Key Recovery on Hidden Monomial Multivariate Schemes

Pierre-Alain Fouque[1], Gilles Macario-Rat[2], and Jacques Stern[1]

[1] École normale supérieure,
45 rue d'Ulm, 75005 Paris, France
{Pierre-Alain.Fouque, Jacques.Stern}@ens.fr
[2] Orange Labs
38–40, rue du Général Leclerc, 92794 Issy les Moulineaux Cedex 9, France
Gilles.Macariorat@orange-ftgroup.com

Abstract. In this paper, we study the key recovery problem for the C^* scheme and generalisations where the quadratic monomial of C^* (the product of two linearized monomials) is replaced by a product of three or more linearized monomials. This problem has been further generalized to any system of multivariate polynomials hidden by two invertible linear maps and named the Isomorphism of Polynomials (IP) problem by Patarin. Some cryptosystems have been built on this apparently hard problem such as an authentication protocol proposed by Patarin and a traitor tracing scheme proposed by Billet and Gilbert. Here we show that if the hidden multivariate system is the projection of a quadratic monomial on a base finite field, as in C^*, or a cubic (or higher) monomial as in the traitor tracing scheme, then it is possible to recover an equivalent secret key in polynomial time $O(n^d)$ where n is the number of variables and d is the degree of the public polynomials.

1 Introduction

Multivariate cryptography provides alternative schemes to RSA or DLog based cryptosystems where the underlying hard problem consists of solving a system of multivariate equations over a finite field. This problem is known to be NP-hard [13]. Moreover it seems to be interesting to build cryptosystems based on the assumption that it is hard, since contrary to the factorisation or the DLog problem, there is actually no known polynomial-time quantum algorithm to solve it, and generic algorithms that use Gröbner basis are exponential in time and memory. Finally, the proposed cryptosystems are very efficient in practice and can be implemented on low-cost smartcards since arithmetic on large integer is not required. Consequently, at the end of the nineties, a lot of multivariate cryptosystems were proposed.

One rich family of multivariate scheme is derived from a cryptosystem proposed by Matsumoto and Imai since 1988 and called C^*. Even though this scheme was broken by Patarin in 1995 [18], Patarin proposed various repairs. One of these repairs is the Minus transformation, suggested by Shamir in [23], which is a classical solution to avoid Patarin's or Gröbner basis attack. The SFLASH signature scheme, accepted by the NESSIE project in 2003, is a C^* scheme with this variation. Recently, SFLASH has been attacked by Dubois *et al.* in [7, 6]. However, the attacks were not able to recover the secret key, as they rely on Patarin's attack which is *only* able to invert the public key.

The IP Problem. The corresponding key recovery problem, named the IP Problem, which stands for the Isomorphism of Polynomials has been introduced by Patarin since 1996 in [20] and studied later by Patarin, Goubin and Courtois in [22]. It can be stated as follows: given two sets of n polynomials in n variables A, B over a finite field $\mathbb{K}$ of q elements, find if there exist two linear and invertible mappings S and T in $\mathbb{K}$ such that $A = T \circ B \circ S$. This problem is not NP-hard provided the polynomial hierarchy does not collapse as proved by Faugère and Perret in [10]. However, if we relax S and T to be *any* linear mapping, then the problem is called MP, Morphism of Polynomials, and becomes NP-hard as shown in [22]. Finally, this problem is interesting since many Substitution Permutation Network block ciphers use as SBoxes a high degree monomial such as x^{254} in $GF(256)$ for the AES. Consequently, recovering the key for one round of the AES is equivalent to solve a special instance of the IP Problem, where the system B consists in 8 polynomials coming from a high degree monomial projected on $GF(2)$ and copied 16 times.

1.1 Related Work

Our method for solving the IP problem is not generic but is tailored to work for some cryptographic instances such as C^* based schemes or the traitor tracing scheme of [2]. For these cases, the algorithm is very efficient since it uses only linear algebra. The first step of our attack is similar to the recent attacks on SFLASH which can be extended to high degree monomials. In this case, we define high order differentials which have also been used in the cryptanalysis of symmetric schemes [16, 15, 14].

Previous Attacks on the IP problem. It is obvious that guessing S allows us to solve this problem since we can then compute the T function on some points and check whether it is a bijective linear mapping in time $O(n^3 q^{n^2})$.

