CRYPTANALYSIS OF SFLASH^{v3}

JINTAI DING, DIETER SCHMIDT

Abstract. Sflash is a fast multivariate signature scheme. Though the first version Sflash^{v1} was flawed, a second version, Sflash^{v2} was selected by the Nessie Consortium and was recommended for implementation of low-end smart cards. Very recently, due to the security concern, the designer of Sflash recommended that Sflash^{v2} should not be used, instead a new version Sflash^{v3} is proposed, which essentially only increases the length of the signature. The Sflash family of signature schemes is a variant of the Matsumoto and Imai public key cryptosystem. The modification is through the Minus method, namely given a set of polynomial equations, one takes out a few of them to make them much more difficult to solve. In this paper, we attack the Sflash^{v3} scheme by combining an idea from the relinearization method by Kipnis and Shamir, which was used to attack the Hidden Field Equation schemes, and the linearization method by Patarin. We show that the attack complexity is less than 2^{80}, the security standard required by the Nessie Consortium.

Keywords: open-key, multivariable, quadratic polynomials

1. Introduction

NESSIE, New European Schemes for Signatures, Integrity, and Encryption, is a project within the Information Society Technologies Programme of the European Commission. It made its final selection of the crypto algorithms at the beginning of last year after a process of more than 2 years, see [N].

Sflash^{v2}, a fast multivariate signature scheme was selected by the Nessie Consortium and was recommended for low-cost smart cards. The initial submission **Sflash**^{v1} was flawed, as Henri Gilbert found a way to break it (published at Eurocrypt 2002). The flaw was due to a bad choice of the field elements to minimize the size of the public key, but this was not essential. Specifications for the new scheme Sflash^{v2} were submitted. The new version has the signature length of 259 bits and a public key of 15 KBytes. The submission claimed that Sflash^{v2} is the fastest signature scheme in the world, and is the only digital signature scheme that can be used in practice for smart cards. However, very recently, due to security concerns, the designer of Sflash recommended that Slash^{v2} should not be used, instead a new version Sflash^{v3} is recommended, which is a simple extension of Sflash^{v2} by increasing the length of the signature. Sflash^{v3} has the signature length of 469 bits and a public key of 112 KBytes.

The family of Sflash schemes belongs to the family of the new public key cryptosystems based on multivariable quadratic polynomials. This idea is built on the proven theorem that solving a general set of multivariable polynomial equations over a finite field is an NP-hard problem.

The Sflash scheme is a simple variant of a basic design by Matsumoto and Imai [MI], who suggested to use the map

$$\bar{M} : X \longmapsto X^{1+(2^q)^\theta},$$

over a large field K, a degree n extension of a finite field k of characteristic 2 with 2^q elements, $K \cong k[x]/I(x)$, where $I(x)$ is an irreducible polynomial over k of degree n. Here θ is an integer such that $gcd((2^q)^\theta + 1, (2^q)^n - 1) = 1$.

Let ϕ be the standard k-linear map that identifies K with k^n: $\phi : K \to k^n$, such that

$$\phi(a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1}) = (a_0, a_1, a_2, \cdots, a_{n-1}). \tag{1.1}$$

By identifying K with k^n through ϕ, this map $\bar{M}$ gives a multivariable polynomial map

$$\hat{M} = \phi \circ \bar{M} \circ \phi^{-1} \tag{1.2}$$

from k^n to k^n, (by $\circ$ we mean composition). Then one hides this map $\hat{M}$ by composing from both sides with two invertible affine linear maps L_1 and L_2 over k^n, which produces a quadratic map M:

$$M = L_1 \circ \hat{M} \circ L_2 \tag{1.3}$$

from k^n to k^n. We have

$$M(x_0, \ldots, x_{n-1}) = (M_0(x_0, \ldots, x_{n-1}), M_1(x_0, \ldots, x_{n-1}), \ldots, M_{n-1}(x_0, \ldots, x_{n-1})),$$

where $M_i(x_0, \ldots, x_{n-1})$ are quadratic polynomials and x_i in k.

In this paper we try to follow the notation that a mapping from K to K will be denoted by a bar, as in $\bar{M}$, and the corresponding k^n to k^n map lifted by ϕ will be denoted with a hat, as given in (1.2). After composing this map, as in (1.3), then we drop the bar. Later on a minus as in M^- indicates a new map from k^n to k^{n-r}, where r components are taken out from the map $M : k^n \to k^n$.

The scheme described above was defeated by the linearization attack of Patarin [P]. Sflash is derived from the generalizations and extensions of the Matsumoto-Imai construction. It was developed mainly by Patarin and his collaborators. Sflash is based on a very simple idea, called the Minus method, namely one takes out (Minus) r quadratic polynomial components of M, which eliminates the possibility of the linearization attack. This method was first suggested by Shamir [S]. Thus, we will have a new map

$$M^-(x_0, \ldots, x_{n-1}) = (M_0(x_0, \ldots, x_{n-1}), M_1(x_0, \ldots, x_{n-1}), \ldots, M_{n-1-r}(x_0, \ldots, x_{n-1})),$$

from k^n to k^{n-r}. The Minus method is very suitable for signature schemes, for which one needs only one of the solutions of a set of polynomial equations, not *THE* solution. The security of this family of signature schemes is based on the assumption that to solve this set of $n - r$ quadratic equations with n variables is very difficult.

