Breaking Existential Unforgeability of a Signature Scheme from Asiacrypt 2014

Georg Fuchsbauer*

IST Austria
georg.fuchsbauer@ist.ac.at

Abstract

We show how to compute an existential forgery after querying 4 signatures on chosen messages for a signature scheme presented at Asiacrypt 2014.

1 Introduction

At Asiacrypt 2014 Hanser and Slamanig [HS14] present a new signature primitive they call *structure-preserving signatures on equivalence classes* (SPS-EC). They show how in combination with a type of commitment scheme it yields a novel approach to constructing attribute-based credential systems [Cha85]. Whereas previous schemes used zero-knowledge proofs of knowledge of signatures in order to achieve anonymity, their scheme avoids this by allowing randomization of the signed messages.

The scheme is defined over a bilinear group $\mathsf{BG} := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P, \hat{P})$, that is, a tuple where $\mathbb{G}_1, \mathbb{G}_2$, and $\mathbb{G}_T$ are groups of prime order p generated by $P, \hat{P}$ and $e(P, \hat{P})$, respectively, and e is a bilinear map $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. Signatures defined over bilinear groups are called *structure-preserving* [AFG+10] if public verification keys, signatures and messages are elements of the source groups $\mathbb{G}_1, \mathbb{G}_2$ and signature validity is checked by verifying relations of the form $\prod_i \prod_j e(A_i, \hat{B}_j)^{c_{i,j}} = 1$.

In an SPS-EC scheme messages are length-ℓ vectors M of elements from $\mathbb{G}_1^*$ (i.e. excluding the neutral element) and from a signature on $(M_1, \ldots, M_\ell)$ anyone can derive a signature on $\rho \cdot M := (\rho M_1, \ldots, \rho M_\ell)$. We can partition the message space $(\mathbb{G}_1^*)^\ell$ into classes where two messages M, N are in the same class if $M = \rho \cdot N$ for some $\rho \in \mathbb{Z}_p^*$. Since signatures on one message can be transformed to signatures on any other message in the same class, signatures can be viewed as signing classes of messages rather than single messages.

Given its new functionality, the standard unforgeability notion for signatures cannot hold for the new primitive; however, given signatures for messages from various classes, it should still be hard to compute one for a new class. Existential unforgeability under chosen-message attacks (EUF-CMA) for SPS-EC is thus defined as follows in [HS14]: no adversary, after being given the verification key and an oracle it can query for signatures on messages of its choice, can produce a valid message/signature pair so that the class of the message is different from that of all queried messages.

Hanser and Slamanig [HS14] present an instantiation of their primitive where signatures consist of only 4 group elements and keys of $\ell + 1$ group elements. In the full version they give a proof that their scheme satisfies EUF-CMA for SPS-EC in the generic group model [Sho97]. This proof is however flawed, as we show an attack that breaks the notion. In order to compute an existential forgery, it suffices to make 4 chosen-message queries.

*Supported by the European Research Council, ERC Starting Grant (259668-PSPC)

2 Preliminaries

2.1 Bilinear Groups

An asymmetric bilinear group is a tuple $\mathsf{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, e, P, \hat{P})$, where p is a prime, $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ are groups of order p, and P and $\hat{P}$ generate $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. Moreover, e is a bilinear map $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ such that $e(P, \hat{P})$ generates $\mathbb{G}_T$. We assume an algorithm BGGen, which takes as input a security parameter λ in unary and outputs a bilinear group $(p, \mathbb{G}_1, \mathbb{G}_2, e, P, \hat{P})$ where the bit length of p is λ and there are no efficiently computable homomorphisms from $\mathbb{G}_1$ to $\mathbb{G}_2$ and vice versa.

We denote the groups $\mathbb{G}_1$ and $\mathbb{G}_2$ additively (and $\mathbb{G}_T$ multiplicatively) and elements from $\mathbb{G}_2$ with hats, such as $\hat{X}$. Moreover, we define $\mathbb{G}_i^* := \mathbb{G}_i \setminus \{0\}$ for $i = 1, 2$.

