BUFFing Threshold Signatures

Marc Fischlin*, Katerina Mitrokotsa[$], Jenit Tomy[$]

*Cryptoplexity, TU Darmstadt, Germany

[$]University of St. Gallen, Switzerland

PKC 2025

Threshold Signatures

Definition

sk_1 sk_2 sk_3 sk_4

Verifier

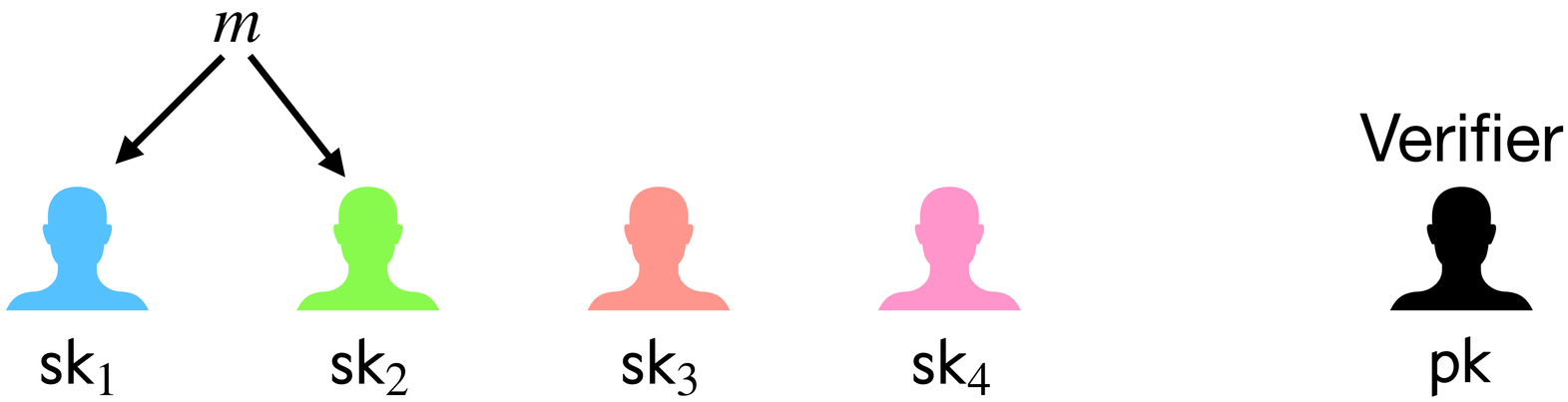
pk

$\text{KeyGen}(1^\lambda, t, n) \rightarrow$
$t = 2,\ n = 4$

Optional: $\text{pk}_1, \text{pk}_2, \text{pk}_3, \text{pk}_4$

Threshold Signatures

Definition



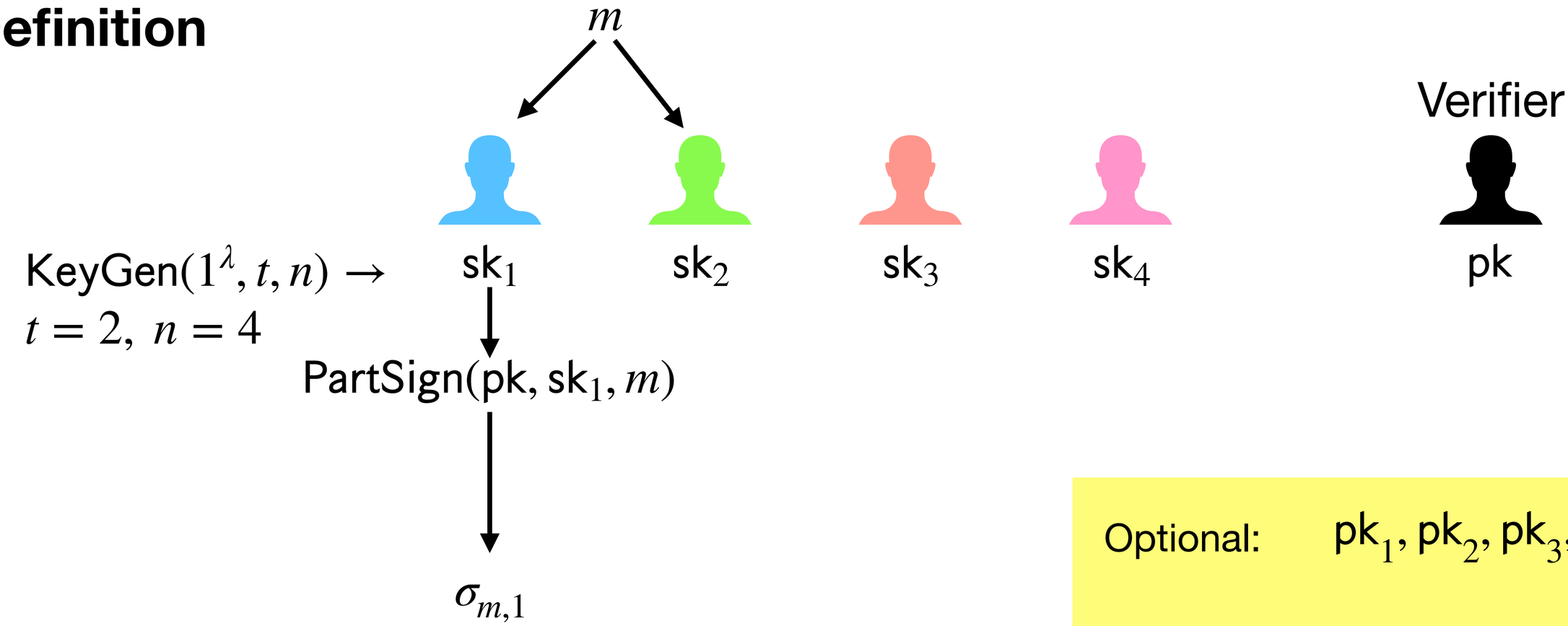
$\mathsf{KeyGen}(1^\lambda, t, n) \rightarrow$

