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

Yanbin Pan **

Key Laboratory of Mathematics Mechanization, NCMIS,
Academy of Mathematics and Systems Science, Chinese Academy of Sciences
Beijing 100190, China
panyanbin@amss.ac.cn

Abstract. At Asiacrypt 2014, Hanser and Slamanig presented a new cryptographic primitive called structure-preserving signature scheme on equivalence classes in the message space $(\mathbb{G}_1^*)^\ell$, where $\mathbb{G}_1$ is some additive cyclic group. Based on the signature scheme, they constructed an efficient multi-show attribute-based anonymous credential system that allows to encode an arbitrary number of attributes. The signature scheme was claimed to be existentially unforgeable under the adaptive chosen message attacks in the generic group model. However, for $\ell = 2$, Fuchsbauer pointed out a valid existential forgery can be generated with overwhelming probability by using 4 adaptive chosen-message queries. Hence, the scheme is existentially forgeable under the adaptive chosen message attack at least when $\ell = 2$. In this paper, we show that even for the general case $\ell \geq 2$, the scheme is *existentially forgeable* under the *non-adaptive* chosen message attack and *universally forgeable* under the *adaptive* chosen message attack. It is surprising that our attacks will succeed all the time and need fewer queries, which give a better description of the scheme's security.

Keywords: Structure-preserving signature, equivalence classes, EUF-CMA, UF-CMA.

1 Introduction

Structure-preserving signatures introduced by Abe *et al.* [2] have many applications in cryptographic constructions, such as blind signatures [2, 8], group signatures [2, 8, 14], homomorphic signatures [13, 3], and tightly secure encryption [12, 1]. Typically, the structure-preserving signatures are defined over some groups equipped with a bilinear map. The public key, the messages and the signatures in

* The final publication is available at http://link.springer.com/book/10.1007%2F978-3-319-29485-8.

** This work was supported in part by the NNSF of China (No. 11201458, No. 11471314 and No. 61572490), and in part by the National Center for Mathematics and Interdisciplinary Sciences, CAS.

a structure-preserving signature scheme consist only of group elements, and the signature can be verified just by deciding group membership and by evaluating some pairing-product equations.

At Asiacrypt 2014, Hanser and Slamanig [10] proposed a new cryptographic primitive called structure-preserving signature scheme on equivalence classes (SPS-EQ), which allows to sign at one time an equivalence class of a group-element vector instead of just the vector itself. As shown in [10], the SPS-EQ scheme asks for some additional conditions to enable its applications to construct an efficient attribute-based multi-show anonymous credential systems. First, given a message-signature pair (here the message can be seen as a representative of some class), another valid signature for every other representative of the class can be efficiently produced, without knowing the secret key. Second, any two representatives of the same class with corresponding signatures seem unlinkable, which was called class hiding in [10].

Hanser and Slamanig [10] also presented a concrete SPS-EQ scheme on equivalence classes in the message space $(\mathbb{G}_1^*)^\ell$, where $\mathbb{G}_1$ is some additive cyclic group. Any two vectors in the same equivalence class are equal up to a scale factor. The scheme is claimed to be existentially unforgeable under adaptive chosen message attack (EUF-CMA) in the generic group model for SXDH groups [5]. However, Fuchsbauer [6] later pointed out their claim is flawed when $\ell = 2$ by showing how to generate a valid existential forgery with overwhelming probability with 4 chosen message queries. For $\ell \geq 3$, Fuchsbauer [6] did not give any discussion and it seems not trivial to generalize his attack to the case when $\ell \geq 3$. Hence, the signature scheme can not be EUF-CMA secure, at least when $\ell = 2$.

In this paper, we study its security further. Both of the cases when $\ell = 2$ and $\ell \geq 3$ are considered.

First, we show that the scheme is *existentially forgeable* under the *non-adaptive* chosen message attack. More precisely, we present a polynomial-time attack which can generate a valid existential forgery with just 2 (*resp.* 3) non-adaptive chosen message queries for $\ell = 2$ (*resp.* $\ell \geq 3$), which is half of the number of the queries needed in Fuchsbauer's adaptive chosen message attack.

Second, we show that the scheme is in fact *universally forgeable* under the *adaptive* chosen message attack. In our polynomial-time attack, we can forge the valid signature for any given message with 3 (*resp.* 4) chosen message queries for $\ell = 2$ (*resp.* $\ell \geq 3$), which is also less than the number of the queries needed in Fuchsbauer's attack.

Moreover, both of our attacks will always succeed, whereas Fuchsbauer's attack succeeds with overwhelming probability.

In a revised version [11], Hanser and Slamanig recently pointed out that the original security proof in [10] was incorrect since in it just the non-adaptive message queries were considered, but the adaptive message queries were neglected. They also proved the scheme can at least provide existential unforgeability under random message attacks (EUF-RMA). Together with our results, the security of this scheme is much more clear, which can be summarized as in Table 1.

