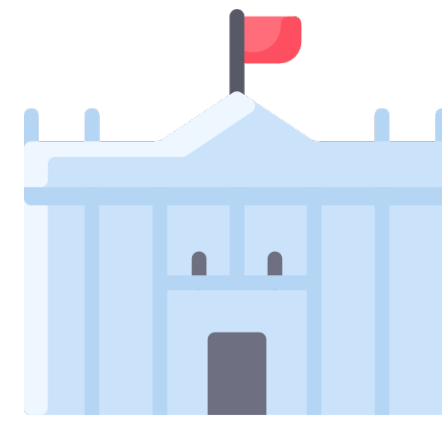


# Delegatable Anonymous Credentials from Mercurial Signatures

Elizabeth Crites (Edinburgh) and Anna Lysyanskaya (Brown)

Certification Authority (CA)



$\sigma_1$

$\sigma'_1$

$pk_A$



$pk'_A$



$\sigma_2$

$\sigma'_2$

$pk_B$

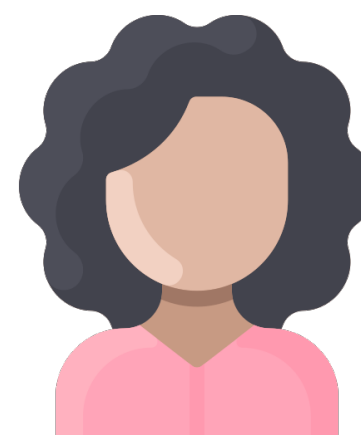


$pk'_B$



$\sigma_3$

$pk_C$



Certificate: public keys  
and signatures

# Prior Work on Delegatable Anonymous Credentials

- [CL06]: proof-of-concept construction
- [BCC+09]: efficiency improvement but not practical
- [CKLM13]: stronger security but as inefficient as [BCC+09]
- [CDD17]: no anonymity in delegation

