

# Äquivalente Schlüssel in Multivariate Quadratic Public Key Systemen — Aktueller Stand

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

## 1 Initial Considerations

In the last 20 years, several schemes based on the problem of Multivariate Quadratic equations (or  $\mathcal{MQ}$  for short) have been proposed. The most important ones certainly are MIA /  $C^*$  and Hidden Field Equations (HFE) plus their variations MIA- /  $C^{*-}$ , HFE-, HFEv, and HFEv-. Both classes have been used to construct signature schemes for the European cryptography project NESSIE, namely the MIA- variation in Sflash, the HFEv- variation in Quartz and the HFE- variation in the tweaked version Quartz-7m. Unbalanced Oil and Vinegar schemes and Stepwise Triangular Schemes are also important in practice. While the first is secure with the correct choice of parameters, the second forms the basis of nested constructions like the enhanced TTM, Tractable Rational Maps, or Rainbow. An overview of all these systems can be found in the taxonomy article [WPC].

In this talk, we give an overview on the question of equivalent keys of  $\mathcal{MQ}$ -schemes. At first glance, this question seems to be purely theoretical. But for practical applications, we need memory and time efficient instances of Multivariate Quadratic public key systems. One important point in this context is the overall *size* of the private key: in restricted environments such as smart cards, we want it as small as possible. Hence, if we can show that a given private key is only a representative of a much larger class of equivalent private keys, it makes sense to compute (and store) only a normal form of this key. Similar, we should construct new Multivariate Quadratic schemes such that they do not have a large number of equivalent private keys but only a small number, preferably only one per equivalence class. This way, we make optimal use of the randomness in the private key space and neither waste computation time nor storage space without any security benefit.

All systems based on  $\mathcal{MQ}$ -equations use a public key of the form

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

with  $n \in \mathbb{Z}^+$  variables and  $m \in \mathbb{Z}^+$  equations. Moreover, we have  $1 \leq i \leq m; 1 \leq j \leq k \leq n$  and  $\alpha_i, \beta_{i,j}, \gamma_{i,j,k} \in \mathbb{F}$  (constant, linear, and quadratic terms). We write the set of all such systems of polynomials as  $\mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$ . Moreover, the private key consists of the triple  $(S, \mathcal{P}', T)$  where  $S \in \text{Aff}^{-1}(\mathbb{F}^n), T \in \text{Aff}^{-1}(\mathbb{F}^m)$  are bijective affine transformations. Moreover, we have  $\mathcal{P}' \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$  is a polynomial-vector  $\mathcal{P}' := (p'_1, \dots, p'_m)$  with  $m$  components; each component is a polynomial in  $n$  variables  $x'_1, \dots, x'_n$ . Throughout this paper, we will denote components of this private vector  $\mathcal{P}'$  by a prime '. In contrast to the public polynomial vector  $\mathcal{P} \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$ , the private polynomial vector  $\mathcal{P}'$  does allow an efficient computation of  $x'_1, \dots, x'_n$  for given  $y'_1, \dots, y'_m$ . Still, the goal of  $\mathcal{MQ}$ -schemes is that this inversion should be hard if the public key  $\mathcal{P}$  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. An introduction to *Multivariate Quadratic* public key systems is given in [WPC].

This talk is based on the two conference papers [WPa,WPb], which deal with the classes MIA, HFE, and UOV. An extended version which also includes STS and shows that the reduction for MIA/MIA for  $q \neq 2$  is tight is [WPd].

## 2 Mathematical Considerations

Before discussing concrete schemes, we start with some general observations and definitions. Obviously, the most important term in this article is “equivalent private keys”. We give a graphical