Attack Model	Security	ℓ
Random Message Attack	Existential Unforgeability [11]	$\ell \geq 2$
Non-Adaptive Chosen Message Attack	Existential Forgeability [this work]	$\ell \geq 2$
Adaptive Chosen Message Attack	Existential Forgeability [6]	$\ell = 2$
	Universal Forgeability [this work]	$\ell \geq 2$

Table 1. The Security of the Hanser-Slamanig SPS-EQ Scheme

To fix the Hanser-Slamanig scheme, Fuchsbauer, Hanser and Slamanig [7] presented a new SPS-EQ scheme which is proved to be secure under adaptive chosen message attacks. We have to point out that the new scheme can resist our attack.

Roadmap. The remainder of the paper is organized as follows. In Section 2, we give some preliminaries needed. We describe the Hanser-Slamanig SPS-EQ scheme in Section 3, and present our attacks in Section 4. Finally, a short conclusion is given in Section 5.

2 Preliminaries

We denote by $\mathbb{Z}$ the integer ring, by $\mathbb{Z}_p$ the residue class ring $\mathbb{Z}/p\mathbb{Z}$ and by $\mathbb{Z}_p^*$ the group of all the invertible elements in $\mathbb{Z}_p$. Let $\mathbb{G}$ be the cyclic group and $\mathbb{G}^*$ be the set of all the non-zero elements in $\mathbb{G}$. Denote by $1_{\mathbb{G}}$ (*resp.* $\mathbf{0}$) the identity element when $\mathbb{G}$ is multiplicative (*resp.* additive). We denote by $\ker(\varphi)$ the kernel of map φ.

2.1 Bilinear Map

As in [10], we first give some definitions about bilinear map.

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

Definition 2 (Bilinear Group Generator). *A bilinear-group generator is a probabilistic polynomial-time (PPT) algorithm BGGen that on input a security parameter 1^κ outputs a bilinear group description $\boldsymbol{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P, P')$ which satisfies the definition of bilinear map and p is a κ-bit prime.*

2.2 Structure-Preserving Signature Scheme on Equivalence Classes

Given a cyclic group $\mathbb{G}$ of prime order p and an integer $\ell > 1$, we first define the equivalence relation $\mathcal{R}$ on length-ℓ vectors of nontrivial group elements as used in [10]:

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

Then we denote by $[M]_\mathcal{R}$ all the elements in $(\mathbb{G}^*)^\ell$ equivalent to $M \in (\mathbb{G}^*)^\ell$ with relation $\mathcal{R}$, that is,

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

We next give the definition of SPS-EQ as in [10].

Definition 3 (Structure-Preserving Signature Scheme for Equivalence Relation $\mathcal{R}$ (SPS-EQ-$\mathcal{R}$)). *An SPS-EQ-$\mathcal{R}$ scheme consists of the following polynomial-time algorithms:*

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

2.3 Security of Digital Signature Scheme

As in [9], the security of digital signature scheme can be considered under random message attack, non-adaptive chosen message attack, adaptive chosen message attack and so on. We just briefly introduce these three attacks.

- Random message attack: The polynomial-time adversary $\mathcal{A}$ has access to a signing oracle which on every call randomly chooses a message M from the message space, generates the signature σ on M and returns (M, σ).
- Non-adaptive chosen message attack (directed chosen message attack): The polynomial-time adversary $\mathcal{A}$ has access to a signing oracle and is allowed to obtain valid signatures for a chosen list of messages $M_1, M_2, \cdots, M_{poly(\kappa)}$ after seeing the public key but before knowing any signatures from the signing oracle.
- Adaptive chosen message attack: The polynomial-time adversary $\mathcal{A}$ has access to a signing oracle and can query it with any chosen message anytime.

A digital signature scheme is considered to be existentially unforgeable under some attack if any PPT adversary $\mathcal{A}$ will generate a valid message-signature pair with only negligible probability, where the message has not been queried to the signing oracle. To define the existentially unforgeability for the SPS-EQ-$\mathcal{R}$ scheme, a little adaption is needed, that is, not just the message but also the equivalence class of the message has not been queried. For example, we give the definition of EUF-CMA as in [10].

