

# Applications of *Multivariate Quadratic* Public Key Systems

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:** In this article, we investigate the class of multivariate quadratic ( $MQ$ ) public key systems. These systems are becoming a serious alternative to RSA or ECC based systems. After introducing the main ideas and sketching some relevant systems, we deal with the advantages and disadvantages of these kinds of schemes. Based on our observations, we determine application domains in which  $MQ$ -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

### 1.1 Public Key Cryptography

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 this paper, we will give a short overview over some of these schemes. A more detailed description of these schemes (*e.g.*, including figures) can be found in the online version of this paper [WP04a].

## 1.2 Outline

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 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 [LN86]. 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  $i(t)$  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  $\mathbb{E}$ . With these preliminaries, we are now able to define the  $\mathcal{MQ}$ -problem more rigorously.

In the multivariate system of equations  $\mathcal{P}$ , 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  $\mathcal{MQ}_m(\mathbb{F}^n)$ -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  $x_1, \dots, x_n$ . In this polynomial vector  $\mathcal{P}$ , the constants  $\alpha_1, \dots, \alpha_m$  are obtained by subtracting coefficient-wise the knowns  $y_1, \dots, y_m$  from the constant part of the original  $\mathcal{MQ}$ -problem.

With these terms defined, we are now able to express the private key as the triple  $(S, \mathcal{P}', T)$  where  $S \in \text{AGL}_n(\mathbb{F}), T \in \text{AGL}_m(\mathbb{F})$  are affine transformations and  $\mathcal{P}' \in \mathcal{MQ}_m(\mathbb{F}^n)$  is a polynomial-vector  $\mathcal{P}' := (p'_1, \dots, p'_m)$  in  $m$  polynomials; each polynomial depends on the input variables  $x'_1, \dots, x'_n$ . To obtain a difficult  $\mathcal{MQ}$ -problem, 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. Throughout this paper, we denote components of this private vector  $\mathcal{P}'$  by a prime  $'$ . 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  $\mathcal{P} \in \mathcal{MQ}_m(\mathbb{F}^n)$ , the design goal for public key schemes based on the  $\mathcal{MQ}$ -problem is to have a private polynomial vector  $\mathcal{P}'$  which allows efficient inversion, *i.e.*, the 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 knowns  $y_1, \dots, y_n$  alone is given. The main difference between  $\mathcal{MQ}$ -schemes lies in their special construction of the central equations  $\mathcal{P}'$  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 equations  $\mathcal{P}' : \mathbb{F}^n \rightarrow \mathbb{F}^m$ , *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].

### 2.3 Decryption/Signing

To decrypt for a given  $y \in \mathbb{F}^m$  (or to compute its signature, respectively), we observe that we have to invert the computation of  $y = \mathcal{P}(x)$ . Using the trapdoor-information  $(S, \mathcal{P}', T)$  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  $S \in \text{AGL}_n(\mathbb{F})$ . 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.

### 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

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

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.

### 3.1 $C^*$

#### 3.1.1 General Scheme

In 1988, Matsumoto and Imai developed the scheme  $C^*$  [MI88]. It is one of the oldest multivariate schemes. Therefore, its own security and also the security of its variations is well understood. In  $C^*$ , the central equation  $\mathcal{P}'$  has the form

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

over the extension field  $\mathbb{E}$  and with  $\lambda \in \mathbb{N}$  such that  $\gcd(q^n - 1, q^\lambda + 1) = 1$ . The main point is that  $C^*$  mixes operations over the ground field  $\mathbb{F}$  with operations in the extension field  $\mathbb{E}$ : the first is used for the affine transformations  $S, T$  and the latter for the private key equations  $\mathcal{P}'$ . We inspect now how we can express  $P'(X')$  over the ground field  $\mathbb{F}$ . We observe that  $X^q = X$  is a linear transformation in the extension field  $\mathbb{E}$ , and notice that we hence can express  $P'(X')$  using multivariate quadratic polynomial equations  $p'_1, \dots, p'_m$  over the ground field  $\mathbb{F} = \text{GF}(q)$ . This way, we are able to construct an  $\mathcal{MQ}_m(\mathbb{F}^n)$ -problem from the equation over the extension field  $\mathbb{E}$ . Moreover, the condition  $\gcd(q^n - 1, q^\lambda + 1) = 1$  ensures that the equation  $h \cdot (q^\lambda + 1) \equiv 1 \pmod{q^n - 1}$  has exactly one solution  $h \in \mathbb{N}$  with  $h < q^n - 1$ . Given  $h$ , we can solve  $Y' = P'(X')$  as  $(Y')^h \equiv X'^{[h \cdot (q^\lambda + 1)]} \equiv X'$  by raising  $Y'$  to the power of  $h$ . Note that these operations take place in the extension field  $\mathbb{E}$ . All in all, this approach is similar to RSA. However, the hardness of  $C^*$  is not based on the difficulty of finding exponent  $h$  but in the intractability to obtain transformations  $S, T$  for given polynomial equations  $\mathcal{P}, \mathcal{P}'$ . A more detailed discussion of  $C^*$  can be found in [MI88]. We want to point out that the basic  $C^*$  has been broken in [Pat95, FJ03]. However, its variation  $C^{*-}$  [Pat96a] is still unbroken and leads to a very efficient signature scheme.

