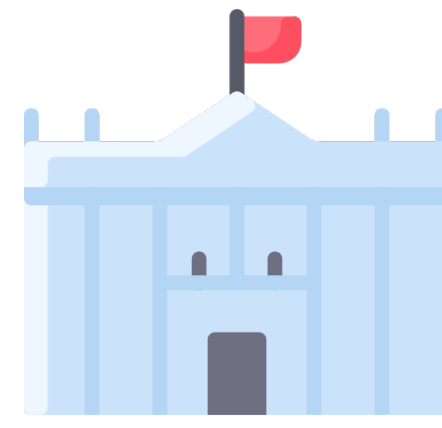


Mercurial Signatures for Variable-Length Messages

Elizabeth C. Crites (IOG) and Anna Lysyanskaya (Brown)

Certification Authority (CA)



pk_A



σ_2



pk_B

pk'_A



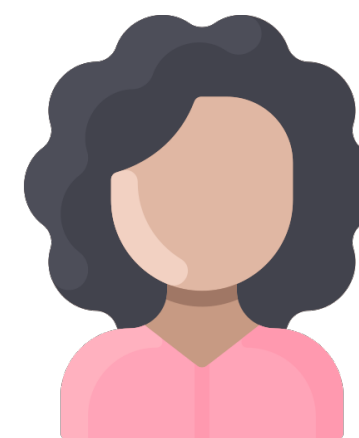
σ'_2



pk'_B

σ_3

pk_C



σ_1

σ'_1



Certificate: public keys and signatures

Mercurial Signatures: Definition

Signatures on Equivalence Classes [FHS19]

$\text{Sign}(\text{pk}, \text{sk}, M) \rightarrow \sigma$

$\text{Verify}(\text{pk}, M, \sigma) \rightarrow 0/1$

Correctness:

$\text{Verify}(\text{pk}, M, \sigma) \rightarrow 1$

$M \approx M$

[FHS19] Construction:

$M = (g^{\mu \cdot a}, g^{\mu \cdot b}, g^{\mu \cdot c}) \approx M = (g^a, g^b, g^c)$

Security:

$\text{Verify}(\text{pk}, M^*, \sigma^*) \rightarrow 1$

$M^* \not\approx M_i \forall M_i \in Q$

Mercurial Signatures [CL19]

$\text{Sign}(\text{pk}, \text{sk}, M) \rightarrow \sigma$

$\text{Verify}(\text{pk}, M, \sigma) \rightarrow 0/1$

Correctness:

$\text{Verify}(\text{pk}, M, \sigma) \rightarrow 1$

$M \approx M, \text{pk} \approx \text{pk}$

Security:

$\text{Verify}(\text{pk}^*, M^*, \sigma^*) \rightarrow 1$

$M^* \not\approx M_i \ \forall M_i \in Q \wedge \text{pk}^* \approx \text{pk}$

Property: Class-Hiding

Message Class-Hiding:

$$M \approx M?$$

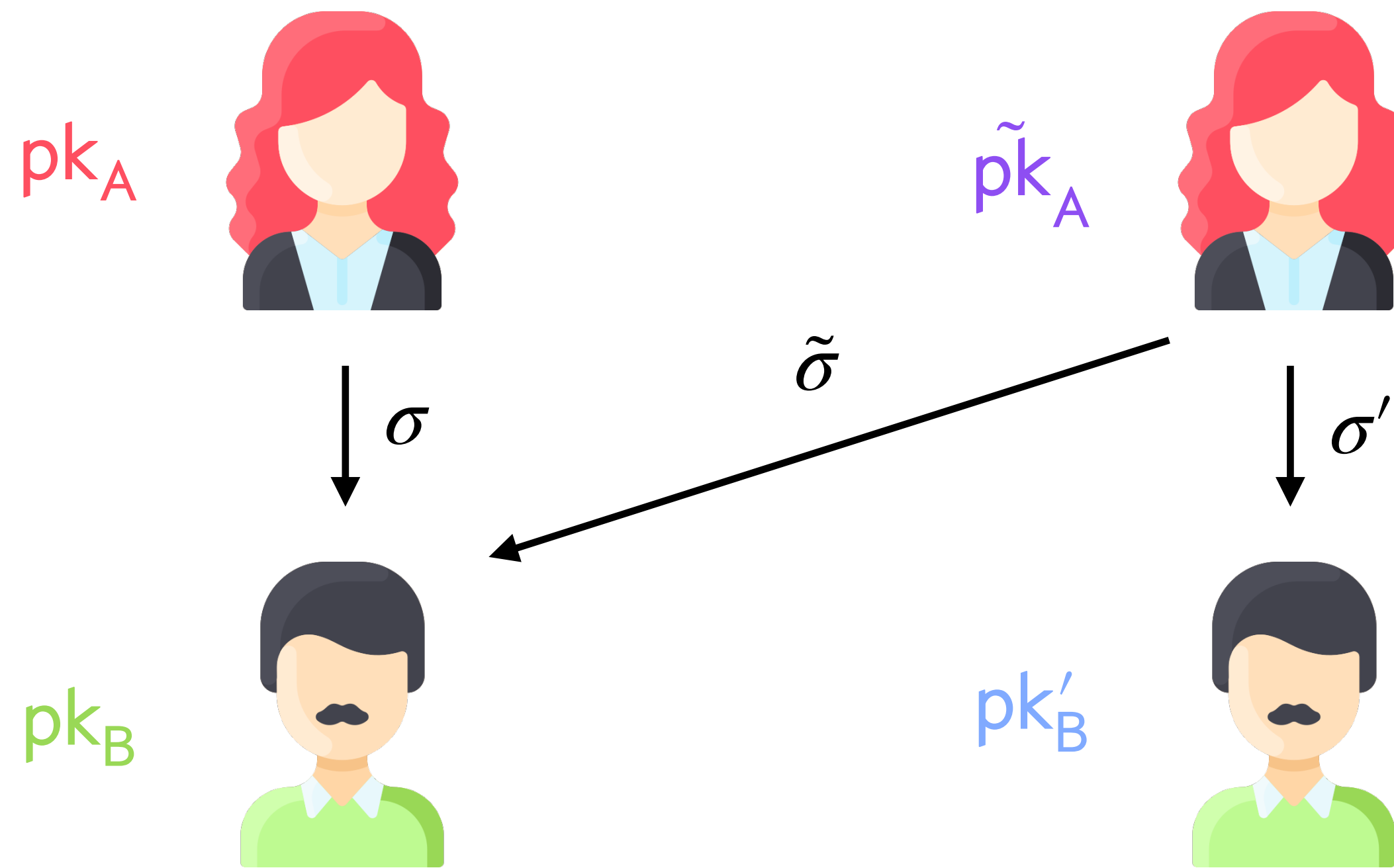
Hard to tell.

Public Key Class-Hiding:

$$pk \approx pk?$$

Hard to tell - even when given signatures under both.

Property: Origin-Hiding



- Transformed $(\tilde{\sigma}, \tilde{pk})$ should be distributed like a fresh signature under $[pk]$
- Transformed (σ', pk') should be distributed like a fresh signature on $[M]$

Mercurial Signatures

Transformation:

$$(\text{pk}, M, \sigma) \rightarrow (\text{pk}, M, \sigma')$$

such that

pk, pk unlinkable

M, M unlinkable

Mercurial Signatures: Construction

Mercurial Signatures: Construction [CL19]



$$e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$$

$$\text{pk}_A = (\hat{P}^{x_1}, \dots, \hat{P}^{x_\ell}) \text{ in } \mathbb{G}_2 \quad \text{sk}_A = (x_1, \dots, x_\ell) \text{ in } \mathbb{Z}_p$$

