IAIK TU Graz

Structure-Preserving Signatures on Equivalence Classes

Georg Fuchsbauer[†], Christian Hanser[‡] and Daniel Slamanig[‡],
[†]Institute of Science and Technology Austria
[‡]IAIK, Graz University of Technology, Austria

8. July 2015

Contribution

- Structure-Preserving Signatures on Equivalence Classes (SPS-EQ)

+ Commitments

⇒ Multi-Show Attribute-Based Anonymous Credentials

Contribution

- Structure-Preserving Signatures on Equivalence Classes (SPS-EQ)

+ Commitments

⇒ Multi-Show Attribute-Based Anonymous Credentials:

  - 1st ABC with $O(1)$ cred-size and communication!

⇒ Blind Signatures in the Standard Model

  - 1st practically efficient construction

⇒ Verifiably Encrypted Signatures in the Standard Model

Preliminaries

- Asymmetric bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$, where
  - $\mathbb{G}_1, \mathbb{G}_2$ additive groups; $\mathbb{G}_T$ multiplicative group
  - $|\mathbb{G}_1| = |\mathbb{G}_2| = |\mathbb{G}_T| = p$ for prime p
  - $\mathbb{G}_1 \neq \mathbb{G}_2$
  - $\mathbb{G}_1 = \langle P \rangle, \mathbb{G}_2 = \langle \hat{P} \rangle$
- $e(aP, b\hat{P}) = e(P, \hat{P})^{ab}$ (Bilinearity)
- $e(P, \hat{P}) \neq 1_{\mathbb{G}_T}$ (Non-degeneracy)
- $e(\cdot, \cdot)$ efficiently computable (Efficiency)

Structure Preserving Signatures [AFG+10]

Signature scheme

- signing group element vectors
- sigs and PKs consist only of group elements
- verification uses solely
  - pairing-product equations
  - + group membership tests

So far mainly used in context of Groth-Sahai proofs

Signing Equivalence Classes [HS14]

As with the projective space, we can partition $\mathbb{G}_i^\ell$ into projective equivalence classes using

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

since $\mathbb{G}_i$ has prime order p.

Signing Equivalence Classes [HS14]

As with the projective space, we can partition $\mathbb{G}_i^\ell$ into projective equivalence classes using

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

since $\mathbb{G}_i$ has prime order p.

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

Signing Equivalence Classes (ctd) [HS14]

Goals:

- Signing class $[M]_{\mathcal{R}}$ by signing representative $M \in [M]_{\mathcal{R}}$

Georg Fuchsbauer†, Christian Hanser‡ and Daniel Slamanig‡, IST & TUG

Signing Equivalence Classes (ctd) [HS14]

Goals:

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

Signing Equivalence Classes (ctd) [HS14]

Goals:

- Signing class $[M]_{\mathcal{R}}$ by signing representative $M \in [M]_{\mathcal{R}}$
- Controlled malleability:
  - ability to switch representative: choose $k \in \mathbb{Z}_p^*$, compute $k \cdot M$
  - + consistent sig update in the public
- IND of updated msgs from random msgs

Signing Equivalence Classes (ctd) [HS14]

Goals:

- Signing class $[M]_{\mathcal{R}}$ by signing representative $M \in [M]_{\mathcal{R}}$
- Controlled malleability:
  - ability to switch representative: choose $k \in \mathbb{Z}_p^*$, compute $k \cdot M$
  - \+ consistent sig update in the public
- IND of updated msgs from random msgs
- Updated sigs must look like valid, random sigs (or in weaker version: like fresh sigs)

Signing Equivalence Classes (ctd) [HS14]

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 msgs considered to be representatives*

Signing Equivalence Classes (ctd) [HS14]

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 msgs 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 sig σ
  - $\mathsf{VKey}_{\mathcal{R}}$

Signing Equivalence Classes (ctd) [HS14]

Security Properties:

- Correctness
- EUF-CMA security
- Perfect adaption of signatures (under malicious/honest keys)

Signing Equivalence Classes (ctd) [HS14]

Security Properties:

- Correctness
- EUF-CMA security
- Perfect adaption of signatures (under malicious/honest keys)

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

$$\Pr\left[\begin{array}{c}\mathsf{BG} \leftarrow \mathsf{BGGen}_{\mathcal{R}}(\kappa),\quad (\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{KeyGen}_{\mathcal{R}}(\mathsf{BG},\ell), \\ (M^*,\sigma^*) \leftarrow \mathcal{A}^{\mathcal{O}(\mathsf{sk},\cdot)}(\mathsf{pk}) : \\ [M^*]_{\mathcal{R}} \neq [M]_{\mathcal{R}} \ \forall \text{ queried } M \ \wedge\ \mathsf{Verify}_{\mathcal{R}}(M^*,\sigma^*,\mathsf{pk}) = 1\end{array}\right] \leq \epsilon(\kappa),$$

Signing Equivalence Classes (ctd) [FHS14]

Outline of EUF-CMA-secure scheme:

- $\mathsf{sk} = (x_i)_{i\in[\ell]} \in_R (\mathbb{Z}_p^*)^\ell, \quad \mathsf{pk} = (\hat{X}_i)_{i\in[\ell]} = (x_i\hat{P})_{i\in[\ell]}$
- Sig for $M = (M_i)_{i\in[\ell]}$:
  - $Z \leftarrow y\sum_i x_i M_i \quad$ for $y \xleftarrow{R} \mathbb{Z}_p^*$
  - $Y \leftarrow \frac{1}{y}P$ and $\hat{Y} \leftarrow \frac{1}{y}\hat{P}$
- Switching M to representative $k \cdot M$ (via $\mathit{ChgRep}_{\mathcal{R}}$):
  - $Z' \leftarrow \psi \cdot k \cdot Z \quad$ for $\psi \xleftarrow{R} \mathbb{Z}_p^*$
  - $Y' \leftarrow \frac{1}{\psi}Y$ and $\hat{Y}' \leftarrow \frac{1}{\psi}\hat{Y}$

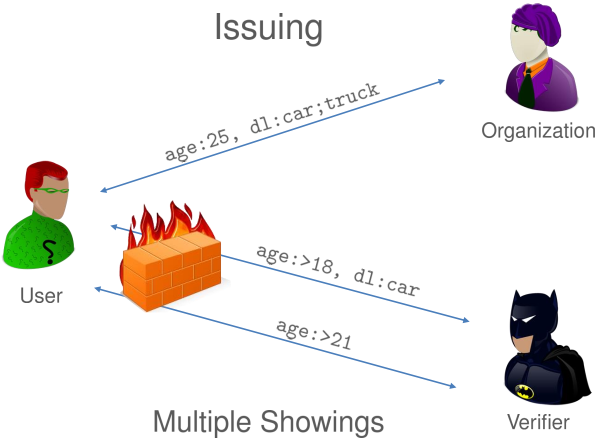
Signing Equivalence Classes (ctd) [FHS14, FHS15]

Outline of EUF-CMA-secure scheme:

- Signature size:
  - $2\ \mathbb{G}_1 + 1\ \mathbb{G}_2$ elements
- PK size:
  - $\ell\ \mathbb{G}_2$ elements
- #PPEs:
  - 2

Construction optimal (SPS-EQ implies SPS)

Multi-Show ABCs



ABCs from SPS-EQ [HS14]

New ABC construction type + Appropriate Security Model

Ingredients:

- SPS-EQ
- Randomizable set commitments (allowing subset openings)
- A single $O(1)$ OR PoK
- Collision-resistant hash function $H : \{0, 1\}^* \rightarrow \mathbb{Z}_p$

ABCs from SPS-EQ (ctd) [HS14]

Outline of Obtain/Issue:

- Compute set commitment $C \in \mathbb{G}_1$ to attribute set:
  - encode attributes to $\mathbb{Z}_p$ elements using H
  - include user secret into C
- Obtain SPS-EQ sig σ on (C, P)
- Credential: (C, σ)

ABCs from SPS-EQ (ctd) [HS14]

During showing, user:

- runs $((k \cdot C, k \cdot P), \tilde{\sigma}) \leftarrow \mathsf{ChgRep}_{\mathcal{R}}(((C, P), \sigma), k, \mathsf{pk})$
- opens $k \cdot C$ to subset corr. to selected attributes
- sends $((k \cdot C, k \cdot P), \tilde{\sigma})$, partial opening and performs OR PoK on k or knowledge of dlog of a CRS value

ABCs from SPS-EQ (ctd) [HS14]

During showing, user:

- runs $((k \cdot C, k \cdot P), \tilde{\sigma}) \leftarrow \mathsf{ChgRep}_{\mathcal{R}}(((C, P), \sigma), k, \mathsf{pk})$
- opens $k \cdot C$ to subset corr. to selected attributes
- sends $((k \cdot C, k \cdot P), \tilde{\sigma})$, partial opening and performs OR PoK on k or knowledge of dlog of a CRS value

During showing, verifier checks:

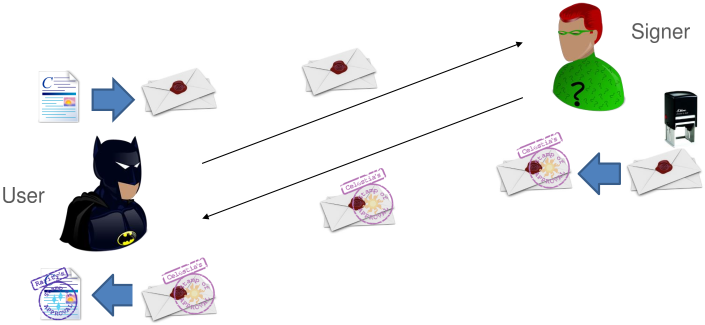
- validity of $((k \cdot C, k \cdot P), \tilde{\sigma})$
- validity of partial opening of $k \cdot C$
- PoK

ABCs from SPS-EQ (ctd) [HS14]

Efficiency (when using SPS-EQ from [FHS14]):

- Credential size:
  - $3\ \mathbb{G}_1 + 1\ \mathbb{G}_2$ elements
- Communication:
  - $O(1)$
- Showing:
  - User $O(\#(\text{unshown attributes}))$
  - Verifier $O(\#(\text{shown attributes}))$

Blind Signatures



Georg Fuchsbauer†, Christian Hanser‡ and Daniel Slamanig‡, IST & TUG

Blind Signatures from SPS-EQ [FHS15]

Ingredients:

- SPS-EQ
- Pedersen commitments (with modified opening)

Blind Signatures from SPS-EQ [FHS15]

Ingredients:

- SPS-EQ
- Pedersen commitments (with modified opening)

Signer PK:

- SPS-EQ public key $\mathsf{pk}_{\mathcal{R}}$
- $(Q, \hat{Q}) \leftarrow q \cdot (P, \hat{P})$ for $q \stackrel{R}{\leftarrow} \mathbb{Z}_p^*$

Blind Signatures from SPS-EQ [FHS15]

Outline of Obtain/Issue:

- Create Ped. commitment to msg m: $C = mP + rQ$
- Send blinded commitment (sC, sP) for $s \xleftarrow{R} \mathbb{Z}_p^*$ to signer
- Signer returns SPS-EQ sig π on (sC, sP)

Blind Signatures from SPS-EQ [FHS15]

Outline of Obtain/Issue:

- Create Ped. commitment to msg m: $C = mP + rQ$
- Send blinded commitment (sC, sP) for $s \xleftarrow{R} \mathbb{Z}_p^*$ to signer
- Signer returns SPS-EQ sig π on (sC, sP)
- Check whether π valid
  - if so, use $\mathsf{ChgRep}_{\mathcal{R}}$ to get sig σ on (C, P)
  - set sig $\tau \leftarrow (\sigma, rP, rQ)$

Blind Signatures from SPS-EQ (ctd) [FHS15]

Verification:

- Given m and $\tau = (\sigma, R, T)$
- Check whether
  - σ valid SPS-EQ sig on $(mP + T, P)$ under $\mathsf{pk}_{\mathcal{R}}$
  - $e(T, \hat{P}) = e(R, \hat{Q})$
- If so, return 1 and 0 otherwise.

