Taxonomy of Public Key Schemes based on the problem of $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic equations

Christopher Wolf, and Bart Preneel
{Christopher.Wolf, Bart.Preneel}@esat.kuleuven.ac.be
chris@Christopher-Wolf.de
K.U.Leuven, ESAT-COSIC
Kasteelpark Arenberg 10
B-3001 Leuven-Heverlee, Belgium
http://www.esat.kuleuven.ac.be/cosic/

Abstract

Multivariate quadratic systems can be used to construct both secure and efficient public key schemes. In this article, we introduce the necessary mathematical tools to deal with multivariate quadratic systems, present an overview of important schemes known so far and outline how they fit into a taxonomy of only four basic schemes and some generic modifiers. Moreover, we suggest new constructions not previously considered. In this context, we propose some open problems and new research directions in the field of multivariate quadratic schemes.

Cryptology ePrint Archive, Report 2005/077
http://eprint.iacr.org/

Current Version: 2005-12-15
First Revision: 2005-05-12
First Version: 2005-03-12

Contents

1 Introduction

Public key cryptography is used in e-commerce systems for authentication (electronic signatures) and secure communication (encryption). The security of cryptosystems widely used at the moment is based on the difficulty of solving a small class of problems: the RSA scheme relies on the difficulty of factoring large integers, while the hardness of solving discrete logarithms provide the basis for ElGamal and Elliptic Curves [MvOV96]. Given that the security of these public key schemes relies on such a small number of problems that are currently considered to be hard, research on new schemes based on other classes of problems is necessary as such work will provide greater diversity and hence forces cryptanalysts to spend additional effort concentrating on completely new types of problems. Moreover, we make sure that not all "crypto-eggs" are in one basket. In this context, we want to point out that important results on the potential weaknesses of existing public key schemes are emerging. In particular techniques for factorisation and solving discrete logarithm improve continually. For example, polynomial time quantum algorithms [Sho97] can be used to solve both problems. Therefore, the existence of quantum computers in the range of 1000 bits would be a real-world threat to systems based on factoring or the discrete logarithm problem. This stresses the importance of research into new algorithms for asymmetric cryptography.

One proposal for secure public key schemes is based on the problem of solving $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic equations ($\mathcal{MQ}$-problem) over finite fields. This article introduces the necessary mathematical tools and develops a taxonomy of $\mathcal{MQ}$-schemes.

1.1 Related Work

As outlined above, we concentrate on $\mathcal{M}$ultivariate $\mathcal{Q}$*uadratic* equations over finite fields in this text. They have the nice property that an attacker does not even know which type of scheme he attacks, given the public key alone, *i.e.*, we have a kind of "secret public key schemes" [Pat00]. When organising the material for this article, we had to draw the line somewhere. Therefore, we decided to use the degree of the public key polynomials, *i.e.*, other multivariate schemes which are based on equations of higher degree are not considered, *e.g.*, the polynomial substitution scheme of [FD85], or the Dragon scheme from [Pat96a]. In this context we also want to mention the Bi-Quadratic C* scheme of [DF05]. Similarly, we do not consider birational permutations [Sha93], as they are based on finite rings rather than finite fields. Moreover, they have been successfully cryptanalysed in [CSV93, The95, CSV97]. In addition, we do not consider the matrix based schemes from [PGC98a] either, as its use has been strongly discouraged in the very paper were it has been developed, and also is not an $\mathcal{MQ}$-system in this stronger sense. Moreover, there is also a survey paper [DS04] which includes several schemes based on factoring, too.

In this context we refer to Section 2.2: there, we outline while quadratic equations play such a prominent role. In a nutshell, they are already $\mathcal{NP}$-complete while the number of coefficients is still reasonably small. This also stresses why we decided to concentrate on schemes based on $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic equations rather than including other schemes.

1.2 Outline

After having briefly considered related work, we move on to the organisation of this paper. In the next section, we give some basic mathematical theory necessary for the development of $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic schemes. This includes formulas for the size of the public key, the signing and encryption process, the general $\mathcal{MQ}$-trapdoor, and $\mathcal{MQ}$-related problems. After this, we move on to the core of this paper, *i.e.*, the taxonomy of schemes based on $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic polynomials. These basic schemes are Unbalanced Oil and Vinegar (UOV, Section 3.1), Stepwise Triangular Systems (STS, Section 3.2), the Matsumoto-Imai Scheme A (MIA, Section 3.3), and Hidden Field Equations (HFE, Section 3.4). Following this, we continue with generic modifiers of multivariate schemes, *i.e.*, modifications which can be applied for any form of the central equations, cf Section 4 for more details. After developing this taxonomy we briefly discuss how the basic trapdoors and the modifiers were applied in practice to derive concrete schemes. This is followed by a brief discussion of the recent development of “mixed schemes” in Section 6. Using the theory developed in the previous sections of this article, we sketch some new schemes in Section 7. This article concludes with Section 8.

2 General $\mathcal{MQ}$-construction

In this section, we introduce some properties and notations useful for the remainder of this article. After briefly introducing finite fields, we concentrate on the general problem of multivariate polynomial equations, consider affine transformations, and also the two related problems MinRank and Isomorphism of Polynomials.

2.1 Finite Fields

As finite fields are a very basic building block for these kind of schemes, we start with properly introducing them. Loosely speaking, a finite field consists of a (finite) set of elements, and two operations, namely addition (denoted "+") and multiplication (denoted "·"). These operations need to fulfil certain criteria:

Definition 2.1 *Let* $(\mathbb{F}, +, \cdot)$ *be a set of* $q \in \mathbb{N}$ *elements with the two operations addition* $+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ *and multiplication* $\cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$*. We call* $(\mathbb{F}, +, \cdot)$ *a* field *if the following axioms are fulfilled:*

1. additive Abelian group $(\mathbb{F}, +)$*:*

   (a) associativity*:* $\forall a, b, c \in \mathbb{F} : ((a + b) + c) = (a + (b + c))$

   (b) additive neutral*:* $\exists e \in \mathbb{F} : \forall a \in \mathbb{F} : a + e = a$*. In the remainder of this article, we denote this* e *with 0*

   (c) additive inverse*:* $\forall a \in \mathbb{F}\ \exists a' \in \mathbb{F} : a + a' = 0$*. In the remainder of this article, we denote this* a' *with* $-a$

   (d) commutativity*:* $\forall a, b \in \mathbb{F} : a + b = b + a$

2. multiplicative Abelian group $(\mathbb{F}^*, \cdot)$ *for* $\mathbb{F}^* := \mathbb{F} \setminus \{0\}$*:*

   (a) associativity*:* $\forall a, b, c \in \mathbb{F} : ((a \cdot b) \cdot c) = (a \cdot (b \cdot c))$

   (b) multiplicative neutral*:* $\exists e \in \mathbb{F} : \forall a \in \mathbb{F} : a \cdot e = a$*. In the remainder of this article, we denote this* e *with 1*

   (c) multiplicative inverse*:* $\forall a \in \mathbb{F}^*\ \exists a' \in \mathbb{F}^* : a \cdot a' = 1$*. In the remainder of this article, we denote this* a' *with* a^{-1}

   (d) commutativity*:* $\forall a, b \in \mathbb{F} : a \cdot b = b \cdot a$

3. distributivity*:* $\forall a, b, c \in \mathbb{F} : a \cdot (b + c) = a \cdot b + a \cdot c$

Remark. For brevity, we write ab instead of $a \cdot b$. If it is clear from the context which addition and multiplication we use with the field, we also write $\mathbb{F}$ instead of $(\mathbb{F}, +, \cdot)$.

Definition 2.2 *Let* q *be a prime number,* $\mathbb{F} := \{0, \ldots, q - 1\}$*, and addition and multiplication usual integer addition and multiplication modulo this prime number* q*. Then we call* $(\mathbb{F}, +, \cdot)$ *a* prime field*.*

Definition 2.3 *Let $\mathbb{F}$ be a field and $i(t) \in \mathbb{F}[t]$ an irreducible univariate polynomial in the variable t over $\mathbb{F}$ with degree n. Furthermore, we define the set $\mathbb{E} := \mathbb{F}[t]/i(t)$,* i.e.*, polynomials in t with coefficients from $\mathbb{F}$, the operation addition "+" as normal addition of polynomials, and "$\cdot$" multiplication of polynomials modulo the irreducible polynomial $i(t)$. Then we call $(\mathbb{E}, +, \cdot)$ a* polynomial field *and also say that it is a degree n* extension *of the* ground field *$\mathbb{F}$.*

We want to point out that definitions 2.1, 2.2, and 2.3 are consistent: it it possible to prove that the construction from the two latter comply with the field axioms from the first. The corresponding proofs and further properties of finite fields can be found in [LN00]. In particular, we want to stress the following

Lemma 2.4 *Let $\mathbb{F}$ be a finite field and let $q := |\mathbb{F}|$ be the number of its elements. Then we have $\forall x \in \mathbb{F} : x^q = x$* (Frobenius automorphism)*.*

This lemma will prove particular useful in the context of schemes defined over extension fields (cf sections 3.3 and 3.4) and in the context of affine transformations (cf Section 2.3); efficient implementation of arithmetic on finite fields can be found in [BSS99, LD00].

2.2 Considerations about Multivariate Polynomial Equations

After introducing finite fields, we move on to the problem of solving a system of multivariate polynomial equations. Let $n \in \mathbb{N}$ be the number of variables, $m \in \mathbb{N}$ the number of equations, and $d \in \mathbb{N}$ the degree of the system. Here $x_1, \ldots, x_n$ are variables over $\mathbb{F}$. By convention, we set $x_0 := 1$, *i.e.*, the multiplicative neutral in $\mathbb{F}$. Furthermore, for given $n, d \in \mathbb{N}$ we define

$$\mathcal{V}_n^d := \begin{cases} \{0\} & \text{for } d = 0 \\ \{v \in \{0, \ldots, n\}^d : i \leq j \Rightarrow v_i \leq v_j\} & \textit{otherwise} \end{cases}$$

where we denote components of the vector v by $v_1, \ldots, v_d \in \{0, \ldots, n\}$. We are now able to state the problem of multivariate polynomial equations. Let $\mathcal{P}$ be a system of m polynomials in n variables with maximum degree $d \in \mathbb{N}$ each, *i.e.*, we have $\mathcal{P} := (p_1, \ldots, p_m)$ where all p_i have the form

$$p_i(x_1, \ldots, x_n) := \sum_{v \in \mathcal{V}_n^d} \gamma_{i,v} \prod_{j=1}^{d} x_{v_j} \text{ for } 1 \leq i \leq m$$

with the coefficients $\gamma_{i,v} \in \mathbb{F}$ and vectors $v \in \mathcal{V}_n^d$.

This allows us to define the problem of Simultaneous Multivariate Equations (SME): Let $y_1, \ldots, y_m \in \mathbb{F}$ be some field elements and multivariate polynomials $p_1, \ldots, p_m$ defined as above. Then finding a solution $x \in \mathbb{F}^n$ for the simultaneous system of equations in the polynomial vector $\mathcal{P}$ and given $y \in \mathbb{F}^m$ is called an SME-problem, cf Figure 1.

$$\left\{\begin{array}{rcl} y_1 & = & p_1(x_1, \ldots, x_n) \\ y_2 & = & p_2(x_1, \ldots, x_n) \\ & \vdots & \\ y_m & = & p_m(x_1, \ldots, x_n) \end{array}\right.$$

Figure 1: Example of an SME-problem with n variables and m equations

The key-length in a system based on the intractability of the simultaneous solving of multivariate, non-linear equations (*i.e.*, $d \geq 2$) can be computed using the following formulas. Therefore, we first define

$$\tau^d(\mathbb{F}^n) \quad := \quad \sum_{i=0}^{d} \tau_{(i)}(\mathbb{F}^n) \tag{1}$$

for the number of terms in a single polynomial equation over $\mathbb{F}$, maximal degree d and in n variables. Here, we have

$$\tau_{(d)}(\mathbb{F}^n) := \left\{\begin{array}{ll} \sum_i^{\min(|\mathbb{F}|-1,d)} \binom{n}{i} & \text{for } d > 0 \\ 1 & \text{for } d = 0 \end{array}\right. \tag{2}$$

for the number of terms for all degrees. For the correctness of the above formula, we notice that we have $x^{q-1} = 1$ with $q := |\mathbb{F}|$ in all finite fields (cf Lemma 2.4).

In particular, this leads to the following size function for given parameters $\mathbb{F}, n, m, d$:

$$\mathit{size}(\mathbb{F}, n, m, d) := m\tau^d(\mathbb{F}^n) \log_2 q\ . \tag{3}$$

In general, we obtain a key-length of $O(mn^d)$ for the public key — or $O(n^{d+1})$ for $m = n$.

For any q and $d = 2$, we speak about the problem of $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic equations and denote the class of corresponding polynomial vectors $\mathcal{P}$ with $\mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$ (cf Figure 1 for the general case). As we will see below, this class plays an important role for the construction of public key schemes based on the problem of polynomial equations in finite fields. Therefore, we state the polynomials p_i explicitly for this case:

$$\begin{aligned}
p_1(x_1, \ldots, x_n) &:= \sum_{1 \le j \le k \le n} \gamma_{1,j,k} x_j x_k + \sum_{j=1}^{n} \beta_{1,j} x_j + \alpha_1 \\
&\vdots \\
p_i(x_1, \ldots, x_n) &:= \sum_{1 \le j \le k \le n} \gamma_{i,j,k} x_j x_k + \sum_{j=1}^{n} \beta_{i,j} x_j + \alpha_i \\
&\vdots \\
p_m(x_1, \ldots, x_n) &:= \sum_{1 \le j \le k \le n} \gamma_{m,j,k} x_j x_k + \sum_{j=1}^{n} \beta_{m,j} x_j + \alpha_m
\end{aligned}$$

for $1 \le i \le m, 1 \le j \le k \le n$, and the coefficients $\gamma_{i,j,k}, \beta_{i,j}, \alpha_i \in \mathbb{F}$. In the case of $d = 2$, we call them quadratic ($\gamma_{i,j,k}$), linear ($\beta_{i,j}$), and constant (α_i) coefficients, respectively. For short, we write the polynomial vector $\mathcal{P} := (p_1, \ldots, p_m)$ and we have $\mathcal{P} \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$. By convention, we have $j < k$ for $q = 2$ as $x_i^2 = x_i$ in GF(2). For brevity, we write $\mathcal{MQ}(\mathbb{F}^n)$ rather than $\mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^n)$, *i.e.*, if the number of variables is equal to the number of equations.

In addition, we give the formula for the number of terms for *one* polynomial of the $\mathcal{MQ}$-problem explicitly:

$$\tau(n) := \begin{cases} 1 + n + \frac{n(n-1)}{2} = 1 + \frac{n(n+1)}{2} & \text{if } \mathbb{F} = GF(2) \\ 1 + n + \frac{n(n+1)}{2} = 1 + \frac{n(n+3)}{2} & \text{otherwise .} \end{cases} \tag{4}$$

The above formula assumes polynomials with quadratic and linear terms plus a constant term.

The prominent role of $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic equations is easily seen by the two following observations: first, the public key size increases with $O(mn^d)$ — and is hence very sensitive to the degree d. Therefore, we want d to be as small as possible. On the other hand, solving quadratic systems is already $\mathcal{NP}$-complete and also hard on average. We refer the reader to cf [GJ79, p. 251] and [PG97, App.]. A detailed proof can be found in [Wol02, Sect. 3.2].

2.3 Affine Transformations

As we will see in the following sections, affine transformations play an important role in the theory of $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic public key systems. Hence, to have all necessary tools at hand in the next section, we review some of their properties. In this context, the following proves useful:

Lemma 2.5 *Let $\mathbb{F}$ be a finite field with $q := |\mathbb{F}|$ elements. Then we have $\prod_{i=0}^{n-1} \left(q^n - q^i\right)$ invertible $(n \times n)$-matrices over $\mathbb{F}$.*

Proof. We observe that we have full choice for the first row vector of our matrix — except the zero-vector. With an inductive argument we see that we have full choice for each consecutive row vector — except the span of the previous row vectors. Hence, we have $\left(q^n - q^{j-1}\right)$ independent choices for the j^{th} row vector. □

Next, we recall some basic properties of affine transformations over the finite field $\mathbb{F}$ and its n^{th} degree extension $\mathbb{E}$.

Remark. In the remainder of this text, we denote elements of vector spaces by small letters and elements of extension fields by capital letters, *e.g.*, vector $x \in \mathbb{F}^n$ but element $X \in \mathbb{E}$.

Definition 2.6 *Let $M_S \in \mathbb{F}^{n \times n}$ be an $(n \times n)$ matrix and $v_s \in \mathbb{F}^n$ a vector and let $S(x) := M_S x + v_s$. We call this the "matrix representation" of the affine transformation S.*

Definition 2.7 *Moreover, let $s_1, \ldots, s_n$ be n polynomials of degree 1 at most over $\mathbb{F}$,* i.e., *$s_i(x_1, \ldots, x_n) := \beta_{i,1}x_1 + \ldots + \beta_{i,n}x_n + \alpha_i$ with $1 \leq i, j \leq n$ and $\alpha_i, \beta_{i,j} \in \mathbb{F}$. Let $S(x) := (s_1(x), \ldots, s_n(x))$ for $x := (x_1, \ldots, x_n)$ a vector over $\mathbb{F}^n$. We call this the "multivariate representation" of the affine transformation S.*

Remark. The multivariate and the matrix representation of an affine transformation S are interchangeable. We only need to identify the corresponding coefficients: $(M_S)_{i,j} \leftrightarrow \beta_{i,j}$ and $(v_S)_i \leftrightarrow \alpha_i$ for $1 \leq i, j \leq n$.

In addition, we can also use the "univariate representation" over the extension field $\mathbb{E}$ of the transformation S.

Definition 2.8 *Let $0 \leq i < n$ and $A, B_i \in \mathbb{E}$. Then we call the polynomial $S(X) := \sum_{i=0}^{n-1} B_i X^{q^i} + A$ the "univariate representation" of the affine transformation $S(X)$.*

Lemma 2.9 *An affine transformation in univariate representation can be transfered efficiently in multivariate representation and vice versa.*

Proof. This lemma follows from [KS99, Lemmata 3.1 and 3.2] by a simple extension from the linear to the affine case. □

In the remainder of this paper, we will denote the class of *affine* transformations $\mathbb{F}^n \to \mathbb{F}^n$ by $\mathrm{Aff}_0(\mathbb{F}^n)$, and the class of linear transformations, *i.e.*, with the constant term equal to 0, will be denoted by $\mathrm{Hom}_0(\mathbb{F}^n)$ for *homomorphism*. In both cases, the subscript $_0$ indicates that the all zero transformation is also included in this set. Moreover, for affine and linear transformations, we can use the matrix representation to determine if the corresponding transformation is a bijection or not. For a bijection, the matrix M_S needs to have full rank. In most cases, we will use bijections in this paper and hence, use $\mathrm{Aff}^{-1}(\mathbb{F}^n)$ and $\mathrm{Hom}^{-1}(\mathbb{F}^n)$, *i.e.*, the class of *invertible* affine and homomorphic transformations, respectively. In this context we want to stress that $(\mathrm{Aff}^{-1}(\mathbb{F}^n), \circ)$ and $(\mathrm{Hom}^{-1}(\mathbb{F}^n), \circ)$ form groups where $\circ$ denotes function composition.