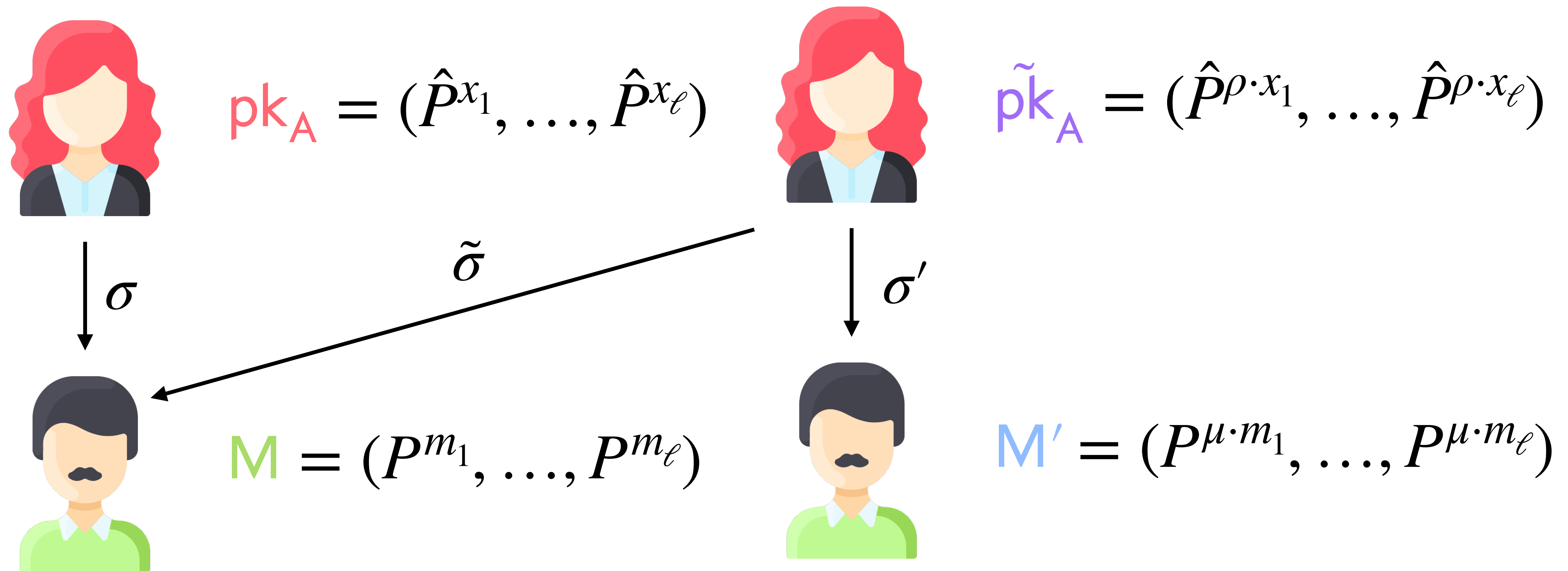


$$\sigma = (Z, Y, \hat{Y}) \text{ in } \mathbb{G}_1 \times \mathbb{G}_1 \times \mathbb{G}_2$$



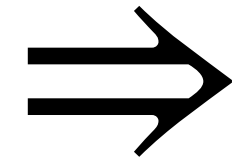
$$\text{pk}_B = M = (P^{m_1}, \dots, P^{m_\ell}) \text{ in } \mathbb{G}_1$$

Mercurial Signatures: Construction



Prior Results [CL19]

(Certain) Mercurial Signatures

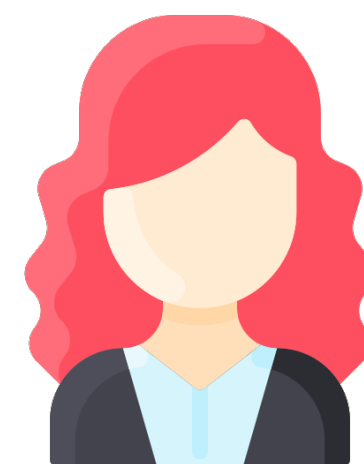
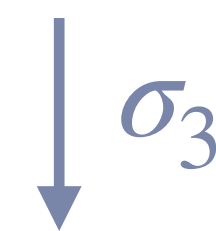
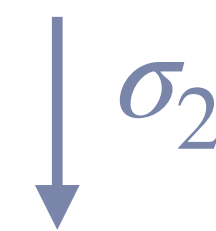
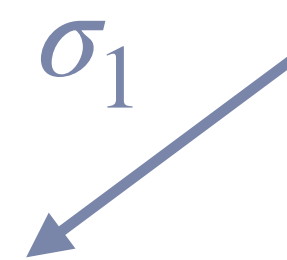
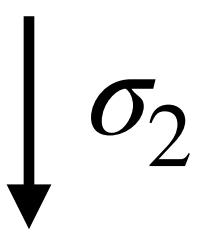
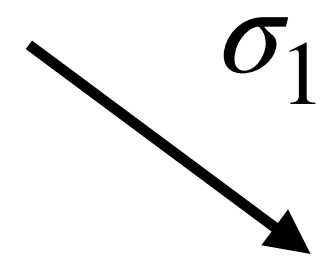
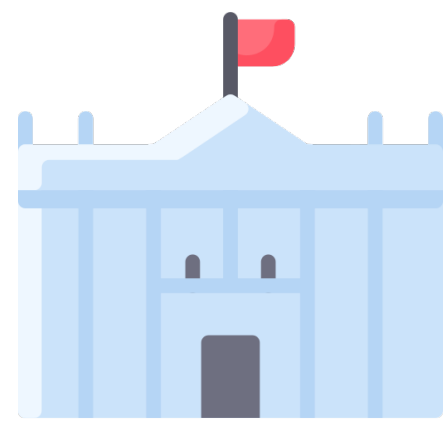


Delegatable Anonymous Credentials

First direct construction.

