

Introduction to \mathcal{MQ} Multivariate Quadratic Public Key Systems and their Applications

Christopher Wolf

École Normale Supérieure, Département d'Informatique
45 rue d'Ulm, F-75230 Paris Cedex 05, France
Christopher.Wolf@ens.fr or chris@Christopher-Wolf.de

March 22, 2006

Abstract

In this article, we investigate the class of multivariate quadratic (\mathcal{MQ}) public key systems. These systems are becoming a serious alternative to RSA or ECC based systems. In particular, we outline the four basic trapdoors Matsumoto-Imai Scheme A (MIA), Hidden Field Equations (HFE), Unbalanced Oil and Vinegar (UOV), and Stepwise Triangular System (STS), give some typical choices of parameters and discuss the advantages and disadvantages of these kinds of schemes. After this concise overview, we determine specific application domains in which \mathcal{MQ} -schemes have advantages over RSA or ECC. We concentrate on product activation keys, electronic stamps and fast one-way functions.

Keywords: Multivariate Quadratic Equations, Public Key Schemes, Applications

1 Introduction

Public key cryptography is used in e-commerce systems for authentication (electronic signatures) and secure communication (encryption). The security of using current public key cryptography centres on the difficulty of solving certain classes of problems. The RSA scheme relies on the difficulty of factoring large integers, while the difficulty 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 hard, research on new schemes that are based on other classes of problems is worthwhile. Such work provides greater diversity and hence forces cryptanalysts to expend additional effort concentrating on completely new types of problems. In addition, important results on the potential weaknesses of existing public key schemes are emerging as techniques for factorisation and solving discrete logarithm continually improve. Polynomial time quantum algorithms [Sho97] can be used to solve both problems and hence, 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 log problem. This points to the importance of research into new algorithms for asymmetric encryption. We want to stress at this point that there are not many results known about the vulnerability of cryptographic hard problems against quantum algorithm. We are only aware of [Sho97] at this point. Hence, more research effort in this direction seems to be imperative if we assume the existence of quantum computers within the next decades.

In addition, we want to point out that different types of schemes have different kinds of properties: with schemes based on ECC, rather short signatures in the range of 320 bits (cf [MvOV96]) are possible, in comparison to 1024–4096 for RSA. On the other hand, the patents on RSA have expired, while there are still patents guarding the use of ECC (cf [MvOV96]). Hence, applications which require a patent-free algorithm are likely to prefer RSA while the requirement for short signatures would lead to the use of ECC. There are other properties of schemes such as verification time, signature creation time, public and private key size. All of them play an important role when choosing a specific algorithm for a particular application domain. Hence, having secure schemes based on different problems, increases the variety of algorithms and hence gives the users of cryptographic primitives more choice. In turn, this increases the chance to have the “right fit” for a particular problem and reduces the necessity to make compromises — either in terms of speed, memory, or security.

One proposal for secure public key schemes is based on the problem of solving *Multivariate Quadratic* equations (\mathcal{MQ} -problem) over finite fields. In the last two decades, several such public key schemes have been proposed, *e.g.*, [MI88, Pat96b, KPG99]. All of them use the fact that the \mathcal{MQ} -problem is difficult, namely \mathcal{NP} -complete (cf [GJ79, p. 251] and [PG97, App.] for a detailed proof)). Here, we mean with \mathcal{MQ} -problem finding a solution $x \in \mathbb{F}$ for a given system of quadratic polynomials (cf Fig. 1) and a given vector $y \in \mathbb{F}^m$. We will introduce the \mathcal{MQ} -problem more formally in Sect. 2.1. In this context, we want to stress that linear

$$\mathcal{P} := \begin{cases} y_1 & = & p_1(x_1, \dots, x_n) \\ y_2 & = & p_2(x_1, \dots, x_n) \\ & \vdots & \\ y_m & = & p_m(x_1, \dots, x_n), \end{cases}$$

Fig. 1: Example of an \mathcal{MQ} -problem with n variables and m equations

or affine polynomial equations can be solved in polynomial time, *e.g.*, using Gaussian elimination. The knapsack cryptosystem is also based on an \mathcal{NP} -complete problem (cf [MvOV96]). Due to special properties of these kinds of schemes, it was possible to break most of the proposals in this area. Therefore, basing a scheme on an \mathcal{NP} -complete problem does not guarantee its security. But in the case of \mathcal{MQ} -schemes, much research has been done on the average complexity of solving the corresponding equations with trapdoor. Although some schemes have been broken (*e.g.*, [Pat95, CSV97, KS98, KPG99, KS99, FJ03, WBP04]), the area is vital and promises efficient algorithms — at present mostly for signing, but encryption should be possible, too, at least from a theoretical perspective. As this article can only give a short overview, we point to [WP05c] for the mathematical background and more details on the schemes discussed here.