For the Sflash^{v2}, k is chosen to be of size 2^7 and K is a degree 37 extension of k, $\theta = 11$, and $r = 11$.

For the Sflash^{v3}, k is chosen to be of size 2^7 and K is a degree 67 extension of k, $\theta = 33$, and $r = 11$.

The only method, besides a brute force attack, is to search for the missing r quadratic polynomials using the property that $\bar{M}$ is a permutation polynomial over K, then put them back into M^- to recover M and apply the linearization attack. This is how Henri Gilbert defeated the previous version of Sflash, Sflash^{v1}. However, this attack cannot be applied to the new versions of Sflash because $(2^q)^r$ is too big.

Our method is completely different. We try to find directly the secret key. For this we will apply an idea of Kipnis and Shamir for attacking the Hidden Field Equation schemes, which is another

multivariable cryptosystem. Namely, the map M^- can be represented as a new function $\bar{M}^-$ over K in the following form:

$$\bar{M}^-(X) = \sum_{0,0}^{n-1,n-1} g_{i,j} X^{(2^q)^i} X^{(2^q)^j} + \sum_{0}^{n-1} g_i X^{(2^q)^i} + g, \tag{1.4}$$

which follows from a simple theorem by Kipnis and Shamir [KS]. Using the ideas in [KS], we can transform the problem to find the secret key into a problem of solving a set of $67 \times 56 \times 33$ quadratic equations with 67^2 variables over $GF(2^7)$. However we show that the relinearization method in [KS] can not be applied here any more.

Our new attack method includes two crucial ideas. The first one is the idea of using the affine part of the secret key. Because of the reformulation of the problem, we can actually normalize the linear terms of the secret keys as we wish. Namely any affine linear transformation H over k^n can be lifted as a K map in the form:

$$\bar{H}(X) = \sum_{0}^{n-1} \alpha_i X^{2^{qi}} + \alpha. \tag{1.5}$$

We then can normalize the map by multiplying a non-zero element β in K:

$$\bar{H}(X) = \omega^{-1} \circ \omega \circ \bar{H}(X) = \beta^{-1} \times (\sum_{0}^{n-1} \beta \times \alpha_i X^{2^{qi}} + \beta \times \alpha) = \omega^{-1} \circ \bar{H}_1, \tag{1.6}$$

where $\omega(X) = \beta \times X$. This allows us to choose the constant terms of the secret linear transformation L_2 to be anything nonzero we wish. Applying this idea to our reformulated problem, we could obtain a large amount of linearly independent linear equations ($n \times (n-r)$) satisfied by the secret keys. For the case of Sflash^{v3} this produces 67×56 linearly independent linear equations. Then to solve the set of quadratic polynomial equations is reduced to a problem of solving a set of $67 \times 56 \times 33$ quadratic equations with 67×11 variables over $GF(2^7)$. After this, the second step is the straightforward linearization method, because we now have a family of very overly defined quadratic equations. The solution gives us the secret keys. The total complexity of our attack is less than 2^{80}.

One crucial point of our attack is the normalization above, which however could not be performed without the idea of lifting a problem over k^n to K in [KS].

Our method is very general and it can be applied to all M^- schemes. However, it does not necessarily work very well on all cases, it depends on the choice of n and r and in general it works if n/r is larger than 6.

In the first section of the paper, we will introduce Slash. Then we will present our attack on Sflash^{v3}.

2. Sflash

We introduce the basic structure of the Sflash signature schemes family, which is a variant of the Matsumoto-Imai cryptosystem.

2.1. The Matsumoto-Imai Cipher of Sflash.

In this section, we fix k to be the finite field $GF(2^7)$ of characteristic 2 with $2^q = 2^7 = 128$ elements. k is a field extension of $GF(2)$ and

$$k \cong GF(2)[x]/(x^7 + x + 1).$$

Let $\bar{M}(X) = X^{1+(2^q)^\theta}$, over K, and $gcd((2^q)^\theta + 1, (2^q)^n - 1) = 1$. $\bar{M}$ is an invertible map and its inverse is given by $\bar{M}^{-1}(X) = X^t$, where $t \times ((2^q)^\theta + 1) = 1 \bmod ((2^q)^n - 1)$, which can be computed easily.

Remark 1. In all the Sflash schemes, θ is chosen to be 11 or 33 so that the decryption can be computed fast. However, this choice plays no role in our attack.

