Overview of Cryptanalysis Techniques in Multivariate Public Key Cryptography

Olivier Billet and Jintai Ding

Abstract This paper summarizes most of the main developments in the cryptanalysis of multivariate cryptosystems and discuss some problems that remain open. A strong emphasis is put on the symbolic computation tools that have been used to achieve these advances.

1 Introduction

The most widely deployed public key cryptosystem nowadays is without any doubt the RSA cryptosystem. Its security is somewhat related to the fact that no reasonably fast algorithm for the factorization of large integers is known up to now. Due to fast developments in the field of integer factorization, a secure public key cryptosystem relying on the assumption that factoring integers is a hard problem must use integers $N = pq$ where p and q are prime numbers of size at least 1024 bits and preferably 2048 bits. This implies heavy computations during the encryption process, which makes it inefficient and costly. Moreover, a new threat has recently appeared that would break the RSA cryptosystem: quantum computers. Under the assumption that quantum computers can be built, Shor (1997) discovered an algorithm that could factor an integer in polynomial time in terms of its size in bits, thus rendering the RSA cryptosystem useless. Shor's algorithm can also break essentially all number theoretic based public key cryptosystem as well as the elliptic curve cryptosystems or the Diffie–Hellman key exchange. There have been great efforts dedicated to the construction of quantum computers and although nobody has built such computers able to attack the RSA or the discrete logarithm based cryptosystems, definitely there is a need for other efficient and secure cryptosystems.

There are currently a few families of cryptosystems that could potentially resist future quantum computers: these are the cryptosystems based on error-correcting codes (McEliece 1978; Niederreiter 1986), the public key cryptosystems based on

O. Billet
Orange Labs, 38–40 rue du Général Leclerc, 92794 Issy-les-Moulineaux, France
e-mail: olivier.billet@orange-ftgroup.com

J. Ding
Department of Mathematical Sciences, Department of Computer Sciences,
University of Cincinnati, Cincinnati, OH 45220, USA
e-mail: ding@math.uc.edu

M. Sala et al. (eds.), *Gröbner Bases, Coding, and Cryptography*,
DOI 10.1007/978-3-540-93806-4_15, © Springer-Verlag Berlin Heidelberg 2009

lattices (Regev 2006; Nguyen and Stern 2001), and the multivariate public key cryptosystems.

The class of multivariate cryptosystems is a special class of schemes whose security is related to the hardness of solving sets of multivariate equations. The obvious way of solving them is to compute a Gröbner basis (Buchberger 1965, 1970, 1985, 1998, 2006). Solving sets of multivariate equations is a well known hard problem that is not only hard on the average but already for sets of equations that are practical to evaluate, like for instance a hundred of randomly chosen quadratic equations in a hundred of unknowns defined over the binary field (Bardet 2004; Fraenkel and Yesha 1980). For obvious efficiency reasons, the multivariate polynomials that constitute the system are generally chosen to be quadratic polynomials defined over a small finite field—that is ranging from $\mathbb{F}_2$ to $\mathbb{F}_{2^8}$—though there exist rare exceptions (Billet and Gilbert 2003; Wang et al. 2006).

In the particular case of symmetric cryptographic primitives, it is often possible to randomly draw the multivariate polynomials with carefully selected parameters in order to obtain a security reduction to a generic instance of the underlying NP-hard problem: this is for instance the case for the stream-cipher QUAD proposed in Berbain et al. (2006), Berbain and Gilbert (2007), but also for the hash function MQ-HASH proposed in Billet et al. (2007). However in the case of asymmetric multivariate schemes, the designer has to embed a trapdoor in order to enable the owner of the secret key to solve the system of equation derived from the public key and the cipher text or the message to be signed. The side effect of embedding such a trapdoor in the public set of polynomials is that there is usually no reduction to a generic instance of the underlying hard problem anymore, since the corresponding systems are not randomly chosen. The security of the scheme has to be assessed by other means, usually by conducting experiments with the best system solvers or by mounting a specially crafted algebraic attack that exploits the underlying algebraic structure.

The current proposals for multivariate asymmetric cryptosystems might be classified into three main categories, some of which combine features from several categories: Matsumoto-Imai like schemes, Oil and Vinegar like schemes, stepwise triangular schemes, and an additional fourth category called *Polly Cracker* schemes. In this survey however, we focus on the first three categories; the reader can find more information on Polly Cracker schemes in Fellows and Koblitz (1994), Caboara et al. (2008) and especially in Levy-dit-Vehel et al. (2009). All of the schemes from the first three categories rely on the hardness of system solving, but some of them additionally rely on other hard problems such as finding rational mappings between polynomial maps or finding a linear combination of small rank of a given set of matrices.

2 Inversion Attacks

Although there exist several multivariate authentication schemes, we hereafter focus on multivariate asymmetric encryption schemes and multivariate signature schemes.

We tried to unify the notations as much as possible with the problem of system solving in mind: We denote the base field by $\mathbb{K}$, and use x and y to respectively denote the input and the output of a public key function. The input of the public key being an element of the vector space $\mathbb{K}^n$, we sometimes make use of the standard underlying coordinate system and write $x = (x_1, \ldots, x_n)$. Finally, we denote a multivariate public key by a polynomial mapping from the vector space $\mathbb{K}^n$ to the vector space $\mathbb{K}^m$:

$$\begin{aligned} f : \mathbb{K}^n &\longrightarrow \mathbb{K}^m, \\ x = (x_1, \ldots, x_n) &\longmapsto y = (p_1(x), \ldots, p_m(x)), \end{aligned} \tag{1}$$

where $p_1, \ldots, p_m$ are multivariate polynomials defined over $\mathbb{K}[x_1, \ldots, x_n]$. In the case of encryption schemes, x and y respectively denote the plain text and the cipher text. In the case of signature schemes, x and y respectively denote the signature and the hashed value to be signed.

This part describes several attacks against the underlying system solving problem of several multivariate cryptosystems, that is, it reports successful methods to invert the public key of some asymmetric cryptosystems. We first review the linearization attack of Patarin (1995) against Matsumoto–Imai scheme A, and then describe different attacks against a generalisation of it named Hidden Field Equations (HFE), that was proposed in Patarin (1996).

2.1 Matsumoto–Imai Scheme A and Its Variations

Starting from 1983, Matsumoto and Imai proposed a series of public key cryptosystems relying on the hardness of system solving. In Imai and Matsumoto (1985), they proposed a scheme "based on obscure representation of polynomials" often called C^* and hereafter called Matsumoto–Imai scheme A. This scheme uses exponentiation over an extension $\mathbb{E}$ of degree n of a base finite field $\mathbb{K}$ of size q. (We denote by φ the canonical embedding of $\mathbb{K}^n$ into $\mathbb{E}$ and $\mathbf{x} = \varphi(x)$.) The exponent is chosen of the form $1 + q^\theta$ and prime to $q^n - 1$ so as to allow efficient inversion. This exponentiation is then concealed by two change of variables S and T of $\mathbb{K}^n$. The public key is therefore given by the n-tuple $(p_1, \ldots, p_n)$ of polynomials in n unknowns $x_1, \ldots, x_n$ defined over $\mathbb{K}$ via:

$$\begin{aligned} &\mathbb{K}^n \longrightarrow \mathbb{K}^n, \\ &x = (x_1, \ldots, x_n) \quad \longmapsto \big(p_1(x), \ldots, p_n(x)\big) = T \circ \varphi^{-1}\big((\varphi \circ S(x))^{1+q^\theta}\big). \end{aligned} \tag{2}$$

One key fact allowing an efficient representation of the public key as the n-tuple of polynomials $(p_1, \ldots, p_n)$ is that the mapping $\mathbf{x} \mapsto \mathbf{x}^q$ (which is often also called the Frobenius endomorphism) is a $\mathbb{K}$-linear mapping and thus elevating to the power of $1 + q^\theta$ is $\mathbb{K}$-quadratic. Another mandatory property is the ability for the owner of the secret key to efficiently compute a solution to the system:

$$\begin{cases} p_1(x_1,\ldots,x_n) = y_1, \\ \vdots \\ p_n(x_1,\ldots,x_n) = y_n, \end{cases} \tag{3}$$

for every n-tuple $y = (y_1, \ldots, y_n)$, which should ideally correspond to the ability of performing decryption or signature. In order to solve (3), the secret key owner uses his knowledge of the secret linear mappings S and T and of an exponent e such that $e(1+q^\theta) \equiv 1 \pmod{q^n - 1}$ to invert each component of the public map in turn, which amounts to the following computation: $x = S^{-1} \circ \varphi^{-1}((\varphi \circ T^{-1}(y))^e)$. The name "obscure representation" comes from the assumption that the input and output coordinate systems are unknown to anyone but the secret key owner. Hence, the security of the cryptosystem not only relies on the hardness of solving (3), but also on the hardness of recovering any pair of mappings S_0 and T_0 such that: $\forall x \in \mathbb{K}^n$, $T_0 \circ \varphi^{-1}((\varphi \circ S_0(x))^{1+q^\theta}) = T \circ \varphi^{-1}((\varphi \circ S(x))^{1+q^\theta})$. A more general version of this problem of crucial importance to the security of multivariate public schemes is discussed later on in this paper.

