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

Patrick Felke

Department of Mathematics
Ruhr-University Bochum
D-44780 Bochum
Patrick.Felke@ruhr-uni-bochum.de

17th December 2004

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 build on 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. Dispite the fact that systems with branches are not used anymore (see [10, 6]), our second result is a still of interest as it applies to a very general class of HFE-cryptosystems and thus is a contribution 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-Cryptosysstems or to generalize other attacks known so far.

1 Introduction

At Eurocrypt'88 Imai and Matsumoto proposed a promising Cryptosystem called C^* based on multivariate polynomials, especially useful for smart cards. To speed up computation and to enhance the security, they introduced the idea of branches. The basic system was broken independently by Dobbertin in '93 (unpublished, see [4, 5]) and by Patarin in '95 (see [10]). To repair these systems Dobbertin studied bijective power functions of higher degree, whereas Patarin introduced the HFE-Cryptosystem and variants of it with branches (see [10, 11, 12]). Probabilistic polynomial time attacks to separate the branches are only known for special cases, all other attacks are exponential in the size of the branches (see [6, 10]). If an attacker is able to

separate the branches, he also benefits from the speed up, because he can attack the single branches separately.
As a consequence only systems with large branches could be considered to be secure. Thus the speed up of computation was no longer given and such systems were not used anymore. We will show that the situations is even more worse. We will give an algorithm to recover the branches for an arbitrary system in polynomial time on average and thereby proving that branches cannot be hidden by the HFE-principle at all, i.e. by composition with the secret affine transformations.

Section 3 of this paper will be concerned with the secret affine transformations used to construct the trapdoor. It is still an open problem, if the security is affected when linear mappings are chosen instead of affine mappings. In [1] it was shown, that the affine parts can be eliminated for the Sflash-Signature system. Toli proposed in [14] to change to an equivalent system, where the affine parts are combined with the hidden polynomial. We will show, that the affine parts can be eliminated for certain HFE-systems, including systems like Sflash, without affecting the hidden polynomial, i.e. keeping the same hidden polynomial and changing from affine to linear mappings.

2 Preliminaries

We assume that the reader is familiar with the theory of finite fields and multivariate polynomials as can be found in for example [9]. 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-systems can be found in [10, 12]. More details about representation of mappings are given in [7] 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 on $\mathbb{F}_{q^n}$ can be uniquely represented by a polynomial

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

and of course 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 restriction, 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 such a vector induces a mapping.

For any choice of a basis $b_1, \ldots, b_n$ of $\mathbb{F}_{q^n}$, there exists for every mapping F over $\mathbb{F}_{q^n}$ a unique mapping $f = (f_1, \ldots, f_n)$ 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 $d \leq q^n - 1$ with $F(a) = P(a)$ is called the univariate representation of F. The uniquely determined reduced vector $(p_1(\underline{x}), \ldots, p_n(\underline{x}))$ with $f(\underline{a}) = (p_1(\underline{a}), \ldots, p_n(\underline{a}))$ is called the multivariate representation of F.

If we set the degree of a vector of polynomials as $\max\{\deg(p_i) | i = 1, \ldots, n\}$, then 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 usually denoted by $A\underline{x} + \underline{c}$, where A denotes an $n \times n$-matrix, $\underline{x} = (x_1, \ldots, x_n)$ and $\underline{c} \in \mathbb{F}_q^n$. To keep the description in the rest of the paper as simple as possible, we interprete the result of a matrix-vector-multiplication as a row vector again. This convention fits to concept of the multivariate representation, which is written as a row vector.