In this paper, we introduce the basic concepts of multivariate quadratic schemes and investigate for which types of applications they are particularly suitable. This paper is organised as follows: after introducing the necessary mathematical notation in Sect. 2, we give a concise overview of proposed basic schemes and discuss their advantages and disadvantages in Sect. 3. Then, we move on to possible applications such as fast one-way functions, electronically signed stamps, and product activation keys (Sect. 4). This paper concludes with Sect. 5.

2 Basic Concepts

2.1 Mathematical Background

Let \mathbb{F} be a finite field of prime characteristic with $q := |\mathbb{F}|$ elements; hence q is a prime-power, cf [LN86] for the theory of finite fields. Moreover, using a polynomial $i(t)$, irreducible over \mathbb{F} , we can define an extension field $\mathbb{E} := \mathbb{F}[t]/i(t)$ over \mathbb{F} . We have the degree of polynomial $i(t)$ to be n and hence, \mathbb{E} is an n -dimensional extension of the ground field \mathbb{F} . Addition in \mathbb{E} is the coefficient-wise addition of polynomials and multiplication corresponds to the multiplication of polynomials, performed modulo the generating polynomial $i(t)$. In this context, we want to recall that we have $x^q = x$ for any $x \in \mathbb{F}$ in the finite field. Consequently, the operation X^q for $X \in \mathbb{E}$ is linear in the extension field \mathbb{E} . We denote with $\phi : \mathbb{E} \rightarrow \mathbb{F}^n$ the canonical, coefficientwise bijection between the extension field \mathbb{E} and the vector space \mathbb{F}^n and with $\phi : \mathbb{F}^n \rightarrow \mathbb{E}$ its inverse. With these preliminaries, we are now able to define the \mathcal{MQ} -problem more rigorously.

In the multivariate system of equations \mathcal{P} (cf fig. 1 and 2), the polynomials p_i have the form

$$p_i(x_1, \dots, x_n) := \sum_{1 \leq j \leq k \leq n} \gamma_{i,j,k} x_j x_k + \sum_{j=1}^n \beta_{i,j} x_j + \alpha_i,$$

for $1 \leq i \leq m$ and $\alpha_i, \beta_{i,j}, \gamma_{i,j,k} \in \mathbb{F}$ (constant, linear, and quadratic terms), *i.e.*, they form an instance of an $\mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$ -problem with m equations in n variables x_1, \dots, x_n each. For the ease of notation, we define the polynomial-vector $\mathcal{P} := (p_1, \dots, p_m)$. Each coefficient p_i is a quadratic polynomial in the n variables x_1, \dots, x_n .

With these terms defined, we are now able to express the private key as the triple (S, \mathcal{P}', T) where $S \in \text{Aff}^{-1}(\mathbb{F}^n), T \in \text{Aff}^{-1}(\mathbb{F}^m)$ are affine transformations and $\mathcal{P}' \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$ is a polynomial-vector $\mathcal{P}' := (p'_1, \dots, p'_m)$ in m polynomials; each polynomial depends on the input variables x'_1, \dots, x'_n . Throughout this paper, we denote components of this private vector \mathcal{P}' by a prime $'$. To obtain a difficult \mathcal{MQ} -problem,