$t = 2,\ n = 4$

Optional: $\mathsf{pk}_1, \mathsf{pk}_2, \mathsf{pk}_3, \mathsf{pk}_4$

Threshold Signatures

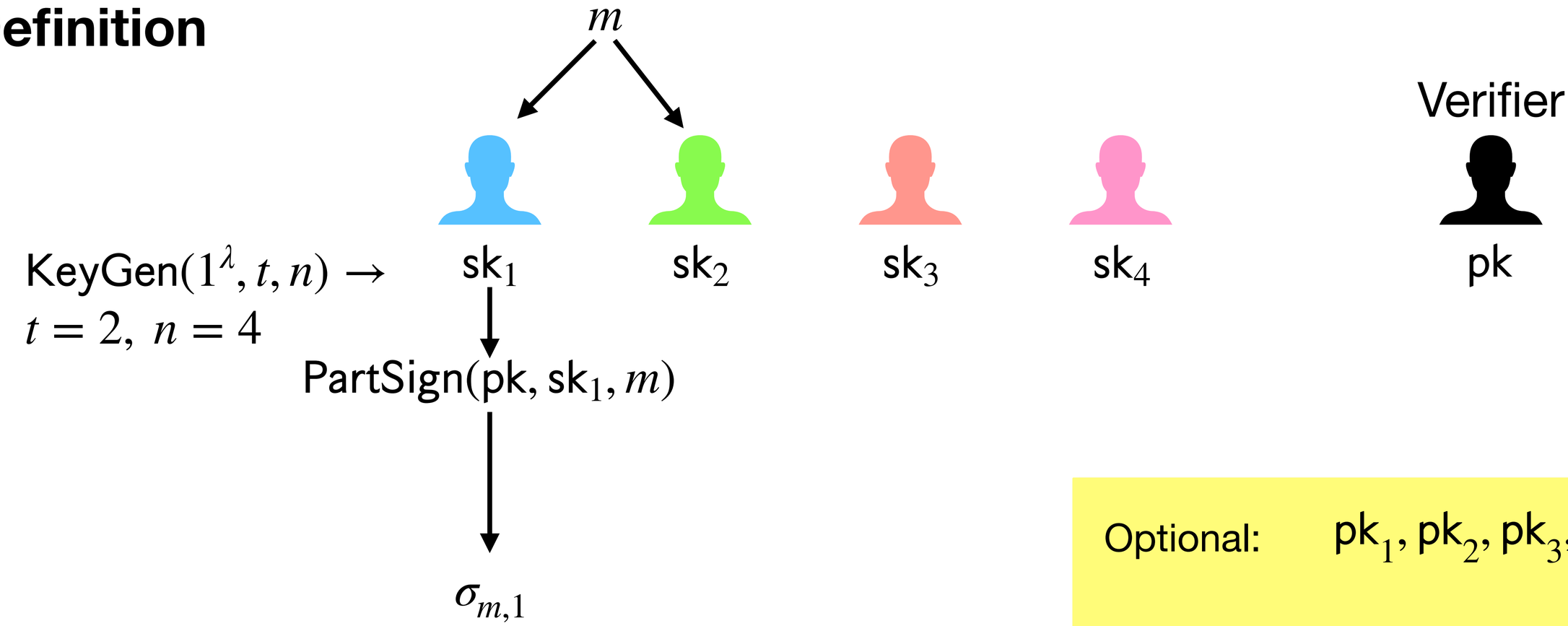
Definition



Optional: $\mathsf{pk}_1, \mathsf{pk}_2, \mathsf{pk}_3, \mathsf{pk}_4$

Threshold Signatures

Definition

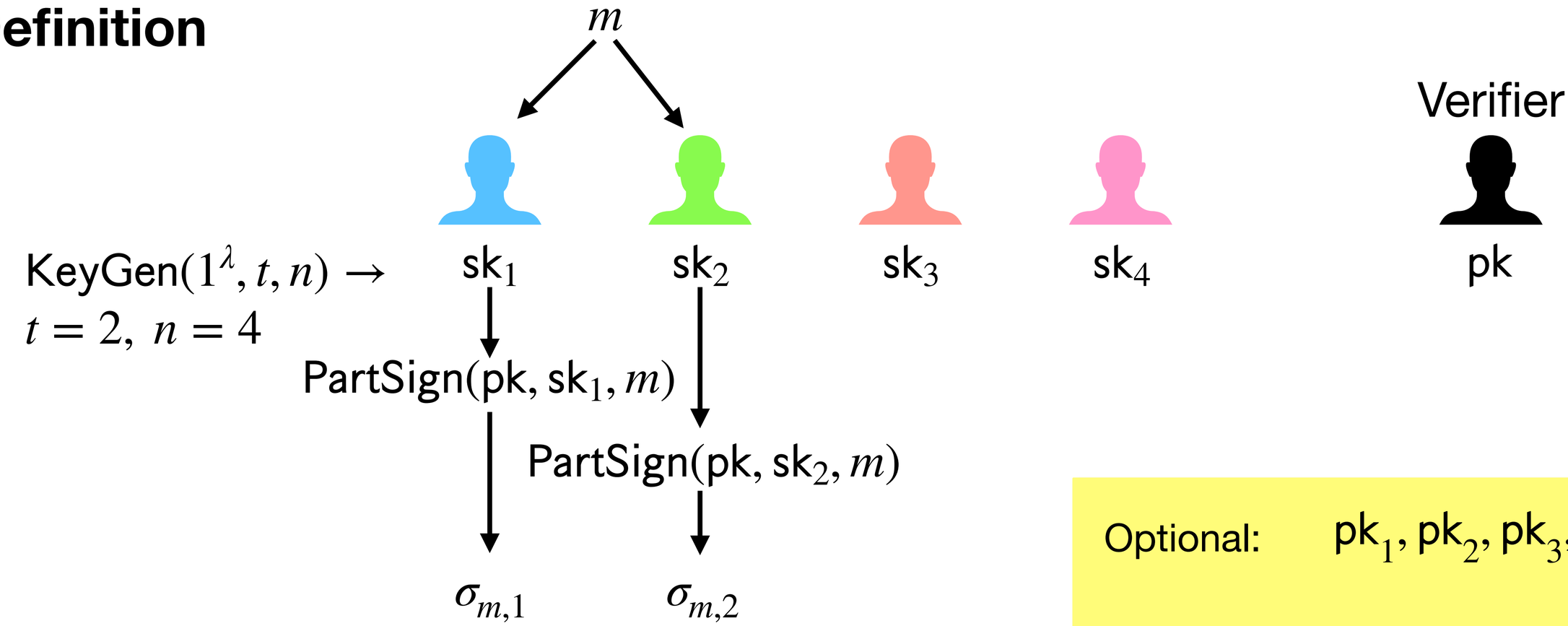


Optional: $\mathsf{pk}_1, \mathsf{pk}_2, \mathsf{pk}_3, \mathsf{pk}_4$

$\mathsf{PartVer}(\mathsf{pk}, \mathsf{pk}_1, m, \sigma_{m,1}) \rightarrow 0/1$

Threshold Signatures

Definition

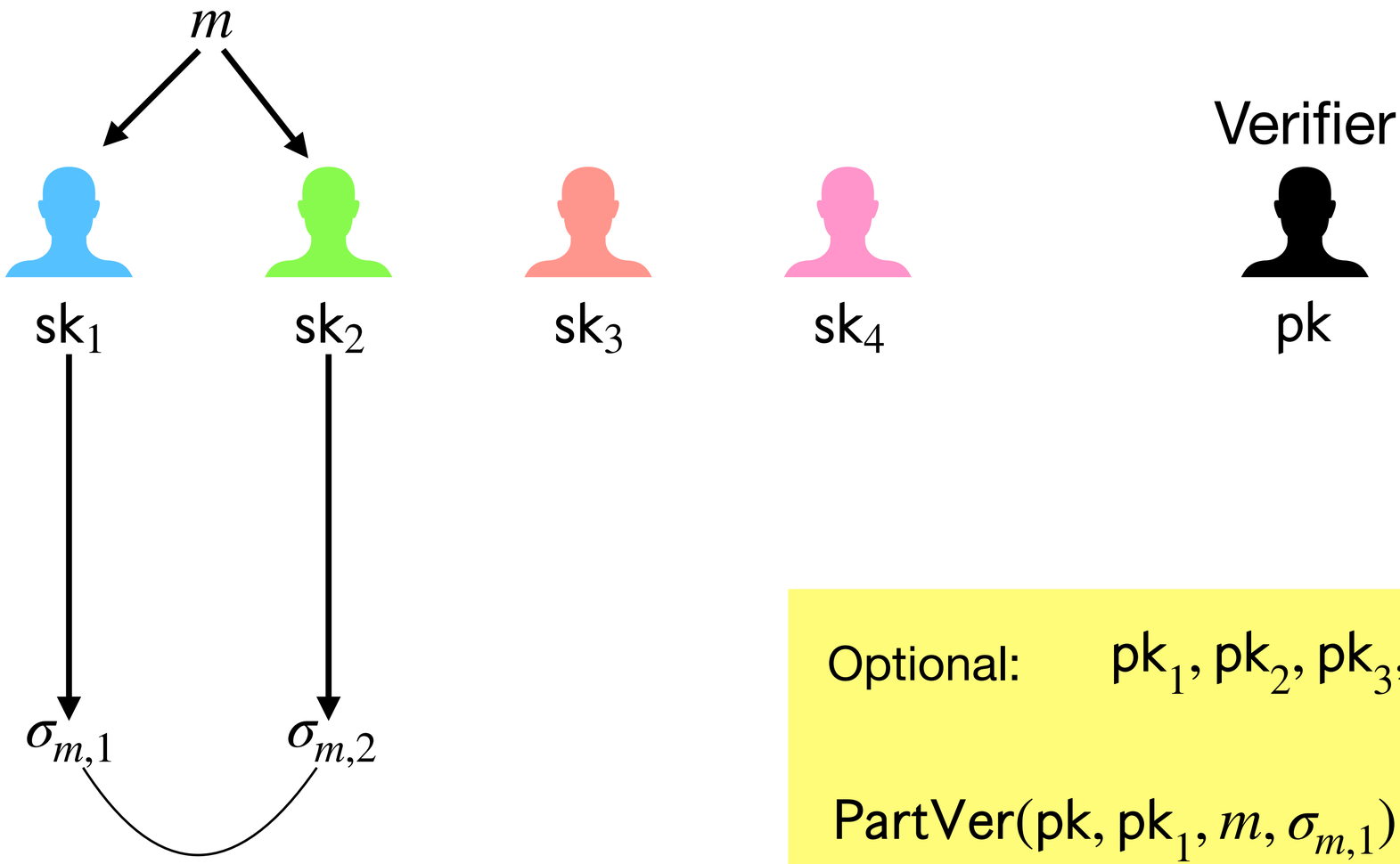


Optional: $\mathsf{pk}_1, \mathsf{pk}_2, \mathsf{pk}_3, \mathsf{pk}_4$

PartVer(pk, pk_1, m, $\sigma_{m,1}$) $\rightarrow$ 0/1

Threshold Signatures

Definition

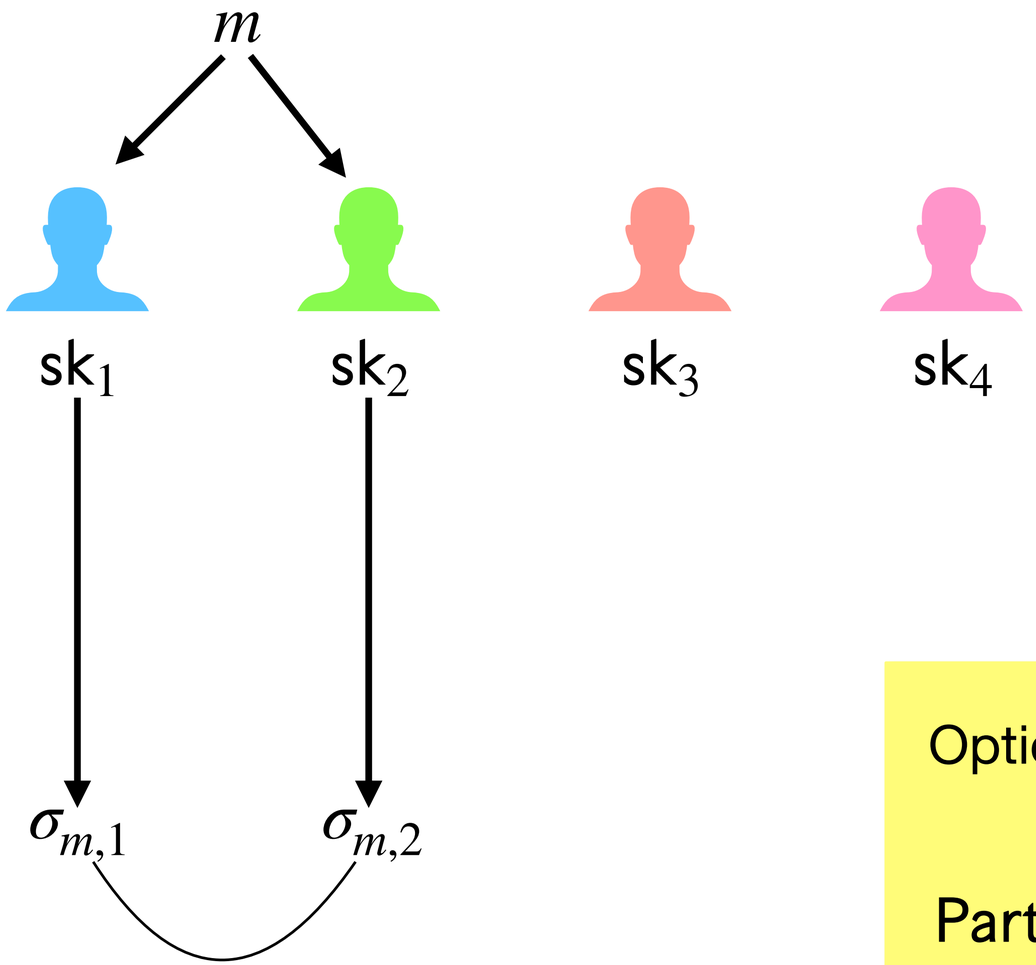


Optional: $\mathsf{pk}_1, \mathsf{pk}_2, \mathsf{pk}_3, \mathsf{pk}_4$

$\mathsf{PartVer}(\mathsf{pk}, \mathsf{pk}_1, m, \sigma_{m,1}) \rightarrow 0/1$

Threshold Signatures

Definition



Verifier

$\mathsf{KeyGen}(1^\lambda, t, n) \rightarrow$
$t = 2,\ n = 4$

pk

$\mathsf{Ver}(\mathsf{pk}, m, \Sigma_m) \rightarrow 0/1$

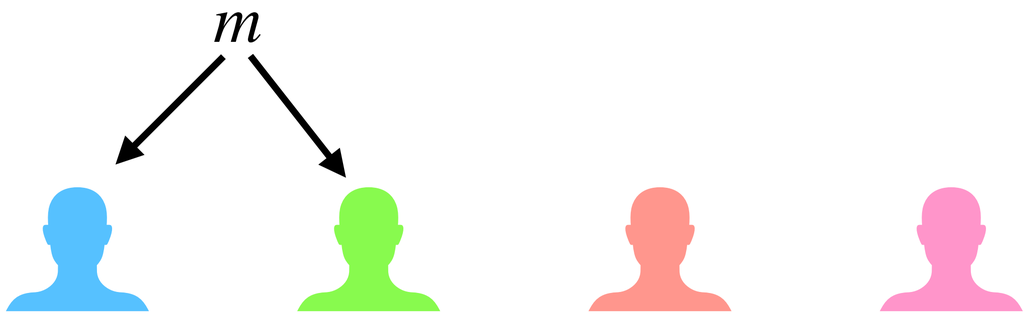
$\mathsf{Comb}(\mathsf{pk}, m, \sigma_{m,1}, \sigma_{m,2}) \rightarrow \Sigma_m$

Optional: $\mathsf{pk}_1, \mathsf{pk}_2, \mathsf{pk}_3, \mathsf{pk}_4$

$\mathsf{PartVer}(\mathsf{pk}, \mathsf{pk}_1, m, \sigma_{m,1}) \rightarrow 0/1$

Threshold Signatures

Correctness



Verifier

$\mathsf{KeyGen}(1^\lambda, t, n) \rightarrow$
$t = 2,\ n = 4$

pk

$\mathsf{Ver}(\mathsf{pk}, m, \Sigma_m) \rightarrow 0/1$

$\mathsf{PartSign}(\mathsf{pk}, \mathsf{sk}_1, m)$

$\sigma_{m,1}$ $\sigma_{m,2}$

$\mathsf{Comb}(\mathsf{pk}, m, \sigma_{m,1}, \sigma_{m,2}) \rightarrow \Sigma_m$

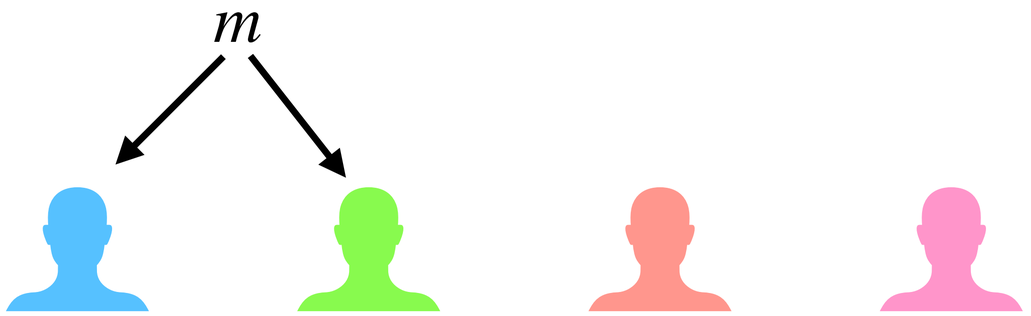
Honestly generated $\sigma_{m,1}, \sigma_{m,2}$
AND
$\mathsf{Comb}(\mathsf{pk}, m, \sigma_{m,1}, \sigma_{m,2}) \rightarrow \Sigma_m$
Then, $\mathsf{Ver}(\mathsf{pk}, m, \Sigma_m) \rightarrow 1$

Optional: $\mathsf{pk}_1, \mathsf{pk}_2, \mathsf{pk}_3, \mathsf{pk}_4$

$\mathsf{PartVer}(\mathsf{pk}, \mathsf{pk}_1, m, \sigma_{m,1}) \rightarrow 0/1$

Threshold Signatures

Correctness



Verifier

$\mathsf{KeyGen}(1^\lambda, t, n) \rightarrow$

$t = 2,\ n = 4$

sk_1

pk

$\mathsf{Ver}(\mathsf{pk}, m, \Sigma_m) \rightarrow 0/1$

$\mathsf{PartSign}(\mathsf{pk}, \mathsf{sk}_1, m)$

$\sigma_{m,1}$

Honestly generated $\sigma_{m,1}, \sigma_{m,2}$

AND

$\mathsf{Comb}(\mathsf{pk}, m, \sigma_{m,1}, \sigma_{m,2}) \rightarrow \Sigma_m$

Then, $\mathsf{Ver}(\mathsf{pk}, m, \Sigma_m) \rightarrow 1$

Honestly generated $\sigma_{m,1}$,

Then,

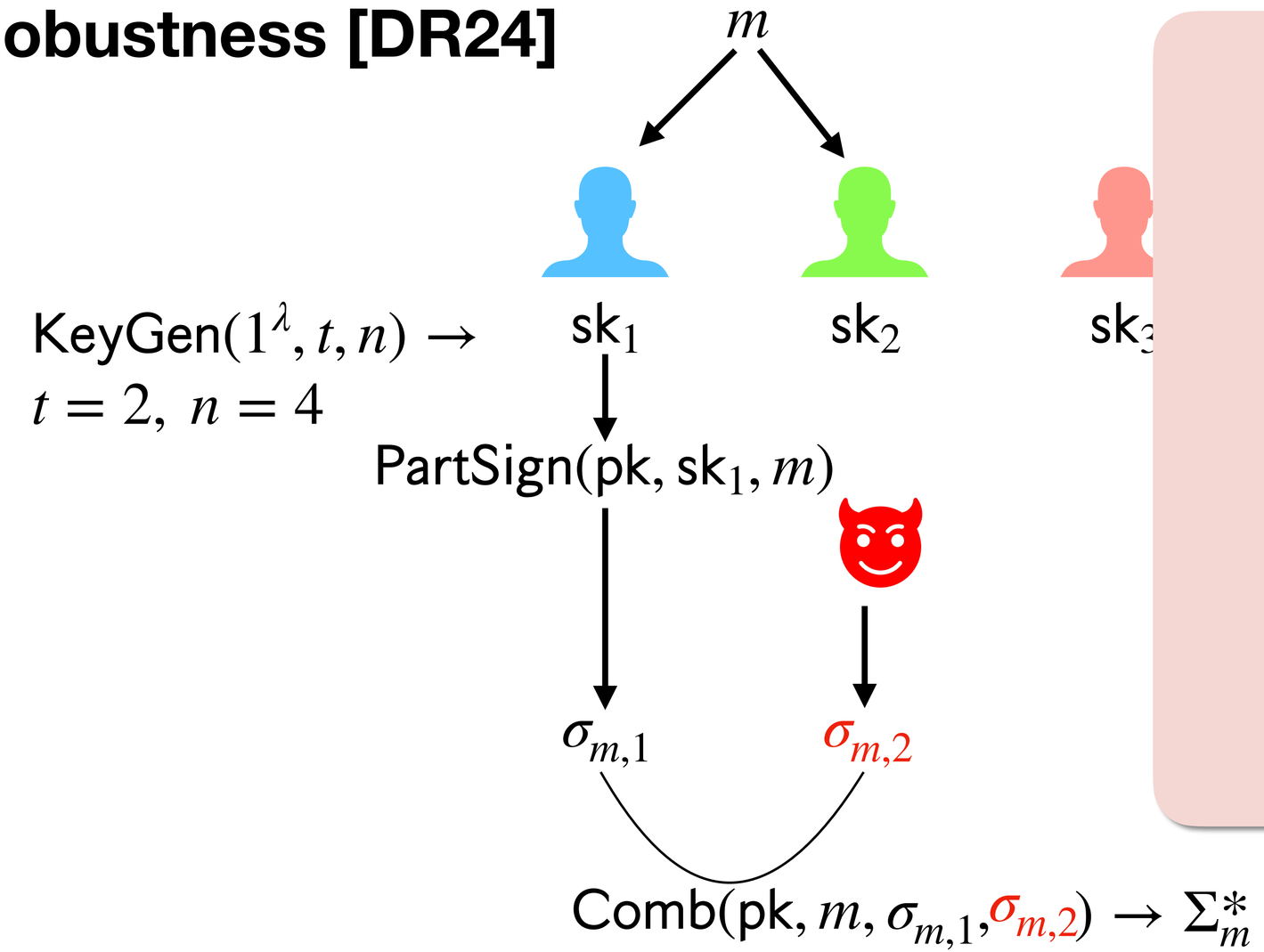
$\mathsf{PartVer}(\mathsf{pk}, \mathsf{pk}_1, m, \sigma_{m,1}) \rightarrow 1$

Optional: $\mathsf{pk}_1, \mathsf{pk}_2, \mathsf{pk}_3, \mathsf{pk}_4$

$\mathsf{PartVer}(\mathsf{pk}, \mathsf{pk}_1, m, \sigma_{m,1}) \rightarrow 0/1$

Threshold Signatures

Robustness [DR24]