At some points, we will not only need affine transformations within the same vector space, but a affine transformations $S(x) : \mathbb{F}^n \to \mathbb{F}^m$ with $n \neq m$. We therefore extend our notation to $\mathrm{Aff}^{-1}(\mathbb{F}^n, \mathbb{F}^m)$ and $\mathrm{Hom}^{-1}(\mathbb{F}^n, \mathbb{F}^m)$ in this case, respectively. Obviously, the corresponding transformations cannot be bijective anymore, but injective in the case $n < m$ and surjective in the case $n > m$. As in the case of bijective transformations, we can use the rank of the corresponding matrix to determine if a given transformation is injective or surjective. Moreover, function composition is no longer defined on these objects and hence, $(\mathrm{Aff}^{-1}(\mathbb{F}^n, \mathbb{F}^m), \circ)$ $(\mathrm{Hom}^{-1}(\mathbb{F}^n, \mathbb{F}^m), \circ)$ are no groups anymore.

2.4 $\mathcal{MQ}$-trapdoor

To be useful for public key cryptology, we do not only need an intractable problem, but also a way of embedding a trapdoor into it. For the $\mathcal{MQ}$-problem as stated in Section 2.2, we are able to embed a trapdoor $(S, \mathcal{P}', T)$ into a system of equations $\mathcal{P}$, cf Figure 2. Here we have $(S, \mathcal{P}', T) \in \mathrm{Aff}^{-1}(\mathbb{F}^n) \times \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m) \times \mathrm{Aff}^{-1}(\mathbb{F}^m)$ and $\mathcal{P} \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$, *i.e.*, S is an invertible affine transformation $S : \mathbb{F}^n \to \mathbb{F}^n$ and T is an invertible affine transformation $T : \mathbb{F}^m \to \mathbb{F}^m$. Moreover, $\mathcal{P}'$ is a polynomial vector as defined in Section 2.2, *i.e.*, all m polynomials in n variables each have degree $d = 2$. In particular, we have $\mathcal{P}'$ as a function $\mathcal{P}' : \mathbb{F}^n \to \mathbb{F}^m$. In the remainder of

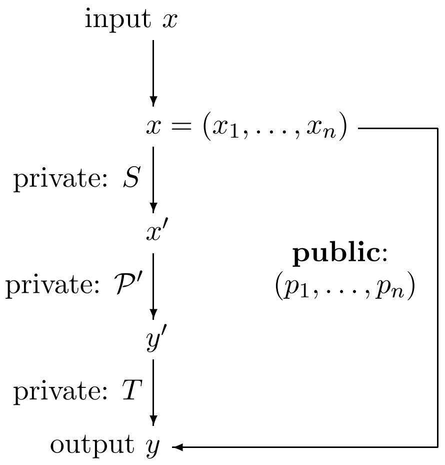

Figure 2: Graphical Representation of the $\mathcal{MQ}$-trapdoor $(S, \mathcal{P}', T)$

this paper, we denote components of the hidden quadratic transformation $\mathcal{P}'$ by a prime $'$, *e.g.*, the variables $x'_1, \ldots, x'_n$ or the coefficients $\alpha'_i, \beta'_{i,j}, \gamma'_{i,j,k}$ for $1 \leq i \leq m$ and $1 \leq j \leq k \leq n$. In general, $\mathcal{P}'$ consists of non-homogeneous polynomials, *i.e.*, we have at least one non-zero $\beta'_{i,j}$ and one non-zero α'_i in this polynomial-vector.

We want to point out that the trapdoor from Figure 2 is the only one possible: as we restricted our attention to $\mathcal{M}$ultivariate $\mathcal{Q}$*uadratic* equations, we cannot have a degree higher than 2 for the public key equations. But this implies immediately that we can have at most one degree 2 transformation in the overall construction. Hence, all variations of $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic systems (cf Section 4) can only use degree one equations for the two affine transformations S, T and some hidden invertible *quadratic* system of polynomials for $\mathcal{P}'$. In particular, these two affine transformations are used to hide the internal structure of the central equations $\mathcal{P}'$ from the eyes of an attacker. This is necessary as we need the central map $\mathcal{P}'$ to be invertible in contrast to the public key $\mathcal{P}$ alone.

Another way of "modifying" the above trapdoor is the use of several affine transformations. However, as we saw in the previous section, this does not help as affine transformations form a group and hence, are closed under composition.

2.4.1 Signature Verification

Signature verification is the same for all schemes based on the difficulty of the $\mathcal{MQ}$-problem: evaluate the polynomial vector $\mathcal{P}$ with a given signature $x \in \mathbb{F}^n$. If the result is the same as the given message vector $y \in \mathbb{F}^m$, we accept the signature, otherwise we reject. For short, we write $y \overset{?}{=} \mathcal{P}(x)$ where $\overset{?}{=}$ denotes comparison.

More detailed, we perform the following m checks in $\mathbb{F}$:

$$\begin{aligned} y_1 &\overset{?}{=} p_1(x_1, \ldots, x_n) \\ &\vdots \\ y_m &\overset{?}{=} p_m(x_1, \ldots, x_n) \end{aligned}$$

As each polynomial has $\tau(n) = O(n^2)$ coefficients (cf Section 2.2), such an evaluation takes a total of $O(mn^2)$ multiplications and additions in the finite field $\mathbb{F}$. Strategies for fast evaluation of the public key are discussed in [CGP01, CGP03a].

2.4.2 Signature Generation

To generate a signature using the trapdoor $(S, \mathcal{P}', T)$, we observe that we need to invert each individual step, *i.e.*, we need to compute the vector $y' := T^{-1}(y)$ for given y, followed by $x' := \mathcal{P}'^{-1}(y')$, and finally $x := S^{-1}(x')$, cf Figure 2.

We start with the inversion of $S(x)$: as we saw in Section 2.3, we can write this affine transformation using an invertible matrix $M \in \mathbb{F}^{n \times n}$ and a vector $v \in \mathbb{F}^n$, *i.e.*, we have $S(x) := Mx + v$. Therefore, its inverse transformation is given by $S^{-1}(x) := M^{-1}(x - v)$. Similar, we can invert the affine transformation T.

Things are more complicated for the system of polynomials $\mathcal{P}'$ as inversion strategies differ for individual trapdoor functions, *e.g.*, MIA, HFE, STS, or UOV. Therefore, we will discuss the inversion strategy in the individual sections (cf Section 3). However, we want to stress that it is enough to find *one* pre-image of $\mathcal{P}$ to obtain a valid signature, *i.e.*, we only need some $x' \in \mathbb{F}^n$ with $\mathcal{P}'(x') = y'$ for given $y' \in \mathbb{F}^m$. In case $\mathcal{P}' : \mathbb{F}^n \to \mathbb{F}^m$ and hence $\mathcal{P} : \mathbb{F}^n \to \mathbb{F}^m$ is not a surjection, we add some random bits to the input $x \in \mathbb{F}^n$, cf [CGP01] for an outline of this idea. In a nutshell, even a small number of random bits, *e.g.*, 7 bits as discussed in [CGP01], ensures that we obtain valid signatures with a probability of $1 - 2^{187}$ for any given message $x \in \mathbb{F}^n$. As we will see in the next section, matters are slightly more complicated for decryption.

2.4.3 Decryption

Decryption and signature generation are quite similar — except for the fact that we usually need to compute *all* possible pre-images $X'_1, \ldots, X'_k \in \mathbb{F}^n$ which satisfy the equation $\mathcal{P}'(X') = y'$ for given $y' \in \mathbb{F}^m$ and some $k \in \mathbb{N}$. Depending on the scheme used, it may happen that we do not have a unique solution X' for this equation. Hence, we need a possibility to pick the right X_i from the set of all possible solutions $Q := \{X_i \in \mathbb{F}^n : X_i := S^{-1}(X'_i) \text{ for } 1 \leq i \leq k\}$. Assuming that we decrypt a valid cipher text, we have Q non-empty and hence, $k \in \mathbb{Z} : k \geq 1$.

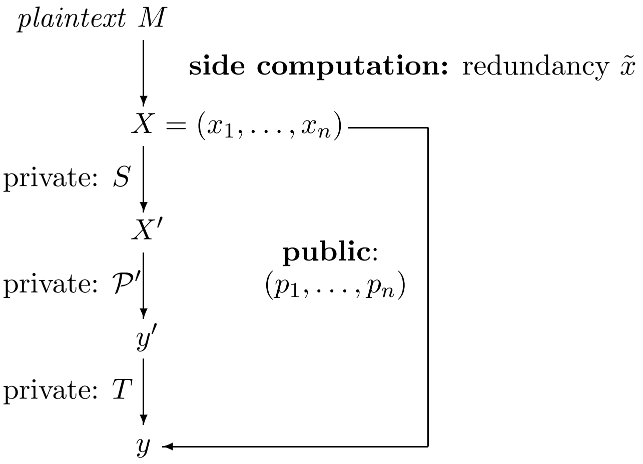

Figure 3: $\mathcal{MQ}$-systems for Encryption of Message M with Ciphertext $(y, \tilde{x})$

This problem has been discussed in [Pat96b] and its author suggests to use either error-correcting codes or a cryptographically secure hash function for this purpose. To the knowledge of the authors of this article, only hash functions have been used so far in this context. Denote such a hash function $H(\cdot) : \mathbb{F}^n \rightarrow \{0,1\}^h$ where h is the length of the hash string. Hence, during encryption (see below), also the hash $\tilde{x} := H(x)$ is computed and then used to pick the right X_i from the set Q by simply checking if the corresponding hashes match, *i.e.*, if we have $H(X_i) \overset{?}{=} \tilde{x}$. As the hash function is assumed to be cryptographically secure, an attacker cannot use the knowledge of $\tilde{x}$ to gain an advantage when computing x. However, the workload of this procedure clearly depends on the size of the set Q: on average, we will need to check $|Q|/2$ elements before finding the right X_i. Hence, Q may not be too large in practice. As we will see below, this is a serious obstacle for constructing a secure and efficient encryption scheme based on the $\mathcal{MQ}$-problem.

In this context, the question of the optimal length of the output of such a hash function is also important: having the corresponding hash too short, we may not be able to find a unique x_i from the set Q. Having h too long, we waste bandwidth. This question has been elaborated in [Dau01, Section 2.3.3]. In a nutshell, we need an 80 bit hash to have a probability of $1-2^{-80}$ for unique decryption. More general, we need h bit to have a probability of $1-2^h$ for unique deciphering.

Using the idea of an error correcting code on x, *i.e.*, to encode a message M using some code word x, and only accepting elements from Q which are a correct codeword, does not seem to have advantages over the idea of using hash-functions but enforces a bigger parameter n. Hence, the number of coefficients increases and also the time for decryption or encryption. Moreover, having redundancy in the clear text is usually not a good idea as it could be exploited in an attack. We therefore do not advise this strategy but encourage the use of hash-functions here.

A similar strategy is padding: here, the first $f < n$ bits of the message vector $X \in \mathbb{F}^n$ are fixed to some values $v_1, \ldots, v_f \in \mathbb{F}$ and only signatures with $x_1 = v_1, \ldots, x_f = v_f$ are accepted. Here, we have the same concerns as for methods using error correcting codes: we need a bigger parameter n for secure schemes but may give the adversary an advantage.

2.4.4 Encryption

As discussed in the previous section, the function $\mathcal{P}'(x') = y'$ is usually not surjective — and consequently, neither is $\mathcal{P}(x) = y$. Hence, we need to compute some redundancy to allow unique decryption, cf Figure 3. Therefore, encryption consists of two steps: first, we evaluate the public key and second, we compute this redundancy $\tilde{x}$:

1. $y := \mathcal{P}(x)$
2. $\tilde{x} := H(x)$

for some hash function $H(\cdot)$, cf previous section. The encrypted message now consists of the pair $(y, \tilde{x}) \in \mathbb{F}^m \times \{0,1\}^h$ for $h \in \mathbb{N}$ being the length of the hash-string used. In contrast to decryption, encryption is always unique as there exists only one $y \in \mathbb{F}^m$ for any given $x \in \mathbb{F}^n$.

2.4.5 General Linearization Attack

Here we describe a very general attack against all public key systems which use $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic equations as their public key. To the knowledge of the authors, it has first been described in [Pat96b, Sect. 3]. Here, we assume that we know $y, \hat{y} \in \mathbb{F}^m$ and some difference $\Delta \in \mathbb{F}^n$ with $\Delta = (\delta_1, \ldots, \delta_n)$. Now we have $y = \mathcal{P}(x)$ and $\hat{y} = \mathcal{P}(x + \Delta)$ for some unknown vector $x \in \mathbb{F}^n$. We subtract the two equations $y = \mathcal{P}(x)$ and $\hat{y} = \mathcal{P}(x + \Delta)$ component-wise, and get

$$\begin{array}{rcl}
y_i - \hat{y}_i & = & p_i(x_1, \ldots, x_n) - p_i(x_1 + \delta_1, \ldots, x_n + \delta_n) \\
& = & (\gamma_{i,0} - \gamma_{i,0}) + \\
& & +\gamma_{i,1}(x_1 - x_1 - \delta_1) + \cdots + \gamma_{i,n}(x_n - x_n - \delta_n) + \\
& & +\gamma_{i,1,1}(x_1^2 - x_1^2 + 2x_1\delta_1 - \delta_1^2) + \\
& & +\gamma_{i,1,2}(x_1x_2 - x_1x_2 - x_1\delta_2 - x_2\delta_1 - \delta_1\delta_2) + \cdots + \\
& & +\gamma_{i,n,n}(x_n^2 - x_n^2 + 2x_n\delta_n - \delta_n^2) \\
& & +\beta_{i,1}(x_1 - x_1 - \delta_1) + \ldots + \beta_{i,n}(x_n - x_n - \delta_n) + +\alpha_i - \alpha_i \\
& = & -\gamma_{i,1}\delta_1 - \cdots - \gamma_{i,n}\delta_n \\
& & +\gamma_{i,1,1}(2x_1\delta_1 - \delta_1^2) + \gamma_{i,1,2}(-x_1\delta_2 - x_2\delta_1 - \delta_1\delta_2) + \cdots + \\
& & +\gamma_{i,n,n}(2x_n\delta_n - \delta_n^2) \\
& & -\beta_{i,1}\delta_1 - \ldots - \beta_{i,n}\delta_n
\end{array}$$

for $1 \le i \le m$. This yields a system of equations linear in $x_1, \ldots, x_n$. A solution can therefore be computed in polynomial time, *e.g.*, by Gaussian elimination.

This attack can be avoided by padding the vector x with random elements of $\mathbb{F}$ or by introducing a linearly resistant permutation (*e.g.*, AES with a publicly known key). Although we need to make sure that they are not valid in a specific application domain, the assumptions that have to be made for the attack are rather unlikely to be satisfied in reality.

2.5 Extension Fields Revisited

After concentrating on the use of $\mathcal{M}$ultivariate $\mathcal{Q}$uadraticpolynomials, we move on to the multivariate representation of univariate functions. Before doing so, we need an isomorphism between the extension field $\mathbb{E}$ of dimension n over the ground field $\mathbb{F}$ (cf Definition 2.3) and the vector space $\mathbb{F}^n$. To this aim, we observe that all field elements $a \in \mathbb{E}$ have the form

$$a_{n-1}t^{n-1} + \cdots + a_1t + a_0 \text{ with } a_i \in \mathbb{F}\,.$$

In addition, we see that a vector $b \in \mathbb{F}^n$ can be represented as $(b_1, \ldots, b_n)$ with $b_i \in \mathbb{F}$.

DEFINITION 2.10 *Let $\mathbb{E}$ be an n^{th}degree extension of the ground field $\mathbb{F}$ and $\mathbb{F}^n$ the corresponding vector space. Then we call $\phi : \mathbb{E} \rightarrow \mathbb{F}^n$ with*

$$\phi(a) := b \textit{ and } b_i := a_{i-1} \textit{ for } 1 \leq i \leq n$$

for $a_0, \ldots, a_{n-1}, b_1, \ldots, b_n \in \mathbb{F}$ as defined above the canonical bijection *between $\mathbb{E}$ and $\mathbb{F}^n$. We also use its inverse ϕ^{-1} and have $\phi(\phi^{-1}(b)) = b$ for all $b \in \mathbb{F}^n$ and $\phi^{-1}(\phi(a)) = a$ for all $a \in \mathbb{E}$.*

With this definition, we are now able to formally prove an important lemma in the context of $\mathcal{MQ}$-systems.

Lemma 2.11 *Let $\mathbb{E}$ be an extension field and $\mathbb{F}$ the corresponding ground field. We have $q := |\mathbb{F}|$ as the number of its elements. In addition, let n be the dimension of $\mathbb{E}$ over the ground field. Moreover, consider the univariate monomial $P(X) := CX^{q^a+q^b}$ over $\mathbb{E}$ for some $a, b \in \mathbb{N}$ and $C \in \mathbb{E}$. Then there exists a polynomial vector $\mathcal{P} \in \mathcal{MQ}(\mathbb{F}^n)$ which computes the same function,* i.e.*, $\forall\ W \in \mathbb{E} : \phi(P(W)) = \mathcal{P}(\phi(W))$.*

PROOF. First, we decompose $P(X)$ into two the univariate monomials $U(X) := CX^{q^a}$ and $V := X^{q^b}$. Second, we observe that computing in the ring $\mathbb{Z}/(q^n - 1)\mathbb{Z}$ allows us to reduce the degree of the monomials $U(X), V$ below q^n. In particular, we can obtain obtain two integers $a', b' \in \mathbb{Z}$ with $0 \leq a', b' < n$ such that $U(X) = U'(X)$ for $U'(X) := CX^{q^{a'}}$ holds for all inputs $X \in \mathbb{E}$. The same is true for $V(X) = V'(X)$ with $V'(X) := X^{q^{b'}}$. Therefore, and w.l.o.g., we can assume $0 \leq a, b < n$.

Next we note that the monomials U, V are affine transformations in univariate representation, *i.e.*, we can apply Lemma 2.9 to obtain the corresponding multivariate representations $\mathcal{U}$ and $\mathcal{V}$. Denoting the components of the polynomial vector $\mathcal{U}$ by $u_1, \ldots, u_n$ we can now write

$$\begin{array}{rcl}
\mathcal{U}(x_1, \ldots, x_n) & = & \phi(U(\phi^{-1}(x_1, \ldots, x_n))) \\
& = & \phi(u_1(x_1, \ldots, x_n) \\
& & +\ tu_2(x_1, \ldots, x_n) \\
& & +\ \ldots \\
& & +\ t^{n-1}u_n(x_1, \ldots, x_n))
\end{array}$$

Similar, we obtain a mixed $\mathbb{F}^n/\mathbb{E}$-representation of the polynomial vector $\mathcal{V}$. Multiplying $\mathcal{U}, \mathcal{V}$ in $\mathbb{E}$, *i.e.*, in particular, modulo the irreducible defining polynomial $i(t)$, yields the corresponding $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic polynomials by construction. □

Remark. Instead of computing the multivariate polynomials as outlined in the above proof, we can also use multivariate polynomial interpolation, cf [MI88, Wol04] for details.