Let $\hat{M}$ be the map over k^n and

$$\hat{M}(x_0, \ldots, x_{n-1}) = \phi \circ \bar{M} \circ \phi^{-1}(x_0, \ldots, x_{n-1})$$

$$= (\hat{M}_0(x_0, \ldots, x_{n-1}), \hat{M}_1(x_0, \ldots, x_{n-1}), \cdots, \hat{M}_{n-1}(x_0, \ldots, x_{n-1})).$$

Here $\hat{M}_i(x_0, \ldots, x_{n-1})$ are quadratic polynomial of n variables. Let L_1 and L_2 be two randomly chosen invertible affine linear maps over k^n.

$$\begin{aligned} M(x_0, \ldots, x_{n-1}) &= L_1 \circ \hat{M} \circ L_2(x_0, \ldots, x_{n-1}) \\ &= (M_0(x_0, \ldots, x_{n-1}), M_1(x_0, \ldots, x_{n-1}), \cdots, M_{n-1}(x_0, \ldots, x_{n-1})) \end{aligned}$$

is the cipher suggested by Matsumoto-Imai for public key encryption, which was defeated by the linearization method of Patarin. This is because the components of M, $M_i(x_0, \ldots, x_{n-1})$, satisfy the linearization equation

$$\sum_{0,0}^{n-1,n-1} b_{ij} x_i M_j(x_0, \ldots, x_{n-1}) + \sum_{0}^{n-1} b_i M_i(x_0, \ldots, x_{n-1}) + \sum_{0}^{n-1} c_i x_i + b = 0,$$

which produces linear equations satisfied by x_i once the values of M_i are given.

2.2. **The Sflash signature scheme.** Select $r = 11$ and consider

$$M^-(x_0, \ldots, x_{n-1}) = (M_0(x_0, \ldots, x_{n-1}), M_1(x_0, \ldots, x_{n-1}), \ldots, M_{n-1-r}(x_0, \ldots, x_{n-1})),$$

which is a map from k^n to k^{n-r}. The Sflash scheme has the following structure:

The public key includes:

(1) the field k including its addition and multiplication structure;
(2) the $n - r$ quadratic polynomials $M_0(x_0, \ldots, x_{n-1}), \ldots, M_{n-1-r}(x_0, \ldots, x_{n-1})$.

The private key includes:

(1) δ a randomly chosen 80 bits long secret key;
(2) the two invertible affine linear maps L_1, L_2.

The signing process

To sign a message Z one goes through the following steps:

(1) Use the hash function SHA-1 and go through a few procedures to create a $(n - r) \times q$ bits long string Y. These procedures are public, which anyone can perform for a given message Z. They are not essential in regard to our attack. Therefore, we omit them here and refer the reader to the original paper [CGP1].
(2) Use Y and the secret key δ to create a bit string R of length $q \times r = 77$
(3) Produce a $n \times q$ long bit string by setting $W = (Y||R)$ and identify W as an element in k^n.

(4) Calculate

$$\bar{W} = M^{-1}(W) = L_2^{-1} \circ (\hat{M}^{-1}) \circ L_1^{-1}(W) = L_2^{-1} \circ \phi \circ (\bar{M})^{-1} \circ \phi^{-1} \circ L_1^{-1}(W).$$

The $n \times q$ bits of $\bar{W}$ are the signature for Z.

The verifying process:

In order to verify the signature, one just has to check if

$$M^-(\bar{W}) = Y.$$

It is clear that to forge a signature for a message Z in terms of such a scheme, one needs to just find one solution of the set of equations $M^-(\bar{W}) = Y$. Here the secret key δ is not at all important in terms of this attack.

3. Our attack method

Our method is very much inspired by and derived from the ideas and methods of Kipnis and Shamir. In this section, we will follow the ideas in the first part of [KS], and we will first reformulate the problem over the bigger field K.

3.1. **Reformulation of the problem by the method of Kipnis and Shamir.** We will reformulate the problem to attack a general Matsumoto-Imai Minus scheme.

Again, we let k be a finite field of characteristic 2 and let $\|k\| = 2^q$.

Let K be a degree n field extension of k with an irreducible polynomial $I(x)$ over $GF(2)$.

Let ϕ be the standard invertible map from K to $k^n = k \times \ldots \times k$ as given in (1.1). Let $\bar{M}$ be a Matsumoto-Imai map from K to itself given by $\bar{M}(X) = X^{2^{q^\theta}+1}$, where $gcd(2^{q\theta}+1, 2^{qn}-1) = 1$.

Let $\hat{M} = \phi \circ \bar{M} \circ \phi^{-1}$, and $\hat{M}(x_0, \ldots, x_{n-1}) = (y_0, \ldots, y_{n-1})$, be a quadratic map from k^n to k^n.

For each integer i the map $\bar{T}_i(X) = X^{2^{qi}}$ over K is actually linear if viewed as a map from k^n to k^n.

The inverse of $\hat{M}$ is given by: $\hat{M}^{-1} = \phi \circ \bar{M}^{-1} \circ \phi^{-1}$.