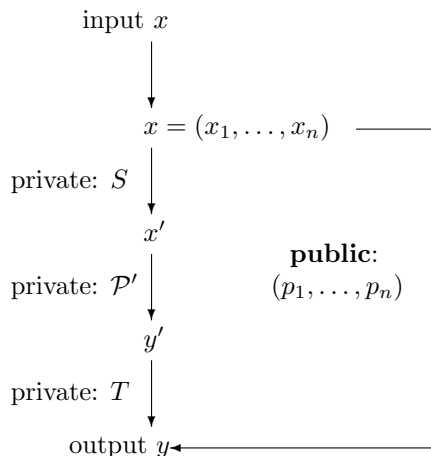


Fig. 2: Graphical Representation of the \mathcal{MQ} -trapdoor (S, \mathcal{P}', T)

it is necessary that the polynomials p'_1, \dots, p'_m are of degree 2 at least. For efficiency reasons, they should be of degree 2 at most. In addition, the affine transformation S can be represented in the form of an invertible matrix $M_S \in \mathbb{F}^{n \times n}$ and a vector $v_s \in \mathbb{F}^n$, *i.e.*, we have $S(x) := M_S x + v_s$. Similarly, we have $T(x) := M_T x + v_t$ for $M_T \in \mathbb{F}^{m \times m}$ an invertible matrix and $v_t \in \mathbb{F}^m$ a vector.

In contrast to the public polynomial vector $\mathcal{P} \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$, the design goal for public key schemes based on the \mathcal{MQ} -problem is to have a central map $\mathcal{P}' : \mathbb{F}^n \rightarrow \mathbb{F}^m$ which allows efficient inversion, *i.e.*, easy computation of x'_1, \dots, x'_n for given y'_1, \dots, y'_m . At least for secure \mathcal{MQ} -schemes, this is not the case if the public key \mathcal{P} together with known y_1, \dots, y_n alone is given. The main difference between \mathcal{MQ} -schemes lies in their special construction of the central map \mathcal{P}' and consequently the trapdoor they embed into a specific class of \mathcal{MQ} -problems.

2.2 Public Key Generation

In all \mathcal{MQ} -schemes, the public key \mathcal{P} is computed as function composition of the affine transformations $S : \mathbb{F}^n \rightarrow \mathbb{F}^n$, $T : \mathbb{F}^m \rightarrow \mathbb{F}^m$ and the central map $\mathcal{P}' : \mathbb{F}^n \rightarrow \mathbb{F}^m$, *i.e.*, we have $\mathcal{P} = T \circ \mathcal{P}' \circ S$. By construction, we have $\forall x \in \mathbb{F}^n : \mathcal{P}(x) = T(\mathcal{P}'(S(x)))$. Efficient algorithms for computing the public key for a given private key can be found in [MI88, Wol04]. Decomposing \mathcal{P} into (S, \mathcal{P}', T) is called the “Isomorphism of Polynomials” (IP), cf [Pat96b]. For $\mathcal{P}, \mathcal{P}'$ without structure, *i.e.*, in particular random equations for \mathcal{P}' , it is considered to be a hard problem in itself. Security evaluations for IP can be found in [PGC98, GMS02, LP03, Per05].

2.3 Decryption/Signing

To decrypt for a given $y \in \mathbb{F}^m$ (or to compute its signature, respectively), we have to invert the computation of $y = \mathcal{P}(x)$. Using the trapdoor-information (S, \mathcal{P}', T) , cf Fig. 2, this is easy. First, we observe that transformation T is a bijection. In particular, we can compute $y' = M_T^{-1}(y - v_t)$. The same is true for given $x' \in \mathbb{F}^n$ and $S \in \text{Aff}^{-1}(\mathbb{F}^n)$. Using the LU-decomposition of the matrices M_S, M_T , this computation takes time $O(n^2)$ and $O(m^2)$, respectively. Hence, the difficulty lies in evaluating $x' = \mathcal{P}'^{-1}(y')$. We will discuss different strategies in Sect. 3 as they depend on the structure of the central map \mathcal{P}' .

2.4 Encryption/Verification

In contrast to decryption/signing, the encryption/verification step is the same for all \mathcal{MQ} -schemes: given a vector $x \in \mathbb{F}^n$, we evaluate the polynomials

$$p_i(x_1, \dots, x_n) := \sum_{1 \leq j \leq k \leq n} \gamma_{i,j,k} x_j x_k + \sum_{j=1}^n \beta_{i,j} x_j + \alpha_i,$$

for $1 \leq i \leq m; 1 \leq j \leq k \leq n$ and given $\alpha_i, \beta_{i,j}, \gamma_{i,j,k} \in \mathbb{F}$. Obviously, all operations can be efficiently computed, in particular if the field \mathbb{F} is of characteristic 2. Assuming uniform costs for the finite field operations, we obtain a total of $O(mn^2)$ steps for evaluating the public key.

