On Proving Equivalence Class Signatures Secure from Non-interactive Assumptions

Balthazar Bauer, Georg Fuchsbauer
and Fabian Regen

PKC, 16 April 24

What is a digital signature scheme?

A *signature scheme* is a triple of p.p.t. algorithms

- Keygen() $\rightarrow (sk, pk)$
- Sign$(sk, m) \rightarrow \sigma$
- Verify$(pk, m, \sigma) \rightarrow 0$ or 1

Equivalence class signatures (EQS) [FHS19]

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

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

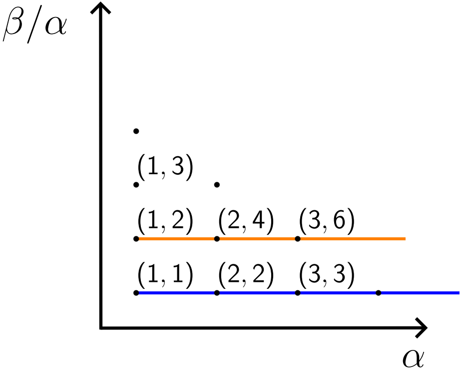
$$m \sim m' :\Leftrightarrow \exists\, \mu \in \mathbb{Z}_p^* : m = \mu \cdot m'$$

Equivalence class signatures (EQS) [FHS19]

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

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

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

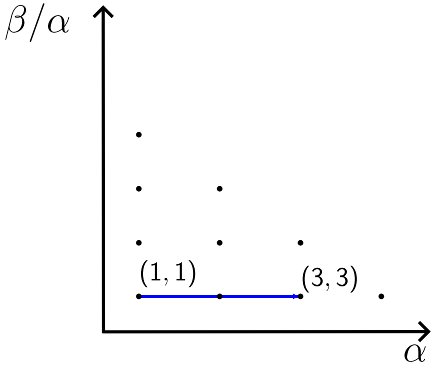


Equivalence classes
for $m = (\alpha \cdot g, \beta \cdot g)$

Equivalence class signatures (EQS) [FHS19]

Additional functionality:

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

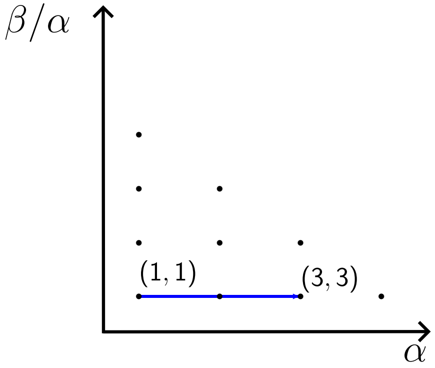


Equivalence classes for $m = (\alpha \cdot g, \beta \cdot g)$

Equivalence class signatures (EQS) [FHS19]

Additional functionality:

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



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

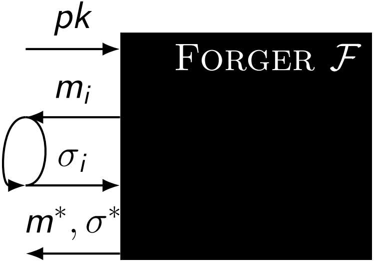
Class hiding:
given m, m'
decide if $m \sim m'$

Unforgeability of signatures

Game UNF:

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

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

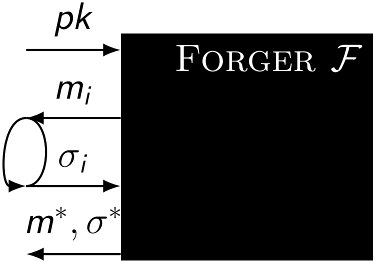


Unforgeability of signatures

Game UNF:

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

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



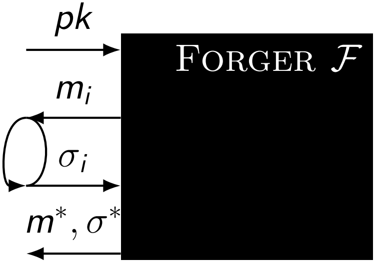
$\mathcal{F}$ wins $\Leftrightarrow$ $\text{Verify}(pk, m^*, \sigma^*) \wedge m^* \neq m_i$

