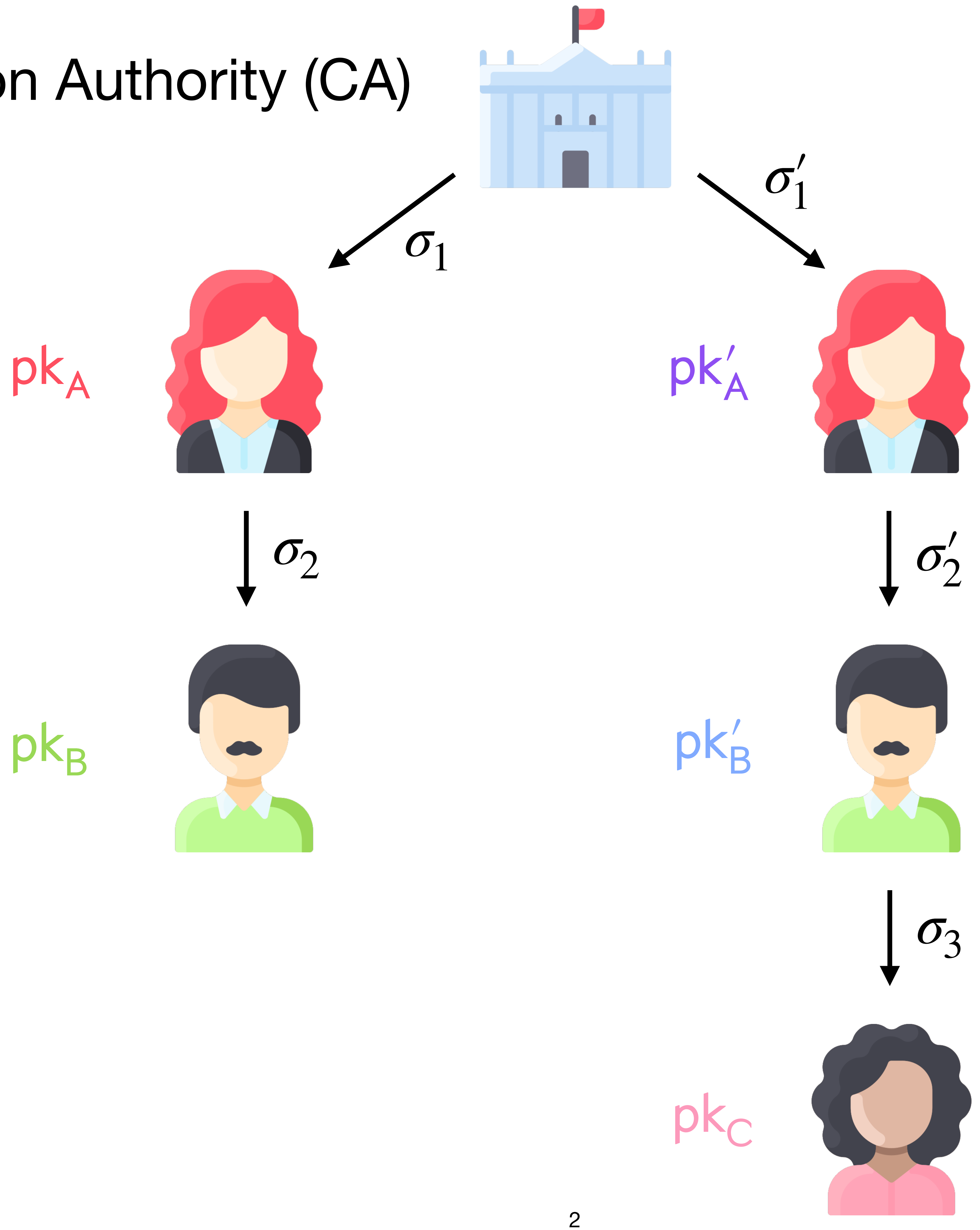
Delegatable Anonymous Credentials from Mercurial Signatures

