RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: CRYP-F03

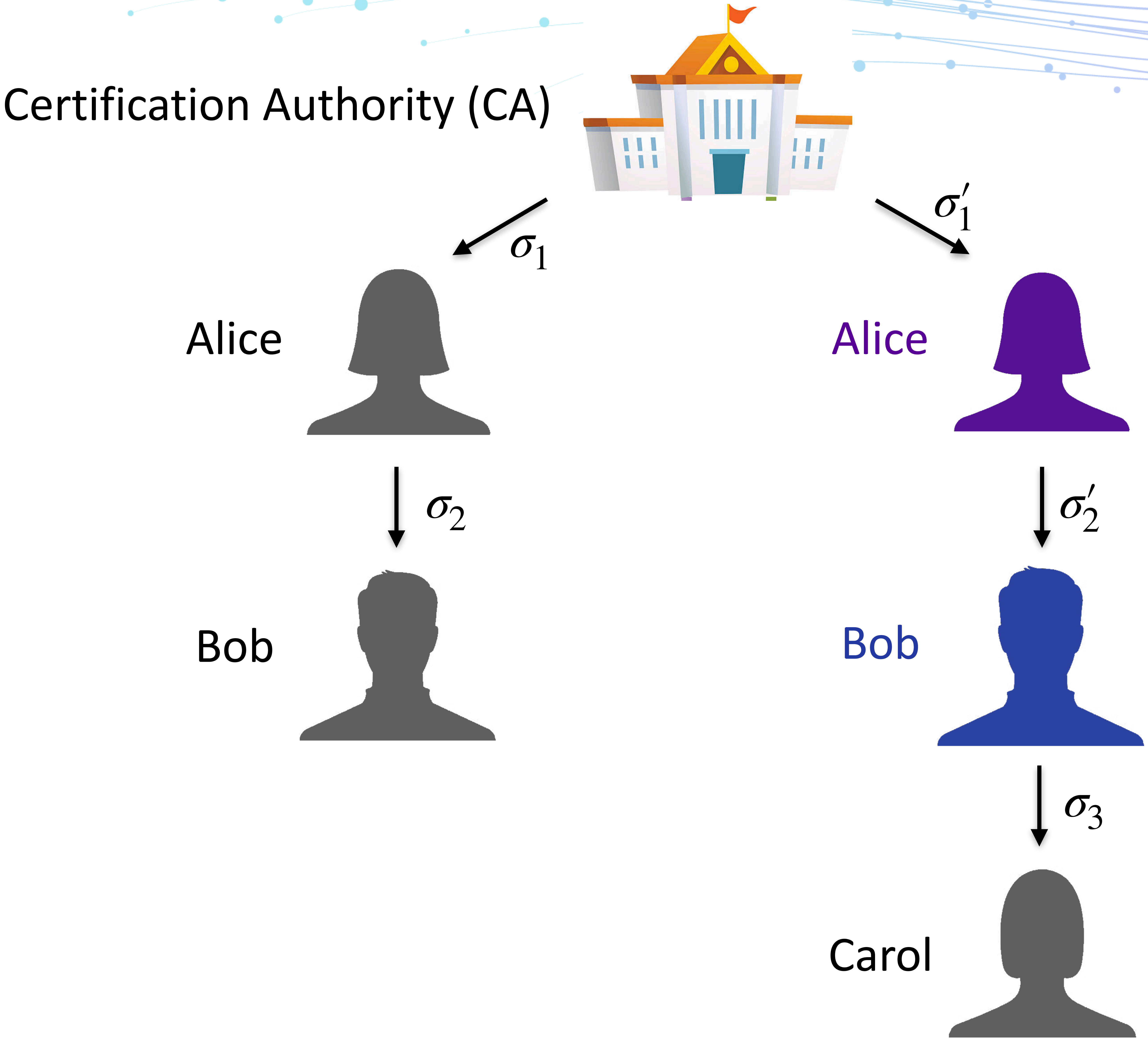
Delegatable Anonymous Credentials from Mercurial Signatures

Elizabeth C. Crites*

Ph.D. Candidate in Mathematics
Brown University

Anna Lysyanskaya

Professor of Computer Science
Brown University



Certification Authority (CA)

σ_1 σ_1'

Alice Alice

σ_2 σ_2'

Bob Bob

σ_3

Carol

Certificate: signatures & public keys

Prior Work on Delegatable Anonymous Credentials

- [CL06]: proof of concept
- [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?