This construction can obviously be extended to accommodate several other internal transformations instead of the original exponentiation. However, there must be an efficient way to invert this internal transformation, and the public key should have an efficient representation. With these constraints in mind, Patarin (1996) proposed to use an internal transformation of type:

$$f : \mathbb{E} \longrightarrow \mathbb{E}, \qquad \mathbf{x} \longmapsto \sum_{\substack{1 \le i \le j \le n \\ q^i + q^j \le D}} a_{i,j} \mathbf{x}^{q^i + q^j} + \sum_{\substack{1 \le k \le n \\ q^k \le D}} b_k \mathbf{x}^{q^k} + c. \tag{4}$$

This internal transformation f of $\mathbb{E}$ has the special property that its overall degree is bounded by some reasonable constant D: this trick enables the owner of the secret key to solve the equation $f(\mathbf{x}) = \mathbf{y}$ in the unknown $\mathbf{x}$ for any value $\mathbf{y}$ of $\mathbb{E}$, since there exist algorithms polynomial in D and n for this task (von zur Gathen and Shoup 1992; Knuth 1997). The resulting cryptosystem is called Hidden Field Equations (HFE).

Another generalization of the Matsumoto–Imai scheme A is the use of a projection instead of a bijection for the change of coordinates T, and the public key then becomes a mapping from $\mathbb{K}^n$ to $\mathbb{K}^m$ with $m < n$. This can be seen as a modification of the original scheme where some of the polynomials in the public key have been removed. Patarin et al. (1998a, 2000) applied this idea to the Matsumoto–Imai scheme A to create the SFLASH signature scheme, and proposed a very similar variation around the HFE cryptosystem (Patarin 1996). We however note that this construction is mainly of interest in the setting of signature schemes since the public key mapping is not a bijection anymore.

Finally, we note that the secret changes of coordinate system can be taken as linear mappings or affine mappings. However, as shown by Geiselmann et al. (2001), the constant parts of the secret affine mappings can often be deduced by an attacker (i.e. with the knowledge of the public key alone) and sometimes even leaks some information about the secret mappings themselves.

2.2 Direct Inversion Attacks

The essence of public key encryption (resp. signature) schemes is to give public access to a mechanism allowing the computation of a cipher text y from a plain text x (resp. verifying a signature x from a hashed value y). In the special case of multivariate schemes, we have seen in the previous section that this mechanism is a polynomial mapping having a low degree in the input variables because of efficiency reasons. This mapping p constitutes the public key and an attacker can directly search for a value x verifying $p(x) = y$ in order to decrypt y or to forge a signature x. Such attacks consist in solving a system of polynomial equations of low degree (quadratic in the case of Matsumoto–Imai and HFE), and there have been several algorithms designed to solve this task. The most famous are Buchberger's algorithm (Buchberger 1965, 1970, 1985, 1998, 2006; Mora 2009), Faugère's algorithms F4 and F5 (Faugére 1999, 2002), and basic algorithms such as the linearization tool XL suggested in Courtois et al. (2000) which is a particular case of F4 (Ars et al. 2004). The rationale behind the design of multivariate asymmetric cryptosystems is that the complexity of solving systems of randomly generated quadratic multivariate equations defined over a finite field is exponential in the number of unknowns on the average. At the same time, the trapdoor introduced in the public key of asymmetric multivariate cryptosystems makes the resulting system of equations specific and sometimes distinguishable from randomly generated ones.

The set of equations derived from the public key of Matsumoto–Imai scheme A instances can be solved by computing Gröbner bases: Dobbertin reported to have successfully solved such systems with Gebauer and Möller's version of Buchberger's algorithm while working at the BSI.[1] However, the first public cryptanalysis of Matsumoto–Imai scheme A was published by Patarin (1995): it is very instructive in that it explains why solving the system of equation through the computation of a Gröbner basis is possible. The key remark is that there exist bilinear equations relating the input and the output of the system. Indeed, recall that the internal transformation maps any element $\mathbf{x}$ of the extension field $\mathbb{E}$ to $\mathbf{y} = \mathbf{x}^{1+q^\theta}$, so that $\mathbf{y}\,\mathbf{x}^{q^{2\theta}} = \mathbf{x}\,\mathbf{y}^{q^\theta}$. This last bilinear equation still holds between the input and output variables x and y since they are $\mathbb{K}$-linear transformations of $\varphi^{-1}(\mathbf{x})$ and $\varphi^{-1}(\mathbf{y})$ respectively, so that the following holds for some set of coefficients $a_{i,j}$, b_i, and c_j:

$$\sum_{1\le i,j\le n} a_{i,j} y_i x_j + \sum_{1\le i\le n} b_i y_i + \sum_{1\le j\le n} c_j x_j + d = 0. \tag{5}$$

[1] Bundesamt für Sicherheit in der Informationstechnik which is the German Federal Office for Information Security.

Recall that $y_i = p_i(x)$. A common way to represent the set I_δ of polynomials of degree δ that belongs to the ideal generated by $(p_1, \ldots, p_n)$ is to construct a matrix whose columns are indexed by the monomials of I_δ and whose lines are obtained by multiplying each p_i with every possible monomial u such that $\deg(up_i) = \delta$. This matrix is called a Macaulay matrix of degree δ, see Macaulay (1916). In the case of Matsumoto–Imai scheme A, we see that the Macaulay matrix of degree 3 already contains the polynomials from (5)—remember that the y_i are polynomials of degree 2 in the x_i—and this explains why a direct Gröbner basis computation is efficient against this cryptosystem. The attack described by Patarin reads as follows Patarin (1995), Koblitz (1999): although the bilinear equations (5) are *a priori* unknown to the attacker, they can be easily interpolated by generating matching plain text/cipher text pairs from the public key. After that, finding an x corresponding to a given y is easy: just replace y in the interpolated equations (5) and solve the resulting linear system in x.

A number of multivariate cryptosystems are actually susceptible to attacks relying on low degree relations between input variables and output variables. This is for instance the case with the weak proposal (Wang et al. 2006) where a cryptanalysis directly stems from the above remarks (Ding et al. 2007a). Variants of another proposal called Tame Transformation Method (TTM) and published in Moh (1999) were also shown to be susceptible in Ding and Schmidt (2003, 2004).

