A short comment on the affine parts of SFLASH^{v3}

Willi Geiselmann and Rainer Steinwandt

IAKS, Arbeitsgruppe Systemsicherheit, Prof. Dr. Th. Beth
Fakultät für Informatik, Universität Karlsruhe,
Am Fasanengarten 5, 76 131 Karlsruhe, Germany

Abstract

In [3] SFLASH^{v3} is presented, which supersedes SFLASH^{v2}, one of the digital signature schemes in the NESSIE Portfolio of recommended cryptographic primitives [2]. We show that a known attack against the affine parts of SFLASH^{v1} and SFLASH^{v2} carries over immediately to the new version SFLASH^{v3}: The 861 bit representing the affine parts of the secret key can easily be derived from the public key alone.

1 Introduction

SFLASH^{v2} is one of the asymmetric signature algorithms that is part of the NESSIE Portfolio of recommended cryptographic primitives [2]. It emerged from an earlier version which is now referred to as SFLASH^{v1} and that has been cryptanalyzed successfully by Gilbert and Minier in [8]. Recently, a new version of SFLASH, called SFLASH^{v3}, has been proposed [3], and its authors "do no longer recommend SFLASH^{v2}."

As shown in [5, 7, 6], parts of the secret key of SFLASH^{v1} and SFLASH^{v2} can be revealed easily by means of a linear algebra based attack. Subsequently we show that the same holds for SFLASH^{v3}: The 861 bit representing the "affine part" of the secret key can be derived immediately from the public key, and thus do not really contribute to the security of the scheme.

2 Public and secret parameters of SFLASH^{v3}

For a complete description of SFLASH^{v3} we refer to [3]. Here we recall only the public and secret parameters of the algorithm, as the details of the signing and verification procedure are not relevant for the discussed attack.

SFLASH^{v3} makes use of two fields along with corresponding bijections:

- $K := \mathbb{F}_2[X]/(X^7 + X + 1)$ along with the bijection

$$\begin{array}{rccl} \pi : & \{0,1\}^7 & \longrightarrow & K \\ & (b_0, \ldots, b_6) & \longmapsto & \sum_{i=0}^{6} b_i X^i \pmod{X^7 + X + 1} \end{array}$$

- $L := K[X]/(X^{67} + X^5 + X^2 + X + 1)$ along with the bijection

$$\begin{array}{rccl} \varphi : & K^{67} & \longrightarrow & L \\ & (b_0, \ldots, b_{66}) & \longmapsto & \sum_{i=0}^{66} b_i X^i \pmod{X^{67} + X^5 + X^2 + X + 1} \end{array}$$

2.1 Secret key

The secret key is comprised of three parts:

- $\Delta \in \{0,1\}^{80}$: a secret 80-bit string
- $s = (S_L, S_C)$: an affine bijection $K^{67} \longrightarrow K^{67}$ given by a 67×67 matrix $S_L \in K^{67 \times 67}$ and a column vector $S_C \in K^{67}$
- $t = (T_L, T_C)$: an affine bijection $K^{67} \longrightarrow K^{67}$ given by a 67×67 matrix $T_L \in K^{67 \times 67}$ and a column vector $T_C \in K^{67}$

For deriving the corresponding public key also the function

$$\begin{array}{rccl} F : & L & \longrightarrow & L \\ & \alpha & \longmapsto & \alpha^{128^{33}+1} \end{array}$$

is needed.

2.2 Public key

The public key is the function $G : K^{67} \longrightarrow K^{56}$ defined by

$$G(X) = [(t \circ \varphi^{-1} \circ F \circ \varphi \circ s)(X)]_{0 \to 55}.$$

Here the notation $[\cdot]_{0 \to 55}$ means that only the first 56 (out of 67) rows are published, and $\circ$ denotes functional composition, i. e., $(f \circ g)(x) := f(g(x))$. By construction, $(Y_0, \ldots, Y_{55}) = G(X_0, \ldots, X_{66})$ can be expressed in the form

$$\begin{array}{rcl} Y_0 & = & P_0(X_0, \ldots, X_{66}) \\ & \vdots & \\ Y_{55} & = & P_{55}(X_0, \ldots, X_{66}) \end{array}$$

where each P_i is a polynomial of total degree ≤ 2 with coefficients in K.

It is worth noting that the public key of SFLASH^{v3} is independent of the secret 80-bit string Δ. Consequently, the verification procedure does not ensure that the correct value of Δ has been used for computing a signature. However, Δ is used for signing and the question of side channel attacks on Δ arises naturally (cf. [4]). The attack described in the sequel does not concern Δ and aims exclusively at the "affine parts" of s and t.

