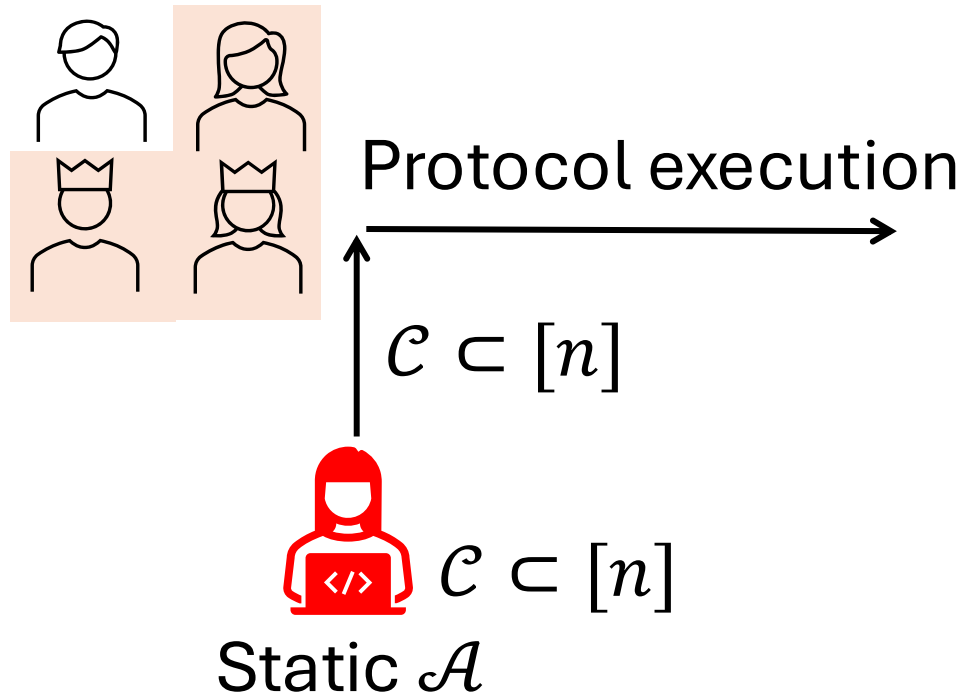
Decide corrupt parties
before the protocol