2.2 Structure-Preserving Signatures on Equivalence Classes

Definition 1 (The equivalence class $\mathcal{R}$)**.** *Let $\ell > 1$ and $\mathbb{G}_1$ be a group of prime order p. We define the following equivalence relation on length-ℓ vectors of non-trivial group elements:*

$$\mathcal{R} := \{(M, N) \in (\mathbb{G}_1^*)^\ell \times (\mathbb{G}_1^*)^\ell \mid \exists\, s \in \mathbb{Z}_p^* : N = s \cdot M\} \ .$$

For an element $M \in (\mathbb{G}_1^*)^\ell$ its equivalence class $[M]_\mathcal{R}$ is defined as $[M]_\mathcal{R} := \{N \in (\mathbb{G}_1^*)^\ell \mid (M, N) \in \mathcal{R}\}$.

Definition 2 (Structure-preserving signature scheme for equivalence relation $\mathcal{R}$ [HS14])**.** *An SPS-EQ-$\mathcal{R}$ scheme consists of the following PT algorithms:*

- $\mathsf{BGGen}_\mathcal{R}(1^\lambda)$*, on input security parameter λ, outputs a bilinear group* BG*. (*BG *will be an (implicit) input to all other algorithms.)*
- $\mathsf{KeyGen}_\mathcal{R}(\mathsf{BG}, \ell)$*, on input a bilinear group* BG *and a vector length $\ell > 1$, outputs a signing and a verification key* $(\mathsf{sk}, \mathsf{pk})$*.*
- $\mathsf{Sign}_\mathcal{R}(\mathsf{sk}, M)$*, on input a signing key* sk *and a vector $M \in (\mathbb{G}_1^*)^\ell$, outputs a signature σ for the equivalence class $[M]_\mathcal{R}$.*
- $\mathsf{ChgRep}_\mathcal{R}(\mathsf{pk}, M, \sigma, \rho)$*, on input a public key* pk*, a vector $M \in (\mathbb{G}_1^*)^\ell$, a signature on $[M]_\mathcal{R}$ for M, and a scalar ρ, returns a signature on $[M]_\mathcal{R}$ but for representative $M' = \rho \cdot M$.*
- $\mathsf{Verify}_\mathcal{R}(\mathsf{pk}, M, \sigma)$*, on input a public key* pk*, a representative M and a signature σ, outputs 1 for acceptance and 0 for rejection.*

In this work we are not concerned with changes of representatives; we only presented ChgRep for completeness. Unforgeability of such a scheme is defined as follows.

Definition 3 (EUF-CMA)**.** *An SPS-EQ-$\mathcal{R}$ scheme* $(\mathsf{BGGen}_\mathcal{R}, \mathsf{KeyGen}_\mathcal{R}, \mathsf{Sign}_\mathcal{R}, \mathsf{ChgRep}_\mathcal{R}, \mathsf{Verify}_\mathcal{R})$ *with message space $(G_1^*)^\ell$ is* existentially unforgeable under adaptively chosen-message attacks *if for all probabilistic polynomial-time adversaries $\mathcal{A}$ having access to a signing oracle* $\mathsf{Sign}_\mathcal{R}(\mathsf{sk}, \cdot)$*, we have*

$$\Pr\left[\begin{array}{ll} \mathsf{BG} \leftarrow \mathsf{BGGen}_\mathcal{R}(1^\lambda);\ (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}_\mathcal{R}(\mathsf{BG}, \ell); & : \quad [M^*]_\mathcal{R} \neq [M]_\mathcal{R}\ \forall M \in Q \wedge \\ (M^*, \sigma^*) \leftarrow \mathcal{A}^{\mathsf{Sign}_\mathcal{R}(\mathsf{sk}, \cdot)}(\mathsf{pk}) & \quad\ \mathsf{Verify}_\mathcal{R}(\mathsf{pk}, M^*, \sigma^*) = 1 \end{array}\right] = \mathsf{negl}(\lambda) \ ,$$

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

Another property, *class hiding*, is also defined for SPS-EQ-$\mathcal{R}$ schemes in [HS14], but not considered here.