Unforgeability of signatures

Game UNF:

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

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



$$\mathcal{F} \text{ wins} \;\Leftrightarrow\; \mathsf{Verify}(pk, m^*, \sigma^*) \;\wedge\; m^* \neq m_i$$

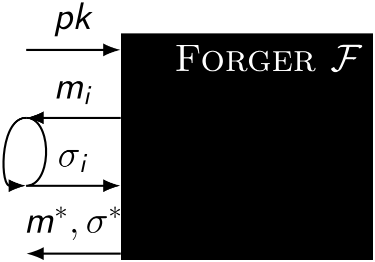
Scheme *secure* if $\mathsf{Adv}^{\mathsf{UNF}}_{\mathcal{F}} := \Pr[\mathcal{F} \text{ wins}] \approx 0$

Security of EQS

Game UNF:

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

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



$$\mathcal{F} \text{ wins } \Leftrightarrow \text{Verify}(pk, m^*, \sigma^*) \wedge [m^*]_\sim \neq [m_i]_\sim$$

Anonymous authentication

Alice chooses $pk = \alpha \cdot g \in \mathbb{G}^*$

– establishes **pseudonym** $(\mu_i \cdot g, \mu_i \cdot pk)$ with party i

Anonymous authentication

Alice chooses $pk = \alpha \cdot g \in \mathbb{G}^*$

– establishes **pseudonym** $(\mu_i \cdot g, \mu_i \cdot pk)$ with party i

– gets **credential**: σ_j on $m_j = (\mu_j \cdot g, \mu_j \cdot pk)$

Anonymous authentication

Alice chooses $pk = \alpha \cdot g \in \mathbb{G}^*$

– establishes **pseudonym** $(\mu_i \cdot g, \mu_i \cdot pk)$ with party i

– gets **credential**: σ_j on $m_j = (\mu_j \cdot g, \mu_j \cdot pk)$

– create credential σ_i for $m_i = (\mu_i \cdot g, \mu_i \cdot pk)$
by running $\mathsf{Adapt}(pk, m, \sigma_j, \mu_i/\mu_j)$

Anonymous authentication

Alice chooses $pk = \alpha \cdot g \in \mathbb{G}^*$

– establishes **pseudonym** $(\mu_i \cdot g, \mu_i \cdot pk)$ with party i

– gets **credential**: σ_j on $m_j = (\mu_j \cdot g, \mu_j \cdot pk)$

– create credential σ_i for $m_i = (\mu_i \cdot g, \mu_i \cdot pk)$
by running $\mathrm{Adapt}(pk, m, \sigma_j, \mu_i/\mu_j)$

Anonymity (even against issuer)**:**

- m_i looks random ($\Leftarrow$ class hiding)
- σ_i is random signature on m_i ($\Leftarrow$ Adapt)

Applications of EQS

Cryptographic concepts constructed from EQS:

Applications of EQS

Cryptographic concepts constructed from EQS:

- Attribute-based credentials [FHS(14|19), DHS15, HS21]

Applications of EQS

Cryptographic concepts constructed from EQS:

- Attribute-based credentials [FHS(14|19), DHS15, HS21]
- Blind signatures [FHS15, FHKS16, Han23]

Applications of EQS

Cryptographic concepts constructed from EQS:

- Attribute-based credentials [FHS(14|19), DHS15, HS21]
- Blind signatures [FHS15, FHKS16, Han23]
- Group signatures [DS16, CS20, DS18, BHKS18]

Applications of EQS

Cryptographic concepts constructed from EQS:

- Attribute-based credentials [FHS(14|19), 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], incentive systems [BEK+20], mix nets [ST21], anonymous counting tokens [BRS23] ...