3 Schemes based on the \mathcal{MQ} -problem

As explained in the previous section, all schemes based on the \mathcal{MQ} -problem have the same structure for the public key. Hence, their key-sizes can be computed using the same formula. First, we define

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

for the number of terms per polynomial. The first row in the above expression comes from the fact that we have $x_i^2 = x_i$ for $\mathbb{F} = GF(2)$ and $1 \leq i \leq n$, *i.e.*, quadratic terms of the form x_i^2 over $GF(2)$ reduce to linear terms.

Using the above formula, we obtain $m\tau(n) = O(mn^2)$ for the number of coefficients and hence a memory requirement of $\log_{256}(q)m\tau(n)$ byte. For a secure \mathcal{MQ} -system, the public key polynomials should behave similar to random equations. Therefore, we do not expect to find efficient compression techniques for these keys but move on to a detailed description of concrete examples for the central map \mathcal{P}' .

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 $\alpha'_i, \beta'_{i,j}, \gamma'_{i,j,k} \in \mathbb{F}$ for $1 \leq i \leq m$ and $1 \leq j \leq k \leq n$. We say that the polynomials below are central equations in UOV-shape:*

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

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 then be solved, *e.g.*, using Gaussian elimination.

Moreover, Unbalanced Oil and Vinegar schemes (UOV) omit the affine transformation T but only use $S \in \text{Aff}^{-1}(\mathbb{F}^n)$. 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 the same shape. Hence, we do not need T to hide a special structure. Moreover, using the notion of equivalent private keys [WP05a, WP05b] we can actually show that the transformation T could always be moved into the central equations \mathcal{P}' and hence, does not give a security-gain.

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]. Possible choices for UOV are $q = 2, m = 64, n = 192$ or $n = 256$, respectively, as suggested in [KPG03].

3.2 Stepwise Triangular Systems: STS

Another approach to obtain an invertible central map is used in step-wise triangular systems (STS) as a generalisation of Bilinear Maps [Sha93], Triangular Plus Minus [GC00], and RSSE(2)PKC [KS05] — and can be found in [WBP04]. As UOV, STS are defined over a finite field \mathbb{F} and use a special structure for the

$$\begin{array}{l}
\text{Step 1} \\
\vdots \\
\text{Step } l \\
\vdots \\
\text{Step } L
\end{array}
\left\{ \begin{array}{l}
p'_1 \quad (x'_1, \dots, x'_r) \\
\vdots \\
p'_r \quad (x'_1, \dots, x'_r) \\
\\
p'_{(l-1)r+1} \quad (x'_1, \dots, x'_r, \dots, x'_{(l-1)r+1}, \dots, x'_{l_r}) \\
\vdots \\
p'_{l_r} \quad (x'_1, \dots, x'_r, \dots, x'_{(l-1)r+1}, \dots, x'_{l_r}) \\
\\
p'_{(L-1)r+1} \quad (x'_1, \dots, x'_r, \dots, x'_{(l-1)r+1}, \dots, x'_{l_r}, \dots, x'_{n-r+1}, \dots, x_n) \\
\vdots \\
p'_{L_r} \quad (x'_1, \dots, x'_r, \dots, x'_{(l-1)r+1}, \dots, x'_{l_r}, \dots, x'_{n-r+1}, \dots, x_n)
\end{array} \right.$$

Fig. 3: Central Equations p'_i in a Regular STS Scheme

central map \mathcal{P}' which allows easy inversion (cf Figure 3 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. The overall shape of the private polynomials leads to the name step-wise Triangular Scheme (STS), cf Figure 3.

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 $(x'_{(l-1)r+1}, \dots, x'_{l_r})$ which satisfy the corresponding equations

$$\begin{aligned}
y'_{(l-1)r+1} &= p'_{(l-1)r+1}(x'_1, \dots, x'_{l_r}) \\
&\vdots \\
y'_{l_r} &= p'_{l_r}(x'_1, \dots, x'_{l_r})
\end{aligned}$$

for given $y'_{(l-1)r+1}, \dots, y'_{l_r} \in \mathbb{F}$. 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. 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.