2.3 The Construction from [HS14]

The scheme proposed in [HS14] is defined as follows.[1]

Scheme 1. $\mathsf{BGGen}_{\mathcal{R}}(1^\lambda)$*: Return* $\mathsf{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, e, P, \hat{P}) \leftarrow \mathsf{BGGen}(1^\lambda)$.

$\mathsf{KeyGen}_{\mathcal{R}}(\mathsf{BG}, \ell)$ *(for* $\ell > 1$*): Choose* $x \leftarrow \mathbb{Z}_p^*, (x_i)_{i=1}^\ell \leftarrow (\mathbb{Z}_p^*)^\ell$ *uniformly at random, set* $\hat{X} := x\hat{P}$*,* $\hat{X}_i := x_i x\hat{P}$*, for* $i = 1, \ldots, \ell$*, and output* $\mathsf{sk} := (x, (x_i)_{i=1}^\ell)$ *and* $\mathsf{pk} := (\hat{X}, (\hat{X}_i)_{i=1}^\ell)$.

$\mathsf{Sign}_{\mathcal{R}}(\mathsf{sk}, M)$*: On input* $\mathsf{sk} = (x, (x_i)_{i=1}^\ell) \in (\mathbb{Z}_p^*)^{\ell+1}$ *and* $M = (M_i)_{i=1}^\ell \in (\mathbb{G}_1^*)^\ell$*, choose* $y \leftarrow \mathbb{Z}_p^*$ *uniformly at random and output*

$$Z := x\textstyle\sum_{i=1}^\ell x_i M_i \qquad V := y\sum_{i=1}^\ell x_i M_i \qquad Y := yP \qquad \hat{Y} := y\hat{P}$$

$\mathsf{Verify}_{\mathcal{R}}(\mathsf{pk}, M, \sigma)$*: Given a public key* $\mathsf{pk} = (\hat{X}, (\hat{X}_i)_{i=1}^\ell) \in (\mathbb{G}_2^*)^{\ell+1}$*, a vector* $M = (M_i)_{i=1}^\ell \in (\mathbb{G}_1^*)^\ell$ *representing equivalence class* $[M]_{\mathcal{R}}$*, and a signature* $\sigma = (Z, V, Y, \hat{Y}) \in \mathbb{G}_1^3 \times \mathbb{G}_2$*, return 1 if the following equations hold, and 0 otherwise:*

$$\textstyle\prod_{i=1}^\ell e(M_i, \hat{X}_i) = e(Z, \hat{P}) \qquad e(Z, \hat{Y}) = e(V, \hat{X}) \qquad e(P, \hat{Y}) = e(Y, \hat{P})$$

3 The Attack

Consider the following (deterministic) polynomial-time adversary $\mathcal{A}$ against EUF-CMA (Definition 3) of Scheme 1 for $\ell = 2$:

0. $\mathcal{A}$ receives $\mathsf{pk} = (\hat{X}, \hat{X}_1, \hat{X}_2)$ and has access to a signing oracle $\mathsf{Sign}_{\mathcal{R}}(\mathsf{sk}, \cdot)$.
1. $\mathcal{A}$ makes a signing query (P, P) and receives $(Z_1, V_1, Y_1, \hat{Y}_1)$.
2. $\mathcal{A}$ makes a signing query (Z_1, P) and receives $(Z_2, V_2, Y_2, \hat{Y}_2)$.
3. $\mathcal{A}$ makes a signing query (P, Z_1) and receives $(Z_3, V_3, Y_3, \hat{Y}_3)$.
4. $\mathcal{A}$ makes a signing query (Z_1, Z_2) and receives $(Z_4, V_4, Y_4, \hat{Y}_4)$.
5. $\mathcal{A}$ outputs $(Z_4, V_4, Y_4, \hat{Y}_4)$ as a forgery for the equivalence class represented by (Z_3, Z_1).