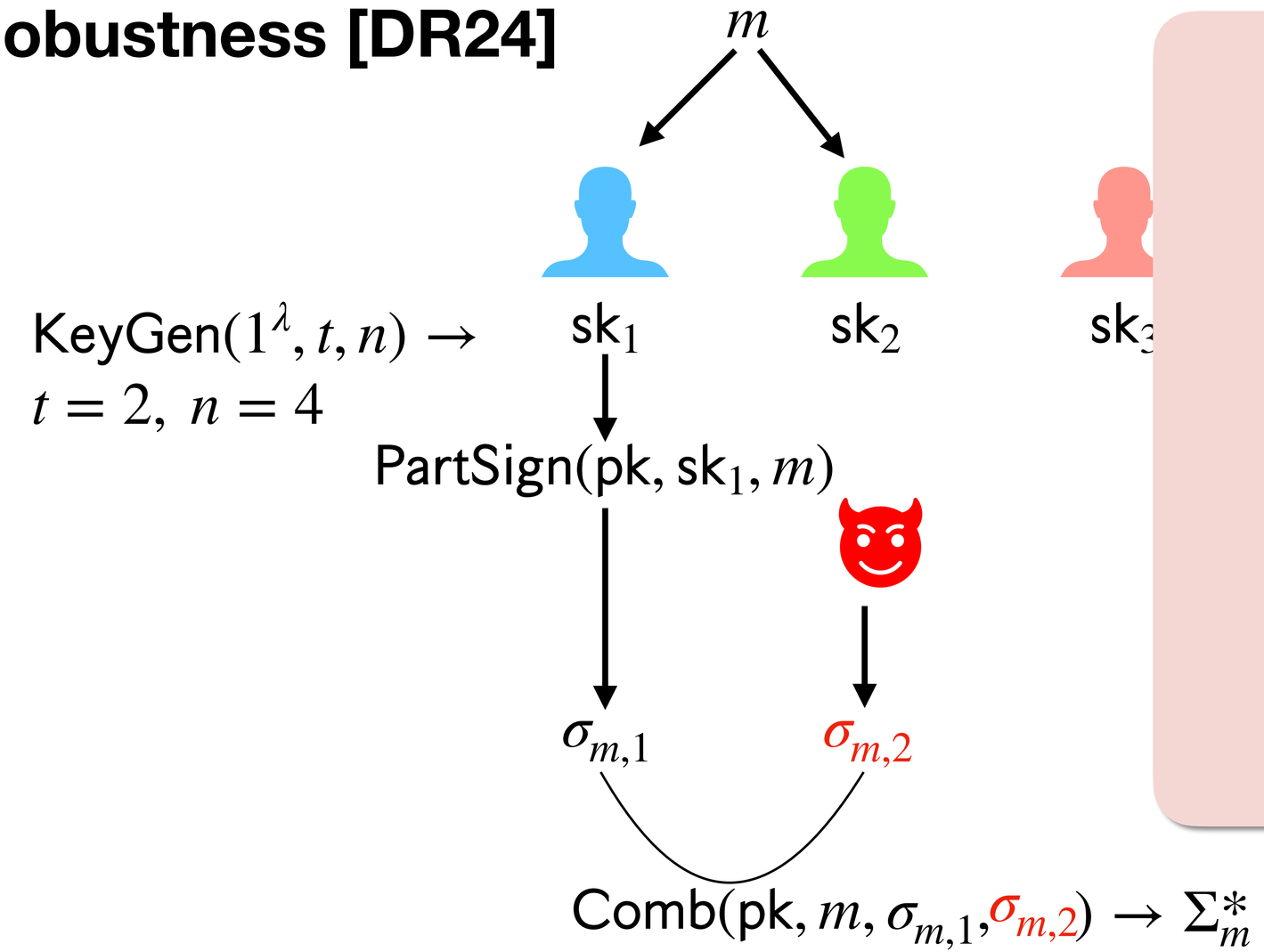


Honestly generated $\sigma_{m,1}$,

$\mathsf{PartVer}(\mathsf{pk}, \mathsf{pk}_1, m, \sigma_{m,1}) \rightarrow 1$

Threshold Signatures

Robustness [DR24]



Honestly generated $\sigma_{m,1}$,

$\mathsf{PartVer}(\mathsf{pk}, \mathsf{pk}_1, m, \sigma_{m,1}) \rightarrow 1$

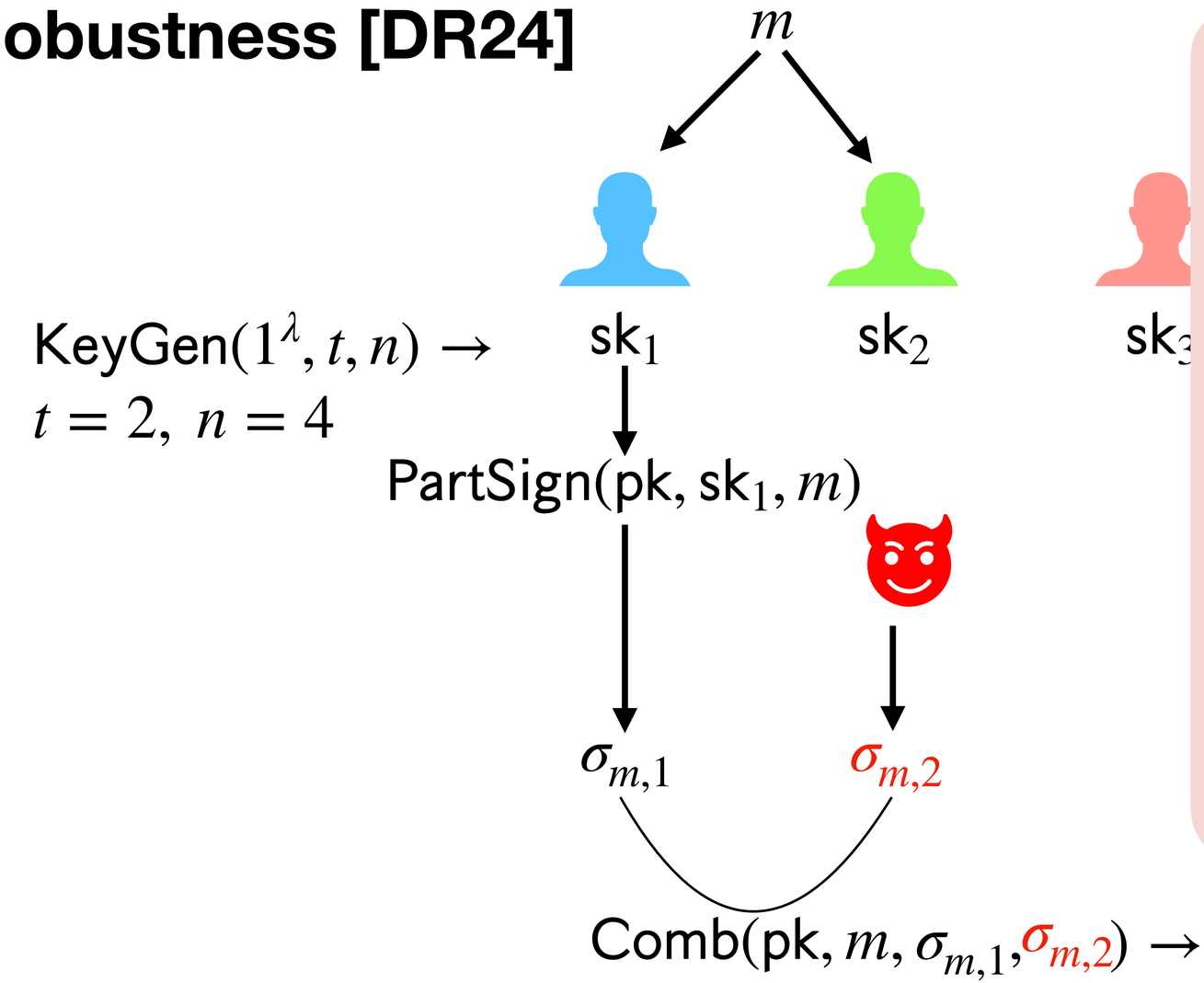
AND

Maliciously generated $\sigma_{m,2}$,

$\mathsf{PartVer}(\mathsf{pk}, \mathsf{pk}_2, m, \sigma_{m,2}) \rightarrow 1$

Threshold Signatures

Robustness [DR24]



Honestly generated $\sigma_{m,1}$,

$\mathsf{PartVer}(\mathsf{pk}, \mathsf{pk}_1, m, \sigma_{m,1}) \rightarrow 1$

AND

Maliciously generated $\sigma_{m,2}$,

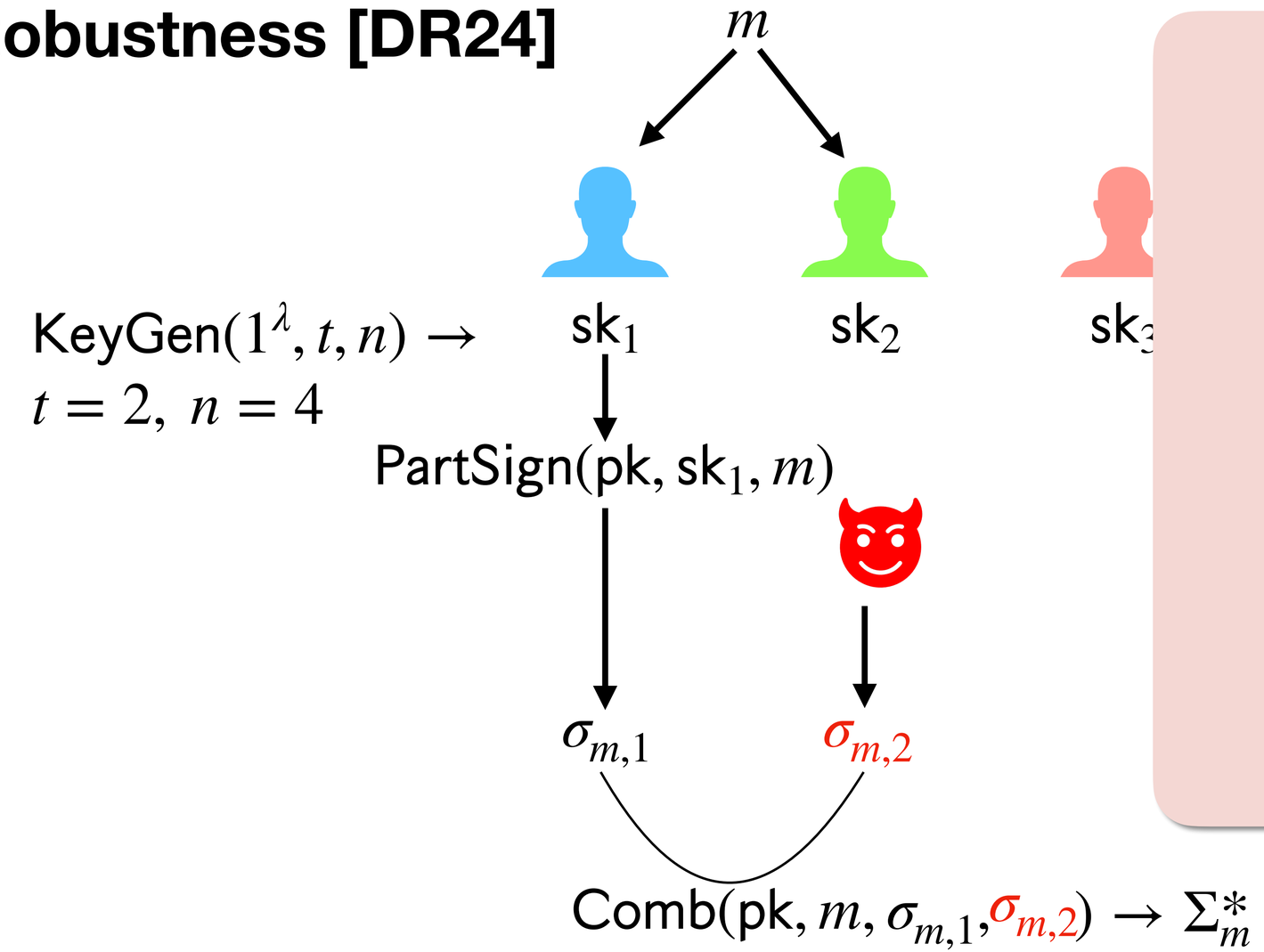
$\mathsf{PartVer}(\mathsf{pk}, \mathsf{pk}_2, m, \sigma_{m,2}) \rightarrow 1$

AND

$\mathsf{Comb}(\mathsf{pk}, m, \sigma_{m,1}, \sigma_{m,2}) \rightarrow \Sigma^*_m$

Threshold Signatures

Robustness [DR24]



Honestly generated $\sigma_{m,1}$,

$\mathsf{PartVer}(\mathsf{pk}, \mathsf{pk}_1, m, \sigma_{m,1}) \rightarrow 1$

AND

Maliciously generated $\sigma_{m,2}$,

$\mathsf{PartVer}(\mathsf{pk}, \mathsf{pk}_2, m, \sigma_{m,2}) \rightarrow 1$

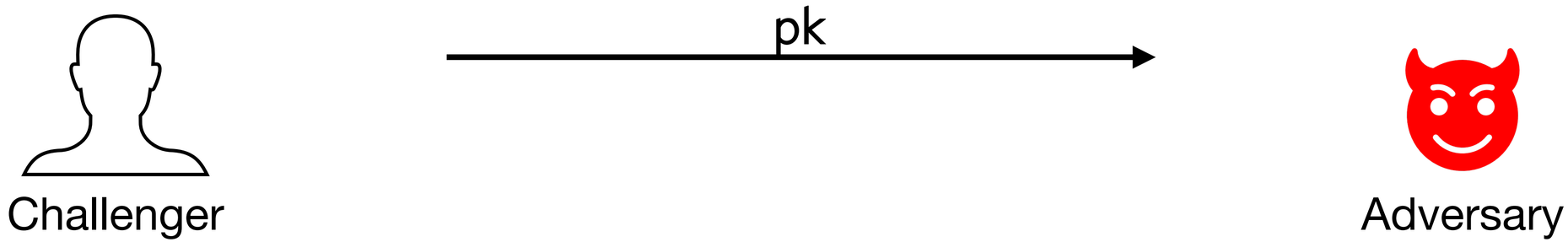
AND

$\mathsf{Comb}(\mathsf{pk}, m, \sigma_{m,1}, \sigma_{m,2}) \rightarrow \Sigma^*_m$