If each polynomials of B only depends on a *small* number of variables such as 8 among the n in the case of the AES SBox, then polynomial time algorithms exist such as those described by Biryukov and Shamir in [4] or by Biham in [1].

However, when n is sufficiently large and each polynomial of B depends on many variables, the best known algorithm proposed so far by Patarin *et al.* has a complexity of $O(n^3 q^n)$. This last algorithm is very similar to the one proposed by Biryukov *et al.* in [3] in the context of linear equivalence problem for arbitrary permutations. In the case of SFLASH, where the set B is the projection of a quadratic monomial defined over $\mathbb{F}$ an extension of degree n of $\mathbb{K}$, then the Patarin *et al.* best algorithm has a complexity in $O(q^{n/2})$.

At Eurocrypt' 06, Faugère and Perret describe a Gröbner basis algorithm to solve the IP problem when B is a set of polynomials defined over a small number n of variables in an extension $\mathbb{F}$. Their algorithm is very efficient when the system of polynomials B is *random* and has small degree terms such as in the authentication scheme proposed by Patarin and some parameters of the traitor tracing scheme of Billet and Gilbert. However, for larger parameters proposed by Billet and Gilbert or for the parameters of SFLASH, the algorithm does not work. Their algorithm considers only terms of small degree in the system of polynomials so that the system they defined in the unknowns of S and T will be overdetermined. The complexity of this algorithm is dominated by the computation of a Gröbner basis for which we do not have complexity bound reflecting the practical behaviour. So, they conjecture that the complexity depends on the smallest value d so that there exists terms of degree d in B. For high degree monomial, as in the cases we consider in this paper, this parameter is exactly the degree of the monomials.

Differential Attack on SFLASH. As our attack relies on some information gained during the recent attacks on SFLASH, we informally describe here how they work.

Recently, some breakthrough results have been published on the cryptanalysis of the SFLASH signature scheme by Dubois *et al.* in [7, 6]. SFLASH comes from the C^* family, *i.e.* the internal quadratic monomial of the form $P(x) = x^{1+q^\theta}$ over an extension $\mathbb{F}$ of degree n of the base finite field $\mathbb{K}$ is hidden by two linear bijective mappings S and T. The public key is $\mathbf{P} = T \circ P \circ S$ and if some polynomials of the public key are removed, we get a SFLASH public key. In [7], the authors consider the case where $\gcd(\theta, n) > 1$.

The basic idea of [14, 7, 6] is to recover some of these polynomials or equivalent polynomials by noticing that the internal polynomial $P \circ S$ over $\mathbb{F}$ forms a set of n polynomials over $\mathbb{K}$. Then, the action of T consists of linear combination of these n polynomials. Consequently, if we are able to recover other linear combinations of these polynomials with independent coefficients, we will be able to recover a complete public key.

The last results show that it is possible to reconstruct equivalent missing polynomials using only 3 polynomials of the public key. The way to do it is to reconstruct some special linear applications related to the secret S, of the form $N_u = S^{-1} M_u S$ so that M_u denotes the multiplications by u in $\mathbb{F}$. In [7], it is shown that the maps N_u where u are solutions of $x^{q^\theta} + x = 0$ are easy to recover using a linear characterization, whereas in [6], more involved analysis are needed. However, this last attack is more powerful since any multiplication can be recovered. Then, the composition of these maps N_u with the public key $\mathbf{P}$ is of the form $T \circ P \circ M_u \circ S$ and since P is multiplicative, $\mathbf{P} \circ N_u$ is of the form $T' \circ P \circ S$ and if T' contains rows independent of those of T, then we get new polynomials of the public key which will be independent from the first ones. Finally, once the public key is recovered, Patarin's attack can be applied.

Consequently, in this paper we can assume that no equation is removed.

1.2 Our Results

In this paper, we show that the recent attacks on multivariate schemes can be made more devastating and lead to total break of the C^* schemes family. More precisely, we show that the IP problem for C^* is easy and we can recover secret keys S and T or equivalent can be recovered given a $N_u = S^{-1}M_uS$ linear mappings. Indeed, these matrices depend on the secret S, but M_u are unknown. Here, we show how we can recover u and then, how we can recover S' and T'. This last step is not always easy and when $\gcd(n, \theta) > 1$, many parasitic solutions can exist. For the SFLASH signature scheme, the recent attacks rely on Patarin's attack in their final stage. However, this attack can become exponential in some bad cases. Here, our attack on the C^* schemes family is always polynomial to recover the secret key and can be seen as a new attack on the C^* scheme.