Elizabeth Crites (Edinburgh) and Anna Lysyanskaya (Brown)

Future of PI - Sept. 6, 2021

Certification Authority (CA)



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]

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

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

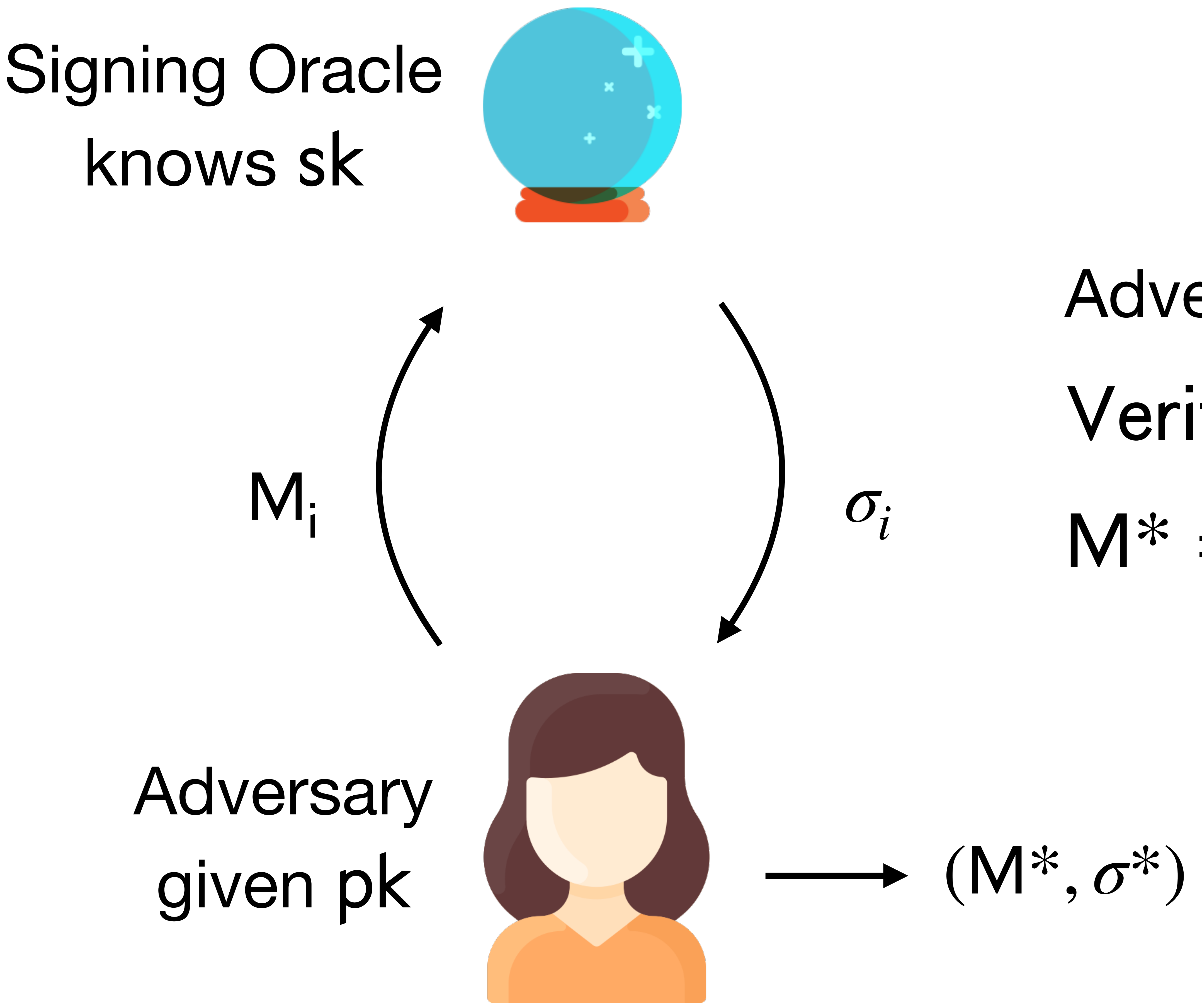
Correctness:

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

$\mathsf{M} = \mathsf{M}$

Security: (EUF-CMA)

Standard Signatures [GMR88]



Adversary wins if:

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

$M^* \neq M_i \ \forall M_i \in Q$

Signatures on Equivalence Classes [FHS19]

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

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

Correctness:

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

$\text{M} \approx \text{M}$

Security:

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

$\text{M}^* \not\approx \text{M}_i \ \forall \text{M}_i \in \text{Q}$

[FHS19] Construction:

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

Mercurial Signatures [CL19]

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

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

Correctness:

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

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

Security:

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

$\mathrm{M}^* \not\approx \mathrm{M}_i \; \forall \mathrm{M}_i \in \mathrm{Q} \wedge \mathrm{pk}^* \approx \mathrm{pk}$

Property: Class-Hiding

Message Class-Hiding:

$$\mathsf{M} \approx \mathsf{M}?$$

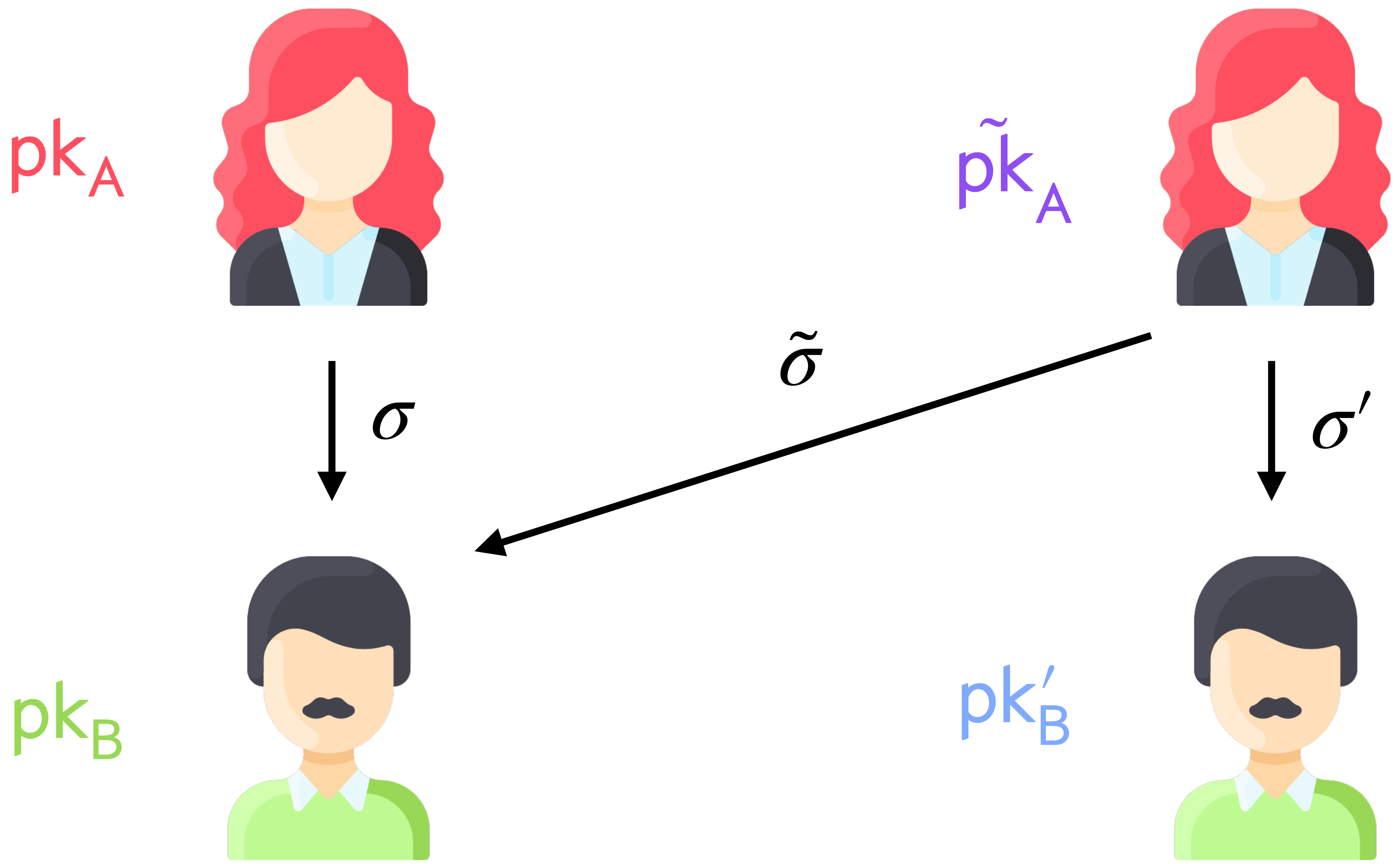
Hard to tell.