Let $\bar{L}$ denote the space of all maps from K to K in the form of

$$\bar{H}(X) = \sum_0^{n-1} \alpha_i X^{2^{qi}} + \alpha, \tag{3.1}$$

where $\alpha_i \in K$, $\alpha \in K$. $\bar{L}$ is a linear space.

Let L denote the space of all maps from k^n to k^n in the form of

$$H = \phi \circ \bar{H} \circ \phi^{-1}. \tag{3.2}$$

Lemma 1. [KS] *L is the space of all affine linear maps from k^n to k^n.*

This means that any linear map on k^n can be lifted and transformed into an element in $\bar{L}$. This can be achieved easily by solving a set of n^2 linear equations over k. This transformation is clearly invertible.

Let $(x_0, \ldots, x_{n-1})$ be an element in k^n.

Let P_r be the linear projection map over k^n such that

$$P_r(x_0, \ldots, x_{n-1}) = (x_0, \ldots, x_{n-1-r}, 0, 0, \ldots, 0).$$

Let $\bar{M}^-$ be a map over K such that

$$\bar{M}^-(X) = \phi^{-1} \circ \hat{M}^- \circ \phi(X)$$

and

$$\hat{M}^-(x_0, \ldots, x_{n-1}) = (M^-(x_0, \ldots, x_{n-1}), 0, \ldots, 0) = P_r \circ M(x_0, \ldots, x_{n-1}).$$

a map from k^n to k^n. Thus

$$\begin{aligned}\bar{M}^- &= \phi^{-1} \circ P_r \circ L_1 \circ (\phi \circ \bar{M} \circ \phi^{-1}) \circ L_2 \circ \phi \\ &= \phi^{-1} \circ P_r \circ L_1 \circ \phi \circ \bar{M} \circ \phi^{-1} \circ L_2 \circ \phi \\ &= (\phi^{-1} \circ (P_r \circ L_1) \circ \phi) \circ \bar{M} \circ (\phi^{-1} \circ L_2 \circ \phi).\end{aligned}$$

Then, from Lemma 1, we have

Lemma 2. [KS]

$$\bar{M}^- = \bar{S} \circ \bar{M} \circ \bar{Q}$$

such that $\bar{S} = \phi^{-1} \circ (P_r \circ L_1) \circ \phi$ *and* $\bar{Q} = \phi^{-1} \circ L_2 \circ \phi$ *are in* $\bar{L}$ *and*

$$\bar{M}^-(X) = \sum_{0,0}^{n-1,n-1} g_{ij} X^{2^{qi}} X^{2^{qj}} + \sum_{0}^{n-1} g_i X^{2^{qi}} + g$$

where g_{ij}, g_i *and* g *are in* K.

Lemma 3. [KS] *Let* $\hat{F}$ *be a map of total degree less than 3 from* k^n *to* k^n *and* $(x_0, \ldots, x_{n-1})$ *be the variables in* k^n. *Then, there exists an unique map* $\bar{F}$ *such that*

$$\begin{aligned}\bar{F}(X) &= \sum_{0,0}^{n-1,n-1} f_{ij} X^{2^{qi}} X^{2^{qj}} + \sum_{0}^{n-1} f_i X^{2^{qi}} + f, \\ \hat{F} &= \phi \circ \bar{F} \circ \phi^{-1},\end{aligned}$$

where f_{ij}, f_i *and* f *are in* K. *For any given* $\hat{F}$, *the linear equation derived from the second equation above gives a unique solution for* $\bar{F}$.

This means that we can lift any quadratic map over k^n into a map of a special form over K. From this we know that once we have the $n - r$ quadratic polynomials for the Sflash scheme, we can find the function $\bar{M}^-$ by solving a small set of linear equations.

Therefore, the direct way to attack the Sflash is to find the secret key for this version of Sflash scheme, which are the two maps $\bar{Q}$ and $\bar{S}$, where $\bar{Q}$ is invertible and $\bar{S}$ is not.

$$\bar{Q}(X) = \sum_{0}^{n-1} \bar{q}_i X^{2^{qi}} + \bar{a}_1, \tag{3.3}$$

$$\bar{S}(X) = \sum_{0}^{n-1} \bar{s}_i X^{2^{qi}} + \bar{a}_2, \tag{3.4}$$

here $\bar{a}_i$, $\bar{q}_i$ and $\bar{s}_i$ are in K.

However we can see that the equation in Lemma 2 above will produce $n(n+1)/2$ cubic equations if we expand them in k^n, which is rather difficult to deal with. We will next modify the problem slightly.

Let

$$\bar{Q}^{-1}(X) = \sum_{0}^{n-1} q_i X^{2^{qi}} + a_1,$$

be the inverse of $\bar{Q}$. We know that finding $\bar{S}$ and $\bar{Q}$ is equivalent to finding $\bar{S}$ and $\bar{Q}^{-1}$.

