On Security Proofs of Existing Equivalence Class Signature Schemes

Balthazar Bauer[1], Georg Fuchsbauer[2], Fabian Regen[2]

[1]UVSQ
[2]TU Wien

Asiacrypt 2024
Kolkata, 11 December 24

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Equivalence class signatures (EQS) [FHS19]

Defined over (additive) Group $(\mathbb{G}, p, g)$

Message space $(\mathbb{G}^*)^2$ partitioned by

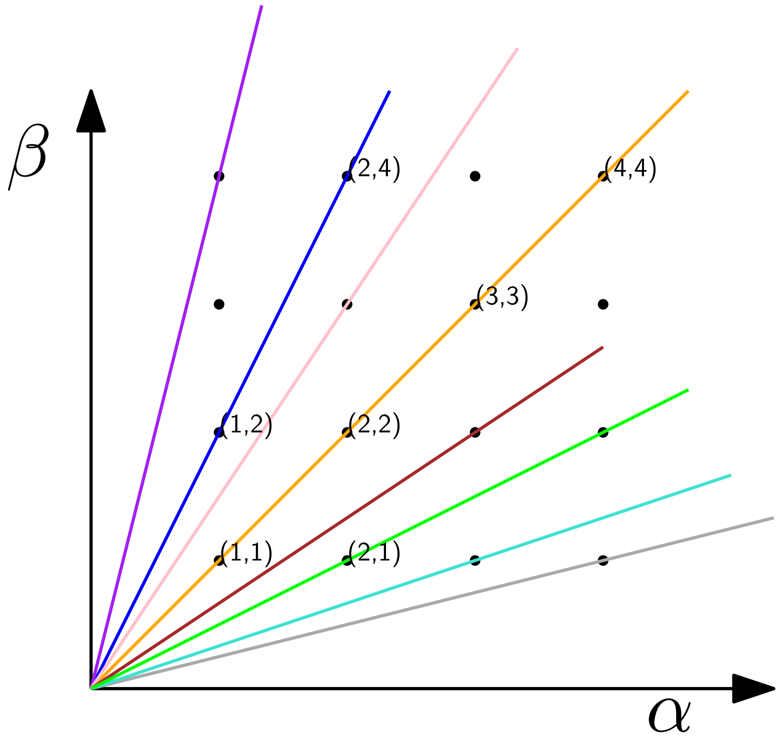
$$m \sim m' :\Leftrightarrow \exists \mu \in \mathbb{Z}_p^* : m = \mu \cdot m'$$

Equivalence class signatures (EQS) [FHS19]

Defined over (additive) Group $(\mathbb{G}, p, g)$

Message space $(\mathbb{G}^*)^2$ partitioned by

$$m \sim m' :\Leftrightarrow \exists \mu \in \mathbb{Z}_p^* : m = \mu \cdot m'$$



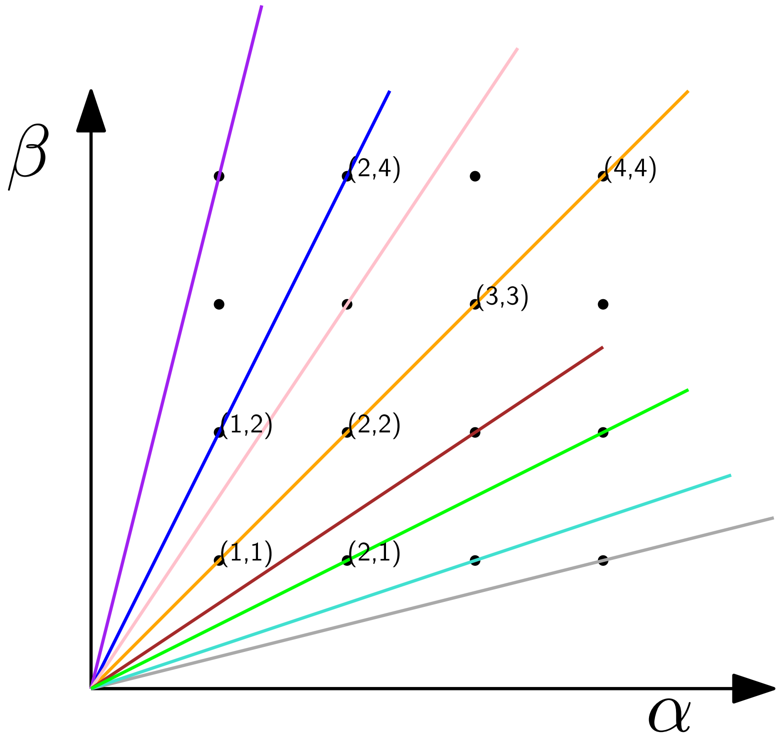
Equivalence classes
for $m = (\alpha \cdot g, \beta \cdot g)$

Equivalence class signatures (EQS) [FHS19]

Defined over (additive) Group $(\mathbb{G}, p, g)$

Message space $(\mathbb{G}^*)^2$ partitioned by

$$m \sim m' :\Leftrightarrow \exists \mu \in \mathbb{Z}_p^* : m = \mu \cdot m'$$



Equivalence classes
for $m = (\alpha \cdot g, \beta \cdot g)$

Class hiding:
given m, m'
decide if $m \sim m'$

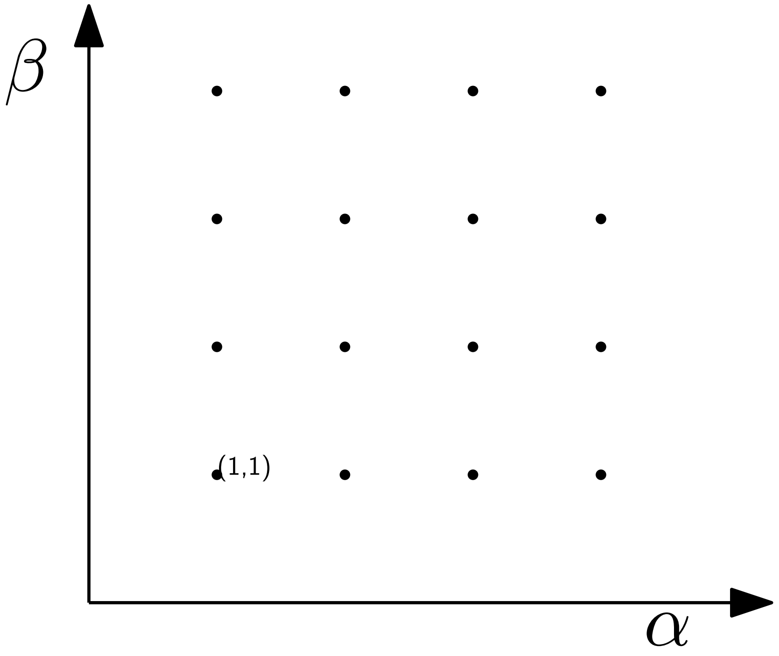
Equivalence class signatures (EQS) [FHS19]

An *EQS* scheme consists of four p.p.t. algorithms:

- Keygen() $\to (sk, pk)$
- Sign$(sk, m) \to \sigma$
- Verify$(pk, m, \sigma) \to 0$ or 1
- Adapt$(pk, m, \sigma, \mu \in \mathbb{Z}_p^*) \to$ signature on $\mu \cdot m$.

Equivalence class signatures (EQS) [FHS19]

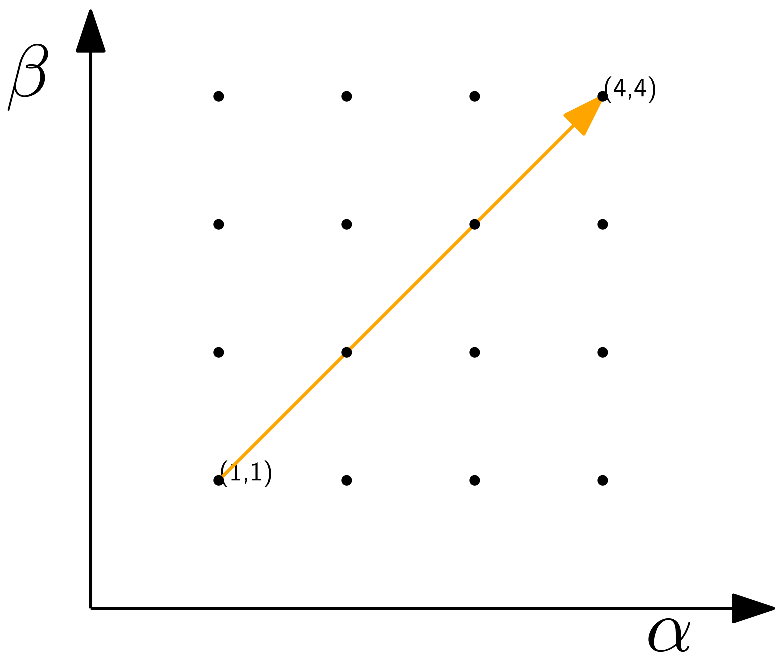
- Adapt$(pk, m, \sigma, \mu \in \mathbb{Z}_p^*) \to$ signature on $\mu \cdot m$.



$$m := (1 \cdot g, 1 \cdot g)$$
$$\sigma := \mathsf{Sign}_{sk}(m)$$

Equivalence class signatures (EQS) [FHS19]

- Adapt$(pk, m, \sigma, \mu \in \mathbb{Z}_p^*) \to$ signature on $\mu \cdot m$.