Definition 4 (EUF-CMA for SPS-EQ-$\mathcal{R}$ scheme). *An SPS-EQ-$\mathcal{R}$ scheme on $(\mathbb{G}^*)^\ell$ is called existentially unforgeable under adaptive message chosen attack if for any PPT adversary $\mathcal{A}$ having access to a signing oracle $\mathcal{O}(\boldsymbol{sk}, \cdot)$, there is a negligible function $\epsilon(\cdot)$ such that:*

$$\boldsymbol{Pr}\left[\begin{array}{c} \boldsymbol{BG} \leftarrow BGGen_{\mathcal{R}}(\kappa), (\boldsymbol{sk}, \boldsymbol{pk}) \leftarrow KeyGen_{\mathcal{R}}(\boldsymbol{BG}, \ell), (M^*, \sigma^*) \leftarrow \mathcal{A}^{\mathcal{O}(\boldsymbol{sk}, \cdot)}(\boldsymbol{pk}) : \\ [M^*]_{\mathcal{R}} \neq [M]_{\mathcal{R}} \ \forall M \in Q \wedge Verify_{\mathcal{R}}(M^*, \sigma^*, \boldsymbol{pk}) = true \end{array}\right]$$

$\leq \epsilon(\kappa)$,

where Q is the set of queries which $\mathcal{A}$ has queried to the signing oracle $\mathcal{O}$.

Similarly we can also define the existentially unforgeability for non-adaptive chosen message attack and random message attack.

Under any attack model, the SPS-EQ-$\mathcal{R}$ scheme is called universal forgeable if there is a polynomial-time adversary $\mathcal{A}$ who can forge with overwhelming probability valid signature on any message, whose equivalence class has not been queried to the signing oracle.

3 The Hanser-Slamanig SPS-EQ Scheme

3.1 Description of the Hanser-Slamanig SPS-EQ Scheme

As follows we describe the SPS-EQ scheme proposed by Hanser and Slamanig.

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

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

  where prime p is the order of cyclic groups $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$, and $\mathbb{G}_1$ and $\mathbb{G}_2$ are additive but $\mathbb{G}_T$ is multiplicative where there is a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$, P and P' generate $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively.
- $\mathbf{KeyGen}_{\mathcal{R}}(\mathbf{BG}, \ell)$: Given a bilinear group description $\mathbf{BG}$ and vector length $\ell > 1$, chooses $x \xleftarrow{R} \mathbb{Z}_p^*$ and $(x_i)_{i=1}^{\ell} \xleftarrow{R} (\mathbb{Z}_p^*)^\ell$, sets the secret key as

$$\mathbf{sk} \leftarrow (x, (x_i)_{i=1}^{\ell}),$$

  computes the public key

$$\mathbf{pk} \leftarrow (X', (X_i')_{i=1}^{\ell}) = (xP', (x_i x P')_{i=1}^{\ell})$$

  and outputs $(\mathbf{sk}, \mathbf{pk})$.

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

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

Then, outputs $\sigma = (Z, V, Y, Y')$ as signature for the equivalence class $[M]_{\mathcal{R}}$.
– $\mathbf{ChgRep}_{\mathcal{R}}(M, \sigma, \rho, \mathbf{pk})$: On input a representative $M = (M_i)_{i=1}^{\ell} \in (\mathbb{G}_1^*)^{\ell}$ of an equivalence class $[M]_{\mathcal{R}}$, the corresponding signature $\sigma = (Z, V, Y, Y')$, a scalar $\rho \in \mathbb{Z}_p^*$ and a public key $\mathbf{pk}$, this algorithms picks $\hat{y} \xleftarrow{R} \mathbb{Z}_p^*$ and returns $(\hat{M}, \hat{\sigma})$ where $\hat{\sigma} \leftarrow (\rho Z, \hat{y}\rho V, \hat{y}Y, \hat{y}Y')$ is the update of signature σ for the new representative $\hat{M} \leftarrow \rho(M_i)_{i=1}^{\ell}$.
– $\mathbf{Verify}_{\mathcal{R}}(M, \sigma, \mathbf{pk})$: Given a representative $M = (M_i)_{i=1}^{\ell} \in (\mathbb{G}_1^*)^{\ell}$ of equivalence class $[M]_{\mathcal{R}}$, a signature $\sigma = (Z, V, Y, Y')$ and public key $\mathbf{pk} = (X', (X_i')_{i=1}^{\ell})$, 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.

3.2 Fuchsbauer's Attack to Break the EUF-CMA of the Scheme

For completeness, we describe Fuchsbauer's attack [6] for $l = 2$ briefly. Consider the following polynomial-time adversary $\mathcal{A}$:

1. $\mathcal{A}$ receives $\mathbf{pk}$ 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).

Fuchsbauer showed that (Z_4, V_4, Y_4, Y_4') is a valid signature of (Z_3, Z_1) and with overwhelming probability the equivalence class of (Z_3, Z_1) has not been queried to the signing oracle. However, Fuchsbauer gave no discussions about the case when $\ell \geq 3$ and it seems not trivial to generalize his attack to the case when $\ell \geq 3$. Moreover, Fuchsbauer neglected to check whether (Z_3, Z_1) is in $(\mathbb{G}_1^*)^2$ or not in his proof.