A much less obvious behavior is exhibited by the HFE cryptosystem described above. Here again, the attacker can take advantage of the specific structure of the internal transformation to invert the public key with Gröbner basis methods efficiently. A simple counting argument briefly sketched in Faugère and Joux (2003) shows that the biggest Macaulay matrix constructed during a Gröbner basis computation with F4 has a much lower degree than that of a randomly drawn system of the same size. To see why, first remember that the internal transformation of HFE defined over $\mathbb{E}$ of characteristic 2 has a degree bounded by D. Let us denote the public key of HFE by g. Then consider a constant H such that $D \leq H < 2^n$, and the number of pairs of integers (d_i, k) for which d_i is a sum of at most $w-2$ powers of 2 such that $\varphi(x)^{d_i}(\varphi \circ g(x))^{2^k}$ has its degree bounded by H. It can be shown that there exists a value of H such that the number of monomials appearing in the set of equations generated this way is lower than the number of equations. Since $\mathbf{x} \mapsto \mathbf{x}^{2^k}$ is a $\mathbb{K}$-linear mapping, the number w exactly corresponds to the degree of the biggest Macaulay matrix constructed during the Gröbner basis computation. This degree is smaller than the one encountered in the Gröbner basis computation for a randomly chosen system of equivalent size. This theoretical explanation is supported by various experiments. Indeed, with his own optimized implementation of F5, Faugère solved the HFE challenge posted on Courtois' web page (Patarin 1998). This challenge is an HFE public key with 80 equations in 80 unknowns defined over $\mathbb{F}_2$ corresponding to an internal transformation of total degree 96. It was first solved by Faugère in about 52 hours on an HP workstation with an alpha EV68 processor running at 1000 MHz and 2^{33} bytes of memory, and later on by Steel with Magma in about 22 hours on a 750 MHz Sunfire v880 using about 2^{34} bytes of memory. As suggested by the above explanation, the degree of the biggest Macaulay matrix encountered was especially low and always bounded by w. And indeed, the data from Faugère and Joux (2003) obtained from several runs on various HFE parameters confirmed the fact that this value w is way too small for the cryptosystem to be secure:

$$\begin{array}{ll} 5 \le D \le 12 \to w = 4, & 128 \le D \le 1280 \to w = 6, \\ 16 \le D \le 96 \to w = 5, & 1536 \le D \le 4096 \to w = 7. \end{array}$$

An interesting fact is that these values are independent of the number n of unknowns, at least for $n < 160$, which corresponds to public keys of practical sizes.

Along with the first challenge that was originally broken by Faugère, a second challenge was proposed that is still not broken. It consists in an HFE public key with 36 variables defined over the finite field $\mathbb{F}_{2^4}$ of which four quadratic polynomials have been removed.

One might wonder if it is not possible to escape Gröbner basis attacks by tweaking the internal transformation so that its degree is not bounded anymore. Obviously, since the internal transformation has to be invertible by the legitimate user, this means that something must be relaxed somewhere. There has been some proposals along those lines in Ding et al. (2007b), Wang et al. (2006), all of which have been broken (Fouque et al. 2008a; Ding et al. 2007a). While these proposals were very specific, one might consider a broadest class that encompass such schemes and that we call Intermediate Field Systems: it comprises the schemes that have as internal transformation a set of multivariate polynomials in a small number of variables and defined over an intermediate extension field $\mathbb{L}$. Such an internal transformation might be inverted through the computation of Gröbner bases. In Billet et al. (2008), this class of schemes has been analyzed from the point of view of Gröbner basis attacks and it has been shown that the security achieved is asymptotically the same as that of the HFE cryptosystem.

2.3 MinRank

We just reviewed attacks against Matsumoto–Imai like cryptosystems aiming at directly solving the system arising from the public key. These "direct inversion" attacks do not try to recover a hidden specific structure implied by the presence of a trapdoor, though they rely on the existence of low degree relations between the value of the polynomials and their input variables. We describe here another family of attacks that first recover the hidden structure so that the attacker is in a position similar to that of the secret key's owner. More precisely, we focus on multivariate asymmetric cryptosystems whose public key consist of quadratic polynomials having rank peculiarities, like Fell and Diffie (1985), Shamir (1993), Moh (1999). The general structure of such cryptosystems is based on the family of triangular (or "de

Jonquière") mappings $x \mapsto y = J(x)$ defined as

$$\begin{cases} y_1 = x_1, \\ y_2 = x_2 + p_2(x_1), \\ y_3 = x_3 + p_3(x_1, x_2), \\ \vdots \\ y_n = x_n + p_n(x_1, x_2, \ldots, x_{n-1}), \end{cases} \tag{6}$$

where the p_i are polynomial mappings, and for efficiency reasons usually restricted to quadratic polynomial mappings. It can be easily checked that inverting such an application is easy since it amounts to incrementally solve linear equations in a single variable. The first cryptanalysis against such cryptosystems is given by Coppersmith et al. (1997) and uses the rank in order to break the bi-rational permutations scheme proposed by Shamir (1993).

Before describing the underlying rank problem, we recall basic properties of multivariate quadratic polynomials. The first fact is that every quadratic form p has a canonical form that can be computed in polynomial time, that is there exists a change of coordinates $S : (x_1, \ldots, x_n) \mapsto (z_1, \ldots, z_m)$ which can be efficiently found so that $m \leq n$ is minimal and there exists another quadratic form $\tilde{p}$ such that for all x, $p(x) = \tilde{p}(S(x))$. This minimal m is called the rank of p. The other fact is that a unique symmetric matrix of size n can be associated to any quadratic form in n unknowns the usual way: entry (i, j) of the matrix is half the coefficient of monomial $x_i x_j$ in the quadratic form and the diagonal coefficients are the ones of the monomials x_i^2. There are some difficulties in the case of a field of characteristic two that can be resolved by defining both entry (i, j) and entry (j, i) as the coefficient of monomial $x_i x_j$ in the quadratic form when $i \neq j$ and by defining entry (i, i) to be zero. Then, the rank of the symmetric matrix is equal to the rank of the quadratic form.

Thus, in the process of cancelling the effect of the linear mixing of the polynomials in the triangular form (aimed at hiding this specific structure), or alternatively in the process of recovering an equivalent version of the secret change of coordinates, the following problem naturally arises:

Definition 1 (Minimun Rank) Given a set $\{\mathsf{A}_1, \ldots, \mathsf{A}_m\}$ of $n \times n$ matrices defined over a finite field $\mathbb{K}$ and an integer $r < n$, find a non-trivial linear combination over $\mathbb{K}$ of rank less than or equal to r.

The complexity of the general MinRank problem over various fields has been studied by Buss et al. (1999), where it has been shown to be NP-complete when r varies with n. However, for a fixed r, there are polynomial algorithms to solve this problem. Several of them are described in Goubin (2003). One of it was devised and used in Goubin and Courtois (2000) by Goubin and Courtois to break the TTM scheme proposed in Moh (1999), and was later on extended in Billet and Gilbert (2006) by Billet and Gilbert to take advantage of particular settings. The exhaustive search was also extended in a similar way in Yang and Chen (2005). Most of these algorithms merely use linear system solving combined with some form of exhaustive search.

Another point of view has been given by the authors of Coppersmith et al. (1993): the solutions of a MinRank instance with a set of m matrices of size $n \times n$ *are* also the solutions of the system encoding the fact that every sub-matrix of size $(r+1) \times (r+1)$ of the sought linear combination has determinant zero. The overall complexity[2] of solving such a system of equations is $O\big(\frac{1}{(r+1)!}m^{\omega(r+1)}\big)$ provided there are enough equations to apply the linearization technique. Hence, this strategy works well if the rank is small and enough linearly independent equations can be derived.

An attack against HFE suggested by Kipnis and Shamir (1999) uses matrices over the extension field $\mathbb{E}$ of degree n over $\mathbb{K}$ of size q, and can be reduced to solving a huge system of equations. We briefly describe now this attack aiming at recovering HFE's private key. First of all, notice that the equation relating the public key and the private key can be rewritten as: $t^{-1} \circ g = f \circ s$, where s and t are the secret one-to-one linear mappings defined over $\mathbb{E}$, f is a $\mathbb{K}$-quadratic mapping defined over $\mathbb{E}$, and g is the public mapping resulting from their composition. Since any linear mapping can be written in the form of $x \mapsto \sum_{1 \le i \le n} \alpha_i x^{q^i}$, the homogeneous component of degree two of the public mapping can be described as:

$$g^{(2)}(x) = \sum_{1 \le i,j \le n} \gamma_{i,j} x^{q^i + q^j}.$$

Hence, a symmetric matrix G can be associated to g such that ${}^t XGX = g^{(2)}(x)$ where $X = (x^q, \ldots, x^{q^n})$. (Again, some care has to be taken in the case of characteristic 2.) If $s(x) = \sum_{1 \le i \le n} s_i x^{q^i}$ and $t^{-1}(x) = \sum_{1 \le i \le n} t_i x^{q^i}$, then the authors of Kipnis and Shamir (1999) show that $\tilde{G} = {}^t WFW$ where F is the symmetric matrix associated to f as described above, W is defined by $W_{i,j} = s_{i-j}^{q^j}$, $G_{i,j}^{\circlearrowright k} = G_{i+k,j+k}$ with indices taken modulo n, and $\tilde{G} = \sum_{1 \le k \le n} t_k G^{\circlearrowright k}$. The authors of Kipnis and Shamir (1999) then tried to solve a huge system of equations derived from this property, the complexity of which remained unclear. However, the equation $\tilde{G} = {}^t WFW$ can be re-interpreted from a rank point of view when remembering that F has rank $r = \log_q D$—because the degree of f has been bounded by D so as to allow efficient inversion of f. This remark was formulated by Courtois in Courtois (2001) who showed that the problem of recovering the right t_k basically amounts to solve a MinRank problem with r about $\log_q D$ given the set of matrices $G^{\circlearrowright k}$ that are directly derived from the public key and suggested to use the sub-matrices strategy to solve it, the complexity of which would be:

$$\frac{1}{(\alpha \log_q n)!} \exp\big[O\big(\omega\alpha(\log_q n)^2\big)\big], \tag{7}$$

