On multivariate signature-only public key cryptosystems

Nicolas T. Courtois[1,2]
courtois@minrank.org
http://www.minrank.org

[1] Systèmes Information Signal (SIS), Université de Toulon et du Var
BP 132, F-83957 La Garde Cedex, France
[2] INRIA Rocquencourt, Projet Codes, Domaine de Voluceau
BP 105, 78153 Le Chesnay, France

Abstract. In a paper published at Asiacrypt 2000 a signature scheme that (apparently) cannot be abused for encryption is published. The problem is highly non-trivial and every solution should be looked upon with caution. What is especially hard to achieve is to avoid that the public key should leak some information, to be used as a possible "shadow" secondary public key.

In the present paper we argument that the problem has many natural solutions within the framework of the multivariate cryptography. First of all it seems that virtually any non-injective multivariate public key is inherently unusable for encryption.

Unfortunately having a lot of leakage is inherent to multivariate cryptosystems. Though it may appear hopeless at the first sight, we use this very property to remove leakage. In our new scenario the Certification Authority (CA) makes extensive modifications of the public key such that the user can still use the internal trapdoor, but has no control on any publicly verifiable property of the actual public key equations published by CA. Thus we propose a very large class of multivariate non-encryption PKI schemes with many parameters q, d, h, v, r, u, f, D.

The paper is also of independent interest, as it contains all variants of the HFE trapdoor public key cryptosystem. We give numerous and precise security claims that HFE achieves or appears to achieve and establish some provable security relationships.

Key Words: Asymmetric cryptography, finite fields, Hidden Field Equations, HFE problem, *basic* HFE, HFEv-, MinRank problem, short signature, escrowed cryptography, exportable cryptography.

1 Acknowledgments

I would like to thank to Moti Yung who motivated the present paper and anonymous referees for their comments and few corrections.

2 Introduction

2.1 Non-encrypting schemes

The general problem we consider is message authentication without secrecy studied in many papers [22, 21] since the 80's. Though the encryption technologies became widespread in the 90's, the problem remains quite important. Typically an organization provides users with means of signature, wants to achieve confidence in these and is dedicated to maintain transparency and trust. Still it needs an effective way of preventing different abuses of communication channels such as conspiracy, intrigues, pornography, blackmailing, and in general any forbidden or illegal activity.

There are many negative results on the subject that show how to add subliminal channels into various schemes, for example in [22, 23], and very few positive results that show how to avoid it. For example though it was initially believed that the NSA designed DSA in a way that it could not be abused for encryption, several people subsequently demonstrated that it could. Moreover following the terminology of Simmons [21, 23] it has a broad-band subliminal channel, not only a narrow-band one [23].

At Asiacrypt 2000 paper [30] Moti Yung and Adam Young consider a more precise problem posed by NIST of building a PKI that cannot be abused for encryption. In order to achieve better confidence the (private) signature keys should be privately and securely generated. Indeed, if they cannot indeed be used for encryption they should not, and don't need to be escrowed. The problem was known as quite non-trivial and (apparently) the only solutions known are the one proposed from Asiacrypt 2000 [30] and the one proposed in the present paper.

Achieving the sole non-encryption property is not enough, neither it is in [30]. The public key itself, widely distributed and bound to the user in the authority, may conceal some data usable for encryption. It may constitute a secondary "shadow" public key: used as an encryption key to a different algorithm (that does encryption). It is not obvious that it is possible to avoid encryption in general. We need to asses what is possible and what is not.

2.2 The problem of a secondary key

Unfortunately leaking information that would be bound to user's public key is inevitable in general. For example one may produce several signatures of new messages in some special order that yields information. However such a leakage is not practical, requires prior preparation and uses many signatures.

Can then single signature leak more than one bit of information (is it a correct signature or not). At this point we disagree with authors of [30] that suggest that it wouldn't leak more than one bit provided a signature of a message is unique.

First, a simple signature of a completely natural message will leak $10 - 30$ bits of information, depending only how fast are the secret key operations and regardless of the unicity of the signature. Here is how it works. The user will produce $2^{10} - 2^{30}$ signatures of a given message if it is not deterministic, and when it is deterministic he will sign $2^{10} - 2^{30}$ versions of the same message, for example with added spaces, commas, additional information etc. He tries it 2^t times to achieve t bits of his choice in the signature itself. Thus with only $11 - 32$ signatures the user will transmit a shadow $314 - bit$ shadow public key. Paradoxically multivariate schemes that are very slow, for example Quartz [18], or our proposal from section 21 will allow slower leakage that a faster solution proposed in [30].

Secondly, and after all, the user might as well publish his new public key for encryption, signed with his official signature key. One signature is therefore enough to defeat the non-encryption property of any signature scheme. There is no solution for the leakage problem in general.

What we claim to prevent is a leakage that is contained in the public key directory itself. We call it *centralized leakage* or *key-only leakage* as it is reaches all users of the PKI that will be able to send private messages to the owner of the secret key, even those that have no access to the network other that a possibility to send mail.

This *centralized leakage* or *key-only leakage* is to be opposed to the inevitable *local leakage* or *signature leakage* in which the user publishes some signed messages. The word *local* suggests that, even if there is no way to prevent leaking information by signed messages, we may expect that this leakage will be in practice available to a much smaller group of people, that are recipients of the message(s)/postings containing the leaked public key and moreover must be able to extract this information and store it in advance. Another important difference is that in the *centralized leakage* or *key-only leakage* everyone can receive private messages. In the *signature leakage*, the recipient needs to take steps in this direction.

2.3 Solutions

In the Asiacrypt 2000 paper [30] the CA knows the factors of a randomly generated specially structured modulus N. A controversial, though plausible claim is made that there is no way to derive an encryption scheme out of N such that CA cannot decrypt it. The signature is performed with an additional trapdoor nested inside the one known to CA. In the present paper we show that the problem has many easy solutions within the framework of the multivariate cryptography. First we will argument that for virtually any non-injective multivariate public key is inherently unusable in encryption.

Unfortunately the very nature of the public key of multivariate cryptosystems allows to leak quite a lot of information. We may usually make quite a lot of modifications to it, while conserving a (more or less functional) trapdoor. For example in the operation "+" described in the section 12.1 we may add just any equation to the public key and this allows an important *centralized leakage*. Though it may appear hopeless at the first sight, this very property of "flexibility" of the public key will be used in the schemes 18.0.4 and HFESolution2 to remove leakage. In our new scenario we require the authority to make extensive modifications of the public key in such a way that the user can still use the internal trapdoor, but has no control on any verifiable property of the actual public key equations published by CA.

2.4 Our specific construction

In the present paper we propose a very large class of multivariate non-encryption PKI schemes with many parameters q, d, h, v, r, u, f, D and in the section 21 we propose a practical implementation. Our construction is based on (already known) multivariate trapdoor constructions mainly, the Hidden Field Equations (HFE) with variants [12].