But we also have

Corollary 1.

$$\bar{M}^- \circ \bar{Q}^{-1} = \bar{S} \circ \bar{M}. \tag{3.5}$$

Then we have

$$\bar{S} \circ \bar{M} = \sum_{0}^{n-1} \bar{s}_i X^{(2^q)^i} X^{(2^q)^{\theta+i}} + \bar{a}_2 = \sum \bar{s}_{ij} X^{2^{qi}} X^{2^{qj}} + \bar{a}_2. \tag{3.6}$$

Since $X^{2^{qn}} = X$, the indices $\theta + i$ and i are considered in the coset of numbers modular n. From this and (3.6) we have

$$\begin{aligned}
\bar{M}^- \circ \bar{Q}^{-1}(X) &= \sum_{0,0}^{n-1,n-1} g_{ij} (\bar{Q}^{-1}(X))^{2^{qi}} (\bar{Q}^{-1}(X))^{2^{qj}} + \sum_{0}^{n-1} g_i (\bar{Q}^{-1}(X))^{2^{qi}} + g \\
&= \sum_{0,0}^{n-1,n-1} g_{ij} (\sum_{0}^{n-1} q_k X^{2^{qk}} + a_1)^{2^{qi}} (\sum_{0}^{n-1} q_k X^{2^{qk}} + a_1)^{2^{qj}} + \sum_{0}^{n-1} g_i (\sum_{0}^{n-1} q_k X^{2^{qk}} + a_1)^{2^{qi}} + g \\
&= \sum_{0}^{n-1} \bar{s}_i X^{(2^q)^i} X^{(2^q)^{\theta+i}} + \bar{a}_2
\end{aligned}$$

By comparing coefficients of $X^{(2^q)^I} X^{(2^q)^J}$ when $|I - J| \neq \theta$, we will produce equations of the form

$$\sum d_{i,j,l,m} q_i^{(2^q)^j} q_l^{(2^q)^m} = 0. \tag{3.7}$$

Unfortunately, this looks even more complicated than solving our original equations. However, we can write the equations in terms of k^n and not K, that is, in the equations above we use

$$q_i = \sum_{0}^{n-1} q_{ij} x^j.$$

Then by comparing the values of the coefficient of x^i, $i = 0, \ldots, n-1$ and due to the linear property of the map $\bar{T}_i$, we can produce n quadratic equations in terms of the n^2 components q_{ij} for each equation (3.7). In this case, we have a set of $n \times n \times (n-1)/2$ quadratic equations with n^2 variables. For the case of Sflash^{v2} and Sflash^{v3}, to solve this is still a daunting task. However this suggests that it is possible to find first $\bar{Q}^{-1}$ by solving a set of quadratic equations. Then we can automatically find $\bar{S}$. This is just the opposite to the method in [KS], where they suggest to use the MinRank method to find first $\bar{S}$ and then $\bar{Q}^{-1}$.

3.2. **Inapplicability of the relinearization method of Kipnis and Shamir.** One may also apply another idea found in [KS] to reformulate the problem into a more standard linear algebra problem. Let $\tilde{\Psi}$ be the n by n matrix that

$$\tilde{\Psi}_{i,j} = \bar{s}_{ij}$$

and let

$$\Psi = \tilde{\Psi} + \tilde{\Psi}^T,$$

which is a symmetric matrix such that all the entries are zero except those where the difference of the row and column index is either θ or $-\theta$ mod n. Denote the non-zero elements of Ψ by s_{ij}. For example for $\theta = 11$ the matrix Ψ has the form

$$\begin{bmatrix}
0 & 0 & \cdots & 0 & s_{0,11} & 0 & \cdots & \cdots & s_{0,n-11} & 0 & \cdots & 0 \\
0 & 0 & \cdots & 0 & 0 & s_{1,12} & \cdots & \cdots & 0 & s_{1,n-10} & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & 0 & 0 & \cdots & \cdots & 0 & 0 & \cdots & s_{10,n-1} \\
s_{0,11} & 0 & \cdots & 0 & 0 & 0 & \cdots & \cdots & s_{11,n-11} & 0 & \cdots & 0 \\
0 & s_{1,12} & \cdots & 0 & 0 & 0 & \cdots & \cdots & 0 & s_{12,n-10} & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots & \vdots \\
s_{0,n-11} & 0 & \cdots & 0 & s_{11,n-11} & 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 \\
0 & s_{1,n-10} & \cdots & 0 & 0 & s_{12,n-10} & \cdots & \cdots & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & s_{10,n-1} & 0 & 0 & \cdots & \cdots & 0 & 0 & \cdots & 0
\end{bmatrix}$$

Let $\tilde{\Gamma}$ be an $n \times n$ matrix such that

$$\tilde{\Gamma}_{ij} = g_{ij}$$

and

$$\Gamma = \tilde{\Gamma} + \tilde{\Gamma}^T.$$

Let Φ be an $n \times n$ matrix such that

$$\Phi_{ij} = q_{i-j}^{(2^q)^j},$$

which is the inverse of the matrix with entries

$$\Phi_{ij}^{-1} = \bar{q}_{i-j}^{(2^q)^j}.$$

Then by calculation we have

Lemma 4. [KS]

$$\Psi = \Phi \times \Gamma \times \Phi^T, \tag{3.8}$$

$$\Gamma = \Phi^{-1} \times \Psi \times (\Phi^{-1})^T. \tag{3.9}$$

Then finding the secret key is essentially the same as finding both Φ and Ψ with a given Γ, which satisfies the second equation above.