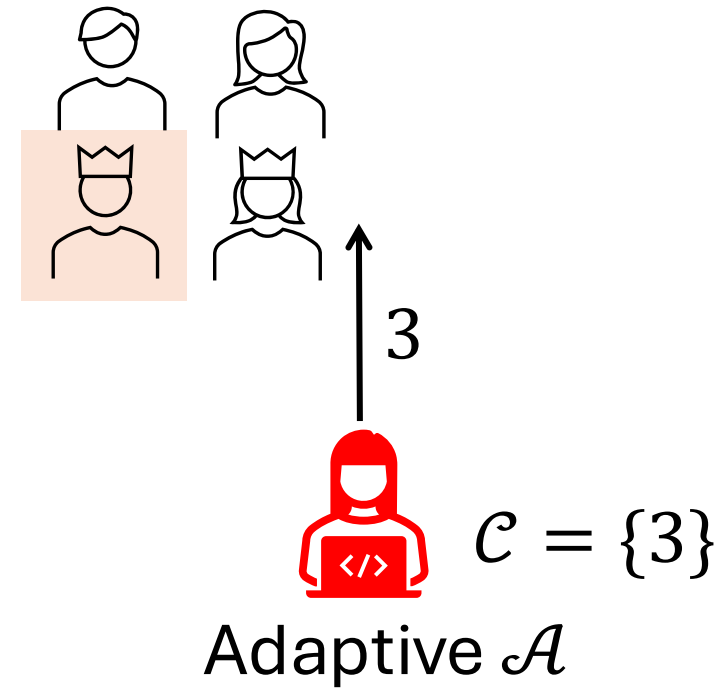
Adaptive \mathcal{A}

No timing restriction on
corruption decision

Static vs Adaptive Security

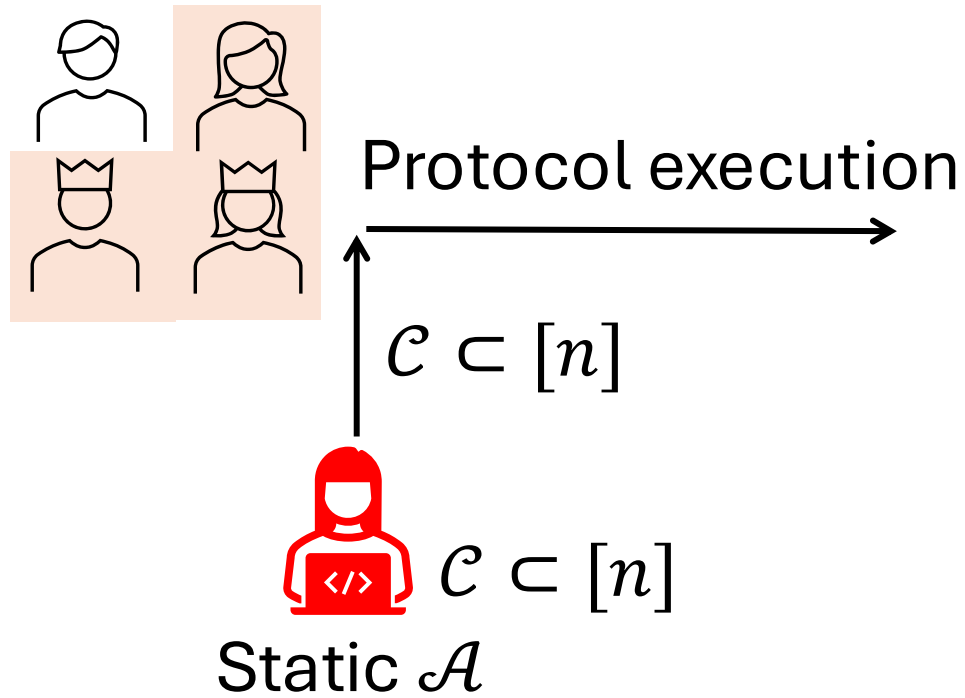


Decide corrupt parties
before the protocol

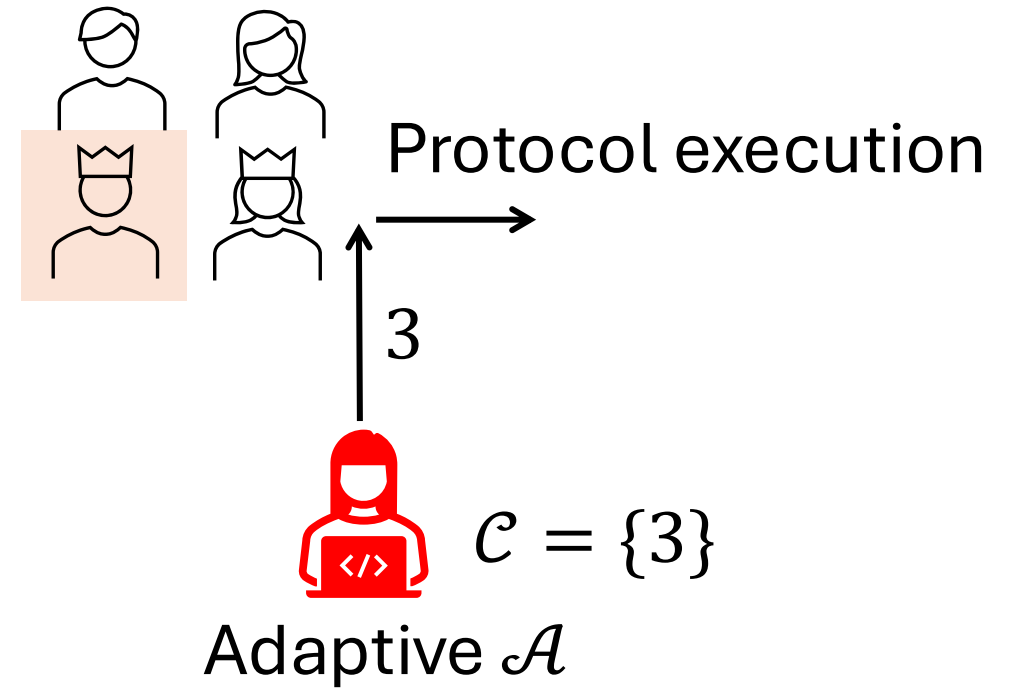


No timing restriction on
corruption decision

Static vs Adaptive Security

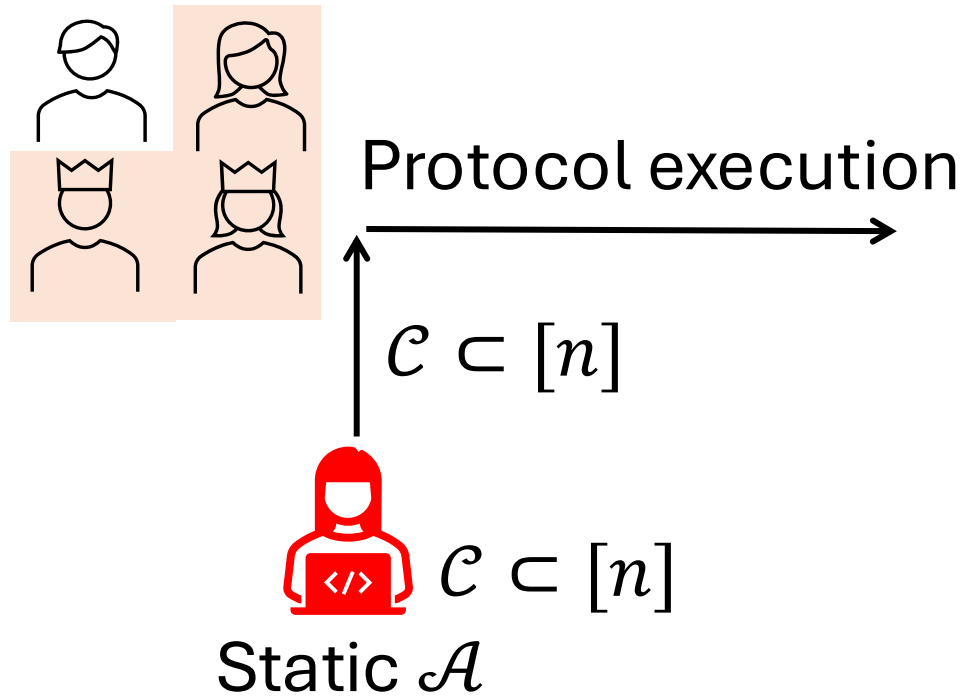


Decide corrupt parties
before the protocol

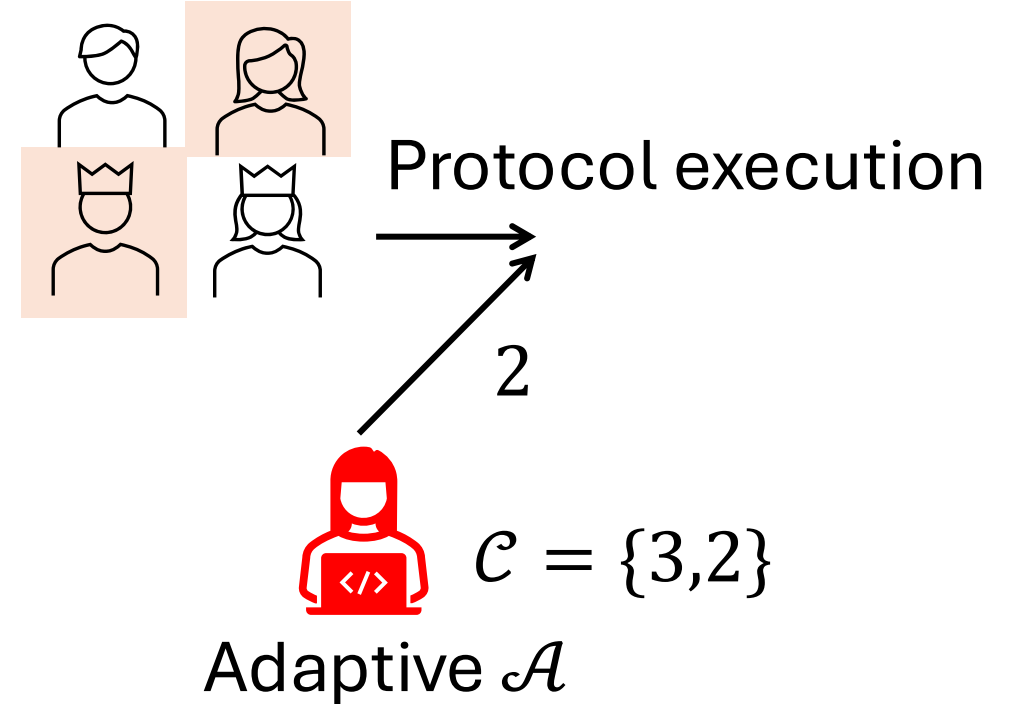


No timing restriction on
corruption decision

Static vs Adaptive Security

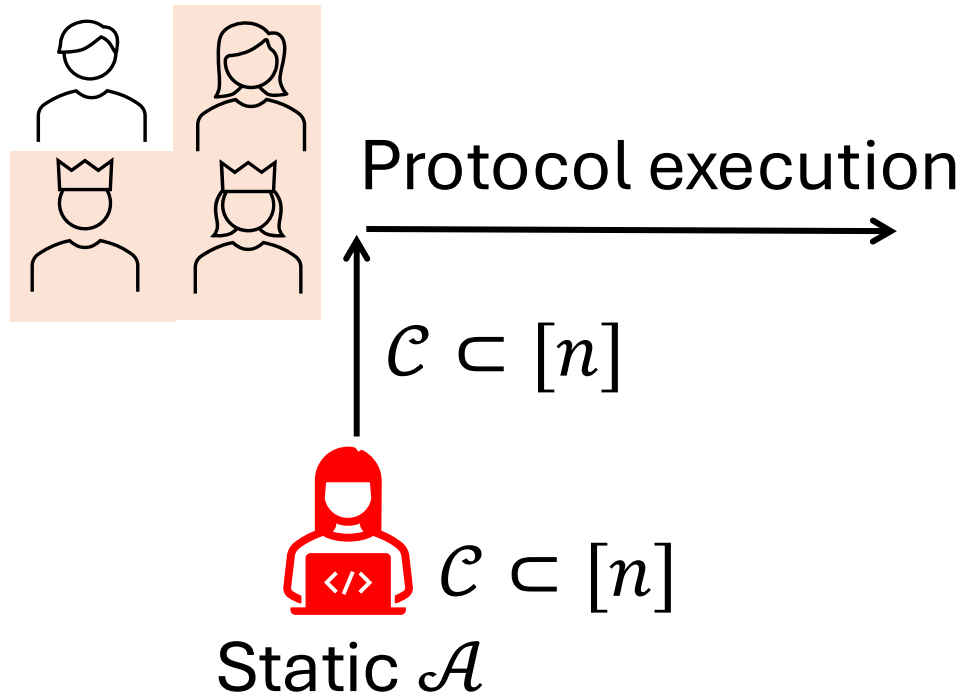


Decide corrupt parties
before the protocol

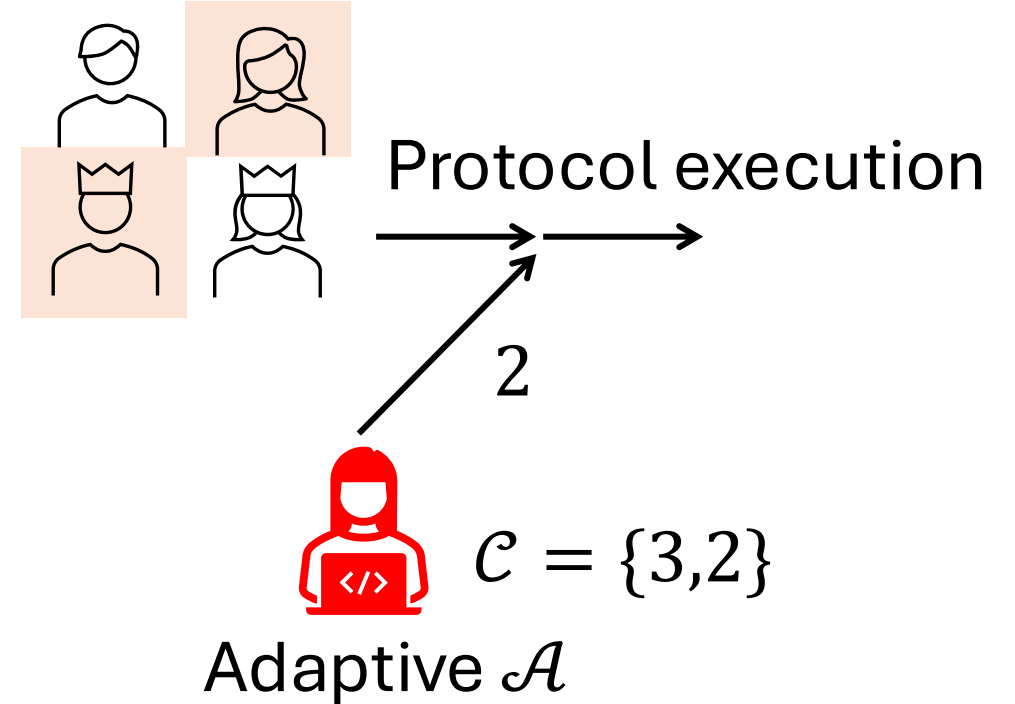


No timing restriction on
corruption decision

Static vs Adaptive Security

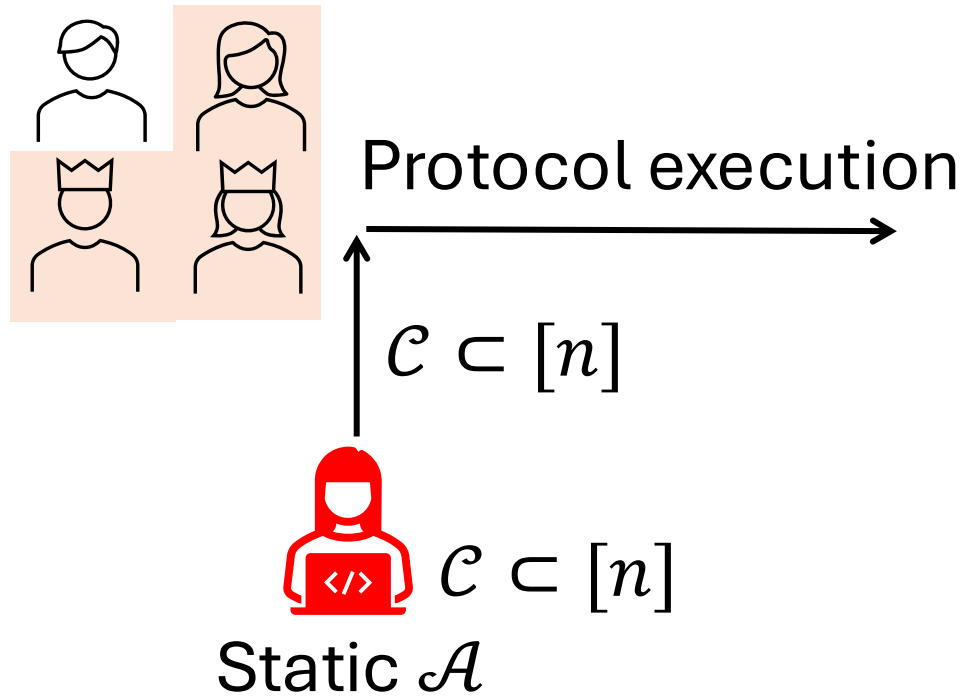


Decide corrupt parties
before the protocol

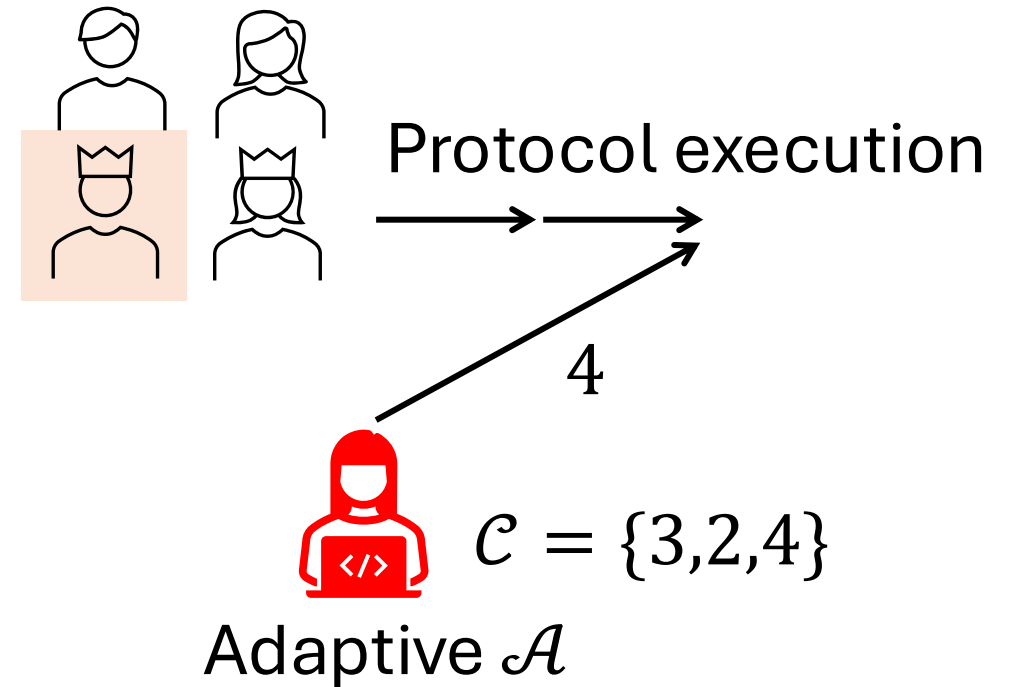


No timing restriction on
corruption decision

Static vs Adaptive Security

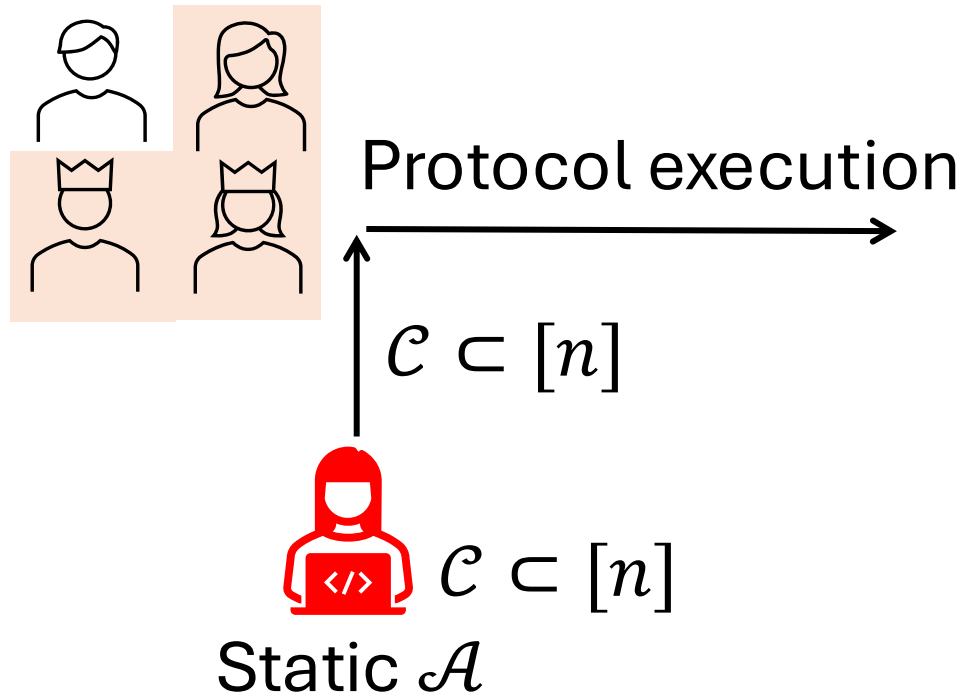


Decide corrupt parties
before the protocol

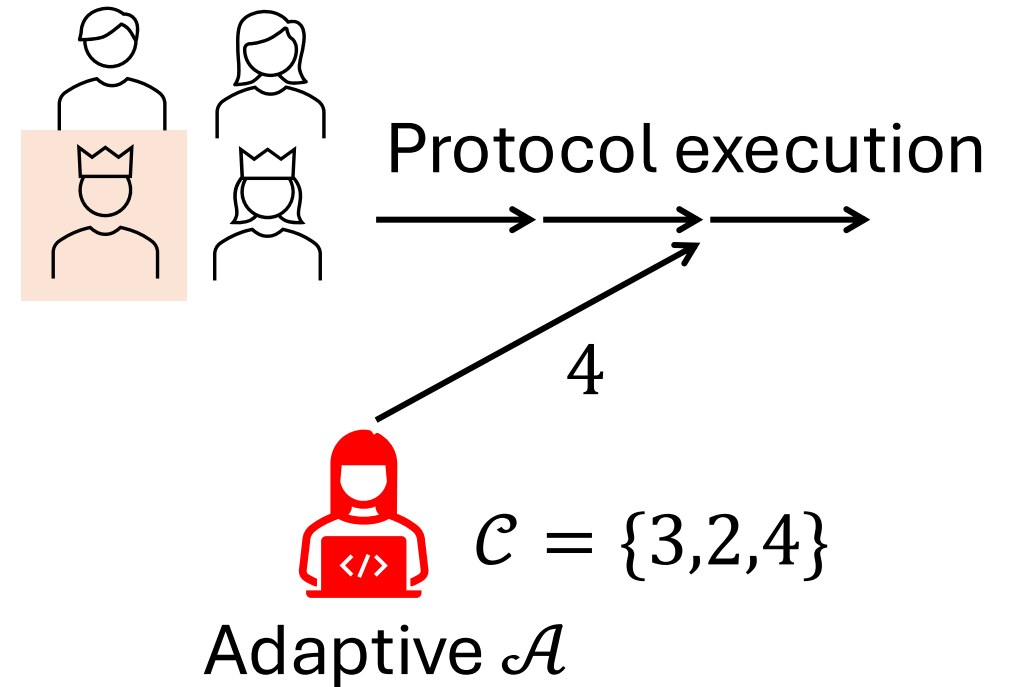


No timing restriction on
corruption decision

Static vs Adaptive Security

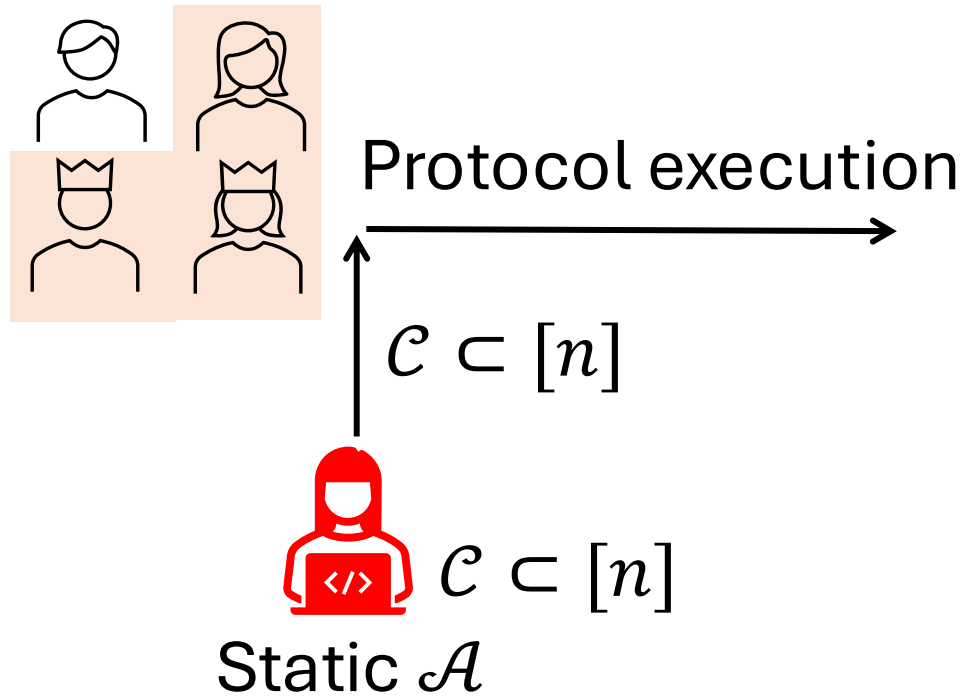


Decide corrupt parties
before the protocol

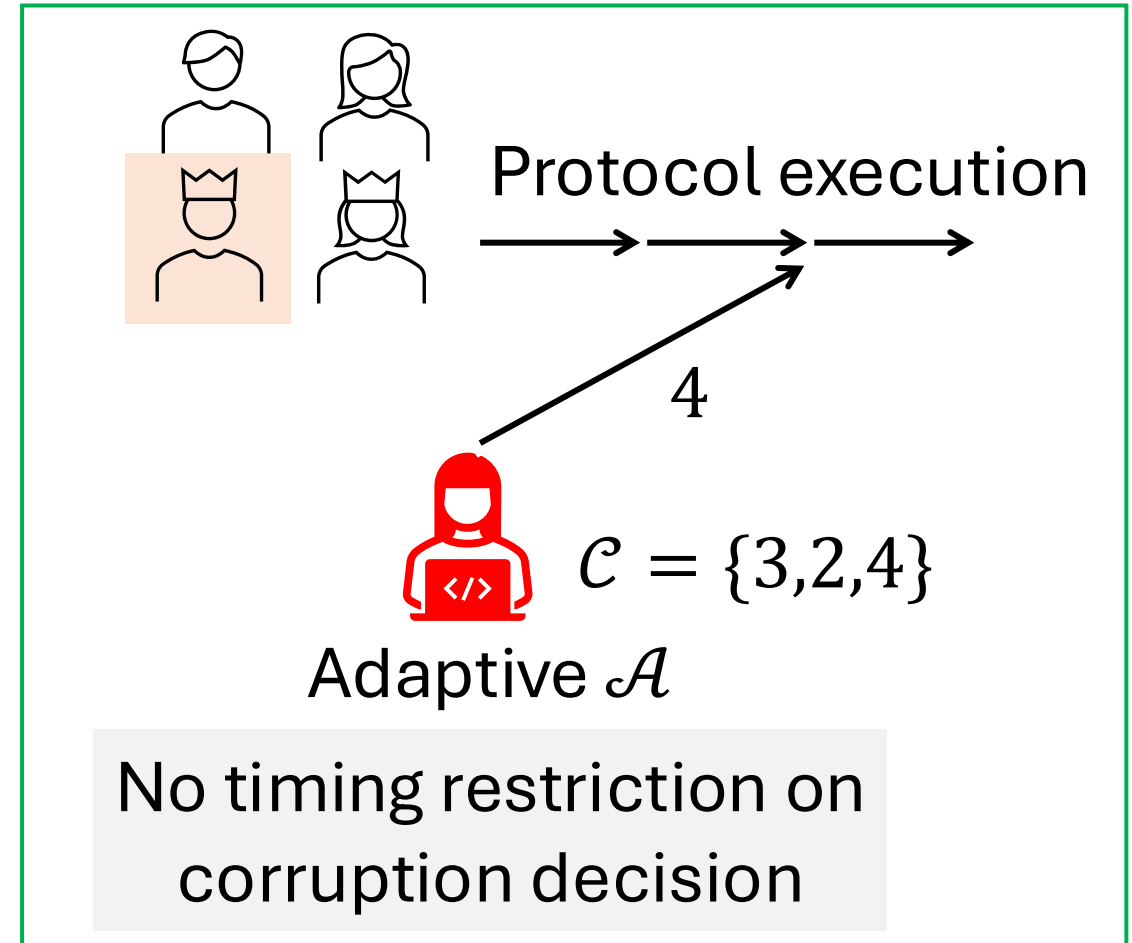


No timing restriction on
corruption decision

Static vs Adaptive Security

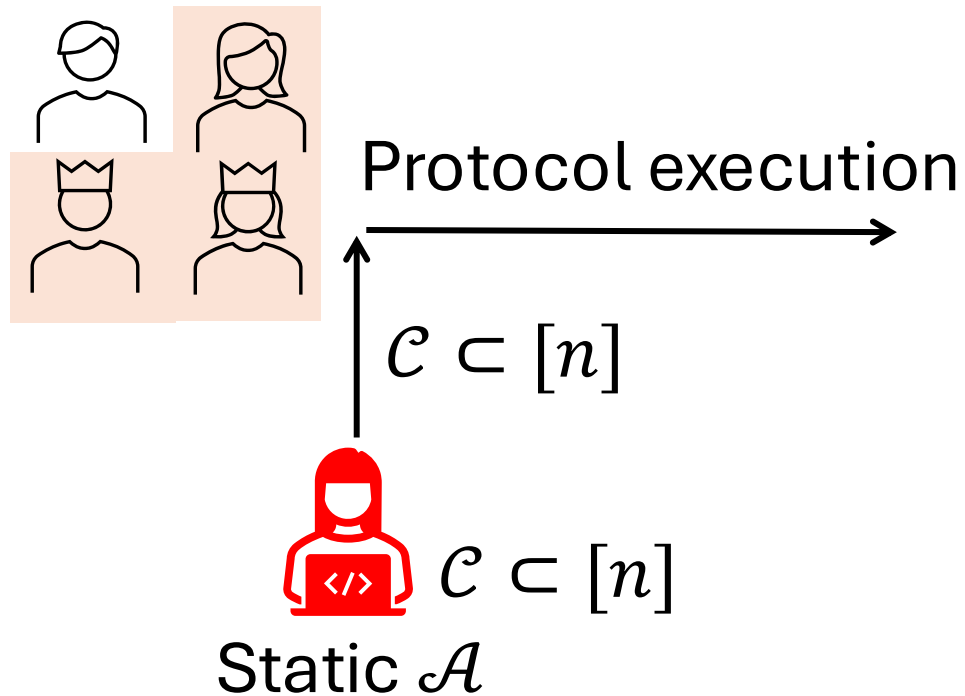


Decide corrupt parties
before the protocol

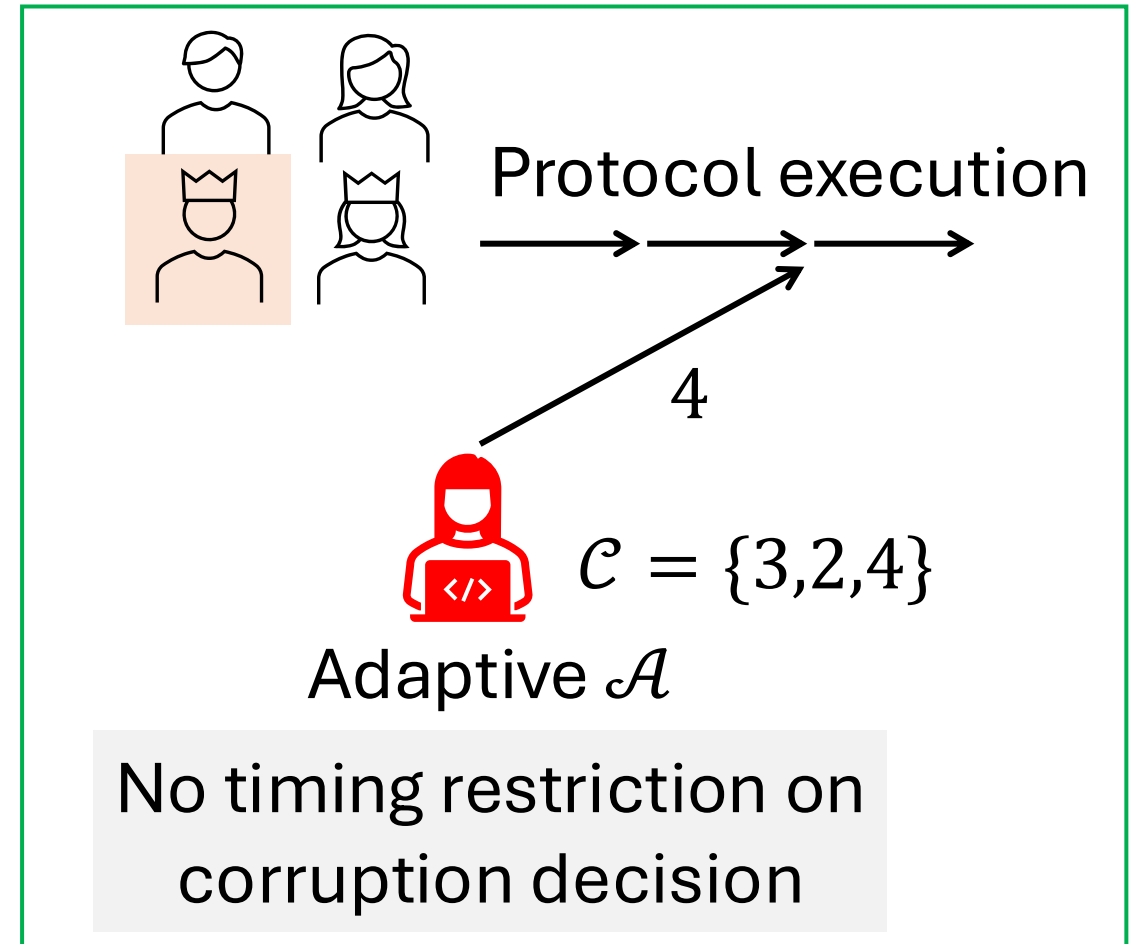


No timing restriction on
corruption decision

Static vs Adaptive Security



Decide corrupt parties
before the protocol



No timing restriction on
corruption decision

Adaptively secure threshold Schnorr signatures from DDH!

Existing Adaptively Secure Schnorr (standard assumptions)

Existing Adaptively Secure Schnorr (standard assumptions)

Scheme	Rounds	Signing key size	Identifiable Abort?	Model + Assumptions
ZeroS [#] [Mak22]	3	1	✓	ROM + DL
KRT [KRT24]	5	$n + 1$	✗	ROM + DL
Glacius [BDLR25]	5	3	✓	ROM + DDH

[#] ZeroS assumes secure channels and secure **erasures**

Existing Adaptively Secure Schnorr (standard assumptions)

Scheme	Rounds	Signing key size	Identifiable Abort?	Model + Assumptions
ZeroS [#] [Mak22]	3	1	✓	ROM + DL
KRT [KRT24]	5	$n + 1$	✗	ROM + DL
Glacius [BDLR25]	5	3	✓	ROM + DDH

[#] ZeroS assumes secure channels and secure **erasures**

Sparkle [CKM23]	3	1	✓	ROM + DL
-----------------	---	---	---	----------

Statically secure

Existing Adaptively Secure Schnorr (standard assumptions)

Scheme	Rounds	Signing key size	Identifiable Abort?	Model + Assumptions
ZeroS [#] [Mak22]	3	1	✓	ROM + DL
KRT [KRT24]	5	$n + 1$	✗	ROM + DL
Glacius [BDLR25]	5	3	✓	ROM + DDH
This work	3	3	✓	ROM + DDH

[#] ZeroS assumes secure channels and secure **erasures**

Sparkle [CKM23]	3	1	✓	ROM + DL
-----------------	---	---	---	----------

Statically secure

Existing threshold Schnorr Design

Standard Threshold Schnorr [BN06, ...]

Standard Threshold Schnorr [BN06, ...]



Standard Threshold Schnorr [BN06, ...]

$$\begin{aligned} a_1 &\leftarrow \mathbb{Z}_p \\ A_1 &:= g^{a_1} \\ \mu_1 &:= H_{\text{com}}(A_1) \end{aligned}$$



Standard Threshold Schnorr [BN06, ...]

$$\begin{aligned} a_1 &\leftarrow \mathbb{Z}_p \\ A_1 &:= g^{a_1} \\ \mu_1 &:= H_{\text{com}}(A_1) \end{aligned}$$

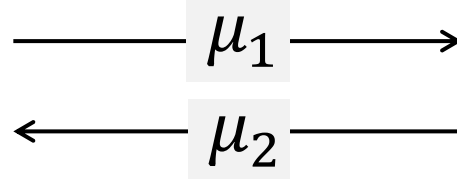


$$\begin{aligned} a_2 &\leftarrow \mathbb{Z}_p \\ A_2 &:= g^{a_2} \\ \mu_2 &:= H_{\text{com}}(A_2) \end{aligned}$$