Public Key Class-Hiding:

$$\mathsf{pk} \approx \mathsf{pk}?$$

Hard to tell - even when given signatures under both.

Property: Origin-Hiding



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

Mercurial Signatures

Transformation:

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

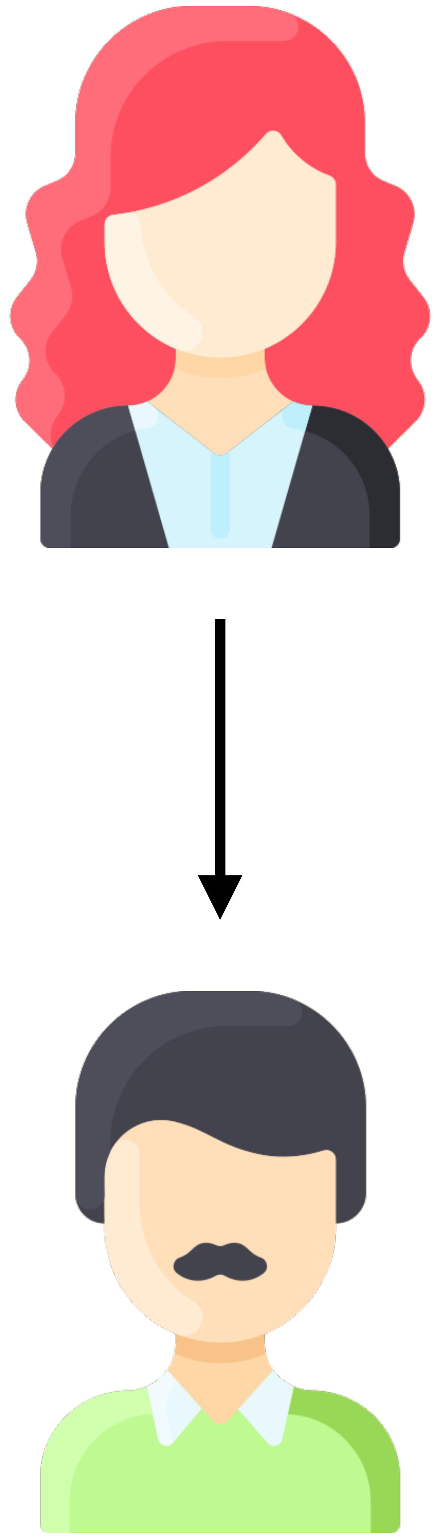
such that

pk, pk unlinkable

M, M unlinkable

Mercurial Signatures: Construction

Mercurial Signatures: Construction



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

$\mathsf{pk_A} = (\hat{P}^{x_1}, \ldots, \hat{P}^{x_\ell})$ in $\mathbb{G}_2$ $\quad$ $\mathsf{sk_A} = (x_1, \ldots, x_\ell)$ in $\mathbb{Z}_p$

