Cryptanalysis of the Structure-Preserving Signature Scheme on Equivalence Classes from Asiacrypt 2014

Yanbin Pan

Academy of Mathematics and Systems Science,
Chinese Academy of Sciences

CT-RSA 2016, San Francisco
2016-3-3

Contents

Structure-Preserving Signature Scheme on Equivalence Classes

Digital Signature Scheme

- **KeyGen**(1^n): Generate public key **pk** and private key **sk**;
- **Sign**: Given message m, the signer computes the signature $\sigma = \text{Sign}_{\mathbf{pk},\mathbf{sk}}(m)$ and publishes the pair

$$(m, \sigma).$$

- **Verify**: the verifier accepts the message-signature pair if and only if $\text{Verify}_{\mathbf{pk}}(m, \sigma) = \mathit{true}$.

Structure-Preserving Signature Scheme (SPS)

- Proposed by Abe *et al.* in CRYPTO 2010;
- Employs bilinear map;

Structure-Preserving Signature Scheme (SPS)

- Proposed by Abe *et al.* in CRYPTO 2010;
- Employs bilinear map;

Bilinear Map

Let $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ be cyclic groups of prime order p, where $\mathbb{G}_1$ and $\mathbb{G}_2$ are additive and $\mathbb{G}_T$ is multiplicative. Let P and P' generate $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. We call

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

a bilinear map if it is efficiently computable and satisfies

- For any $a, b \in \mathbb{Z}_p$, $e(aP, bP') = e(P, P')^{ab} = e(bP, aP')$.
- $e(P, P') \neq 1_{\mathbb{G}_T}$.

Structure-Preserving Signature Scheme (SPS)

- Proposed by Abe *et al.* in CRYPTO 2010;
- Employs bilinear map;
- The **pk**, m and σ consist only of group elements;
- The signature can be verified just by deciding group membership and by evaluating some pairing-product equations;

Structure-Preserving Signature Scheme (SPS)

- Proposed by Abe *et al.* in CRYPTO 2010;
- Employs bilinear map;
- The **pk**, m and σ consist only of group elements;
- The signature can be verified just by deciding group membership and by evaluating some pairing-product equations;
- Many applications: blind signatures, group signatures, homomorphic signatures, tightly secure encryption...

SPS on Equivalence Classes (SPS-EQ)

- Proposed by Hanser and Slamanig in Asiacrypt 2014;
- A structure-preserving signature with message space $(\mathbb{G}^*)^\ell$;
- For any message N equivalent to M, its valid signature can be efficiently obtained by the signature of M.

SPS on Equivalence Classes (SPS-EQ)

- Proposed by Hanser and Slamanig in Asiacrypt 2014;
- A structure-preserving signature with message space $(\mathbb{G}^*)^\ell$;
- For any message N equivalent to M, its valid signature can be efficiently obtained by the signature of M.

Equivalence Relation in [HS2014]

Given a cyclic group $\mathbb{G}$ with order p and an integer $\ell > 1$:

- The equivalence relation:

$$\mathcal{R} = \{(M, N) \in (\mathbb{G}^*)^\ell \times (\mathbb{G}^*)^\ell : \exists \rho \in \mathbb{Z}_p^* \text{ s.t. } N = \rho M\}.$$

- The equivalence class:

$$[M]_\mathcal{R} = \{N \in (\mathbb{G}^*)^\ell : \exists \rho \in \mathbb{Z}_p^* \text{ s.t. } N = \rho M\}.$$

SPS on Equivalence Classes (SPS-EQ)

- Proposed by Hanser and Slamanig in Asiacrypt 2014;
- A structure-preserving signature with message space $(\mathbb{G}^*)^\ell$;
- For any message N equivalent to M, its valid signature can be efficiently obtained by the signature of M.
- Used to construct an efficient multi-show attribute-based anonymous credential system [HS2014].

SPS-EQ

Definition (SPS-EQ-$\mathcal{R}$)

An SPS-EQ-$\mathcal{R}$ scheme consists of the following polynomial-time algorithms:

- $\mathbf{BGGen}_{\mathcal{R}}(1^{\kappa})$: Given a security parameter κ, outputs a bilinear group description $\mathbf{BG}$.
- $\mathbf{KeyGen}_{\mathcal{R}}(\mathbf{BG}, \ell)$: Given $\mathbf{BG}$ and vector length $\ell > 1$, outputs a key pair $(\mathbf{sk}, \mathbf{pk})$.
- $\mathbf{Sign}_{\mathcal{R}}(M, \mathbf{sk})$: On input a representative M of equivalence class $[M]_{\mathcal{R}}$ and secret key $\mathbf{sk}$, outputs a signature σ for the equivalence class $[M]_{\mathcal{R}}$.
- $\mathbf{ChgRep}_{\mathcal{R}}(M, \sigma, \rho, \mathbf{pk})$: On input a representative M of an equivalence class $[M]_{\mathcal{R}}$, the corresponding signature σ, a scalar ρ and a public key $\mathbf{pk}$, outputs $(\rho M, \hat{\sigma})$, where $\hat{\sigma}$ is the signature on ρM.
- $\mathbf{Verify}_{\mathcal{R}}(M, \sigma, \mathbf{pk})$: Given a representative M of equivalence class $[M]_{\mathcal{R}}$, a signature σ and public key $\mathbf{pk}$, outputs true if σ is a valid signature for $[M]_{\mathcal{R}}$ and false otherwise.