[2] Where the constant ω depends on the method for solving linear systems; for instance ω is about 2.807 when using Strassen's algorithm.

if enough linearly independent equations can be derived, since $D = O(n^{\alpha})$ for some $\alpha \geq 1$. An interesting point is that the resulting complexity estimate is slightly better than the one given in Granboulan et al. (2006) and gives an even stronger result: HFE's secret key can be recovered in quasi-polynomial time. However, the authors of Jiang et al. (2007) expressed some doubts about the ability to solve the MinRank problem by these means: they indeed proved that the algebraic system constructed as explained above has a lot of solutions, which shows that the complexity estimate (7) is too optimistic.

Obviously, being able to solve systems of equations arising from MinRank problems more efficiently than via linearization attacks would advance the state of the art in the cryptanalysis of many multivariate cryptosystems, such as schemes from the TTM family (Moh 1999; Yang and Chen 2005), Rainbow (Ding and Schmidt 2005a), or even HFEv (Ding and Schmidt 2005b). A new approach has just been proposed for special MinRank instances (Faugère and Perret 2008a).

2.4 Unbalanced Oil and Vinegar

The Oil and Vinegar signature scheme has been designed by Patarin and was first exposed in Patarin (1997). This design with a radically different trapdoor might have been inspired to Patarin by the linearization attack against Matsumoto–Imai like cryptosystems. In Oil and Vinegar schemes indeed, the secret transformation is made of o multivariate quadratic polynomials whose homogeneous part of degree two have the following specific form:

$$\sum_{\substack{1 \leq i \leq o \\ 1 \leq j \leq v}} a_{i,j}\, x_i y_j + \sum_{1 \leq i,j \leq v} b_{i,j}\, y_i y_j . \tag{8}$$

That is, two sets of variables $O = \{x_i\}_{1 \leq i \leq o}$ and $V = \{y_j\}_{1 \leq j \leq v}$ are used, but only monomials from $\{zy\}_{(z,y) \in (O \cup V) \times V}$ are allowed to appear in the polynomials. It is easy to find a pre-image for a tuple of o such polynomials: after random values have been assigned to the variables from V, only a linear system in the variables from O remains. Finding a pre-image is then reduced to solving a linear system in these o variables. (Assuming these systems are uniformly distributed in the set of randomly drawn systems and there are o polynomials defined over a finite field of size q, the probability that such a system is invertible is given by $(1 - \frac{1}{q}) \cdots (1 - \frac{1}{q^o})$.) Hence, after a few trials with others randoms choices for the variables from V, a pre-image of the original system will be found.) This is why variables from O and V are respectively called oil and vinegar variables: assigning values to vinegar variables makes oil variables appear. As usual, this specific structure of the secret polynomials is hidden by a change of coordinates.

The balanced version of this Oil and Vinegar scheme, that is with $o = v$, was broken by Kipnis and Shamir (1998). The security of the unbalanced case as exposed by Kipnis et al. (1999) is still not well understood, although it is definitely not secure when the number of vinegar variables is much bigger than the number of oil variables. A system of m randomly chosen multivariate quadratic equations in n unknowns can be easily solved when $n \geq m^2$, see Kipnis et al. (1999). Kipnis and Shamir (1998) also show that the attack against the balanced case, which is heavily relying on the fact that $o = v$, can actually be used in the case where v is only slightly bigger than o with the help of exhaustive search—the overall complexity then becomes $O(o^4 q^{v-o-1})$. The experiments from Braeken et al. (2005) show that if direct Gröbner basis attacks can be efficient against the balanced Oil and Vinegar scheme, it is of exponential complexity in the unbalanced case. Faugère and Perret (2008b) also showed than it is possible to attack some set of parameters by computing Gröbner basis of several modified versions of the original system. It is however possible to select the parameters of the system so as to escape this signature forgery attack.

Several other asymmetric multivariate schemes are closely related to the Oil and Vinegar construction like for instance the signatures schemes Rainbow (Ding and Schmidt 2005a) and TTS (Yang et al. 2004). It is not difficult to see that the balanced and unbalanced Oil and Vinegar constructions are broken as soon as an attacker is able to recover an isomorphic version of the secret oil vector space. Up to now, no such structural attack is known against the unbalanced schemes.

2.5 *Defense Mechanisms*

In the previous paragraph, we reviewed several attacks using system solving techniques against asymmetric multivariate cryptosystems. Several extensions have consequently been proposed to slow down these attacks by making inefficient the system solving algorithms. We now briefly describe the most widespread of these and discuss their effects. These experiments might be classified into two families: the removal of some information in the published mappings and the addition of randomly chosen quadratic polynomials.

2.5.1 Removing Equations

The idea of discarding some of the polynomials from the public key was originally introduced by Shamir (1993). Patarin later suggested to use it to strengthen HFE in the context of signature and called the resulting scheme HFE^{--}. Patarin et al. (2000) designed a signature scheme by applying this idea to the original Matsumoto–Imai scheme A that they submitted to the NESSIE project. It seems that the effect of the removal of polynomials from the public key is quite efficient against the system solving threat: the second challenge on HFE is still unbroken and the NESSIE proposal SFLASH withstood all system solving attacks. Yet this is not enough for these schemes to be secure and an attack taking advantage of the underlying monomial structure of SFLASH has recently been found by Dubois et al. (2007a). This attack uses the associated bilinear form to regenerate the missing polynomials, and thus allows for the application of the attack originally found by Patarin against Matsumoto–Imai scheme A. The applicability of analogous techniques to HFE^{--} remains an open question. Furthermore, a rigorous analysis of the impact of removing equations from the public key of such schemes on the system solving techniques is still an open problem.

2.5.2 Perturbations

Another strategy devised to thwart system solving techniques is to perturb the public key by mixing additional randomly chosen multivariate quadratic polynomials to the public key. This strategy is quite natural since the problem of solving randomly chosen systems of multivariate quadratic equations is a hard problem. Let us denote by $g = (g_1, \dots, g_n)$ the n-tuple of polynomials corresponding to the original public key and $\tilde{g} = (g_1 + q_1, \dots, g_n + q_n)$ the public key after the introduction of m randomly chosen polynomials $\rho_1, \dots, \rho_m$. The introduction of the random polynomials should obviously not disallow the legitimate user to invert the resulting public key. To this end, it is limited in one of the two following ways: either $m = n$ and there exists some linear mapping $\lambda : \mathbb{K}^n \to \mathbb{K}^r$ of rank r such that

$$q_i(x_1, \dots, x_n) = \rho_i \circ \lambda(x_1, \dots, x_n), \quad 1 \le i \le n,$$

or $m = r$ and there is a linear mapping $\lambda : \mathbb{K}^r \to \mathbb{K}^n$ of rank r such that

$$\big(q_1(x_1, \dots, x_n), \dots, q_n(x_1, \dots, x_n)\big) = \lambda\big(\rho_1(x_1, \dots, x_n), \dots, \rho_r(x_1, \dots, x_n)\big).$$

In the first type of perturbation, called internal perturbation, the random polynomials ρ_i only depend on a small number r of variables. Then given some cipher text c and knowing the polynomials ρ_i, it is enough for the legitimate user to compute the value $z = \rho(w)$ for all the possible inputs w and try to invert the original public key g on the corresponding value $c + z$. In the second type of perturbation, often denoted by '$^+$', the random polynomials depend on all the variables $x_1, \dots, x_n$ but there are only r of them and so their value can be guessed as well by the legitimate user.