Unfortunately the relinearization method in [KS] can not work here anymore because it requires first a procedure of somehow reducing the rank of Γ to the minimum. This is so because in the case of the HFE scheme Ψ is a matrix where all s_{ij} are zero except those with indices i and j less or equal to a small number D. The matrix Ψ has, therefore, a very small rank D. The MinRank

method is then applied to solve the problem. In our case we can see easily that the rank of Ψ is, in general, not necessarily small at all. Our computer experiments have shown that it is not less than r. We can prove this directly.

One more idea available to solve this problem is also from [KS], namely the idea of the null space. Let's assume that we know the values of Ψ as well, then we can find the left null space of Ψ. Let v be a non-zero vector in this space. Then we have

$$\Phi\Gamma\Phi^T v = \Psi v = 0$$

thus

$$\Gamma\Phi^T v = 0,$$

which can be used to derive linear equations if we write down those equations in k^n instead of K as is done in (3.7). However, in our case Ψ is not known, therefore we can not apply it directly.

We can also use the standard method of averaging. Namely we compose from both sides of the equation $\bar{M}^- = \bar{S} \circ \bar{M} \circ \bar{Q}$ by the map $\bar{A}(X) = \sum_0^{n-1} X^{(2^q)^i}$, which gives us

$$\bar{A} \circ \bar{M}^- = (\bar{A} \circ \bar{S} \circ \bar{M}) \circ \bar{Q}.$$

Because $\bar{A}(x)$ is invariant under the composition from the left by the map $\bar{T}_i(X) = X^{2^{qi}}$, $i = 1, \ldots, n-1$ we know that

$$\bar{A} \circ \bar{S} \circ \bar{M}(X) = \sum_0^{n-1} a^{(2^q)^i} X^{(2^q)^i} = \bar{A} \circ \bar{M} \circ \bar{l}_a$$

for some a in K and $l_a(X) = aX$. Then we have

$$\bar{A} \circ \bar{M}^- = \bar{A} \circ \bar{M} \circ \bar{l}_a \circ \bar{Q} = \bar{A} \circ (\bar{M}) \circ (\bar{l}_a \circ \bar{Q}).$$

Through this, in some way, we transform Ψ into a known new matrix whose entries are all zero except those where the difference between the indices is either θ or $-\theta$ and have the value 1 there. In this case, our only problem is to find $(\bar{l}_a \circ \bar{Q})$. It seems that in this case, the null space method may work. However, our computer experiments have shown that it can really only produce one non-equivalent equation over $\bar{L}$, which will produce n linear equations over k and it is not enough for our purpose.

3.3. **The method of linear terms.** In this section, we will use the general design of Sflash, that is both secret linear maps are affine. In this case, according to the notation above, (3.3) and (3.4), we have

$$\begin{aligned} \bar{Q}(X) &= \sum_0^{n-1} \bar{q}_i X^{2^{qi}} + \bar{a}_1, \\ \bar{S}(X) &= \sum_0^{n-1} \bar{s}_i X^{2^{qi}} + \bar{a}_2, \end{aligned}$$

where $\bar{a}_1$ and $\bar{a}_2$ are in K. Here we realize that we can normalize $\bar{Q}$ in the following way such that

$$\bar{Q}^{-1}(X) = \sum_0^{n-1} q_i X^{2^{qi}} + \rho,$$

where ρ is an element in K we randomly choose such that ρ is a generator of the multiplicative group of K without the zero element.

The reason we could do this is that for any linear function $\omega(X) = \beta \times X$, where β, X in K, we have

$$\bar{M}^- = \bar{S} \circ \bar{M} \circ \omega \circ \omega^{-1} \circ \bar{Q} = (\bar{S} \circ \bar{\omega}) \circ \bar{M} \circ \omega^{-1} \circ \bar{Q}, \tag{3.10}$$

where $\bar{\omega}(X) = \beta^{1+(2^q)^\theta} X$. Such a normalization does not affect at all our attack because $(\bar{S} \circ \bar{\omega})$ and $\omega^{-1} \circ \bar{Q}$ are just another set of equivalent secret keys. This means that we can normalize $\bar{Q}$ and therefore $\bar{Q}^{-1}$ as we wish.

Remark 2. With this normalization of selecting an appropriate ρ the solution for q_i is unique up to a multiple of an element in k. If we select one of the components in the field k then the solution is unique, which reduces the complexity of solving the equations.