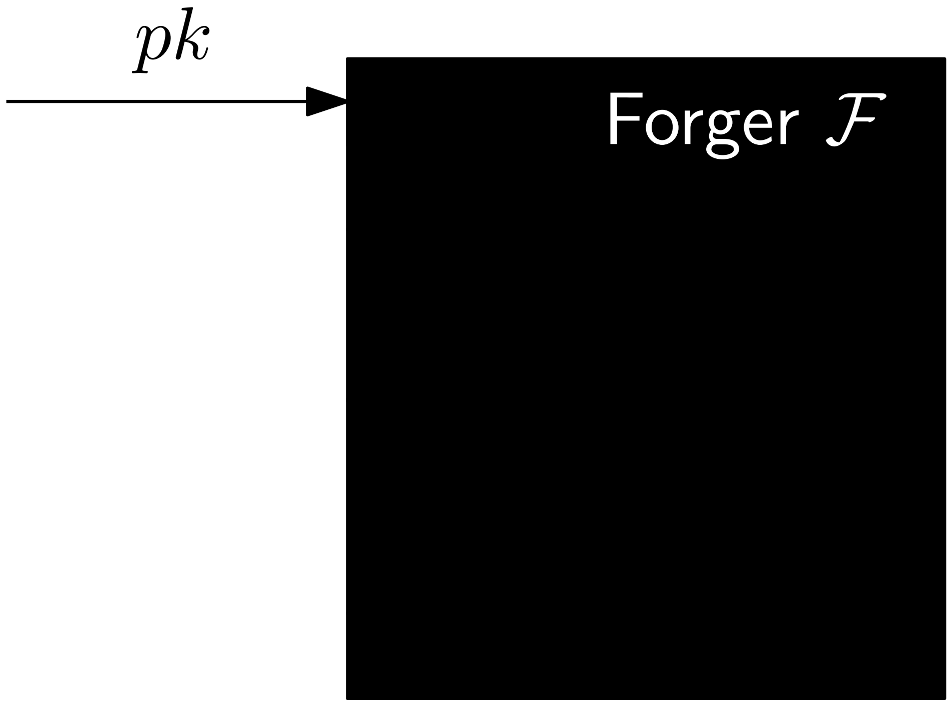
$$m := (1 \cdot g, 1 \cdot g)$$
$$\sigma := \mathsf{Sign}_{sk}(m)$$

$$\sigma' := \mathsf{Adapt}(pk, m, \sigma, 4)$$

Unforgeability of EQS

Game UNF:

$(sk, pk) \leftarrow \text{Keygen}()$

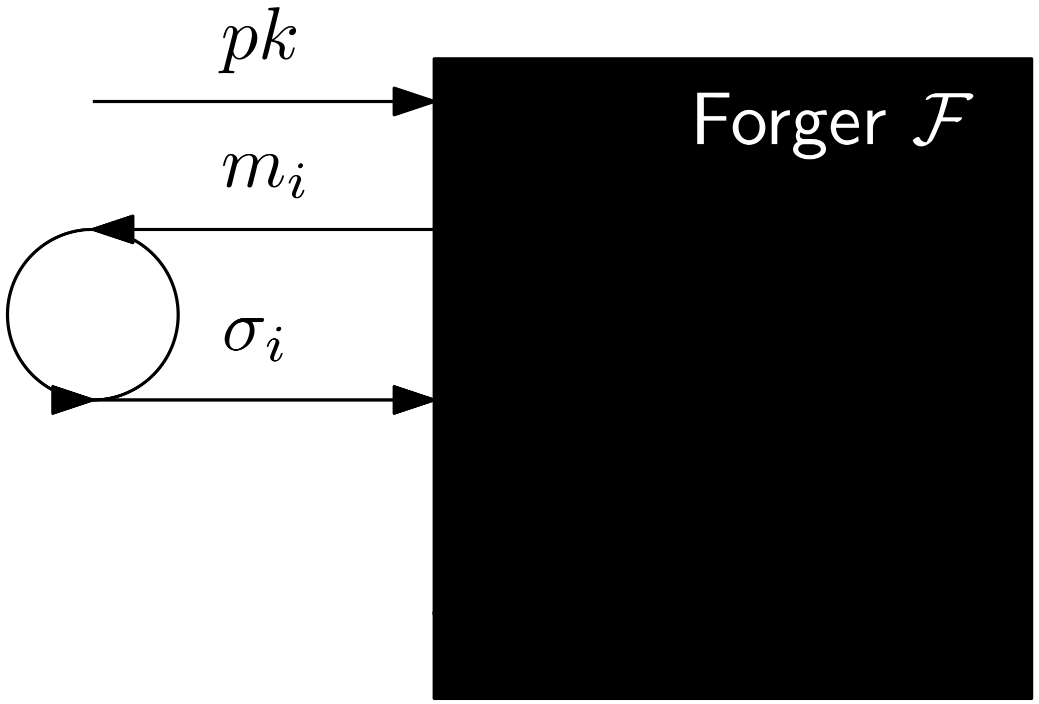


Unforgeability of EQS

Game UNF:

$$(sk, pk) \leftarrow \mathsf{Keygen}()$$

$$\sigma_i \leftarrow \mathsf{Sign}(sk, m_i)$$

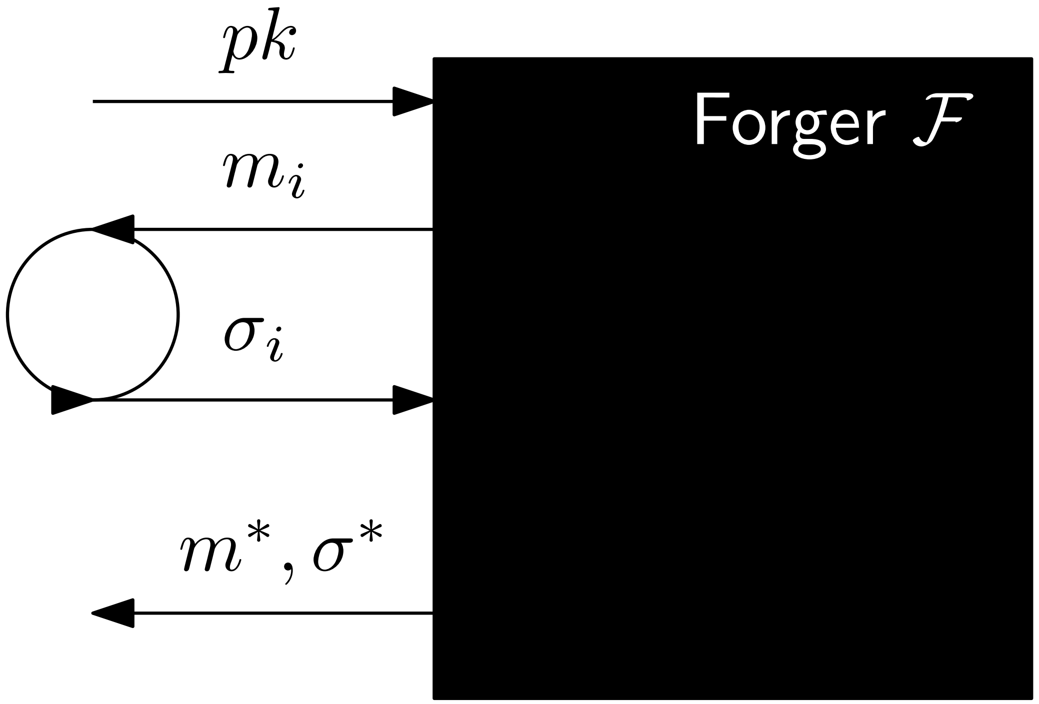


Unforgeability of EQS

Game UNF:

$(sk, pk) \leftarrow \mathsf{Keygen}()$

$\sigma_i \leftarrow \mathsf{Sign}(sk, m_i)$



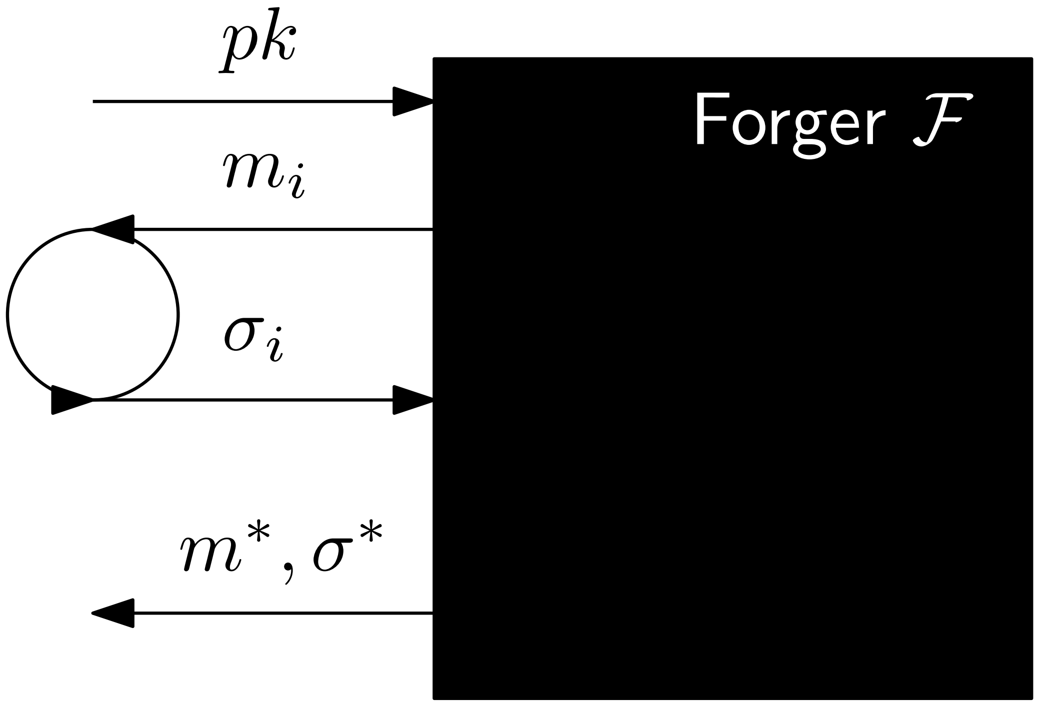
$\mathcal{F}$ wins $:\Leftrightarrow \mathsf{Verify}(pk, m^*, \sigma^*) \wedge m^* \not\sim m_i$

Unforgeability of EQS

Game UNF:

$(sk, pk) \leftarrow$ Keygen$()$

$\sigma_i \leftarrow$ Sign(sk, m_i)



$\mathcal{F}$ wins $:\Leftrightarrow$ Verify$(pk, m^*, \sigma^*) \wedge m^* \not\sim m_i$

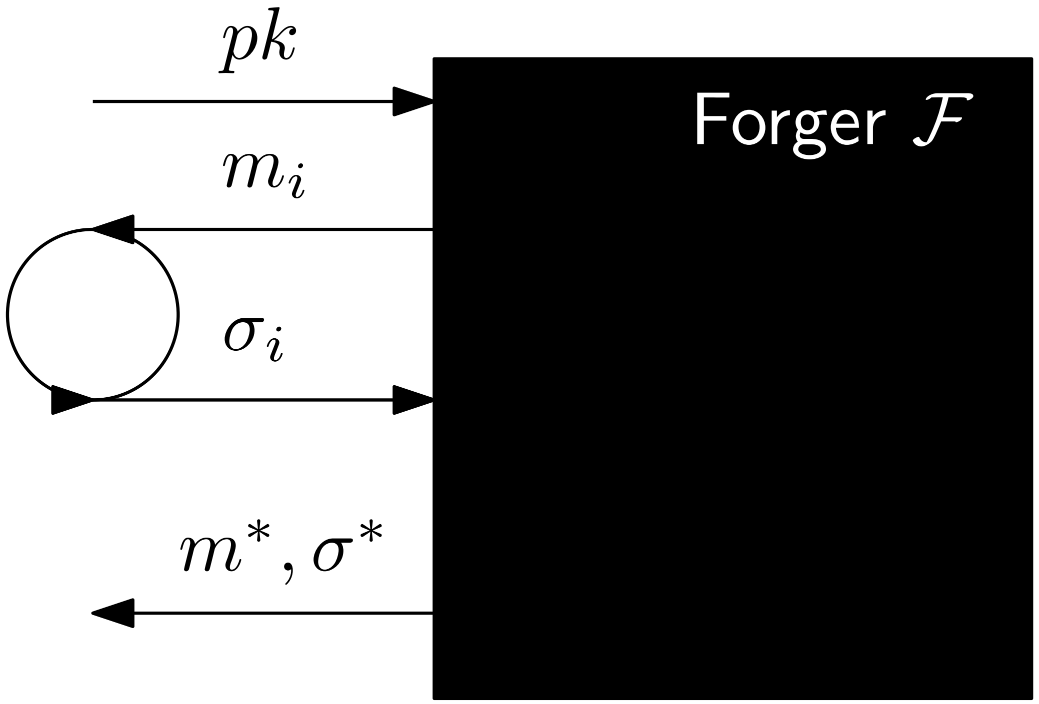
assuming **CH**:
non falsifiable

Unforgeability of EQS

Game UNF:

$(sk, pk) \leftarrow$ Keygen()

$\sigma_i \leftarrow$ Sign(sk, m_i)



$\mathcal{F}$ wins $:\Leftrightarrow$ Verify$(pk, m^*, \sigma^*) \wedge m^* \not\sim m_i$

Scheme *unforgeable* if Adv$_{\mathcal{F}}^{\text{UNF}} := \Pr[\mathcal{F} \text{ wins}] \approx 0$

Anonymous authentication

Alice

$$h = \alpha \cdot g \in \mathbb{G}^*$$

Anonymous authentication

$\mu_j \leftarrow \mathbb{Z}_p^*$

Alice

I am $\quad m_j = (\mu_j \cdot g, \mu_j \cdot h)$ →

Party j

$h = \alpha \cdot g \in \mathbb{G}^*$

Anonymous authentication

$\mu_j \leftarrow \mathbb{Z}_p^*$

Alice

I am $m_j = (\mu_j \cdot g, \mu_j \cdot h)$ →

Party j

$h = \alpha \cdot g \in \mathbb{G}^*$

credential σ_j on m_j ←

Anonymous authentication

$\mu_j \leftarrow \mathbb{Z}_p^*$

Alice

I am $m_j = (\mu_j \cdot g, \mu_j \cdot h)$ →

Party j

$h = \alpha \cdot g \in \mathbb{G}^*$

← credential σ_j on m_j

Party i

Anonymous authentication

$\mu_j \leftarrow \mathbb{Z}_p^*$

Alice

I am $m_j = (\mu_j \cdot g, \mu_j \cdot h)$ →

Party j

$h = \alpha \cdot g \in \mathbb{G}^*$

← credential σ_j on m_j

$\mu_i \leftarrow \mathbb{Z}_p^*$

I am $(\mu_i \cdot g, \mu_i \cdot h)$

Party i

my credential is Adapt$(pk_j, m_j, \sigma_j, \mu_i/\mu_j)$ →

Anonymous authentication

$\mu_j \leftarrow \mathbb{Z}_p^*$

Alice

$h = \alpha \cdot g \in \mathbb{G}^*$

I am $m_j = (\mu_j \cdot g, \mu_j \cdot h)$ →

Party j

← credential σ_j on m_j

$\mu_i \leftarrow \mathbb{Z}_p^*$

I am $(\mu_i \cdot g, \mu_i \cdot h)$

Party i

my credential is Adapt$(pk_j, m_j, \sigma_j, \mu_i/\mu_j)$ →

Class hiding: m_i looks random, Adapt guarantees credential looks random

Applications of EQS

Cryptographic concepts constructed from EQS:

- Attribute-based credentials [FHS19, DHS15, HS21]

Applications of EQS

Cryptographic concepts constructed from EQS:

- Attribute-based credentials [FHS19, DHS15, HS21]
- Blind signatures [FHS15, FHKS16, Han23]

Applications of EQS

Cryptographic concepts constructed from EQS:

- Attribute-based credentials [FHS19, DHS15, HS21]
- Blind signatures [FHS15, FHKS16, Han23]
- Group signatures [DS16, CS20, DS18, BHKS18]

Applications of EQS

Cryptographic concepts constructed from EQS:

- Attribute-based credentials [FHS19, DHS15, HS21]
- Blind signatures [FHS15, FHKS16, Han23]
- Group signatures [DS16, CS20, DS18, BHKS18]
- Verifiably encrypted signatures [HRS15], access-control-encryption [FGKO17], sanitizable signatures [BLL+19], privacy-preserving incentive systems [BEK+20], mix nets [ST21], anonymous counting tokens [BRS23], policy-compliant signatures [BSW23], e-voting [Poi23], . . .