The second strategy has been proposed by Patarin et al. (1998a) while the first one was later on suggested by Ding and Gower (2005). Once again, the effect of these perturbations against system solving techniques is not well understood and waits for a rigorous analysis. However, it is interesting to see that the proposal of Ding and Gower (2005) was again defeated by Fouque et al. (2005) by analyzing a distinguisher based on the kernel of the differential of the public key and extended their attack to the perturbed HFE in Dubois et al. (2007b).

3 Structural Attacks

In the previous part, we have reviewed several direct inversion attacks against various multivariate asymmetric cryptosystems. We now describe algebraic attacks against the trapdoor's structure of some of these cryptosystems. The two basic mechanisms we focus on are the problem of finding isomorphisms between two sets of polynomials, and the problem of polynomials decomposition. The first problem is related to the problem of recovering the key of UOV cryptosystems and Matsumoto–Imai like cryptosystems such as HFE and SFLASH. This problem is also related to the study of substitution and permutation networks in symmetric cryptography (Biryukov et al. 2003). The second problem is a natural problem arising in multivariate cryptography. It has been used to design an interesting public encryption scheme (Patarin and Goubin 1997) mixing techniques from symmetric cryptography and multivariate polynomials to turn it into an asymmetric scheme.

3.1 Isomorphism of Polynomials

There is a natural equivalence class on the set of tuples of multivariate polynomials in n variables. For two m-tuples $f = (f_1, \dots, f_m)$ and $g = (g_1, \dots, g_m)$ of multivariate polynomials in n variables we say that f and g are equivalent if and only if there exists an invertible change of coordinates S such that $f(x) = g \circ S(x)$. This equivalence relation in the special case $m = 1$ and with f_1 and g_1 multivariate quadratic polynomials exactly corresponds to the classification of multivariate quadratic forms, which has been completed by Dickson (1971); the problem of isomorphism between polynomials of degree d is studied in Thierauf (2000). The equivalence can be further generalized as follows: two m-tuples f and g are IP-equivalent if and only if there exist two invertible changes of coordinates S and T such that $T \circ f(x) = g \circ S(x)$. This second equivalence relation has been formally introduced by Patarin (1996) in cryptography and further studied by Patarin et al. (1998b). (However, Matsumoto and Imai already made the implicit assumption that this problem is hard when they designed their scheme A.) Thus, the computational problem associated to deciding the IP-equivalence can be stated as follows:

Definition 2 (IP Problem) Given f and g, two m-tuples of multivariate polynomials in n variables, find two invertible linear mappings $S \in \mathrm{GL}_n(\mathbb{K})$ and $T \in \mathrm{GL}_m(\mathbb{K})$ such that:

$$g(x_1, \dots, x_n) = T \circ f \circ S(x_1, \dots, x_n). \tag{9}$$

One might wonder why not keep the map f secret and only publish g. The reason is that in multivariate asymmetric cryptosystems, the existence of a trapdoor considerably reduces the number of possible mappings f. For instance, only a few monomial can be used as the internal transformation in Matsumoto–Imai scheme A. It is therefore safer to assume that map f is also publicly known.

It has been proved in Patarin et al. (1998b) that deciding IP-equivalence is not NP-complete. It was also shown in the same paper that deciding another equivalence—which has been called MP-equivalence for it does not require the linear mappings S and T to be invertible—is NP-hard. Finally, the authors of Patarin et al. (1998b) reduced the problem of deciding graphs isomorphism to the problem of deciding for two m-tuples of quadratic multivariate polynomials f and g the existence of a linear mapping S (not necessarily invertible) such that $g(x) = f \circ S(x)$. The problem of deciding graphs isomorphism is a well known problem in complexity theory and it is used to define a whole complexity class which is thought to be disjoint both from P and NP-complete although this has not yet been proven. However, while most practical instances of the graph isomorphism problem are easy to solve, most practical instances of IP seem to be difficult to solve.

Thus, the IP-equivalence seems to be a good candidate to be used as a hard problem in cryptology. We already mentioned that the security of Matsumoto–Imai like cryptosystems rely on this problem, but other types of cryptosystems can be built based on the hardness of the IP problem like for instance the authentication scheme proposed by Patarin (1996), or the traitor tracing scheme proposed by Billet and Gilbert (2003). The IP problem is also of interest in symmetric cryptography where it was studied as a means to derive equivalent descriptions of block ciphers, and as a way of describing big S-boxes by substitution and permutation networks with much smaller S-boxes in order to ease their analysis (Biryukov et al. 2003).

There have been several algorithms designed to solve the IP problem, most of which are described in Patarin et al. (1998b), Biryukov et al. (2003), Perret (2005), Faugère and Perret (2006a). The best algorithm from Patarin et al. (1998b) to solve instances of the IP problem is based on a “to and fro” algorithm and has a complexity of $n^{O(1)}q^{\frac{n}{2}}$ both in time and memory; However, this algorithm only work for (almost) one-to-one mappings and the above mentioned complexity relates to the case of quadratic polynomials. In the case of non bijective mappings, another algorithm proposed in Patarin et al. (1998b) has polynomial complexity in memory and $n^{O(1)}q^n$ in time. The algorithm designed by Biryukov et al. (2003) share some features with the “to and fro” strategy and basically has the same time complexity. Biryukov et al. (2003) also contains a generalization to the affine setting. Perret also presented in Perret (2005) an algorithm for the simple equivalence of polynomials with has a time complexity lower bounded by n^6q^n. We focus here on an algorithm presented in Faugère and Perret (2006a) since it amounts to solve a system of equations; unfortunately, its complexity is not well understood. First of all, let us summarize the basic solving problem one is faced with the IP problem: assuming an internal transformation that consists of an m-tuple of multivariate polynomials of degree d in n variables and using additional variables to describe the unknown changes of coordinates, (9) gives a set of equations in the variables representing the change of coordinates. A quick counting of these equations shows that the system is over-defined with $m\binom{n+d}{d}$ equations in $m^2 + n^2$ variables when m is about n as is the case with several multivariate asymmetric cryptosystems. However, as the overall degree d increases, the number of equations and terms the attacker has to deal with increases at fast pace. This basic way to put the IP problem into equations can actually be much improved in the case where the internal transformation f contains monomials of low degree—constant, linear, or quadratic—so as to be independent of the overall degree d. Such a strategy has been proposed in Faugère and Perret (2006a) in the case of non homogeneous systems and is described hereafter. First of all, notice that (9) arising from the IP problem can be rewritten as:

$$T^{-1} \circ g(x_1, \dots, x_n) = f \circ S(x_1, \dots, x_n), \tag{10}$$

so that using variables for the unknown entries of the matrices corresponding to S and T^{-1} gives a lower total degree in the resulting equations. Let us denote these variables by $s_{1,1}, \dots, s_{n,n}$ and $t_{1,1}, \dots, t_{m,m}$ respectively. Then taking advantage of the fact that the internal transformation is not homogeneous, the above equation also holds for the homogeneous parts alone: $\forall k \leq d,\ T^{-1} \circ g^{(k)}(x) = f^{(k)} \circ S(x)$, where $g^{(k)}$ and $f^{(k)}$ denotes the homogeneous part of degree k of g and f. Thus, when the internal transformation has both a constant component and a degree one component, a lot more linear constraints in the variables $s_{i,j}$ and $t_{i,j}$ can be derived. But this set of $m(n+1)$ linear equations in the n^2+m^2 variables is not big enough to be over-defined. One has to adjunct another set of equations derived from a component of higher degree, usually a component of homogeneous degree two: these additional equations then suffice to render the system over-defined, in most cases of interest. (This is for instance the case with an internal transformation consisting of an n-tuple of quadratic multivariate polynomials in n variables which is quite representative in asymmetric multivariate cryptography.) This is the reason why the IP problem with internal transformations composed of low degree monomials is insensitive to the value of the overall degree d. However, this is *not true at all* for IP problems with homogeneous internal transformations of degree d, which explains the discrepancies between experiments with Matsumoto–Imai scheme A of degree four and experiments with randomly generated polynomials (with components of every degree) of overall degree four in the results of Faugère and Perret (2006a). It is not straightforward to derive the complexity of the strategy just described. However, experimental results from Faugère and Perret (2006a) show that the complexity of the IP problem for cryptographic purposes has sometimes been over-estimated (Patarin 1996; Billet and Gilbert 2003; Patarin et al. 1998b).