Security of SPS-EQ

	Unforgeability	Existential Unforgeability
Random Message Attack	UF-RMA	EUF-RMA
Non-Adaptive CMA	UF-NACMA	EUF-NACMA
Adaptive CMA	UF-ACMA	EUF-ACMA

- EUF-ACMA:

$$\mathbf{Pr}\left[\begin{array}{c}(\mathbf{sk},\mathbf{pk}) \leftarrow \mathit{KeyGen}(1^n), (M^*,\sigma^*) \leftarrow \mathcal{A}^{\mathcal{O}(\mathbf{sk},\cdot)}(\mathbf{pk}) : \\ [M^*]_{\mathcal{R}} \text{has not been queried} \wedge \mathit{Verify}_{\mathcal{R}}(M^*,\sigma^*,\mathbf{pk}) = \mathit{true}\end{array}\right] \leq \mathrm{negl}(n)$$

The Hanser-Slamanig SPS-EQ Scheme

The Hanser-Slamanig SPS-EQ Scheme

- $\mathbf{BGGen}_{\mathcal{R}}(1^\kappa)$: Given a security parameter κ, outputs

$$\mathbf{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, P, P', e).$$

- $\mathbf{KeyGen}_{\mathcal{R}}(\mathbf{BG}, \ell)$: Given $\ell > 1$, chooses $x \xleftarrow{R} \mathbb{Z}_p^*$ and $(x_i)_{i=1}^{\ell} \xleftarrow{R} (\mathbb{Z}_p^*)^{\ell}$, computes

$$\begin{aligned} \mathbf{sk} &\leftarrow (x, (x_i)_{i=1}^{\ell}), \\ \mathbf{pk} &\leftarrow (X', (X_i')_{i=1}^{\ell}) = (xP', (x_i x P')_{i=1}^{\ell}). \end{aligned}$$

The Hanser-Slamanig SPS-EQ Scheme

- **Sign**$_{\mathcal{R}}(M, \mathbf{sk})$: On input a representative $M = (M_i)_{i=1}^{\ell} \in (\mathbb{G}_1^*)^{\ell}$ of $[M]_{\mathcal{R}}$, chooses $y \xleftarrow{R} \mathbb{Z}_p^*$ and computes

$$Z \leftarrow x \sum_{i=1}^{\ell} x_i M_i, \quad V \leftarrow y \sum_{i=1}^{\ell} x_i M_i, \quad (Y, Y') \leftarrow y \cdot (P, P').$$

  Then, outputs $\sigma = (Z, V, Y, Y')$.

- **Verify**$_{\mathcal{R}}(M, \sigma, \mathbf{pk})$: checks whether

$$\prod_{i=1}^{\ell} e(M_i, X_i') \stackrel{?}{=} e(Z, P) \bigwedge e(Z, Y') \stackrel{?}{=} e(V, X') \bigwedge e(P, Y') \stackrel{?}{=} e(Y, P')$$

  or not and outputs true if this holds and false otherwise.

Fuchsbauer's Attack when $\ell = 2$

1. $\mathcal{A}$ receives **pk** and has access to a signing oracle.
2. $\mathcal{A}$ makes a signing query (P, P) and receives the signature (Z_1, V_1, Y_1, Y_1').
3. $\mathcal{A}$ makes a signing query (Z_1, P) and receives the signature (Z_2, V_2, Y_2, Y_2').
4. $\mathcal{A}$ makes a signing query (P, Z_1) and receives the signature (Z_3, V_3, Y_3, Y_3').
5. $\mathcal{A}$ makes a signing query (Z_1, Z_2) and receives the signature (Z_4, V_4, Y_4, Y_4').
6. $\mathcal{A}$ outputs (Z_4, V_4, Y_4, Y_4') as a forgery for the equivalence class represented by (Z_3, Z_1).

Some Remarks on Fuchsbauer's attack

- It needs 4 adaptive queries;
- Succeeds with high probability;

- Neglected to check whether (Z_3, Z_1) is in $(\mathbb{G}_1^*)^2$ or not;
- Break EUF-CMA just for $\ell = 2$;

- Amazing but hard to follow the idea. It is hard to point out which component of the scheme is weak from his attack.

Our Attacks

Main Result

Attack Model	**Security**	ℓ
RMA	Existential Unforgeability [HS14]	$\ell \geq 2$
NACMA	Existential Forgeability [this work]	$\ell \geq 2$
ACMA	Existential Forgeability [Fuch14]	$\ell = 2$
	Universal Forgeability [this work]	$\ell \geq 2$

Our Attacks

- Never Fail;
- Use less queries;

	$\ell = 2$	$\ell > 2$
Non-Adaptive CMA	2	3
Adaptive CMA	3	4

- Easy to understand, and provide clear hint to fix the scheme.

The Key Observation

- **Sign**$_{\mathcal{R}}(M, \mathbf{sk})$: On input a representative $M = (M_i)_{i=1}^{\ell} \in (\mathbb{G}_1^*)^{\ell}$ of $[M]_{\mathcal{R}}$, chooses $y \xleftarrow{R} \mathbb{Z}_p^*$ and computes

$$Z \leftarrow x \sum_{i=1}^{\ell} x_i M_i, \qquad V \leftarrow y \sum_{i=1}^{\ell} x_i M_i, \qquad (Y, Y') \leftarrow y \cdot (P, P').$$

Then, outputs $\sigma = (Z, V, Y, Y')$.