We use nested variants of HFE in a new context of non-encrypting signatures, this requires notably to add interaction with a third party in the key generation. The present paper extends the application area of multivariate cryptography, and increases the interest of it, as we exploit features that are unique to multivariate cryptosystems.

2.5 Evaluating the security

We formalize the security requirements on trapdoor functions we use, as a Pseudo-Random Multivariate Quadratic Systems (PRMQ). Finally we formalize also the non-abuse property of our schemes. The final claim is similar to the first paper that attempted to solve the problem [30], namely that our signature schemes achieve the least possible abuse.

One might object the numerous strong and unproven security claims we are making in this paper. In fact we don't rely on them, and have in mind a pragmatic construction of practical schemes, that should be far from being broken.
Many claims are simply a set of criteria for further evaluation of multivariate cryptographic primitives and constructing test-cases. They are not considered as axioms, and we are aware that some of them might prove faulty. However we expect that several of them are correct. Because of the modular multi-level construction of multivariate cryptosystems if one assumption fails, it is expected to impact the security of only some schemes.

We make a distinction between various, more or less founded security **Claims**, which if proven incorrect will only affect the security of a few multivariate cryptographic schemes, and so called **Critical Claims**, which would call to reconsider the security of potentially many (or all) multivariate schemes.

3 Building on HFE

In the present document we attempt to use (as long as it is possible) similar notations as in the Quartz signature scheme [18] except that our indexes start from 1.

Quartz belongs to the family of HFEv- multivariate schemes [12] that we are going to describe fully. More generally we will describe a composition of (up to) all the basic building blocks HFE, "v", -", "+", "f'" described by Jacques Patarin in the extended version of [12]. In addition we are going to specify and evaluate various security claims that can be made on the described HFE variants.

In the second part of the paper we are going to use those building blocks to build a very large class of non-encryption PKI schemes.

4 Basic notations

The parameters used in our schemes are integers q, d, h, v, r, u, f. A practical implementation example is given in the section 21. Some additional integer variables such as n, m will be defined with respect to above parameters, e.g. $n \overset{def}{=} h - v$.

Let $GF(q)$ be a finite field. We study multivariate schemes over K, i.e. the input and the output values are several variables in $GF(q)$, for example $x = (x_1, \ldots, x_n)$ will be in $GF(q)^n$. Usually $q = 2$ in practice and thus we consider strings of bits, otherwise we manipulate strings of $GF(q)$-values.

In all the present document, $||$ will denote the "concatenation" operation. If $x = (x_1, \ldots, x_m)$ and $y = (y_1, \ldots, y_n)$ are two strings of $GF(q)$-values, then $x||y$ denotes the string of $GF(q)$-values defined by:

$$x||y = (x_1, \ldots, x_m, y_1, \ldots, y_n).$$

For a given string $x = (x_1, \ldots, x_m)$ of $GF(q)$-values and two integers r, s, such that $1 \leq r \leq s \leq m$, we denote by $[x]_{r \to s}$ the string of $GF(q)$-values defined by:

$$[x]_{r \to s} = (x_r, x_{r+1}, \ldots, x_{s-1}, x_s).$$

5 Multivariate trapdoor functions

An essential part of a public key of a multivariate scheme is usually a system of multivariate polynomials $F : GF(q)^n \to GF(q)^m$. All multivariate polynomials we consider are quadratic. The secret key is a hidden internal algebraical or combinatorial structure of F.

Let F be a multivariate (trapdoor or not) function defined by some probability distribution $\mathcal{F}$. Usually $\mathcal{F}$ will have parameters (q, n, m) and possibly some other that we ignore for simplification. For example $\mathcal{F}(q, n)$ can be a randomly selected *basic* HFE scheme from [12] and described later, which is a trapdoor function with n variables over $GF(q)$. We write then $F \leftarrow \mathcal{F}(q, n)$ with $F : GF(q)^n \to GF(q)^n$.

For each multivariate trapdoor public key scheme $\mathcal{F}$, we propose to study it's security in terms of 3 distinct problems: the Distinguishability Problem, the Structural Cracking Problem and the Cracking Problem.

5.1 Cracking Problems

Definition 5.1.1 (The Cracking Problem). Given $F \leftarrow \mathcal{F}$, with $F : GF(q)^n \rightarrow GF(q)^m$ and a random $y \leftarrow GF(q)^m$, find with a non-negligible probability $\geq$ some $\varepsilon(q, n, m)$ and in time bounded by some $T(q, n, m)$ (at least) one solution $x \in GF(q)^n$ to

$$y = F(x).$$

We always assume $\varepsilon > 0$.

We denote $\mathcal{MQ}(q, n, m)$ the probability distribution that consists of taking a random set of m quadratic equations over $GF(q)$ with n variables. The cracking problem for such a random set of quadratic equations is:

Definition 5.1.2 (MQ problem). Given $F \leftarrow \mathcal{MQ}(q, n, m)$ and a random y, find with a non-negligible probability $\geq \varepsilon$ and in time bounded by T (at least) one solution x to $y = F(x)$.

The MQ problem is not only worst-case difficult, as it is proven NP-complete in [6, 14], but it seems very hard on average. At Eurocrypt 2000 [25] authors claimed that:

Critical Claim 5.1.3. For practical values of q, m, n and with $m \approx n$, no method is known to solve a randomly chosen $F \leftarrow MQ(q, n, m)$ considerably faster that the exhaustive search in q^m.

More precisely we conjecture the following absolute hardness property to hold at least for the practical MQ instances:

Conjecture 5.1.4 (Absolute Hardness of MQ instances). Let $m \approx n$. For all Adversaries A running in T CPU clocks such that

$$Pr[F \leftarrow MQ(q, n, m), y \leftarrow GF(q)^m : F(A^{F,y}) = y] \geq \varepsilon > 0$$

we have the following inequality

$$T \geq \varepsilon \times q^m.$$

It is doubtful this conjecture always holds as the general problem might prove subexponential some day [25], but so far it holded for instances used in practice. This motivates the current research in multivariate cryptography:

We note that we need to have $m \approx n$. Indeed, when $m >> n$ the problem is probably at most subexponential [25], and several algorithms much faster than exhaustive search for the case $n >> m$ are presented in [3] and one in [16].

Design Criterion 5.1.5 (Near-exhaustive security). A good multivariate cryptographic scheme is expect to achieve a security very close to the exhaustive search (in q^m).

The idea is that it should be considerably better than the square root $q^{m/2}$ of the exhaustive search. Otherwise no one probably will bother with multivariate cryptography and use deeply mathematical and extensively studied group-based schemes such as RSA and Elliptic Curves. Their drawback is that on any group there are generic algorithms, precisely much faster than the exhaustive search (in the square root of the group size or less), such as Pollard's rho algorithm.