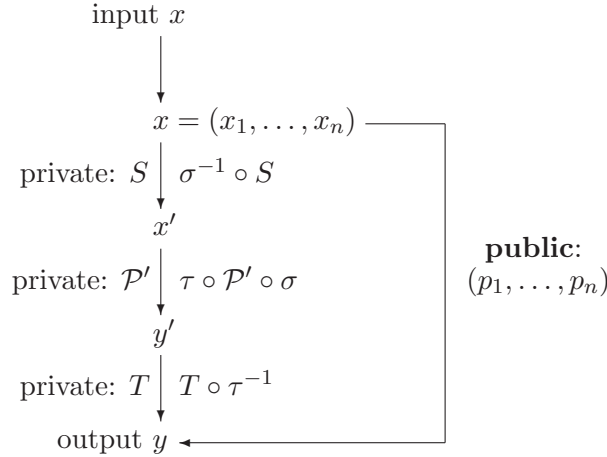


Figure 1: Equivalent private keys using affine transformations  $\sigma, \tau$

representation of this idea in Figure 1. We can also express this idea in the following definition:

DEFINITION 2.1 *We call two private keys*

$$(S, \mathcal{P}', T), (\tilde{S}, \tilde{\mathcal{P}}', \tilde{T}) \in \text{Aff}^{-1}(\mathbb{F}^n) \times \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m) \times \text{Aff}^{-1}(\mathbb{F}^m)$$

“equivalent” if they lead to the same public key, i.e., if we have

$$T \circ \mathcal{P}' \circ S = \mathcal{P} = \tilde{T} \circ \tilde{\mathcal{P}}' \circ \tilde{S}.$$

In the above definition,  $\text{Aff}^{-1}(\cdot)$  denotes the class of bijective affine transformations. In order to find equivalent keys, we consider the following transformations:

DEFINITION 2.2 *Let  $(S, \mathcal{P}', T) \in \text{Aff}^{-1}(\mathbb{F}^n) \times \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m) \times \text{Aff}^{-1}(\mathbb{F}^m)$ , and consider the four transformations  $\sigma, \sigma^{-1} \in \text{Aff}^{-1}(\mathbb{F}^n)$  and  $\tau, \tau^{-1} \in \text{Aff}^{-1}(\mathbb{F}^m)$ . Moreover, let*

$$\mathcal{P} = T \circ \tau^{-1} \circ \tau \circ \mathcal{P}' \circ \sigma \circ \sigma^{-1} \circ S. \quad (1)$$

*We call the pair  $(\sigma, \tau) \in \text{Aff}^{-1}(\mathbb{F}^n) \times \text{Aff}^{-1}(\mathbb{F}^m)$  “sustaining transformations” for an  $\mathcal{MQ}$ -system if the “shape” of  $\mathcal{P}'$  is invariant under the transformations  $\sigma$  and  $\tau$ . For short, we write  $(\sigma, \tau) \bullet (S, \mathcal{P}', T)$  for (2.2) and  $(\sigma, \tau)$  sustaining transformations. This idea has already been outlined in Figure 1.*

### 3 Sustaining Transformations

We have several sustainers which can be used with different multivariate quadratic public key systems.

**Additive Sustainer:** Add a constant  $A \in \mathbb{E}$  or  $a \in \mathbb{F}^n, b \in \mathbb{F}^m$ .

**Big Sustainer:** Multiply with a non-zero constant  $B \in \mathbb{E}^*$ .

**Small Sustainer:** Multiply with a diagonal matrix with non-zero coefficients  $b_1, \dots, b_n, b'_1, \dots, b'_m \in \mathbb{F}^*$ , respectively.

**Permutation Sustainer:** Permute the input variables / the equations.

**Gauss Sustainer:** Perform Gauss operations.

**Frobenius Sustainer:** Perform the operation  $X \rightarrow X^{q^i}$  for  $1 \leq i \leq n$  and  $i \in \mathbb{N}$ .

**Reduction Sustainer:** Observe that the last  $r$  rows have no effect with  $r \in \mathbb{N}$  being the number of equations missing.

These sustainers can now be combined with different multivariate quadratic public key systems. We summarise their effects in the next section.