Proposition 1. *Adversary* $\mathcal{A}$ *wins the EUF-CMA game for Scheme 1 with overwhelming probability over the random choices of the challenger.*

Proof. We analyze the attack. Let $\mathsf{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, e, P, \hat{P})$ be the chosen bilinear group, $(x, x_1, x_2) \in (\mathbb{Z}_p^*)^3$ be the challenger's secret key and let $y_i \in \mathbb{Z}_p^*$ be the randomness chosen by the challenger when answering the i-th signing query, for $i \in [1, 4]$. Then we have:

$$\begin{array}{llll}
Z_1 := (xx_1 + xx_2)P & V_1 := (y_1x_1 + y_1x_2)P & Y_1 := y_1P & \hat{Y}_1 := y_1\hat{P} \\
Z_2 := (x^2x_1^2 + x^2x_1x_2 + xx_2)P & V_2 := (y_2xx_1^2 + y_2xx_1x_2 + y_2x_2)P & Y_2 := y_2P & \hat{Y}_2 := y_2\hat{P} \\
Z_3 := (xx_1 + x^2x_1x_2 + x^2x_2^2)P & V_3 := (y_3x_1 + y_3xx_1x_2 + y_3xx_2^2)P & Y_3 := y_3P & \hat{Y}_3 := y_3\hat{P} \\
Z_4 := (x^2x_1^2 + x^2x_1x_2 + x^3x_1^2x_2 + x^3x_1x_2^2 + x^2x_2^2)P & & & \\
V_4 := (y_4xx_1^2 + y_4xx_1x_2 + y_4x^2x_1^2x_2 + y_4x^2x_1x_2^2 + y_4xx_2^2)P & & Y_4 := y_4P & \hat{Y}_4 := y_4\hat{P}
\end{array} \quad (1)$$

[1] We denote signatures by $(Z, V, Y, \hat{Y})$ and keys by $\hat{X}, \hat{X}_i$ instead of (Z_1, Z_2, Y, Y') and X', X_i', respectively, in [HS14]

Let us first show that the first winning condition in Definition 3 is satisfied, that is, $[(Z_3, Z_1)]_{\mathcal{R}} \neq [(M_1, M_2)]_{\mathcal{R}}$ for all (M_1, M_2) queried to the signing oracle. Every equivalence class $[(M_1, M_2)]_{\mathcal{R}}$ can be uniquely described by an element from $\mathbb{Z}_p^*$, namely

$$r_{[(M_1,M_2)]_{\mathcal{R}}} := (\log_P M_1 / \log_P M_2) \bmod p$$

(where $\log_P M_i$ for $M_i \in \mathbb{G}_1^*$ is defined as the value $m_i \in \mathbb{Z}_p^*$ such that $M_i = m_i P$).

We thus have to show that $r_{[(Z_3,Z_1)]_{\mathcal{R}}} \notin \{r_{[(P,P)]_{\mathcal{R}}}, r_{[(Z_1,P)]_{\mathcal{R}}}, r_{[(P,Z_1)]_{\mathcal{R}}}, r_{[(Z_1,Z_2)]_{\mathcal{R}}}\}$. We have:

$$r_{[(P,P)]_{\mathcal{R}}} = 1 =: p_1 \qquad r_{[(Z_1,P)]_{\mathcal{R}}} = xx_1 + xx_2 =: p_2 \qquad r_{[(P,Z_1)]_{\mathcal{R}}} = 1/(xx_1 + xx_2) =: p_3$$
$$r_{[(Z_1,Z_2)]_{\mathcal{R}}} = (xx_1 + xx_2)/(x^2x_1^2 + x^2x_1x_2 + xx_2) \qquad r_{[(Z_3,Z_1)]_{\mathcal{R}}} = (xx_1 + x^2x_1x_2 + x^2x_2^2)/(xx_1 + xx_2)$$

and since $x \neq 0$:

$$r_{[(Z_1,Z_2)]_{\mathcal{R}}} = (x_1 + x_2)/(xx_1^2 + xx_1x_2 + x_2) =: p_4 \qquad r_{[(Z_3,Z_1)]_{\mathcal{R}}} = (x_1 + xx_1x_2 + xx_2^2)/(x_1 + x_2) =: p^*$$