Constructions of EQS

- Original [FHS19] (efficient: $\sigma \in \mathbb{G}^2 \times \hat{\mathbb{G}}$)
    - *but*: proof in *generic group model*

Constructions of EQS

- Original [FHS19] (efficient: $\sigma \in \mathbb{G}^2 \times \hat{\mathbb{G}}$)
    - *but*: proof in *generic group model*

- Relaxed unforgeability notion [FG18]:
    - *but*: too weak for many applications

Constructions of EQS

- Original [FHS19] (efficient: $\sigma \in \mathbb{G}^2 \times \hat{\mathbb{G}}$)
  - *but*: proof in *generic group model*
- Relaxed unforgeability notion [FG18]:
  - *but*: too weak for many applications
- CRS model [KSD19] ($\sigma \in \mathbb{G}^8 \times \hat{\mathbb{G}}^9$),

  [CLP22] ($\sigma \in \mathbb{G}^9 \times \hat{\mathbb{G}}^4$)
  - *but*: anonymity relies on trusted CRS

Constructions of EQS

- Original [FHS19] (efficient: $\sigma \in \mathbb{G}^2 \times \hat{\mathbb{G}}$)
  - *but*: proof in *generic group model*

- Relaxed unforgeability notion [FG18]:
  - *but*: too weak for many applications

- CRS model [KSD19] ($\sigma \in \mathbb{G}^8 \times \hat{\mathbb{G}}^9$),
  [CLP22] ($\sigma \in \mathbb{G}^9 \times \hat{\mathbb{G}}^4$)
  - *but*: anonymity relies on trusted CRS

SXDH

extKerMDH

Constructing EQS from standard assumptions?

Is there a scheme satisfying the original notion with a proof from a non-interactive assumption?

Constructing EQS from standard assumptions?

Is there a scheme satisfying the original notion with a proof from a non-interactive assumption?

No such scheme can exist [BFR24]

Constructing EQS from standard assumptions?

Is there a scheme satisfying the original notion with a proof from a non-interactive assumption?

No such scheme can exist [BFR24]

Impossibility result does not apply to schemes in the CRS model

want EQS from standard assumptions $\Rightarrow$ **need** CRS?

Constructing EQS from standard assumptions?

Is there a scheme satisfying the original notion with a proof from a non-interactive assumption?

No such scheme can exist [BFR24]

Impossibility result does not apply to schemes in the CRS model

want EQS from standard assumptions $\Rightarrow$ **need** CRS?

proofs of CRS-based schemes are flawed!

Flaw in proof of CRS based schemes [KSD19, CLP22]

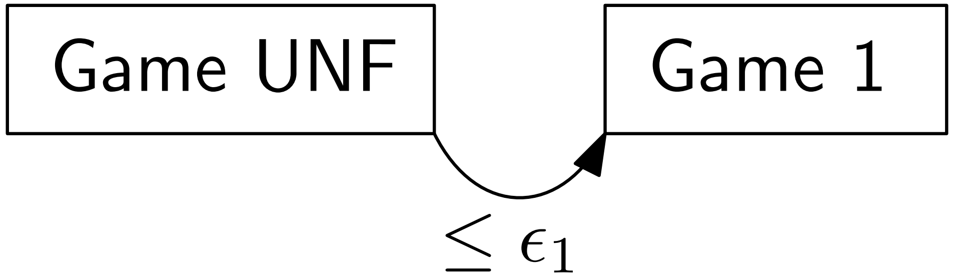
Game UNF

Flaw in proof of CRS based schemes [KSD19, CLP22]

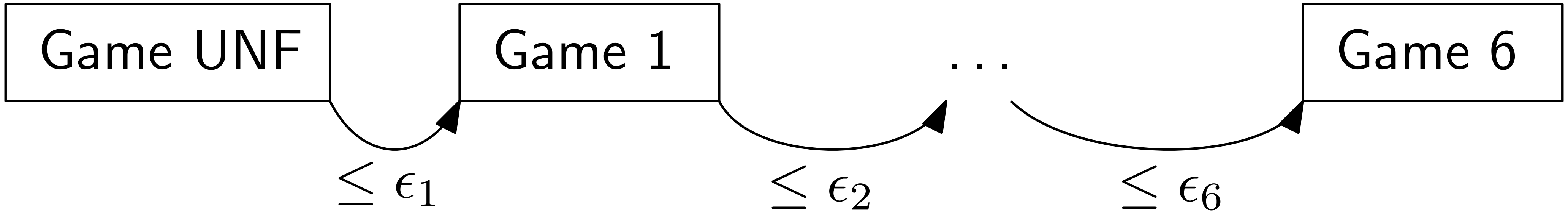
Game UNF

Game 1

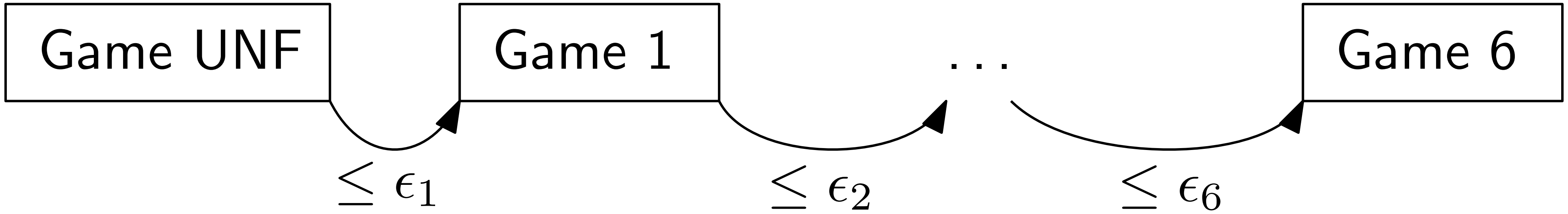
Flaw in proof of CRS based schemes [KSD19, CLP22]



Flaw in proof of CRS based schemes [KSD19, CLP22]



Flaw in proof of CRS based schemes [KSD19, CLP22]



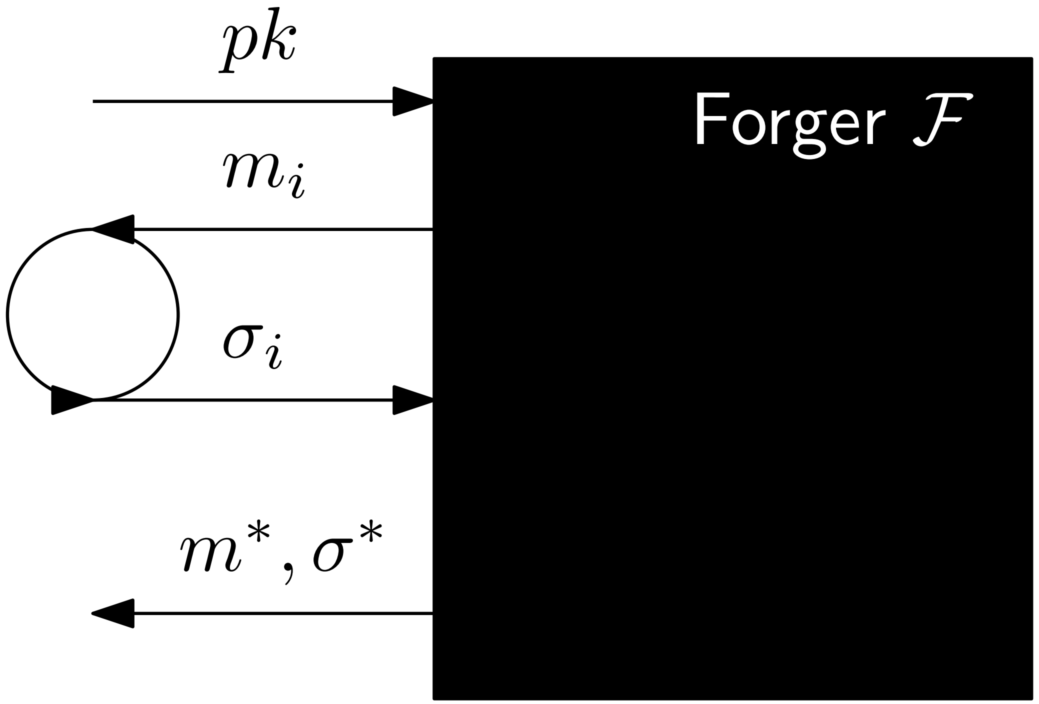
$$\mathsf{Adv}^{\mathsf{UNF}} \leq \epsilon_1 + \ldots + \epsilon_6 + \mathsf{Adv}^{\mathsf{Game\ 6}}$$
$$\leq \mathsf{Adv}^{\mathsf{SXDH}} + \epsilon$$

