The Security of the Hanser-Slamanig Signature Scheme Revisited

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 structure-preserving signatures and prove its EUF-CMA security. Very recently, Fuchsbauer gave a very surprising attack to point out their claim is flawed by showing how to generate a valid existential forgery with overwhelming probability with 4 chosen-message queries for $l = 2$. However, we go further in this paper to show that the Hanser-Slamanig signature scheme is not unforgeable under the adaptive chosen message attack. We present a deterministic polynomial-time chosen-message attack which can forge the valid signature for any message with 3 (*resp.* 4) chosen-message queries for $l = 2$ (*resp.* $l \geq 3$).

Keywords: Structure-preserving signature, chosen-message attack.

1 Introduction

At Asiacrypt 2014, Hanser and Slamanig [2] presented a structure-preserving signatures on equivalence classes (SPS-EC). Instead of using zero-knowledge proofs of knowledge of signatures as before, the Hanser-Slamanig signature scheme allows to randomize the signed message in particular ways to achieve anonymity. They also showed that their scheme is EUF-CMA secure in the generic group model for SXDH groups.

However, very recently, Fuchsbauer [1] pointed out their claim is flawed by showing how to generate a valid existential forgery with overwhelming probability with 4 chosen-message queries for $l = 2$. Hence the Hanser-Slamanig signature scheme is not EUF-CMA secure.

In this paper, we show that the Hanser-Slamanig signature scheme can not even be unforgeable under the adaptive chosen message attack. More precisely, we present

a deterministic polynomial-time chosen-message attack which can forge the valid signature for any message. The new attack appears more simple and never fails. To forge a valid signature, we just need 3 chosen-message queries for $l = 2$. We also consider the general case when $l \geq 3$ and show that 4 chosen-message queries is needed to forge the signature of any message. In fact, if we take 2 (*resp.* 3) non-adaptive chosen-message queries for $l = 2$ (*resp.* $l \geq 3$) as precomputation, we can always forge any signature by only 1 additional chosen-message query. Moreover, the new attack reveals the weakness of the Hanser-Slamanig signature scheme obviously and seems natural eanough whereas Fuchsbauer's attack seems too clever so that one may wonder how he gets it.

2 The Hanser-Slamanig Signature Scheme

Before giving the description of the signature scheme, we first define the equivalence relation $\mathcal{R}$ as used in [2]:

$$\mathcal{R} = \{(M, N) \in (\mathbb{G}_1^*)^l \times (\mathbb{G}_1^*)^l : \exists s \in \mathbb{Z}_p^* \text{ s.t. } N = sM\}.$$

Then we denote $[M]_{\mathcal{R}}$ all the elements in $(\mathbb{G}_1^*)^l$ equivalent to $M \in (\mathbb{G}_1^*)^l$ with relation $\mathcal{R}$.

As in [1], we just describe the Hanser-Slamanig signature scheme as below but omit its **ChgRep** step.

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

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

  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 $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, P and P' generate $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively.

- $\mathbf{KeyGen}_{\mathcal{R}}(\mathbf{BG}, l)$: Given a bilinear group description $\mathbf{BG}$ and vector length $l > 1$, choose $x \xleftarrow{R} \mathbb{Z}_p^*$ and $(x_i)_{i=1}^l \xleftarrow{R} (\mathbb{Z}_p^*)^l$, set the secret key as $\mathbf{sk} \leftarrow (x, (x_i)_{i=1}^l)$, compute the public key $\mathbf{pk} \leftarrow (X', (X_i')_{i=1}^l) = (xP', (x_i x P')_{i=1}^l)$ and output $(\mathbf{sk}, \mathbf{pk})$.

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

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

  Then, output $\sigma = (Z, V, Y, Y')$ as signature for the equivalence class $[M]_R$.

- **Verify**$_{\mathcal{R}}(M, \sigma, \mathbf{pk})$: Given a representative $M = (M_i)_{i=1}^l \in (\mathbb{G}_1^*)^l$ of equivalence class $[M]_{\mathcal{R}}$, a signature $\sigma = (Z, V, Y, Y')$ and public key $\mathbf{pk} = (X', (X'_i)_{i=1}^l$, check whether

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

and if this holds output true and false otherwise.

3 The Attack

3.1 Key Idea

Consider the following map:

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

We claim that

Lemma 1. *For any $(K_i)_{i=1}^l \in ker(\varphi)$, if $\sigma = (Z, V, Y, Y')$ is a valid signature of any message $(M_i)_{i=1}^l$, then it is also a valid signature of $(M_i + K_i)_{i=1}^l$*

