On the Affine Transformations of HFE-Cryptosystems and Systems with Branches

Patrick Felke *

CITS Research Group
Ruhr-University Bochum
D-44780 Bochum
Patrick.Felke@ruhr-uni-bochum.de

Abstract

We show how to recover the affine parts of the secret key for a certain class of HFE-Cryptosystems. Further we will show that any system with branches can be decomposed in its single branches in polynomial time on average. The first part generalizes the result from [1] to a bigger class of systems and is achieved by a different approach. Despite the fact that systems with branches are not used anymore (see [11, 6]), our second result is a still of interest, as it shows that branches belong to the list of algebraic properties, which cannot be hidden by composition with the secret affine transformations. We derived both algorithms by considering the cryptosystem as objects from the theory of nonassociative algebras and applying classical techniques from this theory. This general framework might be useful for future investigations of HFE-Cryptosystems or to generalize other attacks known so far.

1 Introduction

At Eurocrypt'88 Imai and Matsumoto (see [7]) proposed a promising cryptosystem called C^* based on multivariate polynomials, especially useful for smartcards. To speed up computation and to enhance security, they introduced the idea of branches. C^* was broken independently by Dobbertin in '93 (unpublished, see [4, 5]) and by Patarin in '95 (see [11]). To repair these systems Dobbertin studied bijective power functions of higher degree, whereas Patarin introduced the HFE-Cryptosystem and also variants of it with branches (see [11, 12, 13]). The disadvantage of the latter systems is, if an attacker is able to separate the branches, he also benefits from the speed up, because he can attack the single branches separately.

*The work described in this paper has been supported in part by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT. The information in this document reflects only the author's views, is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

In the beginning probabilistic polynomial time attacks to separate the branches were only known for very special systems like C^*. Later more general probabilistic attacks with exponential running time (exponential in the size of the branches, see [6, 11]) were discovered. As a consequence only systems with branches of moderate size could be considered secure. Thus the speed up of computation was no longer given and such systems were not used anymore. As only small branches could be recovered in general, it was from a theoretical point of view still an open question, if branches can be hidden by the HFE-principle, i.e. by composition with the secret affine transformations. In Section 4 we consider this question from the perspective of nonassociative algebras. This will yield to an algorithm to recover the branches for an arbitrary system in polynomial time on average and thus proving that the answer is no.

Section 3 of this paper is concerned with the secret affine transformations used to construct the trapdoor. It is an open problem, if the security is affected when linear mappings are chosen instead of affine mappings. At first we briefly describe what we understand by eliminating the affine parts. Then by applying classical techniques from the theory of nonassociative algebras we show, that the affine parts can be eliminated for certain class of HFE-systems, including systems like Sflash. This generalizes the result in [1], but we make use of a different approach.

2 Preliminaries

We assume that the reader is familiar with the theory of finite fields and multivariate polynomials as it can be found in [10] for example. In the following we briefly sum up some facts about HFE-Cryptosystems and representations of mappings over finite fields. A detailed description about encryption and signing with HFE-Cryptosystems can be found in [11, 13]. More details about representations of mappings are given in [8] and in the extended version of this paper.

With $\mathbb{F}_q$, $q = p^m$, we denote the finite field of characteristic p and with $\mathbb{F}_{q^n}$ the extension of degree n. We will often consider $\mathbb{F}_{q^n}$ as an n-dimensional $\mathbb{F}_q$-vector space and via a choice of a basis we will identify it with the vector space $\mathbb{F}_q^n$. Elements $(a_1, \ldots, a_n)$ of $\mathbb{F}_q^n$ will often be denoted by $\underline{a}$. Any mapping over $\mathbb{F}_{q^n}$ can be uniquely represented by a polynomial

$$P(X) = \sum_{i=0}^{q^n-1} a_i X^i,$$

and of course every such polynomial $P(X)$ induces a mapping by $a \mapsto P(a), a \in \mathbb{F}_{q^n}$. Any mapping from $\mathbb{F}_q^n$ into $\mathbb{F}_q^n$ can be uniquely represented by a vector of polynomials

$$(p_1(x_1, \ldots, x_n), \ldots, p_n(x_1, \ldots, x_n)),$$

with the property, that if a monomial $\beta x_1^{l_1} \cdots x_n^{l_n}$ occurs in p_k, then $l_i < q$ for $i = 1, \ldots, n$. We will call such a vector reduced. Of course, as above, every such a vector induces a mapping.