The Key Observation

- **Sign**$_{\mathcal{R}}(M, \mathbf{sk})$: On input a representative $M = (M_i)_{i=1}^{\ell} \in (\mathbb{G}_1^*)^{\ell}$ of $[M]_{\mathcal{R}}$, chooses $y \xleftarrow{R} \mathbb{Z}_p^*$ and computes

$$Z \leftarrow x \sum_{i=1}^{\ell} x_i M_i, \qquad V \leftarrow y \sum_{i=1}^{\ell} x_i M_i, \qquad (Y, Y') \leftarrow y \cdot (P, P').$$

Then, outputs $\sigma = (Z, V, Y, Y')$.

For any two messages M and M^*, if

$$\sum_{i=1}^{\ell} x_i M_i = \sum_{i=1}^{\ell} x_i M_i^*,$$

then M and M^* share the same signature.

The Key Observation

- **Sign**$_{\mathcal{R}}(M, \mathbf{sk})$: On input a representative $M = (M_i)_{i=1}^{\ell} \in (\mathbb{G}_1^*)^{\ell}$ of $[M]_{\mathcal{R}}$, chooses $y \overset{R}{\leftarrow} \mathbb{Z}_p^*$ and computes

$$Z \leftarrow x \sum_{i=1}^{\ell} x_i M_i, \qquad V \leftarrow y \sum_{i=1}^{\ell} x_i M_i, \qquad (Y, Y') \leftarrow y \cdot (P, P').$$

Then, outputs $\sigma = (Z, V, Y, Y')$.

Generally, for any $K \in \ker(\varphi)$, that is, $\sum_{i=1}^{\ell} x_i K_i = 0$,

$$\varphi : \begin{array}{ccc} (\mathbb{G}_1)^{\ell} & \to & \mathbb{G}_1 \\ (M_i)_{i=1}^{\ell} & \mapsto & \sum_{i=1}^{\ell} x_i M_i, \end{array}$$

M and $M + K$ share the same signature.

Find a Non-Trivial K

- $\textbf{Sign}_{\mathcal{R}}(M, \textbf{sk})$: On input a representative $M = (M_i)_{i=1}^{\ell} \in (\mathbb{G}_1^*)^{\ell}$ of $[M]_{\mathcal{R}}$, chooses $y \xleftarrow{R} \mathbb{Z}_p^*$ and computes

$$Z \leftarrow x \sum_{i=1}^{\ell} x_i M_i, \qquad V \leftarrow y \sum_{i=1}^{\ell} x_i M_i, \qquad (Y, Y') \leftarrow y \cdot (P, P').$$

  Then, outputs $\sigma = (Z, V, Y, Y')$.

Find a Non-Trivial K

- **Sign**$_{\mathcal{R}}(M, \mathbf{sk})$: On input a representative $M = (M_i)_{i=1}^{\ell} \in (\mathbb{G}_1^*)^{\ell}$ of $[M]_{\mathcal{R}}$, chooses $y \stackrel{R}{\leftarrow} \mathbb{Z}_p^*$ and computes

$$Z \leftarrow x \sum_{i=1}^{\ell} x_i M_i, \qquad V \leftarrow y \sum_{i=1}^{\ell} x_i M_i, \qquad (Y, Y') \leftarrow y \cdot (P, P').$$

Then, outputs $\sigma = (Z, V, Y, Y')$.

Note that

$$K = (xx_2 P, -xx_1 P, \mathbf{0}, \cdots, \mathbf{0}) \in \ker(\varphi) \backslash (\mathbf{0}, \cdots, \mathbf{0}).$$

Find K when $\ell = 2$

1. $\mathcal{A}$ receives **pk** and has access to a signing oracle.
2. $\mathcal{A}$ first chooses any invertible matrix

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in \mathbb{Z}_p^{*2\times 2}$$

   and computes its inverse

$$\begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \in \mathbb{Z}_p^{2\times 2},$$

   such that

$$\begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod p.$$

Find K when $\ell = 2$

3. $\mathcal{A}$ makes a signing query with (a_1P, a_2P) and gets its signature (Z_1, V_1, Y_1, Y_1').
4. $\mathcal{A}$ makes a signing query with (a_3P, a_4P) and gets its signature (Z_2, V_2, Y_2, Y_2').
5. $\mathcal{A}$ computes $((b_3Z_1 + b_4Z_2), -(b_1Z_1 + b_2Z_2))$.

We claim that

$$((b_3Z_1 + b_4Z_2), -(b_1Z_1 + b_2Z_2)) = (xx_2P, -xx_1P).$$

Find K when $\ell > 2$

1. $\mathcal{A}$ receives **pk** and has access to a signing oracle.
2. $\mathcal{A}$ makes a signing query with $(P, P, P, \cdots, P)$ and gets (Z_1, V_1, Y_1, Y_1').
3. $\mathcal{A}$ makes a signing query with $(2P, P, P, \cdots, P)$ and gets (Z_2, V_2, Y_2, Y_2').
4. $\mathcal{A}$ makes a signing query with $(P, 2P, P, \cdots, P)$ and gets (Z_3, V_3, Y_3, Y_3').
5. $\mathcal{A}$ computes $(Z_3 - Z_1, Z_1 - Z_2, \mathbf{0}, \cdots, \mathbf{0})$.