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

$\mathsf{pk_B} = \mathsf{M} = (P^{m_1}, \ldots, P^{m_\ell})$ in $\mathbb{G}_1$

Mercurial Signatures: Construction

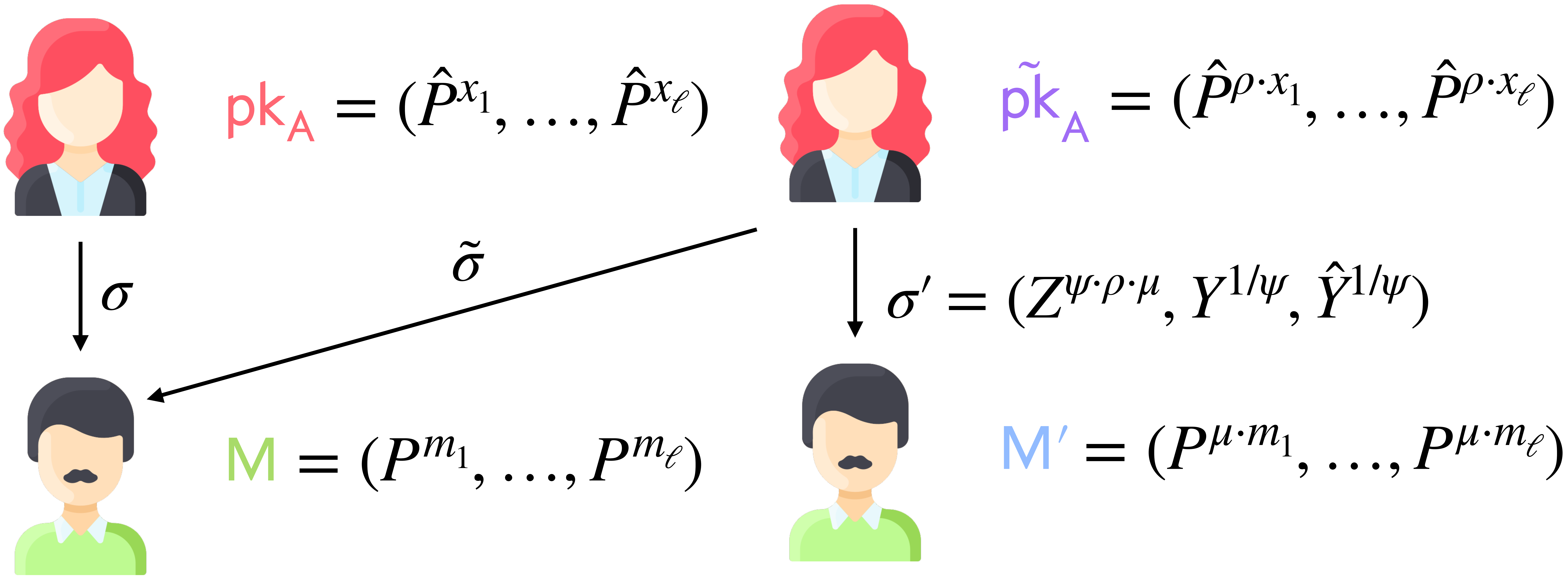
$$\sigma = (Z, Y, \hat{Y}) \text{ in } \mathbb{G}_1 \times \mathbb{G}_1 \times \mathbb{G}_2$$

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

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

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

Mercurial Signatures: Construction



Results [CL19]