Corollary 2.12 *For a polynomial of the form*

$$P(X) \quad := \sum_{\substack{0 \leq i,j \leq D \\ q^i + q^j \leq D}} C_{i,j} X^{q^i+q^j} \textit{ with } C_{i,j} \in \mathbb{E}$$

with $D \in \mathbb{N}$ and $D < q^n$, there exists a polynomial vector $\mathcal{P} \in \mathcal{MQ}(\mathbb{F}^n)$ which computes the same function.

Lemma 2.13 *Let $\mathbb{F}$ be a ground field and $\mathbb{E}$ an n-dimensional extension of $\mathbb{F}$. Then for the polynomial*

$$P(X) := \sum_{0 \leq i \leq j < n} C_{i,j} X^{q^i+q^j} + \sum_{i=0}^{n-1} B_i X^{q^i} + A$$

with coefficients $C_{i,j}, B_i, A \in \mathbb{E}$ there exists a unique multivariate polynomial vector $\mathcal{P} \in \mathcal{MQ}(\mathbb{F}^n)$ which computes the same function, i.e., *we have $P(X) = \phi^{-1}(\mathcal{P}(\phi(X)))\ \forall X \in \mathbb{E}$.*

Proof. We use Corollary 2.12 for the quadratic terms, Lemma 2.9 on the affine part, and add up the result. □

Interestingly, the converse is also true:

Lemma 2.14 *Let $\mathcal{P} \in \mathcal{MQ}(\mathbb{F}^n)$ be a $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic system of equations and $\mathbb{E}$ an n-dimensional extension of the ground field $\mathbb{F}$. Then there exists a unique univariate polynomial*

$$P(X) := \sum_{0 \leq i \leq j < n} C_{i,j} X^{q^i+q^j} + \sum_{i=0}^{n-1} B_i X^{q^i} + A$$

with coefficients $C_{i,j}, B_i, A \in \mathbb{E}$ which computes the same function as $\mathcal{P}$, i.e., *we have $P(X) = \phi^{-1}(\mathcal{P}(\phi(X)))\ \forall X \in \mathbb{E}$.*

Proof. We use a counting argument and will assume $\mathbb{F} \neq$GF(2) for simplicity. Consider all polynomials $P(X) \in \mathbb{E}[X]$ which have the above form. They have $\binom{n}{2}+n+n+1$ coefficients in totals: the quadratics (coefficients $C_{i,j}$ with $i \neq j$), the quadratics in the same variable (coefficients $C_{i,i}$), the linear terms (coefficients B_i) and the constant term A. Hence, there are $q^{n.\left(\frac{n(n+3)}{2}\right)+1}$ choices in total for these polynomials $P(X)$. On the other hand, we know from (4) that we have a total choice of $q^{n.\tau(n)} = q^{n.\left(\frac{n(n+3)}{2}\right)+1}$ for polynomial vectors in $\mathcal{MQ}(\mathbb{F}^n)$. In addition, Lemma 2.13 shows that each of these polynomials $P(X)$ has a unique multivariate representation, denoted $\mathcal{P}(X)$. Moreover, both functions compute the same output for any given input $X \in \mathbb{E}$. This is not true for two polynomials $P_1(X), P_2(X) \in \mathbb{E}[X]$, $P_1 \neq P_2$ and their corresponding polynomial vectors $\mathcal{P}_1, \mathcal{P}_2 \in \mathcal{MQ}(\mathbb{F}^n)$. Hence, using the counting from above we are able to conclude that for each polynomial vector $\mathcal{P}$, there is one unique univariate polynomial $P(X)$. This completes the proof for the case $\mathbb{F} \neq$ GF(2).

The same proof runs through for GF(2), but we have to adjust our counting slightly as $x_i^2 = x_i$ holds for $1 \leq i \leq n$ and consequently no terms of the form $X^{q^i+q^i}$ in the polynomial $P(X)$. However, the overall idea remains the same. □

Remark. The previous lemma has already been shown in a more general setting in [KS99, Lemma 3.3]; in this article, the proof has been simplified for the case of $\mathcal{M}$ultivariate $\mathcal{Q}$uadraticequations. Another proof of this lemma, but this time restricted to the case $\mathbb{F} =$ GF(2), can be found in [MIHM85]. Moreover, the univariate representation of multivariate quadratic equations can be computed efficiently: we use polynomial interpolation on a total of $O(n^2)$ points from $\mathbb{E}$, which translates to $O(n^3)$ elements from $\mathbb{F}$.

Lemma 2.15 *Let $n \in \mathbb{N}$ be the number of variables and $m \in \mathbb{N}$ be the number of equations. Let $\mathcal{P} \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$ be a $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic system of equations. For (a) $m < n$ and (b) $m > n$ there exists a univariate representation $P \in \mathbb{E}[X]$ for $\mathbb{E}$ being an (a) n-dimensional and (b) m-dimensional extension of the ground field $\mathbb{F}$.*

Proof. Case *(a)*: We have $m < n$ and $\mathbb{E}$ an n-dimensional extension of the ground field $\mathbb{F}$ and define $\phi : \mathbb{E} \to \mathbb{F}^n$ (see above). Moreover, consider the reduction/projection transformation $R : \mathbb{F}^n \to \mathbb{F}^m$ defined as

$$R(x_1, \ldots, x_m, x_{m+1}, \ldots, x_n) := (x_1, \ldots, x_m)$$

and its “inverse” transformation $R^{-1} : \mathbb{F}^m \to \mathbb{F}^n$ which is defined as

$$R^{-1}(x_1, \ldots, x_m) := (x_1, \ldots, x_m, 0, \ldots, 0)\,.$$

Using Lemma 2.14, we compute a polynomial $P \in \mathbb{E}[x]$ with

$$P(X) = \phi^{-1}(R^{-1}(\mathcal{P}(\phi(X)))) \text{ with } X \in \mathbb{E}$$

By construction, we have

$$R(\phi(P(\phi^{-1}(x)))) = \mathcal{P}(x)\ \forall x \in \mathbb{F}^n$$

An alternative way of writing the above statement is to replace the “inverse reduction” $R^{-1}(X)$ by adding zero polynomials $p_{m+1}, \ldots, p_n$ to the multivariate function $\mathcal{P}$, *i.e.*, these polynomials are all chosen to be the zero polynomial. This way, we obtain $\mathcal{P} : \mathbb{F}^n \to \mathbb{F}^n$ and can therefore apply Lemma 2.14 directly.

Case *(b)*: We have $m > n$ and $\mathbb{E}$ an m-dimensional extension of the ground field $\mathbb{F}$ and define $\phi : \mathbb{E} \to \mathbb{F}^m$. Moreover, consider the reduction transformation $R : \mathbb{F}^m \to \mathbb{F}^n$ defined as $R(x_1, \ldots, x_n, x_{n+1}, \ldots, x_m) := (x_1, \ldots, x_n)$. Using Lemma 2.14, we compute a polynomial $P \in \mathbb{E}[x]$ with

$$P(X) = \phi^{-1}(\mathcal{P}(R(\phi(X))))\ \forall X \in \mathbb{E}$$

By construction, this polynomial computes the required function. Moreover, due to the definition of the reduction function $R(x)$, the degree of $\mathcal{P}(R(x))$ keeps quadratic. □

Remark. Due to their construction, both polynomials $P(X)$ in (a) and (b) of Lemma 2.15 are an univariate representation of the corresponding $\mathcal{P}(x)$. For a fixed reduction transformation R and a fixed extension field $\mathbb{E}$, this univariate polynomial $P(X)$ is unique by construction.

Theorem 2.16 *Let $n, m \in \mathbb{N}$ and $\mathbb{F}$ a finite field with $q := |\mathbb{F}|$ elements. Moreover, define $k := \max\{n, m\}$ and an extension field $\mathbb{E} := GF(q^k)$. Then there exists a unique univariate representation $P \in \mathbb{E}[X]$ for each multivariate system of equations $\mathcal{P} \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$ and vice versa.*

Proof. We use lemmata 2.13, 2.14, and 2.15. □

Remark. For d the maximal degree of the multivariate equations, and a univariate polynomial $P(X)$ with monomials of the form $X^{q^{i_1} + \cdots + q^{i_{d'}}}$ with $d' \le d$, we are able to prove a generalisation of Lemma 2.9 by induction over d. Similar, we can prove the converse for general polynomials P. However, as this article concentrates on $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic equations, we omit the corresponding proofs.

2.6 Related Problems

Although the $\mathcal{MQ}$-problem is computationally hard, this is not enough for the construction of secure public key schemes. Here, we outline two more problems which are used in the context of these schemes.

2.6.1 Isomorphism of Polynomials

For the construction of secure public key systems based on polynomial equations over finite fields, the security of the IP-problem [Pat96b], *i.e.*, the difficulty to find affine transformations $S \in \text{Aff}^{-1}(\mathbb{F}^n)$ and $T \in \text{Aff}^{-1}(\mathbb{F}^m)$ such that $\mathcal{P} = T \circ \mathcal{P}' \circ S$ for given polynomial vectors $\mathcal{P}, \mathcal{P}'$ is also important. In particular, the private key in such systems is usually the triple $(S, \mathcal{P}', T)$, cf Section 2.4, and the public key the polynomial vector $\mathcal{P}$. Hence, if the IP-problem were easy, the security of these schemes would be seriously jeopardised. Therefore, these constructions have to make the (often not explicitly stated) assumption that the corresponding IP-problem is difficult. If $\mathcal{P}'$ has a special structure — as it is the case for all systems based on the difficulty of solving a system of polynomial equations over a finite field — it is possible that the corresponding IP-problem becomes easy and the system can be broken exploiting this weakness, cf *e.g.*[KS98, GC00, WBP04] for examples of such attacks.

A discussion of the security of the general IP-problem can be found in [Pat96b, PGC98b, GMS02, LP03]. In particular, [LP03, Per05] show that the IP-problem with one secret, *i.e.*, T is given or equal to the identity transformation, can be solved easily if $m \geq n$, *i.e.*, the number of variables does not exceed the number of equations.

2.6.2 MinRank

Let $(M_1, \ldots, M_k)$ be a sequence of $k \in \mathbb{N}$ matrices over $\mathbb{F}^{n \times n}$ each. Moreover, let $r \in \mathbb{N}$. For the MinRank-problem, we are interested in finding a linear combination of the above matrices, *i.e.*, a vector $\lambda \in \mathbb{F}^k$ such that

$$\text{Rank}(\sum_{i=1}^{k} \lambda_i M_i) \leq r \, .$$

The above problem has been shown to be $\mathcal{NP}$-complete when stated over finite fields [BFS96].

In special cases, namely when the rank r is extremely small or the maximal rank $R \in \mathbb{N}$ of the matrices $M_1, \ldots, M_k$ is very close to n, the problem becomes tractable. In particular, [GC00] gives two algorithms with complexity $O(q^r)$ and $O(q^{n-R})$, respectively, for these two special cases. The question if a more efficient algorithm for these cases or even the general MinRank-problem exists remains open. A positive answer would have serious implications for the security of several schemes based on the $\mathcal{MQ}$-problem as the MinRank-problem has been used in the cryptanalysis of several systems, *e.g.*, in [CSV93, CSV97, KS98, KS99, GC00, WBP04].

3 Basic Trapdoors

After talking about the general $\mathcal{MQ}$-problem and how to embed a trapdoor into it, we will now consider special constructions of this trapdoor. We start with two constructions which use only a finite field $\mathbb{F}$, denoted UOV and STS. We then move on to the two schemes MIA and HFE; both use a ground field $\mathbb{F}$ and an extension field $\mathbb{E}$.

3.1 Unbalanced Oil and Vinegar Schemes: UOV

The "Unbalanced Oil and Vinegar" (UOV) scheme was introduced in [KPG99], cf [KPG03] for an extended version of this paper. UOV is a generalisation of the original Oil and Vinegar scheme of Patarin [Pat97].

DEFINITION 3.1 *Let $\mathbb{F}$ be a finite field and $n, m \in \mathbb{N}$ with $m < n$ and $\alpha'_i, \beta'_{i,j}, \gamma'_{i,j,k} \in \mathbb{F}$. We say that the polynomials below are central equations in UOV-shape:*

$$p_i(x'_1, \ldots, x'_n) := \sum_{j=1}^{n-m} \sum_{k=1}^{n} \gamma'_{i,j,k} x'_j x'_k + \sum_{j=1}^{n} \beta'_{i,j} x'_j + \alpha'_i \,.$$

In this context, the variables x'_i for $1 \leq i \leq n-m$ are called the "vinegar" variables and x'_i for $n-m < i \leq n$ the "oil" variables. We also write $o := m$ for the number of oil variables and $v := n - m = n - o$ for the number of vinegar variables. Note that the vinegar variables are combined quadratically while the oil variables are only combined with vinegar variables in a quadratic way. Therefore, assigning random values to the vinegar variables, results in a system of linear equations in the oil variables which can than be solved, *e.g.*, using Gaussian elimination.

Moreover, Unbalanced Oil and Vinegar schemes (UOV) omit the affine transformation T but only use $S \in \mathrm{Aff}^{-1}(\mathbb{F}^n)$. To fit in our framework, we set it to be the identity transformation, *i.e.*, we have $T = id$ for UOV by definition. UOV is able to omit T as all equations have exactly the same shape. Hence, we do not need T to hide any special structure. Moreover, using the ideas of [WP04b, WP05] we can actually show that the transformation T could always be moved into the central equations $\mathcal{P}'$ and hence, does not give any gain in security.

The UOV scheme can only be used for signature schemes as we need $v \geq 2o$ for a secure construction. The first attack against the original OV, *i.e.*, with parameters $o = v$ or $n = 2m$ can be found in [KS98]. This attack has been extended to UOV in [KPG99]. The latest security evaluation — also taking Gröbner bases into account, can be found in [BWP05]. As shown in all these papers, we have on average q^v different pre-images $x \in \mathbb{F}^n$ on average for a given vector $y \in \mathbb{F}^m$, so decryption is by no means efficient. In a nutshell, the most efficient attacks have a complexity of $O(q^{v-m-1}m^4) = O(q^{n-2m-1}m^4)$ and are due to [KPG99].

We also want to point to [WP05] for the question of equivalent private keys: this article shows that UOV needs too much memory for its private key as each of them is only a representative of a class of

$$q^n \prod_{i=0}^{n-m-1} (q^{n-m} - q^i) \prod_{i=0}^{m-1} (q^m - q^i)$$

equivalent private keys. Hence, for memory efficient implementations, only a normal form of the private key should be stored. Such a form can be computed using the algorithm presented in the proof of [WP05, Thm. 4.6].

3.2 Stepwise Triangular Systems: STS

Another approach to obtain an invertible central map is used in Stepwise Triangular Systems (STS). They have been introduced in [WBP04]. As UOV, STS are defined over a finite field $\mathbb{F}$ and use a special structure for the central equations $\mathcal{P}'$ which allows easy inversion (cf Figure 4 for regular STS). Here, the step-width (number of new variables) and the step-height (number of new equations) is controlled by the parameter r. As usual, we use m for the number of equations and n for the number of variables. In addition, we denote L the number of layers, q the size of the ground field $\mathbb{F}$, and r the step-width.

Let $r_1, \ldots, r_L$ be L integers such that $r_1 + \cdots + r_L = n$, the number of variables, and $m_1, \ldots, m_L \in \mathbb{N}$ such that $m_1 + \cdots + m_L = m$, the number of equations. Here r_l represents the number of new variables (step-width) and m_l the number of equations (step-height), both in step l for $1 \leq l \leq L$.

$$
\begin{array}{rl}
\text{Step } 1 & \left\{ \begin{array}{rl} p'_1 & (x'_1, \ldots, x'_r) \\ & \vdots \\ p'_r & (x'_1, \ldots, x'_r) \end{array} \right. \\
\vdots & \\
\text{Step } l & \left\{ \begin{array}{rl} p'_{(l-1)r+1} & (x'_1, \ldots, x'_r, \quad \ldots, \quad x'_{(l-1)r+1}, \ldots, x'_{lr}) \\ & \vdots \\ p'_{lr} & (x'_1, \ldots, x'_r, \quad \ldots, \quad x'_{(l-1)r+1}, \ldots, x'_{lr}) \end{array} \right. \\
\vdots & \\
\text{Step } L & \left\{ \begin{array}{rl} p'_{(L-1)r+1} & (x'_1, \ldots, x'_r, \quad \ldots, \quad x'_{(l-1)r+1}, \ldots, x'_{lr}, \quad \ldots, \quad x'_{n-r+1}, \ldots, x_n) \\ & \vdots \qquad\qquad\qquad \vdots \\ p'_{Lr} & (x'_1, \ldots, x'_r, \quad \ldots, \quad x'_{(l-1)r+1}, \ldots, x'_{lr}, \quad \ldots, \quad x'_{n-r+1}, \ldots, x_n) \end{array} \right.
\end{array}
$$

Figure 4: Central Equations p'_i in a Regular STS Scheme

In a general Stepwise Triangular Scheme (gSTS), the m_l private quadratic polynomials of each layer l, contain only the variables x'_k with $k \leq \sum_{j=1}^{l} r_j$, *i.e.*, only the variables defined in all previous steps plus r_l new ones. The overall shape of the private polynomials leads to the name Stepwise Triangular Scheme (STS), cf Figure 4 for regular STS. We want to stress in this context that we do not assume any specific structure for the private polynomials $p'_1, \ldots, p'_m$ here. In particular, all coefficients $\gamma'_{i,j,k}, \beta'_{i,j}, \alpha'_i \in \mathbb{F}$ may be chosen at random.

When not mentioned otherwise, we concentrate on regular STS schemes (rSTS or STS for short) in this section to simplify explanations. For regular STS schemes we set $r_1 = \cdots = r_N = m_1 = \cdots = m_L$, which we denote by r. Consequently, we have $n = m = Lr$.

To invert a system of central equations $\mathcal{P}'(x') = y'$ for given $y' \in \mathbb{F}^m$, we exploit the step-structure: in each level l, we have q^r possible vectors and only need to keep the intermediate values $(x'_{(l-1)r+1}, \ldots, x'_{lr})$ which satisfy the corresponding equations

$$
\begin{array}{rcl}
y'_{(l-1)r+1} & = & p'_{(l-1)r+1}(x'_1, \ldots, x'_{lr}) \\
& \vdots & \\
y'_{lr} & = & p'_{lr}(x'_1, \ldots, x'_{lr})
\end{array}
$$

for given $y'_{(l-1)r+1}, \ldots, y'_{lr} \in \mathbb{F}$. Having a bijective structure in each level makes sure we get only one possible solution — this way, STS becomes particularly efficient. However, we impose some conditions on our choices for the coefficients $\gamma'_{i,j,k}, \beta'_{i,j}, \alpha'_i \in \mathbb{F}$ this way. Anyway, in a signature scheme, it is even enough if we only get *one* solution for the corresponding equation. For general STS, we use the same idea but for each individual layer and hence with a different number of equations and variables. However, observe that the legitimate user has a workload growing with q^r which implies that this number cannot be too large if there is no special trapdoor embedded for each layer, cf Section 6 for examples of such constructions with a special trapdoor embedded.

After outlining both regular and general Stepwise Triangular Schemes, we give a brief account of constructions suggested so far. We begin with the Birational Permutation Schemes of Shamir [Sha93]. They are regular STS schemes with $r = 1$. However, as previously mentioned, they are not defined over a (small) finite field but over a (large) finite ring. So strictly speaking, they are no STS schemes although they are clearly related. In contrast, the TPM (Triangle Plus Minus, [GC00]) class of Goubin and Courtois coincides with STS for the parameters $r_1 = u$, $m_L = v$, $m_1 = \cdots = m_{L-1} = r_2 = \cdots = r_L = 1$, *i.e.*, we remove $u \in \mathbb{N}$ initial layers, add $v \in \mathbb{N}$ polynomials in the last step, and have exactly one new variable at all intermediate levels. TPM is a subclass of STS as it is not defined over a ring but over a field, and hence, is an example of an $\mathcal{MQ}$-scheme.