We first show that $p^* \neq p_i$ for all $i \in [1, 4]$ when interpreted as polynomials in $\mathbb{Z}_p[x, x_1, x_2]$. (We multiply each equation with the denominators of both sides.)

1. $p_1 \neq p^*$ since $x_1 + x_2 \neq x_1 + xx_1x_2 + xx_2^2$.
2. $p_2 \neq p^*$ since $(xx_1 + xx_2)(x_1 + x_2) = xx_1^2 + 2xx_1x_2 + xx_2^2 \neq x_1 + xx_1x_2 + xx_2^2$.
3. $p_3 \neq p^*$ since $x_1 + x_2 \neq xx_1^2 + x^2x_1^2x_2 + 2x^2x_1x_2^2 + xx_1x_2 + x^2x_2^3 = (xx_1 + xx_2)(x_1 + xx_1x_2 + xx_2^2)$.
4. $p_4 \neq p^*$ since $\begin{aligned}(x_1 + x_2)^2 &= x_1^2 + 2x_1x_2 + x_2^2 \\ &\neq xx_1^3 + x^2x_1^3x_2 + 2x^2x_1^2x_2^2 + xx_1^2x_2 + x^2x_1x_2^3 + x_1x_2 + xx_1x_2^2 + xx_2^3 \\ &= (xx_1^2 + xx_1x_2 + x_2)(x_1 + xx_1x_2 + xx_2^2).\end{aligned}$

By the Schwartz-Zippel lemma [Sch80] it follows that for all $i \in [1, 4]$ the probability that $p^*(x, x_1, x_2) = p_i(x, x_1, x_2)$ for uniformly chosen $x, x_1, x_2 \leftarrow \mathbb{Z}_p^*$ is negligible. By the union bound we have that the probability that $\bigvee_{i=1}^4 \left[p^*(x, x_1, x_2) = p_i(x, x_1, x_2)\right]$ is also negligible, and thus with overwhelming probability over the challenger's random choices the class $[(Z_3, Z_1)]_{\mathcal{R}}$ is different from those queried to the signing oracle.

It remains to show that the second winning condition in Definition 3 is also satisfied, that is, $(Z_4, V_4, Y_4, \hat{Y}_4)$ is valid for (Z_3, Z_1). A signature $(Z^*, V^*, Y^*, \hat{Y}^*)$ on (Z_3, Z_1), using randomness y^*, is defined as

$$\begin{aligned} Z^* &:= (x^2x_1^2 + x^3x_1^2x_2 + x^3x_1x_2^2 + x^2x_1x_2 + x^2x_2^2)P \\ V^* &:= (y^*xx_1^2 + y^*x^2x_1^2x_2 + y^*x^2x_1x_2^2 + y^*xx_1x_2 + y^*xx_2^2)P \end{aligned} \qquad Y^* := y^*P \qquad \hat{Y}^* := y^*\hat{P}$$

Thus, $(Z_4, V_4, Y_4, \hat{Y}_4)$ from Equation (1) is a signature on (Z_3, Z_1) using randomness y_4. Since we showed that with overwhelming probability (over the choice of sk by the challenger) $[(Z_3, Z_1)]_{\mathcal{R}}$ is different from all queried classes, this means that $\mathcal{A}$ outputs a valid forgery. □

We conclude by noting that excluding the class $[(P, P)]_{\mathcal{R}}$ from the message space would not make the scheme secure, as the following attack, where a and b are arbitrarily fixed elements from $\mathbb{Z}_p^*$, shows.