#### 3.1.2 $C^{*-}$

We move on to a description of  $C^{*-}$  [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  $C^*$ . In terms of cryptanalysis, the new scheme has a strength of  $q^r$  (cf [Pat96a, CGP03]). In particular, the construction of  $C^{*-}$  has been used in the signature scheme Sflash<sup>v3</sup>. It uses the parameters  $q = 128, n = 67, r = 11$ . This leads to a private/public key size of 112.3/7.8kB. In [CGP03, 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.

### 3.2 Hidden Field Equations

The Hidden Field Equations (HFE) are a generalisation of the  $C^*$ -scheme. They have been proposed by Patarin [Pat96b]. The central map has the form

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

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  $d \in \mathbb{N}$ . As the degree of the polynomial  $P'$  is bounded by  $d$ , this allows efficient inversion of the equation  $P'(X') = Y'$  for given  $Y' \in \mathbb{E}$ , cf [Pat96b, Sect. 5] for an overview of possible algorithms for this problem. In any case, HFE is not a bijection but with 7 additional bits and with probability  $1 - 2^{-187}$ , we are able to find a pre-image for any given  $Y'$ , cf [Pat96b, CGP01] for details.

A Cryptanalysis of HFE can be found in [KS99, Cou01]. A signature scheme based on HFE called ‘‘Quartz’’ has been proposed in [CGP01] but broken in [FJ03]. A version of Quartz which is resistant against all known attacks is discussed in [WP04b, Sect. 4.3]. They use  $q = 2$ ,  $n = 107$  and remove  $r = 7$  equations (cf minus modification of  $C^*$ , Sect. 3.1.2). Using the values of [CGP01, Sect. 8], we obtain a public/private key size of 71/3kB, a signature verification time of less than 1 ms but a signature generation time of 10 s on a Pentium II 500 MHz.

### 3.3 Unbalanced Oil and Vinegar

Due to space limitations in this paper, we will only quote results for UOV and refer the reader to the corresponding papers for the construction of the central equations.

As  $C^{*-}$ , the Unbalanced Oil and Vinegar schemes (UOV) can only be used for signing [KPG99]. With the parameters from [KPG03], we have  $q = 16$ ,  $m = 16$ ,  $n = 32/48$  and a public key of 9/16kB (for  $n = 32/48$ ). The corresponding private key is 512/1152 Byte. Unfortunately, we are not aware of empirical measurements for the signing or verification time. However, based on the results given in [CGP03], we estimate for both a timing of less than 1 ms on a PC. Attacks against UOV can be found in [KPG03, CGMT02, BWP05].

### 3.4 Other Schemes

The schemes from this section have been proposed recently. They have nice characteristics in terms of speed and key size, but they are all rather new and hence, their security is not well understood yet. Therefore, we do not recommend them for current constructions. In addition, we point out broken proposals to give the reader a bibliography for the corresponding cryptanalysis.

The Tame Transformation Method (TTM) was proposed in [Moh99]. Practical versions of it have been broken in [GC00, DS04]. A signature scheme based on TTM has been proposed in [YC04]. Its security is an open problem but its authors claim that it is immune against all known attacks. According to [YC04], an earlier version of this scheme has been broken in [DY04]. RSE(2)PKC and its generalisation RSSE(2)PKC was proposed in [KS04b, KS04a]. This scheme has been further generalised to STS [WBP04] and this generalisation has been broken in the same paper.

### 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 can be smaller, *e.g.*, down to 512 byte in UOV. In terms of signature or message sizes, we can go down until 128 bits (Quartz). 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), 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. Unfortunately, most variations of  $\mathcal{MQ}$ -schemes are not suitable for encryption.

## 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. All proposals of this section have this security level. Due to space limitations of this paper, the tables of this section had to be removed. They can be found in [WP04a].

### 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.

Choosing  $q = 128$ ,  $n = 67$ , and  $r = 11$ , we obtain a private key size of 7.8 kByte, a public key size of 112.3 kByte, and a signature expansion of 237 bit. We expect both signature generation and verification to take less than 1 ms.

A more detailed explanation of this idea can be found in [WP04a].