Mercurial Signatures for Variable- Length Messages

Why variable-length?



sk_A of length ℓ or $\ell - 2$?

$$\underbrace{(\text{pk}_A, \text{attr}_A)}_{\ell} = (\hat{P}^{x_1}, \dots, \hat{P}^{x_\ell}, P^a)$$

$$\underbrace{(\text{pk}_B, \text{attr}_B)}_{\ell - 1} = (P^{z_1}, \dots, P^{z_{\ell-1}}, P^b)$$

Mercurial Signatures for Variable- Length Messages: Construction

Signing Variable-Length Messages

$$m = (\hat{g}, u_1, \dots, u_n) \text{ in } \mathbb{G}_1$$

Break into n messages:

$$M_1 = (\tilde{g}, \tilde{g}^1, \tilde{g}^n, \tilde{h}, \tilde{u}_1)$$

$$M_2 = (\tilde{g}, \tilde{g}^2, \tilde{g}^n, \tilde{h}, \tilde{u}_2)$$

\vdots

$$M_n = (\tilde{g}, \tilde{g}^n, \tilde{g}^n, \tilde{h}, \tilde{u}_n)$$

If m' gets signed,

$$M'_i \approx M_i \quad \forall i$$

Sign each with original scheme [CL19] for $\ell = 5$.

How To Build Glue

$$m = (\hat{g}, u_1, \dots, u_n) \text{ in } \mathbb{G}_1$$

$$u_i = \hat{g}^{m_i} \quad \forall i$$

$$p_m(x) = m_1 + m_2x + m_3x^2 + \dots + m_nx^{n-1}$$

Evaluate $p_m(x)$ at secret point \hat{x} and compute glue as:

$$\hat{h} = \hat{g}^{p_m(\hat{x})}$$

How To Build Glue

Sample random w and set:

$$\begin{aligned}\tilde{g} &= \hat{g}^w, \tilde{u}_i = u_i^w \quad \forall i \\ \tilde{m} &= (\tilde{g}, \tilde{u}_1, \dots, \tilde{u}_n)\end{aligned}$$

Compute glue using secret y as:

$$\tilde{h} = \tilde{g}^{y \cdot p_m(\hat{x})} = \left(\prod_{i=1}^n \tilde{u}_i^{\hat{x}^{i-1}} \right)^y$$

Output \tilde{m} and signature (\tilde{h}, σ) .

MS for Variable-Length Messages



$$pk_A = (\hat{P}^{x_1}, \dots, \hat{P}^{x_5}, \hat{P}^{x_6}, \hat{P}^{x_6 \cdot \hat{x}}, \hat{P}^{x_8}, \hat{P}^{x_8 \cdot y_1}, \hat{P}^{x_8 \cdot y_2}), y = y_1 \cdot y_2$$



$$(\tilde{h}, \sigma = \sigma_1, \dots, \sigma_n)$$

$$(\hat{P}^{x_1}, \dots, \hat{P}^{x_5}), M_i = (\tilde{g}, \tilde{g}^i, \tilde{g}^n, \tilde{h}, \tilde{u}_i), \sigma_i \quad [\text{CL19}], \ell = 5$$



$$M = (P^{m_1}, \dots, P^{m_n})$$

MS for Variable-Length Messages

Unforgeability ?

Message Class-Hiding ✓

Public Key Class-Hiding ✓

Origin-Hiding of $(pk, \sigma) \rightarrow (\tilde{pk}, \tilde{\sigma})$?

Origin-Hiding of $(m, \sigma) \rightarrow (m', \sigma')$?

Interactive Signing Protocol

$$m = (\hat{g}, u_1, \dots, u_n)$$

$$[\text{Signer} \leftrightarrow \text{Receiver}] \rightarrow (\tilde{h}, \sigma)$$

Step 1. Receiver gives ZKPoK of m_i 's such that $u_i = \hat{g}^{m_i} \forall i$.

Step 2. Signer computes \tilde{h} and σ .

Step 3. Signer gives ZKPoK that \tilde{h} was computed correctly.

EUF-CoMA: existential unforgeability against chosen open message attacks (Step 1) [FG18].

Results

Mercurial signatures for variable-length messages for the equivalence relation

$$(g^{\mu \cdot a}, g^{\mu \cdot b}, g^{\mu \cdot c}) \approx (g^a, g^b, g^c)$$

that are secure in the generic group model (under ABDDH).

Thank you!

elizabeth_crites@alumni.brown.edu