Flaw in proof of CRS based schemes [KSD19, CLP22]

Game UNF:

$(sk, pk) \leftarrow$ Keygen()

$\sigma_i \leftarrow$ Sign(sk, m_i)



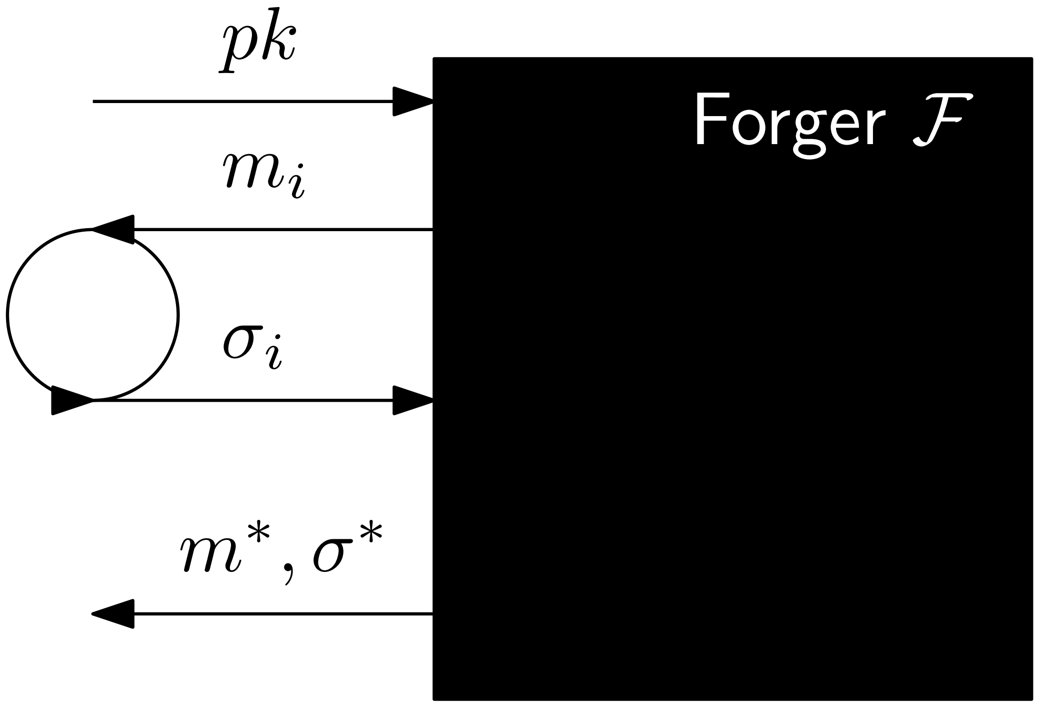
$\mathcal{F}$ wins $:\Leftrightarrow$ Verify$(pk, m^*, \sigma^*) \wedge m^* \not\sim m_i$

Flaw in proof of CRS based schemes [KSD19, CLP22]

Game 1:

$(sk, pk) \leftarrow \text{Keygen}()$

$\sigma_i \leftarrow \text{Sign}(sk, m_i)$



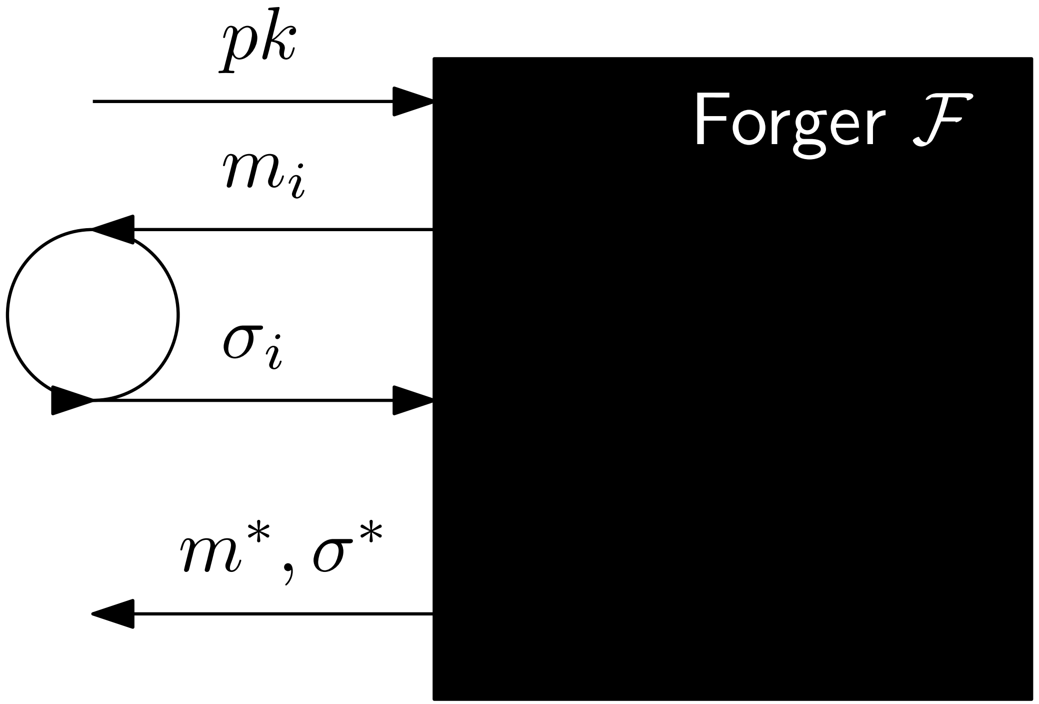
$\mathcal{F}$ wins $:\Leftrightarrow \text{Verify}'(pk, m^*, \sigma^*) \wedge m^* \not\sim m_i$

Flaw in proof of CRS based schemes [KSD19, CLP22]

Game 1:

$(sk, pk) \leftarrow \mathsf{Keygen}()$

$\sigma_i \leftarrow \mathsf{Sign}(sk, m_i)$



$\mathcal{F}$ wins $:\Leftrightarrow \mathsf{Verify}'(pk, m^*, \sigma^*) \wedge m^* \not\sim m_i$

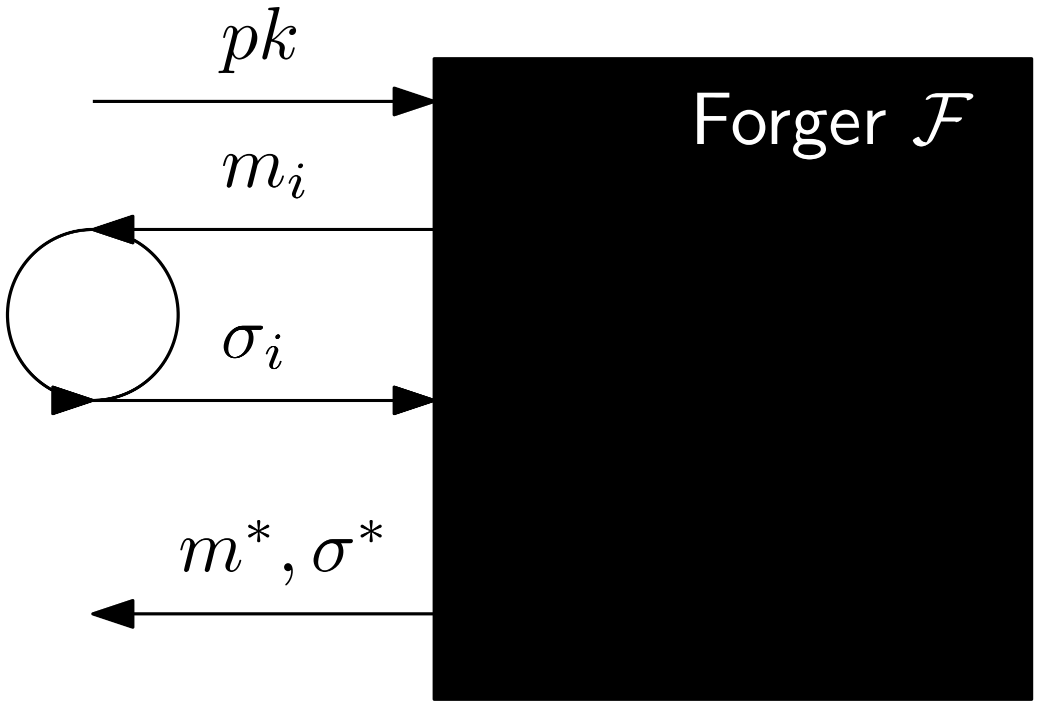
$$|\mathsf{Adv}^{\mathsf{UNF}} - \mathsf{Adv}^{\mathsf{Game\ 1}}| \leq \mathsf{Adv}^{\mathsf{SXDH}}$$