Obviously, the above idea can be easily extended: let r_1, \dots, r_L be L integers such that $r_1 + \dots + r_L = n$, the number of variables, and $m_1, \dots, m_L \in \mathbb{N}$ such that $m_1 + \dots + m_L = m$, 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 $1 \leq l \leq L$. In a general step-wise 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. We want to stress in this context that we do not assume any specific structure for the private polynomials p'_1, \dots, 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 $r_1 = \dots = r_L = m_1 = \dots = m_L$, which we denote by r (see above). Consequently, we have $n = m = Lr$.

After outlining both regular and general step-wise 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, 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 $r_1 = u$, $m_L = v$, $m_1 = \dots = m_{L-1} = r_2 = \dots = r_L = 1$, *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 true 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 $O(mn^3Lq^r + n^2Lrqr)$, 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. Still, there are some nested constructions like Rainbow, enTTS, and TRMS possible. Picking enTTS as a typical example, we have $1 = 256, m = 20, n = 28$, which leads to a public key of 8 kB and a private key of 1.4 kB.

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} . To relate between the extension field \mathbb{E} and the vector space \mathbb{F}^n , we use the canonical bijection $\phi : \mathbb{E} \rightarrow \mathbb{F}^n$.

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 univariate polynomial over \mathbb{E} is of the MIA-type:*

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

Now we say the central map $\mathcal{P}' := \phi \circ P' \circ \phi^{-1}$ is in MIA-shape.

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 $h \cdot (q^\lambda + 1) \equiv 1 \pmod{q^n - 1}$ 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 $(Y')^h = X'^{[h \cdot (q^\lambda + 1)]} = X'$ 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 [Pat96b]). As X and X^{q^λ} with $q := |\mathbb{F}|$ are linear over the vector space \mathbb{F}^n , their product $P(X') := (X')^{q^\lambda + 1}$ leads to a Multivariate Quadratic system over \mathbb{F}^n .

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 [WP05a, WP05b] 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 [WP05c] for the terminology) 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, CGP02]. 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.

3.3.1 MIA-

We move on to a description of MIA- or C^{*-} [Pat96a]. Its name is motivated by the fact that many of the public key polynomials are “subtracted”. Less loosely speaking, we use the idea of a projection $\pi : \mathbb{F}^n \rightarrow \mathbb{F}^{n-r}$ for $n, r \in \mathbb{N}$ and $r \geq 1$. The overall construction of the public key becomes $\mathcal{P} = \pi \circ T \circ \mathcal{P}' \circ S$. This means in particular that we obtain the function $\mathcal{P} : \mathbb{F}^n \rightarrow \mathbb{F}^{n-r}$ for the public key by removing the last r polynomials p_{n-r+1}, \dots, p_n from the public key. Hence, for solving the equation $\mathcal{P}(X) = Y$ for a vector $Y \in \mathbb{F}^{n-r}$ and unknown $X \in \mathbb{F}^n$, we add r random elements from \mathbb{F} for the missing components y_{n-r+1}, \dots, y_n before inverting the transformation T . The rest of inversion of \mathcal{P} works as for MIA. In terms of cryptanalysis, the new scheme has a strength of q^r (cf [Pat96a, CGP02]). In particular, the construction of MIA- with a special choice of parameters has been used in the signature scheme Sflash^{v2}. It uses the

parameters $q = 128, n = 37, r = 11$. This leads to a private/public key size of 15.4/2.5kB. In [CGP02, Sect. 8], the time to verify or generate a signature is empirically obtained to be less than 1 ms on a PC, without giving further details on the hardware used.

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:

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

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

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 map $\mathcal{P}' := \phi \circ P' \circ \phi^{-1}$ 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 dimension n of the extension field \mathbb{E} and 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 [Pat96b, WP05c] for possible ways to overcome this problem.

As for MIA, we notice that the HFE polynomial $P'(X')$ can be expressed as *Multivariate Quadratic* equations $\mathcal{MQ}(\mathbb{F}^n)$ and are hence a possible central equation, cf [WP05c].