### 4 Results

The sustainers outlined above can be applied to several basic classes, such as Hidden Field Equations (HFE), Matsumoto-Imai Scheme A (MIA), Unbalanced Oil and Vinegar schemes (UOV), and

Table 1: Summary of the reduction results of this article

Scheme	Reduction
UOV	$q^{n+mn} \prod_{i=0}^{n-m-1} (q^{n-m} - q^i) \prod_{i=0}^{m-1} (q^m - q^i)$
STS	$q^{m+n} \prod_{i=1}^L \left( q^{n_i(n-\sum_{j=1}^i n_j)} \prod_{j=0}^{n_i-1} (q^{n_i} - q^j) \right)$ $\prod_{i=1}^L \left( q^{m_i(n-\sum_{j=1}^i m_j)} \prod_{j=0}^{m_i-1} (q^{m_i} - q^j) \right)$
MIA	$n(q^n - 1)$
MIA-	$n(q^n - 1)q^r \prod_{i=n-r-1}^{n-1} (q^n - q^i)$
HFE	$nq^{2n}(q^n - 1)^2$
HFE-	$nq^{2n}(q^n - 1)(q^{n-r} - 1) \prod_{i=n-r-1}^{n-1} (q^n - q^i)$
HFEv	$n'q^{n+n'+vm}(q^{n'} - 1)^2 \prod_{i=0}^{v-1} (q^v - q^i)$
HFEv-	$n'q^{r+2n'+vn'}(q^{n'} - 1)^2 \prod_{i=0}^{v-1} (q^v - q^i) \prod_{i=n'-r-1}^{n'-1} (q^{n'} - q^i)$

Stepwise-Triangular Systems (STS). We have summarised our results in tables 1 and 2. The first gives an overview on the formulae achieved while the latter features some numerical examples. The

symbols used in Table 1 are defined as follows:  $n \in \mathbb{Z}^+$  denotes the number of variables,  $m \in \mathbb{Z}^+$  is the number of equations,  $q := |\mathbb{F}|$  is the number of elements in the ground field  $\mathbb{F}$ ,  $L$  the number of layers for STS, and  $n_l, m_l$  for  $1 \leq l \leq L$  the number of new variables and equations, respectively.

Table 2: Numerical examples for the reduction results of this article

Scheme	Parameters	Choices for $S, T$ (in $\log_2$ )	Reduction (in $\log_2$ )
UOV	$q = 2, m = 64, n = 192$	37,054	32,956
	$q = 2, m = 64, n = 256$	65,790	57,596
STS	$q = 2, r = 4, L = 25, n = 100$	20,096	11,315
	$q = 2, r = 5, L = 20, n = 100$	20,096	11,630
HFE	$q = 2, n = 80$	12,056	326
HFE-	$q = 2, r = 7, n = 107$	23,108	2129
HFE <sub>v</sub>	$q = 2, v = 7, n = 107$	21,652	1160
HFE <sub>v</sub> -	$q = 2, r = 3, v = 4, n = 107$	22,261	1258
MIA	$q = 128, n = 67$	63,784	469
MIA-	$q = 128, r = 11, n = 67$	63,784	6180

We see applications of our results in different contexts. First, they can be used for memory efficient implementations of the above schemes: instead of saving the whole private key, we can only save a normal form. Second, they apply to cryptanalysis as they allow to concentrate on special forms of the private key. Third, constructors of new schemes should keep these sustaining transformations in mind: there is no point in having a large private key space — if it can be reduced immediately by an attacker who can just apply some sustainers. Moreover, the results obtained in this talk shine new light on cryptanalytic results, in particular key recovery attacks: as each private key is only a representative of a larger class of equivalent private keys, each key recovery attack can only recover it up to these equivalences as the public key  $\mathcal{P}$  cannot contain information about individual private keys but the equivalence class used to construct  $\mathcal{P}$ .

## References

- [WPa] 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/>.
- [WPb] 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.
- [WPC] Christopher Wolf and Bart Preneel. Taxonomy of public key schemes based on the problem of multivariate quadratic equations. Cryptology ePrint Archive, Report 2005/077, 12<sup>th</sup> of May 2005. <http://eprint.iacr.org/2005/077/>, 64 pages.
- [WPD] Christopher Wolf and Bart Preneel. Equivalent Keys in Multivariate Quadratic Public Key Systems. Cryptology ePrint Archive, Report 2005/464, 22<sup>nd</sup> of December 2005. <http://eprint.iacr.org/2005/464/>, 19 pages.