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

1. A base field $\mathbb{F}_q$.
2. $n = n_1 + \cdots + n_l$, a partition of n.
3. Field extensions $\mathbb{F}_{q^{n_k}}$ for $k = 1, \ldots, l$. 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 $\mathbb{F}_{q^{n_k}}$.
4. l HFE-polynomials of degree d_k, that is polynomials of the form $H_k(X) = \sum_{i,j}^{n-1} \beta_{ij,k} X^{q^i + q^j} + \sum_i \alpha_{i,k} X^{q^i}$,
   where $\beta_{ij,k}, \alpha_{i,k} \in \mathbb{F}_{q^{n_k}}, k = 1, \ldots, l$.
5. 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

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

This gives an n-tuple of polynomials $(h_1,\ldots,h_n)$ in n variables. The public key $(p_1,\ldots,p_n)$ is given by the composition $T\circ(h_1,\ldots,h_n)\circ S$ and consists of n quadratic polynomials in n variables. 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 apply the composition of the mappings in the diagram onto $\underline{a}$. 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.

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

Now it becomes apparent, that if an attacker is able to recover the branches, then he can attack every branch separately.
A basic HFE-system is a system where $l=1$. The nowadays proposed systems are variants of this basic system as for example Sflash or Ouartz (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 above chosen bases. An attacker does not need to know these bases, as we will show that he can compute all necessary information directly from the public key.

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

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

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 [13].
Given an HFE-Polynomial $H(X) = \sum_{i,j}^{n-1} \beta_{ij=0} X^{q^i+q^j} + \sum_{i=0}^{n-1} \alpha_i X^{q^i}$ 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 $\sum_{ij=0}^{n-1} \beta_{ij}(a^{q^i}b^{q^j} + b^{q^i}a^{q^j})$ this multiplication induces indeed a commutative but not necessarily associative algebra in the above sense. Again we can again 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 on $\mathbb{F}_{q^n}$, then $M'(a,b) := L_2(M(L_1(a), L_1(b))$ 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 are of 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 from $\mathbb{F}_{q^n}$ 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, q_i is homogeneous of degree 2 and $(q_1, \ldots, q_n)$ is the multivariate representation of $L_2 \circ H \circ L_1$.

The restriction for fields with $q = 2^m$ is necessary, as otherwise the equality $x^2 = x$ would destroy the graduaded structure and the representation of $L_2 \circ H \circ L_1$ could not be recovered. 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.
Now we will show how to eliminate the affine parts of S, T, when the base field is $\mathbb{F}_q$ with $q = 2^m > 2$ and $H(X) = \beta X^{q^i+q^j}, i \neq j$.
Let the notation be as in the lemma. W.log. we can 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, that means a system with different S,T but exactly the same public key and a hidden polynomial of the desired form. From the notation above it is easy to see, why we could skip the constant in the general description of HFE-systems.

For $H(X)$ as above $M(a,b) = a^{q^i}b + b^{q^i}a$. A natural question in the theory of 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.

Lemma 2. *If $M(a,b) = a^{q^i}b + b^{q^i}a = 0, \forall b \in \mathbb{F}_{q^n}$, then $a = 0$. If the characteristic of $\mathbb{F}_{q^n}$ is 2, then the kernel of the mapping $M(a,\cdot) = M(\cdot,a)$ is $a\mathbb{F}_{q^{gcd(i,n)}}$ for $a \neq 0$. The same is true for the second multiplication M'. The kernel for given $a \neq 0$ is then $L_1^{-1}(L_1(a)\mathbb{F}_{q^{gcd(i,n)}})$.*

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

Now we will show how to relate the problem of computing the translations to the problem of finding annihilating elements.

Recall, that here 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 $P(X + Y) + P(X) =$

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

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

An application of lemma 1 shows, that we can compute the multivariate representation of the last term $L_2(L_1(Y)^{q^i}L_1(Y))$ from the public key, so that we can eliminate this term by subtracting it. 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 2 we have that $M'(a + L_1^{-1}(c), Y)$ is the zero mapping iff $a = L_1^{-1}(c)$. From this it is straight forward to eliminate both translations. We note down the algorithm:

1. Compute the multivariate representation of $M'(a+L_1^{-1}(c), Y)$ by computing $p_i(x_1, \ldots, x_n + y_1, \ldots, y_n) + p_i(x_1, \ldots, x_n)$ 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 together with the second part of lemma 2 extends to an attack for base fields of arbitrary characteristic (details are given in the full version) and yields to the following result.