**Why is our solution interesting?**

# Mercurial Signatures: Definition

# Standard Signatures [GMR88]

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

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

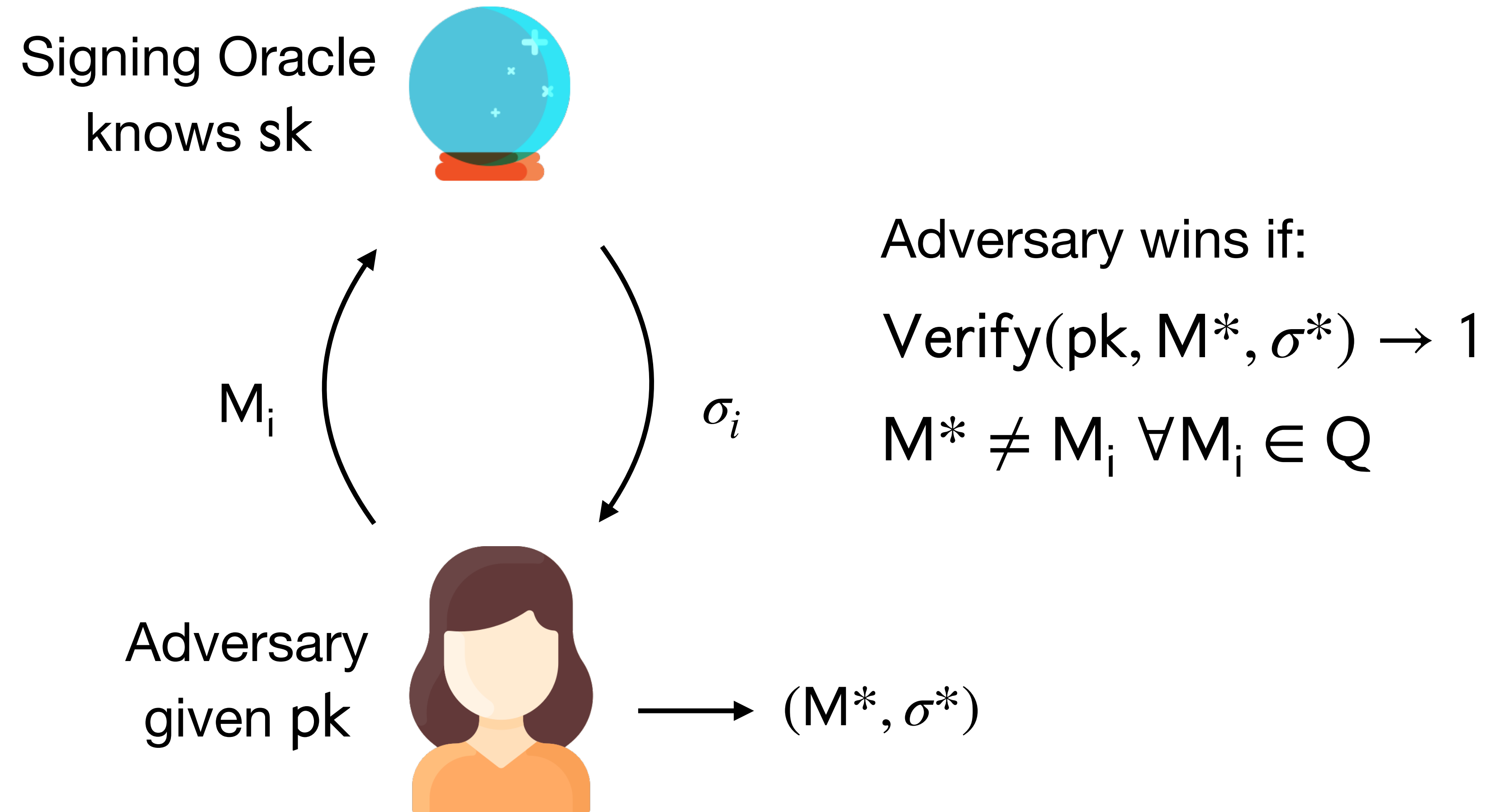
**Correctness:**

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

$M = M$

**Security: (EUF-CMA)**

# Standard Signatures [GMR88]



# Signatures on Equivalence Classes [FHS19]

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

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

**Correctness:**

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

$$\mathbf{M} \approx \mathbf{M}$$

**Security:**

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

$$\mathbf{M}^* \not\approx \mathbf{M}_i \quad \forall \mathbf{M}_i \in \mathcal{Q}$$

**[FHS19] Construction:**

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



# Mercurial Signatures [CL19]

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

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

**Correctness:**

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

$\textcolor{blue}{M} \approx \textcolor{green}{M}, \textcolor{blue}{pk} \approx \textcolor{red}{pk}$

**Security:**

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

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

# Property: Class-Hiding

## Message Class-Hiding:

$$M \approx M?$$

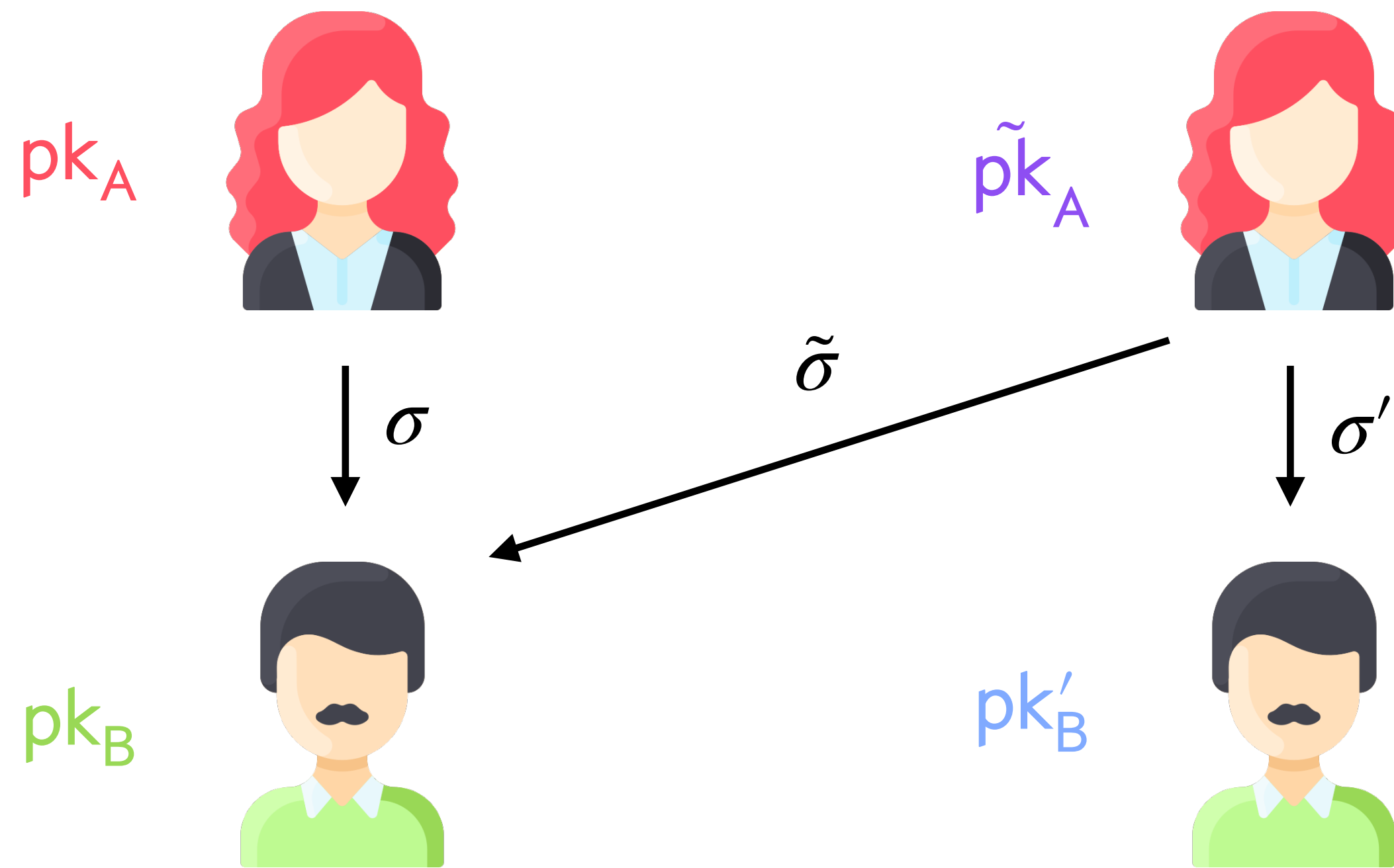
Hard to tell.