Then, $\mathsf{Ver}(\mathsf{pk}, m, \Sigma^*_m) \rightarrow 1$

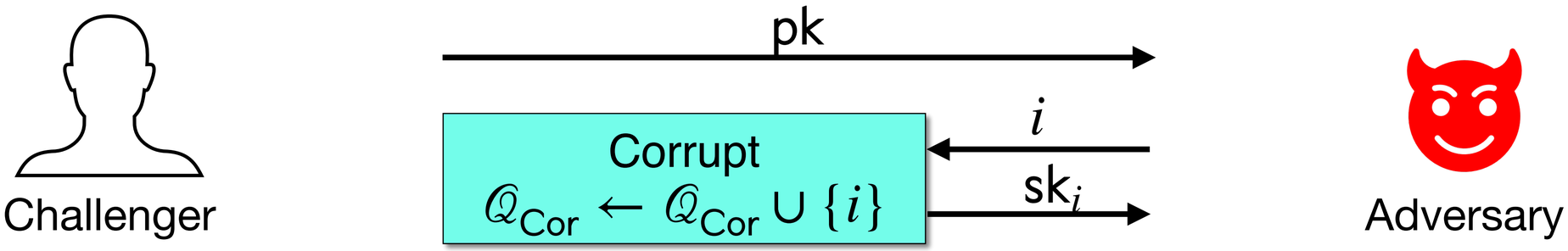
Threshold Signatures

Unforgeability



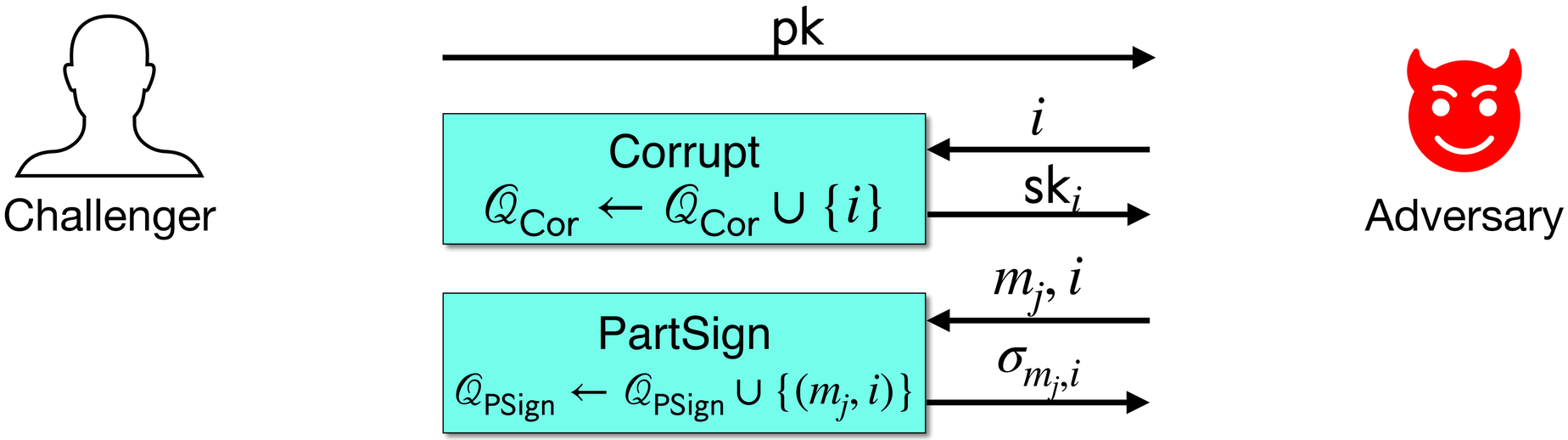
Threshold Signatures

Unforgeability



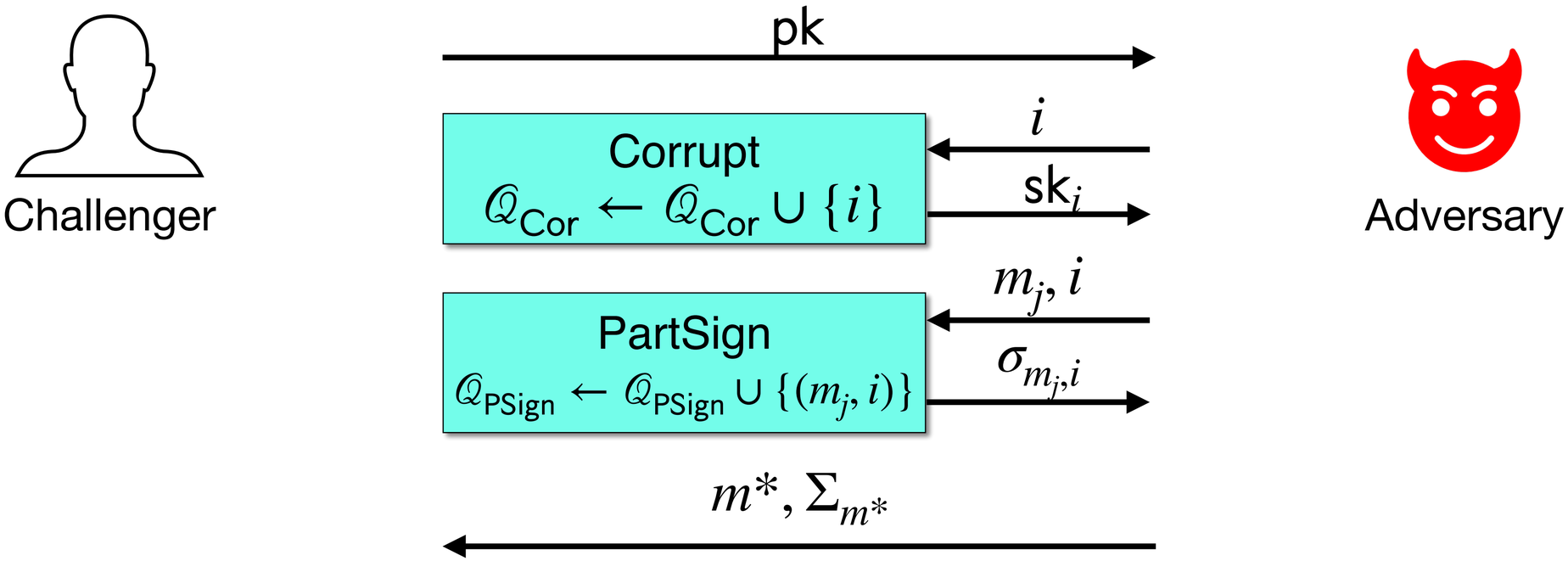
Threshold Signatures

Unforgeability



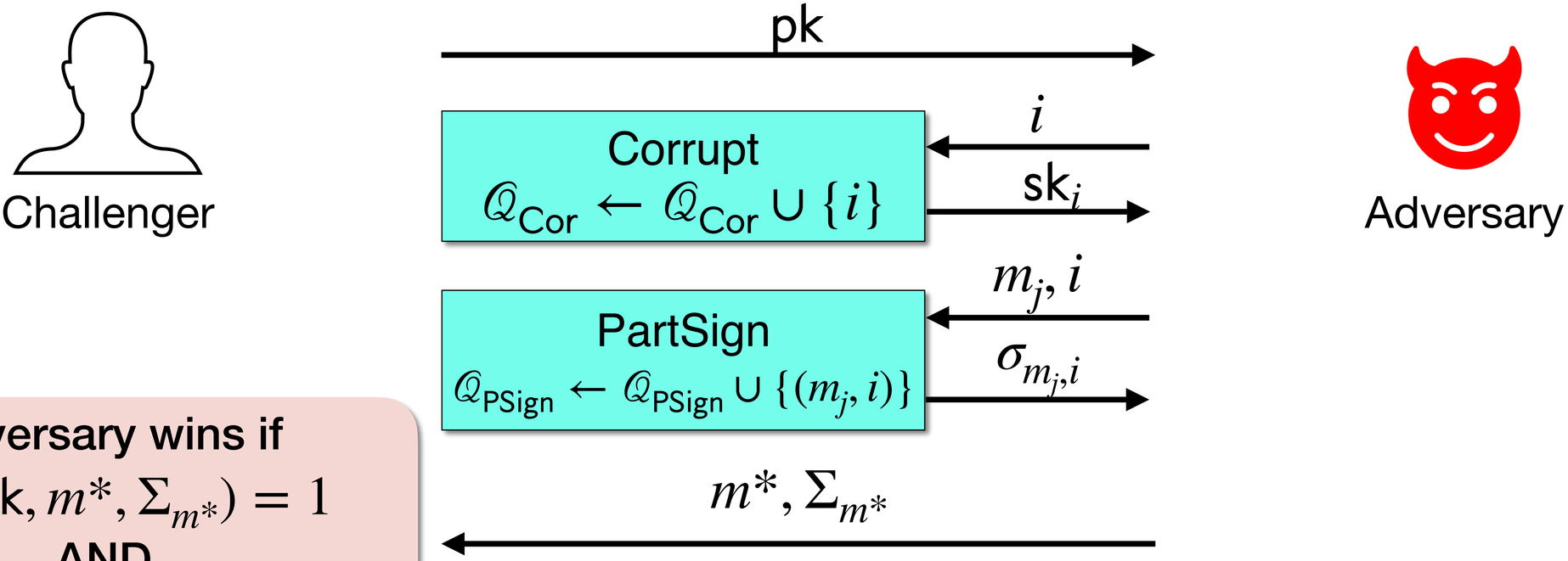
Threshold Signatures

Unforgeability



Threshold Signatures

Unforgeability



Adversary wins if

$$\text{Ver}(\text{pk}, m^*, \Sigma_{m^*}) = 1$$

AND

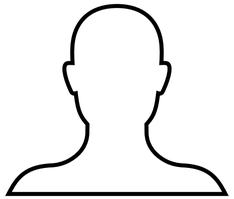
$$|\mathcal{Q}_{\text{Cor}}| < t$$

AND

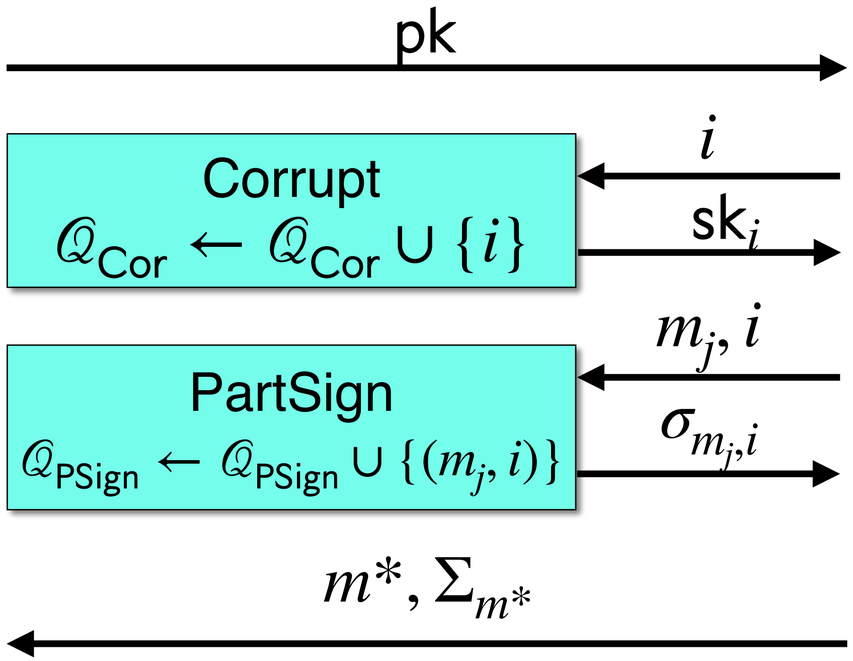
$$(m^*, -) \notin \mathcal{Q}_{\text{PSign}}$$

Threshold Signatures

Unforgeability



Challenger



Adversary

Adversary wins if

$\text{Ver}(\text{pk}, m^*, \Sigma_{m^*}) = 1$

AND

$|\mathcal{Q}_{\text{Cor}}| < t$

AND

$(m^*, -) \notin \mathcal{Q}_{\text{PSign}}$

Pr [Adversary wins]= negl.

Malicious keys?

BUFF Signatures

Malicious keys?

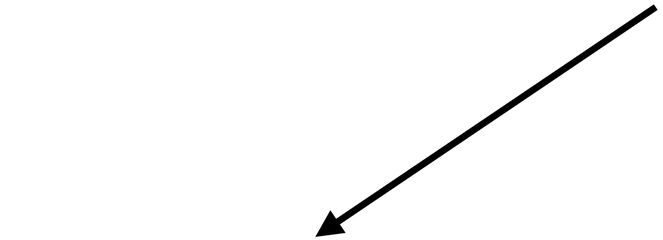
BUFF Signatures

- Digital Signatures with UNF + Beyond UnForgeability Features [CDFFJ21]

Malicious keys?

BUFF Signatures

- Digital Signatures with UNF + Beyond UnForgeability Features [CDFFJ21]

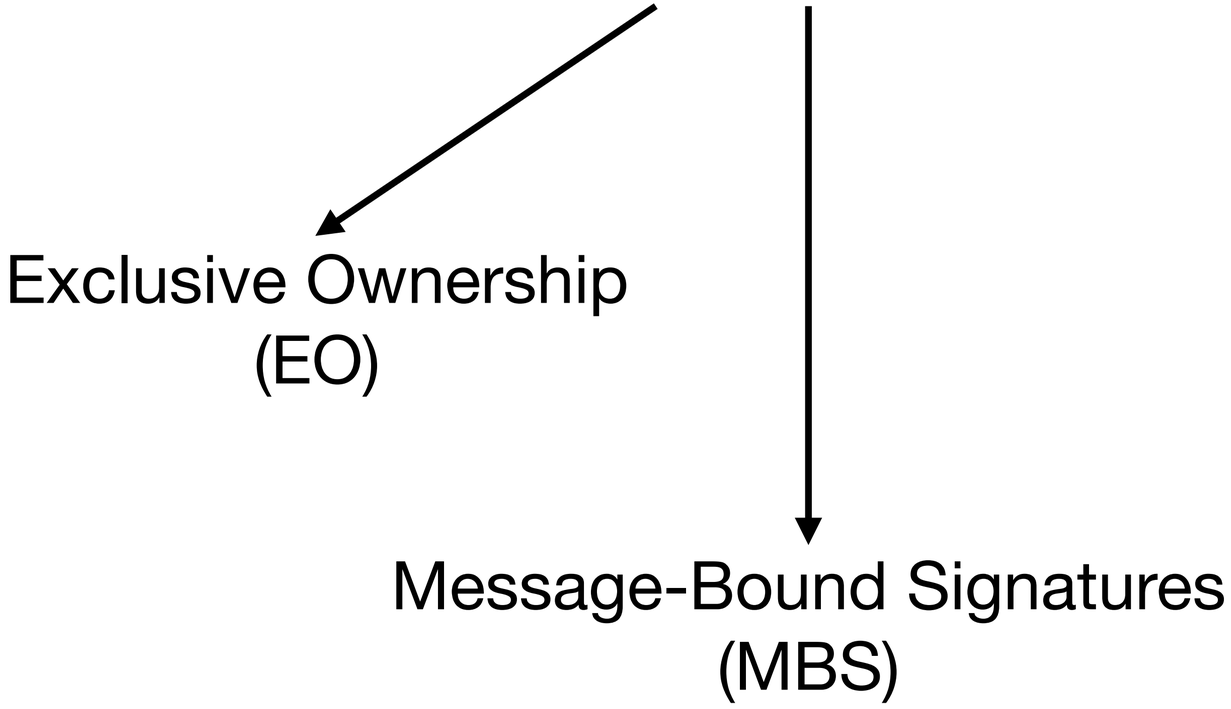


Exclusive Ownership
(EO)

Malicious keys?

BUFF Signatures

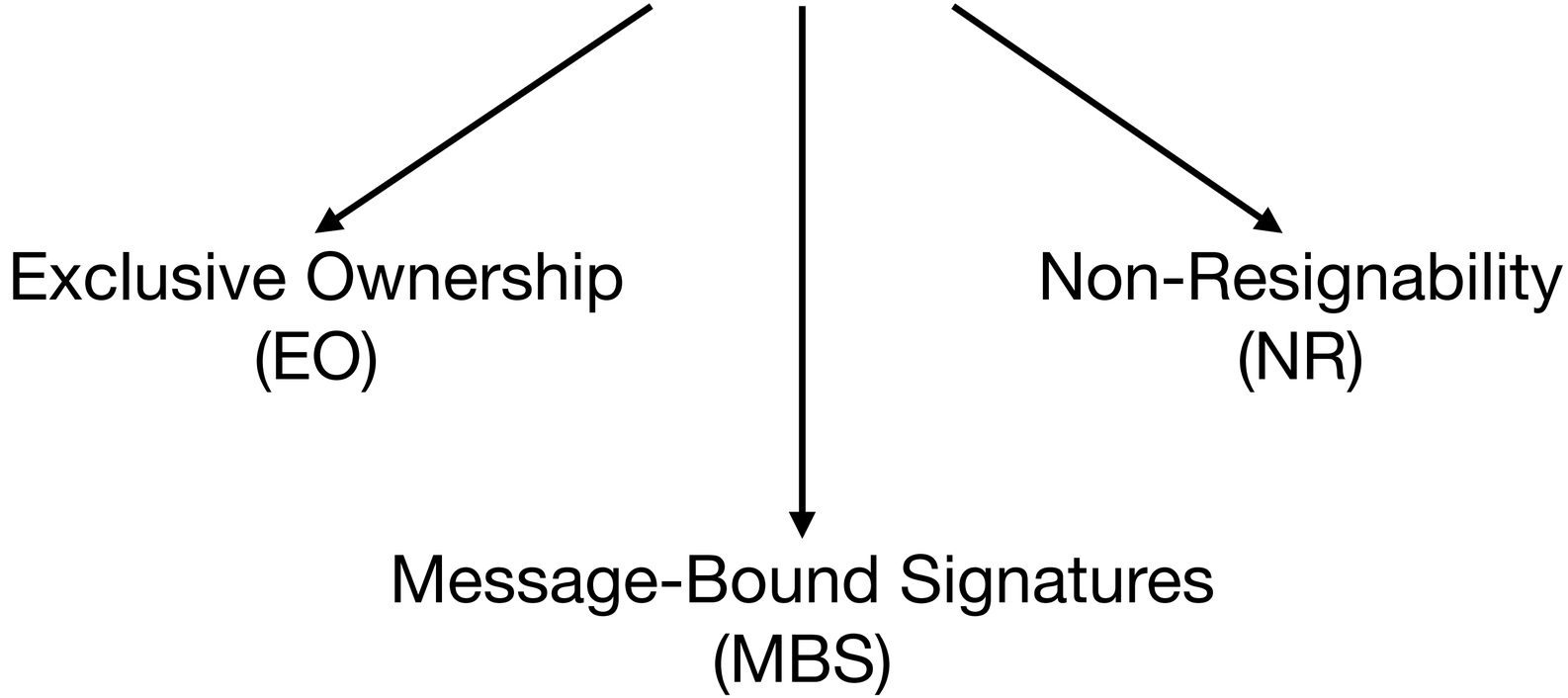
- Digital Signatures with UNF + Beyond UnForgeability Features [CDFFJ21]



Malicious keys?