RSAConference2019

Mercurial Signatures

Usual Signatures [GMR88]

Sign(pk,sk,M) $\rightarrow \sigma$

Verify(pk,M, σ) $\rightarrow$ Accept/Reject

Correctness:

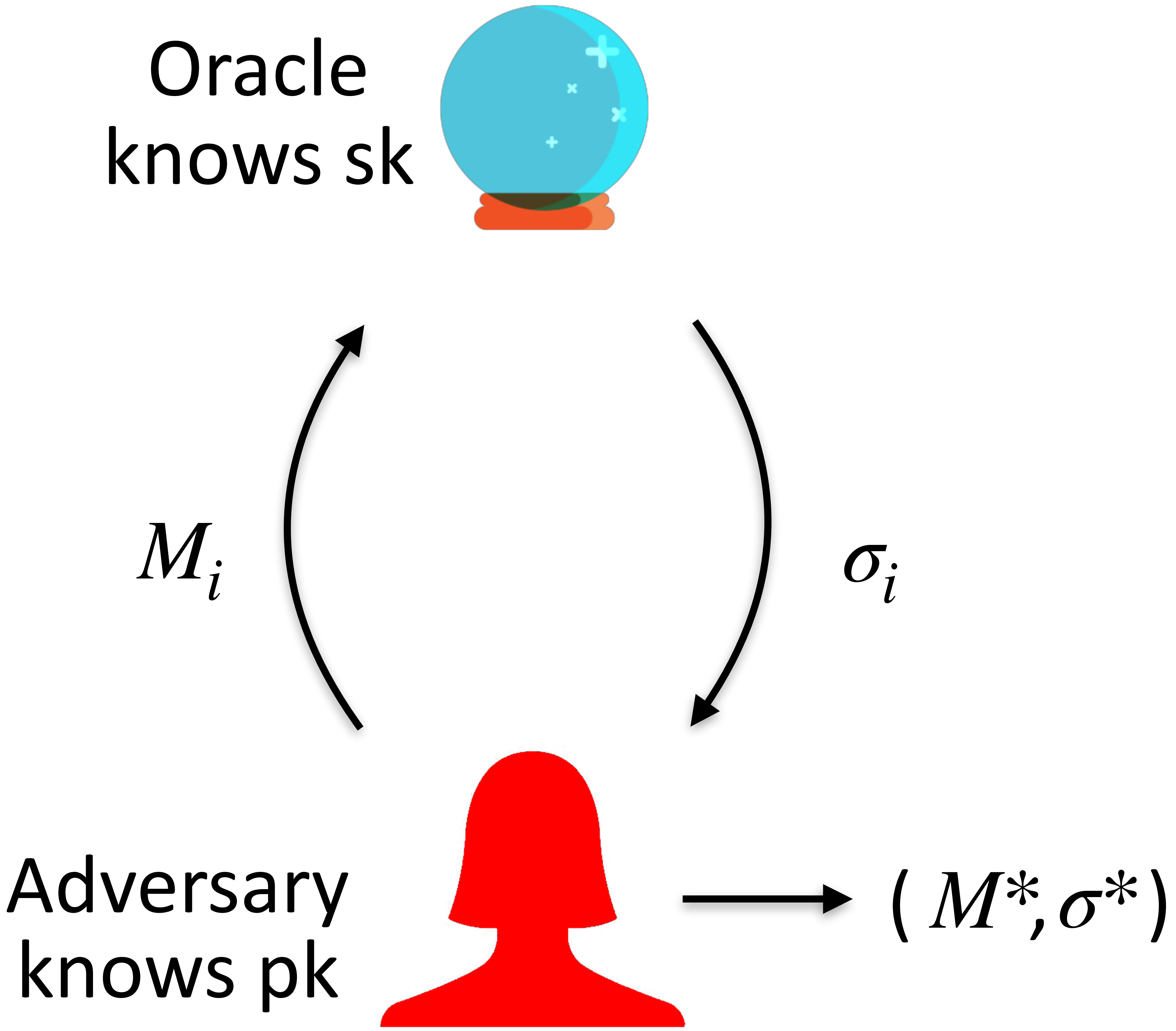
M = M

Verify(pk,M, σ) $\rightarrow$ Accept

Security: Usual (EUF-CMA).

Usual Signatures: Security

EUF-CMA:



Oracle knows sk

M_i

σ_i

Adversary knows pk

(M^*, σ^*)

Adversary wins if:

$M^* \neq M_i \forall i,$

Verify(pk, M^*, σ^*) = Accept

Signatures on Equivalence Classes [FHS14]

Sign(pk,sk,M) $\rightarrow \sigma$

Verify(pk,M, σ) $\rightarrow$ Accept/Reject

Correctness:

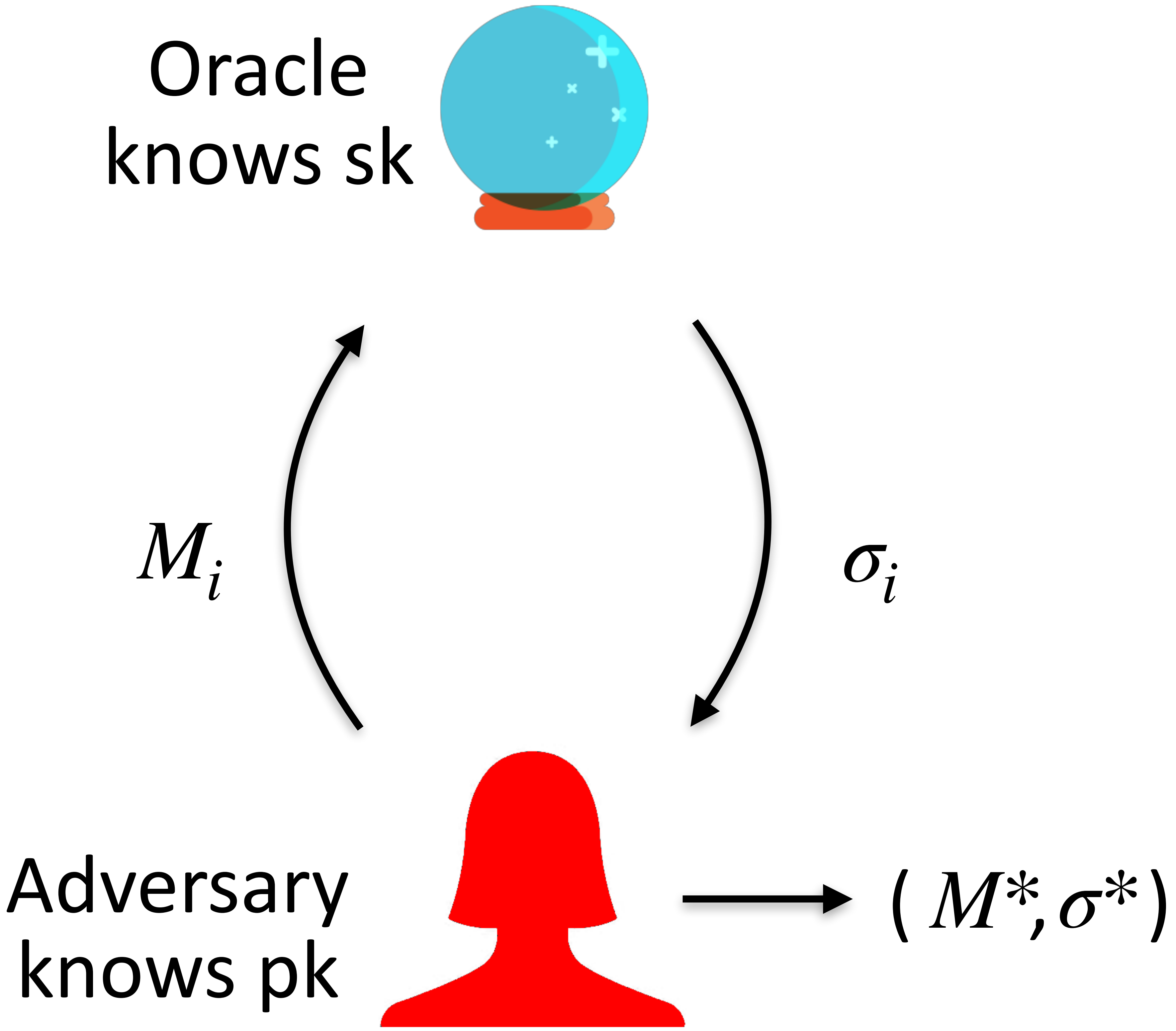
M $\approx$ M

Verify(pk,M, σ) $\rightarrow$ Accept

Security:

[FHS14] Construction: (A,B,C) $\approx$ (rA,rB,rC)

Signatures on Equivalence Classes: Security



Oracle knows sk

M_i

σ_i

Adversary knows pk

(M^*, σ^*)

Adversary wins if:

$M^* \not\approx M_i \forall i,$

Verify(pk, M^*, σ^*) = Accept

Mercurial Signatures (Our Work)