(Certain) Mercurial Signatures

$\Rightarrow$

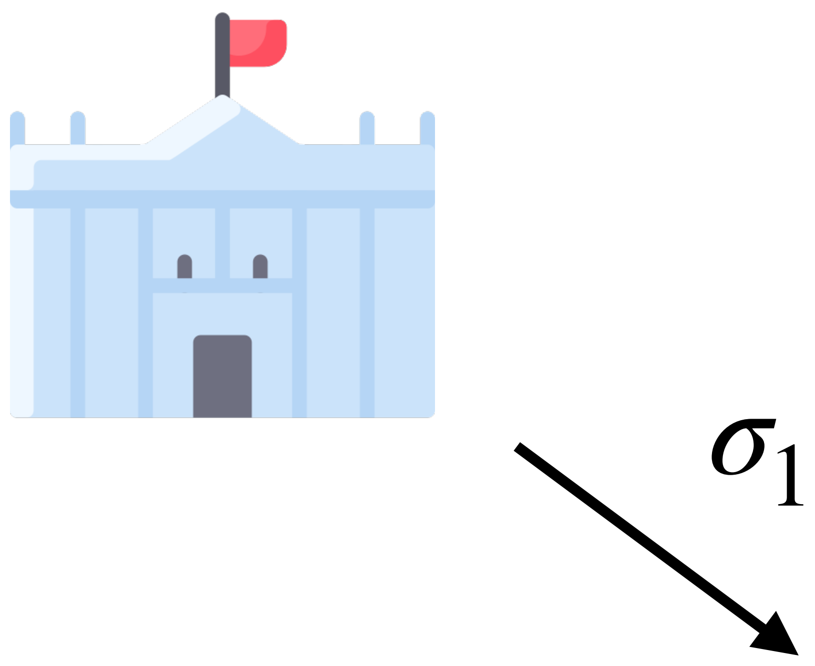
Delegatable Anonymous Credentials

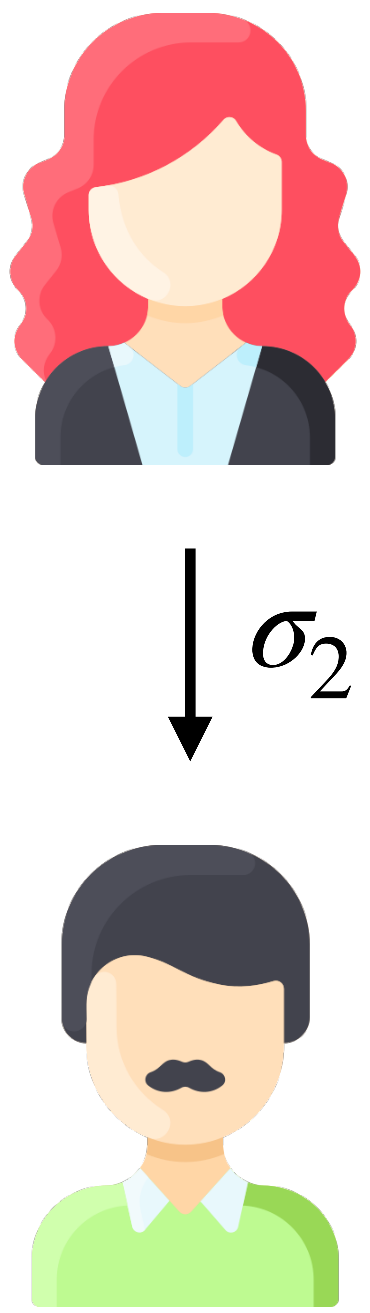
First direct construction.

Proven in the generic group model.