From a cryptanalytic point of view, basic HFE are broken: an efficient key recovery attack, using the MinRank-problem, 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, WP04]. Here, [Pat96b] gives some general considerations of HFE after its development, *e.g.*, a general linearization attack against all multivariate schemes, 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 [WP04]. In particular, this paper outlines two versions of HFE which are secure against all known attacks. Finally, [WP05a, WP05b] show that HFE allow many equivalent keys and hence, waste memory. Typical choices of parameters are $q = 2, n = 107, m = 100, r = 7, d = 129$ for Quartz-7m, which lead to a public/private key of 71/3 kB, respectively [WP04]. Using a so-called “Chained-Patarin-Construction” (CPC), we obtain a signature size of only 128 bits — avoiding the birthday paradox.

3.5 General Characteristics of \mathcal{MQ} -schemes

As we saw in the previous sections, multivariate quadratic schemes have rather large public keys in the range of 8kB – 71kB. The private key is usually much smaller, *e.g.*, 71 kB vs. 3 kB for HFE. In terms of signature or message sizes, we can go down until 128 bits (Quartz-7m). In any case, signature verification and encryption take less than 1 ms on a PC while the time for signature generation reaches 10 s (Quartz-7m), but is usually in the range of 100 ms for the other schemes. Hence, the strong points of multivariate quadratic schemes are short signatures, low message overhead/short signature sizes and fast encryption/signature verification.

4 Applications

Starting from the observations from the previous section, we develop applications based on multivariate quadratic schemes. All proposals in this section have an expected security level of 2^{80} — based on our

current knowledge of cryptanalysis. A level of 2^{80} 3-DES computations has been identified in the European project [NES] as an adequate security level for nowadays cryptographic applications.

4.1 Electronic Stamps

The idea here is to replace the current stamping machines by digitally signed stamps which can then be printed on any normal printer — if they are printed more than once, the person who has bought the stamp will be caught, cf [NS00, PV00] for a thorough discussion of this idea. In a nutshell, we have two objectives in this context. First, we want the corresponding signature to be as short as possible — for example, using message recovery techniques, cf [MvOV96]. Second, the signature verification time should be low as the post service has to verify the signed stamps on a rather high rate. In addition, stamps have a rather low value, so signature verification may not be costly and must hence be fast.

Table 1: Proposed Scheme for Electronic Stamps

| Hash [bit] | Parameter | Priv. Key [kByte] | Pub. Key [kByte] | Sign [ms] | Verify [ms] | Expansion [bit] |
|---------------|-----------------------------------|----------------------|---------------------|--------------|----------------|--------------------|
| 160 | $q = 128$ $n = 37$ $r = 11$ | 2.5 | 15.4 | < 2.7 | 1 0.8 | 237 |

The characteristics of our proposal are summarised in Table 1. We base our proposal on Sflash^{v2} as this is a bijection and hence, we will be able to obtain a valid signature in any case. The overall idea is to compute a 160-bit hash of the whole message, using a cryptographically secure hash function. Due to the ongoing discussion in this field, we do not recommend any at the moment. The remaining $259-160=99$ bits are used to encode a part of the message to sign. Hence, the overall message expansion becomes $77 + 160 = 237$ bits although the whole signature has — strictly speaking — a size of 259 bits, cf [CGP02] for details on Sflash^{v2}.

4.2 Product Activation Keys

For product activation keys, nowadays mostly symmetric key techniques are used. To the knowledge of the authors, the idea to use public key techniques for this problem is due to [Ber03]. In contrast to symmetric key techniques, crackers cannot retrieve the symmetric key and hence, they are not able to compute valid activation keys — even if they manage to get a copy of the (public) key of the corresponding product. Therefore, techniques based on asymmetric cryptology are clearly superior — if they allow similar size and speed as their symmetric counterparts. In this paper, we propose to use a construction based on HFE- as outlined in [CGP01] and with the tweaks proposed in [WP04]. In particular, we suggest to compute an 80-bit