For any choice of a basis $b_1, \dots, b_n$ of $\mathbb{F}_{q^n}$, there exists for every mapping F over $\mathbb{F}_{q^n}$ a unique mapping $f = (f_1, \dots, f_n)$ over $\mathbb{F}_q^n$ with

$$F(a) = F(\sum_{i=1}^{n} \alpha_i b_i) = \sum_{i=1}^{n} f_i(\underline{\alpha}) b_i$$

and vice versa.

Thereby the unique polynomial $P(X)$ of degree $d \le q^n - 1$ with $F(a) = P(a)$ is called the univariate representation of F. The uniquely determined reduced vector $(p_1(\underline{x}), \dots, p_n(\underline{x}))$ with $f(\underline{a}) = (p_1(\underline{a}), \dots, p_n(\underline{a}))$ is called the multivariate representation of F.

We define the degree of a vector of polynomials as $\max\{\deg(p_i) | i = 1, \dots, n\}$. With this definition the above correspondence is degree preserving in the sense, that if the univariate representation has degree d, then the multivariate representation has degree q-weight of d. Thereby the q-weight is the number of non-zero elements in the q-adic representation of d. Affine mappings on $\mathbb{F}_q^n$ will be as usual denoted by $A\underline{x} + \underline{c}$, where A denotes an $n \times n$-matrix, $\underline{x} = (x_1, \dots, x_n)$ and $\underline{c} \in \mathbb{F}_q^n$. To keep the description in the rest of this paper as simple as possible, we consider the result of a matrix-vector-multiplication as a row vector and thus as the multivariate representation of an affine mapping.

Now we very briefly describe a basic HFE-Cryptosystem with branches. The secret key consists of:

1. $n = n_1 + \dots + n_l$, a partition of n.

2. Field extensions $\mathbb{F}_{q^{n_k}}$ over a fixed base field $\mathbb{F}_q$ for $k = 1, \dots, l$. The fields will be represented by the choice of an irreducible polynomial $\mathbb{F}_q[X]$ to construct $\mathbb{F}_{q^{n_k}}$ and an $\mathbb{F}_q$-basis, which determines the isomorphism between $\mathbb{F}_q^{n_k}$ and $\mathbb{F}_{q^{n_k}}$.

3. l HFE-polynomials of degree d_k, that is polynomials of the form $H_k(X) = \sum_{i,j=0}^{n-1} \beta_{ij,k} X^{q^i+q^j} + \sum_i \alpha_{i,k} X^{q^i}$,
   where $\beta_{ij,k}, \alpha_{i,k} \in \mathbb{F}_{q^{n_k}}, k = 1, \dots, l$.

4. Two affine bijective transformations $S = A\underline{x} + \underline{c}, T = B\underline{x} + \underline{d}$ of $\mathbb{F}_q^n$.

This constitutes the secret key. The public key is derived by computing the multivariate representation for each of the H_k denoted by

$$\begin{array}{lcl}
(h_1(x_1, \dots, x_{n_1}), & \dots & , h_{n_1}(x_1, \dots, x_{n_1})) \\
(h_{n_1+1}(x_{n_1+1}, \dots, x_{n_1+n_2}), & \dots & , h_{n_1+n_2}(x_{n_1+1}, \dots, x_{n_1+n_2})) \\
 & \vdots & \\
(h_{n-n_l+1}(x_{n-n_l+1}, \dots, x_n), & \dots & , h_n(x_{n-n_l+1}, \dots, x_n))
\end{array} \qquad (1)$$

Each of these n_i-tuples constitutes a branch. Combining these n_i-tuples gives an n-tuple of polynomials $(h_1, \dots, h_n)$ in n variables. The public key $(p_1, \dots, p_n)$ is given by the composition $T \circ (h_1, \dots, h_n) \circ S$ and consists of n quadratic polynomials in n variables. This implies that the base field $\mathbb{F}_q$ is public. Note, that the polynomials in different branches have different sets of variables and these are mixed up by S, T.