5.2 Distinguishability Problems

The strongest security claims made in cryptography are claims about indistinguishability with respect to (ideal or real) random objects.

Definition 5.2.1 (the Distinguishability Problem). It is the problem of distinguishing $F \leftarrow \mathcal{F}$ from the random set of quadratic polynomials $F' \leftarrow MQ(q, n, m)$.

Definition 5.2.2 (Adversary). A T-time adversary is a probabilistic Turing machine that stops in time $\leq T$ and outputs an answer.

We note that for both T and ε:

- they may be variable and depend on (q, n, m) and possibly other parameters for example $T = q \times n^{\mathcal{O}(1)}$
- they may be fixed and defined as e.g. $\varepsilon = 2^{-64}$ for some range of parameters.

Definition 5.2.3 (Distinguishers). A T-time distinguisher is a T-time adversary that takes a given $F \leftarrow \mathcal{F}(q, n, m)$ as an input and outputs a yes or a no encoded in {0,1}.

The probability it outputs 1 on $F \leftarrow \mathcal{F}$ is

$$Pr[F \leftarrow \mathcal{F}(q, n, m) : A^F = 1]$$

Definition 5.2.4 ((T, ε)-Pseudo Random MQ). Let A be a T-time distinguisher. We define the distinguisher's advantage as:

$$Adv_{\mathcal{F}}^{PRMQ}(A) \overset{def}{=} \left| Pr[F \leftarrow \mathcal{F} : A^F = 1] - Pr[F \leftarrow \mathcal{MQ} : A^F = 1] \right|$$

We say that $\mathcal{F}$ is (T, ε)-indistinguishable from MQ (or a (T, ε)-**PRMQ**) if we have:

$$Max_{\ T\text{-time A}} \ Adv_{\mathcal{F}}^{PRMQ}(A) \ \leq \varepsilon$$

Definition 5.2.5 (PRMQ). We say that $\mathcal{F} : GF(q)^n \rightarrow GF(q)^m$ is a **PRMQ** if it is (T, ε)-PRMQ for all (T, ε) such that

$$T < \varepsilon \times q^m.$$

Design Criterion 5.2.6 (PRMQ trapdoors). A good multivariate cryptographic trapdoor function should be a PRMQ.

5.3 Security against structural attacks

The secret key of a multivariate trapdoor scheme is a hidden internal algebraical or combinatorial structure of F that allows to compute one or several inverses $F^{-1}(y)$, at least with some fixed non-negligible probability ε_0 on y, for example $\varepsilon_0 = 1/3$.

Definition 5.3.1 (the Structural Cracking Problem). The (T, ε)-Structural Cracking Problem is the problem of recovering in time T this hidden structure, or an equivalent one that allows to compute in time T, one (at least) inverse $F^{-1}(y)$ and with at least the probability ε.

We note that the Structural Cracking Problem is still interesting for a much smaller ε that the actual capacity of inversion ε_0 available to the legitimate owner of the secret key.

The following trivial theorem holds:

Theorem 5.3.2. If the (T, ε)-Structural Cracking Problem is solved, then the (T, ε)-Cracking Problem is solved.

In practice, we expect that there is a substantial gap between these two problems. It is so for structural attacks on the *basic* HFE by Shamir-Kipnis [26, 2] and cracking attacks by Courtois [2]. We will be able to compare the complexity of these attack later.

The notion of security based on indistinguishability is the strongest of the three and we have the following trivial theorem:

Theorem 5.3.3. We assume that the conjecture 5.1.4 holds and that $\mathcal{F}$ is a (T, ε)-PRMQ.

Then no one can solve the $(T, \varepsilon + T/q^m)$-Cracking Problem.

Proof. Let us suppose that we can solve the $(T, \varepsilon + T/q^m)$-Cracking Problem for $F \leftarrow \mathcal{F}$. We have $T \leq q^m$ otherwise the theorem is true. Let A be a T-time distinguisher that on F picks a random y and outputs 1 iff he is able to find an x such that $F(x) = y$.

When $F \leftarrow \mathcal{F}$ it outputs 1 with probability at least $\varepsilon + T/q^m$. However when $F \leftarrow \mathcal{MQ}$ it only outputs 1 with probability at most T/q^m as in our assumption 5.1.4.

Thus by the triangular inequality we have $Adv_{\mathcal{F}}^{PRMQ}(A) \geq \varepsilon$. □

Corollary 5.3.4. If the conjecture 5.1.4 holds and if $\mathcal{F}$ is a (T, ε)-PRMQ then no Adversary can solve the $(T, \varepsilon + T/q^m)$-Structural Cracking Problem.

6 The *basic* HFE

The *basic* HFE cryptosystem has been proposed by Jacques Patarin at Eurocrypt'96 [12].

For a given security parameter d, a *basic* HFE will be defined as $G \leftarrow HFE(q,h,d)$, $G : GF(q)^h \rightarrow GF(q)^h$.

6.1 The extension field

We use an extension field $\mathcal{L} = GF(q^h)$.

More precisely, let $P(x)$ be an irreducible polynomial of degree h over $GF(q)$ and let $\mathcal{L} = GF(q)[X]/(P(X))$.

We will denote by φ the bijection between $GF(q)^h$ and $\mathcal{L}$ defined by:

$$\begin{aligned} \varphi(x) = x_h X^{h-1} + \ldots + x_2 X + x_1 \pmod{P} \\ \text{with } \; x = (x_1, \ldots, x_{h-1}) \in GF(q)^h \end{aligned}$$

Design Criterion 6.1.1 (Prime extension). We advocate to use a prime h to avoid hypothetical attacks based on an intermediate field $GF(q^{h'})$, $h'|h$. Yet no attack is known that takes advantage of a composite h.

6.2 The hidden polynomial

Let

$$F(Z) = \sum_{\substack{1 \le i < j \le h \\ q^i + q^j \le d}} \alpha_{i,j} \cdot Z^{q^i + q^j} + \sum_{\substack{1 \le i \le h \\ q^i \le d}} \beta_i \cdot Z^{q^i} + \gamma.$$

be a secret (so called hidden polynomial) $F : \mathcal{L} \rightarrow \mathcal{L}$.

Let $F' = \varphi^{-1} \circ F \circ \varphi$ be a version of F re-written as a system of multivariate polynomials. We assume an important property proven in details in [12]: F' is quadratic. In fact F has been made in such a way that it has the multivariate degree 2, the univariate degree d, and contains as much entropy as possible: all the coefficients should be picked at random in $\mathcal{L}$.

6.3 Public parameters

We conceal F' with two random affine secret bijections $s, t : GF(q)^h \rightarrow GF(q)^h$.