We claim that

$$(Z_3 - Z_1, Z_1 - Z_2, \mathbf{0}, \cdots, \mathbf{0}) = (xx_2P, -xx_1P, \mathbf{0}, \cdots, \mathbf{0}).$$

The Procedure to Find K

Note that

- The procedure to find K only involves non-adaptive queries;
- For $\ell = 2$, we need 2 queries;
- For $\ell > 2$, we need 3 queries.

Framework of Our Attacks

Breaking the EUF-Non-Adaptive-CMA:

- Find K with the non-adaptive queries;
- Output the message-signature pair $(M^* = M + \rho K, \sigma_M)$, where M has been queried in the procedure above and σ_M is its signature.

Breaking the UF-Adaptive-CMA:

- Find K with the non-adaptive queries;
- For any message M^* to be signed, generate $M = M^* + \rho K$, make a signing query with M and get its signature σ_M;
- Output σ_M as the signature of M^*.

Some Remarks

Note that we have to show

- $[M^*]_{\mathcal{R}}$ has not been queried to the signing oracle;
- Every message queried to the signing oracle must be in $(\mathbb{G}_1^*)^\ell$, that is, every component of the message is not zero.

E.g.: Breaking the EUF-NA-CMA when $\ell = 2$ (I)

- Choose any invertible matrix $\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in \mathbb{Z}_p^{*2\times 2}$ with its inverse $\begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \in \mathbb{Z}_p^{2\times 2}$.
- Query with $M^{(1)} = (a_1 P, a_2 P)$ and gets $\sigma_1 = (Z_1, V_1, Y_1, Y_1')$.
- Query with $M^{(2)} = (a_3 P, a_4 P)$ and gets $\sigma_2 = (Z_2, V_2, Y_2, Y_2')$.
- $\mathcal{A}$ computes $K = ((b_3 Z_1 + b_4 Z_2), -(b_1 Z_1 + b_2 Z_2))$.

E.g.: Breaking the EUF-NA-CMA when $\ell = 2$ (II)

- If K is equivalent to neither $M^{(1)}$ nor $M^{(2)}$, output the message K and the signature $\sigma = (\mathbf{0}, \mathbf{0}, yP, yP')$ for any $y \in \mathbb{Z}_p^*$.
- If K is equivalent to $M^{(1)}$, output the message $M^* = M^{(2)} + \rho K$ and the signature σ_2, where $\rho \in \{1, 2, 3\}$ is chosen to ensure that that $M^* \in (\mathbb{G}_1^*)^2$.
- If K is equivalent to $M^{(2)}$, output the message $M^* = M^{(1)} + \rho K$ and the signature σ_1, where $\rho \in \{1, 2, 3\}$ is chosen to ensure that that $M^* \in (\mathbb{G}_1^*)^2$.

There is only One Signature Essentially!

For any $M \notin \ker(\varphi)$,

$$\dot{\bigcup}_{\rho \in \mathbb{Z}_p} (\rho M + \ker(\varphi)) = \mathbb{G}_1^{\ell}.$$

- Given any (M, σ) where $M \notin \ker(\varphi)$, we can forge the signature on any message M', if we could find the unique ρ such that $M' \in \rho M + \ker(\varphi)$.

The Weak Point and How to Fix

In [HS14]:

- **Sign**$_{\mathcal{R}}(M, \mathbf{sk})$: On representative $M \in (\mathbb{G}_1^*)^\ell$ of $[M]_\mathcal{R}$, chooses $y \xleftarrow{R} \mathbb{Z}_p^*$ and computes $\sigma = (Z, V, Y, Y')$, where

$$Z \leftarrow x \sum_{i=1}^{\ell} x_i M_i, \quad V \leftarrow y \sum_{i=1}^{\ell} x_i M_i, \quad (Y, Y') \leftarrow y \cdot (P, P').$$

The Weak Point and How to Fix

In [HS14]:

- **Sign**$_{\mathcal{R}}(M, \mathbf{sk})$: On representative $M \in (\mathbb{G}_1^*)^\ell$ of $[M]_{\mathcal{R}}$, chooses $y \xleftarrow{R} \mathbb{Z}_p^*$ and computes $\sigma = (Z, V, Y, Y')$, where

$$Z \leftarrow x \sum_{i=1}^{\ell} x_i M_i, \qquad V \leftarrow y \sum_{i=1}^{\ell} x_i M_i, \qquad (Y, Y') \leftarrow y \cdot (P, P').$$

In [FHS14] eprint 2014/944:

- **Sign**$_{\mathcal{R}}(M, \mathbf{sk})$: On representative $M \in (\mathbb{G}_1^*)^\ell$ of $[M]_{\mathcal{R}}$, chooses $y \xleftarrow{R} \mathbb{Z}_p^*$ and computes $\sigma = (V, Y, Y')$, where

$$V \leftarrow y \sum_{i=1}^{\ell} x_i M_i, \qquad (Y, Y') \leftarrow \frac{1}{y} \cdot (P, P').$$

Remarks about FHS14

- The FHS14 scheme is proven to be EUF-CMA;

- It certainly can resist our attack;
- It still employs the structure $\sum_{i=1}^{\ell} x_i M_i$.
  - If we can find $K \in \ker(\varphi)$, the scheme will be insecure, but it seems we can not;
  - If part of the private key are leaked, such as x_1 and x_2, we can find K.