A powerful attack against the IP problem in the special case of the Matsumoto and Imai scheme A has also been proposed in Fouque et al. (2008b) and allows to recover the secret key of the Matsumoto and Imai scheme A, not only to invert it. This attack builds on a previous attack against SFLASH (Dubois et al. 2007a) and only uses efficient linear algebra. Finally, there has been no success up to now in attacking the IP problem underlying the HFE cryptosystem.

3.2 Two Rounds

We have seen in the previous sections that embedding a trapdoor in a tuple of quadratic multivariate polynomials is not an easy task. A natural way to try circumventing the difficulty is to rely on the composition of two multivariate mappings f and g. The first proposal based on such a strategy can be found in Patarin and Goubin (1997). In order to ease the exposition, we only describe a restricted version of it. It makes use of three mappings $f = (f_1, f_2, \dots, f_n)$, U, and $g = (g_1, g_2, \dots, g_n)$

where the f_i and g_i are k-tuples of multivariate quadratic polynomials in k variables and U is a change of coordinates over $\mathbb{K}^{kn}$. Thus, the published mapping is the composition $T \circ g \circ U \circ f \circ S$ where S ans T are additional changes of coordinates over $\mathbb{K}^{kn}$. This proposal, called two rounds by their designers, can be thought of as an asymmetric version of the substitution and permutation network construction classical in symmetric cryptography where the f_i and g_i play the role of S-boxes. (Note that these mappings f_i and g_i are not required to be one-to-one.) Obviously, those S-boxes can be easily inverted when considered alone. Thus, the security of the proposed scheme heavily relies on the hardness of the problem of decomposition of the public mapping:

Definition 3 (Decomposition Problem) Given a set of $n+1$ multivariate polynomials $f, h_1, \ldots, h_n$, in n variables defined over some finite field $\mathbb{K}$, find (provided it exists) a polynomial g of degree r such that:

$$f(x_1, \ldots, x_n) = g(h_1(x_1, \ldots, x_n), \ldots, h_n(x_1, \ldots, x_n)).$$

For multivariate polynomials of arbitrary degree, this problem is often assumed to be difficult to solve Dickerson (1989), von zur Gathen et al. (2003), as expected by the authors of two rounds. The decisional version of the decomposition problem is also sometimes referred to as the ring membership problem since it amounts to deciding the membership of f to the ring $\mathbb{K}[h_1, \ldots, h_n]$ restricted to polynomials of degree r. However for efficiency reasons, the degree r of g is assumed to be two in the two round scheme, and in this case, the corresponding decomposition problem becomes easy. Ye, Lam, and Dai indeed proposed in Ye et al. (1999, 2001) an efficient strategy to solve it based on the following simple remark: when the degree of g is two, the partial derivatives of f are nothing but elements $l_i h_j$ where l_i is a linear form and thus span an ideal Δ_f contained in $\langle x_1h_1, \ldots, x_nh_1, x_1h_2, \ldots, x_nh_n\rangle$. Hence, computing $(\Delta_f : \langle x_1, \ldots, x_n\rangle)$ (that is, the set of polynomials p such that Lp lies in Δ_f for every linear form L) reveals $\langle h_1, \ldots, h_n\rangle$. This fact was verified by experiments by the authors of Ye et al. (1999). To complete the attack, a basis of this last ideal gives an n-tuple $\tilde{h} = (\tilde{h}_1, \ldots, \tilde{h}_n)$ where the $\tilde{h}_i$ are linear combinations of the original polynomials h_i, which is enough to recover—by interpolation for instance—the remaining mapping $\tilde{g}$ such that $\tilde{g} \circ \tilde{h} = f$.

The authors of Patarin and Goubin (1997) tweaked their original construction so as to thwart this new threat and proposed to remove several public equations of two rounds, so that $f = g \circ h$ and h are mappings in n variables, but f and g are m-tuples of multivariate polynomials in n variables with $m < n$. But Faugère and Perret (2006b) refined the ideas of Ye et al. (1999) and showed that the scheme can still be cryptanalysed. Let us briefly describe their strategy: the basic idea is to compute $(\Delta_f : x_n^{\delta})$ for some well chosen $\delta > 0$. Indeed, the relations:

$$\frac{\partial f_i}{\partial x_j} = \sum_{1\le k,l\le n} g_{k,l}^{(i)} \left(\frac{\partial h_k}{\partial x_j} h_l + \frac{\partial h_l}{\partial x_j} h_k\right) \tag{11}$$

show that any linear combination of polynomials of the form $z^{[\delta-1]}\frac{\partial f_i}{\partial x_j}$, where $z^{[\delta-1]}$ stands for any monomial of degree $\delta - 1$ in the variables x_i, is also a linear combination of polynomials of the form $z^{[\delta]}h_i$. If V denotes the vector space spanned by the polynomials of the form $z^{[\delta]}h_i$ and $\tilde{V}$ denotes the vector space spanned by the polynomials of the form $z^{[\delta-1]}\frac{\partial f_i}{\partial x_j}$, then $x_n^{\delta}h_i$ belongs to $\tilde{V}$ for all i as soon as the dimension of $\tilde{V}$ as a vector space over V is at least $n\binom{n+\delta-1}{\delta}$. Thus, the computation of a Gröbner basis of $(\Delta_f : x_n^{\delta})$ provides the n-tuple $(\tilde{h}_1, \ldots, \tilde{h}_n)$ we were seeking. Faugère and Perret (2006b) also give an upper bound for the degree δ which helps evaluate the complexity of the Gröbner basis computation: the attack succeeds as soon as $\delta \geq \frac{m}{n}$. Thus, the results of Ye et al. (1999) come as the special case $m = n$.

4 Discussion

This overview of the state of the art in the cryptanalysis of multivariate asymmetric cryptosystems shows that system solving techniques brought a lot to the understanding of multivariate cryptosystems. It helped uncover structural properties of those schemes and pushed the limits of our knowledge with respect to some difficult problems such as the functional decomposition problem or the problem of finding isomorphisms between tuple of polynomials. The extensive experiments with the computation of Gröbner basis of randomly generated systems of polynomials together with the mathematical insights brought by the complexity analyzes from Bardet (2004) yield useful tools for dimensioning symmetric multivariate cryptosystems such as Berbain et al. (2006, 2007).

While several multivariate asymmetric schemes have been shown to be susceptible to some extent to Gröbner basis techniques, a lot of these attacks still lack rigorous complexity analysis. Several of them remain slow and progresses in the understanding of system solving techniques as applied to multivariate asymmetric cryptosystems would be of interest to the cryptographers' community. It also has to be emphasized that the cryptanalytic work performed against asymmetric multivariate cryptosystems has already benefited other areas of cryptography such as the cryptanalysis of stream ciphers which as witness a new range of attacks called algebraic attacks (Faugère and Ars 2003; Courtois and Meier 2003).

Apart from obtaining a better understanding of existing attacks, there are several other challenges for the cryptanalists. Concerning the multivariate schemes, the unbalanced Oil & Vinegar scheme remains unbroken. Furthermore, the effect of removing equations from the public key was shown to be inefficient in the case of the SFLASH cryptosystem and the natural following step is to settle the case of HFE^{--}. On the side of the underlying hard problems, the functional decomposition problem has been shown to be useless to design cryptosystems but the problem of finding isomorphisms between tuples of polynomials needs a lot more study. In particular, cryptographers need a better understanding of the mechanisms behind the attack from Faugère and Perret (2006a) and a natural question is the possibility of mounting a key recovery attack against the HFE cryptosystem, at least with a rigorous complexity analysis.

Acknowledgements Part of these results have been presented at Linz D1 2006, which was a workshop within the Special Semester on Gröbner Bases, February–July 2006, organized by RICAM, Austrian Academy of Sciences, and RISC, Johannes Kepler University, Linz, Austria.

This work has been supported in part by the French government through the ANR MAC project.

References

G. Ars, J. C. Faugère, H. Imai, M. Kawazoe, and M. Sugita, *Comparison between XL and Gröbner basis algorithms*, Proc. of Asiacrypt 2004 (P. J. Lee, ed.), LNCS, vol. **3329**, Springer, Berlin, 2004, pp. 338–353.

M. Bardet, *An investigation on overdetermined algebraic systems and applications to error-correcting codes and to cryptography*, Ph.D. thesis, University of Paris 6, Paris, France, 2004.