Moreover, we show that for high degree monomials, we can also recover the matrices N_u as in the case of the quadratic monomials of SFLASH and recover the secret keys. To get a linear characterization of N_u, we use high order differentials as an analog to symmetric cryptanalysis. These two results improve on a result of Faugère and Perret at Eurocrypt '06 using Gröbner basis [10] which solves only some particular cases but not all the proposed parameters by Billet and Gilbert. For the C^* case, Faugère and Perret indicate that their approach cannot take into account SFLASH parameters since the system of polynomials is too sparse. Here, we only present polynomial time attack to recover these values for SFLASH and the second parameter proposed by Billet and Gilbert in the case of the traitor tracing scheme [2].

1.3 Organization of the Paper

In section 2 we present the problem Isomorphism of Polynomials which represents the key recovery problem in multivariate schemes. Then, we present the differential of the public key which allows to give a characterization of the interesting linear mappings we are looking for. Then, we show how to solve the IP problem when the internal polynomial is a monomial in section 4. In section 5, we show that the SFLASH public key can be recovered in all cases and on monomial of higher degree of the traitor tracing scheme before the conclusion.

2 Isomorphisms of Polynomials Problem (IP)

In this section, we present the Isomorphism of Polynomials problem stated by Patarin *et al.* in [20, 22]. It has been used by Billet and Gilbert in [2] to define a traitor tracing scheme.

2.1 Description of the IP Problem

The IP Problem is defined for any two sets A, B of n multivariate polynomials and the problem is to find S and T two linear and bijective maps on n variables so that $A = T \circ B \circ S$. In this paper, we focus on special instances of this problem when the system B is the projection on the base field $\mathbb{K}$ of a polynomial defined over an extension of degree n of $\mathbb{K}$.

Let $\mathbb{K}$ be a small finite field of q elements and $\mathbb{F}$ an extension of degree n over $\mathbb{K}$. Let π be an isomorphism from $\mathbb{K}^n$ onto $\mathbb{F}$ and P some polynomial over $\mathbb{F}$. Then, let S and T be two linear or affine invertible transformations over $\mathbb{K}^n$. The maps S and T are kept secret. Finally let $\mathbf{P} = T \circ \pi^{-1} \circ P \circ \pi \circ S$ be a set of n polynomial forms over $\mathbb{K}^n$. This system of multivariate polynomials $\mathbf{P}$ is also named the public key. The problem can now be expressed as follows:

IP Problem. *Given $\mathbb{K}$, n, P, and $\mathbf{P}$ defined as above, find S' and T' affine transformations over $\mathbb{K}^n$ and π' isomorphism from $\mathbb{K}^n$ onto an extension of degree n of $\mathbb{K}$ such as:*

$$\mathbf{P} = T' \circ \pi'^{-1} \circ P \circ \pi' \circ S'.$$

Remark 1. The choice of π' is indifferent. Indeed, should we choose $\tilde{\pi}$, then there exists some change of coordinates such that $\varphi = \tilde{\pi}^{-1} \circ \pi'$. If (T', S', π') is a solution, then $(\tilde{T} = T' \circ \varphi^{-1}, \tilde{S} = \varphi \circ S', \tilde{\pi})$ is another solution.

In the sequel, by some misuse of language, we avoid writing the isomorphism π and its inverse π^{-1} when their use is obvious and simply write $\mathbf{P} = T \circ P \circ S$.

IP with Polynomials. In this article, we mainly study the case where P is a monomial of the form $P(x) = x^{1+q^{\theta_1}+\ldots+q^{\theta_{d-1}}}$ defined over an extension field $\mathbb{F}$ of degree n of $\mathbb{K}$. If we project this monomial over the base field $\mathbb{K}$, we get n multivariate polynomial of degree d since the mappings $x \mapsto x^{q^i}$ for integers i are $\mathbb{K}$-linear. Consequently, the changes between the public key $\mathbf{P}$ and the internal polynomial P are changes of variables, which do not modify the degree of the multivariate polynomials.