## 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  $(\sigma', pk')$  should be distributed like a fresh signature on  $[M]$

# Mercurial Signatures

## Transformation:

$$(\textcolor{red}{pk}, \textcolor{green}{M}, \sigma) \rightarrow (\textcolor{purple}{pk}, \textcolor{blue}{M}, \sigma')$$

such that

$\textcolor{red}{pk}, \textcolor{purple}{pk}$  unlinkable

$\textcolor{green}{M}, \textcolor{blue}{M}$  unlinkable

# Mercurial Signatures: Construction

# Mercurial Signatures: Construction



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

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



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

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

# Mercurial Signatures: Construction

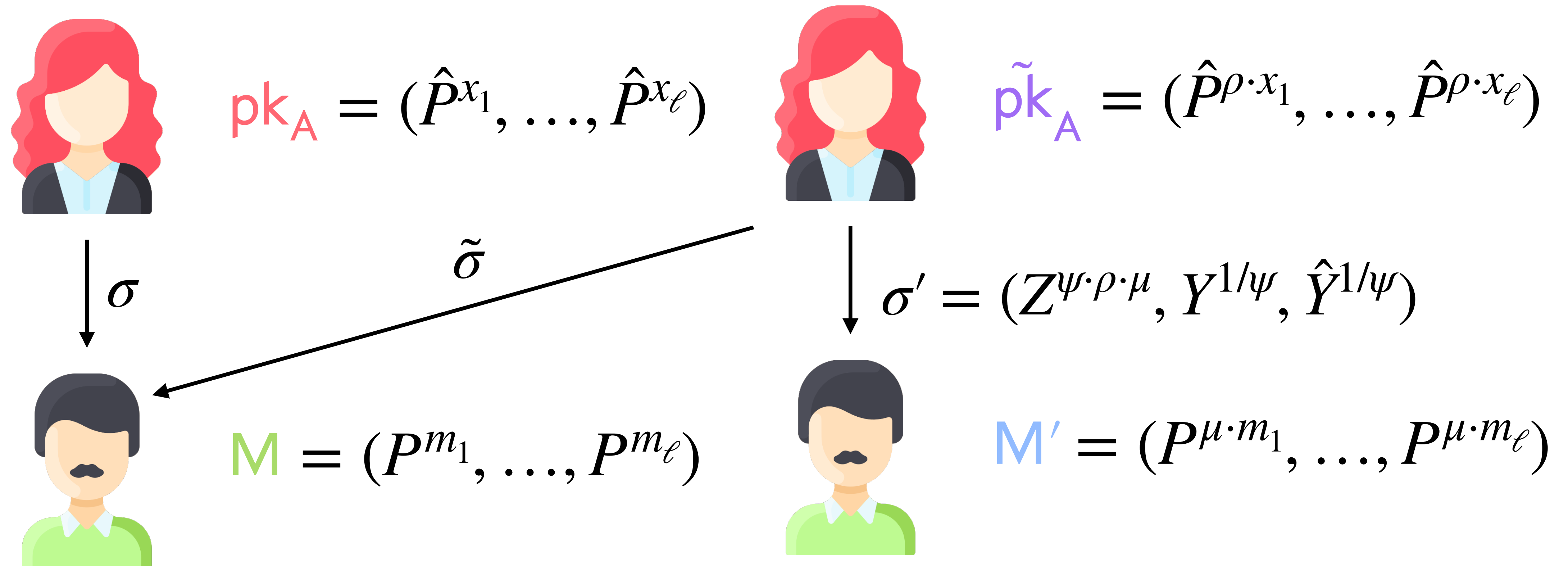
$$\sigma = (Z, Y, \hat{Y}) \text{ in } \mathbb{G}_1 \times \mathbb{G}_1 \times \mathbb{G}_2$$