Mercurial Signatures for Variable-Length Messages

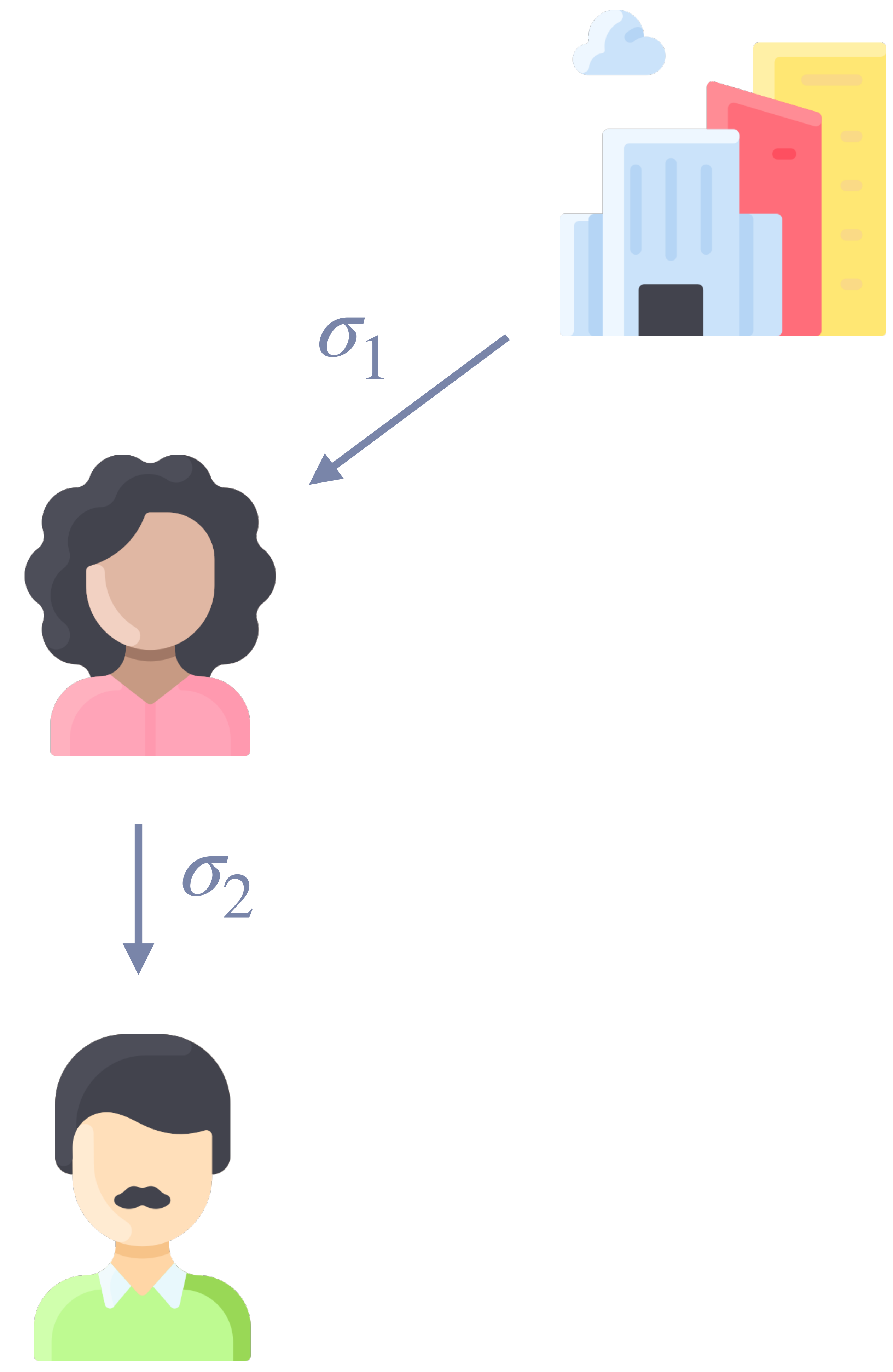
Why variable-length?

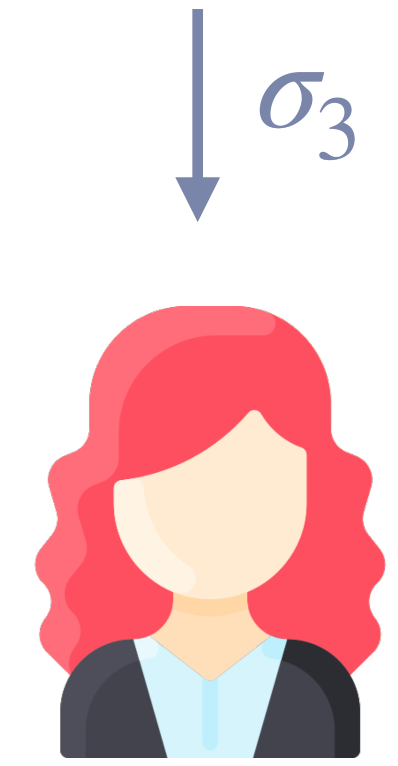




$$\underbrace{(\mathsf{pk_A}, \mathsf{attr_A})}_{\ell} = (\hat{P}^{x_1}, \ldots, \hat{P}^{x_\ell}, P^{a})$$

$$\underbrace{(\mathsf{pk_B}, \mathsf{attr_B})}_{\ell - 1} = (P^{z_1}, \ldots, P^{z_{\ell-1}}, P^{b})$$





$\mathsf{sk_A}$ of length ℓ or $\ell - 2$?