Flaw in proof of CRS based schemes [KSD19, CLP22]

Game 2:

$(sk, pk) \leftarrow$ Keygen$'()$

$\sigma_i \leftarrow$ Sign(sk, m_i)



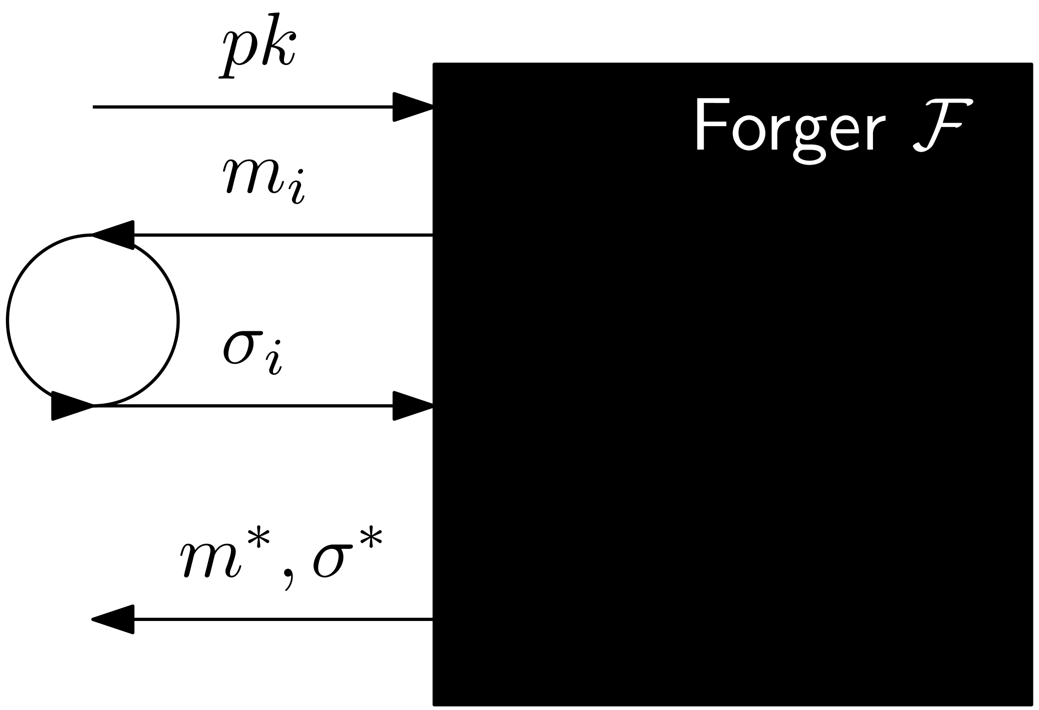
$\mathcal{F}$ wins $:\Leftrightarrow$ Verify$'(pk, m^*, \sigma^*) \land m^* \nsim m_i$

Flaw in proof of CRS based schemes [KSD19, CLP22]

Game 2:

$(sk, pk) \leftarrow \text{Keygen}'()$

$\sigma_i \leftarrow \text{Sign}(sk, m_i)$



$\mathcal{F}$ wins $:\Leftrightarrow \text{Verify}'(pk, m^*, \sigma^*) \wedge m^* \not\sim m_i$

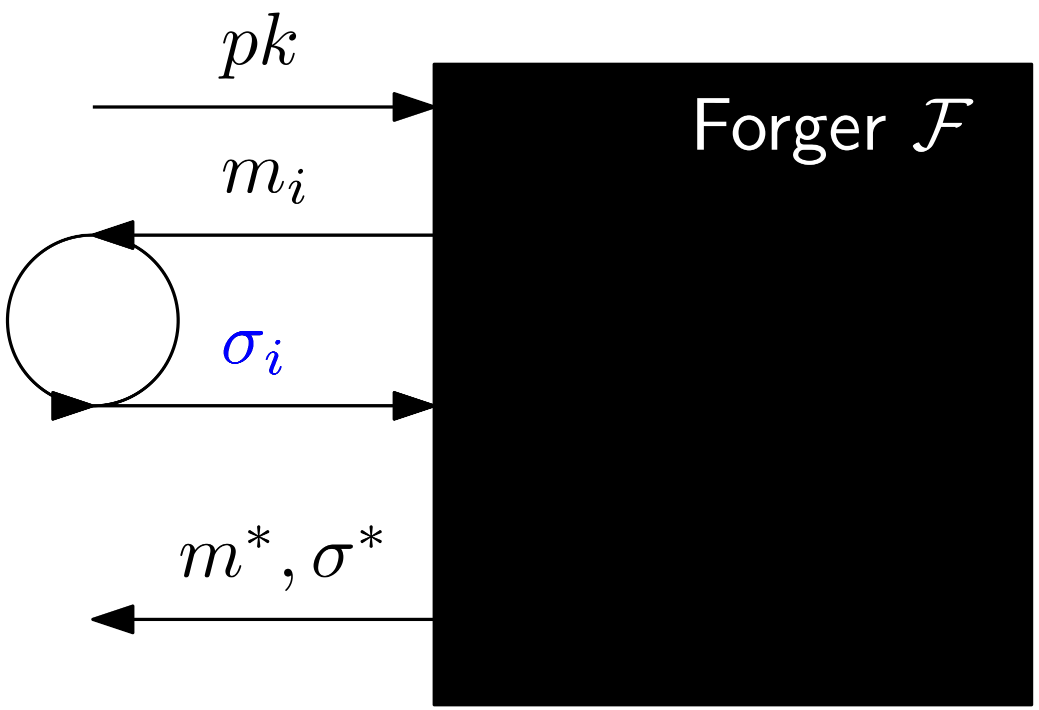
$$\text{Adv}^{\text{Game 1}} = \text{Adv}^{\text{Game 2}}$$

Flaw in proof of CRS based schemes [KSD19, CLP22]

Game 3:

$(sk, pk) \leftarrow \mathsf{Keygen}'()$

$\sigma_i \leftarrow \mathsf{Sign}'(sk, m_i)$



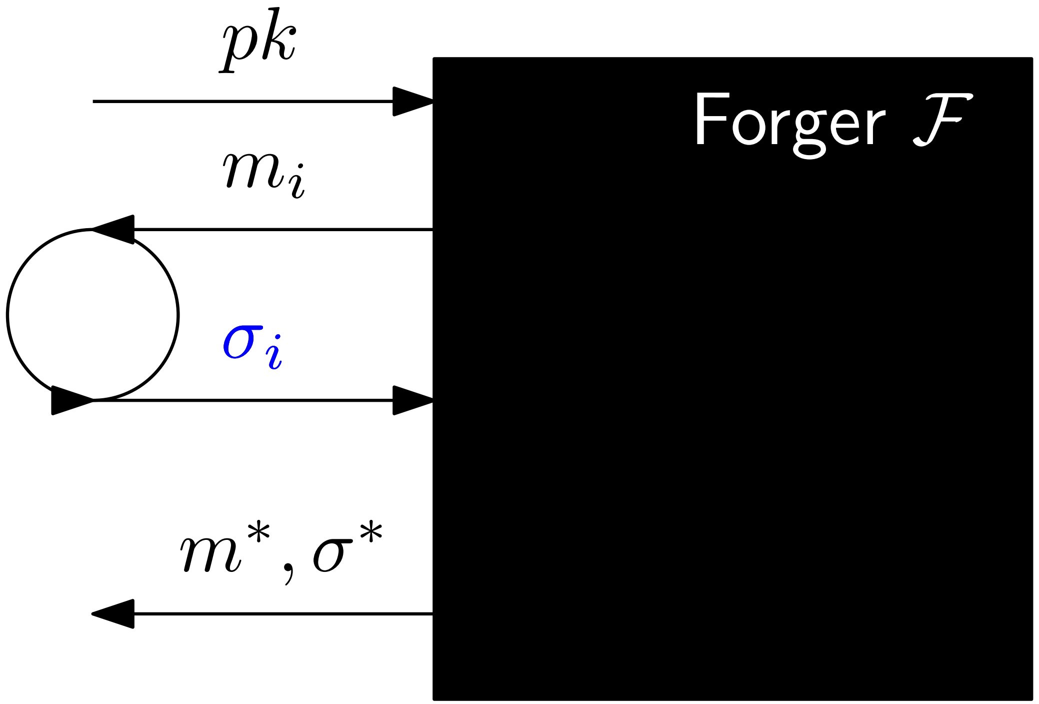
$\mathcal{F}$ wins $:\Leftrightarrow \mathsf{Verify}''(pk, m^*, \sigma^*) \wedge m^* \not\sim m_i$