The public key is defined as F' with a double variable change s and t on respectively the input and the output variables. It gives:

$$G = t \circ \varphi^{-1} \circ F \circ \varphi \circ s$$

By construction G is quadratic, and it's direct expression as a multivariate quadratic transformation $G : GF(q)^h \rightarrow GF(q)^h$ constitutes the public key.

$$\begin{cases} y_1 = G_1(x_1, \ldots, x_h) \\ \quad \vdots \\ y_h = G_h(x_1, \ldots, x_h) \end{cases}$$

with each G_i being a quadratic polynomial of the form

$$G_i(x_1, \ldots, x_h) = \sum_{1 \le j < k \le h} \zeta_{i,j,k} x_j x_k + \sum_{1 \le j \le h} \nu_{i,j} x_j + \rho_i,$$

all the elements $\zeta_{i,j,k}$, $\nu_{i,j}$ and ρ_i being in $GF(q)$.

6.4 Secret key

The secret key are (t, F, s).

6.5 IP problem

Definition 6.5.1 (Isomorphism of Polynomials). The Isomorphism of Polynomials [IP] problem is the problem of recovering s, t given F and G.

This problem is used in interactive authentication as proposed in [12]. However in [15] it is shown not to be NP-complete. The fastest known algorithm for IP is in $q^{h/2}$ [15], which is still exponential. A very special case of IP is the graph isomorphism GI that is widely believed not to be polynomial [15]. We actually conjecture a much stronger property about it's average-case complexity:

Conjecture 6.5.2 (IP complexity). There is no algorithm for solving the average-case IP problem faster than $q^{\mathcal{O}(h)}$.

Even if IP was easy, it does not break the HFE cryptosystem. The attacker is **not** given F in HFE.

6.6 Using the HFE trapdoor

The inverse of the function F can be computed because by construction it's (univariate) degree is bounded by d. This operation uses an algorithm (e.g. Berlekamp) that factors the polynomial $(F(x) - y)$ over the finite field $\mathcal{L}$. It can be achieved within $d^2(\ln d)^{\mathcal{O}(1)} n^2$ $GF(q)$ operations, for details see [12, 7, 4, 18].

The parameter d will be selected as a tradeoff between the desired speed and security.

Design Criterion 6.6.1 (Next after q power). We advocate to take d of the form $d = q^k + 1$ because the security with respect to all known attacks depends on $\lceil log_q d \rceil$, and at constant security it will be the fastest possible d.

7 The HFE problem and *basic* HFE

7.1 The HFE Problem

Definition 7.1.1. The HFE Problem is the Cracking Problem for *basic* HFE.

First we have a trivial theorem from [12]:

Theorem 7.1.2 (HFE→MQ, Patarin 1996). If in the *basic* HFE scheme d is big enough, then it is a PRMQ.

Moreover it holds for $T = \infty$ and with $\varepsilon \approx 1$.

7.2 The HFE problem and secure encryption

We note that the hardness of the HFE problem as defined above is enough to achieve provably secure public key cryptosystems in the strongest known sense. Indeed, the conversion called REACT by Pointcheval and Okamoto is described [10]. It transforms any encryption function that is secure against inversion, into a scheme that is semantically secure and non-malleable against adaptive chosen ciphertext attacks, and also achieves the stronger version of Plaintext Awareness as defined in [1]. After conversion, the security of HFE in encryption will depend **only** on two problems: the HFE problem and on the pseudorandomness of the hash function used inside REACT [10].

7.3 The HFE problem and secure signatures

The HFE problem is sufficient to achieve provably secure signatures in the random oracle model, as long as **all** values to be inversed are given by the hash function. A more general result is easy to show:

Theorem 7.3.1 (security of HFE signatures).

Let F be a trapdoor one-way function such that the signature is computed by applying one or several times $F^{-1}(y)$ on y, such that at least in one case y is given by the hash function, and that this value y is always recovered completely in the signature verification.

If an attacker having (only) the access to the public key is able to compute a valid pair (message,signature) with probability ε and with Q queries to the hashing oracle.

Then it can be then transformed into a machine to inverse at least one out of Q values y chosen at random.

Proof. Since the function behaves as a random oracle, the attacker can only use it as a black box that gives some random hash values. We replace the output of this black box by a random sequence L of Q possible values for y, one of each we want to inverse. The adversary cannot distinguish between the two situations. A valid pair (message,signature) must allow to compute an inverse of at least one y that is in the sequence L.

We note that the security of the hash function as a random oracle impacts (again) the security of the signature schemes. Such schemes proven secure in the random oracle model are believed secure in practice, see for example [20].

It is unclear if HFE signatures are secure against known or chosen message attacks. Because of the presence of the hash function, the two cases are equivalent. However because multivariate quadratic schemes are usually not-bijective, such attack will provide the attacker with a distribution probability of entries to F that is not uniform. The values x such that $F(x') = F(x)$ has no other solution that $x' = x$ will appear more frequently than the other. It is an open problem to know if such a biased probability distribution gives any advantage that enables to break HFE.

8 The cracking attacks on *basic* HFE

Unfortunately the HFE problem is subexponential. It has been independently demonstrated in 1999 by Shamir-Kipnis [26] and Courtois in [2]

The best known algorithm for this problem is the Courtois "distillation attack" from [2] that runs in less than about:

$$h^{\frac{3}{2}\log_q d}. \tag{1}$$

In practice, we may still build a practical *basic* HFE that is a PRMQ with a respect to known attacks.

Claim 8.0.2 (Practical *basic* HFE vs PRMQ). For practical parameter values the *basic* HFE is already a PRMQ for some d that can still be considered as practical.

For example the Courtois attack (considered just above) gives 2^{62} for the so called "HFE Challenge 1" from [12, 4], while the exhaustive search is in 2^{80}. Still it is practical, one decryption takes 1.750 s on a 500 MHz PC using Victor Shoup's NTL routines [28].

9 The structural security of *basic* HFE

The best known algorithm for this problem is the Shamir-Kipnis MinRank attack from [26] that has been substantially improved by Courtois in [2] and gives the complexity of:

$$h^{3\log_q d}. \tag{2}$$

We observe that there is indeed a gap between the structural MinRank attack in $h^{3\log_q d}$ and the direct cracking attack in $h^{\frac{3}{2}\log_q d}$.

10 The asymptotic security of *basic* HFE

Following [26, 2] we have:

Theorem 10.0.3 (Fixed d HFE $\in$ P). Both the Cracking Problem for *basic* HFE (called also The HFE Problem), and the Structural Cracking Problem are polynomial on average if d is a fixed constant.

Theorem 10.0.4 (Subexponential *basic* HFE). Both the Cracking Problem Structural Cracking Problem for *basic* HFE are subexponential on average for $d \in n^{\mathcal{O}(1)}$.

We recall that $d \in n^{\mathcal{O}(1)}$ is necessary. If the security parameter d were not polynomial, then HFE couldn't be decrypted in a polynomial time as explained in the section 6.6.