Table 2: Proposed Schemes for Product Activation Keys

| User-ID [bit] | Key [char] | Parameter | Priv. Key [byte] | Pub. Key [kByte] | Gen. [s] | Ver. [ms] | Signature [bit] |
|------------------|---------------|-------------------|---------------------|---------------------|--------------|--------------|--------------------|
| 20 | 21 | $q=2, n=107, r=7$ | 3264 | 71 | ≈ 10 | < 1 | 107 |
| 40 | 25 | $q=2, n=127, r=7$ | 4509 | 119 | ≈ 15 | < 2 | 127 |

hash from a user-ID of 20/40 bits. The product activation key is then the signature of the 100/120 bits concatenation of the user-ID and the corresponding hash. In symbols: $m := i || h(i)$ where m is the 100/120 bit message to be signed, i the 20/40-bit user-id, $h(\cdot)$ a cryptographically secure hash function and $||$ the concatenation of bit-strings. In this context we want to point out that this proposal is not vulnerable to the birthday paradox and hence, we do not need a hash-length of 160 bits to achieve a security level of 2^{80} . To distinguish different products, we suggest to use different public (and hence private) keys for each product as this rules out attacks using valid signatures for one product for another product. We want to stress that a public key size in the suggested range is not a problem to be put on a product CD/DVD and hence the additional memory requirement is negligible. Finally, we give the length of the corresponding activation key

in characters, assuming a code with 36 symbols. For information: Microsoft uses a 25 character code for its products. The verification and signature timings are extrapolations from [CGP01].

4.3 Fast One-Way functions

The last application we see are fast but secure one-way functions. In this case, we do not need a trapdoor but merely the intractability of the \mathcal{MQ} -problem. Hence, we suggest to generate random \mathcal{MQ} -polynomials with the parameters as suggested in Table 3. As for Table 1, the evaluation timings are based on [CGP02]. A

Table 3: Proposed Schemes for One-Way functions

| Seed [bit] | Parameter | \mathcal{MQ} -System [kByte] | Evaluation [ms] |
|---------------|-------------------|-----------------------------------|--------------------|
| 259 | $q = 128, n = 37$ | 23 | < 1 |
| 469 | $q = 128, n = 67$ | 134 | < 1 |

similar construction — but based on sparse polynomials over large finite fields — has been used by Purdy in [Pur74] to construct a kind of hash function. While this proposal is based on the intractability of univariate polynomial equations of large degree, our proposal is based on the difficulty of solving polynomial-equations of small degree, but with a high number of variables. Although the construction we propose here is difficult to invert, it is not resistant against collisions. The reason is a general attack from [Pat96b, Sect. 3, “Attack with related messages”] against \mathcal{MQ} -schemes which can be applied here.

5 Conclusions

In this paper, we gave a concise overview of an alternative class of public key schemes, called “Multivariate Quadratic” schemes. A more detailed introduction is given in [WP05c]. In particular — using the variations HFE- and MIA- — we developed practical instantiations for the problems of fast one-way functions, electronic stamps, and product activation keys. In all cases, the short signature verification times and also the rather short signature generation times (resp., encryption and decryption) are a clear advantage over schemes based on RSA and ECC. In particular, the authors is not aware of patent-restrictions for HFE- and MIA-. Hence, they are also a good alternative for projects where patent royalties are a serious consideration. We also want to point out that Sflash^{v2} has been recommended by NESSIE for special application domains. Similar, Quartz was a recommendation in NESSIE for applications which require particularly short signatures.