BUFF Signatures

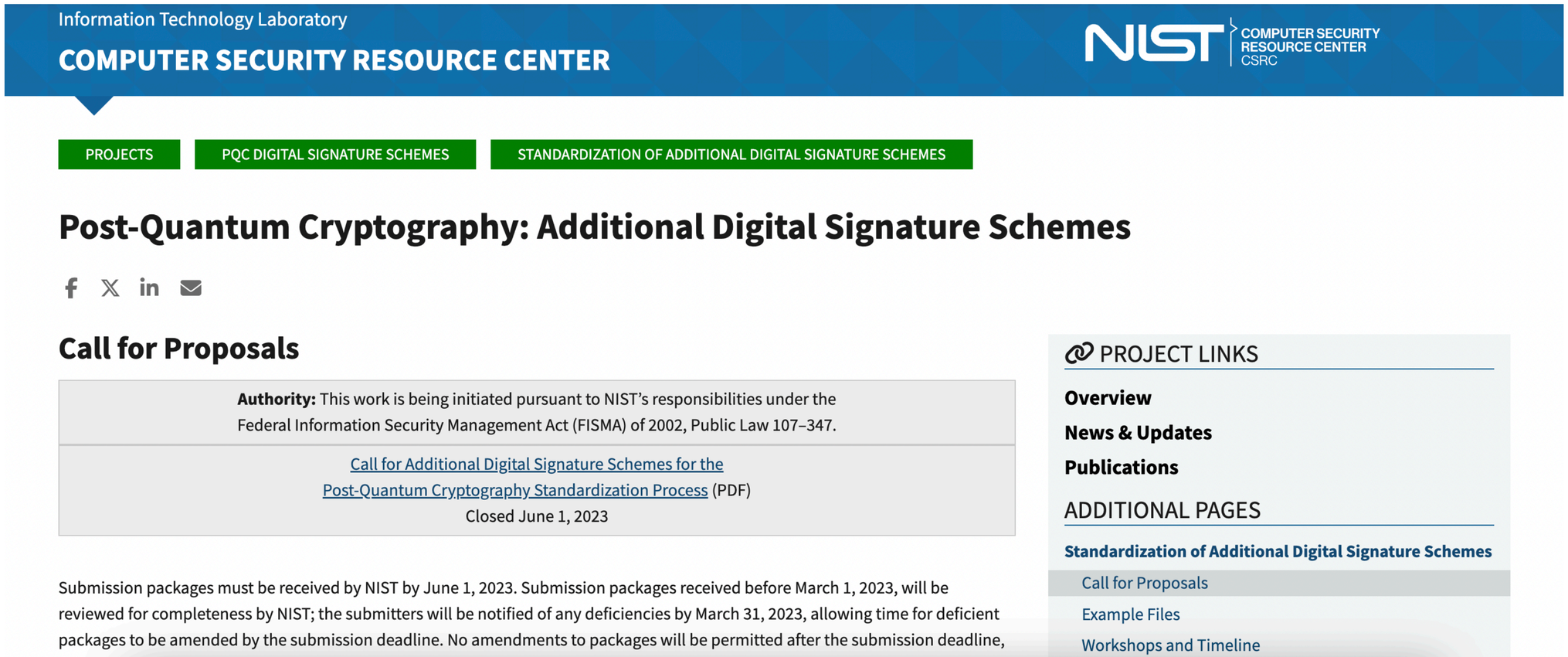
- Digital Signatures with UNF + Beyond UnForgeability Features [CDFFJ21]



Malicious keys?

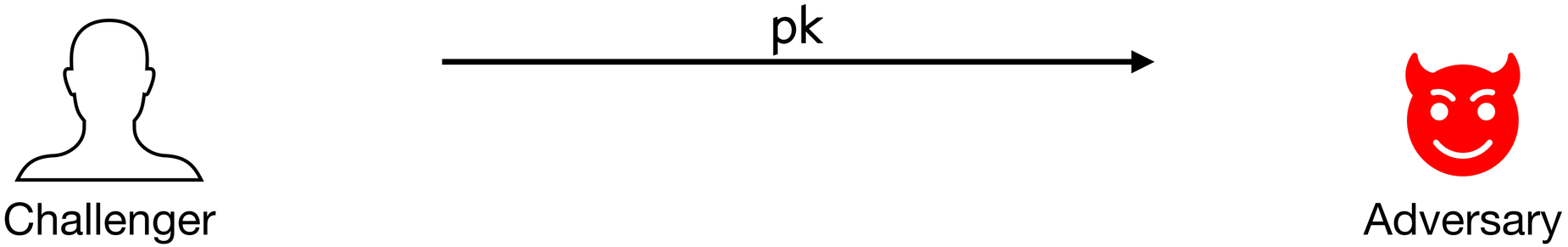
BUFF Signatures

- Digital Signatures with UNF + Beyond UnForgeability Features [CDFFJ21]



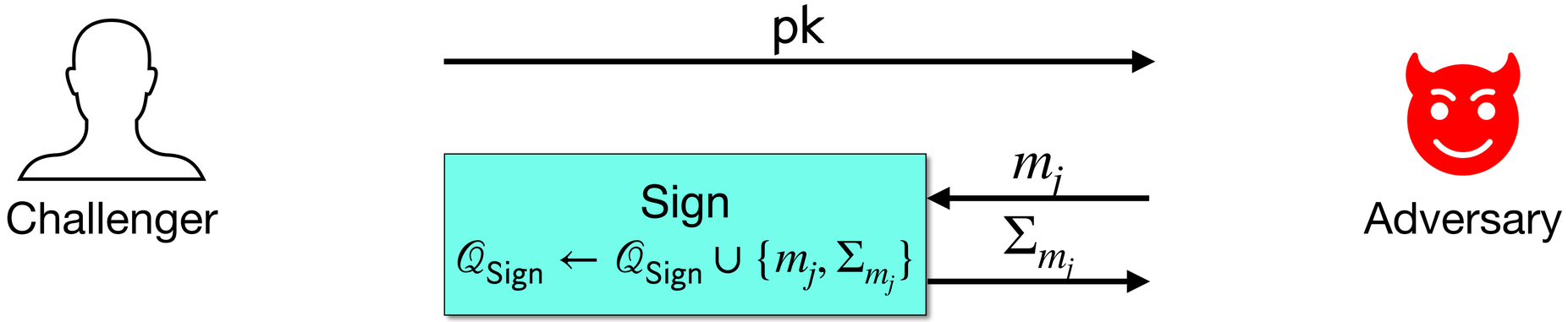
Strong-Conservative Exclusive Ownership

Standard Signatures [CDFFJ21]



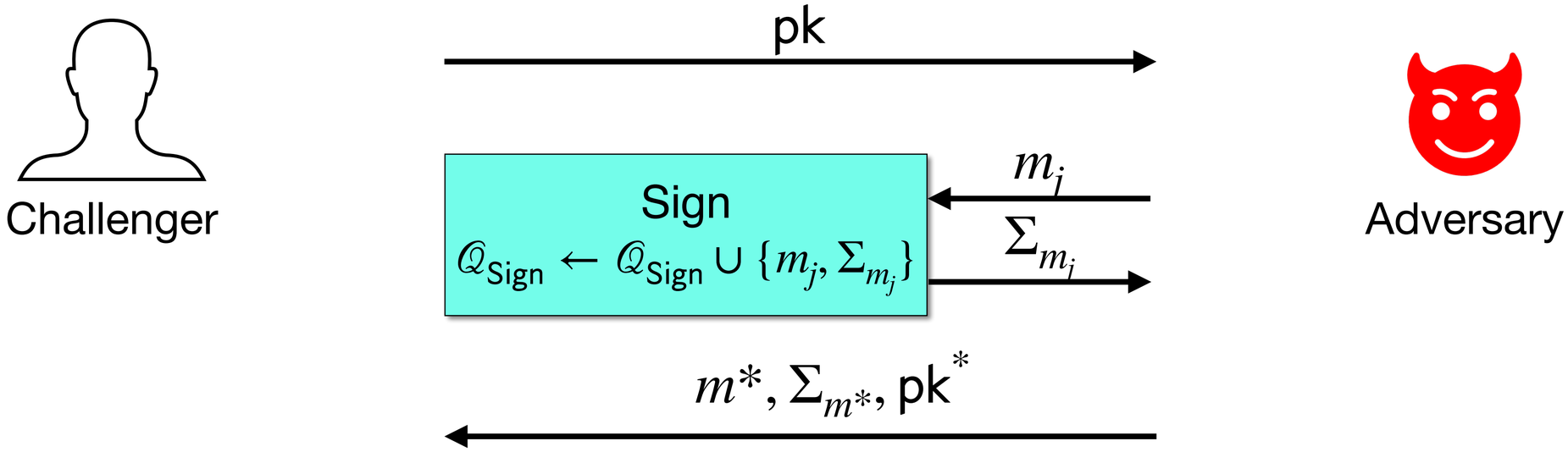
Strong-Conservative Exclusive Ownership

Standard Signatures [CDFFJ21]



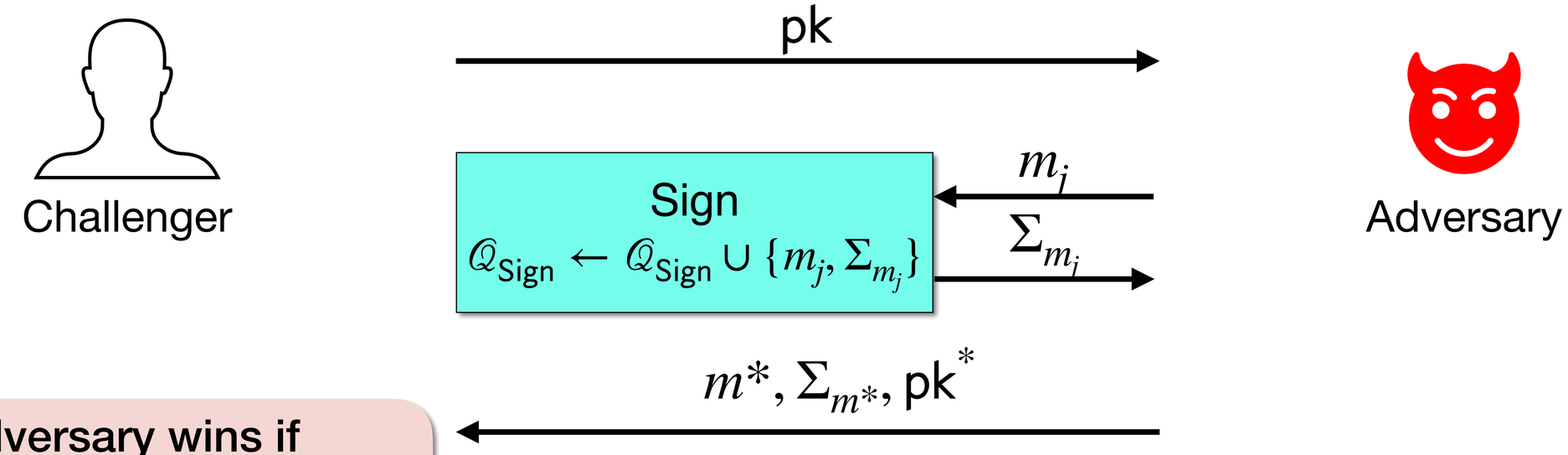
Strong-Conservative Exclusive Ownership

Standard Signatures [CDFFJ21]



Strong-Conservative Exclusive Ownership

Standard Signatures [CDFFJ21]



Adversary wins if

$\text{pk} \neq \text{pk}^*$

AND

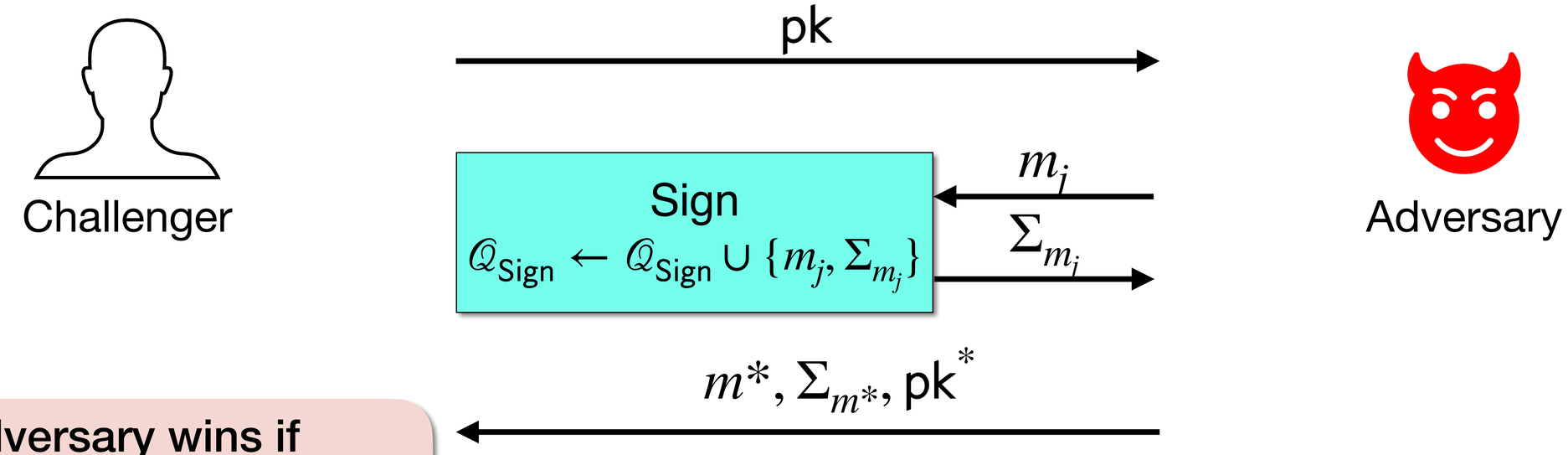
$\text{Ver}(\text{pk}^*, m^*, \Sigma_{m^*}) = 1$

AND

$(m^*, \Sigma_{m^*}) \in \mathcal{Q}_{\text{Sign}}$

Strong-Conservative Exclusive Ownership

Standard Signatures [CDFFJ21]



Adversary wins if

$\text{pk} \neq \text{pk}^*$

AND

$\text{Ver}(\text{pk}^*, m^*, \Sigma_{m^*}) = 1$

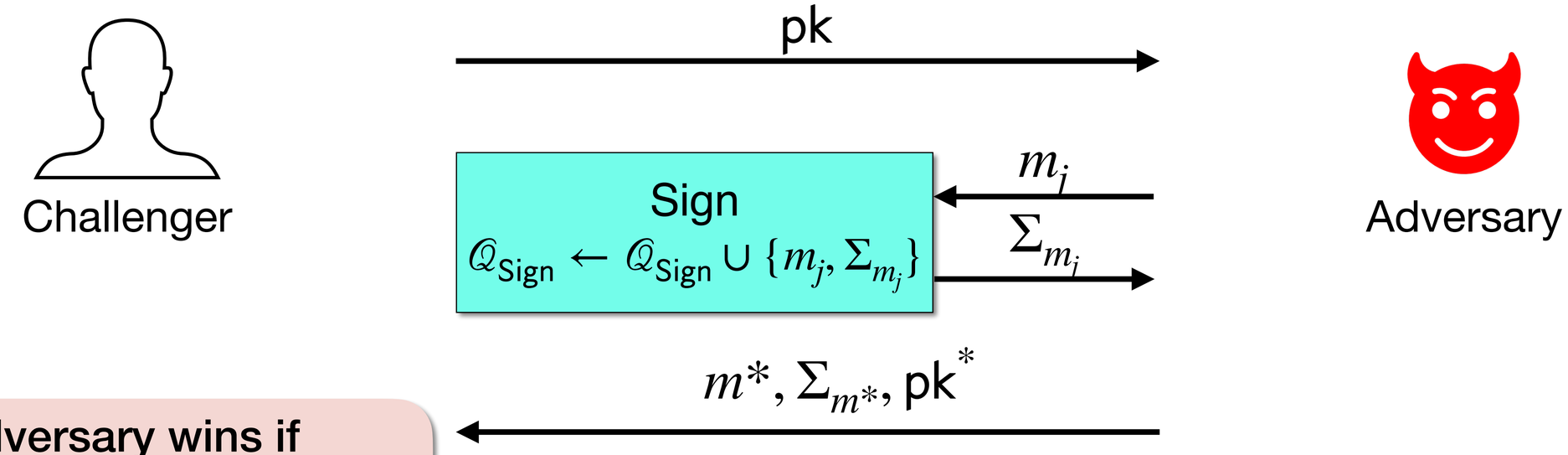
AND

$(m^*, \Sigma_{m^*}) \in \mathcal{Q}_{\text{Sign}}$

Pr [Adversary wins]= negl.