Flaw in proof of CRS based schemes [KSD19, CLP22]

Game 3:

$(sk, pk) \leftarrow \text{Keygen}'()$

$\sigma_i \leftarrow \text{Sign}'(sk, m_i)$



$\mathcal{F}$ wins $:\Leftrightarrow \text{Verify}''(pk, m^*, \sigma^*) \wedge m^* \not\sim m_i$

Flaw in proof of CRS based schemes [KSD19, CLP22]

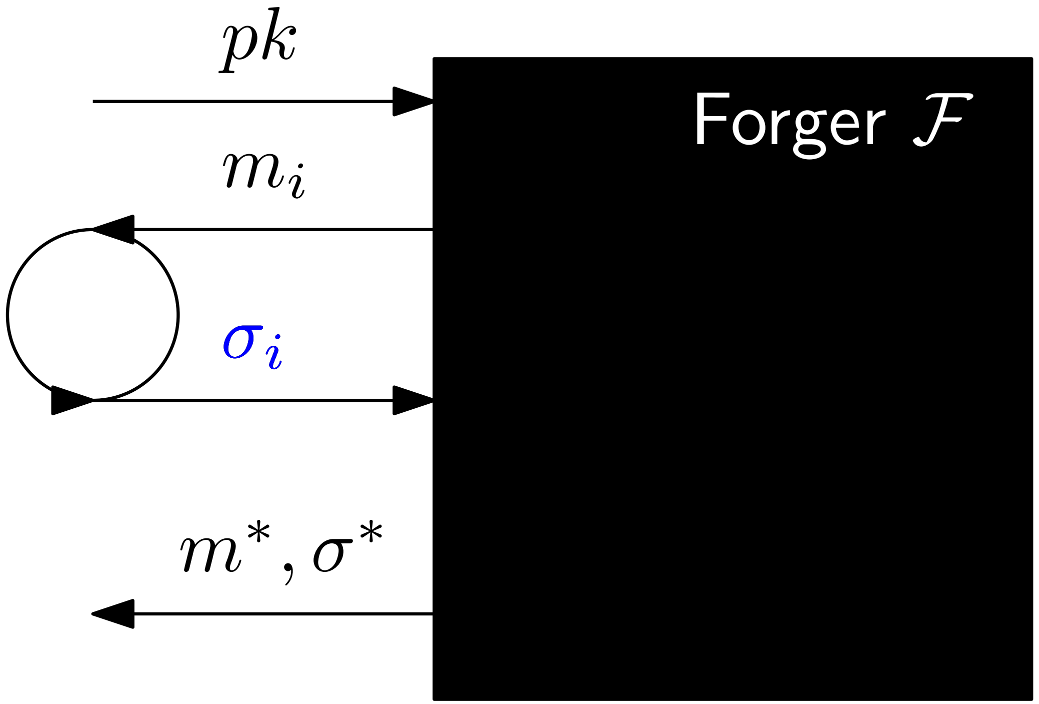
Game 3:

$(sk, pk) \leftarrow \mathsf{Keygen}'()$

$\sigma_i \leftarrow \mathsf{Sign}'(sk, m_i)$

$\not\approx$

$\mathsf{Sign}(sk, m_i)$



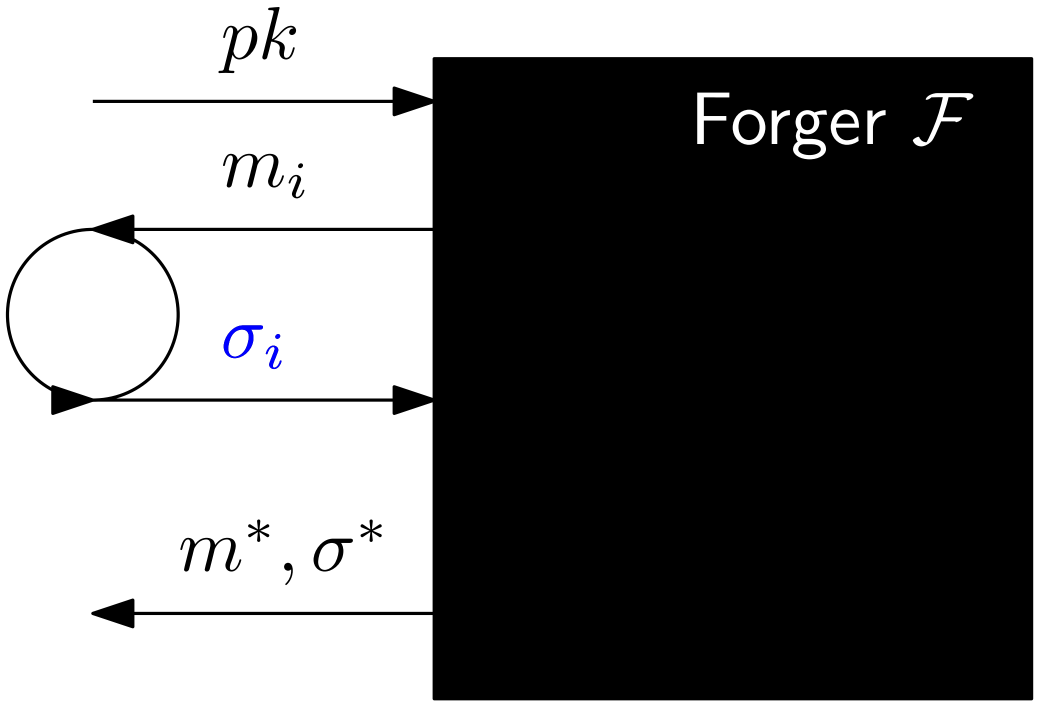
$\mathcal{F}$ wins $:\Leftrightarrow \mathsf{Verify}''(pk, m^*, \sigma^*) \checkmark \wedge m^* \not\sim m_i$

Flaw in proof of CRS based schemes [KSD19, CLP22]

Game 3:

$(sk, pk) \leftarrow \text{Keygen}'()$

$\sigma_i \leftarrow \text{Sign}'(sk, m_i)$
$\not\approx$
$\text{Sign}(sk, m_i)$



probability can change arbitrarily!

$\mathcal{F}$ wins $:\Leftrightarrow$ $\text{Verify}''(pk, m^*, \sigma^*) \wedge m^* \not\sim m_i$

$|\text{Adv}^{\text{Game 3}} - \text{Adv}^{\text{Game 2}}| \gg \text{negl}$

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Can this be fixed?

Class hiding: hard to decide $m \sim m'$

can't check $m^* \not\sim m'$ efficiently!

Can this be fixed?