2.2 Equivalent Keys

Solutions to the IP Problem are in fact not unique. See [24] for a discussion about equivalent keys. For instance, let's analyze the case $P(x) = x^{1+q^\theta}$. Let's note M_u (multiplications) and φ_i (Frobenius) defined by $M_u(x) = ux$ and $\varphi_i(x) = x^{q^i}$. So if (T', S') is a solution then so are

$$(T' \circ \pi^{-1} \circ M_{1/u^{q^\theta+1}} \circ \pi, \pi^{-1} \circ M_u \circ \pi \circ S') \text{ and } (T' \circ \pi^{-1} \circ (\varphi_i)^{-1} \circ \pi, \pi^{-1} \circ \varphi_i \circ \pi \circ S').$$

3 Differential and Properties for Monomials

The differential of the public key of a multivariate scheme has been introduced in a systematic cryptanalytic method by Fouque *et al.* in [11]. Later, this method has been developed and extended in [8, 9, 7, 6] to attack various systems.

3.1 Differential of Polynomials

For a general polynomial P, the differential in some point a, denoted by D_aP, is formally defined by:

$$D_aP(x) = P(x+a) - P(x) - P(a) + P(0).$$

We may also refer it as $DP(x,a)$ which is symmetric since $D_aP(x) = D_xP(a)$. The later notation also represents the fact that the differential is a bilinear expression and consequently, it can be represented by a matrix. In our case, all polynomials of the public key can be represented as a bilinear mapping.
The interest of studying the differential is that it "lowers" the degree and it is homogeneous. For instance, if $\deg(\mathbf{P}) = 2$ then $\deg(D_a\mathbf{P}) = 1$ and $D_a\mathbf{P}$ is linear. In this case, the differential acts as it "kills" the parts of degree 1 and 0 of $\mathbf{P}$.

Differential of Monomials of Higher Degree. For higher degrees, we may define differentials of higher order. For instance, if $\deg(\mathbf{P}) = 3$: $D_{a,b}P(x) = D_a(D_bP(x))$ defines a second order differential and $\deg(D_{a,b}\mathbf{P}(x)) = 1$. We may also note it $DP(a,b,x)$ for the same reason as previously.

Differential of the Public Key. Let us study how the differential operates on the public key. We assume here that $P(x) = x^{1+q^\theta}$. First, if S and T are linear, then we have

$$D_a\mathbf{P}(x) = T(D_{S(a)}P(S(x))) \tag{1}$$

Taking into Account the Affine Parts. If S and T are affine, we denote by Σ_c the addition with c. With this notation, we have: $(P \circ \Sigma_c)(x) = P(x) + xc^{q^\theta} + x^{q^\theta}c + P(c)$. Now, we can easily express that $D_a(P \circ \Sigma_c)(x) = D_aP(x)$, since $xc^{q^\theta} + x^{q^\theta}c + P(c)$ is affine. Since $S(x) = DS(x) + S(0)$ and $P \circ S = P \circ \Sigma_{S(0)} \circ DS$, we deduce a similar relation: $D_a\mathbf{P}(x) = DT(D_{DS(a)}P(DS(x)))$. So, the previous relation is just like relation (1) where S and T are replaced by their linear part DS and DT.

3.2 Multiplicative Property of the Differential

In this section, we show that a characterization equation exists for hidden monomials that involves a linear mapping N. Since the equation is linear in the unknown of N and depends only on the public key, N can be easily found.

Multiplicative Property for SFLASH. For $P(x) = x^{1+q^\theta}$ there is an interesting property of the differential:

$$D_xP(M_u(y)) + D_yP(M_u(x)) = M_{u+u^{q^\theta}}(D_yP(x)) \tag{2}$$

where M_u is the multiplication by u in $\mathbb{F}$. We can also rewrite this equation as $DP(xu, y) + DP(x, yu) = (u + u^{q^\theta})DP(x, y)$. How is this property (2) transfered to the public system? Firstly for the sake of simplicity, we may assume that S and T are linear. Otherwise, we will see that considering only their linear part is a good approach when they are affine.