Standard Threshold Schnorr [BN06, ...]

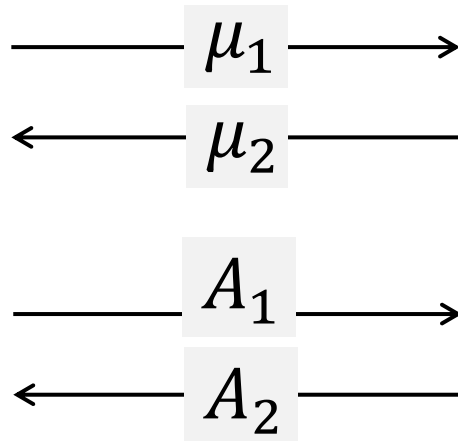
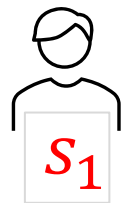
$$\begin{aligned} a_1 &\leftarrow \mathbb{Z}_p \\ A_1 &:= g^{a_1} \\ \mu_1 &:= H_{\text{com}}(A_1) \end{aligned}$$



$$\begin{aligned} a_2 &\leftarrow \mathbb{Z}_p \\ A_2 &:= g^{a_2} \\ \mu_2 &:= H_{\text{com}}(A_2) \end{aligned}$$

Standard Threshold Schnorr [BN06, ...]

$$\begin{aligned} a_1 &\leftarrow \mathbb{Z}_p \\ A_1 &:= g^{a_1} \\ \mu_1 &:= H_{\text{com}}(A_1) \end{aligned}$$



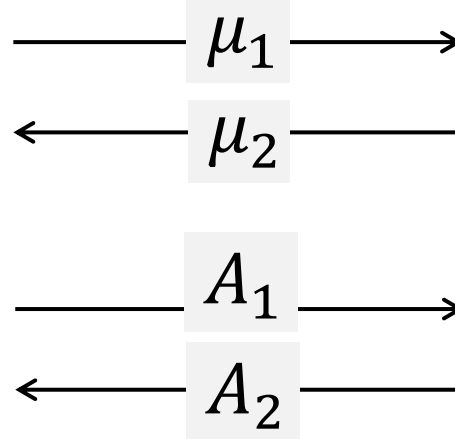
$$\begin{aligned} a_2 &\leftarrow \mathbb{Z}_p \\ A_2 &:= g^{a_2} \\ \mu_2 &:= H_{\text{com}}(A_2) \end{aligned}$$



Standard Threshold Schnorr [BN06, ...]

$$\begin{aligned} a_1 &\leftarrow \mathbb{Z}_p \\ A_1 &:= g^{a_1} \\ \mu_1 &:= H_{\text{com}}(A_1) \end{aligned}$$

$$\begin{aligned} A &:= A_1 \cdot A_2 \\ c &:= H_{\text{sig}}(A, pk, m) \end{aligned}$$



$$\begin{aligned} a_2 &\leftarrow \mathbb{Z}_p \\ A_2 &:= g^{a_2} \\ \mu_2 &:= H_{\text{com}}(A_2) \end{aligned}$$

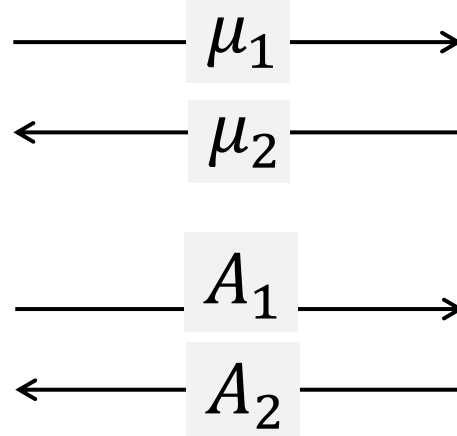
$$\begin{aligned} A &:= A_1 \cdot A_2 \\ c &:= H_{\text{sig}}(A, pk, m) \end{aligned}$$

Standard Threshold Schnorr [BN06, ...]

$$\begin{aligned} a_1 &\leftarrow \mathbb{Z}_p \\ A_1 &:= g^{a_1} \\ \mu_1 &:= H_{\text{com}}(A_1) \end{aligned}$$

$$\begin{aligned} A &:= A_1 \cdot A_2 \\ c &:= H_{\text{sig}}(A, pk, m) \end{aligned}$$

$$z_1 := a_1 + c \cdot s_1$$



$$\begin{aligned} a_2 &\leftarrow \mathbb{Z}_p \\ A_2 &:= g^{a_2} \\ \mu_2 &:= H_{\text{com}}(A_2) \end{aligned}$$

$$\begin{aligned} A &:= A_1 \cdot A_2 \\ c &:= H_{\text{sig}}(A, pk, m) \end{aligned}$$

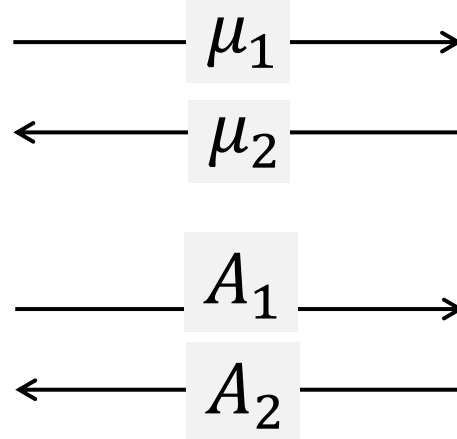


Standard Threshold Schnorr [BN06, ...]

$$\begin{aligned} a_1 &\leftarrow \mathbb{Z}_p \\ A_1 &:= g^{a_1} \\ \mu_1 &:= H_{\text{com}}(A_1) \end{aligned}$$

$$\begin{aligned} A &:= A_1 \cdot A_2 \\ c &:= H_{\text{sig}}(A, pk, m) \end{aligned}$$

$$z_1 := a_1 + c \cdot s_1$$



$$\begin{aligned} a_2 &\leftarrow \mathbb{Z}_p \\ A_2 &:= g^{a_2} \\ \mu_2 &:= H_{\text{com}}(A_2) \end{aligned}$$

$$\begin{aligned} A &:= A_1 \cdot A_2 \\ c &:= H_{\text{sig}}(A, pk, m) \end{aligned}$$

$$z_2 := a_2 + c \cdot s_2$$

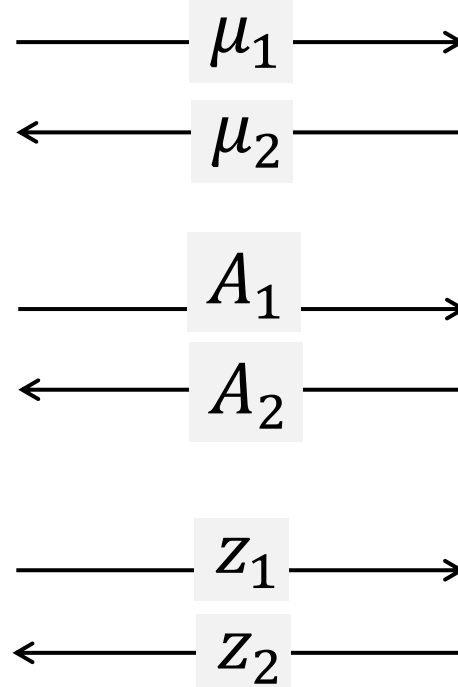


Standard Threshold Schnorr [BN06, ...]

$$\begin{aligned} a_1 &\leftarrow \mathbb{Z}_p \\ A_1 &:= g^{a_1} \\ \mu_1 &:= H_{\text{com}}(A_1) \end{aligned}$$

$$\begin{aligned} A &:= A_1 \cdot A_2 \\ c &:= H_{\text{sig}}(A, pk, m) \end{aligned}$$

$$z_1 := a_1 + c \cdot s_1$$



$$\begin{aligned} a_2 &\leftarrow \mathbb{Z}_p \\ A_2 &:= g^{a_2} \\ \mu_2 &:= H_{\text{com}}(A_2) \end{aligned}$$

$$\begin{aligned} A &:= A_1 \cdot A_2 \\ c &:= H_{\text{sig}}(A, pk, m) \end{aligned}$$

$$z_2 := a_2 + c \cdot s_2$$



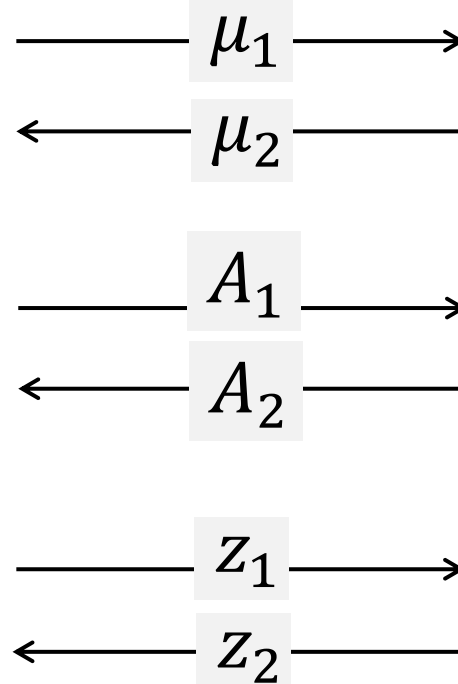
Standard Threshold Schnorr [BN06, ...]

$$\begin{aligned} a_1 &\leftarrow \mathbb{Z}_p \\ A_1 &:= g^{a_1} \\ \mu_1 &:= H_{\text{com}}(A_1) \end{aligned}$$

$$\begin{aligned} A &:= A_1 \cdot A_2 \\ c &:= H_{\text{sig}}(A, pk, m) \end{aligned}$$

$$z_1 := a_1 + c \cdot s_1$$

$$\sigma := (A, z := z_1 + z_2)$$



$$\begin{aligned} a_2 &\leftarrow \mathbb{Z}_p \\ A_2 &:= g^{a_2} \\ \mu_2 &:= H_{\text{com}}(A_2) \end{aligned}$$

$$\begin{aligned} A &:= A_1 \cdot A_2 \\ c &:= H_{\text{sig}}(A, pk, m) \end{aligned}$$

$$z_2 := a_2 + c \cdot s_2$$

$$\sigma := (A, z := z_1 + z_2)$$



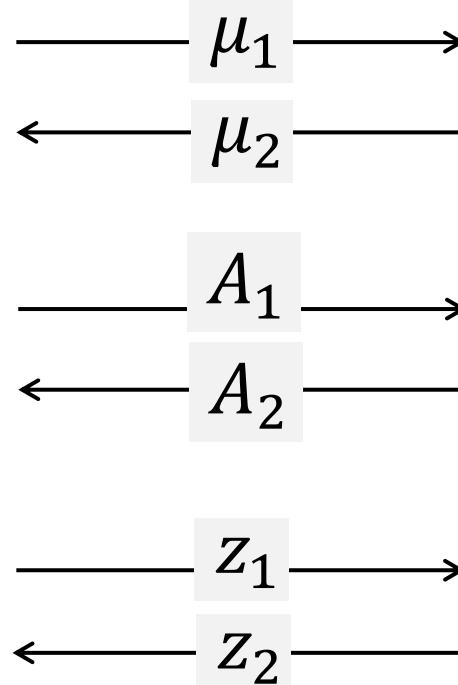
Standard Threshold Schnorr [BN06, ...]