Theorem 3. *Given an arbitrary HFE-system, 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 [10] and [11] a probabilistic polynomial time algorithm to separate the branches is described, when the underlying HFE-polynomials admit special syzygies. The idea was based on the Coppersmith-Patarin attack on Dragon-Schemes (see [11]). From the theory of algebras the idea was to compute all linear mappings C, C' in a kind of mixed multiplication centralizer. If again $S(\underline{x}) = A\underline{x} + \underline{c}, T(\underline{x}) = B\underline{x} + \underline{d}$ denote the affine tranformations, the main step was to compute 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 is l the number of branches, Λ_k the representation matrix of the linear mapping $x \mapsto \lambda_k x$ and λ_k an element of $\mathbb{F}_{q^{n_k}}$, the field belonging to the k-th branch.

If once such a matrix is computed the variables can be separated or the branches can be recovered, respectivley. All necessary steps to overcome this task are described in Shamir's attack on the Oil&Vinegar-Schemes [8] and in [10, 11]. Furthermore one can show, that the matrix C' is not needed to separate the branches. More details are given in the full version of this paper. So the only problem left over is to find the matrix C with the properties as above and we are done. This is what we are going to show in the sequel for a system with l branches.
For every field $\mathbb{F}_{q^{n_k}}$ we have a multiplication $M_k(a,b), k = 1,\ldots,l$. Hence we have a 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

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

Thus the multiplication 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. We get a second multiplication M' on $\mathbb{F}_{q^n}$ 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 desired representation, if we just skip 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. With $(m_1,\ldots,m_n)$ we denote the multivariate representation of M.
A natural object in the theory of algebras is to consider the multiplication centralizer. Here in our situation we will consider the so-called mixed 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 be also written as

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

From this we see, that if C, C' solve the above equation, then $ACA^{-1}, B^{-1}C'B$ is a solution of

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

and if Z, Z' solve the latter equation, then $A^{-1}ZA, BZ'B^{-1}$ solve the above equation. Hence the solutions are conjugated to each other and they 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. We start with a special case.

Theorem 4. *Let $\mathbb{F}_q = 2^m, m \leq 2$. Let M be the multiplication as above derived from univariate polynomials $H_k = X^{q^{i_k}+1}, i_k \neq 0$, where $gcd(2^{mi_k} + 1, 2^{n_k} - 1) = 1$ 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*

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

and $\lambda_k \in \mathbb{F}_{2^{mgcd(i_k,n_k)}}, a \in \mathbb{F}_{q^n}$.

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

To understand the centralizer for an arbitrary HFE-system is a hard problem. It is easy to see, that matrices representing multiplications with elements from the base field $\mathbb{F}_q$ lie in the centralizer. It is very likely and confirmed by our experiments, that these are the only elements, if $H(X)$ is not as simple as above. Thus we have the following reasonable conjecture for the matrices C.

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 $\lambda_k \in \mathbb{F}_q$.

To complete the separation the factorization of the characteristic polynomial of C is needed. Assuming the above conjecture we see, that C can be diagonalized with only a few possible Eigenvalues. Thus the factorization can be computed very fast for an arbitrary system with branches.
How many branches are recovered depends on the number of different Eigenvalues. If only clusters of branches are recovered, the algorithm can be applied separately on the different clusters. For characteristic 2 a speed up of the algorithm is possible. The details can be found in the full version. We have the following result.

Theorem 5. *The branches for an arbitrary system can be recovered with $O(n^6)$ field operations on average.*

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: invited talk at YACC'02

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

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

[8] A. Kipnis, A. Shamir: Crypanalysis of the Oil&Vinegar Signature Scheme,

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

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

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

[12] J. Patarin: Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP), Eurocrypt'96, Springer Verlag, pages 33-48

[13] R. Schafer: Introduction to Nonassociative Algebras

[14] I. Toli: Cryptanalysis of HFE, June 2003, arXiv,preprint server, http://arxiv.org/abs/cs.CR/0305034