4 Our Attacks

4.1 Key Observation of Our Attacks

We first give the key observation of our attacks:

Lemma 1. *Consider the following map:*

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

For any $K = (K_i)_{i=1}^\ell \in \ker(\varphi)$, if $\sigma = (Z, V, Y, Y')$ is a valid signature on message $M = (M_i)_{i=1}^\ell$, then σ is also a valid signature on $M+K = (M_i+K_i)_{i=1}^\ell$.

Proof. Notice that to verify the signature σ for $M + K$, the only thing we need check is $\prod_{i=1}^\ell e(M_i + K_i, X_i') \stackrel{?}{=} e(Z, P)$. Assume $M_i = m_i P$ and $K_i = k_i P$. Since $(K_i)_{i=1}^\ell \in \ker(\varphi)$, we have $(\sum_{i=1}^\ell x_i k_i)P = \mathbf{0}$ which yields $\sum_{i=1}^\ell x_i k_i = 0 \mod p$. Then we have

$$\begin{aligned}\prod_{i=1}^\ell e(M_i + K_i, X_i') &= e(P, P')^{\sum_{i=1}^\ell x x_i (m_i + k_i) \mod p} \\ &= e(P, P')^{\sum_{i=1}^\ell x x_i m_i + \sum_{i=1}^\ell x x_i k_i \mod p} \\ &= e(P, P')^{\sum_{i=1}^\ell x x_i m_i \mod p} \\ &= \prod_{i=1}^\ell e(M_i, X_i') \\ &= e(Z, P).\end{aligned}$$

The last equation holds since σ is a valid signature on M.

By Lemma 1, if we can find any nontrivial $K \in \ker(\varphi)$, we can forge the signature on any message M by querying the signing oracle with $M - K$ and outputting the returned signature. Next we will show the nontrivial K can be obtained efficiently under the non-adaptive chosen message attack.

4.2 Procedure to Find Nontrivial Element in ker(φ)

We claim that

Lemma 2. *Under the non-adaptive chosen message attack, there is a polynomial time adversary $\mathcal{A}$ who can find a nontrivial element in* $\ker(\varphi)$*. Moreover,*

- *If $\ell = 2$, $\mathcal{A}$ needs two non-adaptive chosen message queries;*
- *If $\ell \geq 3$, $\mathcal{A}$ needs three non-adaptive chosen message queries.*

Proof. We present the polynomial-time procedures **FindKernel** for adversary $\mathcal{A}$ to obtain a nontrivial element in $\ker(\varphi)$ in two cases respectively.

i. Case $\ell = 2$

Consider the following procedure **FindKernel** for adversary $\mathcal{A}$:

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

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

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

$$((b_3Z_1 + b_4Z_2), -(b_1Z_1 + b_2Z_2)) = (xx_2P, -xx_1P) \in \ker(\varphi)\backslash(\mathbf{0}, \mathbf{0}).$$

It is obvious that $(xx_2P, -xx_1P) \in \ker(\varphi)\backslash(\mathbf{0}, \mathbf{0})$ since x, x_1, x_2 are not zero. It remains to prove $((b_3Z_1 + b_4Z_2), -(b_1Z_1 + b_2Z_2)) = (xx_2P, -xx_1P)$. Notice that

$$Z_1 = x(a_1x_1 + a_2x_2)P, \quad Z_2 = x(a_3x_1 + a_4x_2)P.$$

Hence

$$\begin{aligned} b_3Z_1 + b_4Z_2 &= b_3x(a_1x_1 + a_2x_2)P + b_4x(a_3x_1 + a_4x_2)P \\ &= x((b_3a_1 + b_4a_3)x_1 + (b_3a_2 + b_4a_4)x_2)P \\ &= xx_2P \end{aligned}$$

and

$$\begin{aligned} b_1Z_1 + b_2Z_2 &= b_1x(a_1x_1 + a_2x_2)P + b_2x(a_3x_1 + a_4x_2)P \\ &= x((b_1a_1 + b_2a_3)x_1 + (b_1a_2 + b_2a_4)x_2)P \\ &= xx_1P. \end{aligned}$$

ii. Case $l \geq 3$

We can generalize the procedure above for the case $\ell \geq 3$ by involving an l-by-l invertible matrix. However, notice that $(xx_2P, -xx_1P, \mathbf{0}, \mathbf{0}, \cdots, \mathbf{0})$ is a non-trivial element in the corresponding $\ker(\varphi)$. We have a more clever procedure **FindKernel** for adversary $\mathcal{A}$ to obtain $(xx_2P, -xx_1P, \mathbf{0}, \mathbf{0}, \cdots, \mathbf{0})$.

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

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

Notice that

$$Z_1 = x(x_1 + x_2 + \sum_{i=2}^{\ell} x_i)P, Z_2 = x(2x_1 + x_2 + \sum_{i=2}^{\ell} x_i)P, Z_3 = x(x_1 + 2x_2 + \sum_{i=2}^{\ell} x_i)P,$$

which implies

$$\begin{aligned} Z_3 - Z_1 &= xx_2P, \\ Z_1 - Z_2 &= -xx_1P. \end{aligned}$$

Hence the lemma follows.