$$\begin{aligned} a_1 &\leftarrow \mathbb{Z}_p \\ A_1 &:= g^{a_1} \\ \mu_1 &:= H_{\text{com}}(A_1) \end{aligned}$$

$$\begin{aligned} A &:= A_1 \cdot A_2 \\ c &:= H_{\text{sig}}(A, pk, m) \end{aligned}$$

$$z_1 := a_1 + c \cdot s_1$$

$$\sigma := (A, z := z_1 + z_2)$$



$$\begin{aligned} a_2 &\leftarrow \mathbb{Z}_p \\ A_2 &:= g^{a_2} \\ \mu_2 &:= H_{\text{com}}(A_2) \end{aligned}$$

$$\begin{aligned} A &:= A_1 \cdot A_2 \\ c &:= H_{\text{sig}}(A, pk, m) \end{aligned}$$

$$z_2 := a_2 + c \cdot s_2$$

$$\sigma := (A, z := z_1 + z_2)$$



$$g^z = A \cdot pk^c$$

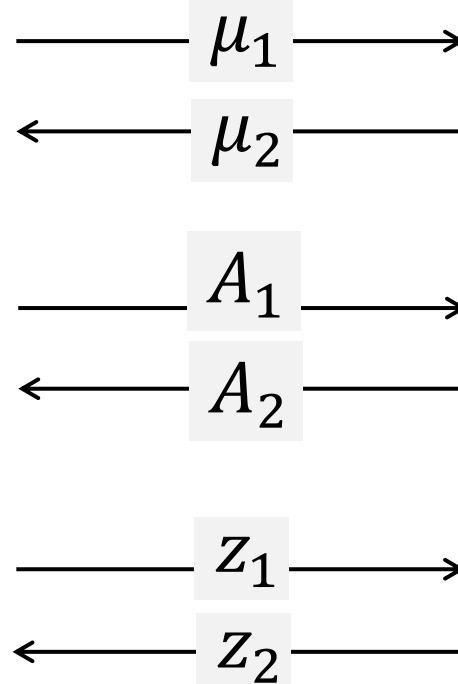
Standard Threshold Schnorr [BN06, ...]

$$\begin{aligned} a_1 &\leftarrow \mathbb{Z}_p \\ A_1 &:= g^{a_1} \\ \mu_1 &:= H_{\text{com}}(A_1) \end{aligned}$$

$$\begin{aligned} A &:= A_1 \cdot A_2 \\ c &:= H_{\text{sig}}(A, pk, m) \end{aligned}$$

$$z_1 := a_1 + c \cdot s_1$$

$$\sigma := (A, z := z_1 + z_2)$$



$$\begin{aligned} a_2 &\leftarrow \mathbb{Z}_p \\ A_2 &:= g^{a_2} \\ \mu_2 &:= H_{\text{com}}(A_2) \end{aligned}$$

$$\begin{aligned} A &:= A_1 \cdot A_2 \\ c &:= H_{\text{sig}}(A, pk, m) \end{aligned}$$

$$z_2 := a_2 + c \cdot s_2$$

$$\sigma := (A, z := z_1 + z_2)$$

$$\begin{aligned} g^z &= A \cdot pk^c \\ g^{a_1+a_2+c \cdot (s_1+s_2)} &= g^{a_1+a_2} \cdot g^{(s_1+s_2) \cdot c} \end{aligned}$$

Glacius [BDLR25]

Glacius [BDLR25]

$$\begin{aligned} a_1 &\leftarrow \mathbb{Z}_p \\ A_1 &:= g^{a_1} \\ \mu_1 &:= H_{\text{com}}(A_1) \end{aligned}$$

$$\begin{aligned} A &:= A_1 \cdot A_2 \\ c &:= H_{\text{sig}}(A, pk, m) \end{aligned}$$

$$z_1 := a_1 + c \cdot s_1$$

$$\sigma := (A, z := z_1 + z_2)$$



———— μ_1 —————>

<———— μ_2 —————

———— A_1 —————>

<———— A_2 —————

———— z_1 —————>

<———— z_2 —————



$$\begin{aligned} a_2 &\leftarrow \mathbb{Z}_p \\ A_2 &:= g^{a_2} \\ \mu_2 &:= H_{\text{com}}(A_2) \end{aligned}$$

$$\begin{aligned} A &:= A_1 \cdot A_2 \\ c &:= H_{\text{sig}}(A, pk, m) \end{aligned}$$

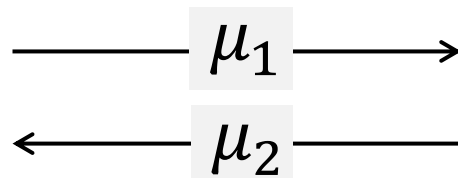
$$z_2 := a_2 + c \cdot s_2$$

$$\sigma := (A, z := z_1 + z_2)$$

$$\begin{aligned} g^z &= A \cdot pk^c \\ g^{a_1+a_2+c \cdot (s_1+s_2)} &= g^{a_1+a_2} \cdot g^{(s_1+s_2) \cdot c} \end{aligned}$$

Glacius [BDLR25]

$$\begin{aligned} a_1 &\leftarrow \mathbb{Z}_p \\ A_1 &:= g^{a_1} \\ \mu_1 &:= H_{\text{com}}(A_1) \end{aligned}$$

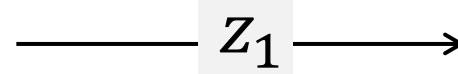
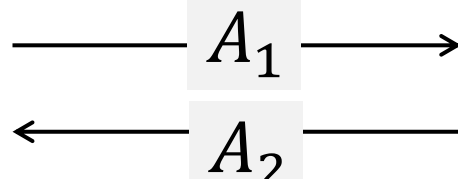


$$\begin{aligned} a_2 &\leftarrow \mathbb{Z}_p \\ A_2 &:= g^{a_2} \\ \mu_2 &:= H_{\text{com}}(A_2) \end{aligned}$$

$$\begin{aligned} A &:= A_1 \cdot A_2 \\ c &:= H_{\text{sig}}(A, pk, m) \end{aligned}$$

$$z_1 := a_1 + c \cdot s_1$$

$$\sigma := (A, z := z_1 + z_2)$$



$$\begin{aligned} A &:= A_1 \cdot A_2 \\ c &:= H_{\text{sig}}(A, pk, m) \end{aligned}$$

$$z_2 := a_2 + c \cdot s_2$$

$$\sigma := (A, z := z_1 + z_2)$$

Glacius [BDLR25]



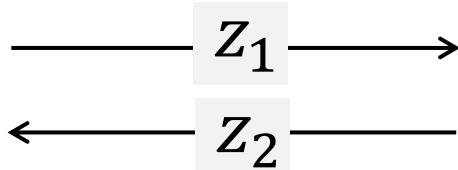
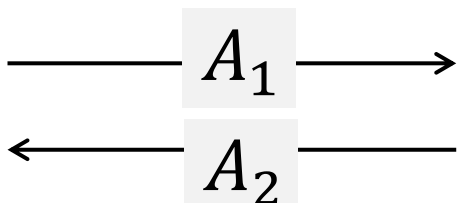
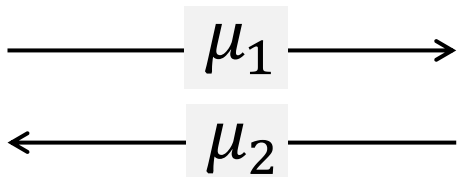
$$\begin{aligned} a_1 &\leftarrow \mathbb{Z}_p \\ A_1 &:= g^{a_1} \\ \mu_1 &:= H_{\text{com}}(A_1) \end{aligned}$$



$$\begin{aligned} A &:= A_1 \cdot A_2 \\ c &:= H_{\text{sig}}(A, pk, m) \end{aligned}$$

$$z_1 := a_1 + c \cdot s_1$$

$$\sigma := (A, z := z_1 + z_2)$$



$$\begin{aligned} a_2 &\leftarrow \mathbb{Z}_p \\ A_2 &:= g^{a_2} \\ \mu_2 &:= H_{\text{com}}(A_2) \end{aligned}$$



$$\begin{aligned} A &:= A_1 \cdot A_2 \\ c &:= H_{\text{sig}}(A, pk, m) \end{aligned}$$

$$z_2 := a_2 + c \cdot s_2$$

$$\sigma := (A, z := z_1 + z_2)$$

Glacius [BDLR25]



$$a_1 \leftarrow \mathbb{Z}_p$$

$$A_1 := g^{a_1}$$

$$\mu_1 := H_{\text{com}}(A_1)$$

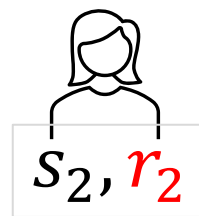
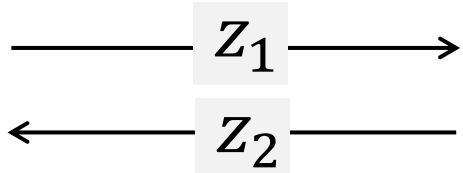
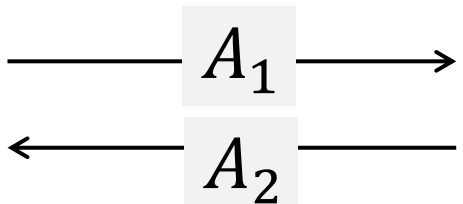
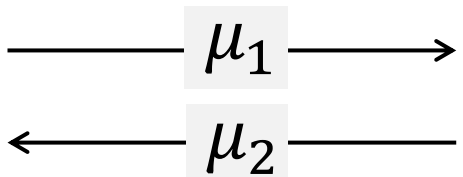
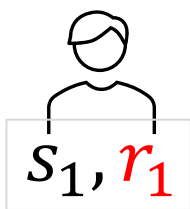


$$A := A_1 \cdot A_2$$

$$c := H_{\text{sig}}(A, pk, m)$$

$$z_1 := a_1 + c \cdot s_1$$

$$\sigma := (A, z := z_1 + z_2)$$



$$a_2 \leftarrow \mathbb{Z}_p$$

$$A_2 := g^{a_2}$$

$$\mu_2 := H_{\text{com}}(A_2)$$



$$A := A_1 \cdot A_2$$

$$c := H_{\text{sig}}(A, pk, m)$$

$$z_2 := a_2 + c \cdot s_2$$

$$\sigma := (A, z := z_1 + z_2)$$

Glacius [BDLR25]



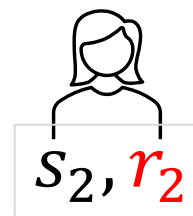
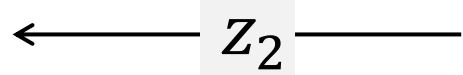
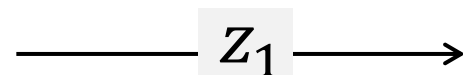
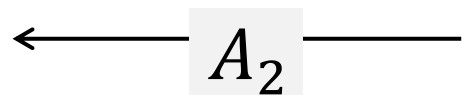
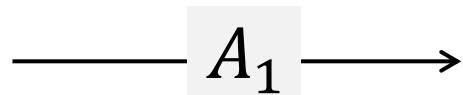
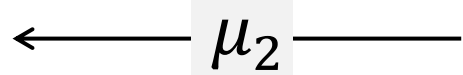
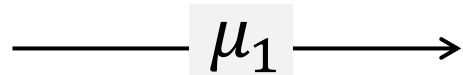
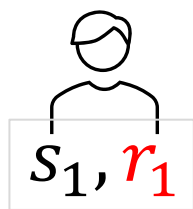
$$a_1 \leftarrow \mathbb{Z}_p$$
$$A_1 := g^{a_1}$$
$$\mu_1 := H_{\text{com}}(A_1)$$



$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_1 := a_1 + c \cdot s_1$$

$$\sigma := (A, z := z_1 + z_2)$$



$$a_2 \leftarrow \mathbb{Z}_p$$
$$A_2 := g^{a_2}$$
$$\mu_2 := H_{\text{com}}(A_2)$$



$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

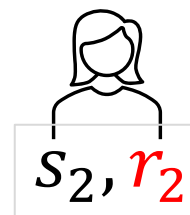
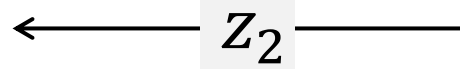
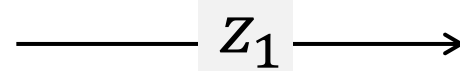
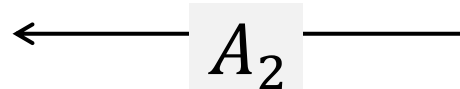
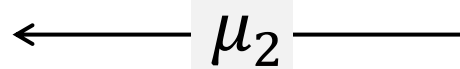
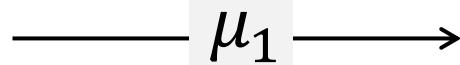
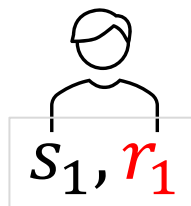
$$z_2 := a_2 + c \cdot s_2$$

$$\sigma := (A, z := z_1 + z_2)$$

Glacius [BDLR25]

$$x_1 \leftarrow \{0,1\}^\lambda$$

$$a_1 \leftarrow \mathbb{Z}_p$$
$$A_1 := g^{a_1}$$
$$\mu_1 := H_{\text{com}}(A_1)$$



$$a_2 \leftarrow \mathbb{Z}_p$$
$$A_2 := g^{a_2}$$
$$\mu_2 := H_{\text{com}}(A_2)$$

$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_1 := a_1 + c \cdot s_1$$

$$\sigma := (A, z := z_1 + z_2)$$

$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

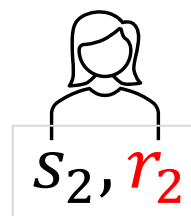
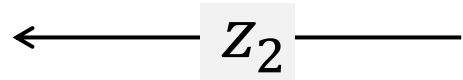
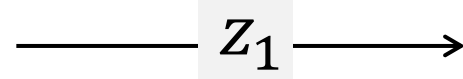
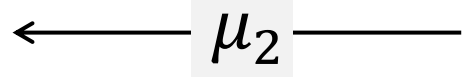
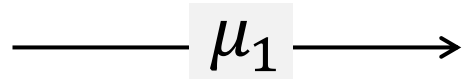
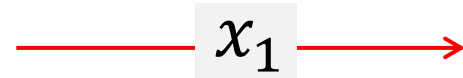
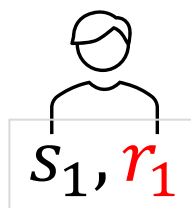
$$z_2 := a_2 + c \cdot s_2$$

$$\sigma := (A, z := z_1 + z_2)$$

Glacius [BDLR25]

$$x_1 \leftarrow \{0,1\}^\lambda$$

$$a_1 \leftarrow \mathbb{Z}_p$$
$$A_1 := g^{a_1}$$
$$\mu_1 := H_{\text{com}}(A_1)$$



$$a_2 \leftarrow \mathbb{Z}_p$$
$$A_2 := g^{a_2}$$
$$\mu_2 := H_{\text{com}}(A_2)$$

$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_1 := a_1 + c \cdot s_1$$

$$\sigma := (A, z := z_1 + z_2)$$

$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

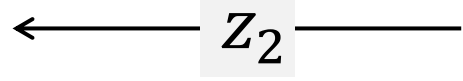
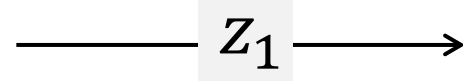
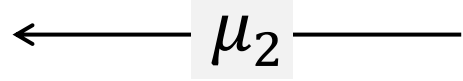
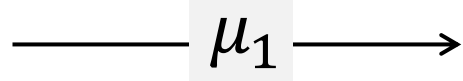
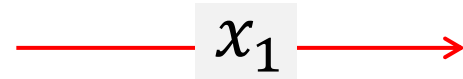
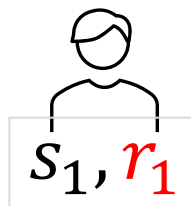
$$z_2 := a_2 + c \cdot s_2$$

$$\sigma := (A, z := z_1 + z_2)$$

Glacius [BDLR25]

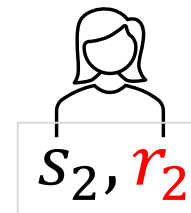
$$x_1 \leftarrow \{0,1\}^\lambda$$

$$a_1 \leftarrow \mathbb{Z}_p$$
$$A_1 := g^{a_1}$$
$$\mu_1 := H_{\text{com}}(A_1)$$



$$x_2 \leftarrow \{0,1\}^\lambda$$

$$a_2 \leftarrow \mathbb{Z}_p$$
$$A_2 := g^{a_2}$$
$$\mu_2 := H_{\text{com}}(A_2)$$