Mercurial Signatures for Variable-Length Messages: Construction

Signing Variable-Length Messages

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

Break into n messages:

$$\begin{gathered}
M_1 = (\tilde{g}, \tilde{g}^1, \tilde{g}^n, \tilde{h}, \tilde{u}_1) \\
M_2 = (\tilde{g}, \tilde{g}^2, \tilde{g}^n, \tilde{h}, \tilde{u}_2) \\
\vdots \\
M_n = (\tilde{g}, \tilde{g}^n, \tilde{g}^n, \tilde{h}, \tilde{u}_n)
\end{gathered}$$

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

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

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

$$p_m(x) = m_1 + m_2 x + m_3 x^2 + \ldots + m_n x^{n-1}$$

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:

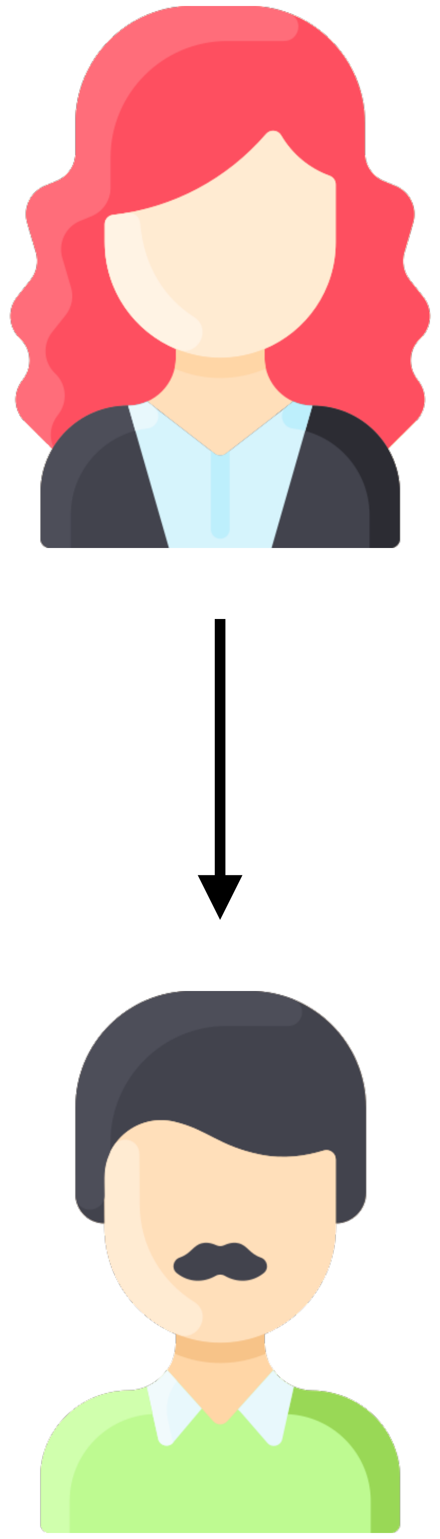
$$\tilde{g} = \hat{g}^{w}, \tilde{u}_i = u_i^{w} \ \forall i$$
$$\tilde{m} = (\tilde{g}, \tilde{u}_1, \ldots, \tilde{u}_n)$$

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



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

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

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

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

MS for Variable-Length Messages

Unforgeability ?

Message Class-Hiding ✓

Public Key Class-Hiding ✓

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

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

Interactive Signing Protocol

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

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

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 <u>*open*</u> 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).

Thank you!

elizabeth_crites@alumni.brown.edu