Constructions of EQS

- Original [FHS(14|19)] (efficient: $\sigma \in \mathbb{G}^2 \times \hat{\mathbb{G}}$)

Constructions of EQS

- Original [FHS(14|19)] (efficient: $\sigma \in \mathbb{G}^2 \times \hat{\mathbb{G}}$)
  - *but:* proof in *generic group model*

Constructions of EQS

- Original [FHS(14|19)] (efficient: $\sigma \in \mathbb{G}^2 \times \hat{\mathbb{G}}$)
  – *but:* proof in *generic group model*
- Weaker unforgeability notion: [FG18]

  (proof from SXDH)

Constructions of EQS

- Original [FHS(14|19)] (efficient: $\sigma \in \mathbb{G}^2 \times \hat{\mathbb{G}}$)
  - *but:* proof in *generic group model*
- Weaker unforgeability notion: [FG18] (proof from SXDH)
  - *but:* too weak for many applications

Constructions of EQS

- Original [FHS(14|19)] (efficient: $\sigma \in \mathbb{G}^2 \times \hat{\mathbb{G}}$)
  - *but:* proof in *generic group model*
- Weaker unforgeability notion: [FG18]
  (proof from SXDH)
  - *but:* too weak for many applications
- CRS model: [KSD19, CLP22]
  (proof from SXDH, (...))

Constructions of EQS

- Original [FHS(14|19)] (efficient: $\sigma \in \mathbb{G}^2 \times \hat{\mathbb{G}}$)
  - *but:* proof in *generic group model*
- Weaker unforgeability notion: [FG18]
  (proof from SXDH)
  - *but:* too weak for many applications
- CRS model: [KSD19, CLP22]
  (proof from SXDH, (...))
  - *but:* anonymity relies on trusted CRS

Constructions of EQS

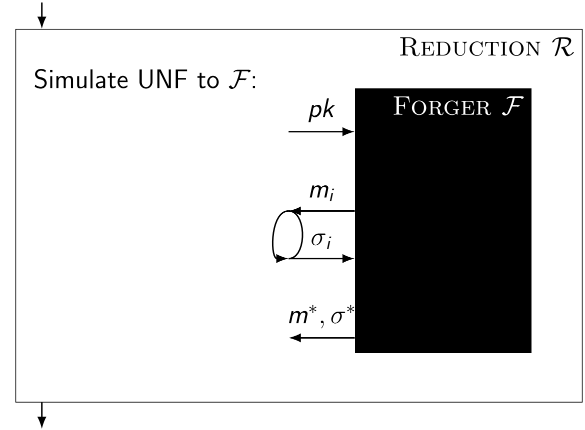
- Original [FHS(14|19)] (efficient: $\sigma \in \mathbb{G}^2 \times \hat{\mathbb{G}}$)
  – *but:* proof in *generic group model*
- Weaker unforgeability notion: [FG18]
  (proof from SXDH)
  – *but:* too weak for many applications
- CRS model: [KSD19, CLP22]
  (proof from SXDH, (...))
  – *but:* anonymity relies on trusted CRS

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

Security reductions

Reduction $\mathcal{R}$ from computational problem Π to UNF
using adversary $\mathcal{F}$

$\Pi : c$



s

Security reductions

If Π is hard and $\mathcal{R}$ reduces Π to UNF,
then UNF is hard

Concrete: $\mathcal{R}$ is ϕ-*tight* if given $\mathcal{F}$ that wins UNF with prob. ϵ, $\mathcal{R}$ breaks Π with prob. $\phi \cdot \epsilon$

Security reductions

If Π is hard and $\mathcal{R}$ reduces Π to UNF,
then UNF is hard

Concrete: $\mathcal{R}$ is ϕ-*tight* if given $\mathcal{F}$ that wins UNF with prob. ϵ, $\mathcal{R}$ breaks Π with prob. $\phi \cdot \epsilon$

Theorem. For any EQS scheme and any Π, no reduction can exist

Proof idea

Simplification: Assume $\mathcal{R}$ partitions $(\mathbb{G}^*)^2$ into **signable** and **exploitable** messages