Shamir's scheme was broken shortly after its publication in [CSV93, The95, CSV97]. The TPM scheme of Goubin and Courtois has been broken in the same paper that proposed it [GC00]. In fact, the aim of their construction was to show that Moh's TTM (Moh's Tame Transformation Method, [Moh99]) construction is weak.

The schemes RSE(2)PKC and RSSE(2)PKC, proposed by Kasahara and Sakai, cf [KS04b, KS04a], also fall in the class of STS schemes. Both schemes — and actually the whole STS class — have been broken in [WBP04]. The first attack is an inversion attack which computes the message/signature for given ciphertext/message with a workload of $O(mn^3Lq^r + n^2Lrq^r)$, the second is a structural attack which recovers an equivalent version of the secret key with a workload of $O(mn^3Lq^r + mn^4)$ operations. Hence, for small parameters of q^r these schemes are highly insecure. Unfortunately, this is exactly the case of STS without any extra trapdoor, so we have to conclude that STS is broken in general.

3.3 Matsumoto-Imai Scheme A: MIA

The scheme MIA is due to Matsumoto and Imai [IM85, MI88]. It is the first scheme in this article which uses two different finite fields, namely a ground field $\mathbb{F}$ and an extension field $\mathbb{E}$.

Definition 3.2 *Let $\mathbb{E}$ be an extension field of dimension n over the finite field $\mathbb{F}$ with $q := |\mathbb{F}|$ elements and $\lambda \in \mathbb{N}$ an integer with $\gcd(q^n - 1, q^\lambda + 1) = 1$. We then say that the following central equation over $\mathbb{E}$ is of MIA-shape:*

$$P(X') := (X')^{q^\lambda + 1}\,.$$

The restriction $\gcd(q^n - 1, q^\lambda + 1) = 1$ is necessary first to obtain a permutation polynomial and second to allow efficient inversion of $P(X')$. This is due to the fact that the equation $h.(q^\lambda + 1) \equiv 1 \pmod{q^n - 1}$ has exactly one solution $h \in \mathbb{N}$ with $h < q^n - 1$, as we have the previously mentioned condition on the possible choices of the value λ. Given h, we can solve $Y' = P'(X')$ as $(Y')^h = X'^{[h.(q^\lambda+1)]} = X'$ by raising Y' to the power of h. Note that these operations take place in the n-th dimensional extension $\mathbb{E}$ of the finite field $\mathbb{F}$. All in all, this approach is similar to RSA. However, the hardness of MIA is not based on the difficulty of finding the exponent h but in the intractability to obtain transformations S, T for given polynomial equations $\mathcal{P}, \mathcal{P}'$ (IP-problem, cf Section 2.6.1). As we saw in Section 2.5, the above monomial can be expressed in terms of $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic equations and hence be used as a trapdoor for an $\mathcal{MQ}$-problem, cf Lemma 2.11 and also Theorem 2.16.

We want to note that MIA is insecure, due to a very efficient attack by Patarin [Pat95]. Moreover, we want to point out that Geiselmann *et al.* showed how to reveal the constant parts of these transformations [GSB01]. Hence, having S, T affine instead of linear does not seem to enhance the overall security of MIA. The papers [WP04b, WP05] discuss the question of equivalent keys for MIA and some variations.

Remark. In the paper [MI88], MIA was introduced under the name C*. Moreover, it used the branching modifier (cf Section 4.4) by default. As branching has been attacked very successfully, C* has been used without this modification for any later construction, *e.g.*, [CGP00b, CGP02, CGP00a, CGP03a]. However, without the branching condition, the scheme C* coincides with the previously suggested “Scheme A” from [IM85]. To acknowledge this historical development, we decided to use the earlier notation and call the scheme presented in this section “MIA” for “Matsumoto-Imai Scheme A”. As an additional benefit, the notation becomes more uniform as all basic schemes are now named with 3 letter acronyms.

3.4 Hidden Field Equations: HFE

After breaking MIA, Patarin generalised the underlying trapdoor to "Hidden Field Equations" [Pat96b]. This generalisation aims at the central equations and uses a univariate *polynomial* rather than a univariate *monomial* here. But the basic idea of MIA, *i.e.*, to mix a given ground field with one of its extension fields is still used in HFE as we see in the following

Definition 3.3 *Let $\mathbb{F}$ be a finite field with $q := |\mathbb{F}|$ elements, $\mathbb{E}$ its n-th degree extension, and $\phi : \mathbb{E} \to \mathbb{F}^n$ the canonical bijection between this extension field and the corresponding vector space (cf Definition 2.10). Moreover, let $P(X)$ a univariate polynomial over $\mathbb{E}$ with*

$$P'(X') := \sum_{\substack{0 \le i,j \le d \\ q^i+q^j \le d}} C'_{i,j} X'^{q^i+q^j} + \sum_{\substack{0 \le k \le d \\ q^k \le d}} B'_k X'^{q^k} + A'$$

$$\text{where} \begin{cases} C'_{i,j} X^{q^i+q^j} & \text{for } C'_{i,j} \in \mathbb{E} \text{ are the quadratic terms,} \\ B'_k X^{q^k} & \text{for } B'_k \in \mathbb{E} \text{ are the linear terms, and} \\ A' & \text{for } A' \in \mathbb{E} \text{ is the constant term} \end{cases}$$

for $i, j \in \mathbb{N}$ and a degree $d \in \mathbb{N}$. Now we say the central equations $\mathcal{P}' := \phi \circ P' \circ \phi^{-1}$ are in HFE-shape.

As the degree of the polynomial P' is bounded by d, this allows efficient inversion of the equation $P'(X') = Y'$ for given $Y' \in \mathbb{E}$ and small d, cf [Pat96b, Section 5] for an overview of possible algorithms for this problem; in a nutshell, these algorithms depend both on the size of the dimension n of the extension field $\mathbb{E}$ and the degree d of the central polynomial P. Hence, from an efficiency point of view, both should be rather small. Moreover, in contrast to MIA, HFE is in general no surjection, cf Section 2.4.3 for possible ways to overcome this problem.

As for MIA, we notice that the HFE polynomial $P'(X')$ can be expressed as $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic equations $\mathcal{MQ}(\mathbb{F}^n)$ and are hence a possible central equation, cf Section 2.5 and in particular Lemma 2.14 and Theorem 2.16.

From a cryptanalytic point of view, basic HFE are broken: an efficient key inversion attack, using the MinRank-problem (cf Section 2.6.2), has been demonstrated in [KS99]. An inversion attack which uses both Gröbner bases and general linearization methods has been shown in [FJ03]. In [SG03] we find an attack which works better if n is not a prime, *i.e.*, we have splitting fields. A more detailed discussion of HFE can be found in [Pat96b, Cou01, WP04a]. Here, [Pat96b] gives some general considerations of HFE after its development, *e.g.*, a general linearization attack against all multivariate schemes (cf Section 2.4.5), while [Cou01] summarised the situation of HFE in 2001 and also improves over the attack from [KS99]. The latest such summary of attacks can be found in [WP04a]. In particular, this paper outlines two versions of HFE which are secure against all known attacks. Finally, [WP04b, WP05] show that HFE allow many equivalent keys and hence, waste memory. Based on [Tol03] these articles show that from a cryptanalytic point of view, it is possible to restrict to HFE with linear transformations $S, T \in \text{Hom}^{-1}(\mathbb{F}^n) \times \text{Hom}^{-1}(\mathbb{F}^m)$ instead of affine transformations $S, T \in \text{Aff}^{-1}(\mathbb{F}^n) \times \text{Aff}^{-1}(\mathbb{F}^m)$. They improve over [Tol03] by showing that also Frobenius transformations and multiples in the extension field can be used to restrict the key space even further.

3.5 Taxonomy and Preliminary Conclusions

The four trapdoors discussed above are actually all basic trapdoors known so far. We notice that all of them are rather old: the first were MIA (1983) and STS (1993 in Shamir's birational permutations and 2004 in STS), followed by HFE (1996) and UOV (1997 as OV and 1999 as UOV). Apart from UOV with well-chosen parameters, all basic trapdoors have to be considered broken. Unfortunately, UOV is rather inefficient in terms of signature expansion and has a rate of 3 between m, *i.e.*, the dimension of the message space and n, *i.e.*, the dimension of the signature space, *i.e.*, it has a signature expansion rate of 3. Moreover, UOV can not be used to construct a secure encryption scheme. Therefore, we need to discuss some generic modifications. A nice property of these modifiers is that they can be used in combination with any of these basic trapdoors (see below). Moreover, we will see how it is possible to combine several basic trapdoors to more elaborated $\mathcal{MQ}$-systems in Section 6.

Before doing so, we build up a taxonomy to get a better view on the different trapdoors used so far, cf Figure 5 for a graphical representation. Using the finite fields as a first criterion, we see that MIA and HFE form the class of "mixed field" schemes: both use the ground field $\mathbb{F}$ and an extension field $\mathbb{E}$ to construct a trapdoor. Therefore, both are vulnerable to attacks using Gröbner bases as these can exploit the structure of the extension field and the rather low number of univariate monomials when compared to a random system of equations. The same is true for the linearization attack as discussed,*e.g.*, in [JKJMR05]. In contrast, UOV and STS are "single field" systems as they only use the ground field $\mathbb{F}$ but construct their trapdoor using special conditions for the polynomials $p'_1, \ldots, p'_m$: the

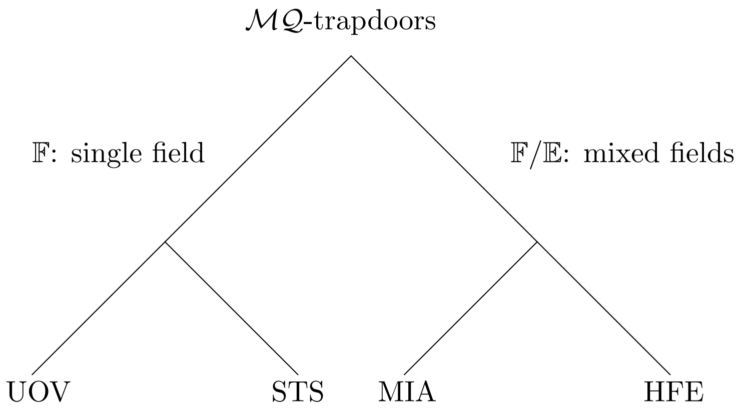
$\mathcal{MQ}$-trapdoors
$\mathbb{F}$: single field
$\mathbb{F}/\mathbb{E}$: mixed fields
UOV
STS
MIA
HFE

Figure 5: Taxonomy of the Basic $\mathcal{MQ}$-trapdoors

concept of vinegar variables for UOV and a layer- or step-structure for STS. In both cases, the ranks of these central equations proved to be a serious vulnerability. While it was possible for UOV to fix this problem with well-chosen parameters, STS does not allow such an option.

At first glance, MIA is a subclass of the HFE system: while MIA uses only one monomial, HFE uses a whole polynomial. So from a cryptanalytic point of view, HFE is much stronger than MIA and all attacks which break HFE will also defeat MIA. The converse is not true though. Moreover, if we inspect both schemes closer, we see the differences: MIA uses a monomial of a high degree, while HFE relies on the existence of efficient root finding algorithms for polynomials — and therefore needs a much smaller degree d than MIA. Hence, using implementation as a criterion, we kept both schemes in different classes.

4 Generic Modification on $\mathcal{MQ}$-schemes

As we saw in the previous section, most basic trapdoors are insecure. To construct secure schemes, we therefore need “modifications” of these basic building blocks. As we will see below, these modifications are quite generic as we can apply them (at least in theory) to *any* of the above trapdoors. However, for some schemes, there are modifications which prove more efficient than for others.

4.1 Minus method: “-”

Although this modification looks rather easy, it proves powerful to defeat a wide class of cryptographic attacks against several $\mathcal{MQ}$-schemes, including Gröbner bases and linearization attacks. The minus method has been introduced in [Sha93]. In this new construction, we set $\tilde{m} := m - r$ for some $r \in \mathbb{N}$ and define the public key equations as $\mathcal{P} := R \circ T \circ \mathcal{P}' \circ S$. In this context, the function $R : \mathbb{F}^m \to \mathbb{F}^{\tilde{m}}$ denotes a *reduction* or *projection*, cf Section 2.5 for details. In addition, we have the affine transformations $S \in \mathrm{Aff}^{-1}(\mathbb{F}^n), T \in \mathrm{Aff}^{-1}(\mathbb{F}^m)$ and the private system of $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic equations $\mathcal{P}' \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$. Less loosely speaking, we consider the function $R(y_1, \ldots, y_m) := (y_1, \ldots, y_{m-r})$, *i.e.*, we neglect the last r components of the output vector $(y_1, \ldots, y_n)$. As a consequence, a given public key $\hat{\mathcal{P}} \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$ is transfered to a new key $\mathcal{P} \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^{\tilde{m}})$, cf Figure 6.

$$\begin{array}{rcl} \hat{p}_1(x_1,\ldots,x_n) & \leftarrow & p_1(x_1,\ldots,x_n)\\ & \vdots & \\ \hat{p}_{m-r}(x_1,\ldots,x_n) & \leftarrow & p_{m-r}(x_1,\ldots,x_n)\\ \left.\begin{array}{c}\hat{p}_{m-r+1}(x_1,\ldots,x_n)\\ \vdots\\ \hat{p}_m(x_1,\ldots,x_n)\end{array}\right\} & \multicolumn{2}{l}{\textit{discarded}} \end{array}$$

Figure 6: Minus modification for $\hat{\mathcal{P}}$ being transfered to $\mathcal{P}$

For MIA (or C^*), the corresponding minus variation is called C^{*--} and has been discussed in [PGC98a]. For HFE, we derive HFE-. In particular, the attacks from [KS99, FJ03] are no longer effective against this variation.

4.2 Plus method: “+”

As the name suggests, the plus method adds equations rather than removing them from the public key. To the knowledge of the authors, this method has been first discussed in [Pat96b, PGC98a]. In a nutshell, the legitimate user inserts a total of $a \in \mathbb{N}$ random quadratic equations $\pi_1, \ldots, \pi_a$ without a trapdoor to the central equations. Let $\tilde{\mathcal{P}} \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^{\tilde{m}})$ be the initial central equations and $\mathcal{P}' \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$ be the new central equations. We have $m := \tilde{m} + a$ for $m, \tilde{m} \in \mathbb{N}$ and

$$\begin{array}{rcl}
p'_1(x'_1, \ldots, x'_n) & := & \tilde{p}_1(x'_1, \ldots, x'_n) \\
& \vdots & \\
p'_{\tilde{m}}(x'_1, \ldots, x'_n) & := & \tilde{p}_{\tilde{m}}(x'_1, \ldots, x'_n) \\
p'_{\tilde{m}+1}(x'_1, \ldots, x'_n) & := & \pi_1(x'_1, \ldots, x'_n) \\
& \vdots & \\
p'_m(x'_1, \ldots, x'_n) & := & \pi_a(x'_1, \ldots, x'_n)
\end{array}$$

Following the notation earlier introduced in this article, the polynomials $p'_1, \ldots, p'_m$ have components of the (new) central equations $\mathcal{P}'$ and $\tilde{p}_1, \ldots, \tilde{p}_{\tilde{m}}$ and components of the (old) central polynomial vector $\tilde{\mathcal{P}}$.

Initially, the plus method was suggested with three affine transformations $S \in \text{Aff}^{-1}(\mathbb{F}^n), T \in \text{Aff}^{-1}(\mathbb{F}^{m'})$ and $U \in \text{Aff}^{-1}(\mathbb{F}^m)$ rather than two transformations $S \in \text{Aff}^{-1}(\mathbb{F}^n), T \in \text{Aff}^{-1}(\mathbb{F}^m)$ as described in this article. However, as proven in [Wol02, Section 4.6], the two methods have equal security as the method with three affine transformations can always be expressed with two transformations and vice versa.

When it was proposed, the plus method was thought to enhance the security of schemes like MIA or HFE. However, a more detailed cryptanalysis showed that this is not the case. In addition, signature schemes have a workload increasing with q^a as only q^{-a} of all solutions to the original problem $\tilde{\mathcal{P}}$ are also a solution for the a equations (without trapdoor) $\pi_1, \ldots, \pi_a$. Hence, this method has not received much attention lately.

4.3 Subfield method: "/"

A big drawback of public key schemes based on the $\mathcal{MQ}$-problem is their rather large public key. To overcome this problem we can choose all coefficients in the transformations $S \in \text{Aff}^{-1}(\mathbb{F}^n)$ and $T \in \text{Aff}^{-1}(\mathbb{F}^m)$ and also the central equations $\mathcal{P}' \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$ in a proper subfield $\tilde{\mathbb{F}}$ of the ground field $\mathbb{F}$. This way, the size of both the public and the private key decrease to a factor of $\frac{\log_2 \tilde{\mathbb{F}}}{\log_2 \mathbb{F}}$. For example, choosing $\mathbb{F} = \text{GF}(256)$ and $\tilde{\mathbb{F}} = \text{GF}(2)$, we reduce the size of all keys to $\frac{1}{8}$. The method works as subfields are closed under addition and multiplication and hence, choosing all coefficients in the components $S, \mathcal{P}', T$ of the private key in a proper subfield $\tilde{\mathbb{F}}$ ensures that the public key $\mathcal{P} := T \circ \mathcal{P}' \circ S$ also has coefficients in $\tilde{\mathbb{F}}$ rather than $\mathbb{F}$.

Hence, the space for storing these coefficients drops from $\log_2 q$ to $\log_2 |\tilde{\mathbb{F}}|$. On the other hand, the message space $\mathbb{F}^n$ is not affected by this change as all operations are still defined over the initial ground field $\mathbb{F}$.

To the knowledge of the authors, this method was introduced in [Pat96b] and has been used in the first version of the Sflash signature scheme [CGP00b] as submitted to [NES]. In addition, it has been used in the context of UOV [KPG03]. In both cases, the construction has been shown to be insecure, cf [GM02, BWP05]. Similar conclusions for HFE have been drawn in [SG03]. All in all, we therefore strongly discourage the use of this “subfield-trick”.

4.4 Branching: “$\perp$”

The idea of this modification is rather old and can already be found in [MI88]. A graphical representation using two branches with $n = n_1 + n_2$ and $m = m_1 + m_2$ for some $n_1, n_2, m_1, m_2 \in \mathbb{N}$ is shown in Figure 7. For example in MIA, this modification gives a speed up for decryption, as we can reduce the dimension of the extension field $\mathbb{E}$ from n to n_1 and n_2. Hence, we are no longer confronted with a workload growing in $O(n^k)$ for some fixed $k \in \mathbb{R}$, $k > 1$, but only in $O(n_1^k + n_2^k)$ for the two smaller numbers n_1 and n_2. Similar conclusions can be drawn for all other basic trapdoors.

