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] France Télécom R&D
38–40, rue du Général Leclerc, 92794 Issy les Moulineaux Cedex 9, France
Gilles.Macariorat@orange-ftgroup.com

Abstract. The problem we study in this paper is the key recovery problem on the C^* schemes and generalizations where the quadratic monomial of C^* (the product of two linear monomials) is replaced by a product of three or more linear monomials. This problem has been further generalized to any multivariate polynomial hidden by two invertible linear maps and named the Isomorphism of Polynomials (IP) problem by Patarin *et al.* Some cryptosystems have been built on this appearing hard problem such as a traitor tracing scheme proposed by Billet and Gilbert. Here we show that if the hidden multivariate monomial is a quadratic monomial, as in SFLASH, 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 the RSA cryptosystem where the hard underlying problem consists in solving a system of multivariate equations over a finite field. This problem is known to be NP-hard and there is no known polynomial-time quantum algorithm to solve it. Moreover, generic solvers that use Gröbner basis require exponential time and memory.

One rich family of multivariate scheme is derived from a cryptosystem proposed by Matsumoto and Imai since 1988. Even though this scheme was broken by Patarin in [12] since 1995, Patarin proposed various countermeasures to increase the security. One variation is the Minus transformation, suggested by Shamir in [17], and is a classical solution to avoid Patarin's or Gröbner basis attack. The SFLASH signature scheme comes from this variation. Another scheme solution is to use a hidden monomial of higher degree such as in the Traitor Tracing scheme proposed by Billet and Gilbert in [1].

1.1 Related Works

The IP problem. The Isomorphism of Polynomials (IP) problem has been introduced by Patarin since 1996 in [14] to capture the key recovery problem of some multivariate schemes such as C^* since Patarin's attack allows only to inverse the public key and not to recover the secret key. Patarin, Goubin and Courtois investigate the hardness of this problem in [16] and conclude that the best algorithm, called To and Fro, for the C^* family requires exponential time in $O(q^{n/2})$ where q is the size of the base finite field and n is the degree of the extension of the large field.

Biryukov *et al.* propose another solutions to this problem in [2] with complexity $O(n^3 \cdot 2^n)$ over $GF(2)$ which is very efficient when $n \leq 32$. They introduce these algorithms to study linear equivalence of Sbox. For our purpose, n can be 128. In the case of the AES cryptosystem, the Sbox can be viewed as polynomial of high degree, namely 7, since the inverse in $GF(256)$ can be explained as the polynomial $P(x) = x^{q-2}$.

Finally, Faugère and Perret in [8] also studied this problem and conjecture that in some cases, Gröbner basis algorithms are subexponential and give some parameters that they were able to solve.

Differential Attack on SFLASH. Recently, some breakthrough results have been published on the cryptanalysis of the SFLASH signature scheme by Dubois *et al.* in [5, 4]. 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[5], the authors consider the case where $\gcd(\theta, n) > 1$.

The basic idea of [10, 5, 4] is to recover some of these polynomials or of 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 $N_z = S^{-1} M_z S$ so that M_z denotes the multiplications by z in $\mathbb{F}$. In [5], it is shown that the maps N_z where z are the $q^\theta - 1$ roots of unity are easy to recover using a linear characterization, whereas in [4], 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_z with the public key $\mathbf{P}$ is of the form $T \circ P \circ M_z \circ S$ and since P is multiplicative, $\mathbf{P} \circ N_z$ 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 $N_z = S^{-1}M_zS$ linear mappings. Indeed, these matrices depend on the secret S, but M_z are unknown. Here, we show how we can recover z 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 happen. 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 N_z as in the case of the quadratic polynomials of SFLASH and recover the secret keys. These two results improve on a result of Faugère and Perret at Eurocrypt '06 using Gröbner basis [8] 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 $n = 19$ and $n = 37$ in SFLASH over a finite field of 2^7 elements. Moreover, for some parameter they define, they conjecture that their attack is subexponential. Here, we only present polynomial time attack to recover these values.

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 [14, 16]. It has been used by Billet and Gilbert in [1] to define a traitor tracing scheme.

2.1 Description of the IP Problem

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, so to say $P(x) = x^d$ for some integer d and we show polynomial time algorithm for these instances. Degree of P and degree of $\mathbf{P}$ are not simply related. Due to the definition of $\mathbb{K}$ and $\mathbb{F}$, we are interested in some special monomials, namely x^{q^i} for some integers i, which are $\mathbb{K}$-linear. The views of these monomials on $\mathbb{K}^n$, namely $\pi^{-1} \circ x^{q^i} \circ \pi$ are linear transformations over $\mathbb{K}^n$. If we take for instance $P(x) = x^{1+q^\theta}$ for some integer θ, then $\mathbf{P}$ will be a set of quadratic polynomial forms, hence here $\deg(\mathbf{P}) = 2$. In the same manner, for $P(x) = x^{1+q^{\theta_1}+\ldots+q^{\theta_{d-1}}}$, $\deg(\mathbf{P})$ will be at most d.