From now on, we assume the normalization above, and we again have that:

$$\bar{M}^- \circ \bar{Q}^{-1} = \bar{S} \circ \bar{M}. \tag{3.11}$$

Then we have

$$\bar{S} \circ \bar{M} = \sum_0^{n-1} \bar{s}_i X^{(2^q)^i} X^{(2^q)^{\theta+i}} + \bar{a}_2 = \sum \bar{s}_{ij} X^{2^{qi}} X^{2^{qj}} + \bar{a}_2. \tag{3.12}$$

where all the "linear" terms of $X^{(2^q)^i}$ disappear.

With the normalization and by looking at the composition formula and comparing the coefficient, we immediately derive n equations in the form:

$$\sum_{0,0}^{n-1,n-1} \gamma_{i,j} q_i^{(2^q)^i} = 0. \tag{3.13}$$

If we look at these equations in the terms of the components of the field k, it seems that we should obtain n^2 linear equations satisfied by the components q_{ij} of q_i, which follows from Lemma 1. However, due to the minus operation, it is clear that we actually only get $n(n-r)$ linear equations. Statistically, a set of $n(n-r)$ linear equations with n^2 variables should be linearly independent with a probability close to one. We did many computer simulations for different values of n, r and θ, including the case of Sflash^{v2}. Our results confirmed that those linear equations are indeed linearly independent. Therefore, we conclude that (3.13) indeed produces $n(n-r)$ linearly independent linear equations in the field k. For the case of Sflash^{v2} and Sflash^{v3}, the dimension of this set of linear equations is therefore 37×26 and 67×56 respectively.

3.4. **The attack on Sflash^{v3}.** In the case of Sflash^{v3}, our attack strategy is to combine the equation in (3.7) and the linear equations derived from the section above.

Through computation, we found out that (3.7) type of equations will produce $n \times (n-1)/2 \times (n-r)$ linearly independent quadratic equations in terms of the components q_{ij} of q_i in the field k. For the case of Sflash^{v2} and Sflash^{v3} there are $37 \times (36/2) \times 26$ and $67 \times (66/2) \times 56$ of these equations respectively.

For the case of Sflash^{v3}, our problem now becomes a problem to solve a set of 67×56 linearly independent linear equations and $67 \times 33 \times 56$ linearly independent quadratic equations with 67^2 variables over k.

We use the Gaussian elimination method to solve the 67×56 linear equations. We substitute this solution into the $67 \times 33 \times 56$ quadratic equations, in order to obtain a set of $67 \times 33 \times 56$

linearly independent quadratic equations with however only $67 \times 11 - 1$ variables. This comes from plugging in solutions of (3.13) and selecting a value for one of the remaining q_{ij}.

Let's denote the new set of variables by z_i, $i = 1, \ldots, 736 (= 67 \times 11 - 1)$ and the new set of equations by $E_i(z_1, \ldots, z_{736}) = 0$, $i = 1, \ldots, 123816 (= 67 \times 33 \times 56)$.

Clearly this is a case of a very over-defined system of equations. We then realize that we can actually apply the linearization method by Patarin to solve it. Namely we will make all possible linear combinations like:

$$\sum_{i,j}^{736,123816} e_{i,j} z_i E_j(z_1, \ldots, z_{736}) + \sum_{j}^{123816} e_{0,j} E_j(z_1, \ldots, z_{736}) + \sum_{i}^{736} e_{i,0} z_i + e_{0,0} = 0 \tag{3.14}$$

to derive linear equations satisfied by z_i. In this case, the number of unknowns $e_{i,j}$ is:

$$737 \times 123817 = 91,253,129.$$

First we know that the total dimension of all polynomials with $736 = 67 \times 11 - 1$ variables z_j and degree less or equal to 3 is:

$$(736 + 3)(736 + 2)(736 + 1)/3! = 66,991,089. \tag{3.15}$$

Since

$$91,253,129 >> 66,991,089$$

and from the arguments in [CKPS], we know that the linear combinations of $z_i E_j(z_1, \ldots, z_{736})$ and $E_j(z_1, \ldots, z_{736})$ should include all terms with degree less or equal to 3 in the ideal generated by $z_i - \eta_i$, that is, it will produce the linear equations we need to find the solutions for all the z_i, where η_i are the values of z_i as the solution of our quadratic equations.

Remark 3. The reason we could conclude so is due to the choice of ρ and the selection of one element q_{ij} in k, which makes the solution unique.

To get what we want, we do not have to solve this equation directly. From a probabilistic point of view, we can randomly choose the values of $91,253,129 - (66,991,089 + 736 + 1)$ variables e_{ij}, $i, j > 0$ and then solve a set of $66,991,089$ equations with $66,991,089 + 736 + 1$ variables $e_{i,j}$. This will produce 736 linearly independent linear equations of z_i. We know that this will work with probability near to one.