If we denote by N_u the conjugate by S of M_u, namely $N_u = S^{-1} \circ M_u \circ S$, property (2) becomes:

$$\begin{aligned} D_x\mathbf{P}(N_u(y)) + D_y\mathbf{P}(N_u(x)) &= T(M_{u+u^{q^\theta}}(D_{S(y)}F(S(x)))) \\ &= (T \circ M_{u+u^{q^\theta}} \circ T^{-1})(D_y\mathbf{P}(x)) \end{aligned} \tag{3}$$

If we consider the vector space of symmetric bilinear forms such that $b(x, x) = 0$ of dimension $n(n-1)/2$, then the bilinear forms of the left hand side are in the vector space V spanned by the bilinear forms of the differential of the public key $D_y\mathbf{P}(x)$ of dimension n. This equation is linear in the n^2 unknowns of N_u and stating that one quadratic form of the LHS is in this vector space gives $n(n-1)/2$ linear equations and n additional unknowns. Therefore, expressing that 3 forms of the LHS are in V is sufficient to completely determine N_u.

Multiplicative Property for Higher Degree. For degree 3 or 4, similar expressions for this property can be derived, by considering respectively:

$$D_{x,y}\mathbf{P}(N_u(z)) + D_{x,z}\mathbf{P}(N_u(y)) + D_{y,z}\mathbf{P}(N_u(x)), \tag{4}$$

$$D_{x,y,z}\mathbf{P}(N_u(v)) + D_{x,y,v}\mathbf{P}(N_u(z)) + D_{x,z,v}\mathbf{P}(N_u(y)) + D_{y,z,v}\mathbf{P}(N_u(x))). \tag{5}$$

In case (4), we get trilinear forms and the multiplication by $u + u^{q^\theta}$ is replaced by $u + u^{q^{\theta_1}} + u^{q^{\theta_2}}$ for degree 3 and by $u + u^{q^{\theta_1}} + u^{q^{\theta_2}} + u^{q^{\theta_3}}$ for degree 4.

Multiplicative Property is a Characterization. The property (2) and the ones infered for higher degree are a characterization. Indeed the only linear mappings M and M' satisfying:

$$D_xP(M(y)) + D_yP(M(x)) = M'(D_yP(x)) \tag{6}$$

are the multiplications.

The idea of the proof is that the $\mathbb{K}$-linear applications over $\mathbb{F}$ can be expressed as linearized polynomials such as $M(x) = \sum_{i=0}^{n-1} \lambda_i x^{q^i}$ where coefficients λ_i belong to $\mathbb{F}$. By replacing this expression in equation (6), provided that n is large enough, all coefficients λ_i must be null except λ_0. Hence the result $M(x) = \lambda_0 x$.

Remark 2. This result is true only if n is not too close to d. When n is too small, there is a side effect that allows linear applications other than multiplications to be solution of equation (6). Experimentally, we have found the lower limit of n according to d. For $d = 2$ and $d = 3$, we must have $n \geq 5$. For $d = 4$, we must have $n \geq 7$.

4 Recovering S and T

The basic idea to recover equivalents for S and T is to find some N_u and use equation: $N_u = S^{-1}M_uS$. If we can recover u, then M_u is known and we can linearized it to $SN_u = M_uS$, where S is the unknown we are looking for.

Description of the Attack. In the following, we describe the different steps of the attack to recover equivalent S and T.

1. Find all linear transformations L such as $D_x\mathbf{P}(L(y)) + D_y\mathbf{P}(L(x))$ is a set of bilinear forms, all of them being linear combinations of the elements of $D_y\mathbf{P}(x)$. Due to the characterization, the space of solutions is the conjugate by S of the multiplications.
2. Pick up at random one solution L which characteristic polynomial is irreducible over $\mathbb{K}$.
3. Find u such as L and M_u are conjugate. Since L and M_u must have the same characteristic polynomial, choose u as any root of the characteristic polynomial of L. Since characteristic polynomial is irreducible over K, roots are primitive elements of $\mathbb{F}$.
4. Solve the linear system $X.L = M_u.X$ where the unknown X is a linear mapping of $\mathbb{K}^n$.
5. Pick up at random any non trivial solution S.
6. Compute T as $\mathbf{P} \circ S^{-1} \circ P^{-1}$.

Recovering $\boldsymbol{L}$. In [7, 6], it is described how the first step of this attack can be mounted since systems in step 1 is overdefined. Consequently, only a few coordinates of $D_y\mathbf{P}(x)$ are sufficient to solve it. This is the same reason why the "Minus" scheme of SFLASH can be defeated even if some public polynomial are removed.