$S := \{m \mid \mathcal{R} \text{ can answer a signing query for } m\}$

$E := \{m \mid \text{given (uniform) forgery on } m, \mathcal{R} \text{ wins } \Pi\}$

Proof idea

Simplification: Assume $\mathcal{R}$ partitions $(\mathbb{G}^*)^2$ into **signable** and **exploitable** messages

$S := \{m \mid \mathcal{R} \text{ can answer a signing query for } m\}$

$E := \{m \mid \text{given (uniform) forgery on } m, \mathcal{R} \text{ wins } \Pi\}$

- S and E must both be "big"

Proof idea

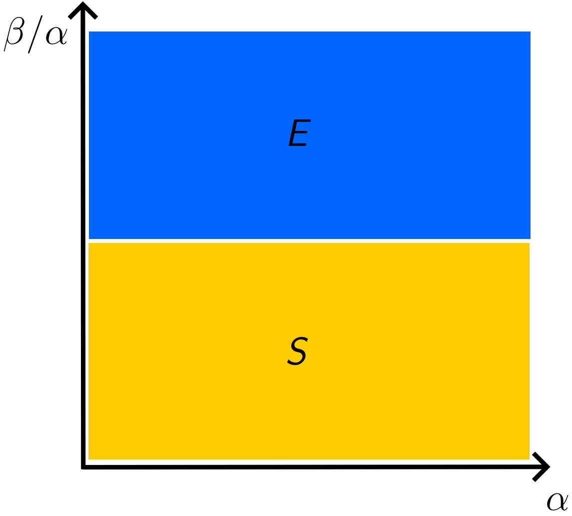
Simplification: Assume $\mathcal{R}$ partitions $(\mathbb{G}^*)^2$ into **signable** and **exploitable** messages

$S := \{m \mid \mathcal{R}$ can answer a signing query for $m\}$

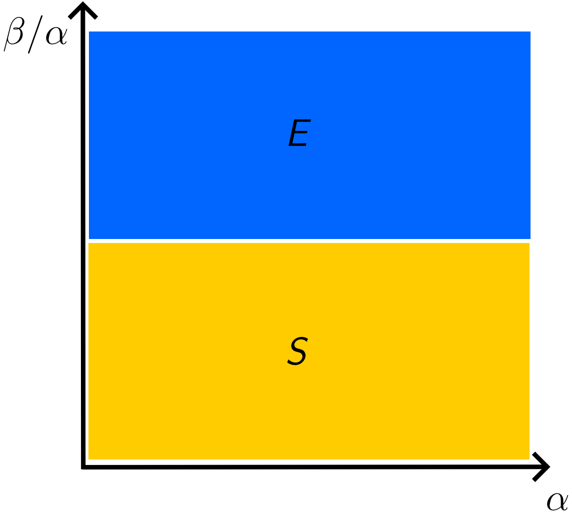
$E := \{m \mid$ given (uniform) forgery on m, $\mathcal{R}$ wins $\Pi\}$