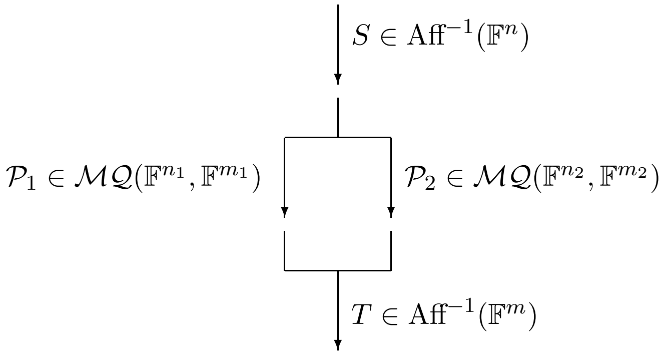
$S \in \mathrm{Aff}^{-1}(\mathbb{F}^n)$
$\mathcal{P}_1 \in \mathcal{MQ}(\mathbb{F}^{n_1}, \mathbb{F}^{m_1})$
$\mathcal{P}_2 \in \mathcal{MQ}(\mathbb{F}^{n_2}, \mathbb{F}^{m_2})$
$T \in \mathrm{Aff}^{-1}(\mathbb{F}^m)$

Figure 7: $\mathcal{MQ}$-trapdoor with two branches $\mathcal{P}_1, \mathcal{P}_2$

More general, the overall computational effort is reduced by partitioning both the polynomials $p'_1, \ldots, p'_m$ and the variables $x'_1, \ldots, x'_n$ in $B \in \mathbb{N}$ sets. Here, we call B the *branching number*. All computations for the central equations $\mathcal{P}'$ are then independently performed in these B sets. Note that we had $B = 2$ in the example of Figure 7. Formalising this idea, we decompose the number of variables into a B-dimensional vector over $\mathbb{N}$ such that $n = n_1 + \cdots + n_B$. Similar, we decompose the number of equations into $m_1, \ldots, m_B \in \mathbb{N}$ such that $m = m_1 + \cdots + m_B$. We use this notation to write down the branching structure, cf. Figure 8. At first glance this closely resembles the idea from STS, cf Section 3.2. However, there is an important difference here: while STS uses the variables from the previous layers (or "branches" for the "$\perp$" modification), this is not the case for the "$\perp$" modification. Here, all branches are completely independent from each other. Hence, all computations can be done in parallel, *e.g.*, in hardware, which allows a considerable speed-up. This was also the initial reason for proposing this idea: having a more efficient public key scheme. Unfortunately, the articles [Pat95, Pat96a] give an algorithm for separating these branches. To the knowledge of the authors, the most efficient algorithm for this problem has been given in [Fel01, Fel04]. It has an overall running time of $O(n^6)$.

$$
\begin{array}{ll}
\text{Branche 1} & \left\{\begin{array}{lcrl}
y'_1 & = & p'_1 & (x'_1, \ldots, x'_{n_1}) \\
 & \vdots & & \\
y'_{m_1} & = & p'_{m_1} & (x'_1, \ldots, x'_{n_1})
\end{array}\right. \qquad \text{with } x'_i \in \mathbb{F} \\
\vdots & \\
\text{Branche } b & \left\{\begin{array}{lcrl}
y'_{m_1+\cdots+m_{b-1}+1} & = & p'_{m_1+\cdots+m_{b-1}+1} & (x'_{n_1+\cdots+n_{b-1}+1}, \ldots, x'_{n_1+\cdots+n_b}) \\
 & \vdots & & \\
y'_{m_1+\cdots+m_b} & = & p'_{m_1+\cdots+m_b} & (x'_{n_1+\cdots+n_{b-1}+1}, \ldots, x'_{n_1+\cdots+n_b})
\end{array}\right. \\
\vdots & \\
\text{Branche } B & \left\{\begin{array}{lcrl}
y'_{m-m_b+1} & = & p'_{m-m_b+1} & (x'_{n-n_B+1}, \ldots, x'_n) \\
 & \vdots & & \\
y'_m & = & p'_m & (x'_{n-n_B+1}, \ldots, x'_n)
\end{array}\right.
\end{array}
$$

Figure 8: Central Equations p'_i with B branches

Hence, we strongly discourage the use of the "$\perp$" modification in multivariate systems — though they lead to more efficient schemes. But this gain in efficiency is paid with a too high price on the security side.

4.5 Fixing: "f"

A similar idea to the "-" modification is the "f" modification: instead of deleting some public key equations, we reduce the number of variables by explicitly assigning values to the variables $x_{n-f+1}, \ldots, x_n$ for a security parameter $f \in \mathbb{N}$. More formally, we pick a random vector $(a_1, \ldots, a_f) \in \mathbb{F}^f$ and partly evaluate the public key polynomials $p_1, \ldots, p_m$. This way, we obtain new polynomials $\tilde{p}_1, \ldots, \tilde{p}_m$ which now depend on the input variables

$$\begin{array}{rcl} \tilde{p}_1(x_1, \ldots, x_{\tilde{n}}) & := & p_1(x_1, \ldots, x_{\tilde{n}}, a_1, \ldots, a_f) \\ & \vdots & \\ \tilde{p}_m(x_1, \ldots, x_{\tilde{n}}) & := & p_m(x_1, \ldots, x_{\tilde{n}}, a_1, \ldots, a_f) \end{array}$$

Figure 9: Fixing Modification for two $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic systems $\tilde{\mathcal{P}}$ and $\mathcal{P}$

$x_1, \ldots, x_{\tilde{n}}$ with $\tilde{n} := n + f$ instead of $x_1, \ldots, x_n$. In Figure 9 we can see this idea explained with an old public key $\mathcal{P} \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$ and a new public key $\tilde{\mathcal{P}} \in \mathcal{MQ}(\mathbb{F}^{\tilde{n}}, \mathbb{F}^m)$ and a fixed vector $a \in \mathbb{F}^f$.

If our initial system did not have any linear or constant terms, *i.e.*, we set the coefficients $\beta_{i,j}$ and α_i equal to zero for $1 \leq i \leq m$ and $1 \leq j \leq n$, we can use the zero vector $(0, \ldots, 0) \in \mathbb{F}^f$ for fixing the variables $x_{n-f+1}, \ldots, x_n$, *i.e.*, we have $a = 0$ in the above setting. This way, we do not introduce new linear or constant terms. From a cryptographic point of view, this does not introduce a weakness *if* the original idea of fixing is secure in the first place.

All in all, the idea works quite well with encryption schemes but gives a slow down of q^f for signature schemes: we only have a probability of q^{-f} for a signature to have the correct values for $x_{n-f+1}, \ldots, x_n$.

After being suggested in [Cou01], there has not been much work done on the security of this modification. In particular, it is unknown how the running time Gröbner attacks depends on this parameter f for systems like MIA and HFE. Therefore, the authors of this article suggest a deeper study of the "f" modification in conjecture with these basic trapdoors before using this modification.

4.6 Sparse Polynomials: "s"

This idea has been used both in [YC04a] and also [WC04, WHL$^+$05] to construct fast asymmetric schemes. In a nutshell, they use basic trapdoors but with polynomials as sparse as possible. In particular, this means that all known attacks against these schemes have to be taken into account very carefully as the newly constructed polynomials only offer "on-the-edge" security.

Obviously, there is a clear benefit: instead of evaluating a total of $\tau(n)$ terms for each hidden polynomial p'_i with $1 \leq i \leq m$, we can concentrate on far less terms. This saves both time and memory. In particular, inverting these systems is now more time efficient.

However, the idea is rather new and there is not much known yet about hidden vulnerabilities of these schemes. Therefore, we suggest to study them in more depth before applying it to concrete schemes.

4.7 Vinegar Variables: “v”

The following modification has been introduced in the context of HFE under the name HFEv in [KPG99]. There, it used a different form for the central equations $\mathcal{P}'$. To the knowledge of the authors, this article is the first to present the “v” modification in a more general form so it can be used with any trapdoor. In particular, the multivariate version of vinegar (cf Definition 4.2) has not been presented before.

Definition 4.1 *Let $\mathbb{E}$ be a finite field with degree n' over $\mathbb{F}$, the number of vinegar variables $v \in \mathbb{N}$, and P'(X') a polynomial over $\mathbb{E}$. Moreover, let $(z'_1, \ldots, z'_v) := s_{n-v+1}(x_1, \ldots, x_n), \ldots, s_n(x_1, \ldots, x_n)$ for s_i polynomials of $S(x)$ in multivariate representation. Then define the central polynomial*

$$P'_{z'_1,\ldots,z'_v}(X') \quad := \quad \sum_{0\le i,j<n} C_{i,j}X'^{q^i+q^j} + \sum_{k=0}^{n-1} B_k(z'_1,\ldots,z'_v)X'^{q^k} + A(z'_1,\ldots,z'_v)$$

$$\textit{where}\begin{cases} C_{i,j}X'^{q^i+q^j} & \textit{for } C_{i,j}\in\mathbb{E} \textit{ are the}\\ & \textit{quadratic terms,}\\ B_k(z'_1,\ldots,z'_v)X'^{q^k} & \textit{for } B_k(z'_1,\ldots,z'_v) \textit{ depending}\\ & \textit{linearly on } z'_1,\ldots,z'_v \textit{ and}\\ A(z'_1,\ldots,z'_v) & \textit{for } A(z'_1,\ldots,z'_v) \textit{ depending}\\ & \textit{quadratically on } z'_1,\ldots,z'_v \end{cases}$$

Then we say the polynomial $P'_{z'_1,\ldots,z'_v}(X')$ is in univariate vinegar *shape.*

The condition that the $B_k(z_1, \ldots, z_v)$ are affine functions (*i.e.*, of degree 1 in the z_i at most) and $A(z_1, \ldots, z_v)$ is a quadratic function over $\mathbb{F}$ ensures that the public key as a whole is still quadratic over $\mathbb{F}$. In addition, we can obtain a similar definition for the case of multivariate quadratic polynomials:

Definition 4.2 *Let $\mathbb{F}$ be a finite field, $v \in \mathbb{N}$ the number of vinegar variables, and $\mathcal{P}' \in \mathcal{MQ}(\mathbb{F}^{\tilde{n}}, \mathbb{F}^m)$ a polynomial-vector over $\mathbb{F}$ in $\tilde{n} \in \mathbb{N}$ input variables and with $m \in \mathbb{F}$ equations. Moreover, let $(z'_1, \ldots, z'_v) :=$*

$s_{n-v+1}(x_1,\dots,x_n),\dots,s_n(x_1,\dots,x_n)$ for s_i polynomials of $S(x)$ in multivariate representation. In addition we have $n=\tilde{n}+v$ for the number of variables. Then define the central polynomials as

$$\begin{aligned}
p'_1(x_1,\dots,x_{\tilde{n}}) &:= \sum_{1\le j\le k\le \tilde{n}} \gamma'_{1,j,k}x_jx_k \\
&\quad + \sum_{j=1}^{\tilde{n}} \beta'_{1,j}(z'_1,\dots,z'_v)x_j + \alpha'_1(z'_1,\dots,z'_v) \\
&\vdots \\
p'_i(x_1,\dots,x_{\tilde{n}}) &:= \sum_{1\le j\le k\le \tilde{n}} \gamma'_{i,j,k}x_jx_k \\
&\quad + \sum_{j=1}^{\tilde{n}} \beta'_{i,j}(z'_1,\dots,z'_v)x_j + \alpha'_i(z'_1,\dots,z'_v) \\
&\vdots \\
p'_m(x_1,\dots,x_{\tilde{n}}) &:= \sum_{1\le j\le k\le \tilde{n}} \gamma'_{m,j,k}x_jx_k \\
&\quad + \sum_{j=1}^{\tilde{n}} \beta'_{m,j}(z'_1,\dots,z'_v)x_j + \alpha'_m(z'_1,\dots,z'_v)
\end{aligned}$$

Here we have a new system of $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic equations with only v input variables $A'\in\mathcal{MQ}(\mathbb{F}^v,\mathbb{F}^m)$ for $A'=:(\alpha'_1,\dots,\alpha'_m)$ and a polynomial vector $B'\in \mathit{Aff}_0(\mathbb{F}^v,\mathbb{F}^{m\tilde{n}})$ with the non-standard equality $B'=:(\beta'_{1,1},\beta'_{1,2},\dots,\beta'_{m,\tilde{n}})$. Then we say the central polynomial $\mathcal{P}'$ is in multivariate vinegar *shape.*

We want to point out that the definition of the central equations $\mathcal{P}'$ is the same as given in Section 2.2, but with a slight twist on the coefficients used: the linear coefficients β are replaced by non-homogeneous degree 1 polynomials, while the constant coefficients α are replaced by non-homogeneous degree 2 polynomials.

Inverting the central equation $P'(X')=Y'$ or $\mathcal{P}'(x')=y'$ for $X',Y'\in\mathbb{E}$ and $x,y\in\mathbb{F}^n$ requires to invert the original trapdoor q^v times. For a signature scheme, this is not a problem as finding a solution for any of these equations will yield a valid signature. However, for an encryption scheme, the workload usually is too high and hence, this modification cannot be used to obtain such a system. In any case: in conjecture with the HFE-trapdoor, this modification does not prove efficient against the recent Gröbner attacks from [FJ03] as it only slightly increases the number of linear independent monomials in P'. In addition, there is a cryptanalysis given in [DS05a] which shows that HFE can be broken with a workload of q^v.

From a mathematical point of view, both the univariate and the multivariate variation are equivalent. This can be seen easily using the ideas of the proof of Lemma 2.15. Hence, it depends on the underlying trapdoor used which of the two is to be preferred.

4.8 Internal Perturbation: "i"

The idea of internal perturbation is due to Ding [Din04]. It was first used in connection with MIA and then denoted PMI ("Perturbated Matsumoto Imai"). One year later, the idea was extended to HFE [DS05a] and called IPHFE ("Internal Perturbation of HFE"). In both cases, an affine subspace of dimension w is used to add some kind of "noise" to the overall system. The idea is similar to HFEv (cf Section 4.7), but with a slight twist: while HFEv increases the number of input variables, internal perturbation does not. In a nutshell, the "old" variables $x'_1, \ldots, x'_n$ are used for two purposes: first, they span an n-dimensional vectorspace in the variables $x'_1, \ldots, x'_n$ and second, they span an w-dimensional perturbation space. The advantage is that such a variation is harder to cryptanalyse. In any case, "internal perturbation" comes in two flavours:

Definition 4.3 *Let $\mathcal{P}', \tilde{\mathcal{P}} \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$ be two systems of m quadratic equations in n input variables $x'_1, \ldots, x'_n$ each. Moreover, let $s(x) : \mathbb{F}^n \to \mathbb{F}^w$ be an affine transformation,* e.g., *represented by a vector $v_s \in \mathbb{F}^w$ and a matrix $M_s \in \mathbb{F}^{n \times w}$ where the matrix M_s has rank w. We denote the output of $s(x)$ by $z' \in \mathbb{F}^w$,* i.e., *we have $z' := s(x)$ and call the components $z'_1, \ldots, z'_w$. In addition, let $\Pi \in \mathcal{MQ}(\mathbb{F}^w, \mathbb{F}^m)$ be a system of m quadratic equations in w input variables $z'_1, \ldots, z'_w$ each with components $\pi_1, \ldots, \pi_m$. Then we call*

$$\mathcal{P}' := \begin{cases} p'_1 & := & \tilde{p}_1(x'_1, \ldots, x'_n) & + & \pi_1(z'_1, \ldots, z'_w) \\ & \vdots & & & \\ p'_m & := & \tilde{p}_m(x'_1, \ldots, x'_n) & + & \pi_m(z'_1, \ldots, z'_w) \end{cases}$$

a multivariate internally perturbated *$\mathcal{M}$ultivariate $\mathcal{Q}$uadratic system of equations.*

Definition 4.4 *Let $\mathbb{E}$ be an n-dimensional extension field over $\mathbb{F}$. Moreover, let $\hat{P}(X') \in \mathbb{E}[X']$ be a central equation in univariate representation* *(cf Lemma 2.14). In addition, let $s(x) : \mathbb{F}^n \to \mathbb{F}^w$ be an affine transformation represented by an $(n \times w)$ matrix of rank w and an w-dimensional vector. We denote the output of $s(x)$ by $z'_1, \ldots, z'_w \in \mathbb{F}$ and we have $Z := \phi^{-1}((z_1, \ldots, z_w, 0, \ldots, 0))$. In addition, let*

$$F(Z') := \sum_{0 \le i \le j < n} \hat{C}_{i,j} Z'^{q^i + q^j} + \sum_{i=0}^{n-1} \hat{B}_i Z'^{q^i} + \hat{A}$$

be a quadratic function with coefficients $\hat{C}_{i,j}, \hat{B}_i, \hat{A} \in \mathbb{E}$. Then we call

$$P'(X', Z') := \tilde{P}(X') + F(Z')$$

a univariate *internally perturbated $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic system of equations.*

As we see, in both cases the perturbation functions Π and F depend on a rather small perturbation subspace of dimension w. In addition, we do not require any trapdoor for these two functions but select their coefficients at random. Hence, we expect a workload of $O(q^w)$ for inverting the new central equation $\mathcal{P}'$. But for q^w small (*e.g.*, $q = 2$ and $w = 4 \ldots 6$), this is feasible.

At first glance, it is not obvious which of the two forms is more secure or efficient and hence advisable for the construction of public key systems. So we need the following

Lemma 4.5 *For every* multivariate *internally perturbated $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic system of equations, there is a* univariate *internally perturbated $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic system of equations and vice versa. Hence, both kinds of internal perturbation are equivalent from a cryptanalytic point of view.*

Proof. We use the notation from definitions 4.3 and 4.4. The overall proof is similar to the proof of Lemma 2.15.
$\Rightarrow$: We start with $\mathcal{P}' \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$ and $\Pi \in \mathcal{MQ}(\mathbb{F}^w, \mathbb{F}^n)$. Our goal is to compute the corresponding univariate representation of both. This is feasible, using Theorem 2.16. By construction, we obtain an internal perturbation function F and a univariate polynomial P'.
$\Leftarrow$: As for the previous proof, we use Theorem 2.16 — but this time to obtain a multivariate representation instead of a univariate representation. The only question to answer is if our perturbation polynomials $\pi_1, \ldots, \pi_n$ depend on all n components $z'_1, \ldots, z'_n$ of Z' or only on the subset $z'_1, \ldots, z'_w$. Theorem 2.16 does not guarantee the latter. However, we observe that the

perturbation variables $z'_1, \ldots, z'_w$ can be expressed as $R : \mathbb{F}^n \to \mathbb{F}^w$ with $R(z'_1, \ldots, z'_n) := (z'_1, \ldots, z'_w, 0, \ldots, 0)$, using the reduction from Lemma 2.15. Hence, the effect of the univariate perturbation function $F(Z)$ is equal to $\phi(F(\phi^{-1}(R(s(x)))))$ for all input vectors $x \in \mathbb{F}^n$. Using Theorem 2.16, this can be rewritten as $\Pi(R(s(x)))$ for some system of polynomials $\Pi \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$. Taking the reduction $R(\cdot)$ "into" the polynomial functions Π shows that they do not depend on the input variables $z'_{w+1}, \ldots, z'_n$, *i.e.*, we have $\Pi \in \mathcal{MQ}(\mathbb{F}^w, \mathbb{F}^m)$. Hence, the polynomial vector $\Pi = (\pi_1, \ldots, \pi_n)$ has the required form. □

By now, the "i" modification has been used with MIA (multivariate version) and HFE (univariate version). By the time of writing, we do not see any benefit when combining it with UOV or STS. However, in mixed schemes this may be different. We want to note that MIAi has been broken in [FGS05], using ideas from differential cryptanalysis to "denoise" the MIA scheme from the internal perturbation.