It is also possible to reconstruct S and T even though they are affine. The computations are the same, but we replace $\mathbf{P}$ by $D\mathbf{P}$. At steps 5 and 6, we can find actually the linear parts of S and T, that is DS and DT. Then, using equation:

$$(DT)^{-1} \circ D\mathbf{P}(x) = D(F \circ S)(x) = (DS(x))^{1+q^\theta} + (DS(x))^{q^\theta} S(0) + DS(x)S(0)^{q^\theta}$$

replace x by random values, in order to gain enough linear independent equations, all of the form $ay^{q^\theta} + by + c = 0$, and find the solution $S(0)$. Then, compute $T(0) = \mathbf{P}(0) - (DT \circ P \circ S)(0)$.

Recovering $\boldsymbol{M_u}$. To recover M_u, we first show how we recover u. Since L is the conjugate of M_u by the secret matrix S, they are similar and so, they have the same minimal polynomial. Furthermore, u is a root of the minimal polynomial of M_u [3]. Indeed, if Π is the minimal polynomial of M_u, then $\Pi(M_u) = 0$ and so

[3] In fact, one can prove that u and M_u have the same minimal polynomial.

$\Pi(ux) = 0$ for all x, and so $\Pi(u) = 0$ for $x = 1$. Moreover, it is also well-known that the roots of a minimal polynomial are conjugates, *i.e.* are the elements $\{u, u^q, u^{q^2}, \ldots, u^{q^{n-1}}\}$. This result can be easily seen since the coefficients of the minimal polynomial belong to $\mathbb{F}_q$, and for any element α of $\mathbb{F}_q$, we have $\alpha^{q^i} = \alpha$, thus for the minimal polynomial p of u, $p(u^{q^i}) = p(u)^{q^i} = 0$. The conjugate property stands also for matrices, since $M_u = (\varphi_q^i)^{-1} M_{u^{q^i}} \varphi_q^i$, where $\varphi_q^i(x) = x^{q^i}$ is the ith frobenius map. Therefore, even though we do not choose the right conjugate, since the frobenius application commutes with the internal monomial, we will always find equivalent secret keys. So, once L is known, it suffices to select any of the roots of its minimal polynomial as value for u.

Equivalent Keys and Space of Solutions. At step 1, solutions should be a subspace of dimension n, isomorphic to $\mathbb{F}$, since it is the conjugate by S of the space of multiplication matrices. For instance, trivial solutions are diagonal matrices which correspond to elements of $\mathbb{K}$. So at this step we just need to select any matrix corresponding to a multiplication by a primitive element of $\mathbb{F}$. At step 3, roots of the characteristic polynomial are conjugate, since it is irreducible over $\mathbb{K}$ and its coefficients belong to $\mathbb{K}$. Thus selecting u^{q^i} instead of u is equivalent to multiply the solutions by φ_i. At step 5, solutions can be obtained from a particular one, by multiplying it by any multiplication matrix M_u.

Remark 3. In the wording of the IP problem, we can assume that P is unknown, only its degree is known, since the number of monomials of a given degree is small.

5 Applications

The following experimental results have been obtained with an Opteron 850 2.2GHz, with 32 GBytes of Ram. The systems associated with the instance of the problems and their solutions have been generated using the Magma software, version 2.13-15.

If the following tables, t_{gen} is the time for computing the coefficient of the problem, mainly the linear application that gives $D_x\mathbf{P}(L(y)) + D_y\mathbf{P}(L(x))$ for any L, at step 1, t_{sol} is the time for solving the problem, which is basically a linear algebra issue, regarding intersection of subspaces. 's.' and 'm.' denote respectively second and minute.

5.1 SFLASH Signature Scheme

The following results concern a general instance of the IP problem for an homogeneous C*scheme of degree 2, that is we are looking for linear S and T. Nevertheless, this is almost the problem of key recovery for the SFLASH Signature scheme, where some coordinates (equations) are missing, since finding M_u enables to regenerate missing coordinates.

q	d	n	t_{gen}	t_{sol}
2^{16}	2	19	0.4 s.	0.5 s.
2^{16}	2	21	0.6 s.	1 s.
2^7	2	37	6 s.	23 s.
2	2	67	55 s.	10 s.
2^7	2	67	60 s.	12 m.