- S and E must both be "big"
- do not intersect

Case 1: E and S do not share classes

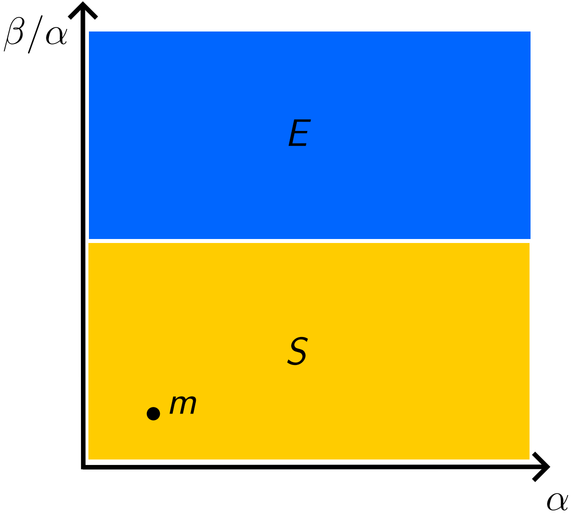


Case 1: E and S do not share classes



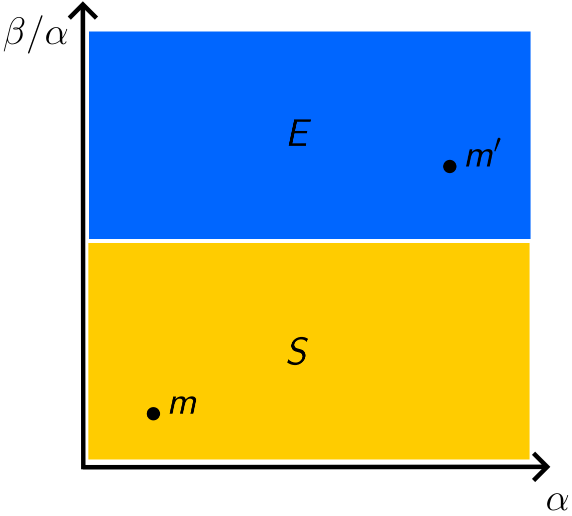
class hiding: given m, m' decide if $m \sim m'$

Case 1: E and S do not share classes



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

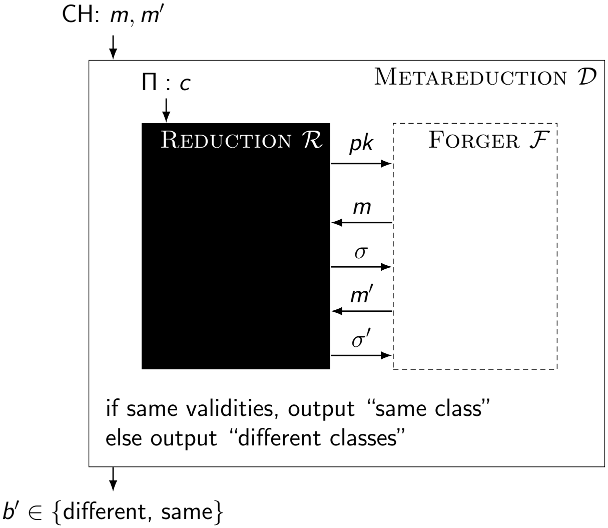
Case 1: E and S do not share classes



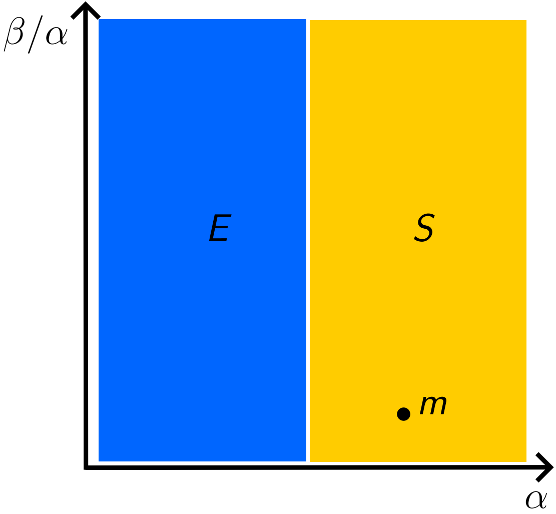
class hiding:
given m, m'
decide if $m \sim m'$