Remark 1. For the **FindKernel** procedure when $\ell \geq 3$, notice that once the difference of two messages queried to the oracle is $(P, \mathbf{0}, \cdots, \mathbf{0})$, we can recover xx_1P. Similar results hold for xx_iP. In fact, we can get all the integer coefficient combination of the elements in the set $\{x^k x_{i_1} x_{i_2} \cdots x_{i_k} P | k = 1, 2, \cdots\}$ with only non-adaptive chosen message quries.

4.3 Breaking the EUF-Non-Adaptive-CMA of the Scheme

Notice that to find the nontrivial element in $\ker(\varphi)$, we just need the non-adaptive queries. To complete the non-adaptive chosen message attack, it remains to decide which message-signature pair should be outputted. Note that the outputted message should satisfy

- The equivalence class of the message has not been queried to the signing oracle;
- The message must be in $(\mathbb{G}_1^*)^\ell$, that is, every component of the message is not zero.

Before giving our attack, we first present some lemmas.

Lemma 3. *There is a polynomial time algorithm on input $(\alpha P, \beta P) \in (\mathbb{G}_1^*)^2$ and $a_i, a_j \in \mathbb{Z}_p^*$ that can decide whether $(\alpha P, \beta P)$ is equivalent to $(a_i P, a_j P)$ or not without knowing α and β.*

Proof. Recall that $(\alpha P, \beta P)$ is equivalent to $(a_i P, a_j P)$ if and only if there exits $\rho \in \mathbb{Z}_p^*$ such that $\rho(\alpha P, \beta P) = (a_i P, a_j P)$, which means that $(\alpha P, \beta P)$ is equivalent to $(a_i P, a_j P)$ if and only if

$$\det \begin{pmatrix} \alpha & \beta \\ a_i & a_j \end{pmatrix} = 0 \mod p,$$

that is,

$$a_i \beta = a_j \alpha \mod p.$$

Hence we can decide the equivalence between $(\alpha P, \beta P)$ and $(a_i P, a_j P)$ by checking if $a_i(\beta P) = a_j(\alpha P)$ in the group $\mathbb{G}_1$, which can be done in polynomial time.

Lemma 4. *For any* $(\alpha P, \beta P) \in (\mathbb{G}_1^*)^2$ *and* $a_i, a_j \in \mathbb{Z}_p^*$*, there must be at least one element* Q *in the set* $\{(a_i P + \rho\alpha P, a_j P + \rho\beta P) : \rho = 1, 2, 3\}$*, such that* $Q \in (\mathbb{G}_1^*)^2$*.*

Proof. For contradiction, suppose that every element in the set has at least one $\mathbf{0}$ as its component. Then there must be a $k \in \{1, 2\}$ such that there are at least two $\mathbf{0}$'s in the k-th components of all the three elements. Without loss of generality, suppose $a_i P + \rho_s \alpha P = a_i P + \rho_t \alpha P = \mathbf{0}$, then it can be concluded that $\rho_s = \rho_t$, which contradicts the fact that $\rho_s \neq \rho_t$.

By the two lemmas above, we have

Theorem 1. *The Hanser-Slamanig SPS-EQ scheme is existentially forgeable under the non-adaptive chosen message attack. Moreover,*

- *If* $\ell = 2$*, two non-adaptive chosen message queries is needed;*
- *If* $\ell \geq 3$*, three non-adaptive chosen message queries is needed.*

Proof. We prove the theorem for two cases respectively.

i. Case $\ell = 2$

We give our non-adaptive chosen message attack as follows:

1. $\mathcal{A}$ runs **FindKernel** to get $(xx_2P, -xx_1P) \in (\mathbb{G}_1^*)^2 \bigcap \ker(\varphi)$, the signature (Z_1, V_1, Y_1, Y_1') for (a_1P, a_2P) and the signature (Z_2, V_2, Y_2, Y_2') for (a_3P, a_4P).
2. If $(xx_2P, -xx_1P)$ is equivalent to neither (a_1P, a_2P) nor (a_3P, a_4P), $\mathcal{A}$ can output the message $M = (xx_2P, -xx_1P)$ and the corresponding signature $\sigma = (\mathbf{0}, \mathbf{0}, yP, yP')$ for any $y \in \mathbb{Z}_p^*$.
3. If $(xx_2P, -xx_1P)$ is equivalent to (a_1P, a_2P), $\mathcal{A}$ can output the message $M = (a_3P + \rho xx_2P, a_4P - \rho xx_1P)$ and the corresponding signature $\sigma = (Z_2, V_2, Y_2, Y_2')$, where ρ is chosen as in Lemma 4 such that $M \in (\mathbb{G}_1^*)^2$.
4. If $(xx_2P, -xx_1P)$ is equivalent to (a_3P, a_4P), $\mathcal{A}$ can output the message $M = (a_1P + \rho xx_2P, a_2P - \rho xx_1P)$ and the corresponding signature $\sigma = (Z_1, V_1, Y_1, Y_1')$, where ρ is chosen as in Lemma 4 such that $M \in (\mathbb{G}_1^*)^2$.