The first row corresponds to the second challenge of Billet and Gilbert. Faugère and Perret in [10] were unable to solve it and conjectured that the system was too sparse. Moreover, row 3 and 5 correspond to the practical instances of SFLASH v2 and SFLASH v3. In this case, the number of variables is too large and Gröbner basis algorithm cannot take into account such parameters. However, contrary to [10], our approach can only deal with internal system of multivariate scheme coming from the projection of a monomial and not any polynomials. In the case of SFLASH parameters, we do not give the value r of the removed equations since previous attacks [7, 6] can always be used to recover missing polynomials of the public key.

5.2 Traitor Tracing of Billet and Gilbert

Here as above, the results concern a general instance of the IP problem for an homogeneous C* scheme, but of degree 3 and 4. The change was in the use of the expressions (4), and (5).

q	d	n	t_{gen}	t_{sol}	θ_1	θ_2	θ_3
2^9	3	10	0.6 s.	0.1 s.	1	4	
2^9	3	18	12 s.	5 s.	1	6	
2^9	3	19	15 s.	7 s.	1	4	
2^9	3	20	20 s.	11 s.	1	4	
2^9	3	21	26 s.	15 s.	1	6	
2^{16}	4	7	0.2 s.	0.2 s.	1	2	6
2^{16}	4	8	0.65 s.	0.4 s.	1	3	7
2^{16}	4	9	1.4 s.	0.3 s.	1	2	7
2^8	4	10	11 s.	8 s.	1	3	5
2^8	4	11	19 s.	44 s.	1	2	6
2^8	4	12	32 s.	80 s.	1	2	10

In these experiments, we give the values of θ_1, θ_2 and θ_3 such that the monomials can be inverted and so that there is no intermediate finite field of $\mathbb{F}$, *i.e.* $\gcd(\theta_1, \theta_2, n) = 1$. We can remark that from $n = 7$ for $d = 4$, we can solve the IP problem for monomials more efficiently than [10]. These results confirm experimentally the complexity of the resolution of the problem, namely $O(\log(q)^2 n^d)$. We can finally remark that the degree d is exactly the heuristic value given by Faugère and Perret in the case of high degree monomials defined over an extension field.

5.3 The ℓ-IC scheme

At PKC'07, Ding *et al.* presented a new multivariate scheme based on Cremona maps in [5]. This scheme has been attacked at PKC'08 by Fouque *et al.* in [12]. In this attack, the authors are also able to recover equivalent secret keys. The way they recover u consists in raising N_u to some power so that u^α has a small order and then, exhaustive search can be performed. Fortunately, for the proposed parameters, it is always the case. However, if this trick is not possible, our method that computes the minimal polynomial can be done and we get directly the value u. Consequently, we can improve the cryptanalysis of the ℓ-IC scheme.

6 Conclusion

Here, we describe a key recovery attack on the C*schemes family which lead to the recovery of equivalent secret keys. This means that an attacker would be in the same position than a legitimate user. Moreover, this attack is polynomial in time and space, and so it is very practical and can be executed within few seconds on the recommended values of the parameters of the schemes.

Acknowledgements

The first and last authors are very grateful to Adi Shamir and Vivien Dubois for interesting discussions on this subject.

The work described in this paper has been supported by the ANR MAC project and by the European Commission through the IST Program under contract IST-2002-507932 ECRYPT.

References

1. E. Biham. Cryptanalysis of Patarin's 2-Round Public Key System with S Boxes (2R). In *Eurocrypt' 00*, volume 1807 of *Lecture Notes in Computer Science*, pages 408–416. Springer-Verlag, 2000.
2. O. Billet and H. Gilbert. A Traceable Block Cipher. In *Asiacrypt '03*, volume 2894 of *Lecture Notes in Computer Science*, pages 331–346. Springer-Verlag, 2003.
3. A. Biryukov, C. De Cannière, A. Braeken, and B. Preneel. A Toolbox for Cryptanalysis: Linear and Affine Equivalence Algorithms. In *Eurocrypt' 03*, volume 2656 of *Lecture Notes in Computer Science*, pages 33–50. Springer-Verlag, 2003.
4. A. Biryukov and A. Shamir. Structural Cryptanalysis of SASAS. In *Eurocrypt' 01*, volume 2045 of *Lecture Notes in Computer Science*, pages 394–405. Springer-Verlag, 2001.
5. J. Ding, C. Wolf, and B.-Y. Yang. ℓ-Invertible Cycles for Multivariate Quadratic Public Key Cryptography. In *PKC '07*, volume 4450 of *Lecture Notes in Computer Science*, pages 266–281. Springer-Verlag, 2007.
6. V. Dubois, P.-A. Fouque, A. Shamir, and J. Stern. Practical Cryptanalysis of SFLASH. In *Crypto '07*, volume 4622 of *Lecture Notes in Computer Science*. Springer-Verlag, 2007.

