Delegatable Anonymous Credentials from Mercurial Signatures

Elizabeth Crites and Anna Lysyanskaya

Brown University

Aug. 22, 2017

Usual Signatures

$$\mathsf{Sign}(\mathsf{pk}; \mathsf{sk}; M) \;\; ! \;\;$$

$$\mathsf{Verify}(\mathsf{pk}; M; \;\;) \;\; ! \;\; \mathsf{Accept}/\mathsf{Reject}$$

Correctness: $M = M$, $\mathsf{Verify}(\mathsf{pk}; M; \;\;) = \mathsf{Accept}$.

Security: Usual.

Signatures on Equivalence Classes

$\mathsf{Sign}(\mathsf{pk}; \mathsf{sk}; M) \to \sigma$

$\mathsf{Verify}(\mathsf{pk}; M; \sigma) \to \mathsf{Accept}/\mathsf{Reject}$

Correctness: $M \quad {}_R \; M$, $\mathsf{Verify}(\mathsf{pk}; M; \sigma) = \mathsf{Accept}$.

Security:

FHS14 Construction: $(A; B; C) \quad (rA; rB; rC)$

Mercurial Signatures (Our Work)

$\mathsf{Sign}(\mathsf{pk}; \mathsf{sk}; M) \;\; ! \;\;$

$\mathsf{Verify}(\mathsf{pk}; M; \;\;) \;\; ! \;\; \mathsf{Accept}/\mathsf{Reject}$

Correctness: $M \;\; {}_R \; M; \mathsf{pk} \;\; {}_R \; \mathsf{pk}$,
$\mathsf{Verify}(\mathsf{pk}; M; \;\;) = \mathsf{Accept}$.

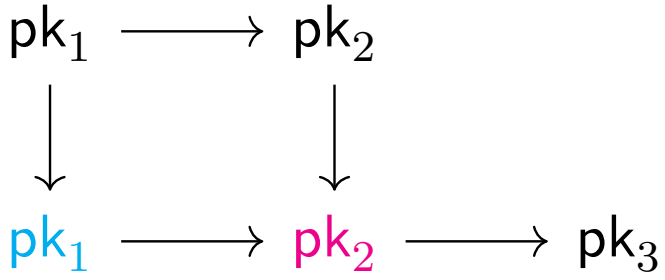
Security:

Our Results

1. Mercurial signatures for this equivalence class that are secure in the generic group model.

Our Results

Why? Allow delegatable anonymous credentials:



2. (certain) Mercurial sigs $=)$ Del. creds

First direct construction.