Thank You!

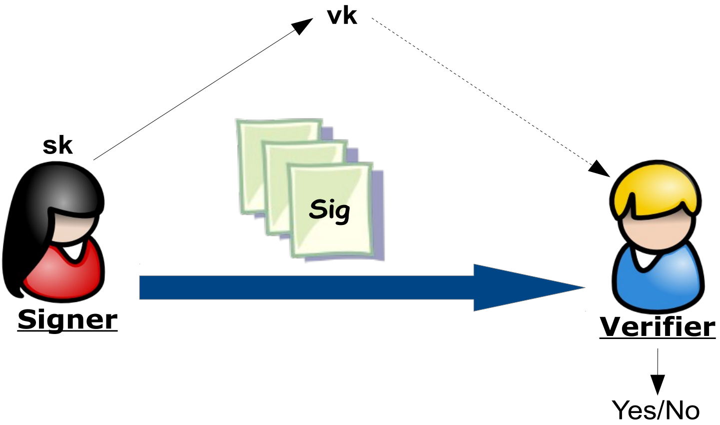
Short Structure-Preserving Signatures

Essam Ghadafi

e.ghadafi@ucl.ac.uk
Department of Computer Science,
University College London

CT-RSA 2016

Outline



Unforgeabiltiy: You can only sign messages if you have the signing key

$\mathbb{G}$, $\tilde{\mathbb{G}}$, $\mathbb{T}$ are finite cyclic groups of prime order p, where $\mathbb{G} = \langle G \rangle$ and $\tilde{\mathbb{G}} = \langle \tilde{G} \rangle$

Pairing $(e : \mathbb{G} \times \tilde{\mathbb{G}} \longrightarrow \mathbb{T})$:
The function e must have the following properties:

- Bilinearity: $\forall P \in \mathbb{G}$, $\forall \tilde{Q} \in \tilde{\mathbb{G}}$, $\forall x, y \in \mathbb{Z}$, we have

$$e(P^x, \tilde{Q}^y) = e(P, \tilde{Q})^{xy}$$

- Non-Degeneracy: The value $e(G, \tilde{G}) \neq 1$ generates $\mathbb{T}$
- The function e is efficiently computable

Type-III [GPS08]: $\mathbb{G} \neq \tilde{\mathbb{G}}$ and no efficiently computable homomorphism between $\mathbb{G}$ and $\tilde{\mathbb{G}}$ in either direction

Some History:

- The term "Structure-Preserving" was coined by Abe et al. 2010
- Earlier constructions: Groth 2006 and Green and Hohenberger 2008
- Many constructions in the 3 different main types of bilinear groups
- Optimal Type-III constructions are the most efficient

What are they?

DEFINITION (A STRUCTURE-PRESERVING SIGNATURE)

A signature scheme (defined over bilinear groups) where:

- m, vk and σ are elements of $\mathbb{G}$ and/or $\tilde{\mathbb{G}}$
- Verifying signatures only involves deciding group membership and evaluating pairing-product equations (PPE):

$$\prod_i \prod_j e(A_i, \tilde{B}_j)^{c_{i,j}} = Z,$$

where $A_i \in \mathbb{G}$, $\tilde{B}_j \in \tilde{\mathbb{G}}$ and $Z \in \mathbb{T}$ are group elements appearing in $\mathcal{P}, m, \mathsf{vk}, \sigma$, whereas $c_{i,j} \in \mathbb{Z}_p$ are constants

Why Structure-Preserving Signatures?

- Compose well with other pairing-based schemes
  - Easy to encrypt
    - Compose well with ElGamal/BBS linear encryption
  - Easy to combine with NIZK proofs
    - Compose well with Groth-Sahai proofs

Applications of Structure-Preserving Signatures:

- Blind signatures
- Group signatures
- Malleable signatures
- Tightly secure encryption schemes
- Anonymous credentials
- Oblivious transfer
- Network coding
- ...

Lower Bounds (for unilateral messages) in Type-III Bilinear Groups (Abe et al. 2011):

- Signatures contain at least 3 group elements
- Signatures cannot be unilateral (must contain elements from both $\mathbb{G}$ and $\tilde{\mathbb{G}}$)
    - Note: Size of elements of $\tilde{\mathbb{G}}$ are at least twice as big as those of $\mathbb{G}$
- At least 2 PPE verification equations

- A new signature scheme in Type-III bilinear groups with shorter signatures than existing ones:
  - Signatures consist of 3 elements from $\mathbb{G}$ (i.e. unilateral)
  - 2 PPE verification equations (5 pairings in total)
  - Message space is the set of Diffie-Hellman pairs (Abe et al. 2010):
    - The set $\hat{\mathbb{G}} = \{(M, \tilde{N}) | (M, \tilde{N}) \in \mathbb{G} \times \tilde{\mathbb{G}}, e(M, \tilde{G}) = e(G, \tilde{N})\}$
- More efficient instantiations of some existing cryptographic protocols (e.g. DAA)

The Underlying Idea:

- Can be viewed as an extension of the non-structure-preserving scheme of Pointcheval and Sanders (CT-RSA 2016)
- Can be viewed as a more efficient variant of Ghadafi (ACISP 2013) Camenisch-Lysyanskaya based structure-preserving scheme

The Scheme:

- **KeyGen:** Choose $x, y \leftarrow \mathbb{Z}_p$, set $\mathsf{sk} := (x, y)$ and $\mathsf{pk} := (\tilde{X} := \tilde{G}^x, \tilde{Y} := \tilde{G}^y) \in \tilde{\mathbb{G}}^2$
- **Sign:** To sign $(M, \tilde{N}) \in \hat{\mathbb{G}}$,
  - Choose $a \leftarrow \mathbb{Z}_p^\times$, $\sigma := (A := G^a,\ B := M^a,\ C := A^x \cdot B^y) \in \mathbb{G}^3$
- **Verify:** Check that $A \neq 1_{\mathbb{G}}$ and $(M, \tilde{N}) \in \hat{\mathbb{G}}$ and

$$e(A, \tilde{N}) = e(B, \tilde{G})$$
$$e(C, \tilde{G}) = e(A, \tilde{X}) e(B, \tilde{Y})$$

- **Randomize:** Choose $r \leftarrow \mathbb{Z}_p^\times$, return $\sigma' := (A' := A^r,\ B' := B^r,\ C' := C^r)$

Some Properties of the Scheme:

- The scheme is secure in the generic group model
  - $\Rightarrow$ alternatively can be based on an interactive assumption
- Unilateral signatures
- (Perfectly) Fully re-randomizable
- Only M part of the message is needed for signing

Efficiency Comparison

Scheme	Size				R?	Assumptions	Verification	
	σ	vk	$\mathcal{P}$	m			PPE	Pairing
[GH08] [a]	$\mathbb{G}^4 \times \tilde{\mathbb{G}}$	$\tilde{\mathbb{G}}^2$	-	$\mathbb{G}$	Y	q-HLRSW	4	8
[Fuc09]	$\mathbb{G}^3 \times \tilde{\mathbb{G}}^2$	$\mathbb{G} \times \tilde{\mathbb{G}}$	$\mathbb{G}^3$	$\hat{\mathbb{G}}$	N	q-ADHSDH+AWFCDH	3	9
[AFG+10] I	$\mathbb{G}^5 \times \tilde{\mathbb{G}}^2$	$\mathbb{G}^{10} \times \tilde{\mathbb{G}}^4$	-	$\mathbb{G}$	P	q-SFP	2	12
[AFG+10] II	$\mathbb{G}^2 \times \tilde{\mathbb{G}}^5$	$\mathbb{G}^{10} \times \tilde{\mathbb{G}}^4$	-	$\tilde{\mathbb{G}}$	P	q-SFP	2	12
[AGH+11] I	$\mathbb{G}^2 \times \tilde{\mathbb{G}}$	$\mathbb{G} \times \tilde{\mathbb{G}}^3$	-	$\mathbb{G} \times \tilde{\mathbb{G}}$	N	GGM	2	7
[AGH+11] II	$\mathbb{G}^2 \times \tilde{\mathbb{G}}$	$\mathbb{G} \times \tilde{\mathbb{G}}$	-	$\tilde{\mathbb{G}}$	Y	GGM	2	5
[Gha13]	$\mathbb{G}^4$	$\tilde{\mathbb{G}}^2$	-	$\hat{\mathbb{G}}$	Y	DH-LRSW	3	7
[CM14] I	$\mathbb{G} \times \tilde{\mathbb{G}}^2$	$\mathbb{G}^2$	-	$\tilde{\mathbb{G}}$	N	GGM	2	5
[CM14] II	$\mathbb{G} \times \tilde{\mathbb{G}}^2$	$\mathbb{G}^2$	-	$\tilde{\mathbb{G}}$	Y	GGM	2	6
[CM14] III	$\mathbb{G}^2 \times \tilde{\mathbb{G}}$	$\tilde{\mathbb{G}}^2$	-	$\mathbb{G}$	Y	GGM	2	6
[AGO+14] I	$\mathbb{G}^3 \times \tilde{\mathbb{G}}$	$\tilde{\mathbb{G}}$	$\mathbb{G}$	$\mathbb{G}$	Y	GGM	2	6
[AGO+14] II	$\mathbb{G}^2 \times \tilde{\mathbb{G}}$	$\tilde{\mathbb{G}}$	$\mathbb{G}$	$\mathbb{G}$	N	GGM	2	6
[BFF15]	$\mathbb{G} \times \tilde{\mathbb{G}}^2$	$\mathbb{G}^2$	-	$\tilde{\mathbb{G}}$	Y	GGM	2	5
[Gro15] I	$\mathbb{G} \times \tilde{\mathbb{G}}^2$	$\mathbb{G}$	$\tilde{\mathbb{G}}$	$\tilde{\mathbb{G}}$	Y	GGM	2	6
[Gro15] II	$\mathbb{G} \times \tilde{\mathbb{G}}^2$	$\mathbb{G}$	$\tilde{\mathbb{G}}$	$\tilde{\mathbb{G}}$	N	GGM	2	7
Ours	$\mathbb{G}^3$	$\tilde{\mathbb{G}}^2$	-	$\hat{\mathbb{G}}$	Y	GGM	2	5

[a] This scheme is only secure against a random message attack.