$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_2 := a_2 + c \cdot s_2$$

$$\sigma := (A, z := z_1 + z_2)$$

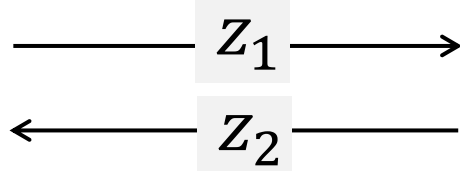
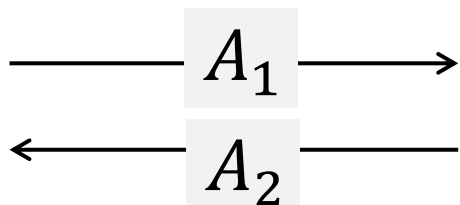
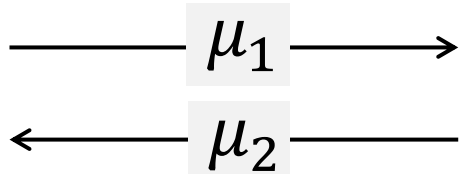
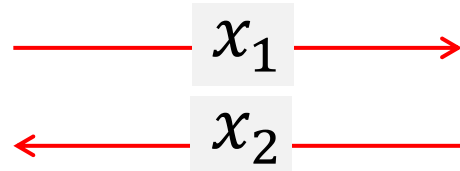
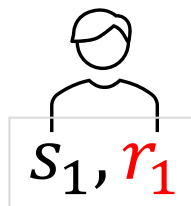
$$z_1 := a_1 + c \cdot s_1$$

$$\sigma := (A, z := z_1 + z_2)$$

Glacius [BDLR25]

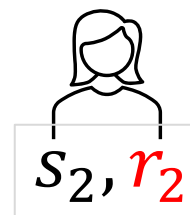
$$x_1 \leftarrow \{0,1\}^\lambda$$

$$a_1 \leftarrow \mathbb{Z}_p$$
$$A_1 := g^{a_1}$$
$$\mu_1 := H_{\text{com}}(A_1)$$



$$x_2 \leftarrow \{0,1\}^\lambda$$

$$a_2 \leftarrow \mathbb{Z}_p$$
$$A_2 := g^{a_2}$$
$$\mu_2 := H_{\text{com}}(A_2)$$



$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_1 := a_1 + c \cdot s_1$$

$$\sigma := (A, z := z_1 + z_2)$$

$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

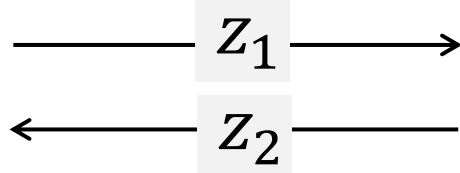
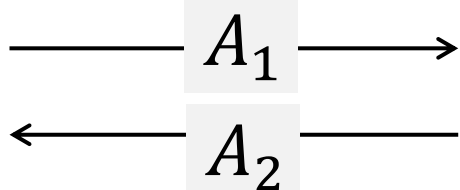
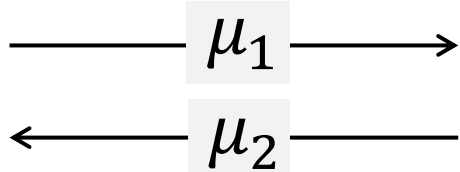
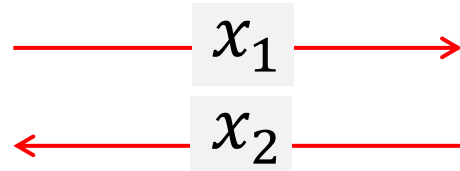
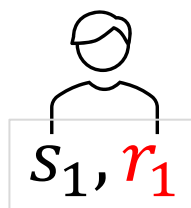
$$z_2 := a_2 + c \cdot s_2$$

$$\sigma := (A, z := z_1 + z_2)$$

Glacius [BDLR25]

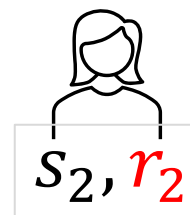
$$x_1 \leftarrow \{0,1\}^\lambda$$
$$x := x_1 | x_2$$

$$a_1 \leftarrow \mathbb{Z}_p$$
$$A_1 := g^{a_1}$$
$$\mu_1 := H_{\text{com}}(A_1)$$



$$x_2 \leftarrow \{0,1\}^\lambda$$
$$x := x_1 | x_2$$

$$a_2 \leftarrow \mathbb{Z}_p$$
$$A_2 := g^{a_2}$$
$$\mu_2 := H_{\text{com}}(A_2)$$



$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_1 := a_1 + c \cdot s_1$$

$$\sigma := (A, z := z_1 + z_2)$$

$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

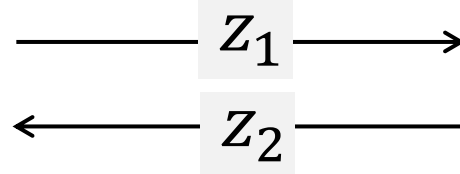
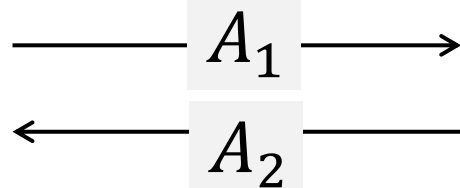
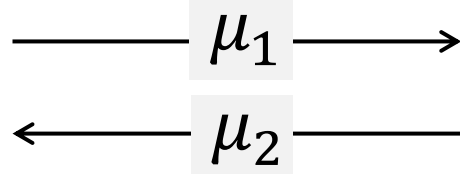
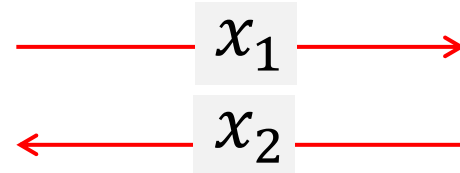
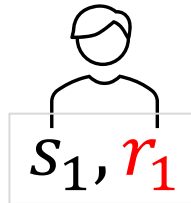
$$z_2 := a_2 + c \cdot s_2$$

$$\sigma := (A, z := z_1 + z_2)$$

Glacius [BDLR25]

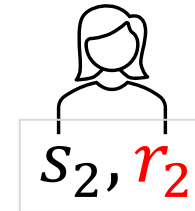
$$x_1 \leftarrow \{0,1\}^\lambda$$
$$x := x_1 | x_2$$

$$a_1 \leftarrow \mathbb{Z}_p$$
$$A_1 := g^{a_1} \cdot F(x)^{r_1}$$
$$\mu_1 := H_{\text{com}}(A_1)$$



$$x_2 \leftarrow \{0,1\}^\lambda$$
$$x := x_1 | x_2$$

$$a_2 \leftarrow \mathbb{Z}_p$$
$$A_2 := g^{a_2} \cdot F(x)^{r_2}$$
$$\mu_2 := H_{\text{com}}(A_2)$$



$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_2 := a_2 + c \cdot s_2$$

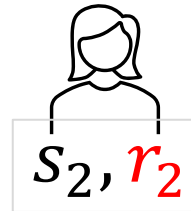
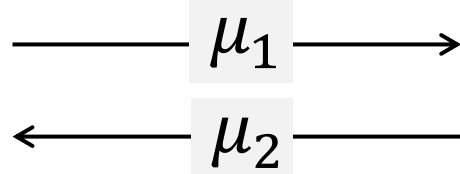
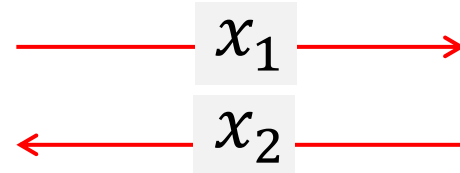
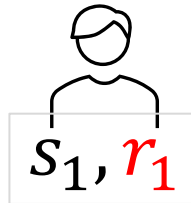
$$\sigma := (A, z := z_1 + z_2)$$

$$z_1 := a_1 + c \cdot s_1$$
$$\sigma := (A, z := z_1 + z_2)$$

Glacius [BDLR25]

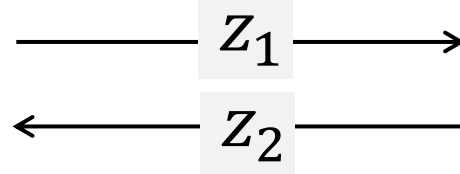
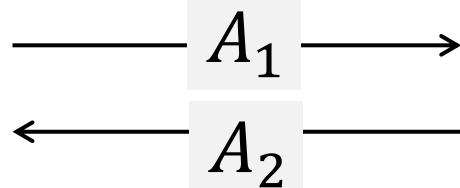
$$x_1 \leftarrow \{0,1\}^\lambda$$
$$x := x_1 | x_2$$

$$a_1 \leftarrow \mathbb{Z}_p$$
$$A_1 := g^{a_1} \cdot F(x)^{r_1}$$
$$\mu_1 := H_{\text{com}}(A_1)$$



$$x_2 \leftarrow \{0,1\}^\lambda$$
$$x := x_1 | x_2$$

$$a_2 \leftarrow \mathbb{Z}_p$$
$$A_2 := g^{a_2} \cdot F(x)^{r_2}$$
$$\mu_2 := H_{\text{com}}(A_2)$$



$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_1 := a_1 + c \cdot s_1$$

$$\sigma := (A, z := z_1 + z_2)$$

$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_2 := a_2 + c \cdot s_2$$

$$\sigma := (A, z := z_1 + z_2)$$

Glacius [BDLR25]

$$x_1 \leftarrow \{0,1\}^\lambda$$
$$x := x_1 | x_2$$

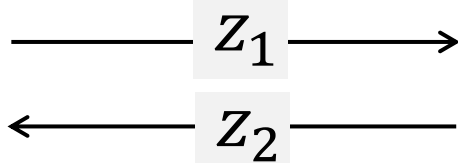
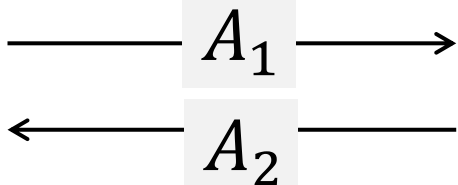
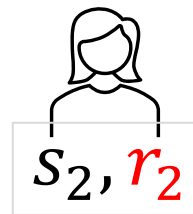
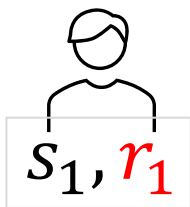
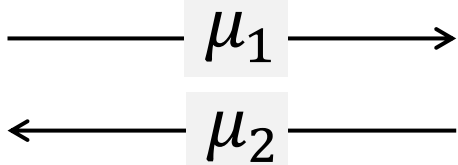
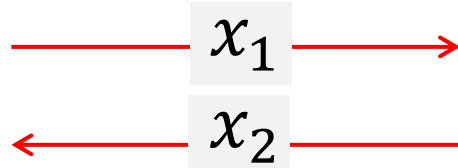
$$a_1 \leftarrow \mathbb{Z}_p$$
$$A_1 := g^{a_1} \cdot F(x)^{r_1}$$
$$\mu_1 := H_{\text{com}}(A_1)$$

$$y_1 := G(x, \mu_1, \mu_2)$$

$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_1 := a_1 + c \cdot s_1$$

$$\sigma := (A, z := z_1 + z_2)$$



$$x_2 \leftarrow \{0,1\}^\lambda$$
$$x := x_1 | x_2$$

$$a_2 \leftarrow \mathbb{Z}_p$$
$$A_2 := g^{a_2} \cdot F(x)^{r_2}$$
$$\mu_2 := H_{\text{com}}(A_2)$$

$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_2 := a_2 + c \cdot s_2$$

$$\sigma := (A, z := z_1 + z_2)$$

Glacius [BDLR25]

$$x_1 \leftarrow \{0,1\}^\lambda$$
$$x := x_1 | x_2$$

$$a_1 \leftarrow \mathbb{Z}_p$$
$$A_1 := g^{a_1} \cdot F(x)^{r_1}$$
$$\mu_1 := H_{\text{com}}(A_1)$$

$$y_1 := G(x, \mu_1, \mu_2)$$

$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_1 := a_1 + c \cdot s_1$$

$$\sigma := (A, z := z_1 + z_2)$$

$$x_1$$

$$x_2$$

$$\mu_1$$

$$\mu_2$$

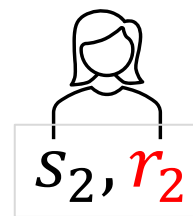
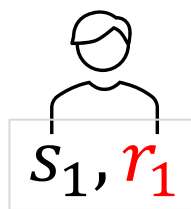
$$y_1$$

$$A_1$$

$$A_2$$

$$z_1$$

$$z_2$$



$$x_2 \leftarrow \{0,1\}^\lambda$$
$$x := x_1 | x_2$$

$$a_2 \leftarrow \mathbb{Z}_p$$
$$A_2 := g^{a_2} \cdot F(x)^{r_2}$$
$$\mu_2 := H_{\text{com}}(A_2)$$

$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_2 := a_2 + c \cdot s_2$$

$$\sigma := (A, z := z_1 + z_2)$$

Glacius [BDLR25]

$$x_1 \leftarrow \{0,1\}^\lambda$$
$$x := x_1 | x_2$$

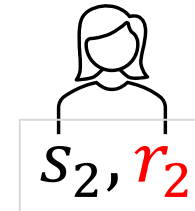
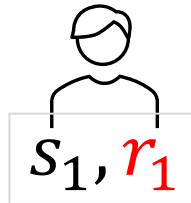
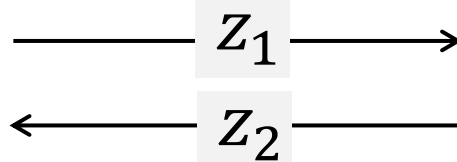
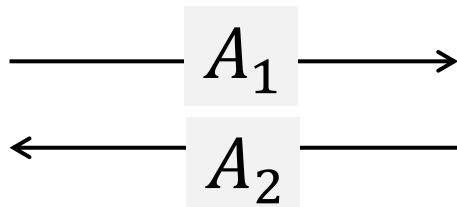
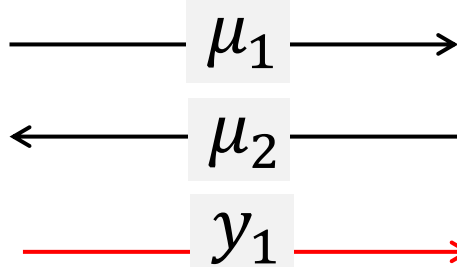
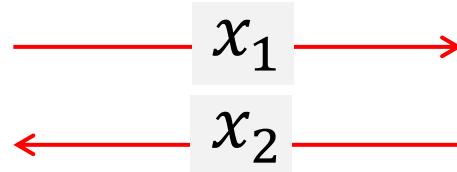
$$a_1 \leftarrow \mathbb{Z}_p$$
$$A_1 := g^{a_1} \cdot F(x)^{r_1}$$
$$\mu_1 := H_{\text{com}}(A_1)$$

$$y_1 := G(x, \mu_1, \mu_2)$$

$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_1 := a_1 + c \cdot s_1$$

$$\sigma := (A, z := z_1 + z_2)$$



$$x_2 \leftarrow \{0,1\}^\lambda$$
$$x := x_1 | x_2$$

$$a_2 \leftarrow \mathbb{Z}_p$$
$$A_2 := g^{a_2} \cdot F(x)^{r_2}$$
$$\mu_2 := H_{\text{com}}(A_2)$$

$$y_2 := G(x, \mu_1, \mu_2)$$

$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_2 := a_2 + c \cdot s_2$$

$$\sigma := (A, z := z_1 + z_2)$$

Glacius [BDLR25]

$$x_1 \leftarrow \{0,1\}^\lambda$$
$$x := x_1 | x_2$$

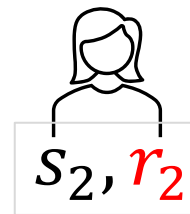
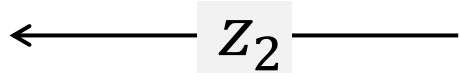
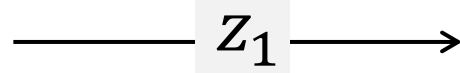
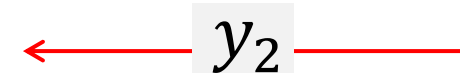
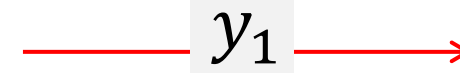
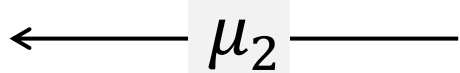
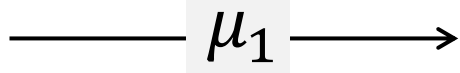
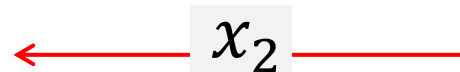
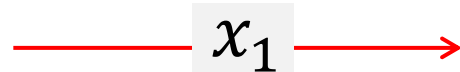
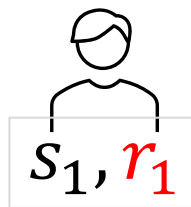
$$a_1 \leftarrow \mathbb{Z}_p$$
$$A_1 := g^{a_1} \cdot F(x)^{r_1}$$
$$\mu_1 := H_{\text{com}}(A_1)$$