References

- [Ber03] Giuliano Bertoletti. Private communication, June 2003.
- [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*, volume 3376 of *Lecture Notes in Computer Science*. Alfred J. Menezes, editor, Springer, 2005. 13 pages, cf <http://eprint.iacr.org/2004/222/>.
- [CGP00a] Nicolas Courtois, Louis Goubin, and Jacques Patarin. *Flash: Primitive specification and supporting documentation*, 2000. <https://www.cosic.esat.kuleuven.be/nessie>, submissions, 9 pages.
- [CGP00b] Nicolas Courtois, Louis Goubin, and Jacques Patarin. *Sflash: Primitive specification and supporting documentation*, 2000. <https://www.cosic.esat.kuleuven.be/nessie>, submissions, Sflash, 10 pages.
- [CGP01] Nicolas Courtois, Louis Goubin, and Jacques Patarin. *Quartz: Primitive specification (second revised version)*, October 2001. <https://www.cosic.esat.kuleuven.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.be/nessie>, Submissions, Sflash, 11 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. *Journal of Cryptology*, 10:207–221, 1997.
- [DBP96] Hans Dobbertin, Antoon Bosselaers, and Bart Preneel. RIPEMD-160: A strengthened version of RIPEMD. In *Fast Software Encryption — FSE 1996*, volume 1039 of *Lecture Notes in Computer Science*, pages 71–82. Dieter Gollmann, editor, Springer, 1996. Updated version at <http://www.esat.kuleuven.be/~cosicart/ps/AB-9601/AB-9601.ps.gz>.
- [FC 00] Yair Frankel, editor. *Financial Cryptography, 4th International Conference, FC 2000 Anguilla, British West Indies, February 20-24, 2000, Proceedings*, volume 1962 of *Lecture Notes in Computer Science*. Springer, 2001. ISBN 3-540-42700-7.
- [FIP] National Institute of Standards and Technology. *Federal Information Processing Standards Publication 180-1: Secure Hash Standard*, 17th April 1995. <http://www.itl.nist.gov/fipspubs/fip180-1.htm>.
- [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.
- [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.
- [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, AAEC-3, Grenoble, France, July 15-19, 1985, Proceedings*, volume 229 of *Lecture Notes in Computer Science*, pages 108–119. Jacques Calmet, editor, Springer, 1985.
- [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 ciphertext 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>.
- [KS05] Masao Kasahara and Ryuichi Sakai. A construction of public-key crypto based on singular simultaneous equations and its variants. Technical report, 2005. <http://www.osaka-gu.ac.jp/php/kasahara/km.pdf>, 6 pages.
- [LN86] Rudolf Lidl and Harald Niederreiter. *Introduction to Finite Fields and their Applications*. Cambridge University Press, 1986. ISBN 0-521-30706-6.

- [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.
- [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/>.
- [NS00] David Naccache and Jacques Stern. Signing on a postcard. In FC — Financial Crypto [FC 00], pages 121–135. <http://citeseer.ist.psu.edu/naccache00signing.html>.
- [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.
- [Per05] Ludovic Perret. A fast cryptanalysis of the isomorphism of polynomials with one secret problem. In *Advances in Cryptology — EUROCRYPT 2005*, Lecture Notes in Computer Science. Ronald Cramer, editor, Springer, 2005. 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>.
- [PGC98] 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>.
- [Pur74] George B. Purdy. A high security log-in procedure. *Communications of the ACM*, 17(8):442–445, August 1974.
- [PV00] Leon A. Pintsov and Scott A Vanstone. Postal revenue collection in the digital age. In FC — Financial Crypto [FC 00], pages 105–120. <http://citeseer.ist.psu.edu/pintsov00postal.html>.
- [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.
- [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*, volume 3352 of *Lecture Notes in Computer Science*, pages 294–309. Springer, September 8–10 2004. Extended version: <http://eprint.iacr.org/2004/237>.
- [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.
- [Wol05] Christopher Wolf. *Multivariate Quadratic Polynomials in Public Key Cryptography*. Ph.D. thesis, Katholieke Universiteit Leuven, Belgium, November 2005. <http://hdl.handle.net/1979/148>, 156+xxiv pages.
- [WP04] 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. Knörzner, editors, Jyväskylä University, 2004. 20 pages, extended version: <http://eprint.iacr.org/2004/072/>.
- [WP05a] Christopher Wolf and Bart Preneel. Equivalent keys in HFE, C^* , and variations. In *Proceedings of Mycrypt 2005*, volume 3715 of *Lecture Notes in Computer Science*, pages 33–49. Serge Vaudenay, editor, Springer, 2005. Extended version <http://eprint.iacr.org/2004/360/>, 15 pages.
- [WP05b] Christopher Wolf and Bart Preneel. Superfluous keys in Multivariate Quadratic asymmetric systems. In *Public Key Cryptography — PKC 2005*, volume 3386 of *Lecture Notes in Computer Science*, pages 275–287. Serge Vaudenay, editor, Springer, 2005. Extended version <http://eprint.iacr.org/2004/361/>.
- [WP05c] Christopher Wolf and Bart Preneel. Taxonomy of public key schemes based on the problem of multivariate quadratic equations. Cryptology ePrint Archive, Report 2005/077, 12th of May 2005. <http://eprint.iacr.org/2005/077/>, 64 pages.