Sign(pk,sk,M) $\rightarrow \sigma$

Verify(pk,M, σ) $\rightarrow$ Accept/Reject

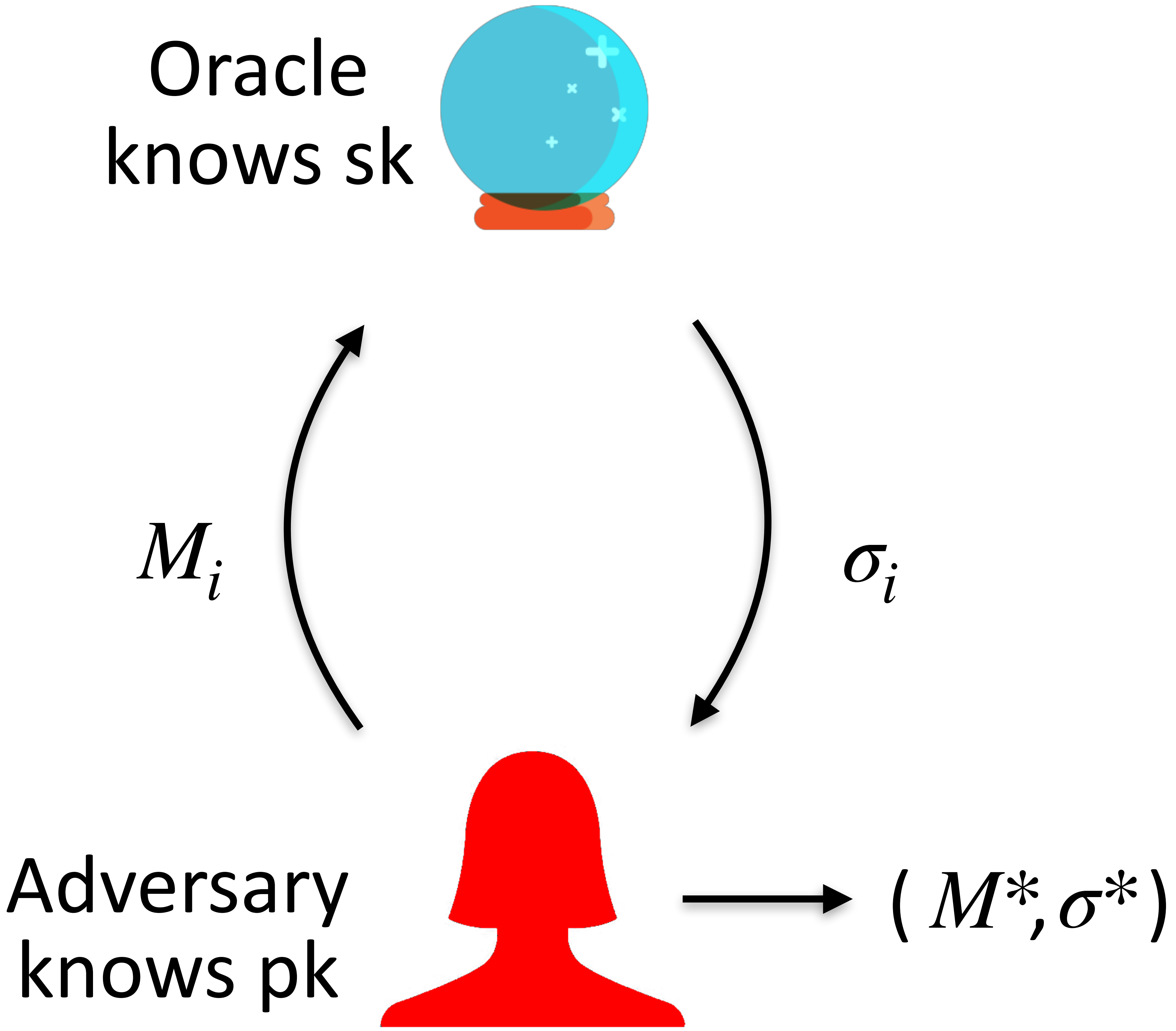
Correctness:

M $\approx$ M, pk $\approx$ pk

Verify(pk,M, σ) $\rightarrow$ Accept

Security:

Mercurial Signatures: Security



Oracle knows sk

M_i

σ_i

Adversary knows pk

(M^*, σ^*)

Adversary wins if:

$M^* \not\approx M_i \forall i,$

Verify(pk*, M^*, σ^*) = Accept

pk* $\approx$ pk

Mercurial Signatures: Construction

- Bilinear groups
- M $= (m_1, m_2, \ldots, m_\ell)$,   pk $= (X_1, X_2, \ldots, X_\ell)$
- M = rM $= (rm_1, rm_2, \ldots, rm_\ell)$,   pk = spk $= (sX_1, sX_2, \ldots, sX_\ell)$
- Transformation (M,pk,σ) $\longrightarrow$ (M,pk,σ') s.t. M, M unlinkable and pk, pk unlinkable (important for anonymity)