Strong-Destructive Exclusive Ownership

Standard Signatures [CDFFJ21]



Adversary wins if

$\text{pk} \neq \text{pk}^*$

AND

$\text{Ver}(\text{pk}^*, m^*, \Sigma_{m^*}) = 1$

AND

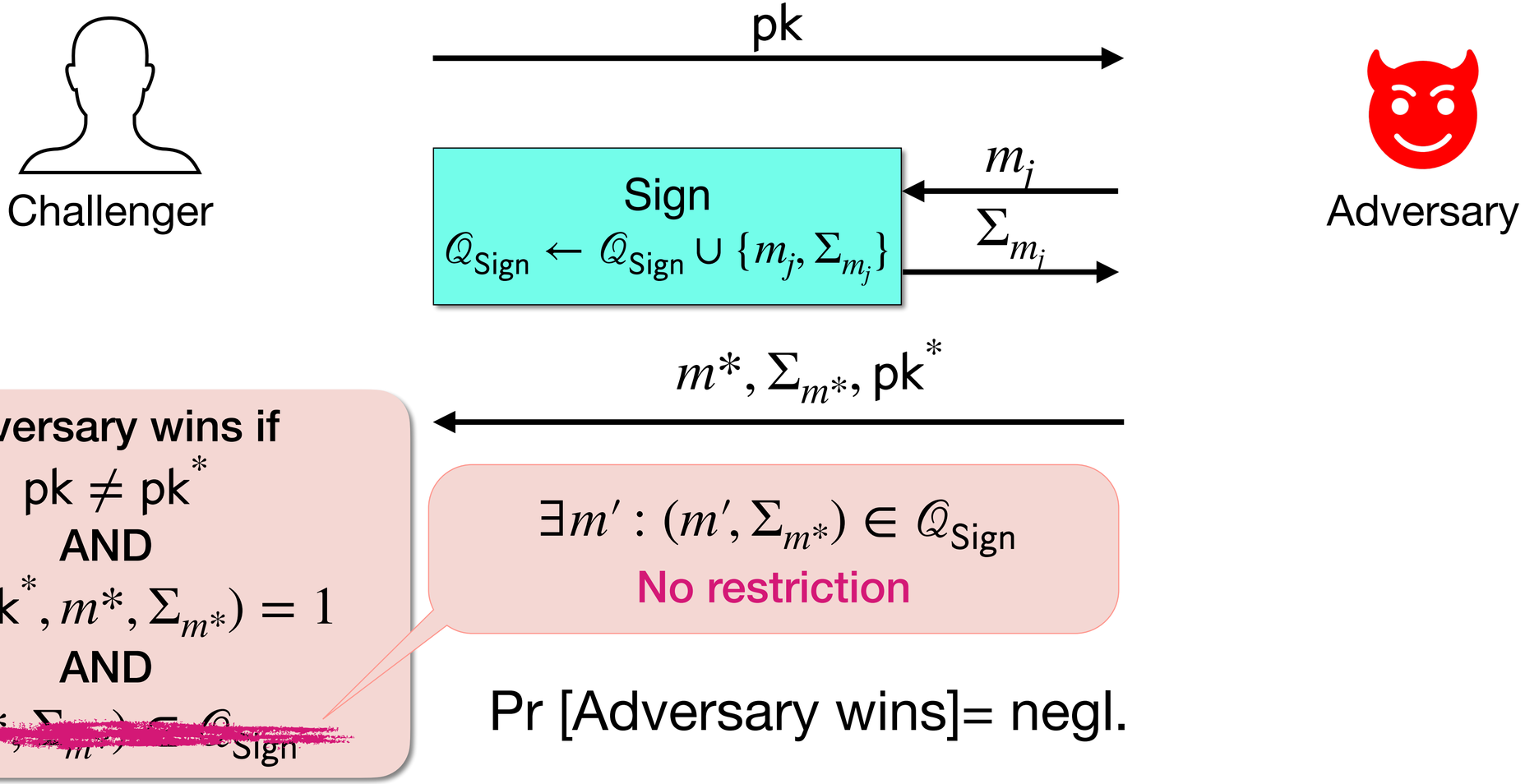
$(m^*, \Sigma_{m^*}) \notin \mathcal{Q}_{\text{Sign}}$

$\exists m' \neq m^* : (m', \Sigma_{m^*}) \in \mathcal{Q}_{\text{Sign}}$

Pr [Adversary wins]= negl.

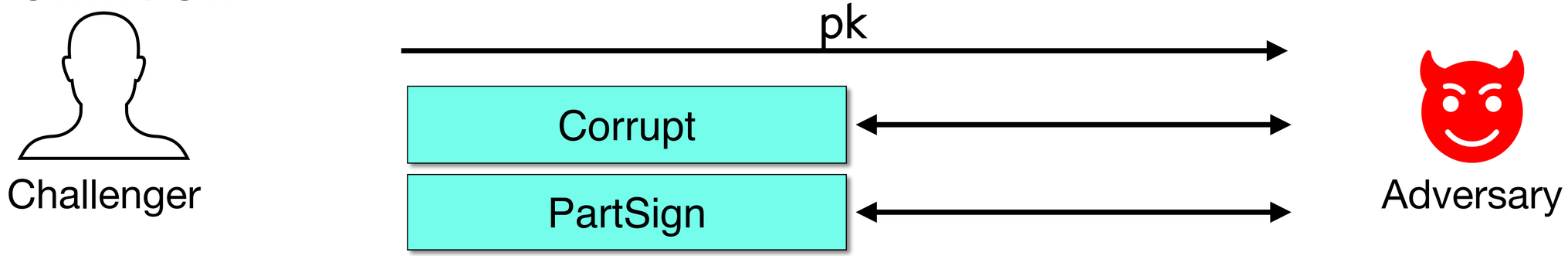
Strong-Universal Exclusive Ownership

Standard Signatures [CDFFJ21]