4.9 Homogenising: "h"

Taking a fresh look at the two modifications vinegar variables ("v", cf Section 4.7) and internal perturbation ("i", cf Section 4.8), we can develop a new generic modifier. Basically, we use the ideas of vinegar variables, but use only linear equations of degree 1 to be multiplied with the linear terms, and homogeneous equations of degree 2 to replace the constant terms. The overall result are homogeneous equations of degree 2, regardless of the trapdoor used. Hence, we have a way of saving a total of $m(1+n)$ coefficients by dropping the constant and the linear terms. As the security of $\mathcal{M}$ultivariate $\mathcal{Q}$uadraticequations lies in the quadratic and not the other terms, the overall security of the corresponding does not degenerate with this modification. To the knowledge of the authors, the "h" modification has not been proposed before. Formally, we can write this modification as

Definition 4.6 *Let $\mathbb{F}$ be a finite field $\mathbb{F}$, $h \in \mathbb{N}$ the number of homogenising variables, and $\tilde{\mathcal{P}} \in \mathcal{MQ}(\mathbb{F}^{\tilde{n}}, \mathbb{F}^m)$ a polynomial-vector over $\mathbb{F}$. Moreover, let $z'_1, \ldots, z'_h$ be new variables which depend linearly on the input variables $x_1, \ldots, x_n$. The central map depends on the variables $x'_1, \ldots, x'_{\tilde{n}}$ for $\tilde{n} \leq n$.*

Then define the central equation as

$$\begin{aligned}
p'_1(x_1,\ldots,x_{\tilde{n})} &:= \sum_{1\le j\le k\le \tilde{n}} \gamma_{1,j,k}x_jx_k \\
&\quad + \sum_{j=1}^{\tilde{n}} \beta'_{1,j}(z'_1,\ldots,z'_h)x_j + \alpha'_1(z'_1,\ldots,z'_h) \\
&\vdots \\
p'_i(x_1,\ldots,x_{\tilde{n}}) &:= \sum_{1\le j\le k\le \tilde{n}} \gamma_{i,j,k}x_jx_k \\
&\quad + \sum_{j=1}^{\tilde{n}} \beta'_{i,j}(z'_1,\ldots,z'_h)x_j + \alpha'_i(z'_1,\ldots,z'_h) \\
&\vdots \\
p'_m(x_1,\ldots,x_{\tilde{n}}) &:= \sum_{1\le j\le k\le \tilde{n}} \gamma_{m,j,k}x_jx_k \\
&\quad + \sum_{j=1}^{\tilde{n}} \beta'_{m,j}(z'_1,\ldots,z'_h)x_j + \alpha'_m(z'_1,\ldots,z'_h)
\end{aligned}$$

Here we have $A' \in \mathcal{MQ}(\mathbb{F}^v, \mathbb{F}^m)$ for $A' = (\alpha'_1,\ldots,\alpha'_m)$ with A' being homogeneous and $B' \in Hom^{-1}(\mathbb{F}^v, \mathbb{F}^{m\tilde{n}})$ with the non-standard equality $B' = (\beta'_{1,1}, \beta'_{1,2}, \ldots, \beta'_{m,\tilde{n}})$. Then we say the central polynomial $\mathcal{P}'$ is in multivariate homogenising *shape.*

This definition is quite similar to the definition of the vinegar modifier (cf Section 4.7), but with a slight twist: first, we ask for homogeneous rather than non-homogeneous equations $\alpha'_i, \beta'_{i,j}$, and second, we did not fix the source of the new variables $z_1,\ldots,z_h$ yet. Here, we may either use internal variables (cf Section 4.8) or "external" variables (cf Section 4.7). Given the cryptanalytic results previously achieved against the "v" modification of HFE, we prefer the use of internal variables. The corresponding modification will be denoted by "h". Obviously, we have $n = \tilde{n}$ and $h \le n$ here. In the case of external variables as for the "v" modification, we denote this variation "*h'* " (h prime). In this case we obtain $n = \tilde{n} + h$ as relationship between the new, the old, and the homogenising variables. We want to stress that we believe that internal variables are better suited for the purpose of homogenising the public key. In addition we want to point out that the homogenising modification only makes sense if the public key has not been constructed carefully not to contain any linear or constant terms. In most cases, there is no need for this modification as it is possible to restrict the private key accordingly. However, in cases where we need linear terms for one reason or another, this modification proves useful to obtain a smaller public key.

4.10 Masking: "m"

The idea of masking variables has been developed in [Wol02, sections 4.9 and 4.10]. It is basically the inverse idea to the "f" modification: instead of reducing the number of input variables, this number is increased. This is realized by changing the initial affine transformation to $\tilde{S} : \mathbb{F}^n \rightarrow \mathbb{F}^{\tilde{n}}$ for $n > \tilde{n}$. This new transformation $\tilde{S}$ can be realized using a matrix $M \in \mathbb{F}^{\tilde{n} \times n}$ of rank $\tilde{n}$ and a vector $v \in \mathbb{F}^{\tilde{n}}$. This construction increases the number of variables on costs of the number of equations. In particular, such a system cannot be a bijection anymore. But as inverting an affine transformation is usually much faster than inverting the central system $\mathcal{P}'$, this modification can be used for the construction time efficient $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic systems.

The effect of this transformation is rather limited when considering, *e.g.*, the attack of [KS99]. However, in attacks which mainly depend on the number of input variables (*e.g.*, Gröbner attacks), such a modification may be worthwhile. However, as this modification has not been systematically studied its security is an open problem.

5 Variations Applied

In this section we point out where the general modifiers developed in the previous sections have been used so far for the construction of new schemes. In particular, we will see that the main attention was focused on schemes from the "mixed field class" in this context.

5.1 Hidden Field Equations

Hidden field equations were mainly used with the minus and the "v" modification so far. The cryptanalysis of [KS99] becomes ineffective if any variation is applied. However, the later work of Faugère and Joux [FJ03] proves very efficient against HFE, HFE+, and also to some extent against HFEv. However, the method HFE- proves a very efficient way to counter this attack.

Recently, Ding and Schmidt suggested to use the variation HFEi — they called it IPHFE ("Internal Perturbation of HFE"). Unfortunately, there is not much independent research known about strength of this new scheme. However, we expect it to be secure against Gröbner attacks. Given that MIAi (see below) has been broken rather unexpectedly, we suggest to wait some time until using HFEi in applications.

5.2 Matsumoto-Imai Scheme A

The MIA scheme has also been used with the modifications "-" and "+" so far. While MIA+ is rejected in [PGC98a], its variation MIA- (under the name C^{*--}) is considered to be secure for well chosen parameter. Unfortunately, this construction does not allow encryption but only signature schemes. In particular, MIA- is the basis for the Sflash scheme [CGP00b, CGP02, CGP03b, CGP03a] which was recommended for special use in the NESSIE project (cf [NES]).

The scheme MIAi has been developed in [Din04] and is there called "Perturbed Matsumoto-Imai" (PMI). It has been broken in [FGS05], using a differential attack.

As already outlined in Section 3.3, MIA was used in the variation MIA$\perp$ in the paper [MI88]. This variation has been broken in [Pat95].

5.3 Further Variations

We are not aware of any successful constructions using variations of UOV or STS. However, it may be worthwhile to study the effect of the "f" modification on STS and UOV — and in particular on the attacks applied against these schemes. Similar, STS- may be worthwhile as the minus modification could make the rank attacks difficult. On the other hand, STSi is certainly not a good idea as this boils down increasing the number of variables in the first layer of STS, *i.e.*, STS and STSi are actually the same scheme. We can draw similar conclusions for UOV. As an overall result, we see that more research in this area may be worthwhile.

6 Mixed Schemes

In this section, we shortly outline two of the rather new schemes *enhanced TTS* [YC04b] and *tractable rational map* [WHL$^+$05]. Both schemes use an STS structure as overall layout and "plug in" trapdoors of other schemes in the individual layers. Hence, they do not use STS in its "pure" form but mix it with other trapdoors. This motivates the name "mixed schemes".

6.1 Enhanced TTS

In [YC04b], Yang and Chen give several constructions of the so-called *enhanced TTS* schemes. For all these schemes, only the central equations $\mathcal{P}'$ change. We concentrate on their first proposal as all other schemes developed only vary the security parameters, but keep the same idea, *i.e.*, using an overall STS structure with an UOVs trapdoor in each layer. For this construction, they use the following central polynomials, cf Figure 10. Here

$$\begin{array}{rcl}
p'_i & := & x'_i + \sum_{j=1}^{7} \gamma'_{i,j} x'_j x'_{8+(i+j \bmod 9)} \text{ , for } i = 8 \ldots 16; \\
p'_{17} & := & x'_{17} + \gamma'_{17,1} x'_1 x'_6 + \gamma'_{17,2} x'_2 x'_5 + \gamma'_{17,3} x'_3 x'_4 + \gamma'_{17,4} x'_9 x'_{16} + \\
 & & + \gamma'_{17,5} x'_{10} x'_{15} + \gamma'_{17,6} x'_{11} x'_{14} + \gamma'_{17,7} x'_{12} x'_{13}; \\
p'_{18} & := & x'_{18} + \gamma'_{18,1} x'_2 x'_7 + \gamma'_{18,2} x'_3 x'_6 + \gamma'_{18,3} x'_4 x'_5 + \gamma'_{18,4} x'_{10} x'_{17} + \\
 & & + \gamma'_{18,5} x'_{11} x'_{16} + \gamma'_{18,6} x'_{12} x'_{15} + + \gamma'_{18,7} x'_{13} x'_{14}; \\
p'_i & := & x'_i + \gamma'_{i,0} x'_{i-11} x'_{i-9} + \sum_{j=19}^{i} \gamma'_{i,j-18} x'_{2(i-j)-(i \mod 2)} x'_j + \\
 & & + \gamma'_{i,i-18} x_0, x_i + \sum_{j=i+1}^{27} \gamma'_{i,j-18} x'_{i-j+19} x'_j \text{ , for } i = 19 \ldots 27;
\end{array}$$

Figure 10: Central Map for enhanced TTS

we have $\gamma'_{i,j} \in_R \mathbb{F}$ random coefficients. We note that the central polynomials do not have linear or constant random terms. As the security of the $\mathcal{MQ}$-problem lies in the quadratic part of these equations alone, this is certainly a good idea as it saves both evaluation time and private key memory.

Having a closer look at the polynomials $p'_8, \ldots, p'_{16}$ we see that they only depend on the input variables $x'_1, \ldots, x'_{16}$, and hence they form the first layer of an STS scheme. The second layer is formed by the two polynomials p'_{17}, p'_{18}, which also depend on x'_{17}, x'_{18}, and the last layer is formed by $p'_{19}, \ldots, p'_{27}$, which depend on *all* 28 input variables $x'_0, \ldots, x'_{27}$.

For inverting this trapdoor, we first assign random values to $x'_1, \ldots, x'_7$, which gives a degree 1 system of equations in $y'_i = p'_i$ for $i = 8 \ldots 16$. Note that we do not always get a solution here. However, in this case we just assign new random values to $x'_1, \ldots, x'_7$ and try again, cf [YC04b] for more details. Second, we notice that the polynomials p'_{17} and p'_{18} are already linear with respect to the variables x'_{17} and x'_{18}. Hence, there will always be a solution at this stage. The final step is to assign a random value to the variable x'_0, which guarantees a solution at this level of the internal equations, too. Hence, we see that the overall structure of enTTS follows UOV. However, in order to speed up computations and to save memory, the equations have been made very sparse (see Figure 10). We want to point out that this sparsity gave some unexpected structure and hence allowed the authors of [DY04] to break an earlier version of the scheme which was presented in [YC04a]. The only difference between [YC04a] and [YC04b] is a slight modification in the last block of equations, see first summation and the missing term between the two summations:

$$\begin{aligned} p'_i \quad := \quad & x'_i + \gamma'_{i,0} x'_{i-11} x'_{i-9} + \sum_{j=19}^{i} \gamma'_{i,j-18} x'_{2(i-j)} x'_j + \\ & + \sum_{j=i+1}^{27} \gamma'_{i,j-18} x'_{i-j+19} x'_j \text{ , for } i = 19 \ldots 27; \end{aligned}$$

Taking a second look at the scheme from Figure 10, we see that the two polynomials p'_{17} and p'_{18} actually can further be classified as UOV with two branches: while p'_{17} does not depend on x'_{18}, the formula for p'_{18} is independent from x'_{17}. This is the reason that we can say enTTS uses a kind of branching structure for these two polynomials. However, as the overall scheme uses more an STS structure, this small branching part cannot be used to launch the attacks mentioned in Section 4.4.

6.2 Tractable Signature Schemes

After enTTS, we move on to the tractable signature scheme from [WHL$^+$05], which is again a scheme with an STS structure. This time, it uses a total of 5 layers. However, the twist in comparison with a normal STS scheme lies in the fact that computations in the different layers are done in extension fields $\mathbb{E}_l$ for $l = 2 \ldots 5$ rather than in the ground field $\mathbb{F}$ only. In the following, we denote with "$\cdot$" multiplication in the corresponding extension field and with ϕ_l for $l = 2 \ldots 5$ the corresponding canonical bijection (cf Definition 2.10).

First Layer. The first layer uses the variables $x'_1, \ldots, x'_8$ as an input and polynomials of the form $p'_i := x'_i$, *i.e.*, we have the simplest polynomials possible for our purpose. Moreover, we assign random values to these variables and hence, there is no need for an extension field in this layer.

Second Layer. We have $\mathbb{E}_2 = \mathbb{F}^6$ and the second layer as

$$\mathcal{P}_2' := \phi(\phi^{-1}(x_9', \ldots, x_{14}') \cdot \phi^{-1}(x_1', \ldots, x_6')) + \begin{pmatrix} c_1' x_1' x_2' \\ c_2' x_2' x_3' \\ \vdots \\ c_6' x_6' x_7' \end{pmatrix} + \begin{pmatrix} c_7' x_3' \\ c_8' x_4' \\ \vdots \\ c_{12}' x_8' \end{pmatrix}$$

We notice that the second layer becomes linear if the variables $x_1', \ldots, x_6'$ are given. In addition, we have $c_1', \ldots, c_{12}' \in_R \mathbb{F}$ random coefficients.

Third Layer. We have $\mathbb{E}_3 = \mathbb{F}^2$ in the third layer

$$\begin{aligned} \mathcal{P}_3' \quad := \quad & \phi([\phi^{-1}(x_{15}', x_{16}')]^2) \\ & + \begin{pmatrix} c_{13}' x_1' x_2' + c_{14}' x_3' x_4' + \ldots + c_{19}' x_{13}' x_{14}' \\ c_{20}' x_{14}' x_1' + c_{21}' x_2' x_3' + \ldots + c_{26}' x_{12}' x_{13}' \end{pmatrix} + \begin{pmatrix} c_{27} x_1' \\ c_{28} x_2' \end{pmatrix} \end{aligned}$$

At first glance, the new variables x_{15}', x_{16}' do not introduce a permutation. However, as the above construction is only specified over fields of characteristic 2, we have X'^2 being a bijection. Unfortunately, [WHL$^+$05] does not go into details how to invert this function, but assuming $\gcd(q^n - 1, \lambda) = 1$, *i.e.*, $\gcd(2^{16} - 1, 2) = 1$ as for the parameters proposed in [WHL$^+$05], we can use the same technique as for the MIA trapdoor (cf Section 3.3) to invert the function $Y' = X'^2$ for given $Y' \in \mathbb{E}_3$ and unknown X'.

Again we notice that this bijection does not depend on the variables $x_1', \ldots, x_{14}'$. Moreover, we have $c_{13}', \ldots, c_{28}' \in_R \mathbb{F}$ random coefficients.

Forth Layer. We have $\mathbb{E}_4 = \mathbb{F}^3$ here and

$$\begin{aligned} \mathcal{P}_4' \quad := \quad & \phi(\phi^{-1}(x_{17}', x_{18}', x_{19}') \cdot \phi^{-1}(x_8', x_9' + x_{11}' + x_{12}', x_{13}' + x_{15}' + x_{16}')) \\ & + \begin{pmatrix} c_{29}' x_4' x_{16}' \\ c_{30}' x_5' x_{10}' \\ c_{31}' x_{15}' x_{16}' \end{pmatrix} + \begin{pmatrix} c_{32}' x_9' \\ c_{33}' x_{10}' \\ c_{34}' x_{11}' \end{pmatrix} \end{aligned}$$

We have $c_{19}', \ldots, c_{34}' \in_R \mathbb{F}$ random coefficients. Moreover, we notice that the forth layer becomes linear if the old variables $x_1', \ldots, x_{16}'$ are given.

Fifth Layer. We have $\mathbb{E}_5 = \mathbb{F}^9$ and

$$\begin{aligned}\mathcal{P}'_5 \quad := \quad & \phi(\phi^{-1}(x'_{20}, x'_{21}, \ldots, x'_{28}) \\ & \cdot\phi^{-1}(x'_1, x'_2 + x'_6 + x'_{11}, x'_3 + x'_7 + x'_{12}, x'_4 + x'_8 + x'_{13}, x'_5 + x'_9 + x'_{14}, \\ & x'_{10} + x'_{14} + x'_{16}, x'_{11} + x'_{15} + x'_{17}, x'_{12} + x'_{16} + x'_{18}, x'_{13} + x'_{17} + x'_{19})) \\ & + \begin{pmatrix} c'_{35}x'_{18}x'_{19} \\ c'_{36}x'_{17}x'_{13} \\ c'_{37}x'_{16}x'_{14} \\ c'_{38}x'_{12}x'_{13} \\ c'_{39}x'_{15}x'_{14} \\ c'_{40}x'_{19}x'_{12} \\ c'_{41}x'_{18}x'_{10} \\ c'_{42}x'_{12}x'_6 \\ c'_{43}x'_{13}x'_5 \end{pmatrix} + \begin{pmatrix} c'_{44}x'_1 \\ c'_{45}x'_2 \\ \vdots \\ c'_{52}x'_9 \end{pmatrix}\end{aligned}$$

We have $c'_{35}, \ldots, c'_{52} \in_R \mathbb{F}$ random coefficients. Moreover, we notice that this last layer becomes linear if the old variables $x'_1, \ldots, x'_{19}$ are given.

As an overall result, we see that the tractable rational map signature scheme is an instance of an STS scheme with sparse polynomials. In contrast to the enhanced TTS from the previous sections, these polynomials are over different extension fields rather than the ground field. Hence, these extension fields have to be chosen carefully to allow fast multiplication and inversion. We refer to [WHL$^+$05] for details on these choices. Using the taxonomy developed in this article, we see that the first and the second layer can actually be combined to one: we view this new layer one/two as a UOV step with $x'_1, \ldots, x'_6$ the vinegar and $x'_8, \ldots, x'_{14}$ the oil variables.

[WHL$^+$05] claims that all known attacks have been taken into account for this construction and it does not cover any hidden weakness. As for enhanced TTS, we suggest to wait a while until using this construction as the sparsity of the polynomials may open the door for previously unknown attacks, in particular as the corresponding encryption scheme from [WC04] has been successfully cryptanalysed in [JKJMR05], using observations on the linearity of the overall system. Using the proofs from [JKJMR05], we expect Gröbner attacks to have a rather low running time, too, against the scheme from [WC04]. However, the attacks from [JKJMR05] do not extend to [WHL$^+$05].