Proof. Notice that the only condition we need check is $\prod_{i=1}^l e(M_i, X'_i) \stackrel{?}{=} e(Z, P)$. Assume $M_i = m_i P$ and $K_i = k_i P$. Since $(K_i)_{i=1}^l \in \ker(\varphi)$, we have $(\sum_{i=1}^l x_i k_i)P = \mathbf{0}$ which yields $\sum_{i=1}^l x_i k_i = 0 \bmod p$. Then we have

$$\begin{array}{rcl} \prod_{i=1}^l e(M_i + K_i, X'_i) = & e(P, P')^{\sum_{i=1}^l x x_i (m_i + k_i)} \\ = & e(P, P')^{\sum_{i=1}^l x x_i m_i + \sum_{i=1}^l x x_i k_i} \\ = & e(P, P')^{\sum_{i=1}^l x x_i m_i} \\ = & \prod_{i=1}^l e(M_i, X'_i), \end{array}$$

which finishes the proof. □

Hence if we find any non-trivial $(K_i)_{i=1}^l \in \ker(\varphi)$, we can forge the signature on any message $(M_i)_{i=1}^l$ by querying the signing oracle with $(M_i - K_i)_{i=1}^l$ and outputting the returned signature.

Next we will show the non-trivial $(K_i)_{i=1}^l$ can be obtained with 2 (*resp.* 3) chosen-message queries for $l = 2$ (*resp.* $l \geq 3$).

3.2 Case $l = 2$

Consider the following polynomial-time adversary $\mathcal{A}$ to obtain a nontrivial element in $\ker(\varphi)$:

1. $\mathcal{A}$ receives **pk** and has access to a signing oracle. $\mathcal{A}$ 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
$$\begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod p.$$
2. $\mathcal{A}$ makes a signing query with (a_1P, a_2P) and gets (Z_1, V_1, Y_1, Y_1').
3. $\mathcal{A}$ makes a signing query with (a_3P, a_4P) and gets (Z_2, V_2, Y_2, Y_2').
4. $\mathcal{A}$ outputs $((b_3Z_1 + b_4Z_2), -(b_1Z_1 + b_2Z_2))$.

We claim that

Proposition 1. $((b_3Z_1 + b_4Z_2), -(b_1Z_1 + b_2Z_2)) = (xx_2P, -xx_1P) \in ker(\varphi)\backslash(\boldsymbol{0}, \boldsymbol{0})$.

Proof. It suffices to prove $((b_3Z_1 + b_4Z_2), -(b_1Z_1 + b_2Z_2)) = (xx_2P, -xx_1P)$. Notice that
$$Z_1 = x(a_1x_1 + a_2x_2)P, Z_2 = x(a_3x_1 + a_4x_2)P.$$
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
$$\begin{aligned} b_1Z_1 + b_2Z_2 &= b_1x(a_1x_1 + a_2x_2)P + b_2x(a_3x_1 + a_4x_2)P \\ &= x((b_1a_1 + b_2a_3)x_1 + (b_1a_2 + b_2a_4)x_2)P \\ &= xx_1P. \end{aligned}$$
The proposition follows. □

Notice that any fixed a_1, a_2, a_3, a_4 can help the attack work well, which shows one can not make the scheme secure by excluding some classes from the message space.

Remark 1. *We would like to point out that by the attack in [1], one can also recover an nontrivial element in Ker(φ) with 4 chosen-message queries for $l = 2$.*

3.3 Case $l \geq 3$

We can also generalize the attack above for the case $l \geq 3$ by involving an invertible matrix. However, notice that $(xx_2P, -xx_1P, \mathbf{0}, \mathbf{0}, \cdots, \mathbf{0})$ is also a nontrivial element in the corresponding $\ker(\varphi)$. We have a more clever attack to obtain a nontrivial element in $\ker(\varphi)$.

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. $\mathcal{A}$ outputs $(Z_3 - Z_1, Z_1 - Z_2, \mathbf{0}, \cdots, \mathbf{0})$.

Proposition 2. $(Z_3 - Z_1, Z_1 - Z_2, \boldsymbol{0}, \cdots, \boldsymbol{0}) = (xx_2P, -xx_1P, \boldsymbol{0}, \cdots, \boldsymbol{0}) \in ker(\varphi) \backslash (\boldsymbol{0}, \cdots, \boldsymbol{0})$.

Proof. Notice that

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

Hence

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

The proposition follows. □

Notice that once the difference of two messages is $(P, \mathbf{0}, \cdots, \mathbf{0})$, we can recover xx_1P and so on. It seems hard to make the scheme secure by excluding some classes from the message space. What's more, by generalizing the attack in Subsection 3.2, we can also make the message queried seem random.

Remark 2. *We would like to point out that if we replace P with any other non-zero element in $\mathbb{G}_1$, the attacks still hold.*

4 Conclusion

We give a simple attack to forge signature on any message with fewer queries. However, the attack is still adaptive. In fact, we can get all the integer coefficient combination of the set $\{x^k x_{i_1} x_{2_2} \cdots x_{i_k} P | k = 1, 2, \cdots\}$, but by now we do not know how to use the fact to construct a non-adaptive chosen-message attack.

References

[1] Georg Fuchsbauer, Breaking Existential Unforgeability of a Signature Scheme from Asiacrypt 2014. Available at http://eprint.iacr.org/2014/892

[2] 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, Springer, 2014. Available at http://eprint.iacr.org/2014/705.