The following diagram describes the encryption scheme via composition of mappings defined on the field extensions, i.e. computing $(p_1(\underline{a}), \ldots, p_n(\underline{a}))$ is equivalent to applying the composition of the mappings in the diagram to $\underline{a}$. This different point of view is important for our analysis. Thereby Ψ denotes the canonical isomorphism from $\mathbb{F}_q^n$ into $\mathbb{F}_q^{n_1} \times \cdots \times \mathbb{F}_q^{n_l}$ and ϕ_i the canonical isomorphism from $\mathbb{F}_q^{n_i}$ into $\mathbb{F}_{q^{n_i}}$ given by the chosen basis.

$$
\begin{array}{ccccccccccccccc}
 & & & & \mathbb{F}_q^{n_1} & \xrightarrow{\phi_1} & \mathbb{F}_{q^{n_1}} & \xrightarrow{H_1} & \mathbb{F}_{q^{n_1}} & \xrightarrow{\phi_1^{-1}} & \mathbb{F}_q^{n_1} & & & & \\
 & & & \overset{\Psi}{\nearrow} & & & & & & & & \overset{\Psi^{-1}}{\searrow} & & & \\
\mathbb{F}_q^n & \xrightarrow{S} & \mathbb{F}_q^n & & \vdots & & & & & & \vdots & & \mathbb{F}_q^n & \xrightarrow{T} & \mathbb{F}_q^n \\
 & & & \searrow & & & & & & & & \nearrow & & & \\
 & & & & \mathbb{F}_q^{n_l} & \xrightarrow{\phi_l} & \mathbb{F}_{q^{n_l}} & \xrightarrow{H_l} & \mathbb{F}_{q^{n_l}} & \xrightarrow{\phi_l^{-1}} & \mathbb{F}_q^{n_l} & & & &
\end{array}
$$

Now it becomes apparent, that if an attacker is able to recover the branches, he is able to attack every branch separately.
A basic HFE-Cryptosystem is a system where $l = 1$. The nowadays proposed schemes are variants of this basic system as for example Sflash or Quartz (see [3, 2]). In some descriptions the univariate polynomials have a constant term. Since these can be captured by T, we skipped it in our description (see also the next section). In the sequel the multivariate and univariate representations are considered with respect to the bases chosen by the designer. For our attacks we do not need to know these bases since we will show, that all necessary information can be computed from the public key.

Now we are going to show how to construct a nonassociative $\mathbb{F}_q$-algebra from an HFE-Cryptosystem. This will be the foundation for the algorithms presented later. By a nonassociative $\mathbb{F}_q$-algebra $\mathcal{U}$ we understand an $\mathbb{F}_q$-vectorspace with a multiplication, which is so that

$$\lambda(xy) = (\lambda x)y = x(\lambda y) \text{ for all } \lambda \in \mathbb{F}_q, x, y \in \mathcal{U},$$

and which is also bilinear (i.e. $(x+y)z = xz + yz, z(x+y) = zx + zy$). The associative law is not being assumed. An introduction to this subject can be found in [14].
Given an HFE-Polynomial $H(X) = \sum_{i,j=0}^{n-1} \beta_{ij} X^{q^i+q^j} + \sum_{i=0}^{n-1} \alpha_i X^{q^i}$ we define a multiplication on $\mathbb{F}_{p^n}$ as follows:

$$M(a, b) := H(a+b) - H(a) - H(b).$$

Since M is given by the sum $\sum_{i,j=0}^{n-1} \beta_{ij}(a^{q^i} b^{q^j} + b^{q^i} a^{q^j})$ this multiplication induces indeed an nonassociative and commutative algebra. Again we can derive n polynomials m_i in $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$, which give the multivariate representation of the mapping M. This is achieved similar to the univariate case, but here we have the defining relation

$$M(\sum_{i=1}^{n} \alpha_i b_i, \sum_{i=1}^{n} \beta_i b_i) = \sum_{i=1}^{n} m_i(\underline{\alpha}, \underline{\beta}) b_i,$$

where $b_1, \ldots, b_n$ is a basis of $\mathbb{F}_{q^n}$. If L_1, L_2 are linear mappings over $\mathbb{F}_{q^n}$, then

$$M'(a,b) := L_2(M(L_1(a), L_1(b)) \text{ induces a second algebra.}$$

We will see, that the multivariate representation of M' can be calculated from the public key by computing $p_i(\underline{x}+\underline{y}) - p_i(\underline{x}) - p_i(\underline{y})$, even when the secret transformations S, T are affine (see Section 4).

3 Eliminating the Affine Parts of S,T

Recall that a polynomial $q(x_1, \ldots, x_n)$ is called homogeneous of degree d, if all monomials that occur have degree d. We start with a lemma, which is crucial for our algorithm. It shows that the affine parts of S, T are not mixed up properly by the application of S, T, when the polynomial $H(X)$ is also homogenous in the sense, that all monomials have the form $\beta_{ij} X^{q^i + q^j}$.

Lemma 1. *Let $\mathbb{F}_q \neq \mathbb{F}_2$. Further let $S(\underline{x}) = A\underline{x} + \underline{c}, T(\underline{x}) = B\underline{x} + \underline{d}$ be bijective affine mappings over $\mathbb{F}_{q^n}$ with univariate representation $L_1 + c, L_2 + d$ and $H(X) = \sum_{i,j=0}^{n-1} \beta_{ij} X^{q^i+q^j}$.*
If $p_1, \ldots, p_n$ denotes the public key of the resulting cryptosystem, then $p_i(\underline{x}) = q_i(\underline{x}) + l_i(\underline{x}) + a_i$, where a_i is a constant, l_i is linear and q_i is homogeneous of degree 2. Furthermore $(q_1, \ldots, q_n)$ is the multivariate representation of $L_2 \circ H \circ L_1$.

Remark 2. The restriction for fields with $q = 2^m$ is necessary, as otherwise the equality $x^2 = x$ would destroy the graduated structure and the representation of $L_2 \circ H \circ L_1$ could not be recovered.

Proof. The proof is given in the full version of this paper. □

In this extended abstract we restrict to a simple case with one branch, i.e. a basic HFE-Cryptosystem with a simple hidden polynomial. The details for the general case will be given in the full version of this paper. We will state the general result of the full version at the end of this section.
We will show how to eliminate the affine parts of S, T, if the base field is $\mathbb{F}_{2^m}$, where $m > 2$ and $H(X) = \beta X^{q^i+q^j}, i \neq j$. By eliminating we understand that we will compute $\underline{d}$ and $A^{-1}(\underline{c})$. From this it is easy to transform the system $T \circ (h_1, \ldots, h_n) \circ S$ into $B \circ (h_1, \ldots, h_n) \circ A$. Note, that if $(\underline{y}, \underline{x})$ is a plaintext/ciphertext pair of the first system, then $(\underline{y} - \underline{d}, \underline{x} + A^{-1}(\underline{c}))$ is the corresponding pair of the second one and vice versa. This implies, that plaintext/ciphertext-attacks can be carried out over the second system.
Without loss of generality we assume that $H(X) = X^{q^i+1}, i \neq 0$. Otherwise consider $((L_2 + d) \circ (\beta X^{q^j})) \circ (X^{q^{n-j}} \circ (X^{q^i+q^j})) \circ (L_1 + c)$, which gives an equivalent system, i.e. a system with different S,T but exactly the same public key and a hidden polynomial of the desired form. From the latter composition it is easy to see, why we could skip the constant in the general description of HFE-systems.