We also mention that in [2] it has been conjectured that:

Claim 10.0.5 (HFE$\notin$P). Neither the Cracking Problem, nor the Structural Cracking problem for any version of HFE is polynomial if $d \in n^{\mathcal{O}(1)}$.

It seems coherent with the theorem 7.1.2.

11 The *basic* HFE and PRMQ

The *basic* HFE corresponds to a well-defined algebraical problem called the HFE Problem. Unfortunately the internal algebraical structure is possible to apprehend and gives subexponential attacks. Even if the *basic* HFE is PRMQ in practice, it is probably not a PRMQ in a general (asymptotic) sense.

Now we conjecture the following:

Conjecture 11.0.6 (MQ is not subexponential). The MQ problem is not subexponential on average.

This is controversial as the authors of [25] presented an algorithm FXL for which it might be subexponential. However if our conjecture 5.1.4 is asymptotically true, then the claim will be true. In that case we would have:

Conjecture 11.0.7 (*basic* HFE $\notin$ PRMQ). Provided that MQ is not subexponential on average, (or that the conjecture 5.1.4 holds) the *basic* HFE is not a PRMQ (in asymptotic sense).

In practice however, with respect to all known attacks [2, 26], it is always possible to choose parameters for a *basic* HFE so that it is a PRMQ and the scheme is still practical.

For example the internal *basic* HFE in the Quartz scheme [18] has been chosen that way, and after that, numerous external perturbations were added that still increase it's hardness.

12 Combinatorial HFE schemes

In order to obtain schemes much closer to the PRMQ requirement, several HFE versions have been proposed. The general paradigm is the following:

Design Criterion 12.0.8. Starting from a trapdoor function with a global algebraical structure, apply several local modifications (perturbations) that increase substantially the complexity of structural attacks.

Thus the Structural Cracking problem loses it's **algebraical** character and becomes a **"combinatorial"** problem (as opposed to algebraical).

We expect such a "combinatorial" modified scheme to be a PRMQ.

12.1 Modified HFE

Four basic operations on HFE has been described in [12, 13]. They are called "+","-","v" and "f" and can be combined in various ways. The basic principle is the following:

"+" It consists of linearly mixing of the public equations with some u random equations.

"$-$" We remove some r of the public equations. The idea is initially due to Adi Shamir [24].

"f" It consists of fixing some f input variables of the public key.

"v" It is defined as a construction (sometimes quite complex) such that the inverse of the function can be found **only** if some v of the (internal) variables, called **v**inegar variables, are fixed. This idea is undoubtedly due to Jacques Patarin [12, 17].

Only because we are in multivariate cryptography over small finite fields that those operations do preserve (to some extend) the trapdoor solvability of the function.

The two operations "-" and "v" increase m with respect to n, and therefore can be freely used to build signature schemes in which one of many possible inverses is selected. The two operations "f" and "+" decrease m with respect to n, and therefore are interesting primarily for encryption schemes, for which they add redundancy. All the four components will be used in the present paper. First we are going to define an HFEv- scheme, as used in Quartz [18]. Subsequently we are also going to use the modifications "+" and "f".

Critical Claim 12.1.1 (Combinatorial HFE $\in$ PRMQ). Perturbations increase substantially the security of HFE and each modified HFE scheme is already a PRMQ even if d is "small".

By caution we advocate however $d \geq 25$. We conjecture also that:

Conjecture 12.1.2 (Exponential improvement of structural security). Let $\mathcal{GX}$ be the modified scheme $\mathcal{G}$, for example $\mathcal{X}$='+' and the number of perturbations (e.g. added equations) is $w > 0$.

Let T be the complexity of the best structural attack against $\mathcal{G}$.

Then the best attack for $\mathcal{GX}$ is in at least $T \cdot q^{\mathcal{O}(w)}$.

For example in [16] an algorithm is presented for solving C^{*-}, a very weak special case of HFE, modified with "-". It has indeed a factor in 2^w with the respect to the C^* attack.

No other structural attack on a modified HFE is known at present.

13 HFEv- specification

The HFEv- is build using the combination of ideas from the initial paper [12]. It constitutes the main component of the Quartz signature scheme [18]. The parameters of the scheme are (q, h, v, r, d) and we have the following two special cases:

Definition 13.0.3 (HFEv). It is a HFEv- scheme as defined below with $r = 0$.

Definition 13.0.4 (HFE-). It is a HFEv- scheme as defined below with $v = 0$, or equivalently a *basic* HFE with r removed public equations.

For a given security parameter d, we describe how to generate a general random $G \leftarrow HFEv-(q, h, v, r, d)$.

It will be a function $G : GF(q)^{h+v} \to GF(q)^{h-r}$ defined below.

13.1 The hidden polynomial(s)

Let

$$F_V(Z) = \sum_{\substack{1 \le i < j \le h \\ q^i+q^j \le d}} \alpha_{i,j} \cdot Z^{q^i+q^j} + \sum_{\substack{1 \le i \le h \\ q^i \le d}} \beta_i(V) \cdot Z^{q^i} + \gamma(V).$$

be a secret family of polynomials $F_V : \mathcal{L} \to \mathcal{L}$.

In the above formula, each $\alpha_{i,j}$ belongs to $\mathcal{L}$ and each β_i is an affine transformation from $GF(q)^v$ to $\mathcal{L}$, *i.e.* a transformation satisfying

$$\forall V = (V_1, V_1, \ldots, V_v) \in GF(q)^v, \;\; \beta_i(V) = \sum_{1 \le k \le v} V_k \cdot \xi_{i,k} + \upsilon_i$$

with all the $\xi_{i,k}$ and υ_i being elements of $\mathcal{L}$. Finally, γ is a quadratic transformation from $GF(q)^v$ to $\mathcal{L}$, *i.e.* of the form

$$\gamma(V) = \sum_{1 \le k < \ell \ge v} V_k V_\ell \cdot \eta_{k,\ell} + \sum_{1 \le k \le v} V_k \cdot \sigma_k + \tau$$

with all the $\eta_{k,\ell}$, σ_k and τ being elements of $\mathcal{L}$.

By construction F has the multivariate degree ≤ 2 which can be verified by inspection, see also [12, 18]. Thus it can be re-written as a system of multivariate quadratic polynomials $F' = \varphi^{-1} \circ F \circ \varphi$.

13.2 The public key of an HFEv-

Let s be a random secret affine bijection $s : GF(q)^{h+v} \to GF(q)^{h+v}$.

Let t be a random secret affine bijection $t : GF(q)^{h} \to GF(q)^{h}$.