The version [WHL$^+$05] has the unfortunate property that we may not obtain a valid signature with the first try of random variables in all cases; we already noticed a similar behaviour for enhanced TTS, see above. To verify that tractable rational maps have this problem, too, we observe that $x'_1 = \ldots = x'_8 = 0$ is a valid assignment in the first layer. Now, in the second layer, the multiplication in the extension field $\mathbb{E}_2$ always yields 0. Hence, no matter which values we choose for $x'_9, \ldots, x'_{14}$, we cannot fulfil the equations $y'_9 = p'_9, \ldots, y'_{14} = p'_{14}$ for $y'_9, \ldots, y'_{14}$ all non-zero. Although the probability for such a behaviour is rather low (2^{-64}), it is not zero and hence, tractable rational maps do not have a constant signing time. We can draw similar conclusions for Layer 4: Assume we have $x'_8 = x_9 + x'_{11} + x'_{12} = x'_{13} + x'_{15} + x'_{16} = 0$. This event happens with probability 2^{-24}. Moreover, assume that the other terms in the corresponding equation are *non-zero*. This happens with probability $1 - 2^{-24}$. Now, we cannot compute a valid solution in the forth layer and hence, cannot find a valid signature. Note that we do not encounter such a problem in the third layer as we can always compute the inverse of $[\phi^{-1}(x'_{15}, x'_{16})]^2$ for any given input. In any case: both problems were independently noticed by the authors of [WHL$^+$05] who suggested the following tweak in their presentation at PKC 2005 [Wan05]: instead of assigning random values to all variables, they suggest to select the first 8 variables $x'_1, \ldots, x'_8 \in_R \mathbb{F}^*$, *i.e.*, without the possibility of getting 0 for any of these hidden variables. This way, they can guarantee that for each try they obtain a valid signature. While we do not expect security problems here, we find it to drastic a solution: just enforcing $x'_1 \neq 0$ and $x'_8 \neq 0$ would have been enough to overcome the problem of not obtaining a valid signature in all tries.

In any case: both mixed schemes are rather complicated to cryptanalyse as they use very specific polynomial equations. In particular for the latter scheme, the rational behind choosing specific structures has not been made explicit. Hence, it is difficult for an outsider to judge if these choices are in fact rational or not. In particular, some more explanation by the authors of [WHL$^+$05] would certainly help here.

6.3 Rainbow

This scheme has been suggested in [DS05b]. Following our classification, it is an STS construction which uses an UOV trapdoor on each layer. In the first layer, the vinegar variables are assigned randomly. In all next layers, the vinegar variables are the variables from the previous layers. As for the two schemes discussed above, it may happen that we do not obtain a solution for a given set of vinegar and oil variables. As above, we simply try again in this case.

From a security point of view, the ideas of rainbow are sound. In particular the suggested sets of parameters in [DS05b, Sec. 2.2] take all practical attacks into account. Here we have a ground field of size $q = 256$, a total of $n = 33$ variables in $m = 27$ equations, and 4 layers. The first layer has 6 oil and 6 vinegar variables, the second and the third layers add both 5 new (oil) variables, and the final forth layer adds additionally 11 oil variables. The latter is due to rank attacks as discussed, *e.g.*, in [WBP04].

There is also an improved version of Rainbow, discussed in [DS05b, Sec. 5]. Again we have $q = 256$, $n = 33$ and $m = 27$. Also, the number of variables in the first and the last layer are the same. However, all intermediate layers now only have one new variable. Hence, the number of layers increases accordingly. This way, we always obtain a solution at these intermediate layers. Therefore, the overall number of repetitions until we get a valid signature drops considerably. A more detailed discussion of this idea can also be found in Section 7.3.

7 New Schemes and Open Questions

Using the taxonomy developed in this article, we are able to derive new schemes — not previously considered in other publications. In particular, we want to stress that mixed schemes should kept rather simple, so it is possible to determine the strength of the underlying trapdoors. As an overall lesson from the schemes known so far we want to point out that a larger q seems to allow smaller public keys: we have 71 kByte for the public key of Quartz with $q = 2$ in comparison to 15.4 kB for Sflash$^{\mathrm{v2}}$ with q=128, and 8.7 kByte for enhanced TTS and tractable rational signatures with $q = 256$. The reasons for this at first glance rather strange behaviour: having a large field size q, we are able to decrease the number of variables. But given that the public key is a function of $O(n^2 \log_2 q)$, we see immediately that decreasing n in contrast to q allows us to construct schemes with smaller public keys. However, we cannot do this endlessly: having a very large q, we would obtain $n = 1$ and hence, are in the univariate rather than the multivariate case. Therefore, a choice of $q = 256 = 2^8$ or $q = 65536 = 2^{16}$ seems reasonable at present. After these initial considerations, we now move on to some concrete examples of new schemes.

7.1 MIO

When looking at the taxonomy developed in Section 3.5, we see that three of the four schemes, namely HFE, STS, and UOV do allow — at least in principle — odd characteristics. The situation is fundamentally different for MIA: by construction, it only allows even characteristic as the equation $\gcd(q^n - 1, q^\lambda + 1) = 1$ does not have any solution $\lambda \in \mathbb{N}$ otherwise for given $q, n \in \mathbb{N}$ with odd q. To make sure that we have a full list of *all* possible schemes, we develop a version of MIA which also works for odd characteristic, called "Matsumoto-Imai odd" (MIO).

As outlined before, we cannot expect any solution for $\gcd(q^n-1, q^\lambda+1) = 1$; the closest we get is $\gcd(q^n - 1, q^\lambda + 1) = 2$. Hence, the inversion step in MIO consists of two parts:

1. Using an h such that $h.(q^\lambda + 1) \equiv 2 \pmod{q^n - 1}$ we compute $A := (Y')^h = (X')^2$ in the extension field $\mathbb{E}$

2. Using a general root finding algorithm, we solve the equation $(X')^2 = A$ for given $A \in \mathbb{E}$ and unknown X' (cf Section 3.4)

The advantage of such a scheme lies in the fact that root finding becomes more difficult with the degree of the polynomial. Having a degree of 2, the corresponding algorithm is more efficient. In contrast to MIA, MIO may not be so efficient as finite fields of even characteristic are particularly well suited for microprocessors.

From a cryptanalytic point of view, MIO offers a few minor advantages over MIA. In particular, the cryptanalysis of [Pat95] is no longer applicable as this paper needs that the scheme in question is a bijection. However, the techniques developed in [FJ03] are still applicable. Hence, MIO is not stronger than MIA. But from a mathematical point of view, it is satisfying to have a complete list of all possible schemes, therefore, we decided to present MIO in this section.

7.2 MIAf

The following construction is also new and we are not aware that it has been proposed elsewhere. In a nutshell, we use the MIA construction from Section 3.3 but evaluate $f \in \mathbb{N}$ variables $x_1, \ldots, x_f \in \mathbb{F}$ of the public key , *i.e.*, we apply the "f" modification from Section 4.5. In symbols: let $\tilde{\mathcal{P}} \in \mathcal{MQ}(\mathbb{F}^m)$ the original public key, $a_1, \ldots, a_f \in_R \mathbb{F}$ random values, and $p_1, \ldots, p_m$ the new polynomials of the public key:

$$\begin{array}{rcl} p_1(x_1, \ldots, x_n) & := & \tilde{p}_1(a_1, \ldots, a_f, x_1, \ldots, x_n) \\ & \vdots & \\ p_m(x_1, \ldots, x_n) & := & \tilde{p}_m(a_1, \ldots, a_f, x_1, \ldots, x_n) \end{array}$$

We notice that the new polynomials p_i have n input variables while the old polynomials $\tilde{p}_i$ have $\tilde{n} := n + f$ input variables. Hence, the new public key $\mathcal{P}$ is now from $\mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$ rather than $\mathcal{MQ}(\mathbb{F}^m)$. Having q^f large, such a scheme is obviously not useful anymore for signature schemes (cf Section 4.5). However, this variation on MIA can be used in encryption schemes: the new conditions on the first f variables of the old polynomials are satisfied by construction; moreover, inversion works as for the original MIA scheme, so there is no need for the legitimate user to adjust his private key.

Obviously, MIAf is only interesting if it cannot be attacked successfully. From our point of view, the most promising attacks are linearization, Gröbner bases, and the algorithm of Meier and Tacier [CGMT02]. However, a thorough security analysis of MIAf, including the suggestion of secure parameters, is unfortunately outside the scope of this article. The same goes for a description of HFEf or MIOf. But assuming that MIAf is secure, these two other schemes should be interesting for multivariate encryption schemes, too.

7.3 STS⊥h

With this construction, we want to test the limits of the STS idea as used already in constructions for mixed schemes, cf sections 6.1 and 6.2. In particular, we want to see which kind of parameters we can use for secure constructions to obtain a lower limit on the public key sizes for schemes of this kind.

We start with noticing that the enhanced TTS class from Section 6.1 used linear terms for the new variables of the medium layer and hence, always got a solution here regardless of the input. Similar, the tractable rational map class uses the same trick to ensure that we always obtain a signature for any input. We can sum up this trick under the "⊥" modifier: each equation is independent from all other equations and hence, we can compute the results for one variable independently from all other variables. Next, we recall that the linear and constant terms do not give us any gain in the security of the corresponding scheme. Therefore, to obtain smaller public keys, we should avoid them. Actually, this idea has been outlined in the "h" modifier. Finally, STS schemes can be attacked quite successfully both from the highest and the lowest layer, each time using the rank. Hence, a minimal scheme would only use two layers: one with a small rank big enough not to allow any attack here and one with a big rank big enough not to allow any attack from this side.

Remark. Obviously, we can use a scheme which uses only one layer. However, we are in the class UOV now (cf Section 7.4 for a version with secure parameters).

Hence, the scheme we propose in this section has the following structure for its two layers. We use the notation $a \in \mathbb{N}$ for the input variables for the quadratic polynomials of layer 1, $\alpha \in \mathbb{N}$ for the linear variables of layer 1. Similar, we denote with $b \in \mathbb{N}$ the input of the quadratic polynomials of layer 2 and with $\beta \in \mathbb{N}$ the linear variables of layer 2. Hence, we have $b = a+\alpha$, the number of equations is $m = \alpha+\beta$ and the number of variables is $n = b+\beta$, cf Figure 11. Here, we have π_i for $1 \le i \le m$ being homogeneous

$$\begin{array}{rcl}
p'_1(x'_1,\ldots,x'_b) & := & \pi_1(x'_1,\ldots,x'_a) + x'_1 x'_{a+1} \\
p'_2(x'_1,\ldots,x'_b) & := & \pi_2(x'_1,\ldots,x'_a) + x'_1 x'_{a+2} \\
 & \vdots & \\
p'_\alpha(x'_1,\ldots,x'_b) & := & \pi_b(x'_1,\ldots,x'_a) + x'_1 x'_{a+\alpha} \\
p'_{\alpha+1}(x'_1,\ldots,x'_n) & := & \pi_{b+1}(x'_1,\ldots,x'_b) + x'_1 x'_{b+1} \\
p'_{\alpha+2}(x'_1,\ldots,x'_n) & := & \pi_{b+2}(x'_1,\ldots,x'_b) + x'_1 x'_{b+2} \\
 & \vdots & \\
p'_m(x'_1,\ldots,x'_n) & := & \pi_m(x'_1,\ldots,x'_b) + x'_1 x'_{b+\beta}
\end{array}$$

Figure 11: STS⊥h with Two Layers

degree 2 polynomials with random coefficients. Therefore, all polynomials p'_i are homogeneous degree 2 polynomials. Hence, using $S \in \mathrm{Hom}^{-1}(\mathbb{F}^n)$ and $T \in \mathrm{Hom}^{-1}(\mathbb{F}^m)$ for the two transformations we obtain a public key which does not contain any linear or constant terms. So the "homogenising modification" has already been built into the trapdoor used. Moreover, the first layer can be inverted by assigning random values to the variables $x'_1,\ldots,x'_a$ as we saw it, *e.g.*, for UOV.

There are three important attacks we have to take into account for this scheme: first, we need to make sure that the low rank attacks do not apply and hence, we need $q^{2(a+1)} \ge C$ for some security parameter C. Second, we need the high rank attacks to be inefficient. Therefore, we obtain $2^{q^{n-b+1}} = 2^{\beta+1} \ge C$. Finally, we need to make sure that the overall construction does not fall to the attacks for schemes from the UOV class, *i.e.*, we need $q^{b-\beta-1} \ge C$. In all cases, we omitted polynomials for the corresponding attacks as we are more interested in the overall asymptotic complexity rather than a “close match”. Moreover, we use a security bound of $C = 2^{80}$ for the following constructions. Such a security bound has been suggested, *e.g.*, in the European NESSIE project [NES].

Now, with $q = 256 = 2^8$ the following sets of parameters allows a secure construction: $a = 4, \alpha = 16$, *i.e.*, $b = 20$. Moreover, we choose $\beta = 9$ and obtain a total of $n = 29$ variables and $m = 20$ equations. This translates to a public key size of 8700 bytes. As we see, this is quite close to the parameters used in enhanced TTS and rational tractable maps. However, these construction use more than two layers and hence, obtain a higher number of quadratic variables for the last layer. Therefore, attacks using the UOV structure of this construction are less efficient. In any case: the other attacks outlined in this paper did not prove efficient against this kind of schemes and are hence omitted from the above security analysis.

Finally, we also give the parameters for $q = 65536 = 2^{16}$. Here we obtain $a = 2, \alpha = 9$, *i.e.*, $b = 11$ and $\beta = 4$ and obtain a total of $n = 15$ variables and $m = 13$ equations. This translates to a public key size of 3120 bytes. As we saw, the previously mentioned rational to choose q rather large helped up obtaining a smaller public key. However, as we need operations over GF(2^{16}) now, the corresponding scheme may be less suited for smart card implementations as low-end cards still widely use 8-bit microprocessors. Moreover, we have to take the running time of Gröbner algorithms into account now. Unfortunately, we are not aware of a systematic study of the exact behaviour of Gröbner attacks and hence, have to leave the security of the parameters proposed here as an open problem.

Using sparse polynomials for π_i with $1 \leq i \leq m$ would allow faster generation of the public key and also faster inversion. However, generating secure sparse polynomials is outside of the scope of this article. Still, we believe that such a modification would allow a more efficient scheme.

7.4 UOV⊥h

The starting point of this construction are [YC04a] and [DS05b]. In a nutshell, they solve the problem of UOV that not all tries in the private key yield a valid signature. They do so by forcing a special matrix structure on the oil variables: no matter which values we choose for the vinegar variables, the oil variables always yield a matrix of full rank, and hence, we can always compute a solution. This can be summarised under the $\perp$ idea, cf previous section.

Here, we use this idea with a slight twist, *i.e.*, with the homogenising modifier. We construct the UOV trapdoor as shown in Figure 12 having

$$\begin{array}{rcl} p'_1(x'_1,\ldots,x'_n) & := & \pi(x'_1,\ldots,x'_v) + x'_1x'_{v+1} \\ p'_2(x'_1,\ldots,x'_n) & := & \pi(x'_1,\ldots,x'_v) + x'_1x'_{v+2} \\ & \vdots & \\ p'_m(x'_1,\ldots,x'_n) & := & \pi(x'_1,\ldots,x'_v) + x'_1x'_{v+o} \end{array}$$

Figure 12: UOV with Branching and Homogenising Modifiers

$o = m$ and $n = v + o$ (cf Section 3.1). By choosing $x'_1 \in_R \mathbb{F}^*$, *i.e.*, non-zero, we always obtain a valid signature. Moreover, if we choose the polynomials $\pi_1, \ldots, \pi_m$ homogeneous degree 2, we obtain a central map $\mathcal{P}'$ which is also homogeneous degree 2. So, having the two transformations $S \in \mathrm{Hom}^{-1}(\mathbb{F}^n)$ and $T \in \mathrm{Hom}^{-1}(\mathbb{F}^m)$ linear rather than affine, we hide this internal structure using the T-transformation and do not introduce any linear terms with the S-transformation. As a consequence, the public key does not have linear or constant terms and hence, we save $m(n+1)$ coefficients in total. The overall scheme does still have the same security as UOV, *i.e.*, all known attacks apply and we need to choose the parameter accordingly.

In any case, multiplying the monomials $x'_1x'v + i$ for $i = 1 \ldots o$ with random coefficients $\gamma'_{i,1,v+i} \in_R \mathbb{F}^*$ does not improve the security of UOV⊥h: applying the ideas developed in [WP05] we see that such coefficients would lead to equivalent keys and are hence a waste of memory.

As for any other scheme, choosing the vinegar polynomials $\pi_1, \ldots, \pi_m$ sparse rather than dense allows a speed up. Again, this is out of the scope of this overview article.

8 Conclusions

In this article, we introduced $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic schemes and showed how the schemes known so far can be grouped into a taxonomy of only four basic schemes (UOV, STS, MIA, and HFE), using 10 modifiers, cf Table 1. We see that there are far more modifiers than basic schemes. So to increase the number of possible $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic schemes, we suggest to concentrate on finding new basic trapdoors rather than new modifiers. However, given that all known trapdoors are rather old, we are not sure if many more basic trapdoors do exist.

Table 1: Modifiers for $\mathcal{MQ}$-schemes

Symbol	Long Name	Page
-	Minus	30
$+$	Plus	30
/	Subfield	31
$\perp$	Branching	32
f	fixing	33
h	homogenising	39
i	internal	37
m	masking	41
s	sparse	34
v	vinegar	35

In any case, $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic equations can be used to construct schemes which allow short signature sizes (in the range of 28 byte or even 128 *bit* for Quartz). Using the generic construction of [Gra05], we may use any $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic scheme to obtain short signatures which depend on the security of the underlying scheme. However, such constructions are only necessary if we have schemes with rather small parameters as we had in the case of Quartz: 107 bit of output for 100 bit of input. Here, the birthday paradox for signatures becomes a problem. In general, an input size of 160 bit and more does prevent this paradox to be of concern for security requirements above 2^{80}.

Obviously, the taxonomy developed in this article can now be used to obtain new and interesting schemes. However, we urge the developers of such schemes not to combine all modifiers and trapdoors available in one scheme but to use as few as possible: if such a scheme is well designed, it will withstand cryptographic attacks while a complex scheme may distract the attention both of the cryptanalyst *and* the designer of the scheme from the real weaknesses hidden in this new construction. Moreover, each designer should make clear the rational behind the choices made. This way it becomes much easier for the cryptographic community to evaluate the strength of the new proposals.

Apart from this, $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic equations have very nice properties when used in restricted environments and can be used as cryptographic primitives for signing applications. By now, the existence of secure *and* efficient encryption primitives based on the $\mathcal{MQ}$-problem is an open question. However, when we look at the authors and dates of the publications in the bibliography, we see that more and more people get interested in this subject. Hence, we may expect such a secure encryption scheme soon.