Comparison with schemes with the same message space

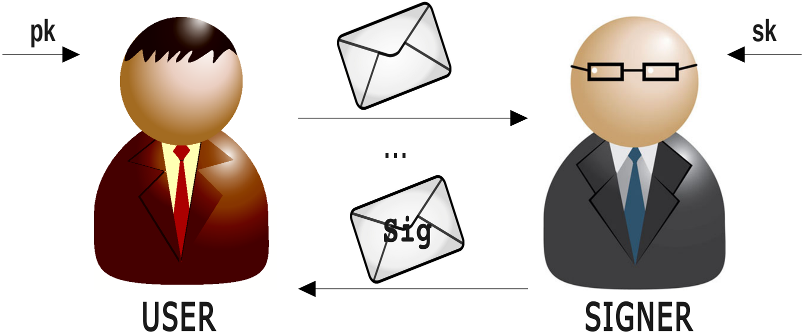
Scheme	Size			R?	Assumptions	Verification	
	σ	vk	$\mathcal{P}$			PPE	Pairing
[Fuc09]	$\mathbb{G}^3 \times \tilde{\mathbb{G}}^2$	$\mathbb{G} \times \tilde{\mathbb{G}}$	$\mathbb{G}^3$	N	q-ADHSDH+AWFCDH	3	9 or (7 & 2 ECAdd)
[Gha13]	$\mathbb{G}^4$	$\tilde{\mathbb{G}}^2$	-	Y	DH-LRSW	3	7 or (6 & 1 ECAdd)
Ours	$\mathbb{G}^3$	$\tilde{\mathbb{G}}^2$	-	Y	GGM	2	5

* Cost does not include checking well-formedness of the message

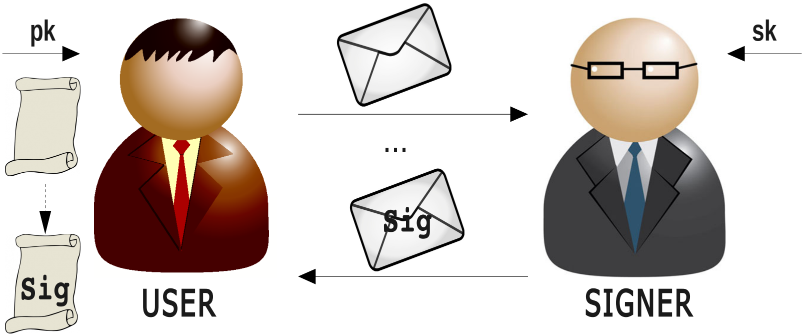
Bernhard et al. 2013 gave a generic construction of DAA which requires the following tools:

- **Randomizable Weakly Blind Signatures (RwBS)**
  - Used by the Issuer to issue certificates as credentials when users join the group
- **Linkable Indistinguishable Tags (LIT)**
  - Needed to provide the linkability of signatures when the same basename is signed by the same user
- **Signatures of Knowledge (SoK)**
  - Used by users to prove they have a credential and that the signature on the basename verifies w.r.t. thier certified secret key


pk
USER
sk
SIGNER

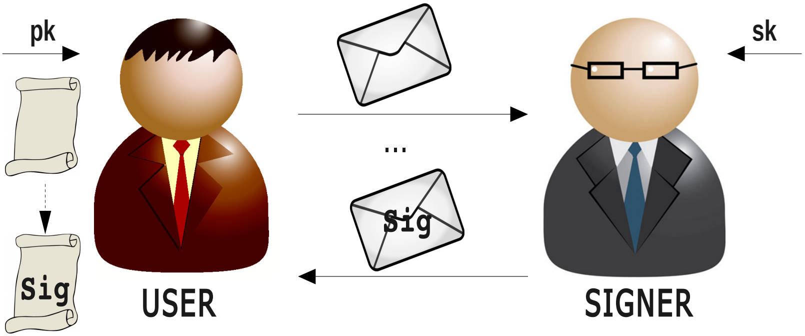

pk
sk
...
sig
USER
SIGNER

BLIND SIGNATURES



Security Requirements:

- **Blindness:** An adversary (i.e. a signer) who chooses the messages, does not learn which message being signed and cannot link a signature to its signing session
- **Unforgeability:** An adversary (i.e. a user) cannot forge new signatures



Security Requirements:

- **Blindness:** An adversary (i.e. a signer) who chooses the messages, does not learn which message being signed and cannot link a signature to its signing session
- **Unforgeability:** An adversary (i.e. a user) cannot forge new signatures

Similar to blind signatures but:

- **Randomizability:** Given a signature σ, *anyone* can produce a new signature σ' on the same message
- **Weak Blindness:** Same as blindness but the adversary never sees the messages $\Rightarrow$ The adversary cannot tell if he was given a signature on a different message or a re-randomization of a signature on the same message

The Idea: Combine the new scheme with SXDH-based Groth-Sahai proofs

- Only M is needed for signing $\Rightarrow$ To request a signature on $(M, \tilde{N})$, send M and a NIZKPoK π of $\tilde{N}$

$$\mathcal{L}_{\text{User}} : \left\{ \left(M, \tilde{N}\right) : e(G, \underline{\tilde{N}}) = e(M, \underline{\tilde{G}'}) \;\wedge\; \underline{\tilde{G}'} \cdot \tilde{G} = 1_{\tilde{\mathbb{G}}} \right\}$$