We have $M(a,b) = a^{q^i} b + b^{q^i} a$. A natural question in the theory of nonassociative algebras is to look for all annihilating elements, i.e. for all mappings $M(a, \cdot)$ or $M(\cdot, a)$ (the so called left or right multiplications), which vanish on $\mathbb{F}_{q^n}$. We begin with a simple lemma. As M and M' are commutative we only have to consider left multiplications.

Lemma 3. *Let $i \notin \{0, n\}$.*

1. *If $M(a,b) = a^{q^i} b + b^{q^i} a = 0$ for all $b \in \mathbb{F}_{q^n}$, then $a = 0$.*

2. *If the characteristic of $\mathbb{F}_{q^n}$ is 2, then the kernel of the mapping $M(a,\cdot)$ is $a\mathbb{F}_{q^{gcd(i,n)}}$ for $a \neq 0$.*

3. *If $M'(a,b) = 0$ for all $b \in \mathbb{F}_{q^n}$, then $a = 0$ for all bijective linear mappings L_1, L_2 over $\mathbb{F}_{q^n}$.*

4. *If the characteristic of $\mathbb{F}_{q^n}$ is 2, then the kernel of the mapping $M'(a,\cdot)$ is $L_1^{-1}(L_1(a)\mathbb{F}_{q^{gcd(i,n)}})$ for $a \neq 0$.*

Proof. The proof will be given in the full version of this paper. $\square$

Now we will show for our special case how to relate the problem of eliminating the translations to the problem of finding annihilating elements.

The public polynomials are the multivariate representation of $P(X) := (L_2 + d) \circ X^{q^i} X \circ (L_1 + c)$. Hence we can compute the multivariate representation of

$$P(X+Y)+P(X) = L_2(L_1(X)^{q^i} L_1(Y)+L_1(Y)^{q^i} L_1(X)+L_1(c)^{q^i} L_1(Y)+L_1(Y)^{q^i} L_1(c))$$

$$+L_2(L_1(Y)^{q^i} L_1(Y)).$$

Using Lemma 1 gives the multivariate representation of the last term $L_2(L_1(Y)^{q^i} L_1(Y))$ from the public key. So we can eliminate this term by subtracting it. This way we get the multivariate representation of

$$L_2(L_1(Y)^{q^i}(L_1(X)+c) + L_1(X+c)^{q^i} L_1(Y)) = M'(X + L_1^{-1}(c), Y).$$

From Lemma 3 we have that $M'(a + L_1^{-1}(c), Y)$ is the zero mapping iff $a = L_1^{-1}(c)$. This yields straightforward to the following algorithm to eliminate the translations:

1. Compute the multivariate representation of $M'(a + L_1^{-1}(c), Y)$ by computing $p_i(x_1 + y_1, \ldots, x_n + y_n) + p_i(x_1, \ldots, x_n)$ and then eliminate the multivariate part describing $L_2(L_1(Y)^{q^i} L_1(Y))$. This gives n polynomials $q_i(x_1, \ldots, x_n, y_1, \ldots, y_n)$.

2. Compute $q_i(\underline{x}, e_1)$ for $i = 1, \ldots, n$, where e_1 denotes the first canonical basis vector $e_1 = (1, 0, \ldots, 0)$. This gives an inhomogeneous system of n linear equations. If it has rank n, the unique solution is $A^{-1}(\underline{c})$. If the rank is $< n$, add the next n equations $q_i(\underline{x}, e_2)$ and so on, until rank n is reached. The unique solution is the vector $A^{-1}(\underline{c})$.

3. Once $c' := A^{-1}(\underline{c})$ is computed, compute $p'_i(\underline{x}) = p_i(\underline{x} + \underline{c}')$ for all i. This gives the multivariate representation of $(L_2 + d) \circ X^{q^i} X \circ L_1$.