C. Berbain and H. Gilbert, *On the security of IV dependent stream ciphers*, FSE 2007 (A. Biryukov, ed.), LNCS, vol. **4593**, Springer, Berlin, 2007, pp. 254–273.

C. Berbain, H. Gilbert, and J. Patarin, *QUAD: A practical stream cipher with provable security*, EUROCRYPT 2006 (S. Vaudenay, ed.), LNCS, vol. **4004**, Springer, Berlin, 2006, pp. 109–128.

O. Billet and H. Gilbert, *A traceable block cipher*, Asiacrypt 2003 (C. S. Laih, ed.), LNCS, vol. **2894**, Springer, Berlin, 2003, pp. 331–346.

O. Billet and H. Gilbert, *Cryptanalysis of Rainbow*, SCN 2006 (R. De Prisco and M. Yung, eds.), LNCS, vol. **4116**, Springer, Berlin, 2006, pp. 336–347.

O. Billet, M. J. B. Robshaw, and T. Peyrin, *On building hash functions from multivariate quadratic equations*, ACISP 2007 (J. Pieprzyk, H. Ghodosi and E. Dawson, eds.), LNCS, vol. **4586**, Springer, Berlin, 2007, pp. 82–95.

O. Billet, J. Patarin, and Y. Seurin, *Analysis of Intermediate Field Systems*, SCC 2008 (D. Wang and J.-C. Faugère, eds.), 2008.

A. Biryukov, B. Preneel, A. Braeken, and C. de Cannière, *A toolbox for cryptanalysis: linear and affine equivalence algorithms*, Eurocrypt 2003 (E. Biham, ed.), LNCS, vol. **2656**, Springer, Berlin, 2003, pp. 33–50.

A. Braeken, B. Preneel, and C. Wolf, *A study of the security of unbalanced Oil & Vinegar signature schemes*, CT-RSA 2005 (A. Menezes, ed.), LNCS, vol. **3376**, 2005, p. 29.

B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, Ph.D. thesis, Innsbruck, 1965.

B. Buchberger, *Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems*, Aequationes Math. **4** (1970), 374–383.

B. Buchberger, *Gröbner-bases: An algorithmic method in polynomial ideal theory*, Multidimensional systems theory, Reidel, Dordrecht, 1985, pp. 184–232.

B. Buchberger, *An algorithmical criterion for the solvability of algebraic systems of equations*, London Math. Soc. LNS **251** (1998), 535–545.

B. Buchberger, *Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal*, J. Symb. Comput. **41** (2006), nos. 3–4, 475–511.

J. F. Buss, G. S. Frandsen, and J. O. Shallit, *The computational complexity of some problems of linear algebra*, J. Comput. Syst. Sci. **58** (1999), no. 3, 572–596.

M. Caboara, F. Caruso, and C. Traverso, *Gröbner bases for public key cryptography*, Proc. of ISSAC 2008 (L. Gonzalez-Vega, ed.), ACM, New York, 2008.

D. Coppersmith, J. Stern, and S. Vaudenay, *Attacks on the birational permutation signature schemes*, CRYPTO93 (D. R. Stinson, ed.), LNCS, vol. **773**, Springer, Berlin, 1993, pp. 435–443.

D. Coppersmith, J. Stern, and S. Vaudenay, *The security of the birational permutation signature schemes*, Journal of Cryptology **10** (1997), no. 3, 207–221.

N. T. Courtois, *The security of Hidden Field Equations (HFE)*, Proc. of CT-RSA 2001 (D. Naccache, ed.), LNCS, vol. **2020**, Springer, Berlin, 2001, pp. 266–281.

N. Courtois and W. Meier, *Algebraic attacks on stream ciphers with linear feedback*, EUROCRYPT 2003 (E. Biham, ed.), LNCS, vol. **2656**, Springer, Berlin, 2003, pp. 345–359.

N. Courtois, A. Klimov, J. Patarin, and A. Shamir, *Efficient algorithms for solving overdefined systems of multivariate polynomial equations*, Proc. of EUROCRYPT 2000, LNCS, vol. **1807**, Springer, Berlin, 2000, pp. 392–407.

M. T. Dickerson, *The functional decomposition of polynomials*, Ph.D. thesis, Cornell University, Ithaca, NY, USA, 1989.

L. E. Dickson, *History of the theory of numbers*, vol. **3**, Chelsea, New York, 1971.

J. Ding and J. E. Gower, *Inoculating multivariate schemes against differential attacks*, Cryptology ePrint Archive, Report 2005/255, 2005.

J. Ding and D. Schmidt, *A defect of the implementation schemes of the TTM cryptosystem*, Cryptology ePrint Archive, Report 2003/085, 2003.

J. Ding and D. Schmidt, *The new implementation schemes of the TTM cryptosystem are not secure*, Progr. Comput. Sci. Appl. Logic **23** (2004), 113–127.

J. Ding and D. Schmidt, *Rainbow, a new multivariable polynomial signature scheme*, ACNS 2005 (J. Ioannidis, A. D. Keromytis and M. Yung, eds.), LNCS, vol. **3531**, Springer, Berlin, 2005a, pp. 164–175.

J. Ding and D. Schmidt, *Cryptanalysis of HVEv and internal perturbation of HFE*, PKC 2005 (S. Vaudenay, ed.), LNCS, vol. **3386**, Springer, Berlin, 2005b, p. 288.

J. Ding, L. Hu, X. Nie, J. Li, and J. Wagner, *High order linearization equation (HOLE) attack on multivariate public key cryptosystems*, PKC 2007 (T. Okamoto and X. Wang, eds.), LNCS, Springer, Berlin, 2007a.

J. Ding, C. Wolf, and B.-Y. Yang, *ℓ-invertible cycles for multivariate quadratic (MQ) public key cryptography*, PKC 2007 (T. Okamoto and X. Wang, eds.), LNCS, vol. **4450**, Springer, Berlin, 2007b, pp. 266–281.

V. Dubois, P.-A. Fouque, A. Shamir, and J. Stern, *Practical cryptanalysis of SFLASH*, CRYPTO 2007 (A. Menezes, ed.), LNCS, vol. **4622**, Springer, Berlin, 2007a, pp. 1–12.

V. Dubois, L. Granboulan, and J. Stern, *Cryptanalysis of HFE with internal perturbation*, PKC 2007 (T. Okamoto and X. Wang, eds.), LNCS, vol. **3494**, Springer, Berlin, 2007b.

J. C. Faugére, *A new efficient algorithm for computing Gröbner bases* (F_4), J. Pure Appl. Algebra **139** (1999), nos. 1–3, 61–88.

J. C. Faugère, *A new efficient algorithm for computing Gröbner bases without reduction to zero* (F_5), Proc. of ISSAC 2002, ACM, New York, 2002, pp. 75–83.

J. Faugère and G. Ars, *An algebraic cryptanalysis of nonlinear filter generators using Gröbner bases*, INRIA Research Report 4739, 2003.

J. C. Faugère and A. Joux, *Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases*, LNCS, vol. **2729** Springer, Berlin, 2003, pp. 44–60.

J. C. Faugère and L. Perret, *Polynomial equivalence problems: algorithmic and theoretical aspects*, EUROCRYPT 2006, LNCS, vol. **4004**, Springer, Berlin, 2006a, pp. 30–47.

J. C. Faugère and L. Perret, *Cryptanalysis of 2R⁻ schemes*, CRYPTO 2006 (C. Dwork, ed.), LNCS, vol. **4117**, Springer, Berlin, 2006b, pp. 357–372.

J.-C. Faugère and L. Perret, *Cryptanalysis of MinRank*, CRYPTO 2008 (D. Wagner, ed.), LNCS, vol. **5157**, Springer, Berlin, 2008a, pp. 280–296.

J.-C. Faugère and L. Perret, *On the security of UOV*, SCC 2008 (D. Wang and J. C. Faugère, eds.), 2008b.

H. J. Fell and W. Diffie, *Analysis of a public key approach based on polynomial substitution*, CRYPTO 85 (H. C. Williams, ed.), LNCS, vol. **218**, Springer, Berlin, 1985, pp. 340–349.

M. Fellows and N. Koblitz, *Combinatorial cryptosystems galore!*, Finite Fields: Theory, Applications, and Algorithms (G. L. Mullen and P. J.-S. Shiue, eds.), Contemporary Mathematics, vol. **168**, AMS, Providence, 1994, pp. 51–61.