$$Z = \left( \prod_{i=1}^{\ell} P^{m_i \cdot x_i} \right)^{\gamma}, Y = P^{1/\gamma}, \hat{Y} = \hat{P}^{1/\gamma}$$

$$\prod_{i=1}^{\ell} e(P^{m_i}, \hat{P}^{x_i}) = e(Z, \hat{Y})$$

$$e(Y, \hat{P}) = e(P, \hat{Y})$$

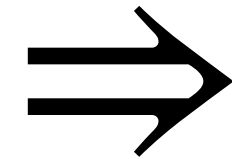
# Mercurial Signatures: Construction





# Results [CL19]

(Certain) Mercurial Signatures



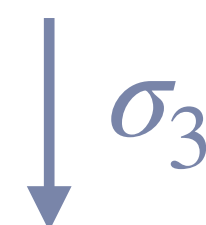
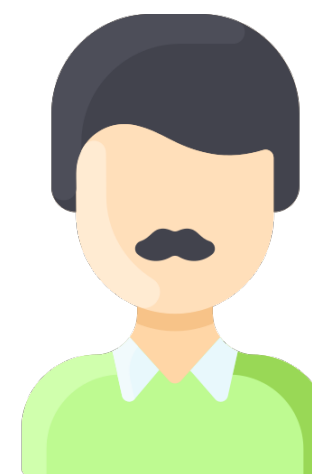
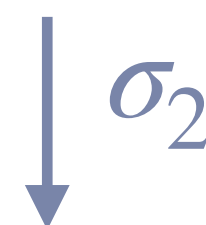
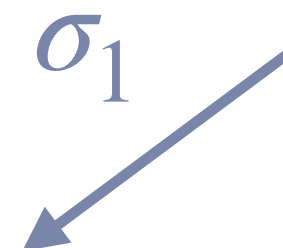
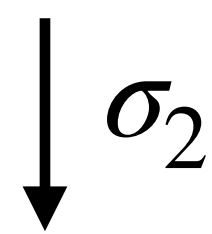
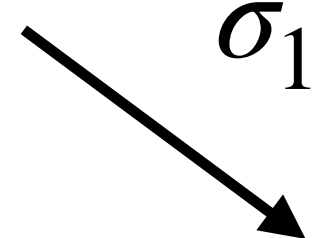
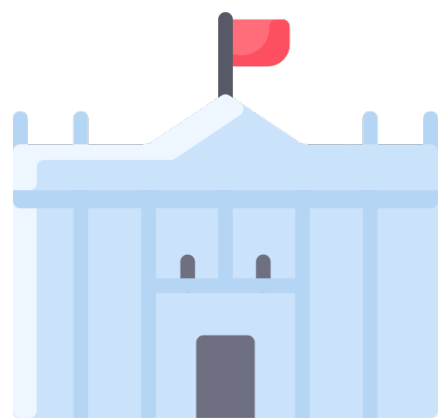
Delegatable Anonymous Credentials

First direct construction.

Proven in the generic group model.

# Mercurial Signatures for Variable- Length Messages

# Why variable-length?



sk<sub>A</sub> of length  $\ell$  or  $\ell - 2$  ?

# 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  $m' \approx m$  gets signed,  $M'_i \approx M_i \ \forall i$ .

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:

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

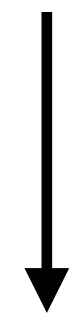
Output  $\tilde{m}$  and signature  $(\tilde{h}, \sigma)$ .



# MS for Variable-Length Messages



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



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

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

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

# 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  $\sigma$ .

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

**EUFCoMA:** existential unforgeability against chosen open message attacks (Step 1) [FG18].

# Results [CL21]

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).

# Future Work

- Efficient multi-authority delegatable anonymous credentials
- Selective disclosure of credential attributes
- Revocation
- Conditional anonymity
- Different equivalence classes
- Post-quantum signature scheme with similar randomization properties

# Thank you!

**elizabeth\_crites@alumni.brown.edu**