4. Compute $p'_i(\underline{0})$ for all i. This gives the vector $\underline{d}$ and $\underline{d}$ can as well be eliminated.

Obviously this algorithm is dominated by the running time for the Gaussian elimination. We have to solve a system with at most n^2 linear equations in n variables. Hence the running time is $O(n^4)$.

This idea generalizes to an attack for base fields of arbitrary characteristic (details are given in the full version) and yields to the following result.

Theorem 4. *Given an arbitrary HFE-Cryptosystem, or a "−"-system like Sflash, over a field* $\mathbb{F}_q \neq \mathbb{F}_2$ *with secret affine transformations* $S = A\underline{x} + \underline{c}$ *and* $T = B\underline{x} + \underline{d}$, *then* $\underline{c}, \underline{d}$ *can be eliminated with* $O(n^4)$ *field operations on average.*

4 A Fast Algorithm for Separating the Branches

In [11] and [12] a probabilistic polynomial time algorithm to separate the branches is described assuming the underlying HFE-polynomials admit special syzygies. The algorithm is based on the Coppersmith-Patarin attack on Dragon-Schemes (see [12]). If again $S(\underline{x}) = A\underline{x} + \underline{c}, T(\underline{x}) = B\underline{x} + \underline{d}$ denote the affine transformations, the crucial step of the attack is the computation of matrices $C = A\Lambda A^{-1}$ and $C' = B^{-1}\Lambda B$, where

$$\Lambda = \begin{pmatrix} \Lambda_1 & 0 & 0 & \cdots & 0 \\ 0 & \Lambda_2 & 0 & \cdots & 0 \\ \vdots & 0 & \Lambda_3 & \cdots & 0 \\ \vdots & \vdots & 0 & \ddots & 0 \\ 0 & 0 & \cdots & 0 & \Lambda_l \end{pmatrix}.$$

Thereby l denotes the number of branches and Λ_k denotes the representation matrix of a linear mapping $x \mapsto \lambda_k x, \lambda_k \in \mathbb{F}_{q^{n_k}}$, where $\mathbb{F}_{q^{n_k}}$ is the field belonging to the k-th branch and $k \in \{1, \ldots, l\}$.
Then from C a matrix G is derived, such that

$$AG = \begin{pmatrix} W_1 & 0 & 0 & \cdots & 0 \\ 0 & W_2 & 0 & \cdots & 0 \\ \vdots & 0 & W_3 & \cdots & 0 \\ \vdots & \vdots & 0 & \ddots & 0 \\ 0 & 0 & \cdots & 0 & W_l \end{pmatrix}, \text{ where } W_i \text{ is a block matrix.}$$

From this the separation is rather straightforward. We present here a variant, which makes no use of C'. The reason for this is given in Remark 6 and 8. As mentioned in Section 2, for all l branches there exists a unique set of variables

$$V_k = \{x_{\sum_{j=1}^{k-1} n_j + 1}, \ldots, x_{\sum_{j=1}^{k} n_j}\}, k = 1, \ldots, l.$$

At first compute $p'_i(\underline{x}) := p_i(G\underline{x})$ for $i = 1, \ldots, n$. The polynomials p'_i have the property, that if $x_s x_t$ is a monomial occuring in p'_i then x_s, x_t are elements of a set V_k. Thus the monomials in p'_i reveal the different sets of variables and can be grouped by using a proper monomial order. After that apply Gaussian elimination to $p'_1, \ldots, p'_n$ to derive the desired polynomials, where the first n_1 polynomials have

only variables from V_1, the next n_2 polynomials have variables from the set V_2 and so on. This completes the separation.
It might happen that the composition with G does not reveal all branches, but more clusters of branches. In this case the clusters are attacked separately afterwards, and the separation is refined step by step. To compute G classical linear algebra related to the theorem of Cayley-Hamilton is needed. In this extended abstract we skip the details, but refer the reader to Shamir's attack on the Oil&Vinegar-Schemes [9] and to [11, 12] for a nice introduction to the tools needed to overcome this task.