Acknowledgements

We want to thank Jasper Scholten (COSIC) for fruitful discussions and An Braeken (COSIC) for helpful remarks. In addition, we want to thank Andrey Sidorenko (TU Eindhoven, The Netherlands) and Jens Zumbrg̈el (University of Zurich, Switzerland) for helpful remarks. Moreover, we want to thank Patrick Felke (RU Bochum, Germany) for sending us a preliminary version of [Fel04] and also for helpful remarks on Section 3.2. Similar, we want to thank Bo-Yin Yang (Tamkang University, Taiwan) for helpful remarks on Section 6.1 and Lih-Chung Wang (Donghwa University, Taiwan) on Section 6.2. Moreover, we want to thank Jintai Ding (University of Cincinnati, USA) for sending us a preliminary version of [DS05b].

This work was supported in part by the Concerted Research Action (GOA) GOA Ambiorix 2005/11 of the Flemish Government and the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT.

References

[BFS96] Jonathan F. Buss, Gudmund Skovbjerg Frandsen, and Jeffrey Outlaw Shallit. The computational complexity of some problems of linear algebra. Research Series RS-96-33, BRICS, Department of Computer Science, University of Aarhus, September 1996. http://www.brics.dk/RS/96/33/, 39 pages.

[BSS99] Ian Blake, Gadiel Seroussi, and Nigel Smart. *Elliptic Curves in Cryptography.* Cambridge University Press, 1999. ISBN 0-521-65374-6.

[BWP05] An Braeken, Christopher Wolf, and Bart Preneel. A study of the security of Unbalanced Oil and Vinegar signature schemes. In *The Cryptographer's Track at RSA Conference 2005*, Lecture Notes in Computer Science. Alfred J. Menezes, editor, Springer, 2005. 13 pages, cf http://eprint.iacr.org/2004/222/.

[CGMT02] Nicolas Courtois, Louis Goubin, Willi Meier, and Jean-Daniel Tacier. Solving underdefined systems of multivariate quadratic equations. In *Public Key Cryptography — PKC 2002*, volume 2274 of *Lecture Notes in Computer Science*, pages 211–227. David Naccache and Pascal Paillier, editors, Springer, 2002.

[CGP00a] Nicolas Courtois, Louis Goubin, and Jacques Patarin. *Flash: Primitive specification and supporting documentation*, 2000. https://www.cosic.esat.kuleuven.ac.be/nessie/workshop/submissions/flash.zip, 9 pages.

[CGP00b] Nicolas Courtois, Louis Goubin, and Jacques Patarin. *SFlash: Primitive specification and supporting documentation*, 2000. https://www.cosic.esat.kuleuven.ac.be/nessie/workshop/submissions/sfla%sh.zip, 10 pages.

[CGP01] Nicolas Courtois, Louis Goubin, and Jacques Patarin. *Quartz: Primitive specification (second revised version)*, October 2001. https://www.cosic.esat.kuleuven.ac.be/nessie Submissions, Quartz, 18 pages.

[CGP02] Nicolas Courtois, Louis Goubin, and Jacques Patarin. *SFlash: Primitive specification (second revised version)*, 2002. https://www.cosic.esat.kuleuven.ac.be/nessie, Submissions, Sflash, 11 pages.

[CGP03a] Nicolas Courtois, Louis Goubin, and Jacques Patarin. *SFlash^{v3}, a fast asymmetric signature scheme — Revised Specificatoin of SFlash, version 3.0*, October 17th 2003. ePrint Report 2003/211, `http://eprint.iacr.org/`, 14 pages.

[CGP03b] Nicolas Courtois, Louis Goubin, and Jacques Patarin. *SFlash^{v3}, a fast asymmetric signature scheme — Revised Specificatoin of SFlash, version 3.0*, October 2nd 2003. ePrint Report 2003/211, `http://eprint.iacr.org/`, 13 pages.

[Cou01] Nicolas T. Courtois. The security of Hidden Field Equations (HFE). In *The Cryptographer's Track at RSA Conference 2001*, volume 2020 of *Lecture Notes in Computer Science*, pages 266–281. D. Naccache, editor, Springer, 2001. `http://www.minrank.org/hfesec.{ps|dvi|pdf}`.

[Cr93] Douglas R. Stinson, editor. *Advances in Cryptology — CRYPTO 1993*, volume 773 of *Lecture Notes in Computer Science*. Springer, 1993. ISBN 3-540-57766-1.

[Cr95] Don Coppersmith, editor. *Advances in Cryptology — CRYPTO 1995*, volume 963 of *Lecture Notes in Computer Science*. Springer, 1995. ISBN 3-540-60221-6.

[CSV93] Don Coppersmith, Jacques Stern, and Serge Vaudenay. Attacks on the birational permutation signature schemes. In Cr [Cr93], pages 435–443.

[CSV97] Don Coppersmith, Jacques Stern, and Serge Vaudenay. The security of the birational permutation signature schemes. *Jounal of Cryptology*, 10:207–221, 1997.

[Dau01] Magnus Daum. Das Kryptosystem HFE und quadratische Gleichungssysteme über endlichen Körpern. Diplomarbeit, Universität Dortmund, August 2001. `http://homepage.ruhr-uni-bochum.de/Magnus.Daum/HFE.{ps.zip|pdf}`, 133 pages.

[DF05] Hans Dobbertin and Patrick Felke. Mistery twister, cryptochallenge 11. `http://www.mistery-twister.com/`, 8 pages, April 2005.

[Din04] Jintai Ding. A new variant of the matsumoto-imai cryptosystem through perturbation. In *Public Key Cryptography — PKC 2004*, volume 2947 of *Lecture Notes in Computer Science*, pages 305–318. Feng Bao, Robert H. Deng, and Jianying Zhou (editors), Springer, 2004.

[DS04] Jintai Ding and Dieter Schmidt. Multivariable public-key cryptosystems. Preprint, 16^{th} of December 2004. 16 pages.

[DS05a] Jintai Ding and Dieter Schmidt. Cryptanalysis of HFEv and internal perturbation of HFE. In PKC [PKC05], pages 288–301.

[DS05b] Jintai Ding and Dieter Schmidt. Rainbow, a new multivariable polynomial signature scheme. In *Conference on Applied Cryptography and Network Security — ACNS 2005, to appear in LNCS*. Springer, 2005. 10 pages.

[DY04] Jintai Ding and Zhijun Yin. Cryptanalysis of TTS and Tame-like multivariate signature schemes. Pre-Proceedings of the The Third International Workshop for Applied PKI, Fukuoka, Japan, October 3-5., 2004.

[ECr05] Ronald Cramer, editor. *Advances in Cryptology — EUROCRYPT 2005*, Lecture Notes in Computer Science. Springer, 2005.

[FD85] Harriet Fell and Whitfield Diffie. Analysis of public key approach based on polynomial substitution. In *Advances in Cryptology — CRYPTO 1985*, volume 218 of *Lecture Notes in Computer Science*, pages 340–349. Hugh C. Williams, editor, Springer, 1985.

[Fel01] Patrick Felke. Multivariate Kryptosysteme, insbesondere das Schema von Imai und Matsumoto. Diplomarbeit, Universität Dortmund, August 2001. 146 pages.

[Fel04] Patrick Felke. On the affine transformations of HFE-cryptosystems and systems with branches. Cryptology ePrint Archive, Report 2004/367, 2004. `http://eprint.iacr.org/2004/367`, version from 2004-12-17, 10 pages.

[FGS05] Pierre-Alain Fouque, Louis Granboulan, and Jacques Stern. Differential cryptanalysis for multivariate schemes. In ECr [ECr05]. 14 pages.

[FJ03] Jean-Charles Faugère and Antoine Joux. Algebraic cryptanalysis of Hidden Field Equations (HFE) using gröbner bases. In *Advances in Cryptology — CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 44–60. Dan Boneh, editor, Springer, 2003.

[GC00] Louis Goubin and Nicolas T. Courtois. Cryptanalysis of the TTM cryptosystem. In *Advances in Cryptology — ASIACRYPT 2000*, volume 1976 of *Lecture Notes in Computer Science*, pages 44–57. Tatsuaki Okamoto, editor, Springer, 2000.

[GJ79] Michael R. Garey and David S. Johnson. *Computers and Intractability — A Guide to the Theory of NP-Completeness.* W.H. Freeman and Company, 1979. ISBN 0-7167-1044-7 or 0-7167-1045-5.

[GM02] Henri Gilbert and Marine Minier. Cryptanalysis of SFLASH. In *Advances in Cryptology — EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 288–298. Lars R. Knudsen, editor, Springer, 2002.

[GMS02] Willi Geiselmann, Willi Meier, and Rainer Steinwandt. An attack on the Isomorphisms of Polynomials problem with one secret. Cryptology ePrint Archive, Report 2002/143, 2002. `http://eprint.iacr.org/2002/143`, version from 2002-09-20, 12 pages.

[Gra05] Louis Granboulan. A generic scheme based on trapdoor oneway permutations with signatures as short as possible. In PKC [PKC05], pages 302–312.

[GSB01] W. Geiselmann, R. Steinwandt, and Th. Beth. Attacking the affine parts of SFlash. In *Cryptography and Coding - 8th IMA International Conference*, volume 2260 of *Lecture Notes in Computer Science*, pages 355–359. B. Honary, editor, Springer, 2001. Extended version: `http://eprint.iacr.org/2003/220/`.

[IM85] Hideki Imai and Tsutomu Matsumoto. Algebraic methods for constructing asymmetric cryptosystems. In *Algebraic Algorithms and Error-Correcting Codes, 3rd International Conference, AAECC-3, Grenoble, France, July 15-19, 1985, Proceed-*

ings, volume 229 of *Lecture Notes in Computer Science*, pages 108–119. Jacques Calmet, editor, Springer, 1985.

[JKJMR05] Antoine Joux, Sébastien Kunz-Jacques, Frédéric Muller, and Pierre-Michel Ricordel. Cryptanalysis of the tractable rational map cryptosystem. In PKC [PKC05], pages 258–274.

[KPG99] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced Oil and Vinegar signature schemes. In *Advances in Cryptology — EUROCRYPT 1999*, volume 1592 of *Lecture Notes in Computer Science*, pages 206–222. Jacques Stern, editor, Springer, 1999.

[KPG03] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced Oil and Vinegar signature schemes — extended version, 2003. 17 pages, `citeseer/231623.html`, 2003-06-11.

[KS98] Aviad Kipnis and Adi Shamir. Cryptanalysis of the oil and vinegar signature scheme. In *Advances in Cryptology — CRYPTO 1998*, volume 1462 of *Lecture Notes in Computer Science*, pages 257–266. Hugo Krawczyk, editor, Springer, 1998.

[KS99] Aviad Kipnis and Adi Shamir. Cryptanalysis of the HFE public key cryptosystem. In *Advances in Cryptology — CRYPTO 1999*, volume 1666 of *Lecture Notes in Computer Science*, pages 19–30. Michael Wiener, editor, Springer, 1999. `http://www.minrank.org/hfesubreg.ps` or `http://citeseer.nj.nec.com/kipnis99cryptanalysis.html`.

[KS04a] Masao Kasahara and Ryuichi Sakai. A construction of public-key cryptosystem based on singular simultaneous equations. In *Symposium on Cryptography and Information Security — SCIS 2004*. The Institute of Electronics, Information and Communication Engineers, January 27–30 2004. 6 pages.

[KS04b] Masao Kasahara and Ryuichi Sakai. A construction of public key cryptosystem for realizing ciphtertext of size 100 bit and digital signature scheme. *IEICE Trans. Fundamentals*, E87-A(1):102–109, January 2004. Electronic version: `http://search.ieice.org/2004/files/e000a01.htm\#e87-a,1,102`.

[LD00] Julio Lopéz and Ricardo Dahab. An overview of elliptic curve cryptography. Technical report, Institute of Computing, State University of Campinas, Brazil, 22nd of May 2000. `http://citeseer.nj.nec.com/333066.html` or `http://www.dcc.unicamp.br/ic-tr-ftp/2000/00-14.ps.gz`.

[LN00] Rudolf Lidl and Harald Niederreiter. *Introduction to Finite Fields and their Applications.* Cambridge University Press, 2000. ISBN 0-521-46094-8.

[LP03] Françoise Levy-dit-Vehel and Ludovic Perret. Polynomial equivalence problems and applications to multivariate cryptosystems. In *Progress in Cryptology — INDOCRYPT 2003*, volume 2904 of *Lecture Notes in Computer Science*, pages 235–251. Thomas Johansson and Subhamoy Maitra, editors, Springer, 2003.

[MI88] Tsutomu Matsumoto and Hideki Imai. Public quadratic polynomial-tuples for efficient signature verification and message-encryption. In *Advances in Cryptology — EUROCRYPT 1988*, volume 330 of *Lecture Notes in Computer Science*, pages 419–545. Christoph G. Günther, editor, Springer, 1988.

[MIHM85] Tsutomu Matsumoto, Hideki Imai, Hiroshi Harashima, and Hiroshi Miyakawa. A cryptographically useful theorem on the connection between uni and multivariate polynomials. *Transactions of the IECE of Japan*, 68(3):139–146, March 1985.

[Moh99] T. Moh. A public key system with signature and master key function. *Communications in Algebra*, 27(5):2207–2222, 1999. Electronic version: `http://citeseer/moh99public.html`.

[MvOV96] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography.* CRC Press, 1996. ISBN 0-8493-8523-7, online-version: `http://www.cacr.math.uwaterloo.ca/hac/`.

[NES] NESSIE: New European Schemes for Signatures, Integrity, and Encryption. Information Society Technologies programme of the European commission (IST-1999-12324). `http://www.cryptonessie.org/`.

[Pat95] Jacques Patarin. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88. In Cr [Cr95], pages 248–261.

[Pat96a] Jacques Patarin. Asymmetric cryptography with a hidden monomial. In *Advances in Cryptology — CRYPTO 1996*, volume 1109 of *Lecture Notes in Computer Science*, pages 45–60. Neal Koblitz, editor, Springer, 1996.

[Pat96b] Jacques Patarin. Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms. In *Advances in Cryptology — EUROCRYPT 1996*, volume 1070 of *Lecture Notes in Computer Science*, pages 33–48. Ueli Maurer, editor, Springer, 1996. Extended Version: `http://www.minrank.org/hfe.pdf`.

[Pat97] Jacques Patarin. The oil and vinegar signature scheme. presented at the Dagstuhl Workshop on Cryptography, September 1997. transparencies.

[Pat00] Jacques Patarin. Secret public key schemes. In *Public-Key Cryptography and Computational Number Theory 2000*, pages 221–237. Stefan Banach, editor, de Gruyter, 2000.

[Per05] Ludovic Perret. A fast cryptanalysis of the isomorphism of polynomials with one secret problem. In ECr [ECr05]. 17 pages.

[PG97] Jacques Patarin and Louis Goubin. Trapdoor one-way permutations and multivariate polynomials. In *International Conference on Information Security and Cryptology 1997*, volume 1334 of *Lecture Notes in Computer Science*, pages 356–368. International Communications and Information Security Association, Springer, 1997. Extended Version: `http://citeseer.nj.nec.com/patarin97trapdoor.html`.

[PGC98a] Jacques Patarin, Louis Goubin, and Nicolas Courtois. C^*_{-+} and HM: Variations around two schemes of T.Matsumoto and H.Imai. In *Advances in Cryptology — ASIACRYPT 1998*, volume 1514 of *Lecture Notes in Computer Science*, pages 35–49. Kazuo Ohta and Dingyi Pei, editors, Springer, 1998. Extended Version: `http://citeseer.nj.nec.com/patarin98plusmn.html`.

[PGC98b] Jacques Patarin, Louis Goubin, and Nicolas Courtois. Improved algorithms for Isomorphisms of Polynomials. In *Advances in Cryptology — EUROCRYPT 1998*, volume 1403 of *Lecture Notes in Computer Science*, pages 184–200. Kaisa Nyberg, editor, Springer, 1998. Extended Version: `http://www.minrank.org/ip6long.ps`.

[PKC05] Serge Vaudenay, editor. *Public Key Cryptography — PKC 2005*, volume 3386 of *Lecture Notes in Computer Science*. Springer, 2005. ISBN 3-540-24454-9.

[SG03] Andrey V. Sidorenko and Ernst M. Gabidulin. The weak keys for HFE. In *Proceedings of the "Seventh International Symposium on Communication Theory and Applications (ISCTA03);, 13th-18th July, 2003, Ambleside, Lake District, UK*, pages 239–244, 2003. 6 pages.

[Sha93] Adi Shamir. Efficient signature schemes based on birational permutations. In Cr [Cr93], pages 1–12.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997.

[The95] Thorsten Theobald. How to break Shamir's asymmetric basis. In Cr [Cr95], pages 136–147.

[Tol03] Ilia Toli. Cryptanalysis of HFE, June 2003. arXiv preprint server, `http://arxiv.org/abs/cs.CR/0305034`, 7 pages.

[Wan05] Lih-Chung Wang. private communication, 16^{th} of March 2005.

[WBP04] Christopher Wolf, An Braeken, and Bart Preneel. Efficient cryptanalysis of RSE(2)PKC and RSSE(2)PKC. In *Conference on Security in Communication Networks — SCN 2004*, Lecture Notes in Computer Science, pages 145–151, September 8–10 2004. Extended version: `http://eprint.iacr.org/2004/237`.

[WC04] Lih-Chung Wang and Fei-Hwang Chang. Tractable rational map cryptosystem. Cryptology ePrint Archive, Report 2004/046, 18th of February 2004. `http://eprint.iacr.org/2004/046/`.

[WHL$^+$05] Lih-Chung Wang, Yuh-Hua Hu, Feipei Lai, Chun-Yen Chou, and Bo-Yin Yang. Tractable rational map signature. In PKC [PKC05], pages 244–257.

[Wol02] Christopher Wolf. *Hidden Field Equations* (HFE) - variations and attacks. Diplomarbeit, Universität Ulm, December 2002. `http://www.christopher-wolf.de/dpl`, 87 pages.

[Wol04] Christopher Wolf. Efficient public key generation for HFE and variations. In *Cryptographic Algorithms and Their Uses 2004*, pages 78–93. Dawson, Klimm, editors, QUT University, 2004.

[WP04a] Christopher Wolf and Bart Preneel. Asymmetric cryptography: Hidden Field Equations. In *European Congress on Computational Methods in Applied Sciences and Engineering 2004*. P. Neittaanmäki, T. Rossi, S. Korotov, E. Oñate, J. Périaux, and D. Knörzer, editors, Jyväskylä University, 2004. 20 pages, extended version: `http://eprint.iacr.org/2004/072/`.

[WP04b] Christopher Wolf and Bart Preneel. Equivalent keys in HFE, C*, and variations. Cryptology ePrint Archive, Report 2004/360, 2004. `http://eprint.iacr.org/2004/360/`, 12 pages.

[WP05] Christopher Wolf and Bart Preneel. Superfluous keys in $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic asymmetric systems. In PKC [PKC05], pages 275–287. Extended version `http://eprint.iacr.org/2004/361/`.

[YC04a] Bo-Yin Yang and Jiun-Ming Chen. Rank attacks and defence in Tame-like multivariate PKC's. Cryptology ePrint Archive, Report 2004/061, 23$^{\text{rd}}$ February 2004. `http://eprint.iacr.org/`, 17 pages.

[YC04b] Bo-Yin Yang and Jiun-Ming Chen. Rank attacks and defence in Tame-like multivariate PKC's. Cryptology ePrint Archive, Report 2004/061, 29$^{\text{rd}}$ September 2004. `http://eprint.iacr.org/`, 21 pages.