It is obvious that $M \in (\mathbb{G}_1^*)^2$ and σ is indeed a valid signature on M by Lemma 1 since $(\rho xx_2P, -\rho xx_1P) \in \ker(\varphi)$.

By Lemma 3, the equivalence can be checked in polynomial time. It is easy to check the attack can be completed in polynomial time.

It remains to show $[M]_{\mathcal{R}}$ has not been queried.

If $(xx_2P, -xx_1P)$ is equivalent to neither (a_1P, a_2P) nor (a_3P, a_4P), $[M]_{\mathcal{R}}$ has not been queried obviously.

If $(xx_2P, -xx_1P)$ is equivalent to (a_1P, a_2P), we can write $xx_2 = ka_1$ and $-xx_1 = ka_2$ for some $k \in \mathbb{Z}_p^*$. We claim that now $(a_3P + \rho xx_2P, a_4P - \rho xx_1P)$

can not be equivalent to either (a_1P, a_2P) or (a_3P, a_4P), since

$$\begin{aligned} &\det\begin{pmatrix} a_1 & a_2 \\ a_3+\rho x x_2 & a_4-\rho x x_1 \end{pmatrix} \\ =&\det\begin{pmatrix} a_1 & a_2 \\ a_3+k\rho a_1 & a_4+k\rho a_2 \end{pmatrix} \\ =&\det\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \\ \neq& 0 \mod p \end{aligned}$$

and

$$\begin{aligned} &\det\begin{pmatrix} a_3+\rho x x_2 & a_4-\rho x x_1 \\ a_3 & a_4 \end{pmatrix} \\ =&\det\begin{pmatrix} a_3+k\rho a_1 & a_4+k\rho a_2 \\ a_3 & a_4 \end{pmatrix} \\ =&k\rho\det\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \\ \neq& 0 \mod p. \end{aligned}$$

If $(xx_2P, -xx_1P)$ is equivalent to (a_3P, a_4P), the proof is similar as above.

ii. Case $l \geq 3$

Similarly, we give our non-adaptive chosen message attack as follows:

1. $\mathcal{A}$ runs **FindKernel** to get $(xx_2P, -xx_1P, \mathbf{0}, \cdots, \mathbf{0}) \in (\mathbb{G}_1^*)^\ell \bigcap \ker(\varphi)$ and the signature (Z_1, V_1, Y_1, Y_1') for $(P, P, P, \cdots, P)$.
2. $\mathcal{A}$ finds $\rho \in \{1, 2, 3\}$ such that $P + \rho x x_2 P \neq \mathbf{0}$ and $P - \rho x x_1 P \neq \mathbf{0}$.
3. $\mathcal{A}$ outputs $M = (P + \rho x x_2 P, P - \rho x x_1 P, P, \cdots, P)$ and the corresponding signature $\sigma = (Z_1, V_1, Y_1, Y_1')$.

It is easy to check that the attack can be completed in polynomial time, $M \in (\mathbb{G}_2^*)^\ell$ and σ is indeed a valid signature on M. It remains to show $[M]_{\mathcal{R}}$ has not been queried, which can be concluded from the fact that

- $(P+\rho x x_2 P, P-\rho x x_1 P, P, \cdots, P)$ is not equivalent to $(P, P, P, \cdots, P)$, since $\rho x x_1$ and $\rho x x_2$ are not 0;
- $(P+\rho x x_2 P, P-\rho x x_1 P, P, \cdots, P)$ is not equivalent to $(2P, P, P, \cdots, P)$, since $-\rho x x_1$ is not 0;
- $(P+\rho x x_2 P, P-\rho x x_1 P, P, \cdots, P)$ is not equivalent to $(P, 2P, P, \cdots, P)$, since $\rho x x_2$ is not 0.

4.4 The Universal Forgery Attack against the Scheme

To commit a universal forgery attack, a natural idea is as follows. The adversary $\mathcal{A}$ runs **FindKernel** first to find a nontrivial K in $\ker(\varphi)$ and then runs the following **Forge** procedure to forge the valid signature on any given message M.

1. $\mathcal{A}$ first finds $\rho \in \{1, 2, 3\}$ such that $M - \rho K \in (\mathbb{G}_1^*)^\ell$.

2. $\mathcal{A}$ then makes a signing query with $M - \rho K$ and gets the signature $\sigma = (Z, V, Y, Y')$.
3. $\mathcal{A}$ outputs σ as the signature on M.