- The signer produces a signature σ and a NIZK proof Ω (without knowing $\tilde{N}$) for the validity of σ

$$\mathcal{L}_{\text{Signer}} : \left\{ \left((A, B, M), \tilde{A}\right) : e(G, \underline{\tilde{A}}) = e(A, \underline{\tilde{G}'}) \;\wedge\; e(M, \underline{\tilde{A}}) = e(B, \underline{\tilde{G}'}) \;\wedge\; \underline{\tilde{G}'} \cdot \tilde{G} = 1_{\tilde{\mathbb{G}}} \right\}$$

- Fully re-randomizable $\Rightarrow$ User verifies Ω and the final signature is a re-randomization of σ

The Idea: Combine the new scheme with SXDH-based Groth-Sahai proofs

- Only M is needed for signing $\Rightarrow$ To request a signature on $(M, \tilde{N})$, send M and a NIZKPoK π of $\tilde{N}$

$$\mathcal{L}_{\text{User}} : \left\{ \left(M, \tilde{N} \right) : e(G, \underline{\tilde{N}}) = e(M, \underline{\tilde{G}'}) \ \wedge \ \underline{\tilde{G}'} \cdot \tilde{G} = 1_{\tilde{\mathbb{G}}} \right\}$$

- The signer produces a signature σ and a NIZK proof Ω (without knowing $\tilde{N}$) for the validity of σ

$$\mathcal{L}_{\text{Signer}} : \left\{ \left((A, B, M), \tilde{A} \right) : e(G, \underline{\tilde{A}}) = e(A, \underline{\tilde{G}'}) \ \wedge \ e(M, \underline{\tilde{A}}) = e(B, \underline{\tilde{G}'}) \ \wedge \ \underline{\tilde{G}'} \cdot \tilde{G} = 1_{\tilde{\mathbb{G}}} \right\}$$

- Fully re-randomizable $\Rightarrow$ User verifies Ω and the final signature is a re-randomization of σ

The Idea: Combine the new scheme with SXDH-based Groth-Sahai proofs

- Only M is needed for signing $\Rightarrow$ To request a signature on $(M, \tilde{N})$, send M and a NIZKPoK π of $\tilde{N}$

$$\mathcal{L}_{\text{User}} : \left\{ \left(M, \tilde{N}\right) : e(G, \underline{\tilde{N}}) = e(M, \underline{\tilde{G}'}) \ \wedge\ \underline{\tilde{G}'} \cdot \tilde{G} = 1_{\tilde{\mathbb{G}}} \right\}$$

- The signer produces a signature σ and a NIZK proof Ω (without knowing $\tilde{N}$) for the validity of σ

$$\mathcal{L}_{\text{Signer}} : \left\{ \left((A, B, M), \tilde{A}\right) : e(G, \underline{\tilde{A}}) = e(A, \underline{\tilde{G}'}) \wedge\ e(M, \underline{\tilde{A}}) = e(B, \underline{\tilde{G}'}) \ \wedge\ \underline{\tilde{G}'} \cdot \tilde{G} = 1_{\tilde{\mathbb{G}}} \right\}$$

- Fully re-randomizable $\Rightarrow$ User verifies Ω and the final signature is a re-randomization of σ

The Idea: Combine the new scheme with SXDH-based Groth-Sahai proofs

- Only M is needed for signing $\Rightarrow$ To request a signature on $(M, \tilde{N})$, send M and a NIZKPoK π of $\tilde{N}$

$$\mathcal{L}_{\text{User}} : \left\{ \left(M, \tilde{N}\right) : e(G, \underline{\tilde{N}}) = e(M, \underline{\tilde{G}'}) \ \wedge \ \underline{\tilde{G}'} \cdot \tilde{G} = 1_{\tilde{\mathbb{G}}} \right\}$$

- The signer produces a signature σ and a NIZK proof Ω (without knowing $\tilde{N}$) for the validity of σ

$$\mathcal{L}_{\text{Signer}} : \left\{ \left((A, B, M), \tilde{A}\right) : e(G, \underline{\tilde{A}}) = e(A, \underline{\tilde{G}'}) \wedge \ e(M, \underline{\tilde{A}}) = e(B, \underline{\tilde{G}'}) \ \wedge \ \underline{\tilde{G}'} \cdot \tilde{G} = 1_{\tilde{\mathbb{G}}} \right\}$$

- Fully re-randomizable $\Rightarrow$ User verifies Ω and the final signature is a re-randomization of σ

Security of the RwBS Scheme:

- Unforgeability of the SPS Scheme + SXDH

Efficiency of the RwBS Scheme:

Scheme	Signature	Verification	
		PPE	Pairing
Bernhard et al. 2013 I	$\mathbb{G}^4$	3	7 or (6 & 1 ECAdd)
Ours	$\mathbb{G}^3$	2	5

- **Summary:**
  - A new unilateral SPS scheme with short signatures
  - More efficient instantiations of building blocks for DAA without random oracles

- **Open Problems:**
  - More efficient constructions of unilateral structure-preserving signatures
  - Constructions based on standard assumptions (e.g. DDH, DLIN, etc.)
  - (Constant-size?) constructions for a vector of Diffie-Hellman pairs

Thank you for your attention!
Questions?