if exactly one message signable then separate classes

Breaking class hiding

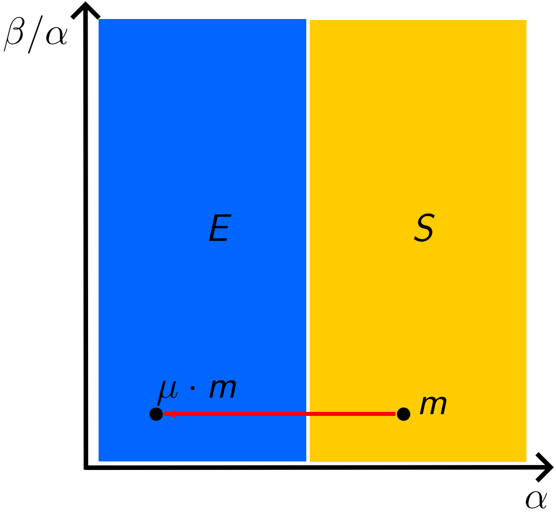


Case 2: E and S share classes



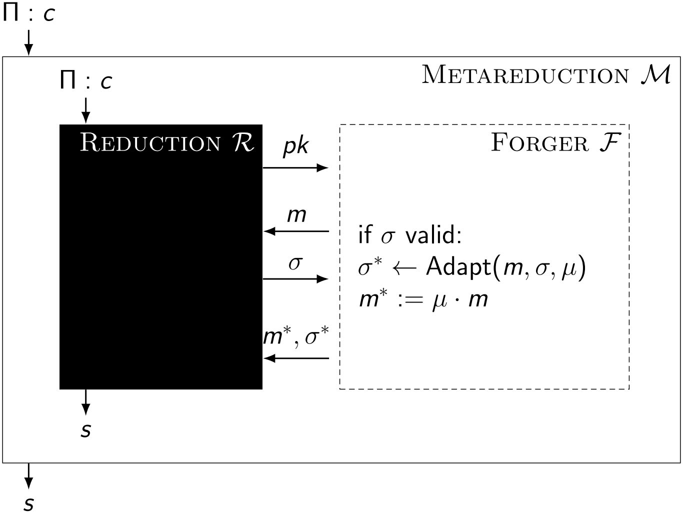
Solve Π:

Case 2: E and S share classes



Solve Π:

Solving Π



Π : c
METAREDUCTION $\mathcal{M}$
Π : c
REDUCTION $\mathcal{R}$
pk
m
σ
m^*, σ^*
FORGER $\mathcal{F}$
if σ valid:
$\sigma^* \leftarrow \mathsf{Adapt}(m, \sigma, \mu)$
$m^* := \mu \cdot m$
s
s

Theorem

For any

- EQS scheme Σ
- computational problem Π
- reduction $\mathcal{R}$ w/ tightness ϕ and running time τ

Theorem

For any

- EQS scheme Σ
- computational problem Π
- reduction $\mathcal{R}$ w/ tightness ϕ and running time τ

there exist

- $\mathcal{D}$ attacking class hiding of Σ running in $\approx 2\tau$
- $\mathcal{M}$ attacking Π running in $\approx \tau$
- $\mathcal{F}$ attacking UNF running in constant time

Theorem

For any

- EQS scheme Σ
- computational problem Π
- reduction $\mathcal{R}$ w/ tightness ϕ and running time τ

there exist

- $\mathcal{D}$ attacking class hiding of Σ running in $\approx 2\tau$
- $\mathcal{M}$ attacking Π running in $\approx \tau$
- $\mathcal{F}$ attacking UNF running in constant time

such that

$$\mathsf{Adv}^{\mathrm{CH}}_{\Sigma,\mathcal{D}^{\mathcal{R}}} + \mathsf{Adv}^{\Pi}_{\mathcal{M}^{\mathcal{R}}} + \mathsf{Adv}^{\Pi}_{\mathcal{R}^{\mathcal{F}}} \geq \frac{\phi^5}{384}$$

Overcoming impossibility?

Impossibility result does not apply to schemes in CRS model [KSD19, CLP22]

Overcoming impossibility?

Impossibility result does not apply to schemes in CRS model [KSD19, CLP22]

Schemes [KSD19, CLP22] claimed secure under standard assumptions

Overcoming impossibility?

Impossibility result does not apply to schemes in CRS model [KSD19, CLP22]

Schemes [KSD19, CLP22] claimed secure under standard assumptions

Result. Their proofs are flawed[1]

[1] B. Bauer, G. Fuchsbauer, F. Regen: On security proofs of existing equivalence class signature schemes (ia.cr/2024/183)