Structure-Preserving Signatures on Equivalence Classes and their Application to Anonymous Credentials

Christian Hanser and Daniel Slamanig,
IAIK, Graz University of Technology, Austria

9. December 2014

Contribution

- Structure-Preserving Signatures on Equivalence Classes (SPS-EQ)
- Polynomial Commitments with Factor Openings

$\Rightarrow$ Multi-Show Attribute-Based Anonymous Credentials

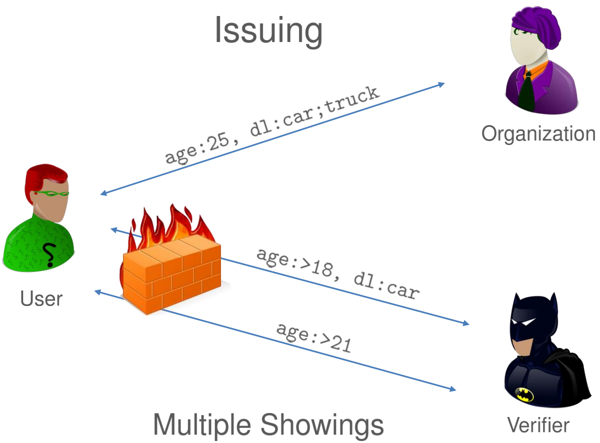
Contribution

- Structure-Preserving Signatures on Equivalence Classes (SPS-EQ)
- Polynomial Commitments with Factor Openings

$\Rightarrow$ Multi-Show Attribute-Based Anonymous Credentials:

  - First ABC system with O(1)-size creds and O(1) communication!
  - Only single $O(1)$ PoK required!
    - only for freshness and reductions!
    - no PoK for possession of signature nor for possession of attributes
  - Simple design

Multi-Show ABCs



Motivation

- Find new, highly efficient way to build attribute-based anonymous credentials
  - Reduce number of PoKs
- **Alternative?** Commitments to sets with subset openings
- **Unlinkability?** Randomizing commitments and witnesses
- **Authenticity?** Needed signature scheme that allows to consistently re-randomize messages and signatures *(compatible with commitment randomization)*

Latest Developments

- Original SPS-EQ scheme broken by Fuchsbauer
  - erroneous GGM proof
  - only secure against RMA (and not EUF-CMA)
- Replacement construction as joint work with Fuchsbauer *(eprint report 2014/944)*
  - Even more efficient (in terms of #PPEs, signature size, PK size)
  - Yields efficient instantiation of our ABC construction

Preliminaries

- Bilinear map $e : G_1 \times G_2 \to G_T$ where G_1, G_2, G_T have prime order p and $G_1 \neq G_2$
- Let $G_1 = \langle P \rangle, G_2 = \langle P' \rangle$
- co-t-SDH assumption:
  - Type-3 counterpart of q-SDH assumption
  - Used in static way

Structure Preserving Signatures [AFG+10]

Signature scheme

- signing group element vectors
- whose signatures and PKs consist only of group elements
- whose verification algorithm uses solely PPEs and group membership tests

So far mainly used in context of Groth-Sahai proofs

Signing Equivalence Classes

As with the projective space, we can partition G_1^ℓ into projective equivalence classes using

$$M \sim_{\mathcal{R}} N \Leftrightarrow \exists k \in \mathbb{Z}_p^* : N = k \cdot M$$

since G_1 has prime order.

Signing Equivalence Classes

As with the projective space, we can partition G_1^ℓ into projective equivalence classes using

$$M \sim_{\mathcal{R}} N \Leftrightarrow \exists k \in \mathbb{Z}_p^* : N = k \cdot M$$

since G_1 has prime order.

Is it possible to build a signature scheme that signs such equivalence classes?

Signing Equivalence Classes (cont.)

Goals:

- Signing a class $[M]_{\mathcal{R}}$ by signing a representative $M \in (G_1^*)^\ell$

Signing Equivalence Classes (cont.)

Goals:

- Signing a class $[M]_{\mathcal{R}}$ by signing a representative $M \in (G_1^*)^\ell$
- Controlled malleability:
  - ability to switch representative in the public: choose $k \in \mathbb{Z}_p^*$, compute $k \cdot M$
  - consistent signature update

Signing Equivalence Classes (cont.)