7. V. Dubois, P.-A. Fouque, and J. Stern. Cryptanalysis of SFLASH with Slightly Modified Parameters. In *Eurocrypt '07*, volume 4515 of *Lecture Notes in Computer Science*, pages 264–275. Springer-Verlag, 2007.
8. V. Dubois, L. Granboulan, and J. Stern. An Efficient Provable Distinguisher for HFE. In *Icalp' 06*, volume 4052 of *Lecture Notes in Computer Science*, pages 156–167. Springer-Verlag, 2006.
9. V. Dubois, L. Granboulan, and J. Stern. Cryptanalysis of HFE with Internal Perturbation. In *PKC' 07*, volume 4450 of *Lecture Notes in Computer Science*, pages 249–265. Springer-Verlag, 2007.
10. J.-C. Faugère and L. Perret. Polynomial Equivalence Problems: Algorithmic and Theoretical Aspects. In *Eurocrypt' 06*, volume 4004 of *Lecture Notes in Computer Science*, pages 30–47. Springer-Verlag, 2006.
11. P.A. Fouque, L. Granboulan, and J. Stern. Differential Cryptanalysis for Multivariate Schemes. In *Eurocrypt' 05*, volume 3494 of *Lecture Notes in Computer Science*, pages 341–353. Springer-Verlag, 2005.
12. P.A. Fouque, G. Macario-Rat, L. Perret, and J. Stern. Total Break of the ℓ-IC Signature Scheme. In *PKC '08*, volume 4939 of *Lecture Notes in Computer Science*, pages 1–17. Springer-Verlag, 2008.
13. M. R. Garey and D. S. Johnson. *Computers and Intractability, A Guide to the Theory of* NP*-Completeness.* Freeman, New-York, 1979.
14. H. Gilbert and M. Minier. Cryptanalysis of SFLASH. In *Eurocrypt' 02*, volume 2332 of *Lecture Notes in Computer Science*, pages 288–298. Springer-Verlag, 2002.
15. L. R. Knudsen. Truncated and Higher Order Differentials. In *FSE '94*, volume 1008 of *Lecture Notes in Computer Science*, pages 196–211. Springer-Verlag, 1994.
16. X. Lai. Higher order derivatives and differential cryptanalysis. In *Proc. Symposium on Communication, Coding and Cryptography*, 1994.
17. T. Matsumoto and H. Imai. Public Quadratic Polynominal-Tuples for Efficient Signature-Verification and Message-Encryption. In *Eurocrypt '88*, volume 330 of *Lecture Notes in Computer Science*, pages 419–453. Springer-Verlag, 1988.
18. J. Patarin. Cryptoanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88. In *Crypto '95*, volume 963 of *Lecture Notes in Computer Science*, pages 248–261. Springer-Verlag, 1995.
19. J. Patarin. Asymmetric Cryptography with a Hidden Monomial. In *Crypto '96*, volume 1109 of *Lecture Notes in Computer Science*, pages 45–60. Springer-Verlag, 1996.
20. J. Patarin. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In *Eurocrypt '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 33–48. Springer-Verlag, 1996.
21. J. Patarin, N. Courtois, and L. Goubin. FLASH, a Fast Multivariate Signature Algorithm. In *CT-RSA 2001*, volume 2020 of *Lecture Notes in Computer Science*, pages 298–307. Springer-Verlag, 2001.
22. J. Patarin, L. Goubin, and N. Courtois. Improved Algorithms for Isomorphisms of Polynomials. In *Eurocrypt '98*, volume 1403 of *Lecture Notes in Computer Science*, pages 184–200. Springer-Verlag, 1998.
23. A. Shamir. Efficient Signature Schemes Based on Birational Permutations. In *Crypto '93*, volume 773 of *Lecture Notes in Computer Science*, pages 1–12. Springer-Verlag, 1993.
24. C. Wolf and B. Preneel. Equivalent Keys in HFE, C^*, and Variations. In *Mycrypt '05*, volume 3715 of *Lecture Notes in Computer Science*, pages 33–49. Springer-Verlag, 2005.