$$y_1 := G(x, \mu_1, \mu_2)$$

$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_1 := a_1 + c \cdot s_1$$

$$\sigma := (A, z := z_1 + z_2)$$



$$x_2 \leftarrow \{0,1\}^\lambda$$
$$x := x_1 | x_2$$

$$a_2 \leftarrow \mathbb{Z}_p$$
$$A_2 := g^{a_2} \cdot F(x)^{r_2}$$
$$\mu_2 := H_{\text{com}}(A_2)$$

$$y_2 := G(x, \mu_1, \mu_2)$$

$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_2 := a_2 + c \cdot s_2$$

$$\sigma := (A, z := z_1 + z_2)$$

Our Approach

Glacius [BDLR25]

$$x_1 \leftarrow \{0,1\}^\lambda$$
$$x := x_1 | x_2$$

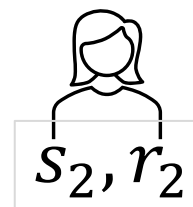
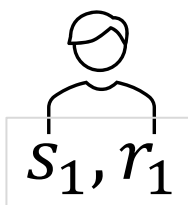
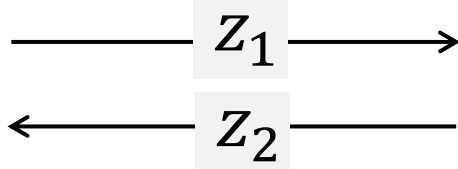
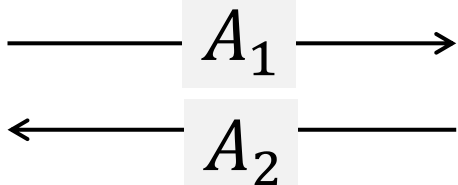
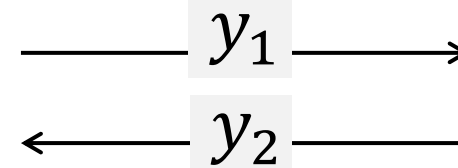
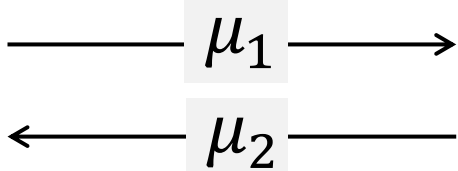
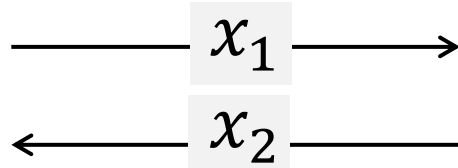
$$a_1 \leftarrow \mathbb{Z}_p$$
$$A_1 := g^{a_1} \cdot F(x)^{r_1}$$
$$\mu_1 := H_{\text{com}}(A_1)$$

$$y_1 := G(x, \mu_1, \mu_2)$$

$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_1 := a_1 + c \cdot s_1$$

$$\sigma := (A, z := z_1 + z_2)$$



$$x_2 \leftarrow \{0,1\}^\lambda$$
$$x := x_1 | x_2$$

$$a_2 \leftarrow \mathbb{Z}_p$$
$$A_2 := g^{a_2} \cdot F(x)^{r_2}$$
$$\mu_2 := H_{\text{com}}(A_2)$$

$$y_2 := G(x, \mu_1, \mu_2)$$

$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

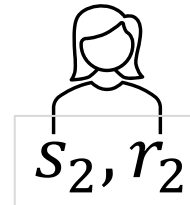
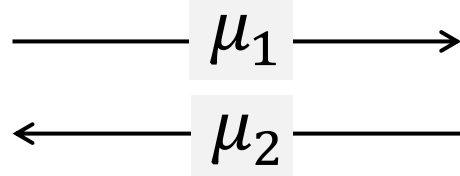
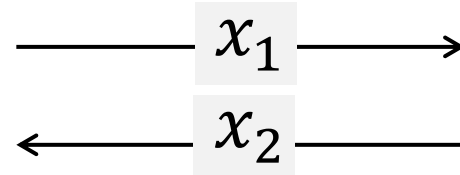
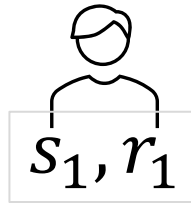
$$z_2 := a_2 + c \cdot s_2$$

$$\sigma := (A, z := z_1 + z_2)$$

Glacius [BDLR25]

$$x_1 \leftarrow \{0,1\}^\lambda$$
$$x := x_1 | x_2$$

$$a_1 \leftarrow \mathbb{Z}_p$$
$$A_1 := g^{a_1} \cdot F(x)^{r_1}$$
$$\mu_1 := H_{\text{com}}(A_1)$$



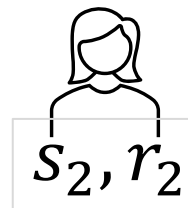
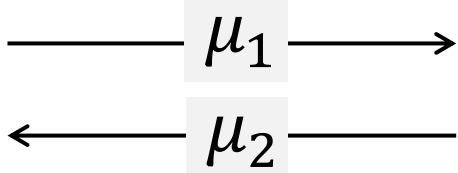
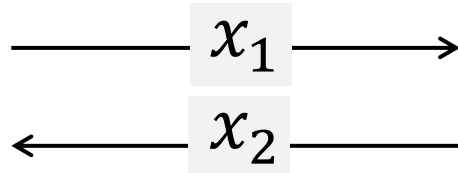
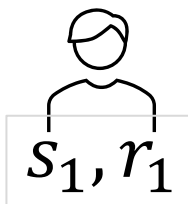
$$x_2 \leftarrow \{0,1\}^\lambda$$
$$x := x_1 | x_2$$

$$a_2 \leftarrow \mathbb{Z}_p$$
$$A_2 := g^{a_2} \cdot F(x)^{r_2}$$
$$\mu_2 := H_{\text{com}}(A_2)$$

Glacius [BDLR25]

$$x_1 \leftarrow \{0,1\}^\lambda$$
$$x := x_1 | x_2$$

$$a_1 \leftarrow \mathbb{Z}_p$$
$$A_1 := g^{a_1} \cdot F(x)^{r_1}$$
$$\mu_1 := H_{\text{com}}(A_1)$$



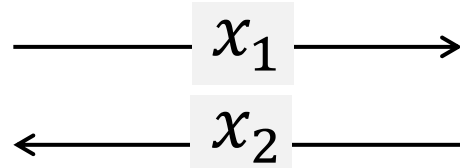
$$x_2 \leftarrow \{0,1\}^\lambda$$
$$x := x_1 | x_2$$

$$a_2 \leftarrow \mathbb{Z}_p$$
$$A_2 := g^{a_2} \cdot F(x)^{r_2}$$
$$\mu_2 := H_{\text{com}}(A_2)$$

Unique x for every signing session

Glacius [BDLR25]

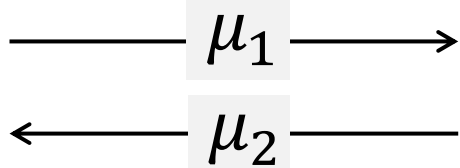
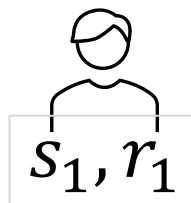
$$x_1 \leftarrow \{0,1\}^\lambda$$
$$x := x_1 | x_2$$



$$x_2 \leftarrow \{0,1\}^\lambda$$
$$x := x_1 | x_2$$

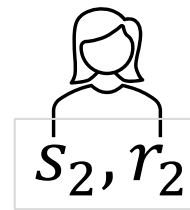
$$a_1 \leftarrow \mathbb{Z}_p$$
$$A_1 := g^{a_1} \cdot F(x)^{r_1}$$

$$\mu_1 := H_{\text{com}}(A_1)$$



$$a_2 \leftarrow \mathbb{Z}_p$$
$$A_2 := g^{a_2} \cdot F(x)^{r_2}$$

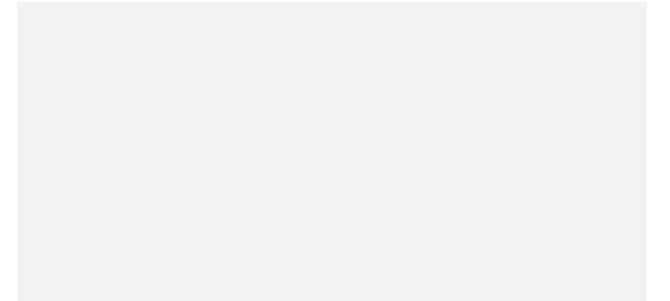
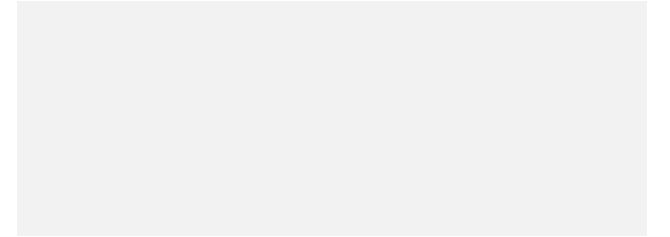
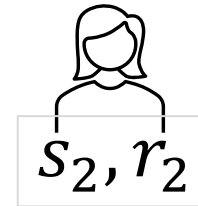
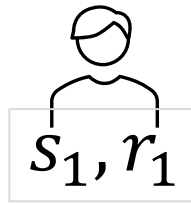
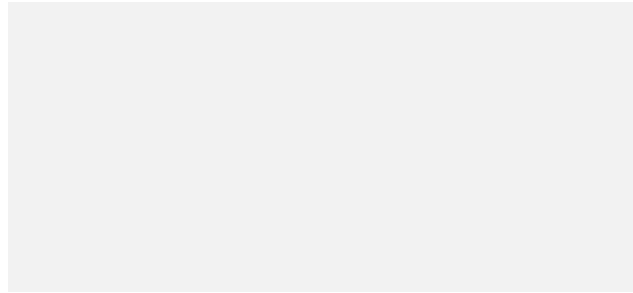
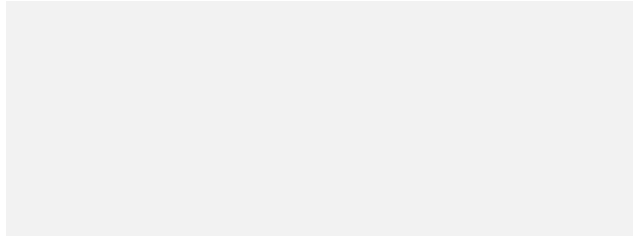
$$\mu_2 := H_{\text{com}}(A_2)$$



Unique x for every signing session

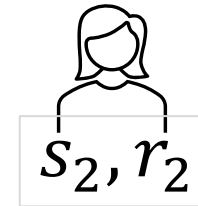
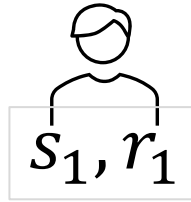
The commitment vector $\mu := \mu_1 | \mu_2$ is also unique

Our protocol



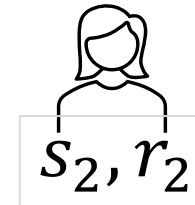
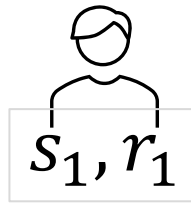
Our protocol

$$a_1 \leftarrow \mathbb{Z}_p$$



Our protocol

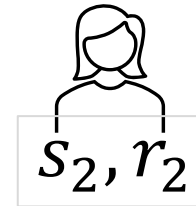
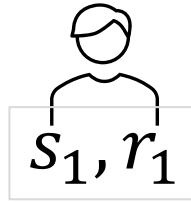
$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$



Our protocol

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$

———— μ_1 ———→

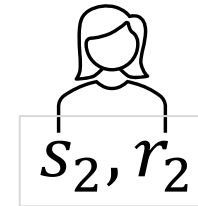
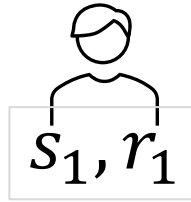


Our protocol

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$

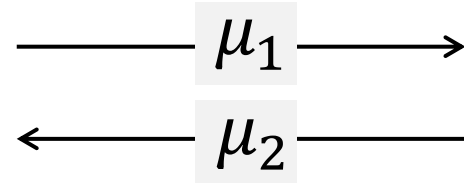
———— μ_1 ———→

$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$

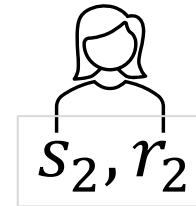
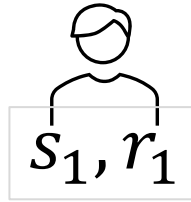


Our protocol

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$



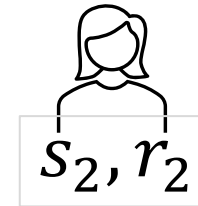
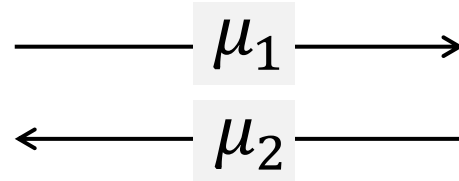
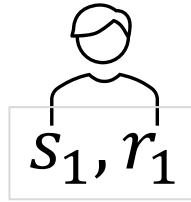
$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$



Our protocol

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$

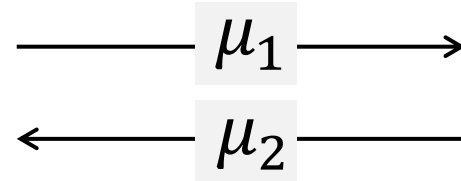
$$\mu := \mu_1 | \mu_2$$



$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$

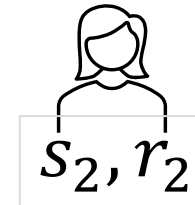
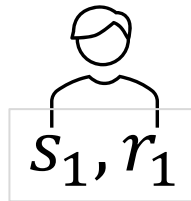
Our protocol

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$



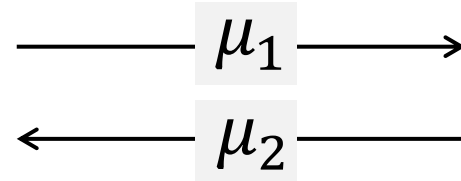
$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$

$$\mu := \mu_1 \parallel \mu_2$$
$$A_1 := g^{a_1} \cdot F(\mu)^{r_1}$$



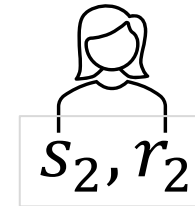
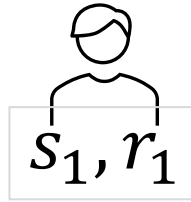
Our protocol

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$



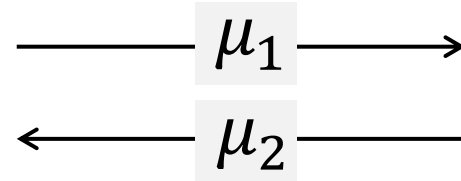
$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$

$$\mu := \mu_1 \parallel \mu_2$$
$$A_1 := g^{a_1} \cdot F(\mu)^{r_1}$$



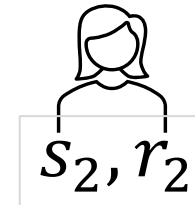
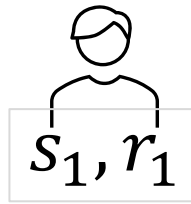
Our protocol

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$



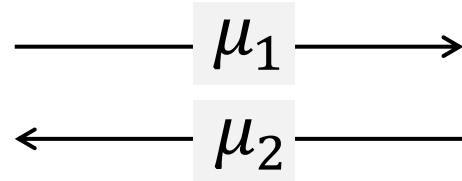
$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$

$$\mu := \mu_1 \parallel \mu_2$$
$$A_1 := g^{a_1} \cdot F(\mu)^{r_1}$$
$$\pi_1 := \text{EQ}(\mu_1, A_1)$$



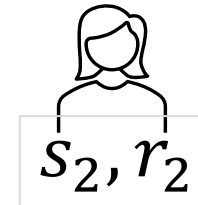
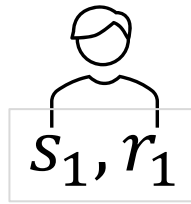
Our protocol

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$



$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$

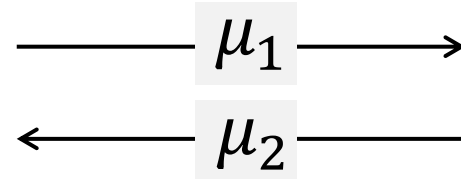
$$\mu := \mu_1 \parallel \mu_2$$
$$A_1 := g^{a_1} \cdot F(\mu)^{r_1}$$
$$\pi_1 := \text{EQ}(\mu_1, A_1)$$



π_i : Proof that identical a_i is used both in μ_i and A_i

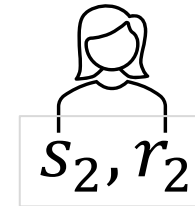
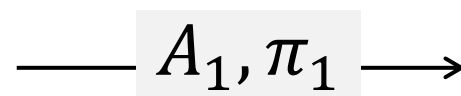
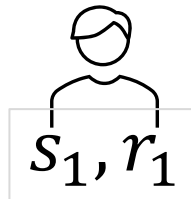
Our protocol