However, to avoid that the equivalence class of M has been queried, a little more attention should be paid. First notice that

Lemma 5. *If $M \notin \ker(\varphi)$, then M can not be equivalent to $M + K$ for any nontrivial $K \in \ker(\varphi)$.*

Proof. For contradiction, if M is equivalent to $M + K$ for some nontrivial $K \in \ker(\varphi)$, then it can be easily concluded that $M \in \ker(\varphi)$.

Then we can show that

Theorem 2. *The Hanser-Slamanig SPS-EQ scheme is universally forgeable under the adaptive chosen message attack. Moreover,*

- *If $\ell = 2$, three chosen message queries is needed;*
- *If $\ell \geq 3$, four chosen message queries is needed.*

Proof. We prove the theorem for two cases respectively.

i. Case $\ell = 2$

We give our universal forgery attack as follows:

1. $\mathcal{A}$ receives **pk** and has access to a signing oracle.
2. Given M, if $\sigma = (\mathbf{0}, \mathbf{0}, P, P')$ is a valid signature on M, then $\mathcal{A}$ outputs σ as the signature on M.
3. Otherwise, $M \notin \ker(\varphi)$. If M is equivalent to (P, P) or $(P, 2P)$, then $\mathcal{A}$ chooses the invertible matrix $\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$ to be $\begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}$, otherwise, $\mathcal{A}$ chooses the invertible matrix $\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$ to be $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$.
4. $\mathcal{A}$ runs **FindKernel** to get a nontrivial $K \in \ker(\varphi)$.
5. $\mathcal{A}$ runs the **Forge** procedure to find a valid signature on M.

Notice that if M is equivalent to (P, P) or $(P, 2P)$, then M must be equivalent to neither $(P, -P)$ nor $(-P, 2P)$ since the order p of $\mathbb{G}_1$ is greater than 3. Together with Lemma 5, it can shown that $[M]_{\mathcal{R}}$ has not been queried.

ii. Case $\ell \geq 3$

We give our universal forgery attack as follows:

1. $\mathcal{A}$ receives **pk** and has access to a signing oracle.
2. Given M, if $\sigma = (\mathbf{0}, \mathbf{0}, P, P')$ is a valid signature on M, then $\mathcal{A}$ outputs σ as the signature on M.

3. Otherwise, we know that $M \notin \ker(\varphi)$. If M is equivalent to $(P, P, P, \cdots, P)$, or $(2P, P, P, \cdots, P)$, or $(P, 2P, P, \cdots, P)$, $\mathcal{A}$ runs the **FindKernel** algorithm with querying messages $(P, -P, P, \cdots, P)$, $(2P, -P, P, \cdots, P)$, and $(P, -2P, P, \cdots, P)$ to get $K = (Z_1 - Z_3, Z_1 - Z_2, \mathbf{0}, \cdots, \mathbf{0}) \in \ker(\varphi)$.
4. Otherwise, $\mathcal{A}$ runs **FindKernel** as before to get $K \in \ker(\varphi)$.
5. $\mathcal{A}$ runs the **Forge** procedure to find a valid signature.

Note that if the message M is equivalent to $(P, P, P, \cdots, P)$, or $(2P, P, P, \cdots, P)$, or $(P, 2P, P, \cdots, P)$, it must be equivalent to neither $(P, -P, P, \cdots, P)$, nor $(2P, -P, P, \cdots, P)$, nor $(P, -2P, P, \cdots, P)$. Together with Lemma 5, it can shown that $[M]_{\mathcal{R}}$ has not been queried.

For both of the two attacks, it is easy to check the correctness, the complexity.

4.5 Interesting Observations

By Lemma 1, we know that the signature is not only valid for the original message M, but also valid for any other message in another equivalent class $M + \ker(\varphi) \in \mathbb{G}_1^\ell / \ker(\varphi)$. Interestingly, we can conclude that

Proposition 1. *For any $M \notin \ker(\varphi)$,*

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

Proof. Recall that

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

Assume that $M_i = \alpha_i P$ where $\alpha_i \in \mathbb{Z}_p$, we know that $\sum_{i=1}^\ell x_i M_i = \mathbf{0}$ if and only if $\sum_{i=1}^\ell x_i \alpha_i = 0 \mod p$. Hence $|\ker(\varphi)| = p^{\ell-1}$. Notice that φ is a group homomorphism, so we have

$$|\mathbb{G}_1^\ell / \ker(\varphi)| = p.$$

On the other hand, since $M \notin \ker(\varphi)$, then for any $i, j \in \mathbb{Z}_p$, $i \neq j$, iM and jM fall into different classes in $\mathbb{G}_1^\ell / \ker(\varphi)$. Therefore, $iM + \ker(\varphi)$'s $(i \in \mathbb{Z}_p)$ are exactly the p different classes in $\mathbb{G}_1^\ell / \ker(\varphi)$, which yields the proposition.