Goals:

- Signing a class $[M]_{\mathcal{R}}$ by signing a representative $M \in (G_1^*)^\ell$
- Controlled malleability:
  - ability to switch representative in the public: choose $k \in \mathbb{Z}_p^*$, compute $k \cdot M$
  - consistent signature update
- Indistinguishability of updated message-signature pair from random message-signature pair

Signing Equivalence Classes (cont.)

Abstract Model:

- As in ordinary SPS scheme:
  - $\mathsf{BGGen}_{\mathcal{R}}$, $\mathsf{KeyGen}_{\mathcal{R}}$, $\mathsf{Sign}_{\mathcal{R}}$, $\mathsf{Verify}_{\mathcal{R}}$
  - *except for messages considered to be representatives*

Signing Equivalence Classes (cont.)

Abstract Model:

- As in ordinary SPS scheme:
  - $\mathsf{BGGen}_{\mathcal{R}}$, $\mathsf{KeyGen}_{\mathcal{R}}$, $\mathsf{Sign}_{\mathcal{R}}$, $\mathsf{Verify}_{\mathcal{R}}$
  - *except for messages considered to be representatives*
- Additionally:
  - $\mathsf{ChgRep}_{\mathcal{R}}(M, \sigma, k, \mathsf{pk})$: Returns representative $k \cdot M$ of class $[M]_{\mathcal{R}}$ plus update of signature σ

Signing Equivalence Classes (cont.)

Security Properties:

- Correctness
- Unforgeability
- Class Hiding

Signing Equivalence Classes (cont.)

Security Properties:

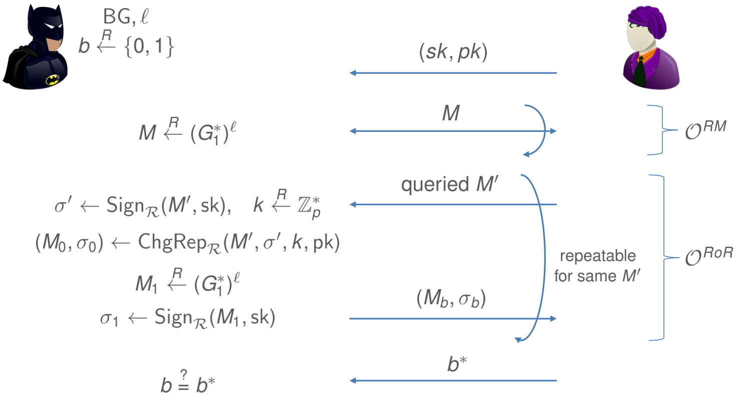
- Correctness
- Unforgeability
- Class Hiding

EUF-CMA security defined w.r.t. equivalence classes:

$$\Pr\left[\begin{array}{c} \mathsf{BG} \leftarrow \mathsf{BGGen}_{\mathcal{R}}(\kappa), \quad (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}_{\mathcal{R}}(\mathsf{BG}, \ell), \\ (M^*, \sigma^*) \leftarrow \mathcal{A}^{\mathcal{O}(\mathsf{sk}, \cdot)}(\mathsf{pk}) : \\ [M^*]_{\mathcal{R}} \neq [M]_{\mathcal{R}} \ \forall \text{ queried } M \ \wedge \ \mathsf{Verify}_{\mathcal{R}}(M^*, \sigma^*, \mathsf{pk}) = \mathtt{true} \end{array}\right] \leq \epsilon(\kappa),$$

Signing Equivalence Classes (cont.)

Class Hiding (relaxed version):



Signing Equivalence Classes (cont.)