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$



$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$

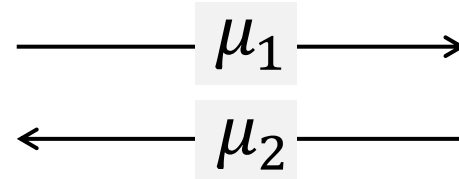
$$\mu := \mu_1 \parallel \mu_2$$
$$A_1 := g^{a_1} \cdot F(\mu)^{r_1}$$
$$\pi_1 := \text{EQ}(\mu_1, A_1)$$



π_i : Proof that identical a_i is used both in μ_i and A_i

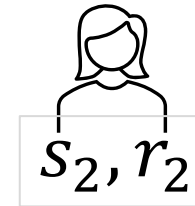
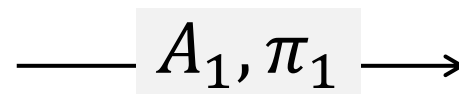
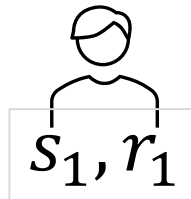
Our protocol

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$



$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$

$$\mu := \mu_1 | \mu_2$$
$$A_1 := g^{a_1} \cdot F(\mu)^{r_1}$$
$$\pi_1 := \text{EQ}(\mu_1, A_1)$$

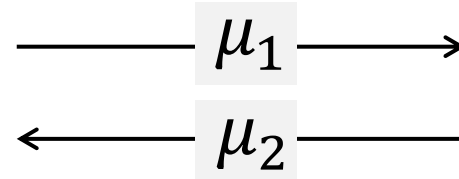


$$\mu := \mu_1 | \mu_2$$
$$A_2 := g^{a_2} \cdot F(\mu)^{r_2}$$
$$\pi_2 := \text{EQ}(\mu_2, A_2)$$

π_i : Proof that identical a_i is used both in μ_i and A_i

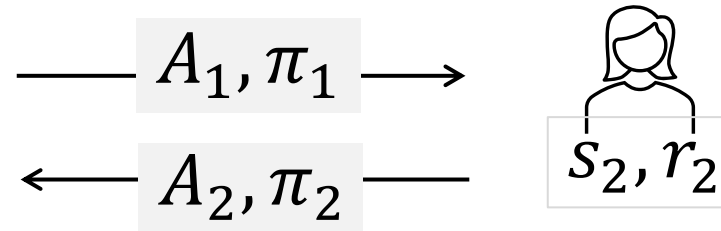
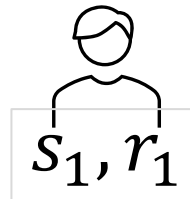
Our protocol

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$



$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$

$$\mu := \mu_1 | \mu_2$$
$$A_1 := g^{a_1} \cdot F(\mu)^{r_1}$$
$$\pi_1 := \text{EQ}(\mu_1, A_1)$$

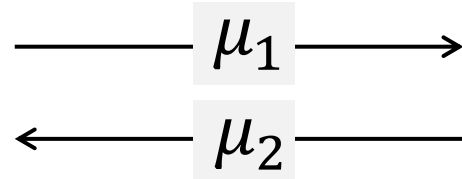


$$\mu := \mu_1 | \mu_2$$
$$A_2 := g^{a_2} \cdot F(\mu)^{r_2}$$
$$\pi_2 := \text{EQ}(\mu_2, A_2)$$

π_i : Proof that identical a_i is used both in μ_i and A_i

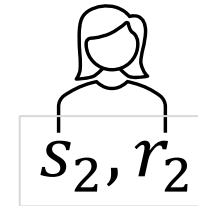
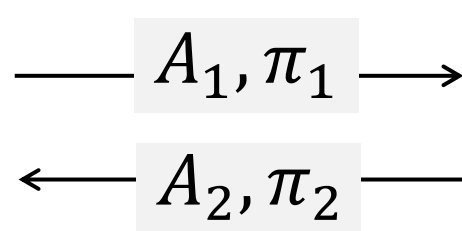
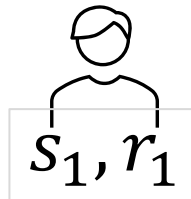
Our protocol

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$



$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$

$$\mu := \mu_1 | \mu_2$$
$$A_1 := g^{a_1} \cdot F(\mu)^{r_1}$$
$$\pi_1 := \text{EQ}(\mu_1, A_1)$$



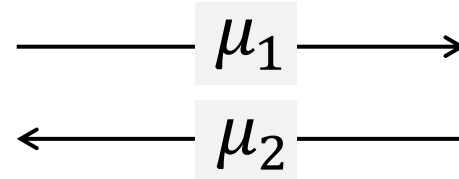
$$\mu := \mu_1 | \mu_2$$
$$A_2 := g^{a_2} \cdot F(\mu)^{r_2}$$
$$\pi_2 := \text{EQ}(\mu_2, A_2)$$

π_i : Proof that identical a_i is used both in μ_i and A_i

Generic SNARK?
Very expensive.

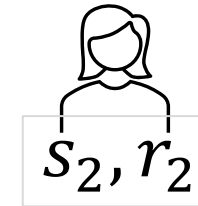
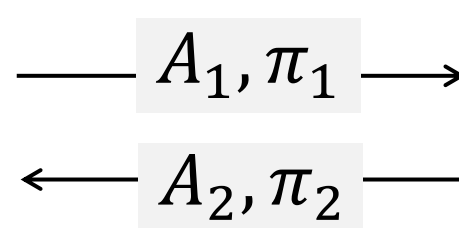
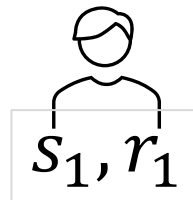
Our protocol

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$



$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$

$$\mu := \mu_1 | \mu_2$$
$$A_1 := g^{a_1} \cdot F(\mu)^{r_1}$$
$$\pi_1 := \text{EQ}(\mu_1, A_1)$$



$$\mu := \mu_1 | \mu_2$$
$$A_2 := g^{a_2} \cdot F(\mu)^{r_2}$$
$$\pi_2 := \text{EQ}(\mu_2, A_2)$$

π_i : Proof that identical a_i is used both in μ_i and A_i

Generic SNARK?
Very expensive.

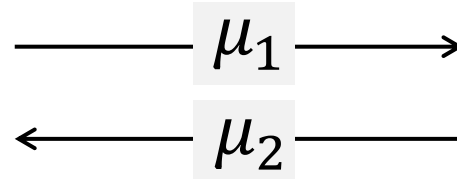


Efficient Σ -protocol!

Our protocol

$$a_1 \leftarrow \mathbb{Z}_p$$

$$\mu_1 := H_{\text{com}}(g^{a_1})$$



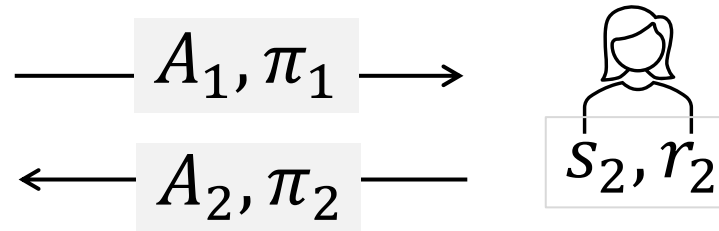
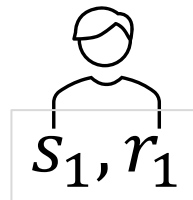
$$a_2 \leftarrow \mathbb{Z}_p$$

$$\mu_2 := H_{\text{com}}(g^{a_2})$$

$$\mu := \mu_1 | \mu_2$$

$$A_1 := g^{a_1} \cdot F(\mu)^{r_1}$$

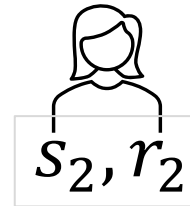
$$\pi_1 := \text{EQ}(\mu_1, A_1)$$



$$\mu := \mu_1 | \mu_2$$

$$A_2 := g^{a_2} \cdot F(\mu)^{r_2}$$

$$\pi_2 := \text{EQ}(\mu_2, A_2)$$



π_i : Proof that identical a_i is used both in μ_i and A_i

Generic SNARK?
Very expensive.



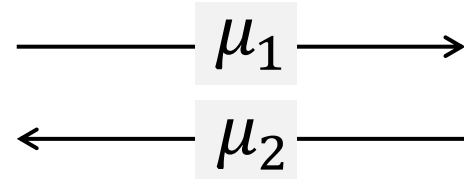
Efficient Σ -protocol!

Merge hash-commitment and unique session identifier sampling round!

Our protocol: removing view consistency check

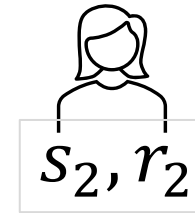
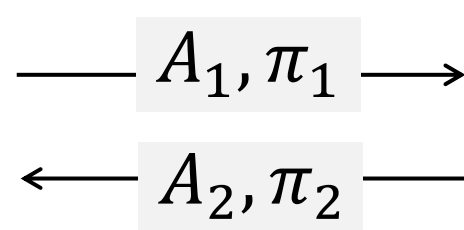
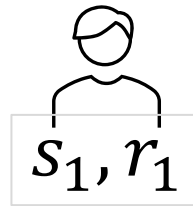
Our protocol: removing view consistency check

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$



$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$

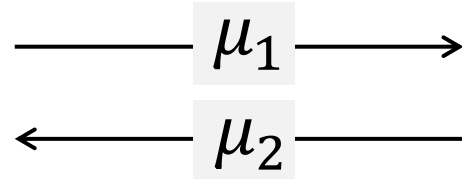
$$\mu := \mu_1 | \mu_2$$
$$A_1 := g^{a_1} \cdot F(\mu)^{r_1}$$
$$\pi_1 := \text{EQ}(\mu_1, A_1)$$



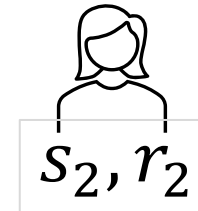
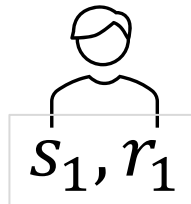
$$\mu := \mu_1 | \mu_2$$
$$A_2 := g^{a_2} \cdot F(\mu)^{r_2}$$
$$\pi_2 := \text{EQ}(\mu_2, A_2)$$

Our protocol: removing view consistency check

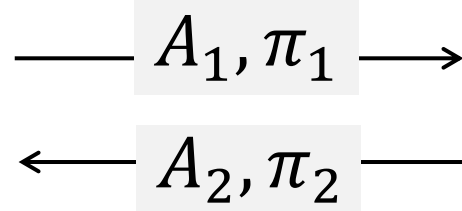
$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$



$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$



$$\mu := \mu_1 | \mu_2$$
$$A_1 := g^{a_1} \cdot F(\mu)^{r_1}$$
$$\pi_1 := \text{EQ}(\mu_1, A_1)$$



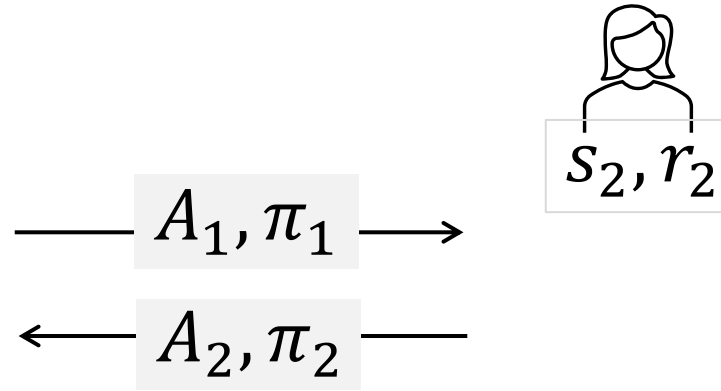
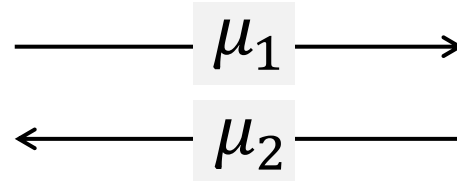
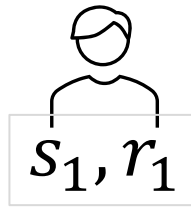
$$\mu := \mu_1 | \mu_2$$
$$A_2 := g^{a_2} \cdot F(\mu)^{r_2}$$
$$\pi_2 := \text{EQ}(\mu_2, A_2)$$

Our protocol: removing view consistency check

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$

$$y_1 := G(\mu_1, \mu_2)$$

$$\mu := \mu_1 | \mu_2$$
$$A_1 := g^{a_1} \cdot F(\mu)^{r_1}$$
$$\pi_1 := \text{EQ}(\mu_1, A_1)$$



$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$

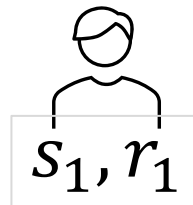
$$\mu := \mu_1 | \mu_2$$
$$A_2 := g^{a_2} \cdot F(\mu)^{r_2}$$
$$\pi_2 := \text{EQ}(\mu_2, A_2)$$

Our protocol: removing view consistency check

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$

$$y_1 := G(\mu_1, \mu_2)$$

$$\mu := \mu_1 | \mu_2$$
$$A_1 := g^{a_1} \cdot F(\mu)^{r_1}$$
$$\pi_1 := \text{EQ}(\mu_1, A_1)$$



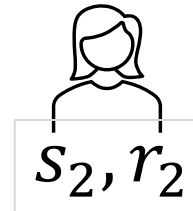
$$\longrightarrow \mu_1 \longrightarrow$$

$$\longleftarrow \mu_2 \longleftarrow$$

$$\longrightarrow y_1 \longrightarrow$$

$$\longrightarrow A_1, \pi_1 \longrightarrow$$

$$\longleftarrow A_2, \pi_2 \longleftarrow$$



$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$

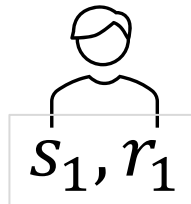
$$\mu := \mu_1 | \mu_2$$
$$A_2 := g^{a_2} \cdot F(\mu)^{r_2}$$
$$\pi_2 := \text{EQ}(\mu_2, A_2)$$

Our protocol: removing view consistency check

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$

$$y_1 := G(\mu_1, \mu_2)$$

$$\mu := \mu_1 | \mu_2$$
$$A_1 := g^{a_1} \cdot F(\mu)^{r_1}$$
$$\pi_1 := \text{EQ}(\mu_1, A_1)$$



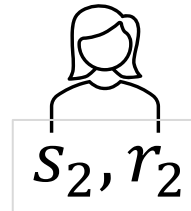
$$\xrightarrow{\mu_1}$$

$$\xleftarrow{\mu_2}$$

$$\xrightarrow{y_1}$$

$$\xrightarrow{A_1, \pi_1}$$

$$\xleftarrow{A_2, \pi_2}$$



$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$

$$y_2 := G(\mu_1, \mu_2)$$

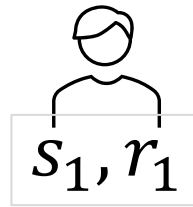
$$\mu := \mu_1 | \mu_2$$
$$A_2 := g^{a_2} \cdot F(\mu)^{r_2}$$
$$\pi_2 := \text{EQ}(\mu_2, A_2)$$

Our protocol: removing view consistency check

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$

$$y_1 := G(\mu_1, \mu_2)$$

$$\mu := \mu_1 | \mu_2$$
$$A_1 := g^{a_1} \cdot F(\mu)^{r_1}$$
$$\pi_1 := \text{EQ}(\mu_1, A_1)$$



$$\mu_1$$

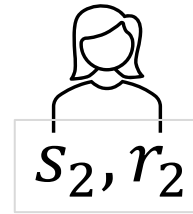
$$\mu_2$$

$$y_1$$

$$y_2$$

$$A_1, \pi_1$$

$$A_2, \pi_2$$



$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$

$$y_2 := G(\mu_1, \mu_2)$$

$$\mu := \mu_1 | \mu_2$$
$$A_2 := g^{a_2} \cdot F(\mu)^{r_2}$$
$$\pi_2 := \text{EQ}(\mu_2, A_2)$$