Our Results

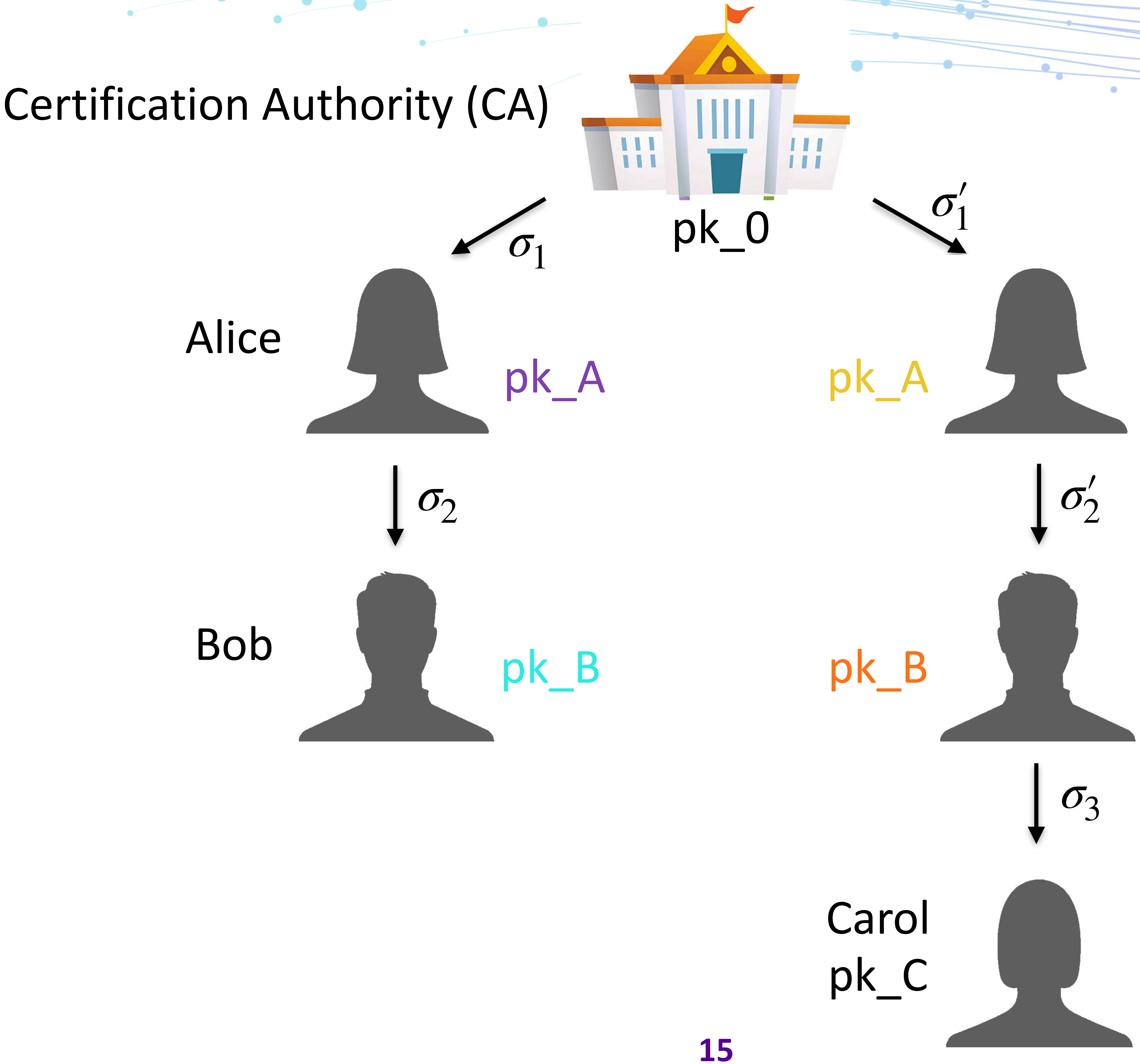
1. Mercurial signatures for the equivalence relation

$$(A,B,C) \approx (rA,rB,rC)$$

that are secure in the generic group model.

RSAConference2019

Delegatable Anonymous Credentials



Certification Authority (CA)

pk_0

σ_1

σ_1'

Alice

pk_A

pk_A

σ_2

σ_2'

Bob

pk_B

pk_B

σ_3

Carol

pk_C

Carol’s Certificate:

{pk_A, pk_B, pk_C, $\sigma_1', \sigma_2', \sigma_3$ }

Our Results

2. (Certain) Mercurial Signatures

$\Rrightarrow$

Delegatable Anonymous Credentials

First direct construction.

Multi-authority credentials.

contact info: elizabeth_crites@brown.edu