The public key G is defined as:

$$G(X) = \Big[t\Big(\varphi^{-1}\big(F_{[s(X)]_{h+1\to h+v}}(\varphi([s(X)]_{1\to h}))\big)\Big)\Big]_{1\to h-r}.$$

It may appear more clear to describe it as follows:

$$y \xleftarrow{1\to h-r} y||R \xleftarrow{t} B \xleftarrow{F_V} A \xleftarrow{1\to h} A||V \xleftarrow{s} x$$

Again G is quadratic, and it's direct expression as a multivariate quadratic transformation $G : GF(q)^{h+v} \to GF(q)^{h-r}$ constitutes the public key.

$$\begin{cases} y_1 = G_1(x_1, \ldots, x_{h+v}) \\ \quad\vdots \\ y_{h-r} = G_h(x_1, \ldots, x_{h+v}) \end{cases}.$$

13.3 Secret key

The secret key are $(t, F_V(Z), s)$.

13.4 Using the HFEv- trapdoor

We describe two ways of doing it. First and default randomised version picks V and R at random and proceeds as follows reiterating the whole process if failed to find an inverse of F_V:

$$y \xrightarrow{Random} y, V, R \xrightarrow{||} y||R, V \xrightarrow{t^{-1}} B, V \xrightarrow{F_V^{-1}} A, V \xrightarrow{||} A||V \xrightarrow{s^{-1}} x$$

A non deterministic version is called HFEv-δ.

Definition 13.4.1 (HFEv-δ). It is a HFEv- scheme which differs only in the way of carrying (secret) operation of computation of an inverse to the public key function, for example in order to compute a signature.

Instead of picking a random (R, V), it is determined by hashing y concatenated with some fixed secret value $\varDelta$ of 80 bits.

$$y \xrightarrow{(R,V)=SHA-1(y)} y, R, V \xrightarrow{||} y||R, V \xrightarrow{t^{-1}} B, V \xrightarrow{F_V^{-1}} A, V \xrightarrow{||} A||V \xrightarrow{s^{-1}} x$$

If failed to find an inverse of F_V, the obtained value is re-hashed to derive a second value that gives (R', V') etc.

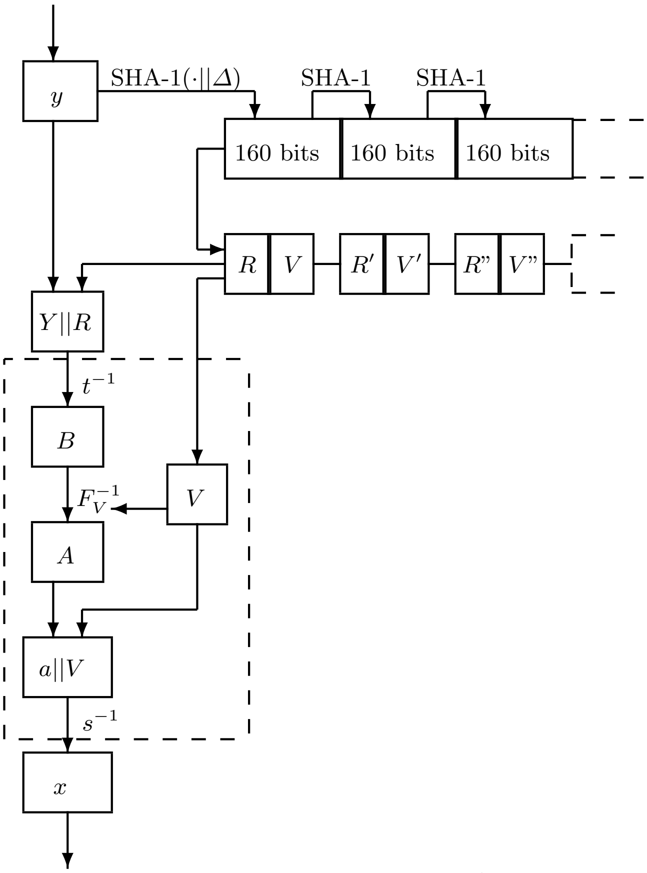

Fig. 1. Computing **one** inverse $x \in G^{-1}(y)$ for G∈HFEv-δ

14 Properties of HFEv-δ

Claim 14.0.2 (Operation δ). HFEv-δ provides better security than HFEv-.

It is not proven, and justified by the fact that there might be a chosen-message attack that exploit relationships between various signatures of the same message to "dismantle" the $v-$ part of the scheme, making it an algebraical trapdoor function, potentially weaker.

15 The structural security of HFEv- schemes

Theorem 15.0.3 (HFEv- ==>> HFE). If $v + r << h$ then the average-case HFEv- is at least as hard as the underlying HFE instance with regard to the Structural Cracking Problem.

Proof. We are going to show that any algorithm that recovers the structure of an HFEv- can be transformed into an algorithm that solves the underlying HFE. We show that we are almost certain that HFE structure is found. The probability that the structure found by structural attack for the HFEv- isn't the one we originally constructed, and that our internal HFE isn't the HFE someone else might have put in it, is bounded by the probability ϵ that two random HFEv- would give the same public key. We show that this probability ϵ is in turn negligible. Indeed since $v + r << h$, the cardinality of all possible $HFEv-$ is very roughly $q^{\mathcal{O}(Max(h^2,v^2,rh))}$, and it is very small compared to the cardinality of $\mathcal{MQ}(q, h+v, h-r)$, about $q^{\mathcal{O}(h^3)}$.

□

By inspection we verify that the claim is true more generally for all other versions of HFE, as long as the number of modifications remains small:

Theorem 15.0.4 (HFEv-+f ==>> HFE). If

$$v + r + f + u << h$$

then the average-case HFEv-+f is at least as hard as the underlying HFE instance with regard to the Structural Cracking Problem.

15.1 The Cracking Problem for HFEv- schemes

There is little hope that the reduction from HFEv- to HFE holds for direct Cracking Problem. It doesn't if, as we conjectured in Claims 12.1.1 and 8.0.2 the cryptosystems' structure is well hidden and they are as secure as MQ, that has no structural properties. In this case cracking attacks on a modified version of the scheme will only depend on the external parameter sizes m, n, and will be easier for HVEv- because m is smaller.

16 Non-encryption features of HFEv- schemes

We claim that there is no way to abuse an HFEv, HFEv- or an HFEv-δ trapdoor function to perform encryption provided that the difference between the number of inputs and outputs $n - m$ is large. First, since the output is shorter than the input, the message must have some redundancy in order to be uniquely decrypted. Such a redundancy can be described as a probability distribution on $x \leftarrow X$. Then we conjecture that:

Claim 16.0.1 (Non-encryption of HFEv-). Let $G \leftarrow HFEv-(q, h, v, r, d)$. The fastest algorithm that decrypts $x \leftarrow X$ given $G(x)$ runs approximately in the time of q^{r+v} inversions of $F_V()$.

We claim therefore that the owner of the secret key still needs to decrypt by exhaustive search on all inverses. When he computes an inverse x for a given y, he must choose and fix some $r + v$ variables (R, V). Then it seems that he has no control whatsoever which of the (average number) q^{r+v} inverses he is going to obtain.