3 Attacking the affine parts

As the last 11 "rows" of t are not reflected in the public key (in particular they are not needed for computing a valid signature), we cannot hope to recover the last 11 entries T_C from the public data. However, finding the remaining $67 \cdot 7 + (67 - 11) \cdot 7 = 861$ bit of the secret key that represent the affine parts of s and t turns out to be rather simple.

3.1 Deriving the first 56 entries of T_C from $S_L^{-1} S_C$

By definition the bijection s has the form

$$s : \begin{array}{ccc} K^{67} & \longrightarrow & K^{67} \\ (b_0, \ldots, b_{66}) & \longmapsto & S_L \cdot (b_0, \ldots, b_{66})^{\mathrm{T}} + S_C \end{array} .$$

Equivalently, we can express s as

$$s : \begin{array}{ccc} K^{67} & \longrightarrow & K^{67} \\ (b_0, \ldots, b_{66}) & \longmapsto & S_L \cdot ((b_0, \ldots, b_{66})^{\mathrm{T}} + S_L^{-1} S_C) \end{array} .$$

In the first part of our attack we will recover $(v_0, \ldots, v_{66})^{\mathrm{T}} := S_L^{-1} S_C$. Once this vector is known, we see with the argument from [6] that the first 56 entries of T_C are obtained by evaluating the public key at $(v_0, \ldots, v_{66})$:

$$\begin{array}{rcl} G(v_0, \ldots, v_{66}) & = & [(t \circ \varphi^{-1} \circ F \circ \varphi \circ s)(v_0, \ldots, v_{66})]_{0 \to 55} \\ & \overset{\mathrm{char}(K)=2}{=} & [(t \circ \varphi^{-1} \circ F \circ \varphi)(0, \ldots, 0)]_{0 \to 55} \\ & = & [t(0, \ldots, 0)]_{0 \to 55} \\ & = & [T_C]_{0 \to 55} \end{array}$$

3.2 Finding $S_L^{-1} S_C$

Exactly as in [6] for SFLASH^{v2}, one makes the following

Observation 1 *The vector* $(v_0, \ldots, v_{66})^{\mathrm{T}} := S_L^{-1} S_C$ *is a solution of the homogeneous system of linear equations obtained by equating the linear part (i. e., the sum of the monomials of total degree* 1*) of the public key to* 0*.*

Proof: By construction, the map

$$\begin{array}{rccl} \widetilde{G}: & K^{67} & \longrightarrow & K^{56} \\ & X & \longmapsto & G(X - S_L^{-1} S_C) = [(t \circ \varphi^{-1} \circ F \circ \varphi(S_L \cdot X))]_{0 \to 55} \end{array}$$

can be expressed in the form

$$\widetilde{G}(x_0, \ldots, x_{66}) = \begin{pmatrix} \sum_{0 \le j,k \le 66} g_{0jk} x_j x_k \\ \vdots \\ \sum_{0 \le j,k \le 66} g_{55jk} x_j x_k \end{pmatrix} + T_C$$

with $g_{ijk} \in K$. In other words, $\widetilde{G}(x_0, \ldots, x_{66})$ involves no linear terms, and we see that the linear part of the public key $G(X) = \widetilde{G}(X + S_L^{-1} S_C)$ has the form

$$\begin{pmatrix} \sum_{0 \le j,k \le 66} g_{0jk}(x_j v_k + v_j x_k) \\ \vdots \\ \sum_{0 \le j,k \le 66} g_{55jk}(x_j v_k + v_j x_k) \end{pmatrix}$$

where $(v_0, \ldots, v_{66})^{\mathrm{T}} := S_L^{-1} S_C$. Finally, from $\mathrm{char}(K) = 2$ we conclude that all expressions of the form $(x_j v_k + v_j x_k)$ vanish when we specialize $(x_0, \ldots, x_{66}) \mapsto (v_0, \ldots, v_{66})$. $\square$

If the linear parts of the 56 components of the public key are linearly independent (which was always the case in our experiments) equating them simultaneously to 0 yields an 11-dimensional K-vector space $U \subseteq K^{67}$. From Observation 1 we know that $S_L^{-1} S_C \in U$ holds, and to eliminate the incorrect candidates in U, we do the same as in [6] when dealing with SFLASH^{v2}. Namely, we exploit

Observation 2 *Let* $v := S_L^{-1} S_C \in K^{67}$*, and denote by* z *the canonical generator of the* K*-algebra* $K[z]/(z^{128} - z)$*. In particular, we have* $z^{128} = z$*.*