P.-A. Fouque, L. Granboulan, and J. Stern, *Differential cryptanalysis for multivariate schemes*, EUROCRYPT 2005 (R. Cramer, ed.), LNCS, vol. **3494**, Springer, Berlin, 2005, pp. 341–353.

P. A. Fouque, G. Macario-Rat, L. Perret, and J. Stern, *Total break of the -IC signature scheme*, PKC 2008, LNCS, vol. **4939**, Springer, Berlin, 2008a, pp. 1–17.

P.-A. Fouque, G. Macario-Rat, and J. Stern, *Key recovery on hidden monomial multivariate schemes*, EUROCRYPT 2008 (N. P. Smart, ed.), LNCS, vol. **4965**, Springer, Berlin, 2008b, pp. 19–30.

A. S. Fraenkel and Y. Yesha, *Complexity of solving algebraic equations*, Inf. Process. Lett. **10** (1980), nos. 4–5, 178–179.

W. Geiselmann, R. Steinwandt, and T. Beth, *Attacking the affine parts of SFLASH*, Cryptography and coding—IMA 2001, Springer, Berlin, 2001, pp. 355–359.

L. Goubin, *Théorie et Pratique de la Cryptologie sur Carte à Microprocesseur*, Mémoire d'habilitation à diriger des recherches, 2003.

L. Goubin and N. T. Courtois, *Cryptanalysis of the TTM cryptosystem*, ASIACRYPT 2000 (T. Okamoto, ed.), LNCS, vol. **1976**, Springer, Berlin, 2000, pp. 44–57.

L. Granboulan, A. Joux, and J. Stern, *Inverting HFE is quasipolynomial*, CRYPTO2006 (C. Dwork, ed.), LNCS, vol. **4117**, Springer, Berlin, 2006, pp. 345–356.

H. Imai and T. Matsumoto, *Algebraic methods for constructing asymmetric cryptosystems*, Proc. of AAECC 3, LNCS, vol. **229**, Springer, Berlin, 1985, pp. 108–119.

X. Jiang, J. Ding, and L. Hu, *Kipnis-Shamir's attack on HFE revisited*, Inscrypt 2007 (D. Feng and Y. Zhang, eds.), LNCS, Springer, Berlin, 2007.

A. Kipnis and A. Shamir, *Cryptanalysis of the oil & vinegar signature scheme*, CRYPTO '98, LNCS, vol. **1462**, Springer, Berlin, 1998, pp. 257–266.

A. Kipnis and A. Shamir, *Cryptanalysis of the HFE public key cryptosystem by relinearization*, CRYPTO 99 (M. J. Wiener, ed.), LNCS, vol. **1666**, Springer, Berlin, 1999, pp. 19–30.

A. Kipnis, J. Patarin, and L. Goubin, *Unbalanced oil & vinegar signature schemes*, EUROCRYPT '99 (J. Stern, ed.), LNCS, vol. **1592**, Springer, Berlin, 1999, pp. 206–222.

D. E. Knuth, *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*, Third ed., Addison–Wesley, Reading, 1997.

N. Koblitz, *Algebraic aspects of cryptography*, Algorithms and computation in mathematics, vol. **3**, Springer, Berlin, 1999.

F. Levy-dit-Vehel, M. G. Marinari, L. Perret, and C. Traverso, *A survey on Polly Cracker systems*, this volume, 2009, pp. 285–305.

F. S. Macaulay, *The algebraic theory of modular systems*, Cambridge University Press, Cambridge, 1916.

R. J. McEliece, *A public key cryptosystem based on algebraic coding theory*, JPL DSN **42–44** (1978), 114–116.

T. T. Moh, *A fast public key system with signature and master key functions*, Proc. of CrypTEC99, Hong Kong City Press, 1999.

T. Mora, *Gröbner technology*, this volume, 2009, pp. 11–25.

P. Q. Nguyen and J. Stern, *The two faces of lattices in cryptology*, CaLC 2001 (J. H. Silverman, ed.), LNCS, vol. **2146**, Springer, Berlin, 2001, pp. 146–180.

H. Niederreiter, *Knapsack-type cryptosystems and algebraic coding theory*, Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform. **15** (1986), no. 2, 159–166.

J. Patarin, *Cryptoanalysis of the Matsumoto and Imai public key scheme of Eurocrypt '88*, CRYPTO 95 (D. Coppersmith, ed.), LNCS, vol. **963**, Springer, Berlin, 1995, pp. 248–261.

J. Patarin, *Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms*, EUROCRYPT '96 (U. M. Maurer, ed.), LNCS, vol. **1070**, Springer, Berlin, 1996, pp. 33–48.

J. Patarin, *The oil & vinegar signature scheme*, Proc. of Dagstuhl Workshop on Cryptography, 1997.

J. Patarin, *Challenge HFE*, http://www.minrank.org/hfe#challenge, 1998.

J. Patarin and L. Goubin, *Asymmetric cryptography with S-boxes*, ICICS 97, LNCS, vol. **1334**, Springer, Berlin, 1997, pp. 369–380.

J. Patarin, L. Goubin, and N. T. Courtois, *C^{*-+} and HM: variations around two schemes of T. Matsumoto and H. Imai*, ASIACRYPT '98 (K. Ohta and D. Pei, eds.), LNCS, vol. **1514**, Springer, Berlin, 1998a, pp. 35–49.

J. Patarin, L. Goubin, and N. T. Courtois, *Improved algorithms for isomorphisms of polynomials*, EUROCRYPT 98 (K. Nyberg, ed.), LNCS, vol. **1403**, Springer, Berlin, 1998b, pp. 184–200.

J. Patarin, L. Goubin, and N. T. Courtois, *SFLASH, a Fast Asymmetric Signature Scheme for Low Cost Smart-Cards*, https://www.cosic.esat.kuleuven.be/nessie/workshop/submissions/sflash.zip, 2000.

L. Perret, *A fast cryptanalysis of the isomorphism of polynomials with one secret problem*, EUROCRYPT 2005 (R. Cramer, ed.), LNCS, vol. **3494**, Springer, Berlin, 2005, pp. 354–370.

O. Regev, *Lattice-based cryptography*, Proc. of CRYPTO2006 (C. Dwork, ed.), LNCS, vol. **4117**, Springer, Berlin, 2006, pp. 131–141.

A. Shamir, *Efficient signature schemes based on birational permutations*, CRYPTO93 (D. R. Stinson, ed.), LNCS, vol. **773**, Springer, Berlin, 1993, pp. 1–12.

P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Comput. **26** (1997), 1484–1509.

T. Thierauf, The computational complexity of equivalence and isomorphism problems, LNCS, vol. **1852**, Springer, Berlin, 2000, pp. 1–135.

J. von zur Gathen and V. Shoup, *Computing Frobenius Maps and Factoring Polynomials*, Computational Complexity **2** (1992), 187–224.

J. von zur Gathen, J. Gutierrez, and R. Rubio, *Multivariate polynomial decomposition*, Appl. Algebra Eng. Commun. Comput. **14** (2003), no. 1, 11–31.

L.-C. Wang, B.-Y. Yang, Y.-H. Hu, and F. Lai, *A "Medium-Field" multivariate public-key encryption scheme*, CT-RSA 2006 (D. Pointcheval, ed.), LNCS, vol. **3860**, Springer, Berlin, 2006, pp. 132–149.

B.-Y. Yang and J.-M. Chen, *Building secure tame-like multivariate public-key cryptosystems: The new TTS*, ACISP 2005 (C. Boyd and J. M. G. Nieto, eds.), LNCS, vol. **3574**, Springer, Berlin, 2005, pp. 518–531.

B.-Y. Yang, J.-M. Chen, and Y.-H. Chen, *TTS: High-speed signatures on a low-cost smart card*, CHES 2004 (M. Joye and J. J. Quisquater, eds.), LNCS, vol. **3156**, Springer, Berlin, 2004, pp. 371–385.

D.-F. Ye, K.-Y. Lam, and Z.-D. Dai, *Cryptanalysis of "2 R" schemes*, CRYPTO 99, LNCS, vol. **1666**, Springer, Berlin, 1999, pp. 315–325.

D.-F. Ye, Z.-D. Dai, and K.-Y. Lam, *Decomposing attacks on asymmetric cryptography based on mapping compositions*, J. of Cryptology **14** (2001), no. 2, 137–150.