Outline of EUF-CMA-secure scheme:

- Signature size:
  - $2 G_1 + 1 G_2$ elements
- PK size:
  - ℓ G_2 elements
- #PPEs:
  - 2

Construction optimal (SPS-EQ implies SPS)

Polynomial Commitments w/ Factor Openings

Overview:

- Perfectly hiding, succinct commitments to monic, reducible $f(X) \in \mathbb{Z}_p[X]$
- Ability to open factors $g(X) \mid f(X)$
  - Alternatively: Compute $f(X)$ having roots in $S \subset \mathbb{Z}_p$ and use $g(X)$ to open $T \subseteq S$
- Commitments + witnesses consistently re-randomizable

Polynomial Commitments w/ Factor Openings

Overview:

- Perfectly hiding, succinct commitments to monic, reducible $f(X) \in \mathbb{Z}_p[X]$
- Ability to open factors $g(X) \mid f(X)$
  - Alternatively: Compute $f(X)$ having roots in $S \subset \mathbb{Z}_p$ and use $g(X)$ to open $T \subseteq S$
- Commitments + witnesses consistently re-randomizable

Alternative to original polynomial commitments [KZG10]

- Less generic, but more efficient for certain use-cases

PolyCommitFO (cont.)

Construction Idea:

- Setup
  - pp $\simeq$ co-t-SDH instance
- Commit to $f(X)$:
  - Evaluate $f(X)$ in group using pp, multiply with random $r \longrightarrow$ commitment $\mathcal{C}$

PolyCommitFO (cont.)

Construction Idea:

- Open factor $g(X) \mid f(X)$ *(let $f(X) = g(X)h(X)$)*:
  - Compute witness W to $h(X)$ in same way as commitment $\mathcal{C}$

PolyCommitFO (cont.)

Construction Idea:

- Open factor $g(X) \mid f(X)$ *(let* $f(X) = g(X)h(X)$*)*:
  - Compute witness W to $h(X)$ in same way as commitment $\mathcal{C}$
- Verify factor opening of $g(X)$:
  - Evaluate $g(X)$ in group and plug everything together in one PPE

PolyCommitFO (cont.)

Re-randomizability:

- Factor verification still works for $k \cdot \mathcal{C}$ and $k \cdot W$

Security:

- Extensive security model
- Construction based on co-t-SDH assumption

ABCs from SPS-EQ

New ABC construction type + Appropriate Security Model

Ingredients:

- SPS-EQ + PolyCommitFO
- A single $O(1)$ OR PoK
- Collision-resistant hash function $H : \{0,1\}^* \rightarrow \mathbb{Z}_p$

ABCs from SPS-EQ (cont.)

Outline of Obtain/Issue Phase:

- Use PolyCommitFO to compute commitment $\mathcal{C}$ to attribute set:
  - commit to $f(X)$ having hashed attribute/value pairs as roots (using H)
  - include user secret into $\mathcal{C}$
- Obtain SPS-EQ signature σ on $(\mathcal{C}, P)$
- Credential: $(\mathcal{C}, \sigma)$

ABCs from SPS-EQ (cont.)

Outline of Showings:

- The prover
  - picks $k \xleftarrow{R} \mathbb{Z}_p^*$, runs $((k \cdot \mathcal{C}, k \cdot P), \tilde{\sigma}) \leftarrow \mathsf{ChgRep}_{\mathcal{R}}(((\mathcal{C}, P), \sigma), k, \mathsf{pk})$
  - opens $k \cdot \mathcal{C}$ to $g(X) \mid f(X)$ corr. to selected attribute set $\rightarrow$ witness W
  - sends $((k \cdot \mathcal{C}, k \cdot P), \tilde{\sigma})$, W and perform OR PoK on k or knowledge of dlog of a CRS value *(freshness + reduction)*

ABCs from SPS-EQ (cont.)

Outline of Showings:

- Verifier checks
  - validity of $((k \cdot \mathcal{C}, k \cdot P), \tilde{\sigma})$
  - whether shown attributes and W give factor opening of $k \cdot \mathcal{C}$
  - PoK

ABCs from SPS-EQ (cont.)

Efficiency (when using repaired SPS-EQ scheme):

- Credential size:
  - $3G_1 + 1G_2$ elements
- Communication:
  - $O(1)$
- Showing:
  - User $O(\#(\text{unshown attributes}))$
  - Verifier $O(\#(\text{shown attributes}))$

Conclusions

- SPS-EQ: new, powerful signature primitive
  - potential applications in many other contexts!
- Efficient, randomizable, perfectly hiding polynomial commitments
- Highly efficient multi-show ABCs
  - first construction having $O(1)$ credential size and communication!

Thank you for your attention!

christian.hanser@iaik.tugraz.at