It seems that the owner of the secret key always gets random inverses. We formalize it as:

Definition 16.0.2 (Pseudo-Randomly Invertible MQ). Let $G \leftarrow \mathcal{G}(q, m, w)$ a probability distribution of MQ functions $G : GF(q)^{m+w} \rightarrow GF(q)^m$, such that for each G there is an effective algorithm Inv_G that outputs with a probability ε one random inverse x of y.

We say that $G : GF(q)^{m+w} \rightarrow GF(q)^m$ is **Pseudo-Randomly Invertible MQ** if no adversary A can produce such a distribution $x \leftarrow X_A$ of values such that he (A) could distinguish between the following probability distributions:
$x \leftarrow X_A$ and
$x \leftarrow Inv_G(G(X_A))$.

Claim 16.0.3 (HFEv- $\in$ PRIMQ). If $r > 3$ and $v > 3$ then we conjecture that HFEv- is Pseudo-Randomly Invertible MQ.

17 Building non-encrypting PKI

As we explained in section 2.1, non-encryption is not enough. We are going to add components to HFEv-δ in order to make the *centralized leakage* impossible. First we put forward a simple construction based on the IP problem, called the HFEv-δ/ scheme, for which the security analysis with regard to the *centralized leakage* is easier and which conserves the security with respect structural and signature forgery attacks. We are going to conjecture that there is no way to leak data with HFEv-δ/.

Then we are going to propose a larger class of schemes called HFEv-δ/+f, with two additional parameters u and f, such that the case $u = f = 0$ is synonymous to HFEv-δ. This time we claim to increase security against structural attacks.

18 The HFEv-δ/ scheme

The scenario is the following:

Definition 18.0.4 (HFEv-δ/).

1. The User generates his secret and public key as $G \leftarrow$HFEv-δ, $G : GF(q)^{h+v} \rightarrow GF(q)^{h-r}$.
2. He sends to CA his public key G.
3. CA picks up a random affine isomorphism s, t.
4. CA sends the (s, t) to the User encrypted with G. It may be shown that only s is necessary.
5. CA publishes $G' = t \circ G \circ s$ as an official public key for the User.
6. The User composes the s, t with his own and modifies his secret information accordingly.
7. CA destroys all intermediate elements (it is not required for security though).

18.1 Inversion of an HFEv-δ/

This signature scheme is used exactly as the underlying $HFEv-$ scheme.

19 The HFEv-δ/+f scheme

Let u, f two integers such that $u + f$ is small and $u + f < v + r$.

Definition 19.0.1 (HFEv-δ+f).

1. The User generates his secret and public key as $G \leftarrow$HFEv-δ. Let $G : GF(q)^n \rightarrow GF(q)^m$ with $n = h + v$ variables and $m = h - r$ equations.
2. He sends to CA his public key G.
3. CA picks up u random quadratic equations with $n = h + v$ variables, we call $(G||H) : GF(q^{h+v}) \rightarrow GF(q^{h-r+u})$ the union of all the equations.
4. CA picks up a random affine injective and **non surjective** variable change $s' : GF(q^{h+v-f}) \rightarrow GF(q^{h+v})$.
   CA also picks a random affine bijection t'. Let:
   $$G' = t' \circ (G||H) \circ s'$$
5. CA sends the (s', t', H) to the User encrypted with G. It may be shown that only s' is necessary, and neither t' neither H need to be communicated.
6. CA publishes G' as an official public key for the User.
7. The User stores s' and t' as additional elements of his secret key.
8. CA destroys all intermediate elements (it is not required for security though).

We notice that a non-bijective s' corresponds to fixing some f entries and mixing (the operation ”f”).

The u added equations H, mixed subsequently with t', constitute the operation ”+”.

19.1 Inversion of an HFEv-δ/+f

It proceeds as the following:

1. Given y the User computes $y'||U = t^{-1}(y)$, with $y' \in GF(q)^{h-r}$ and $U \in GF(q)^u$.
2. Now he computes one possible $x' = G^{-1}(y')$ as in section 13.4 with an internal choice of about q^{v+r} possible inverses.
3. With a probability q^{-u} x' satisfies $H(x') = U$. Otherwise we go to 2.
4. With a probability q^{-f} x' has an inverse $x = s'^{-1}(x')$. Otherwise go to 2.
5. The steps 2-3 are iterated about q^{u+f} times until x is the needed inverse/signature.

Since one signature requires q^{u+f} repetitions of the above algorithm, $u + f$ should be small and for this reason the usage of "f" and "+" in signature was not advocated before. In the present paper we claim that it is interesting to use them, both for achieving better security against structural attacks, and as a tool to remove public key leakage.

20 The security of the HFEv-δ/ schemes

We refer to 12.1.1 and 12.1.2 for the analysis of the security against inversion of these schemes. In 7.3.1 we explain what does it imply in terms of real security. In fact the security of the HFEv-δ/ schemes is proven in 7.3.1, with suitable assumptions, but unfortunately not in the strongest possible sense.

What about the security against the *centralized leakage* ? We claim that the *centralized leakage* in HFEv-δ/+f public key, and even in the simplest version HFEv-δ/ is impossible. Moreover we separate the security against leakage of a $\mathcal{G}/+f$ scheme of the underlying trapdoor $\mathcal{G}$. It is formalized by the following.

Claim 20.0.1 (No centralized leakage). Let $\mathcal{G}/+f$ be the modified scheme $\mathcal{G}$, with $u \geq 0$ and $f \geq 0$. A user generates his public key $G \leftarrow \mathcal{G}$ at random.

Then CA generate a random key G' isomorphic to G. $G' = t \circ G \circ s$

We assume that $\mathcal{G}$ is a PRMQ.

If there is a user A that can embed a T-time verifiable property $A^G = 1$ in such a way that

$$Pr[(s,t) \leftarrow \text{Random} : A^{G'} = 1] > \varepsilon$$

Then

$$T \geq \varepsilon \cdot q^m$$

21 A proposed implementation of a Non-encrypting PKI

We put

$$q = 2, d = 25, h = 167, v = 76, r = 10, u = 4, f = 3.$$

Let $G \leftarrow HFEv - \delta / + f(q, d, h, v, r, u, f)$ be a public key. A valid signature for M is a σ such that

$$G(\sigma) = SHA - 1(M).$$

The claimed security level is 2^{80}.

One signature takes $q^{u+f} * 0.22 \approx 30$ seconds on a Pentium-III 500 MHz. For this we used the state-of-the-art library NTL for factoring polynomials by Victor Shoup [28], using a non-trivial algorithm of [29] for fast repeated squaring.

The signature length is $h + v - f = 240$ bits.