### 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 [WP04b].

Using  $q = 2$ ,  $n = 107$ , and  $r = 7$ , we can use 20 bit to identify an individual user. This way, the corresponding private key needs 3264 byte and the public key has a size of 71 kByte. Using 40 bit to identify an individual user, the parameter  $n$  has to increase to 127 and we obtain 4509 byte for the private key and 119 kByte for the public key. In both cases, signature generation is below 20 seconds and the far more important signature verification time is in the range of 1 ms. In both proposals, we suggest to compute an 80-bit 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  $\cdot || \cdot$  the concatenation of bit-strings.

A more detailed explanation of this idea can be found in [WP04a].

### 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  $q = 128, n = 37$  (23 kByte for the  $\mathcal{MQ}$ -system) or  $q = 128, n = 67$  (134 kByte for the  $\mathcal{MQ}$ -system). In both cases, the evaluation is expected to take less than 1 ms.

A more detailed explanation of this idea — including a security evaluation — can be found in [WP04a].

## 5 Conclusions

In this paper, we gave a concise overview of an alternative class of public key schemes, called “Multivariate Quadratic” schemes. In particular — using the variations HFE- and  $C^{*--}$  — 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  $C^{*--}$ . Hence, they are also a good alternative for projects where patent royalties are a serious consideration. We also want to point out that the predecessor of Sflash<sup>v3</sup>, *i.e.*, Sflash<sup>v2</sup> has been recommended by NESSIE for special application domains. Similar, Quartz was a recommendation in NESSIE for applications which require particularly short signatures.

### Extended Version

An extended and updated version of this papers can be found at [WP04a].

### Acknowledgements

We want to thank Arjen Lenstra (Lucent, USA) for valuable comments on an earlier version of this manuscript which much helped to improve it. In addition, we want to thank Jintai Ding (University of Cincinnati, USA) for pointing out some missing references. Moreover, we want to thank Willi Meier (FH Aargau, Swiss) for pointing out a serious omission in Sect. 4.3. Finally, we want to thank An Braeken (COSIC, KU Leuven, Belgium) for helpful remarks.

This work was supported in part by the Concerted Research Action (GOA) GOA Mefisto 2000/06, GOA Ambiorix 2005/11 of the Flemish Government and the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT.

## 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*, 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.
- [CGP01] Nicolas Courtois, Louis Goubin, and Jacques Patarin. *Quartz: Primitive specification (second revised version)*, October 2001. <https://www.cosic.esat.kuleuven.ac.be/nessie/workshop/submissions/quar%tzv21-b.zip>, 18 pages.
- [CGP03] Nicolas Courtois, Louis Goubin, and Jacques Patarin. *SFlash<sup>v3</sup>, a fast asymmetric signature scheme — Revised Specification of SFlash, version 3.0*, October 17<sup>th</sup> 2003. ePrint Report 2003/211, <http://eprint.iacr.org/>, 14 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/hfesecc.pdf>.
- [DS04] Jintai Ding and Dieter Schmidt. The new implementation schemes of the TTM cryptosystem are not secure. In H. Niederreiter K. Feng and X. Xing, editors, *Coding, Cryptography and Combinatorics*, volume 23 of *Progress in Computer Science and Applied Logic*, pages 113–127. Birkhauser Verlag, Basel, 2004.
- [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.
- [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.
- [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.
- [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.

- [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](http://citeseer.231623.html), 2003-06-11.
- [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>.
- [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 at <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 *Advances in Cryptology — CRYPTO 1995*, volume 963 of *Lecture Notes in Computer Science*, pages 248–261. Don Coppersmith, editor, Springer, 1995.

- [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>.
- [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>.
- [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>.
- [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.
- [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>.
- [WFFP02] Christopher Wolf, Patrick Fitzpatrick, Simon N. Foley, and Emanuel Popovici. HFE in Java: Implementing Hidden Field Equations for Public Key Cryptography. In *Irish Signals and Systems Conference 2002*, pages 295–299. W. Marnane, G. Lightbody, and D. Pesch, editors, 2002.
- [Wol03] Christopher Wolf. Efficient Public Key Generation for Multivariate Cryptosystems. *Cryptology ePrint Archive*, Report 2003/089, 5<sup>th</sup> of May 2003. <http://eprint.iacr.org/2003/089/>, 12 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. Applications of Multivariate Quadratic Public Key Systems. *Cryptology ePrint Archive*, Report 2004/263, 2004. <http://eprint.iacr.org/2004/263/>.
- [WP04b] 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/>.
- [WP05] Christopher Wolf and Bart Preneel. Superfluous Keys in Multivariate Quadratic Asymmetric Systems. In *Public Key Cryptography — PKC 2005*, *Lecture Notes in Computer Science*. Serge Vaudenay, editor, Springer, 2005. 13 pages, to appear.
- [YC04] Bo-Yin Yang and Jiun-Ming Chen. Rank Attacks and Defence in Tame-Like Multivariate PKC's. *Cryptology ePrint Archive*, Report 2004/061, 29<sup>th</sup> September 2004. <http://eprint.iacr.org/>, 21 pages.