To generalize this attack, we consider the key idea from the perspective of nonassociative algebras. From this point of view the crucial step is to determine a *mixed multiplication centralizer* of a proper multiplication, i.e. the mixed centralizer of this multiplication has to contain many pairs of matrices (C', C), where C has properties as above. In the following we show how the multiplications M and M' from Section 2 extend to systems with branches. Then we introduce the notion of *mixed centralizer* and show, that the multiplication is proper.
For every field $\mathbb{F}_{q^{n_k}}$ we have a multiplication $M_k(a,b), k = 1, \ldots, l$. We get the desired multiplication $M(a,b)$ on $\mathbb{F}_{q^n}$ as follows. We consider the multiplication on $\prod_{k=1}^{l} \mathbb{F}_{q^{n_k}}$ defined by

$$((a_1, \ldots, a_l), (b_1, \ldots, b_l)) \mapsto (M_1(a_1, b_1), \ldots, M_b(a_l, b_l)).$$

The multiplication M on $\mathbb{F}_{q^n}$ is given by $\Psi^{-1} \circ M_1 \times \cdots \times M_l \circ \Psi$, where Ψ is the embedding of $\mathbb{F}_{q^n}$ into the product of fields. With $(m_1, \ldots, m_n)$ we denote the multivariate representation of M. The multiplication M' on $\mathbb{F}_{q^n}$ is given by $M'(a,b) := L_2(M(L_1(a), L_2(b)))$. The polynomials

$$m'_i(\underline{x}, \underline{y}) := p_i(\underline{x} + \underline{y}) - p_i(\underline{x}) - p_i(\underline{y})$$

are the multivariate representation of M'. If S, T are affine it is easy to see, that we get the representation by skipping the constant parts after the computation of $p_i(\underline{x} + \underline{y}) - p_i(\underline{x}) - p_i(\underline{y})$. This becomes apparent, if one computes $P(X+Y) - P(X) - P(Y)$ as in section 3.
A well known object in the theory of nonassociative algebras is the *multiplication centralizer*. In our situation we have to generalize this notion. We consider the *mixed multiplication centralizer*, which is given by all linear mappings C, C' fulfilling

$$C'(m'_1(\underline{x}, \underline{y}), \ldots, m'_n(\underline{x}, \underline{y})) = (m'_1(\underline{x}, C\underline{y}), \ldots, m'_n(\underline{x}, C\underline{y})).$$

This can also be written as

$$C'B(m_1(A\underline{x}, A\underline{y}), \ldots, m_n(A\underline{x}, A\underline{y})) = B(m_1(A\underline{x}, AC\underline{y}), \ldots, m_n(A\underline{x}, AC\underline{y})). \quad (2)$$

From this it is easy to see, that if C, C' solve the equation (2), then $ACA^{-1}, B^{-1}C'B$ solve

$$Z'((m_1, \ldots, m_n)) = (m_1(\underline{x}, Z\underline{y}), \ldots, m_n(\underline{x}, Z\underline{y})), \quad (3)$$

and if Z, Z' solve (3), then $A^{-1}ZA, BZ'B^{-1}$ solve equation (2). Hence the solutions are conjugated to each other. The centralizer of M' can be computed from the public key with Gaussian elimination, when the elements c_{ij}, c'_{ij} are set as unknowns and plaintext/ciphertext pairs are plugged in to get equations in the unknowns. Now we analyze the mixed centralizer and show that it has the desired property. We start with a special case.

Theorem 5. *Given the base field $\mathbb{F}_{2^m}$. Let M be the multiplication as above derived from univariate polynomials $H_k = X^{2^{mi_k}+1}$, where $i_k \notin \{0, n_k\}$ and $gcd(2^{mi_k}+1, 2^{n_k}-1) = 1$ for $k = 1, \ldots, l$. Then the centralizer consists of all pairs $(A^{-1}ZA, BZB^{-1})$, where Z is the representation matrix of the mapping*

$$a \mapsto \Psi^{-1}((\lambda_1 \cdot \Psi(a)_1, \ldots, \lambda_l \cdot \Psi(a)_l)),$$

$a \in \mathbb{F}_{q^n}$ and $\lambda_k \in \mathbb{F}_{2^{m\,gcd(i_k,n_k)}}$ for $k = 1, \ldots, l$.