21.1 Short signatures

Still a shorter signature scheme with similar properties can be proposed, for this we need to use our trapdoor function G inside a Feistel-Patarin scheme with several inverses to compute the signatures as for example in [12, 18]. See also [13, 3]. It seems that there is a limit for signature length obtained with the HFEv- schemes, and for the security level of 2^{80} it seems difficult to propose signatures with much less than 128 bits as in Quartz [18]. However as showed in the section 19.4.2. of [3], it is possible to achieve the signatures of 92 bits with HFEf+.

Very recently, a very interesting signature scheme based on McEliece has been proposed by Finiasz, Courtois and Sendrier. It achieves the signature lengths as low as 87 bits [5].

22 Conclusion

The Multivariate Cryptography provides a very wide range of signature schemes that merit confidence for their multiple-level, security reinforcing construction.They seem to verify strong security notions that we defined in a present paper.

We showed how to build signature schemes such that the published key cannot be used to send encrypted messages to the user.

We achieved good confidence in impossibility to leak information by the means of the published key, while it is impossible to avoid leakage in general.

References

1. Mihir Bellare, Anand Desai, David Pointcheval, and Philip Rogaway: *Relations among Notions of Security for Public-Key Encryption Schemes;* In Crypto'98, LNCS 1462, pages 26-45. Springer-Verlag, Berlin, 1998.
2. Nicolas Courtois: *The security of Hidden Field Equations (HFE)*; Cryptographers' Track Rsa Conference 2001, San Francisco 8-12 April 2001, to appear in Springer-Verlag.
3. Nicolas Courtois: *La sécurité des primitives cryptographiques basées sur les problèmes algébriques multivariables MQ, IP, MinRank, et HFE*, PhD thesis, Paris 6 University, to appear in 2001, partly in English.
4. Nicolas Courtois: The HFE cryptosystem home page. Describes all aspects of HFE and allows to download an example of HFE challenge. http://hfe.minrank.org
5. Nicolas Courtois, Matthieu Finiasz and Nicolas Sendrier: *How to achieve a McEliece-based Digital Signature Scheme*; Preprint available at http://www.minrank.org/mceliece/
6. Michael Garey, David Johnson: *Computers and Intractability, a guide to the theory of NP-completeness*, Freeman, p. 251.
7. J. von zur Gathen, Victor Shoup, "Computing Fröbenius maps and factoring polynomials", Proceedings of the 24th Annual ACM Symposium in Theory of Computation, ACM Press, 1992.
8. Neal Koblitz: "Algebraic aspects of cryptography"; Springer-Verlag, ACM3, 1998, Chapter 4: "Hidden Monomial Cryptosystems", pp. 80-102.
9. Tsutomu Matsumoto, Hideki Imai: "Public Quadratic Polynomial-tuples for efficient signature-verification and message-encryption", Eurocrypt'88, Springer-Verlag 1998, pp. 419-453.
10. T. Okamoto and D. Pointcheval: *REACT: Rapid Enhanced-security Asymmetric Cryptosystem Transform;* In the Cryptographers' Track of the RSA Security Conference '2001, LNCS. Springer-Verlag, Berlin, 2001.
11. Jacques Patarin: "Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88"; Crypto'95, Springer-Verlag, pp. 248-261.
12. Jacques Patarin: "Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of Asymmetric Algorithms"; Eurocrypt'96, Springer Verlag, pp. 33-48. The extended version can be found at http://www.minrank.org/∼courtois/hfe.ps
13. Jacques Patarin: *La Cryptographie Multivariable*; Mémoire d'habilitation à diriger des recherches de l'Université Paris 7, 1999.
14. Jacques Patarin, Louis Goubin, Nicolas Courtois, + papers of Eli Biham, Aviad Kipnis, T. T. Moh, et al.: *Asymmetric Cryptography with Multivariate Polynomials over a Small Finite Field*; known as 'orange script', compilation of different papers with added materials. Available from J.Patarin@frlv.bull.fr.
15. Jacques Patarin, Nicolas Courtois , Louis Goubin: *Improved Algorithms for Isomorphism of Polynomials*; Eurocrypt 1998, Springer-Verlag.
16. Jacques Patarin, Nicolas Courtois , Louis Goubin: "C*-+ and HM - Variations around two schemes of T. Matsumoto and H. Imai"; Asiacrypt 1998, Springer-Verlag, pp. 35-49.
17. Jacques Patarin, Aviad Kipnis , Louis Goubin: "Unbalanced Oil and Vinegar Signature Schemes"; Eurocrypt 1999, Springer-Verlag.
18. Jacques Patarin, Louis Goubin, Nicolas Courtois: Quartz, **128**-*bit long digital signatures*; Cryptographers' Track Rsa Conference 2001, San Francisco 8-12 April 2001, to appear in Springer-Verlag.

19. Jacques Patarin, Louis Goubin, Nicolas Courtois: *Flash, a fast multivariate signature algorithm*; Cryptographers' Track Rsa Conference 2001, San Francisco 8-12 April 2001, to appear in Springer-Verlag.
20. D. Pointcheval, J. Stern: *Security arguments for Digital signatures and Blind Signatures;* Journal of Cryptology, Vol.13(3), Summer 2000, pp. 361-396.
21. Gustavus J. Simmons: *Subliminal channels; past and present;* European Trans. on Telecommunications 5 (1994) pp. 459-473.
22. Gustavus J. Simmons: The subliminal channels and Digital Signatures; Eurocrypt 84, Springer-Verlag, LNCS 0209, pp. 364-378.
23. Gustavus J. Simmons: Subliminal Communication is Easy using the DSA; Eurocrypt 93, Springer-Verlag, LNCS 765, pp. 218-232.
24. Adi Shamir: "Efficient signature schemes based on birational permutations"; Crypto'93, Springer-Verlag, pp1-12.
25. Nicolas Courtois, Adi Shamir, Jacques Patarin, Alexander Klimov, *Efficient Algorithms for solving Overdefined Systems of Multivariate Polynomial Equations*, In Advances in Cryptology, Eurocrypt'2000, LNCS 1807, Springer-Verlag, pp. 392-407.
26. Adi Shamir, Aviad Kipnis: "Cryptanalysis of the HFE Public Key Cryptosystem"; Crypto'99. Can be found at http://www.minrank.org/∼courtois/hfesubreg.ps
27. J.O. Shallit, G.S. Frandsen, J.F. Buss, *The computational complexity of some problems of linear algebra*, BRICS series report, Aarhus, Denmark, RS-96-33. Available at http://www.brics.dk/RS/96/33
28. The library NTL for integers, factoring polynomials over finite fields, LL, etc. Available at http://www.shoup.net and free for educational purposes.
29. E. Kaltofen, V. Shoup, *Fast polynomial factorization over high algebraic extensions of finite fields*, in Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation, 1997.
30. Adam Young, Moti Yung: *Towards Signature-Only Signature Schemes*; In Advances of Cryptology, Asiacrypt 2000, LNCS 1976, Springer-Verlag.