Our protocol: removing view consistency check

$$a_1 \leftarrow \mathbb{Z}_p$$

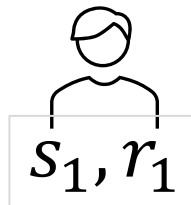
$$\mu_1 := H_{\text{com}}(g^{a_1})$$

$$y_1 := G(\mu_1, \mu_2)$$

$$\mu := \mu_1 | \mu_2$$

$$A_1 := g^{a_1} \cdot F(\mu)^{r_1}$$

$$\pi_1 := \text{EQ}(\mu_1, A_1)$$



$$\longrightarrow \mu_1 \longrightarrow$$

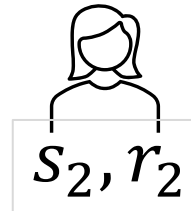
$$\longleftarrow \mu_2 \longleftarrow$$

$$\longrightarrow y_1 \longrightarrow$$

$$\longleftarrow y_2 \longleftarrow$$

$$\longrightarrow A_1, \pi_1 \longrightarrow$$

$$\longleftarrow A_2, \pi_2 \longleftarrow$$



$$a_2 \leftarrow \mathbb{Z}_p$$

$$\mu_2 := H_{\text{com}}(g^{a_2})$$

$$y_2 := G(\mu_1, \mu_2)$$

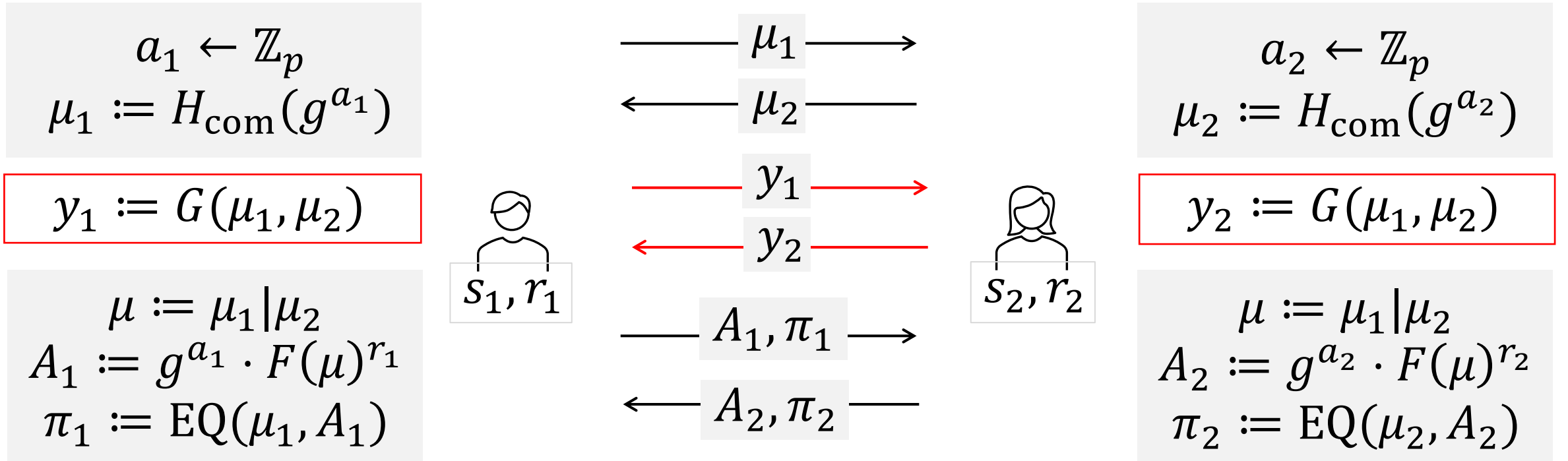
$$\mu := \mu_1 | \mu_2$$

$$A_2 := g^{a_2} \cdot F(\mu)^{r_2}$$

$$\pi_2 := \text{EQ}(\mu_2, A_2)$$

Reduction **can not** simulate when adversary sends **different** commitments

Our protocol: removing view consistency check

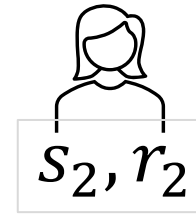
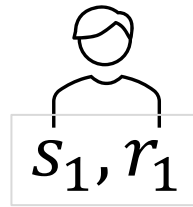


Reduction **can not** simulate when adversary sends **different** commitments

Equivalence class from Twinkle [BLT+24] + other techniques

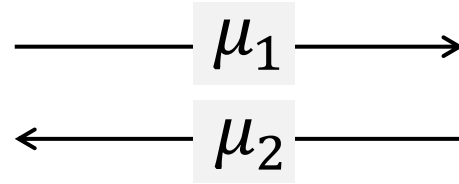
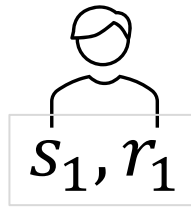
Our final protocol

Our final protocol

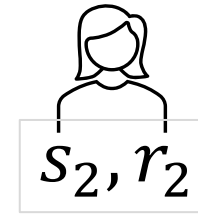


Our final protocol

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$

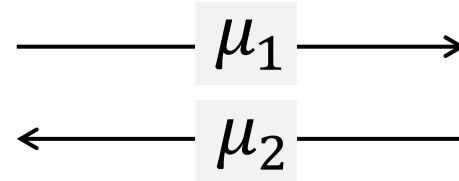


$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$



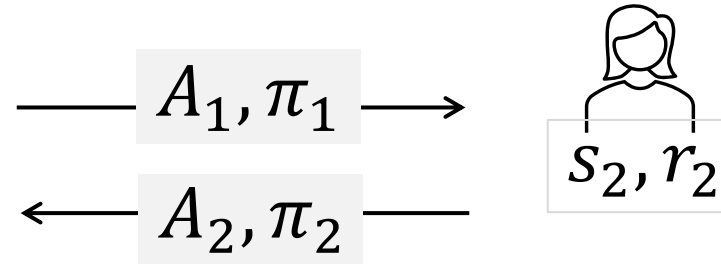
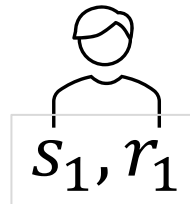
Our final protocol

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$



$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$

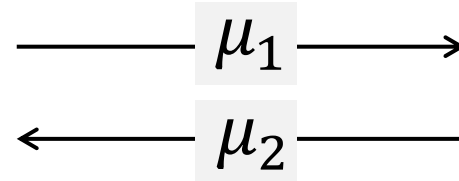
$$\mu := \mu_1 | \mu_2$$
$$A_1 := g^{a_1} \cdot F(\mu)^{r_1}$$
$$\pi_1 := \text{EQ}(\mu_1, A_1)$$



$$\mu := \mu_1 | \mu_2$$
$$A_2 := g^{a_2} \cdot F(\mu)^{r_2}$$
$$\pi_2 := \text{EQ}(\mu_2, A_2)$$

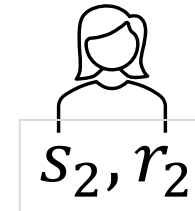
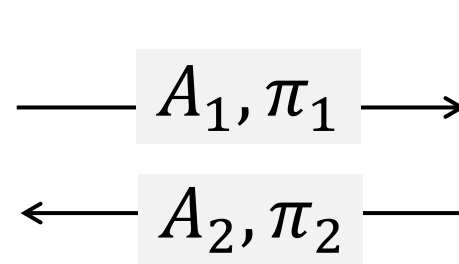
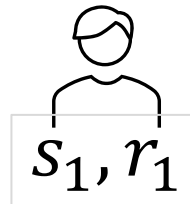
Our final protocol

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$



$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$

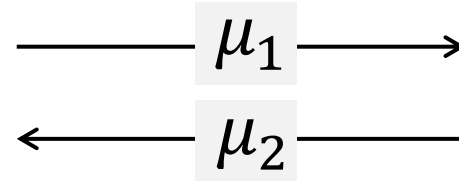
$$\mu := \mu_1 | \mu_2$$
$$A_1 := g^{a_1} \cdot F(\mu)^{r_1}$$
$$\pi_1 := \text{EQ}(\mu_1, A_1)$$



$$\mu := \mu_1 | \mu_2$$
$$A_2 := g^{a_2} \cdot F(\mu)^{r_2}$$
$$\pi_2 := \text{EQ}(\mu_2, A_2)$$

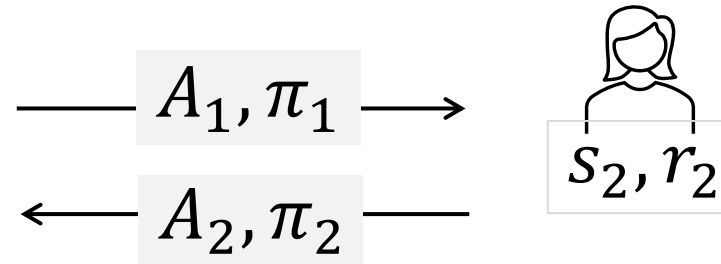
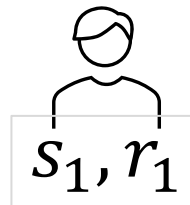
Our final protocol

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$



$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$

$$\mu := \mu_1 | \mu_2$$
$$A_1 := g^{a_1} \cdot F(\mu)^{r_1}$$
$$\pi_1 := \text{EQ}(\mu_1, A_1)$$



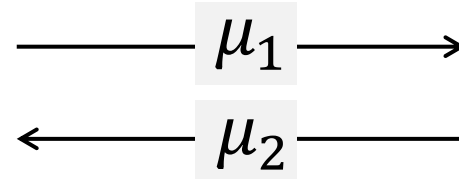
$$\mu := \mu_1 | \mu_2$$
$$A_2 := g^{a_2} \cdot F(\mu)^{r_2}$$
$$\pi_2 := \text{EQ}(\mu_2, A_2)$$

$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_1 := a_1 + c \cdot s_1$$

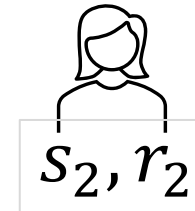
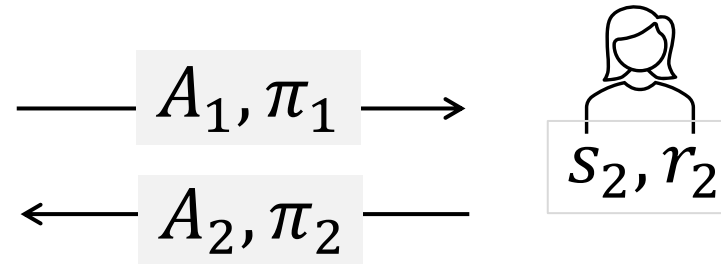
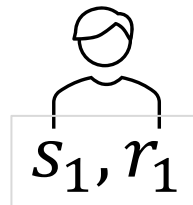
Our final protocol

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$



$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$

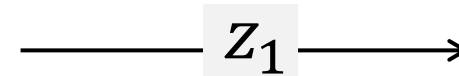
$$\mu := \mu_1 | \mu_2$$
$$A_1 := g^{a_1} \cdot F(\mu)^{r_1}$$
$$\pi_1 := \text{EQ}(\mu_1, A_1)$$



$$\mu := \mu_1 | \mu_2$$
$$A_2 := g^{a_2} \cdot F(\mu)^{r_2}$$
$$\pi_2 := \text{EQ}(\mu_2, A_2)$$

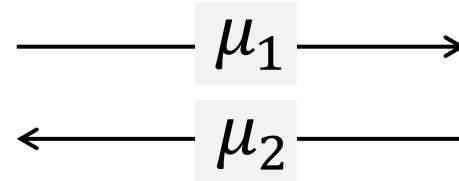
$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_1 := a_1 + c \cdot s_1$$



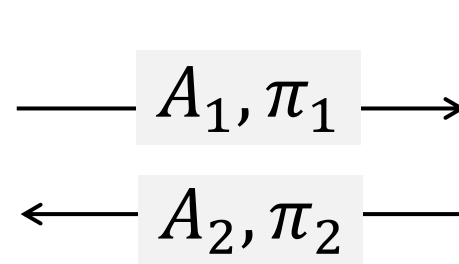
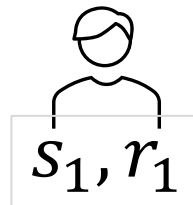
Our final protocol

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$

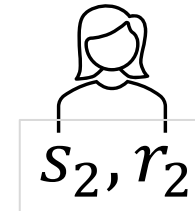


$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$

$$\mu := \mu_1 | \mu_2$$
$$A_1 := g^{a_1} \cdot F(\mu)^{r_1}$$
$$\pi_1 := \text{EQ}(\mu_1, A_1)$$

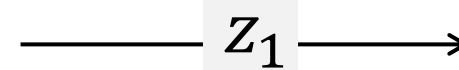


$$\mu := \mu_1 | \mu_2$$
$$A_2 := g^{a_2} \cdot F(\mu)^{r_2}$$
$$\pi_2 := \text{EQ}(\mu_2, A_2)$$



$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_1 := a_1 + c \cdot s_1$$

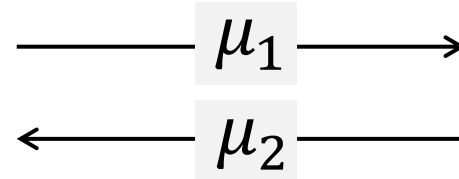


$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_2 := a_2 + c \cdot s_2$$

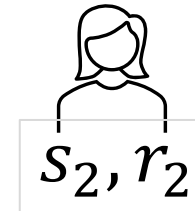
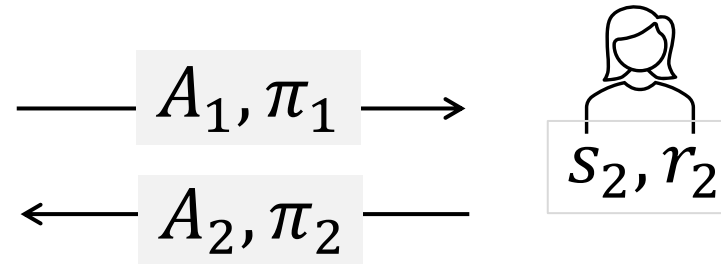
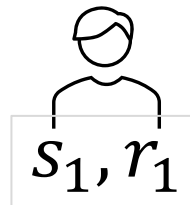
Our final protocol

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$



$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$

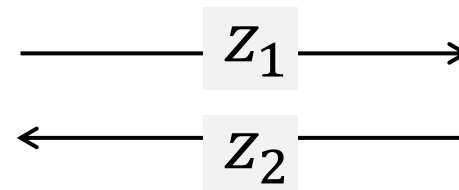
$$\mu := \mu_1 | \mu_2$$
$$A_1 := g^{a_1} \cdot F(\mu)^{r_1}$$
$$\pi_1 := \text{EQ}(\mu_1, A_1)$$



$$\mu := \mu_1 | \mu_2$$
$$A_2 := g^{a_2} \cdot F(\mu)^{r_2}$$
$$\pi_2 := \text{EQ}(\mu_2, A_2)$$

$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_1 := a_1 + c \cdot s_1$$

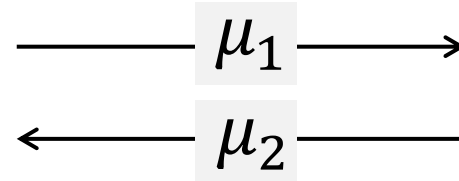


$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_2 := a_2 + c \cdot s_2$$

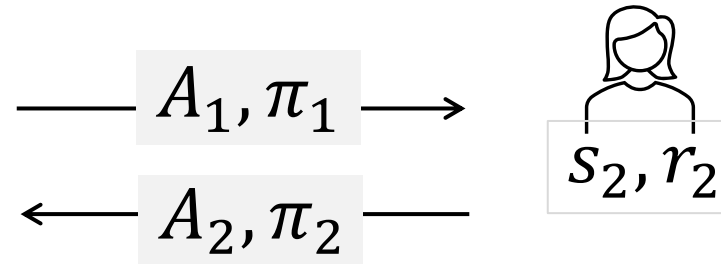
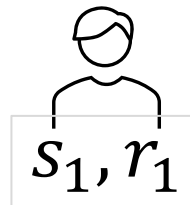
Our final protocol

$$a_1 \leftarrow \mathbb{Z}_p$$
$$\mu_1 := H_{\text{com}}(g^{a_1})$$

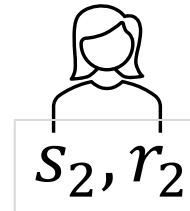


$$a_2 \leftarrow \mathbb{Z}_p$$
$$\mu_2 := H_{\text{com}}(g^{a_2})$$

$$\mu := \mu_1 | \mu_2$$
$$A_1 := g^{a_1} \cdot F(\mu)^{r_1}$$
$$\pi_1 := \text{EQ}(\mu_1, A_1)$$

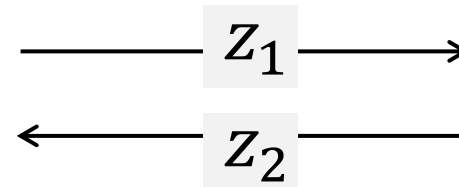


$$\mu := \mu_1 | \mu_2$$
$$A_2 := g^{a_2} \cdot F(\mu)^{r_2}$$
$$\pi_2 := \text{EQ}(\mu_2, A_2)$$



$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_1 := a_1 + c \cdot s_1$$



$$A := A_1 \cdot A_2$$
$$c := H_{\text{sig}}(A, pk, m)$$

$$z_2 := a_2 + c \cdot s_2$$

$$\sigma := (A, z := z_1 + z_2)$$

$$\sigma := (A, z := z_1 + z_2)$$

Summary: Adaptively secure threshold Schnorr

Scheme	Rounds	Signing key size	Identifiable Abort?	Model + Assumptions
ZeroS [#] [Mak22]	3	1	✓	ROM + DL
KRT [KRT24]	5	$n + 1$	✗	ROM + DL
Glacius [BDLR25]	5	3	✓	ROM + DDH
This work	3	3	✓	ROM + DDH

[#] ZeroS assumes secure channels and secure **erasures**

Sparkle [CKM23]	3	1	✓	ROM + DL
-----------------	---	---	---	----------

Statically secure