By the proposition, given any message-signature pair (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 $M' \in \rho M + \ker(\varphi)$. What we need do is computing the signature on ρM with the algorithm $\mathbf{ChgRep}_{\mathcal{R}}(M, \sigma, \rho, \mathbf{pk})$, and then outputting it.

Another discussion is about the leakage of the private keys. Although the private keys consist of $x_1, x_2, \cdots, x_\ell$, the scheme will be insecure when just x_i and x_j are leaked since from any two of $x_1, x_2, \cdots, x_\ell$ we can get a nontrivial element in $\ker(\varphi)$.

5 Conclusion

In this paper, we show that the Hanser-Slamanig SPS-EQ scheme is existentially forgeable under a non-adaptive chosen message attack and is universally forgeable under an adaptive chosen message attack. More precisely, we can produce a valid existential forgery with just 2 (*resp.* 3) non-adaptive chosen-message queries for $l = 2$ (*resp.* $l \geq 3$). Under the adaptive chosen message attack, we can forge the valid signature for any given message with just 3 (*resp.* 4) chosen-message queries for $l = 2$ (*resp.* $l \geq 3$). Both of the attacks need fewer queries, which give a better description of the scheme's security.

Acknowledgments. We very thank the anonymous referees for their valuable suggestions on how to improve the presentation of this paper.

References

1. David, B., Kohlweiss, M., Nishimaki, R., and Ohkubo, M.: Tagged one-time signatures: Tight security and optimal tag size. In Proc. of PKC 2013, volume 7778 of LNCS, pp. 312-331, Springer (2013)
2. Abe, M., Fuchsbauer, G., Groth, J., Haralambiev, K., and Ohkubo, M.: Structure-Preserving Signatures and Commitments to Group Elements. In Proc. of CRYPTO 2010, volume 6223 of LNCS, pp. 209-236, Springer (2010)
3. Attrapadung, N., Libert, B., and Peters, T.: Efficient completely context-hiding quotable and linearly homomorphic signatures. In Proc. of PKC 2013, volume 7778 of LNCS, pp. 386-404, Springer (2013)
4. Barthe, G., Fagerholm, E., Fiore, D., Scedrov, A., Schmidt, B., Tibouchi, M.: Strongly-Optimal Structure Preserving Signatures from Type II Pairings: Synthesis and Lower Bounds. In Proc. of PKC 2015, volume 9020 of LNCS, pp. 355-376, Springer (2015)
5. Ballard, L., Green, M., Medeiros, B., and Monrose, F.: Correlation- Resistant Storage via Keyword-Searchable Encryption. IACR Cryptology ePrint Archive 2005: 417 (2005) (http://eprint.iacr.org/2005/417)
6. Fuchsbauer, G.: Breaking Existential Unforgeability of a Signature Scheme from Asiacrypt 2014. IACR Cryptology ePrint Archive 2014: 892 (2014) (http://eprint.iacr.org/2014/892)
7. Fuchsbauer, G., Hanser, C., Slamanig, D.: EUF-CMA-Secure structure-preserving signatures on equivalence classes. IACR Cryptology ePrint Archive 2014: 944 (2014) (http://eprint.iacr.org/2014/944)
8. Fuchsbauer, G., Vergnaud, D.: Fair blind signatures without random oracles. In Proc. of AFRICACRYPT 2010, volume 6055 of LNCS, pp. 16-33, Springer (2010)
9. Goldwasser, S., Micali, S., Rivest, R.: A digital signature scheme secure against adaptive chosen-message attacks. SIAM J. Computing, 17(2):281-308, 1988.
10. Hanser, C., Slamanig, D.: Structure-preserving signatures on equivalence classes and their application to anonymous credentials. In Proc. of ASIACRYPT 2014, volume 8874 of LNCS, pp. 491-511, Springer (2014)
11. Hanser, C., Slamanig, D.: Structure-preserving signatures on equivalence classes and their application to anonymous credentials. Revised version, IACR Cryptology ePrint Archive 2014: 705 (2014) (http://eprint.iacr.org/2014/705)

12. Hofheinz, D., Jager, T.: Tightly secure signatures and public-key encryption. In Proc. of CRYPTO 2012, volume 7417 of LNCS, pp. 590-607, Springer (2012)
13. Libert, B., Peters, T., Joye, M., Yung, M.: Linearly homomorphic structure-preserving signatures and their applications. In Proc. of CRYPTO 2013, volume 8043 of LNCS, pp. 289-307, Springer (2013)
14. Libert, B., Peters, T., and Yung, M.: Group signatures with almost-for-free revocation. In Proc. of CRYPTO 2012, volume 7417 of LNCS, pp. 571-589, Springer (2012)