0. $\mathcal{A}$ receives $\mathsf{pk} = (\hat{X}, \hat{X}_1, \hat{X}_2)$ and has access to a signing oracle $\mathsf{Sign}_{\mathcal{R}}(\mathsf{sk}, \cdot)$.
1. $\mathcal{A}$ makes a signing query (aP, bP) and receives $(Z_1, V_1, Y_1, \hat{Y}_1)$.
2. $\mathcal{A}$ makes a signing query (Z_1, aP) and receives $(Z_2, V_2, Y_2, \hat{Y}_2)$.

3. $\mathcal{A}$ makes a signing query (aP, Z_1) and receives $(Z_3, V_3, Y_3, \hat{Y}_3)$.
4. $\mathcal{A}$ makes a signing query (Z_1, Z_2) and receives $(Z_4, V_4, Y_4, \hat{Y}_4)$.
5. $\mathcal{A}$ makes a signing query (bP, aP) and receives $(Z_5, V_5, Y_5, \hat{Y}_5)$.
6. $\mathcal{A}$ outputs $(Z_4, V_4, Y_4, \hat{Y}_4)$ as a forgery for the equivalence class represented by (Z_3, Z_5).

As above, let $(x, x_1, x_2) \in (\mathbb{Z}_p^*)^3$ be the challenger's secret key and let $y_i \in \mathbb{Z}_p^*$ be the randomness chosen for the i-th signing query. Then we have:

$$
\begin{array}{llll}
Z_1 := (xx_1a + bxx_2b)P & V_1 := (y_1x_1a + y_1x_2b)P & Y_1 := y_1P & \hat{Y}_1 := y_1\hat{P} \\
Z_2 := (x^2x_1^2a + x^2x_1x_2b + xx_2a)P & V_2 := (y_2xx_1^2a + y_2xx_1x_2b + y_2x_2a)P & Y_2 := y_2P & \hat{Y}_2 := y_2\hat{P} \\
Z_3 := (xx_1a + x^2x_1x_2a + x^2x_2^2b)P & V_3 := (y_3x_1a + y_3xx_1x_2a + y_3xx_2^2b)P & Y_3 := y_3P & \hat{Y}_3 := y_3\hat{P} \\
\multicolumn{2}{l}{\begin{array}{l} Z_4 := (x^2x_1^2a + x^2x_1x_2b + x^3x_1^2x_2a + x^3x_1x_2^2b + x^2x_2^2a)P \\ V_4 := (y_4xx_1^2a + y_4xx_1x_2b + y_4x^2x_1^2x_2a + y_4x^2x_1x_2^2b + y_4xx_2^2a)P \end{array}} & Y_4 := y_4P & \hat{Y}_4 := y_4\hat{P} \\
Z_5 := (xx_1b + xx_2a)P & V_5 := (y_5x_1b + y_5x_2a)P & Y_5 := y_5P & \hat{Y}_5 := y_5\hat{P}
\end{array}
$$

The attack is successful, since $(Z_4, V_4, Y_4, \hat{Y}_4)$ is also a signature on (Z_3, Z_5) with randomness y_4.

References

[AFG+10] Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Structure-preserving signatures and commitments to group elements. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 209–236. Springer, August 2010.

[Cha85] David Chaum. Security without identification: Transaction systems to make big brother obsolete. *Commun. ACM*, 28(10):1030–1044, 1985.

[HS14] Christian Hanser and Daniel Slamanig. Structure-preserving signatures on equivalence classes and their application to anonymous credentials. In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT 2014*, volume 8874 of *LNCS*, pages ??–?? Springer, 2014. Available at `http://eprint.iacr.org/2014/705`.

[Sch80] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4), 1980.

[Sho97] Victor Shoup. Lower bounds for discrete logarithms and related problems. In Walter Fumy, editor, *EUROCRYPT'97*, volume 1233 of *LNCS*, pages 256–266. Springer, May 1997.