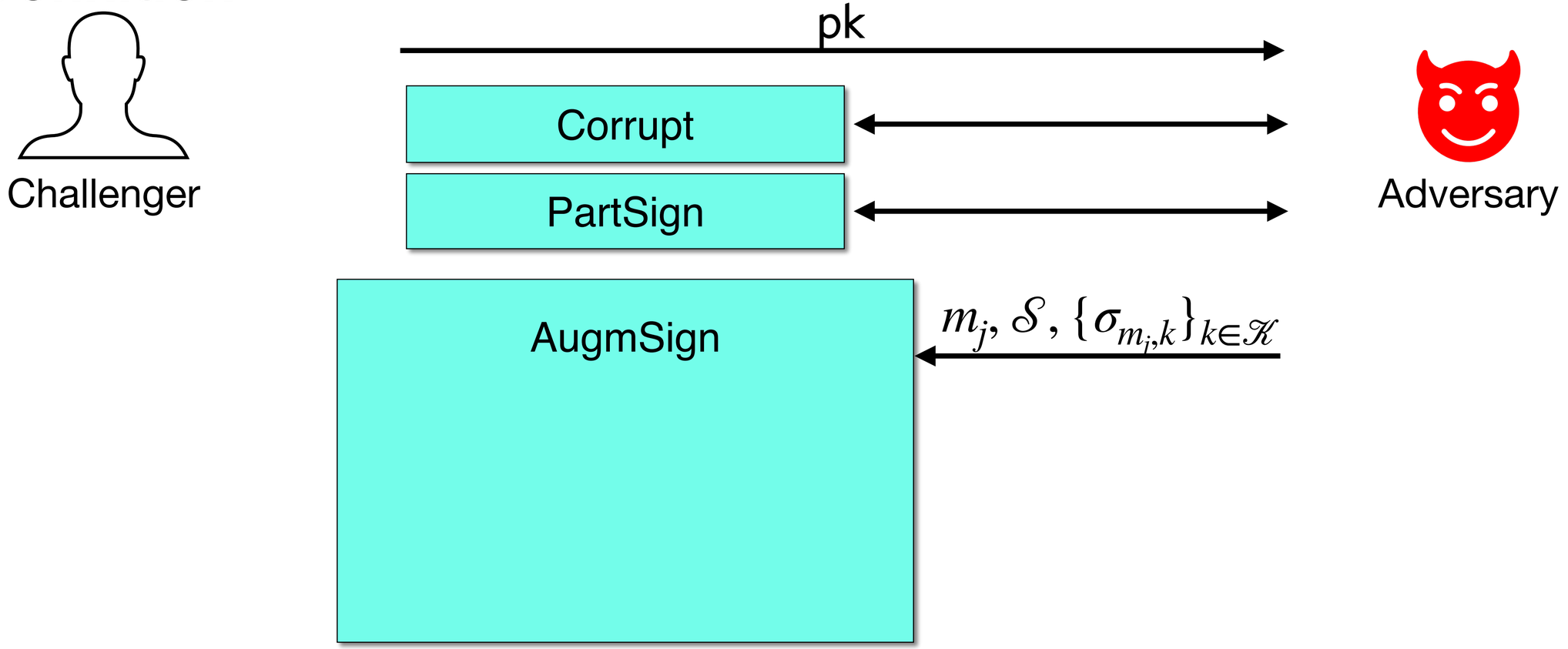
Strong-CEO in Threshold Setting

Our Definition



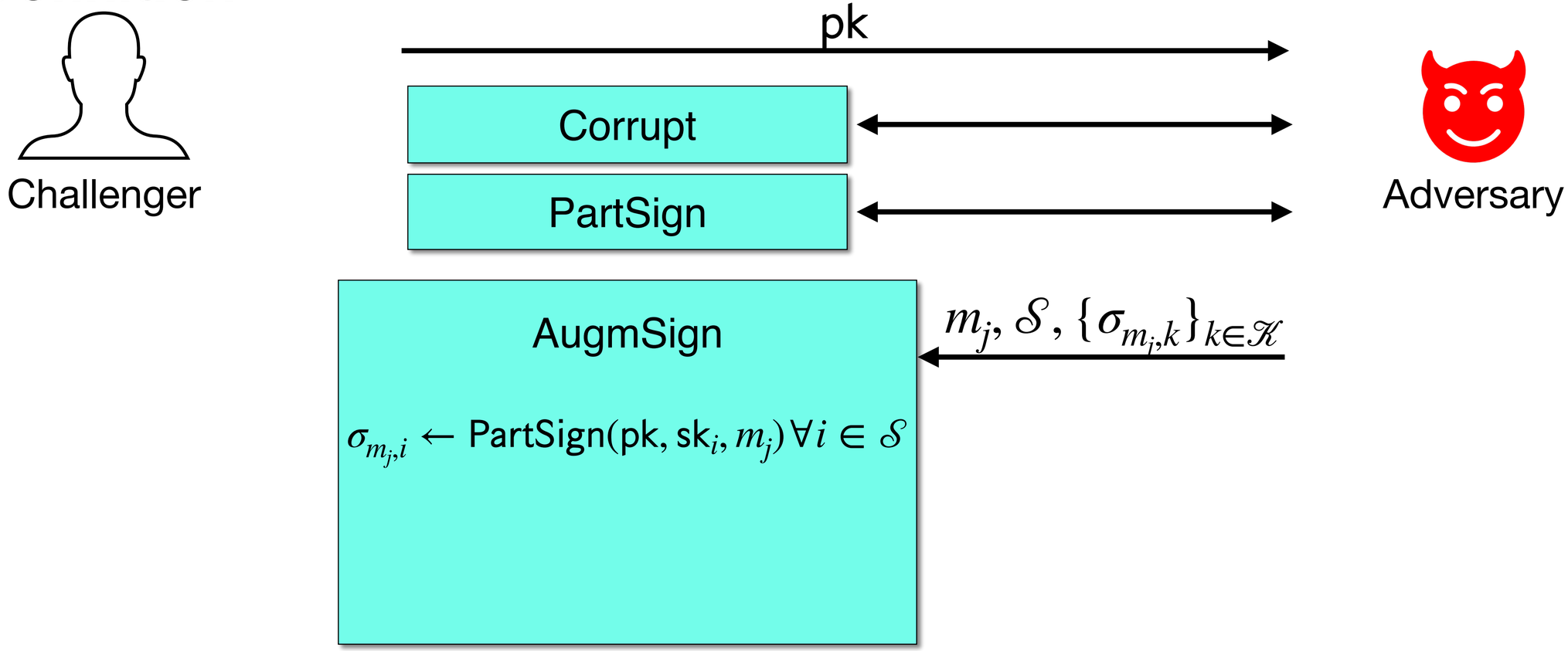
Strong-CEO in Threshold Setting

Our Definition



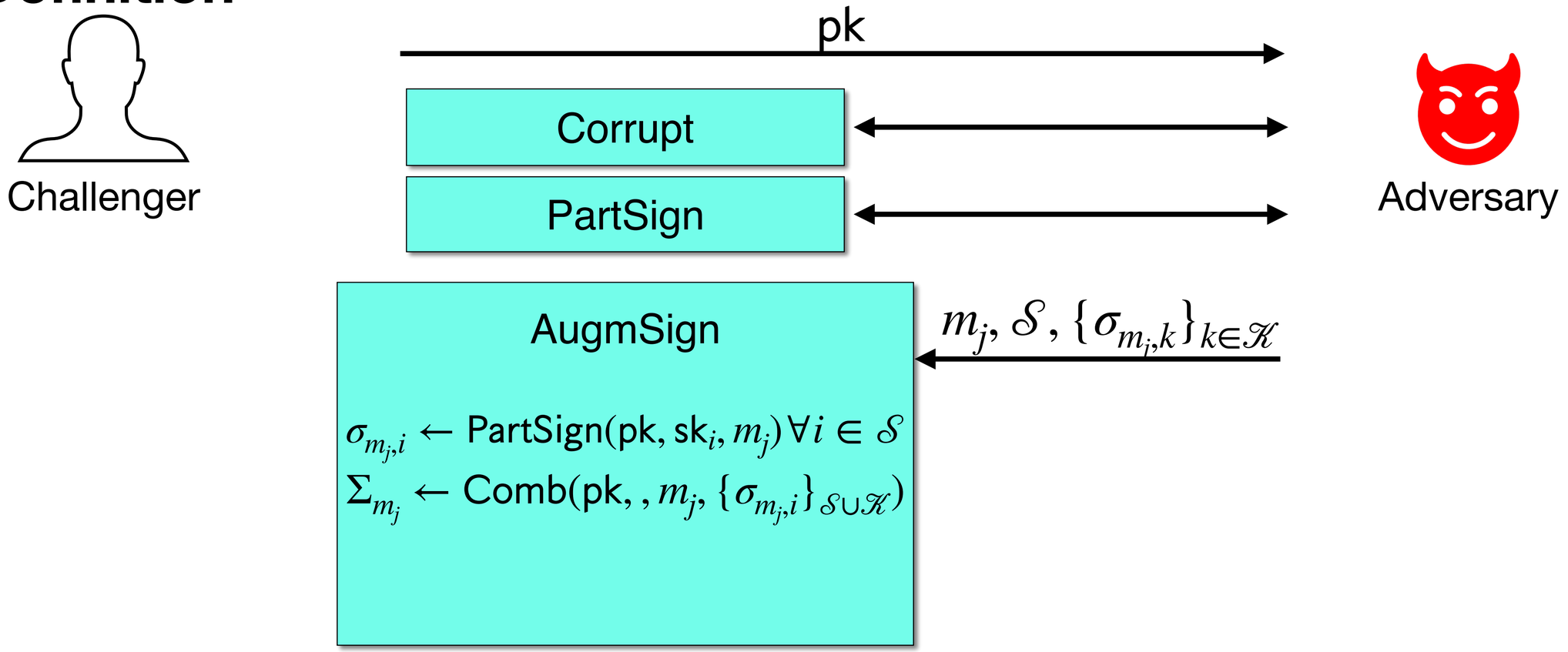
Strong-CEO in Threshold Setting

Our Definition



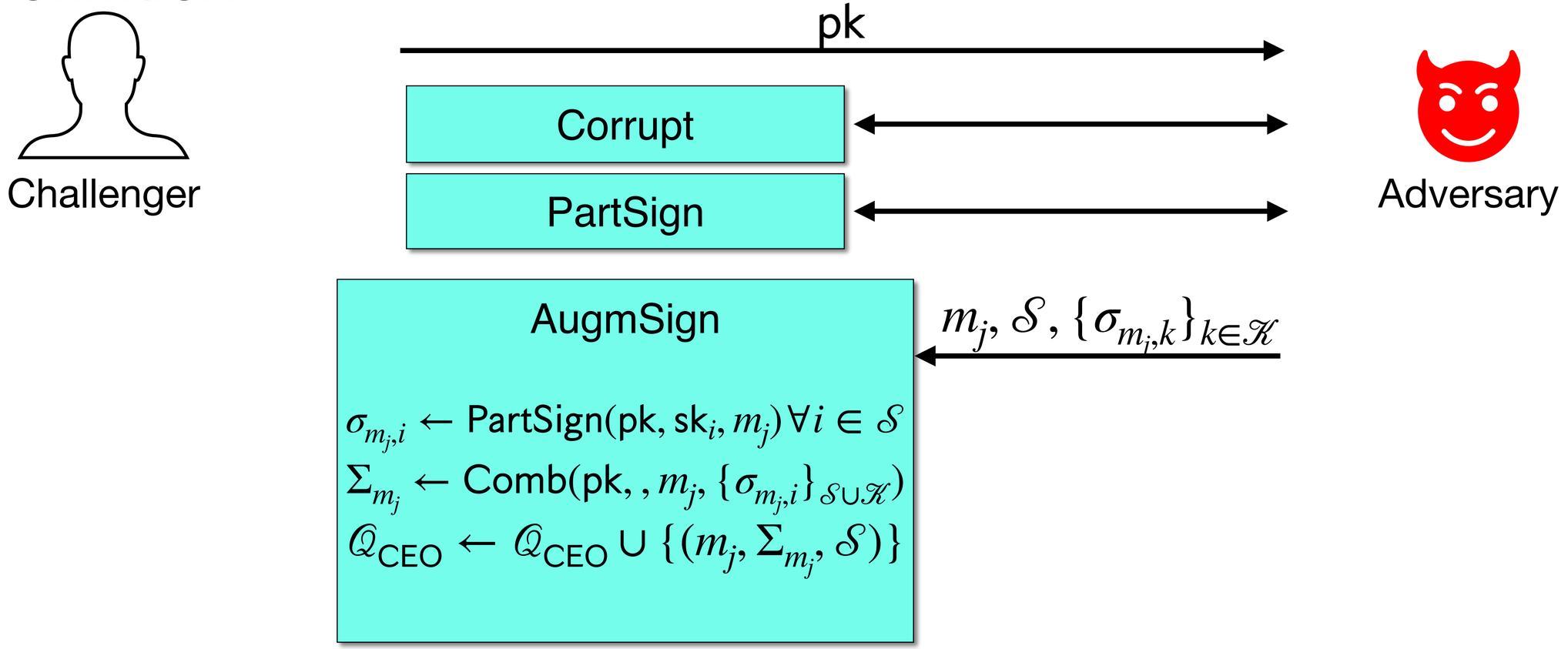
Strong-CEO in Threshold Setting

Our Definition



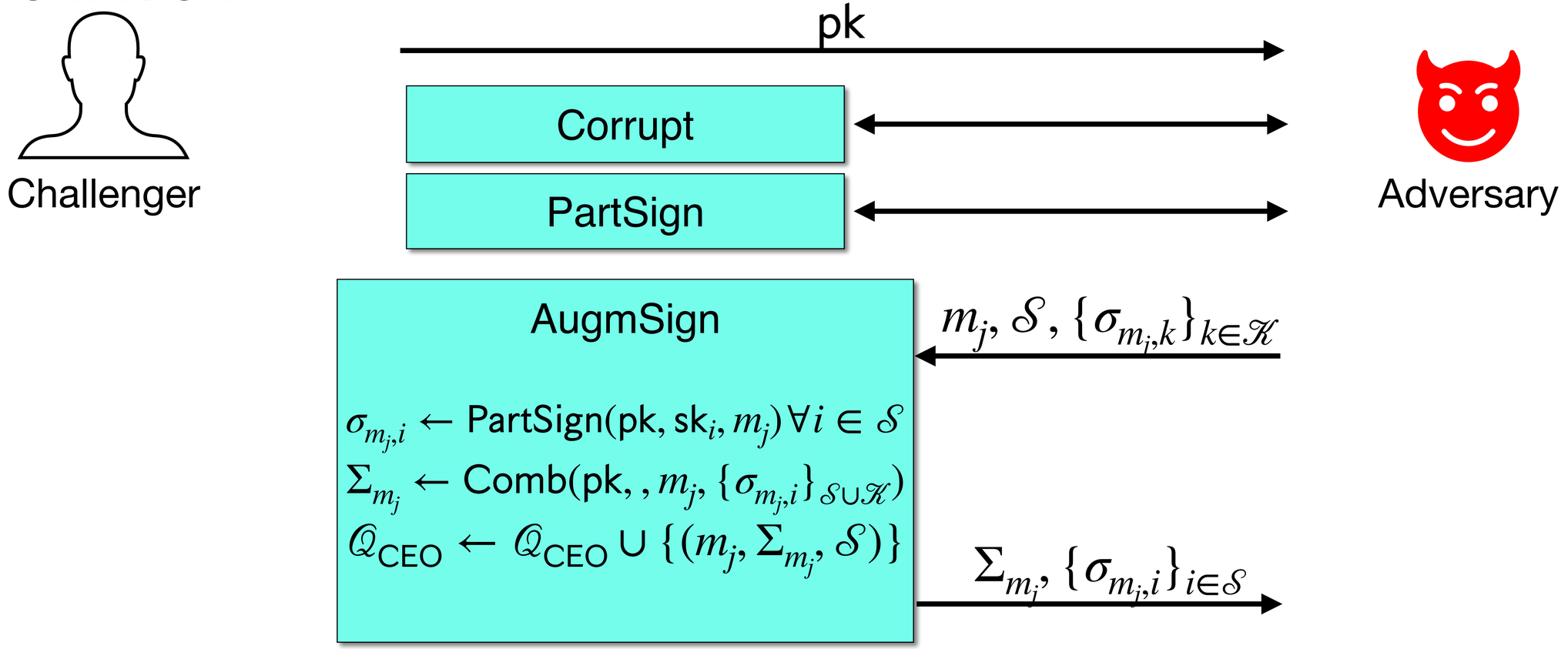
Strong-CEO in Threshold Setting

Our Definition



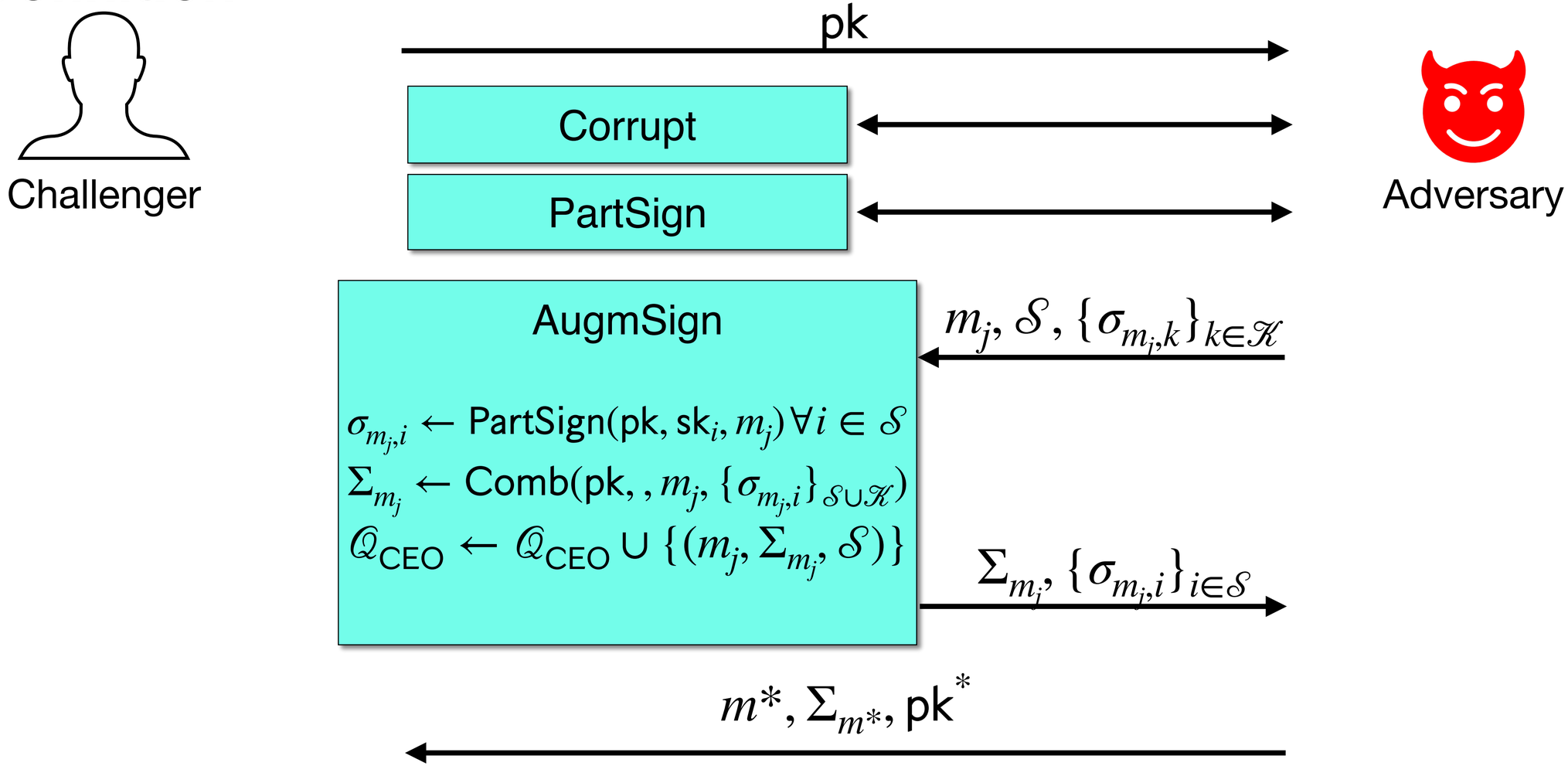
Strong-CEO in Threshold Setting

Our Definition



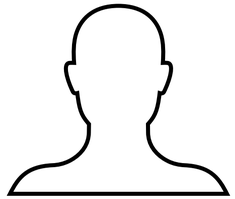
Strong-CEO in Threshold Setting

Our Definition



Strong-CEO in Threshold Setting

Our Definition



Challenger

pk

Corrupt

PartSign

Adversary

AugmSign

$\sigma_{m_j,i} \leftarrow \text{PartSign}(\text{pk}, \text{sk}_i, m_j) \forall i \in \mathcal{S}$

$\Sigma_{m_j} \leftarrow \text{Comb}(\text{pk}, , m_j, \{\sigma_{m_j,i}\}_{\mathcal{S} \cup \mathcal{K}})$

$\mathcal{Q}_{\text{CEO}} \leftarrow \mathcal{Q}_{\text{CEO}} \cup \{(m_j, \Sigma_{m_j}, \mathcal{S})\}$

$m_j, \mathcal{S}, \{\sigma_{m_j,k}\}_{k \in \mathcal{K}}$

$\Sigma_{m_j}, \{\sigma_{m_j,i}\}_{i \in \mathcal{S}}$

$m^*, \Sigma_{m^*}, \text{pk}^*$

Pr [Adversary wins]= negl.

Adversary wins if

$\text{Ver}(\text{pk}^*, m^*, \Sigma_{m^*}) = 1$

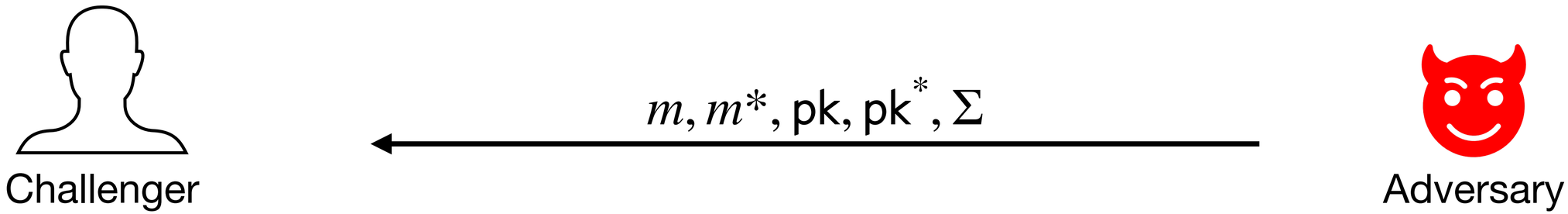
AND

$(m^*, \Sigma_{m^*}, \mathcal{S}) \in \mathcal{Q}_{\text{CEO}},$

$\mathcal{S} \backslash \mathcal{Q}_{\text{Cor}} \neq \phi$

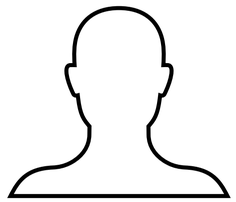
Malicious-Strong-UEO in Threshold Setting

Our Definition



Malicious-Strong-UEO in Threshold Setting

Our Definition



Challenger

$m, m^*, \mathsf{pk}, \mathsf{pk}^*, \Sigma$

Adversary

Adversary wins if

$\mathsf{Ver}(\mathsf{pk}, m, \Sigma) = 1$

AND

$\mathsf{Ver}(\mathsf{pk}^*, m^*, \Sigma) = 1$

AND

$\mathsf{pk} \neq \mathsf{pk}^*$

Pr [Adversary wins]= negl.