Then for all $w \in K^{67}$ *the vector* $s(z \cdot w - v) = S_L \cdot (z \cdot w) \in K^{67}$ *contains entries from* $K \cdot z$ *only, i. e., there are no non-zero constant terms. Moreover, owing to the definition of* F*, the vector* $(F \circ \varphi \circ s)(z \cdot w - v)$ *has entries from* $K \cdot z^2$ *only, i. e., it contains no linear or constant terms.*

Let $\{b_0, \ldots, b_{10}\}$ be a basis of the K-vector space U, and consider the linear combination $\sum_{i=0}^{10} \alpha_i \cdot b_i$ where the α_i are indeterminates. Then according to Observation 2 all the terms linear in z of

$$\begin{aligned} &(t \circ \varphi^{-1} \circ F \circ \varphi \circ s)\left(z \cdot w - \sum_{i=0}^{10} \alpha_i \cdot b_i\right) \\ = \quad & T_L \cdot (\varphi^{-1} \circ F \circ \varphi \circ s)\left(z \cdot w - \sum_{i=0}^{10} \alpha_i \cdot b_i\right) + T_C \end{aligned}$$

vanish when specializing the α_i so that the sum $\sum_{i=0}^{10} \alpha_i \cdot b_i$ evaluates to $S_L^{-1} S_C$.

This yields 56 linear equations in the 11 indeterminates $\alpha_0, \ldots, \alpha_{10}$, and $S_L^{-1} S_C \in K^{67}$ is a solution of this system. In several hundred examples we did with the computer algebra system Magma [1], $S_L^{-1} S_C$ was always the only solution, and it could always be found within a few seconds. From $S_L^{-1} S_C$ we can derive $[T_C]_{0\to 55}$ as described in the previous section, so that we are in the position where for forging signatures it is sufficient to reveal the secret linear parts S_L and (the first 56 rows of) T_L.

4 Conclusion

The above discussion shows that the affine parts of SFLASH^{v3} succumb to basically the same attack as the affine parts of its predecessors SFLASH^{v1} and SFLASH^{v2}. Although this attack does not "break" SFLASH^{v3}, it may raise some questions on its design.

References

[1] W. Bosma, J. Cannon, and C. Playoust. The Magma Algebra System I: The User Language. *Journal of Symbolic Computation*, 24:235–265, 1997.

[2] NESSIE consortium. NESSIE Portfolio of recommended cryptographic primitives. At the time of writing available at `https://www.cosic.esat.kuleuven.ac.be/nessie/deliverables/decision-final.pdf`, 2003.

[3] N. Courtois, L. Goubin, and J. Patarin. SFLASH^{v3}, a fast asymmetric signature scheme. Cryptology ePrint Archive: Report 2003/211, 2003.

Revised Specification of SFLASH, version 3.0., October 2nd, 2003. At the time of writing available at `http://eprint.iacr.org/2003/211/`.

[4] W. Geiselmann, R. Steinwandt, and Th. Beth. A Theoretical DPA-Based Cryptanalysis of the NESSIE Candidates FLASH and SFLASH. In G. I. Davida and Y. Frankel, editors, *Information Security, 4th International Conference, ISC 2001 Proceedings*, volume 2200 of *Lecture Notes in Computer Science*, pages 280–293. Springer, 2001. Also presented at the 2nd NESSIE Workshop.

[5] W. Geiselmann, R. Steinwandt, and Th. Beth. Attacking the Affine Parts of SFLASH. In Bahram Honary, editor, *Cryptography and Coding, 8th IMA International Conference Proceedings*, volume 2260 of *Lecture Notes in Computer Science*, pages 355–359. Springer, 2001. Also presented at the 2nd NESSIE workshop.

[6] W. Geiselmann, R. Steinwandt, and Th. Beth. Revealing 441 Key Bits of SFLASH^{v2}. Workshop record of the 3rd NESSIE Workshop, November 2002.

[7] W. Geiselmann, R. Steinwandt, and Th. Beth. Revealing the Affine Parts of SFLASH^{v1}, SFLASH^{v2}, and FLASH. In Santos González Jiménez and Consuelo Martínez López, editors, *Actas de la VII Reunión Española de Criptología y Seguridad de la Información. Tomo I*, pages 305–314, 2002.

[8] H. Gilbert and M. Minier. Cryptanalysis of SFLASH. In Lars Knudsen, editor, *Advances in Cryptology — EUROCRYPT 2002*, volume 2332, pages 288–298, 2002.