2.2 Equivalent Keys

Solutions to the IP Problem are in fact not unique. See [18] for a discussion about equivalent keys. For instance, let's analyze the case $P(x) = x^{1+q^\theta}$. Let's note M_z (multiplications) and φ_i (Frobenius) defined by $M_z(x) = zx$ and $\varphi_i(x) = x^{q^i}$. So if (T', S') is a solution then so are

$$(T' \circ \pi^{-1} \circ M_{1/z^{q^\theta+1}} \circ \pi, \pi^{-1} \circ M_z \circ \pi \circ S')$$

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 [9]. Later, this method has been developed and extended in [6, 7, 5, 4] 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:

$$D_a\mathbf{P}(x) = DT(D_{DS(a)}P(DS(x))). \tag{2}$$

So, relation (2) 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:

$$D_x P(M_z(y)) + D_y P(M_z(x)) = M_{z+z^{q^\theta}}(D_y P(x)) \tag{3}$$

where M_z is the multiplication by z in $\mathbb{F}$. We can also rewrite this equation as

$$DP(xz, y) + DP(x, yz) = (z + z^{q^\theta})DP(x, y).$$

How is this property (3) 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_z the conjugate by S of M_z, namely $N_z = S^{-1} \circ M_z \circ S$, property (3) becomes:

$$\begin{aligned} D_x \mathbf{P}(N_z(y)) + D_y \mathbf{P}(N_z(x)) &= T(M_{z+z^{q^\theta}}(D_{S(y)} F(S(x)))) \\ &= (T \circ M_{z+z^{q^\theta}} \circ T^{-1})(D_y \mathbf{P}(x)) \end{aligned} \tag{4}$$

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

$$D_{x,y}\mathbf{P}(N_z(u)) + D_{x,u}\mathbf{P}(N_z(y)) + D_{y,u}\mathbf{P}(N_z(x)), \tag{5}$$

$$D_{x,y,u}\mathbf{P}(N_z(v)) + D_{x,y,v}\mathbf{P}(N_z(u)) + D_{x,u,v}\mathbf{P}(N_z(y)) + D_{y,u,v}\mathbf{P}(N_z(x))). \tag{6}$$

Multiplicative Property is a Characterization. The property (3) and the ones infered for higher degree are indeed a characterization. Indeed the only linear mappings M and M' satisfying:

$$D_x P(M(y)) + D_y P(M(x)) = M'(D_y P(x)) \tag{7}$$

are the multiplications.

[Proof is ...]

However, this result is true only if n is not too close to d. Experimentally, we have tried to find the lower limit of n according to d.

4 Recovering S and T

The basic idea to recover equivalents for S and T is to find some N_z and use equation:

$$N_z = S^{-1} M_z S.$$

If we can recover z, then M_z is known and we can linearized it to:

$$S N_z = M_z S$$

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 z such as L and M_z are conjugate. Since L and M_z must have the same characteristic polynomial, choose z 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 $X.L = M_z.X$ 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 *L*. In [5, 4], 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:

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

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 *z*. Since M_z and L are similar they have the same characteristic and minimal polynomial. Furthermore, z is a root of the minimal polynomial of M_z, since for any polynomial $p \in \mathbb{F}_q[X]$, we have $p(M_z) = M_{p(z)}$. Furthermore, it is also well-known that the roots of a minimal polynomial are conjugates, 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 z, $p(z^{q^i}) = p(z)^{q^i} = 0$. The conjugate property stands also for matrices, since $M_z = (\varphi_q^i)^{-1} M_{z^{q^i}} \varphi_q^i$, where $\varphi_q^i(x) = x^{q^i}$ is the ith frobenius map.

So, once L is known, it suffices to select any of the roots of its minimal polynomial as value for z. Other conjugates would lead to equivalent keys.

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 z^{q^i} instead of z 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_z.

Remark 2. 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.

Remark 3. When n is very close to d, experimentally $n < 5$ for $d = 2$ or $d = 3$, and $n < 7$ for $d = 4$, unfortunately, at step 1, solutions are subspace of dimension greater than n. For greater values of n, dimension of such subspace is n and the attack works.

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.' denotes respectively second and minute.

5.1 SFLASH Signature Scheme

The following results concern a general instance of IP problem of a C*scheme homogeneous of degree 2, so to say 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_z enables to renegerate 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.

In the cases $\gcd(n, \theta) > 1$, there exists parasitic solutions when searching the solution for equation $XL = M_z X$ for z a $q^{\gcd(n,\theta)} - 1$ of the unity. It is easy to show that if we have two solutions for this equation X and X', then $X'X^{-1}$ commutes with M_z. In this case, the idea is to apply the second attack of [4] to reconstruct a conjugate of multiplication where z does not live in a subgroup.

5.2 Traitor Tracing of Billet and Gilbert

Here as above, the results concern a general instance of IP problem of a C*scheme homogeneous, but of degree 3 and 4. The change was in the use of the expressions (5), and (6).

q	d	n	t_{gen}	t_{sol}
2^9	3	10	0.6 s.	0.1 s.
2^9	3	18	12 s.	5 s.
2^9	3	19	15 s.	7 s.
2^9	3	20	20 s.	11 s.
2^9	3	21	26 s.	15 s.
2^8	4	10	11 s.	8 s.
2^8	4	11	19 s.	44 s.
2^8	4	12	32 s.	80 s.

These results confirm experimentally the complexity of the resolution of the problem, namely $\log(q)d^n$. Compare with the results of Faugère and Perret in [8], this is better, since we can handle directly the maximum degree.

6 Conclusion

Here, we describe a key recovery attack on the C*schemes family which lead to recover 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 pratical and can be executed within few seconds on the recommended values of the parameters of the schemes.

References

1. 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.
2. 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.
3. 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.

4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.
19. C. Wolf and B. Preneel. Taxonomy of Public Key Schemes based on the problem of Multivariate Quadratic equations. Cryptology ePrint Archive, Report 2005/077, 2005. http://eprint.iacr.org/.