Relations between the Definitions

Standard vs Threshold

- Strong-Conservative-EO + Strong-Destructive-EO $\Longleftrightarrow$ Strong-Universal-EO

  (similar to the standard setting)

Relations between the Definitions

Standard vs Threshold

- In the standard setting,

$$\text{Malicious-Strong-Universal-EO} \Rightarrow \begin{array}{c}\text{Strong-Conservative-EO} \\ \& \\ \text{Strong-Destructive-EO}\end{array}$$

Relations between the Definitions

Standard vs Threshold

- In the threshold setting,

Malicious-Strong-Universal-EO $\not\Rightarrow$ Strong-Conservative-EO
&
Strong-Destructive-EO

Relations between the Definitions

Standard vs Threshold

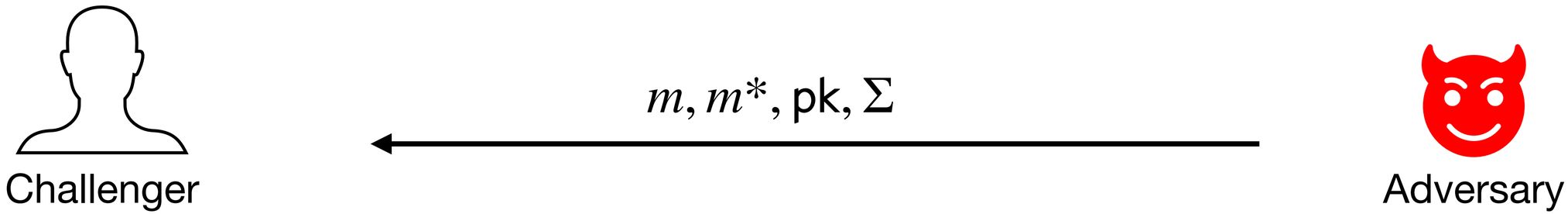
- In the threshold setting,

Malicious-Strong-Universal-EO $\not\Rightarrow$ Strong-Conservative-EO & Strong-Destructive-EO

Malicious-Strong-Universal-EO + **Robustness** $\Rightarrow$ Strong-Conservative-EO & Strong-Destructive-EO

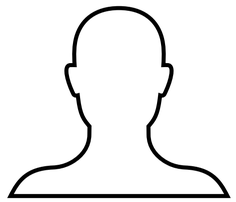
Message-Bound-Signatures in Threshold Setting

Our Definition



Message-Bound-Signatures in Threshold Setting

Our Definition



Challenger

$m, m^*, \text{pk}, \Sigma$

Adversary

Adversary wins if

$\text{Ver}(\text{pk}, m, \Sigma) = 1$

AND

$\text{Ver}(\text{pk}, m^*, \Sigma) = 1$

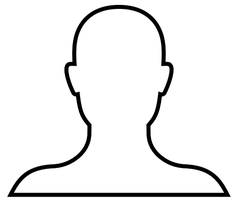
AND

$m \neq m^*$

Pr [Adversary wins]= negl.

Non-Resignability

Standard Signatures [CDFFJ21]



Challenger

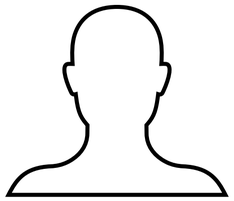
$\mathsf{KeyGen}(1^\lambda) \to (\mathsf{pk}, \mathsf{sk})$

pk

Adversary

Non-Resignability

Standard Signatures [CDFFJ21]



Challenger

Adversary

pk

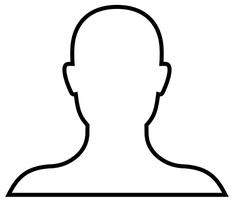
$\mathsf{KeyGen}(1^\lambda) \to (\mathsf{pk}, \mathsf{sk})$

$(m, \mathsf{aux}) \leftarrow \mathscr{D}(\mathsf{pk})$

$\Sigma \leftarrow \mathsf{Sign}(\mathsf{pk}, \mathsf{sk}, m), \mathsf{aux}$

Non-Resignability

Standard Signatures [CDFFJ21]



Challenger

Adversary

pk

$\mathsf{KeyGen}(1^\lambda) \to (\mathsf{pk}, \mathsf{sk})$

$(m, \mathsf{aux}) \leftarrow \mathscr{D}(\mathsf{pk})$

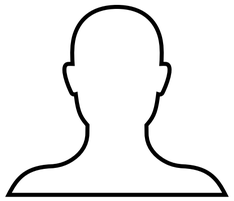
$\Sigma \leftarrow \mathsf{Sign}(\mathsf{pk}, \mathsf{sk}, m), \mathsf{aux}$

Computationally independent of m

pk^*, Σ^*

Non-Resignability

Standard Signatures [CDFFJ21]



Challenger

Adversary

pk

$\text{KeyGen}(1^\lambda) \rightarrow (\text{pk}, \text{sk})$

$\Sigma \leftarrow \text{Sign}(\text{pk}, \text{sk}, m), \text{aux}$

$(m, \text{aux}) \leftarrow \mathscr{D}(\text{pk})$

Computationally independent of m

pk^*, Σ^*

Adversary wins if

$\text{Ver}(\text{pk}^*, m, \Sigma^*) = 1$

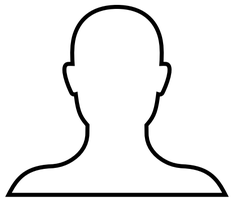
AND

$\text{pk} \neq \text{pk}^*$

Pr [Adversary wins]= negl.

Non-Resignability

Standard Signatures [CDFFJ21]



Challenger

Adversary

pk

$\text{KeyGen}(1^\lambda) \rightarrow (\text{pk}, \text{sk})$

$\Sigma \leftarrow \text{Sign}(\text{pk}, \text{sk}, m), \text{aux}$

$(m, \text{aux}) \leftarrow \mathscr{D}(\text{pk})$

Computationally independent of m

pk^*, Σ^*

Adversary wins if

$\text{Ver}(\text{pk}^*, m, \Sigma^*) = 1$

AND

$\text{pk} \neq \text{pk}^*$

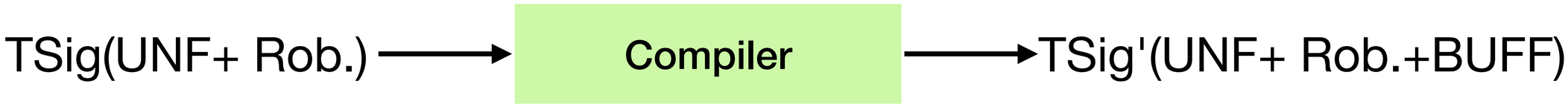
Pr [Adversary wins]= negl.

Our Results

- Formalised BUFF properties in the threshold setting

Our Results

- Formalised BUFF properties in the threshold setting
- Compiler:



Our Results

- Formalised BUFF properties in the threshold setting
- Compiler:

- Construction : Key-prefixed Threshold-BLS with no overhead

Our Results

- Formalised BUFF properties in the threshold setting
- Compiler:

- Construction : Key-prefixed Threshold-BLS with no overhead
- Analysis: FROST [KG20], Tracoon[PKM+24], Thresholdizer [BGG+18]

Our Results

- Formalised BUFF properties in the threshold setting
- Compiler:

- Construction : Key-prefixed Threshold-BLS with no overhead
- Analysis: FROST [KG20], Tracoon[PKM+24], Thresholdizer [BGG+18]

  (Inherits BUFF properties from the underlying standard Signature)

Compiler:

TSig with UNF+ Rob →TSig' with UNF+Rob. + BUFF

$\mathsf{KeyGen}'(1^\lambda, t, n)$:

H, $\mathsf{KeyGen}(1^\lambda, t, n) \rightarrow$

$t = 2,\ n = 4$


sk_1


sk_2


sk_3


sk_4

Verifier


pk, H

$\mathsf{pk}_1, \mathsf{pk}_2, \mathsf{pk}_3, \mathsf{pk}_4$

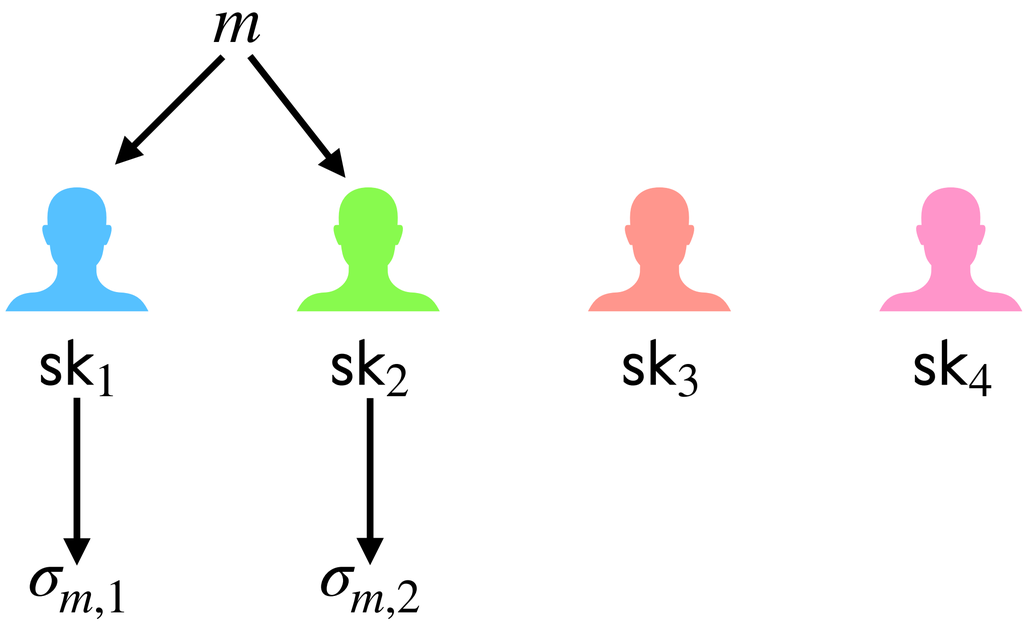
Compiler:

TSig with UNF+ Rob →TSig' with UNF+Rob. + BUFF

KeyGen′$(1^\lambda, t, n)$:

H, KeyGen$(1^\lambda, t, n) \rightarrow$

$t = 2,\ n = 4$



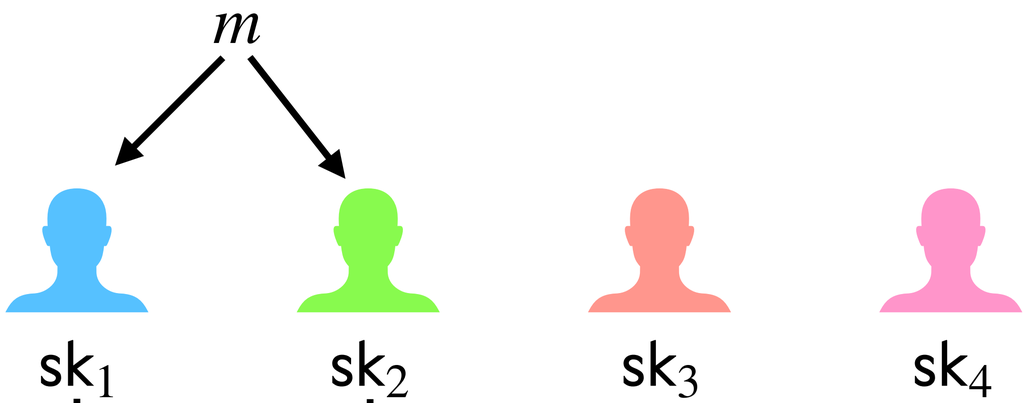
Compiler:

TSig with UNF+ Rob →TSig' with UNF+Rob. + BUFF

KeyGen′$(1^\lambda, t, n)$:

H, KeyGen$(1^\lambda, t, n) \rightarrow$

$t = 2,\ n = 4$



Verifier

pk, H

$\mathsf{pk}_1, \mathsf{pk}_2, \mathsf{pk}_3, \mathsf{pk}_4$

Comb′(pk, H, $m, \sigma_{m,1}, \sigma_{m,2}$) $\rightarrow (\Sigma_m, h_m)$

Comb(pk, $m, \sigma_{m,1}, \sigma_{m,2}$) $\rightarrow \Sigma_m$

$h_m = \mathsf{H}(\mathsf{pk}, m)$

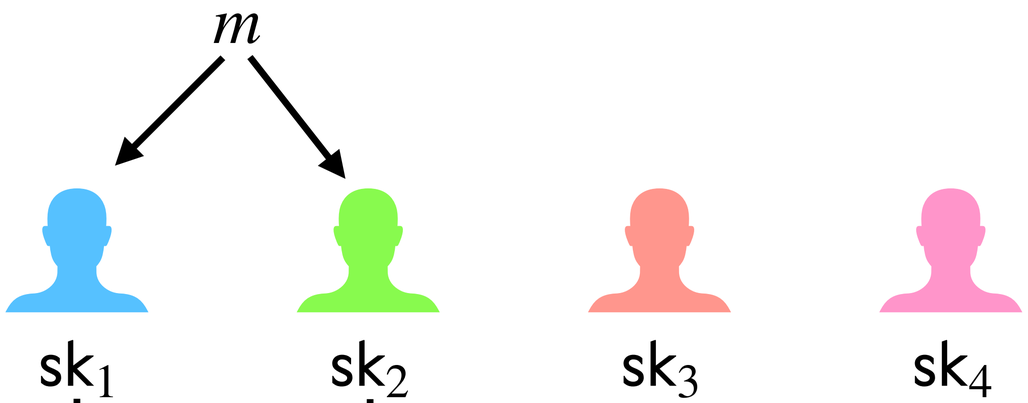
Compiler:

TSig with UNF+ Rob →TSig' with UNF+Rob. + BUFF

KeyGen′$(1^\lambda, t, n)$:

H, KeyGen$(1^\lambda, t, n) \rightarrow$

$t = 2,\ n = 4$



Verifier

pk,H

$\mathsf{pk}_1, \mathsf{pk}_2, \mathsf{pk}_3, \mathsf{pk}_4$

Ver′(pk, m, $(\Sigma_m, h_m)) \rightarrow 0/1$

Comb′(pk, H, $m, \sigma_{m,1}, \sigma_{m,2}) \rightarrow (\Sigma_m, h_m)$

Comb(pk, $m, \sigma_{m,1}, \sigma_{m,2}) \rightarrow \Sigma_m$

$h_m = \mathsf{H}(\mathsf{pk}, m)$

Ver(pk, $m, \Sigma_m) \rightarrow 0/1$

AND

$h_m = = \mathsf{H}(\mathsf{pk}, m)$

BUFF Threshold Constructions

	S-CEO	S-DEO	M-S-UEO	MBS
Compiler : TSig(UNF+ Rob.) → TSig' (UNF+ Rob.+BUFF)	✔	✔	✔	✔
Construction: Key-prefixed Threshold BLS	✔	✔	✔	✔
Analysis: Tracoon[PKM+24]			✔	✔
Analysis: FROST [KG20]			✔	✔
Analysis: Thresholdizer [BGG+18]			✔	✔

Conclusion

- Formalised BUFF properties in the threshold setting
- Compiler:

- Construction : Key-prefixed Threshold-BLS with no overhead
- Analysis: FROST [KG20], Tracoon[PKM+24], Thresholdizer [BGG+18]

Thank you!