Class hiding: hard to decide $m \sim m'$

can't check $m^* \not\sim m'$ efficiently!

can't construct efficient reduction!

proof strategy does not work for EQS

Constructions of EQS

- Original [FHS19] (efficient: $\sigma \in \mathbb{G}^2 \times \hat{\mathbb{G}}$)
  - *but*: proof in *generic group model*

- Relaxed unforgeability notion [FG18]:
  - *but*: too weak for many applications

- CRS model [KSD19]($\sigma \in \mathbb{G}^8 \times \hat{\mathbb{G}}^9$),
  [CLP22] ($\sigma \in \mathbb{G}^9 \times \hat{\mathbb{G}}^4$)
  - *but*: anonymity relies on trusted CRS

Constructions of EQS

- Original [FHS19] (efficient: $\sigma \in \mathbb{G}^2 \times \hat{\mathbb{G}}$)
  - *but*: proof in *generic group model*
  - *but*: proof in *algebraic group model*
- Relaxed unforgeability notion [FG18]:
  - *but*: too weak for many applications
- CRS model [KSD19]($\sigma \in \mathbb{G}^8 \times \hat{\mathbb{G}}^9$),

  [CLP22] ($\sigma \in \mathbb{G}^9 \times \hat{\mathbb{G}}^4$)
  - *but*: anonymity relies on trusted CRS

The Generic Group Model

Adversary $(\mathbb{G}, p, g)$ Challenger

The Generic Group Model

Adversary $(\mathbb{G}, p, g)$ Challenger

$X_1, \ldots, X_n \in \mathbb{G}$ ←

$Y_1, \ldots, Y_n \in \mathbb{G}$ →

The Generic Group Model

Adversary $(\mathbb{G}, p, g)$ Challenger

$$\clubsuit, \ldots, \spadesuit$$

$\longleftarrow$

$$\clubsuit \sim X_1$$

$$\vdots$$

$$\spadesuit \sim X_n$$

The Generic Group Model

Adversary $\quad (\mathbb{G}, p, g) \quad$ Challenger

$$\clubsuit \sim X_1$$

$$\vdots$$

$$\spadesuit \sim X_n$$

$$\xleftarrow{\clubsuit, \ldots, \spadesuit}$$

$$\xrightarrow{\spadesuit + \clubsuit ?}$$

$$\heartsuit := \spadesuit + \clubsuit$$

$$\xleftarrow{\heartsuit = \spadesuit + \clubsuit}$$

The Generic Group Model

Adversary $\qquad (\mathbb{G}, p, g) \qquad$ Challenger

$\longleftarrow \; \clubsuit, \ldots, \spadesuit$

$\spadesuit + \clubsuit ? \; \longrightarrow$

$\longleftarrow \; \heartsuit = \spadesuit + \clubsuit$

$\diamondsuit \; \longrightarrow$

$$\clubsuit \sim X_1$$

$$\vdots$$

$$\spadesuit \sim X_n$$

$$\heartsuit := \spadesuit + \clubsuit$$

$$\diamondsuit \sim \sum \alpha_i X_i$$

The Algebraic Group Model [FKL19]

Adversary $(\mathbb{G}, p, g)$ Challenger

$$X_1, \ldots, X_n \in \mathbb{G}$$

$\longleftarrow$

The Algebraic Group Model [FKL19]

Adversary $(\mathbb{G}, p, g)$ Challenger

$X_1, \ldots, X_n \in \mathbb{G}$ ←

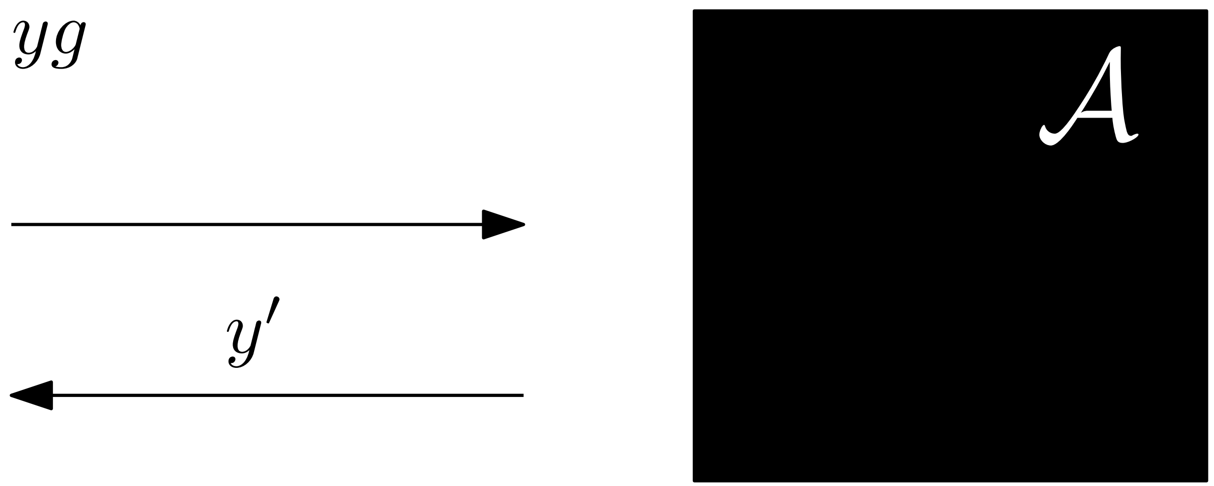
$Y \in \mathbb{G}$ →

$\exists$ Extractor E finding α_i such that $Y = \sum_i \alpha_i X_i$

FHS in the AGM

Definition. DL hard for group $\mathbb{G}$ with generator g

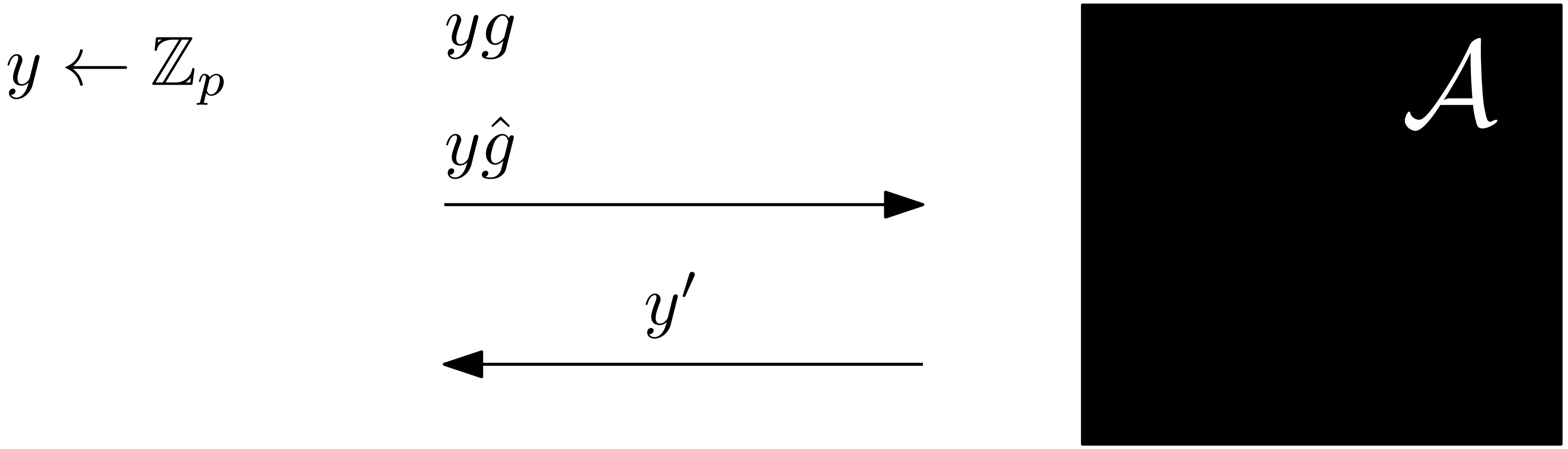
$y \leftarrow \mathbb{Z}_p$



$\mathcal{A}$ wins if $y = y'$

FHS in the AGM

Definition. DL hard for bilinear group $\mathbb{G}, \hat{\mathbb{G}}$ with generators $g, \hat{g}$



$\mathcal{A}$ wins if $y = y'$

FHS in the AGM

Definition. (q_1, q_2)-"power"-DL hard for bilinear group $\mathbb{G}, \hat{\mathbb{G}}$ with generators $g, \hat{g}$

$y \leftarrow \mathbb{Z}_p$

$yg, y^2 g, \ldots, y^{q_1} g$

$y\hat{g}, y^2 \hat{g}, \ldots, y^{q_2} \hat{g}$

$\longrightarrow$

y'

$\longleftarrow$

$\mathcal{A}$ wins if $y = y'$

FHS in the AGM

Theorem. Let $q \in \mathbb{N}$ and $\mathcal{A}$ be algebraic making q signing queries, then there exists $\mathcal{B}$ such that

$$\mathsf{Adv}^{(3q,q+1)\text{-}\mathsf{DL}}_{\mathbb{G},\mathcal{B}} \geq \mathsf{Adv}^{\mathsf{UNF}}_{\mathsf{FHS},\mathcal{A}} - \frac{4q+1}{p-1}$$

FHS in the AGM

Theorem. Let $q \in \mathbb{N}$ and $\mathcal{A}$ be algebraic making q signing queries, then there exists $\mathcal{B}$ such that

$$\mathsf{Adv}_{\mathbb{G},\mathcal{B}}^{(3q,q+1)\text{-}\mathsf{DL}} \geq \mathsf{Adv}_{\mathsf{FHS},\mathcal{A}}^{\mathsf{UNF}} - \frac{4q+1}{p-1}$$

(or from a slightly stronger assumption if not assuming random generators)

Thank you!

questions?