Blind Signatures from SPS-EQ (ctd) [FHS15]

Security:

- *Unforgeable* under
  - EUF-CMA security of SPS-EQ
  - + a variant of the Diffie-Hellman-Inversion assumption
- *Blind* under an interactive variant of DDH assumption (malicious keys)

in the standard model (first practically efficient construction!)

Blind Signatures from SPS-EQ (ctd) [FHS15]

Security:

- *Unforgeable* under
  - EUF-CMA security of SPS-EQ
  - + a variant of the Diffie-Hellman-Inversion assumption
- *Blind* under an interactive variant of DDH assumption (malicious keys)

in the standard model (first practically efficient construction!)

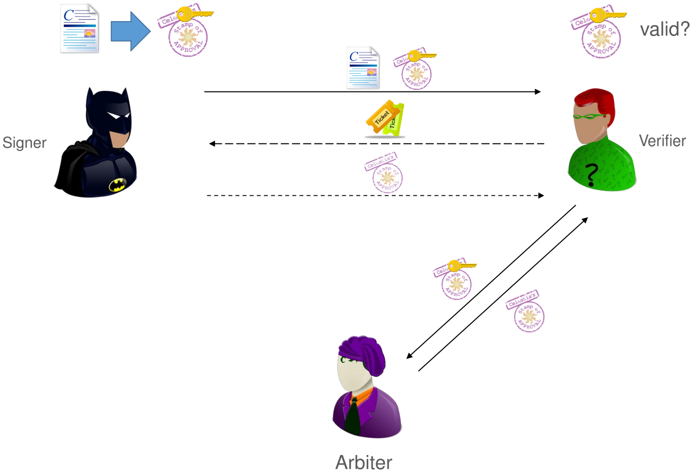
allows standard-model construction of one-show ABCs

Verifiably Encrypted Signatures

Outline:

- Fair contract signing
- Two types of sigs:
  - Plain
  - + encrypted sigs
- Three parties
  - Signer
  - Verifier
  - Arbiter

Verifiably Encrypted Signatures



VES from SPS-EQ [HRS15]

Efficient Construction from SPS-EQ (+ DL commitments):

- Arbiter key: $\mathsf{sk} = a \xleftarrow{R} \mathbb{Z}_p^*$, $\mathsf{pk} = A = aP$
- Plain and encrypted sigs created from representatives of same equivalence class:

$$\begin{aligned} \text{Plain: } & \text{sig } \sigma \text{ created from } (m \cdot sP, sP, P) \\ \text{Encrypted: } & \text{sig } \omega \text{ created from } (m \cdot sA, sA, A) \\ & \text{for } s \xleftarrow{R} \mathbb{Z}_p^* \end{aligned}$$

$\Rightarrow$ arbiter sk allows switching representative and obtaining plain sig

Conclusions

- SPS-EQ: new, powerful signature primitive
- Application in many contexts
  - ABCs
  - Blind signatures
  - VES
  - ...
- Often allows very efficient constructions
  - 1st ABC with $O(1)$ showings + cred size
  - 1st practically efficient blind signature scheme

Thank you for your attention!

christian.hanser@iaik.tugraz.at

Supported by:

prisma cloud

matthew

References

HS14 C. Hanser and D. Slamanig. *Structure-Preserving Signatures on Equivalence Classes and their Application to Anonymous Credentials*. ASIACRYPT 2014

FHS14 G. Fuchsbauer, C. Hanser and D. Slamanig. *EUF-CMA-Secure Structure-Preserving Signatures on Equivalence Classes*. Cryptology ePrint Archive 2014

FHS15 G. Fuchsbauer, C. Hanser and D. Slamanig. *Practical Round-Optimal Blind Signatures in the Standard Model*. CRYPTO 2015 (in press)

HRS15 C. Hanser, M. Rabkin and D. Schröder. *Verifiably Encrypted Signatures: Security Revisited and a New Construction.* ESORICS 2015 (in press)