Proof. The proof is simple but rather technical, so we skip the details here. □

Understanding the centralizer of an arbitrary HFE-Cryptosystem with branches is a hard problem. But it is easy to see, that all block matrices Z, where every block Λ_k represents a multiplication with an element from the base field $\mathbb{F}_q$, lie in the centralizer of M. It is very likely and confirmed by our experiments, that these are the only elements when $H(X)$ is not as simple as above. Thus we have the following reasonable conjecture.

Conjecture 1. The elements C of the centralizer for an arbitrary system with l branches are the matrices $A^{-1}ZA$ with

$$Z = \begin{pmatrix} \Lambda_1 & 0 & 0 & \cdots & 0 \\ 0 & \Lambda_2 & 0 & \cdots & 0 \\ \vdots & 0 & \Lambda_3 & \cdots & 0 \\ \vdots & \vdots & 0 & \ddots & 0 \\ 0 & 0 & \cdots & 0 & \Lambda_l \end{pmatrix}.$$

Thereby Λ_k denotes the representation matrix of a multiplication with $\lambda_k \in \mathbb{F}_q$.

Remark 6. The conjecture does not state anything about C'. As C' is only needed to compute C but not to complete the actual separation, no further knowledge about the structure is necessary.

The separation requires the factorization of the characteristic polynomial of C. Assuming Conjecture 1 the matrices C can be diagonalized with only a few possible Eigenvalues. Consequently the factorization is feasible.
The number of recovered branches depends on the number of different Eigenvalues. If only clusters of branches are recovered, the algorithm can be applied separately to the different clusters. We have the following result.

Theorem 7. *The branches for an arbitrary system can be recovered with $O(n^6)$ field operations on average.*

Remark 8. For base fields $\mathbb{F}_{2^m}$ a faster variant of the algorithm is possible, because in this case it is possible to compute C without C'. The details can be found in the full version.

References

[1] T. Beth, W. Geiselmann, R. Steinwandt: Revealing 441 Key Bits of SFLASHv2, Nessie Workshop Munich, November 2002

[2] Nicolas Courtois, Louis Goubin, Jacques Patarin: Quartz, 128-bit long digital signatures, Cryptographers' Track Rsa Conference 2001, LNCS 2020, pp.282-297, Springer-Verlag

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

[4] H. Dobbertin: internal report 93/94, German Information Security Agency

[5] H. Dobbertin: Analysis of HFE Schemes Based on Power Functions, invited talk at YACC '02, 03-07 June, 2002

[6] Louis Goubin, J. Patarin: Improved algorithms for Isomorphisms of Polynomials, Eurocrypt '98, Springer-Verlag

[7] H. Imai, T. Matsumoto: Public Quadratic Polynomial-tuples for efficient signature-verification and message-encryption, Eurocrypt '88, Springer-Verlag

[8] A. Kipnis, A. Shamir:Cryptanalysis of the HFE Public Key Cryptosystem by Relinearisation, Crypto '99, Springer-Verlag

[9] A. Kipnis, A. Shamir: Crypanalysis of the Oil&Vinegar Signature Scheme, Crypto '98

[10] R. Lidl, H. Niederreiter: Finite Fields, Encyclopedia of Mathematics and its Applications, Vol. 20, 2nd Edition, Cambridge University Press, Cambridge, 1997

[11] J. Patarin: Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt '88, Crypto '95, Springer-Verlag

[12] J. Patarin: Asymmetric Cryptography with a Hidden Monomial, Crypto '96, Springer Verlag

[13] J. Patarin: Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP), Eurocrypt '96, Springer Verlag

[14] R. Schafer: Introduction to Nonassociative Algebras, Academic Press, 1966