Then we can use the original 67×56 linear equations to find all the solution for q_{ij} and therefore the q_i and $\bar{q}_i$ and $\bar{s}_i$. From Lemma 1, we know this gives us L_2 and $P_r \circ L_1$. Clearly $\hat{M} \circ L_2$ gives us all the n quadratic polynomials since $M_i(x_0, ..., x_{n-1})$ are just some linear combinations of the components of$\hat{M} \circ L_2$. Then we can add r components from these polynomials to M^- to derive a new invertible linear map L_1^+ such that

$$P_r \circ L_1 = P_r \circ L_1^+.$$

Then L_1^+ and L_2 gives us an equivalent set of secret keys which we can use to forge a signature. This defeats the scheme.

3.5. **The complexity of the attack on Sflash^{v3}.** We know that the attack complexity is determined by the process of solving a set of $66,991,089$ equations with $66,991,089 + 736 + 1$ variables and the rest of computations can be ignored if we compare it with this step. Because solving a set of n equations with n variables is of a complexity proportional to n^3 including addition and multiplication, we then know that our attack complexity is definitely less than $(66,991,089 + 736 + 1)^3 < 2^{78}$. Therefore we conclude that the attack complexity is less than 2^{80}.

However, one difficulty remains. We know that we have to work with around 67 million equations with around 67 million variables. Requesting memory for that many equations is not very practical. We need to investigate how to implement this efficiently for example with the help of sparse matrices.

3.6. **Testing.** We have tested our method with much smaller k, n and r and with $n/r > 6$. In this case our method worked as we predicted.

4. Conclusion

In this paper, we used ideas from the attack method of Kipnis and Shamir on the Hidden Field Equation [KS]. We reformulated the problem to find the secret keys of Sflash into a problem of solving a set of quadratic equations and further into a more standard problem in linear algebra about bilinear forms. Then we used the weakness caused by the constant term of the secret affine linear transformation to find a large set of linear equations satisfied by the secret keys. Applying the linearization method by Patarin, we have shown that defeating the scheme Sflash^{v3} has a complexity less than 2^{80}. However our attack may require a huge memory.

One interesting fact is that our method does not work well on Sflash^{v2}. In this case the linearization method would not work due to the fact that the ratio n/r is only around 3.4. We believe our method in general works as long as n/r is large ($n/r > 6$).

On the other hand, we see that attacking Sflash family can be transformed into a problem as stated in Lemma 4. This new problem looks like a very standard problem concerning bilinear forms over finite fields with characteristic 2, whose solution might be known already. The subtlety of the problem comes from the requirement of the special form for Ψ. Very recently, we discovered some very interesting mathematical structure related to this new problem, and we are currently in the process of testing another new attack method. This new method should be a more efficient method than the one in this paper, though we do not know for sure if it will work.

At this moment we feel that the idea of [KS] of transforming a problem in a vector space over a finite field k into a problem over a bigger field K, is a very powerful but not well understood idea. It seems that the Matsumoto-Imai-Minus family of the cryptosystems has too rigid a structure due to Lemma 4, and we start to doubt that any practical scheme from the Matsumoto-Imai-Minus family of the cryptosystems can remain to be secure no matter how one chooses the parameters k, n, r and θ.

References

[CKPS] Courtois, Nicolas; Klimov, Alexander; Patarin, Jacques; Shamir, Adi *Efficient algorithms for solving overdefined systems of multivariate polynomial equations.* Advances in cryptology—EUROCRYPT 2000 (Bruges), 392–407, LNCS, 1807, Springer, 2000.

[CGP] Nicolas Courtois, Louis Goubin, Jacques Patarin, *FLASH, a Fast Multivariate Signature Algorithm*, LNCS 2020, pp 0298.

[CGP1] Nicolas Courtois, Louis Goubin, Jacques Patarin, *SFLASH, a Fast Asymmetric Signature Algorithm*, http://www.minrank.org/sflash/

[KS] Kipnis, Aviad; Shamir, Adi *Cryptanalysis of the HFE public key cryptosystem by relinearization.* Advances in cryptology—CRYPTO '99 (Santa Barbara, CA), 19–30, LNCS, 1666, Springer, 1999.

[MI] Matsumoto, T., Imai, H., *Public quadratic polynomial-tuples for efficient signature-verification and message-encryption*, Advances in cryptology—EUROCRYPT '88 (Davos, 1988), 419–453, LNCS, 330, Springer, Berlin, 1988.

[N] http://www.cosic.esat.kuleuven.ac.be/nessie.

[P] Patarin, J., *Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88.*, Advances in cryptology – Crypto'95, LNCS, 248-261.

[P1] Patarin, J., *Hidden filed equations (HFE) and isomorphism of polynomials (IP); two new families of asymetric algorithms* , Eurocrypto'96, 1996, LNCS, 33-48,

[S] Shamir, A., *Efficient signature schemes based on birational permutations*, Advances in crytology – CRYPTO '93, (Santa Barbara, CA, 1993), LNCS, 773, 1-12, Springer, 1993.

Department of Mathematical Sciences, University of Cincinnati, Cincinnati, OH, 45220, USA