Equivalent Keys in HFE, C*, and variations

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

Abstract

In this article, we investigate the question of equivalent keys for two $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic public key schemes HFE and C^{*--} and improve over a previously known result, to appear at PKC 2005. Moreover, we show a new non-trivial extension of these results to the classes HFE-, HFEv, HFEv-, and C^{*--}, which are cryptographically stronger variants of the original HFE and C* / MIA schemes. In particular, we are able to reduce the size of the private — and hence the public — key space by at least one order of magnitude. While the results are of independent interest themselves, we also see applications both in cryptanalysis and in memory efficient implementations.

Keywords: Multivariate Quadratic Equations, Public Key signature, Hidden Field Equations, HFE, HFE-, HFEv, HFEv-, C*, MIA, C^{*--}, MIA-

Cryptology ePrint Archive, Report 2004/360
http://eprint.iacr.org/

Current Version: 2005-08-09
First Revision: 2005-01-28
First Version: 2004-12-16

This is the extended version of the article with the same title [WP05a].
The original article has been published in Proceedings of Mycrypt 2005*, volume 3715 of* Lecture Notes in Computer Science*, pages 33–49. Serge Vaudenay, editor, Springer, 2005.*

1 Introduction

In the last 15 years, several schemes based on the problem of $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic equations have been proposed. The most important ones certainly are C* / MIA [MI88] and Hidden Field Equations (HFE, [Pat96b]) plus their variations C^{*--}, HFE-, HFEv, and HFEv- [KPG99, Pat96a, Pat96b]. Both have been used to construct signature schemes, namely C^{*--} in Sflash [CGP03], and HFEv- in Quartz [CGP01]. As for all systems based on $\mathcal{MQ}$-equations, the public key has the form

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

for $1 \le i \le m; 1 \le j \le k \le n$ 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 equations as $\mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$. Moreover, the private key consists of the triple $(S, \mathcal{P}', T)$ where $S \in \mathrm{Aff}^{-1}(\mathbb{F}^n), T \in \mathrm{Aff}^{-1}(\mathbb{F}^m)$ are affine transformations (cf Sect. 2.2) and $\mathcal{P}' \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$ is a polynomial-vector $\mathcal{P}' := (p'_1, \ldots, p'_m)$ with m components; each component is a polynomial in n variables $x'_1, \ldots, x'_n$. 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 $x'_1, \ldots, x'_n$ for given $y'_1, \ldots, y'_m$. Hence, 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.

In this paper, we investigate the question of equivalent keys for selected $\mathcal{MQ}$-schemes. Due to space limitations, we concentrate on HFE, HFE-, HFEv, HFEv-, C^*, and C^{*--}. As outlined above, they are quite important as they have been used in constructions submitted to the NESSIE project [NES]. However, we want to point out that the techniques outlined here are quite general and can also be applied to other schemes. The first paper on the topic of equivalent keys is [WP05b]. In this paper, we introduce the Frobenius sustainer and are hence able to improve over the results from [WP05b]. Moreover, this paper is the first to deal with variations of $\mathcal{MQ}$-schemes, cf [WP05c] for the terminology of $\mathcal{MQ}$-trapdoors. To this aim, we needed to develop the reduction sustainer, as we would not have been able to deal with the HFE- and the C^{*--} modification otherwise.

This paper is outlined as follows: after this general introduction, we move on to the necessary mathematical background in Sect. 2. This includes particularly a definition of the term *equivalent keys*. In Sect. 3, we concentrate on a subclass of affine transformations, denoted *sustaining transformations*, which can be used to generate equivalent keys. These transformations are applied to different variations of $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic equations in Sect. 4. This paper concludes with Sect. 5, cf [WP05b] for results on Unbalanced Oil and Vinegar schemes (UOV). A general overview of $\mathcal{MQ}$-schemes can be found in [WP05c].

2 Mathematical Background

In this section, we outline some observations useful in the remainder of this paper.

2.1 Basic Definitions

We start with a formal definition of the term "equivalent private keys":

DEFINITION 2.1 *We call two private keys*

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

"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 order to find equivalent keys, we consider the following transformations:

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

$$\mathcal{P} = T \circ \tau^{-1} \circ \tau \circ \mathcal{P}' \circ \sigma \circ \sigma^{-1} \circ S \tag{1}$$

We call the pair $(\sigma, \tau) \in \mathit{Aff}^{-1}(\mathbb{F}^n) \times \mathit{Aff}^{-1}(\mathbb{F}^m)$ *"sustaining transformations" for an* $\mathcal{MQ}$*-system if the "shape" of* $\mathcal{P}'$ *is invariant under the transformations* σ *and* τ*. For short, we write* $(\sigma, \tau) \bullet (S, \mathcal{P}', T)$ *for (1) and* (σ, τ) *sustaining transformations.*

Remark. In the above definition, the meaning of "shape" is still open. In fact, its meaning has to be defined for each $\mathcal{MQ}$-system individually. For example, in HFE, it is the bounding degree $d \in \mathbb{N}$ of the polynomial $P'(X')$. In the case of C^* / MIA, the "shape" is the fact that we have a single monomial with factor 1 as the central equation. However, for σ, τ sustaining transformations, we are now able to produce equivalent keys for a given private key by $(\sigma, \tau) \bullet (S, \mathcal{P}', T)$. A trivial example of sustaining transformations is the identity transformation, *i.e.*, to set $\sigma = \tau = \mathit{id}$.

Lemma 2.3 *Let (σ, τ) be sustaining transformation. If $G := (\sigma, \circ)$ and $H := (\tau, \circ)$ form a subgroup of the affine transformations, they produce equivalence relations within the private key space.*

Proof. We start with a proof of this statement for $G := (\sigma, \circ)$. First, we have reflexivity as the identity transformation is contained in G. Second, we have symmetry as subgroups are closed under inversion. Third, we also have transitivity as subgroups are closed under composition. Therefore, the group G partitions the private key space into equivalence classes. The proof for $H := (\tau, \circ)$ is analogous. □

Remark. We want to point out that the above proof does not use special properties of sustaining transformations, but the fact that these are a subgroup of the group of affine transformations. Hence, the proof does not depend on the term "shape" and is therefore valid even if the latter is not rigorously defined yet. In any case, instead of proving that sustaining transformations form a subgroup of the affine transformations, we can also consider normal forms of private keys. As we see below, normal forms have some advantages to avoid double counts in the private key space.

After these initial observations over equivalent keys, we concentrate on bijections between ground fields and their extension fields as both HFE and C* / MIA use an extension field to define their central equations $\mathcal{P}'$. Let $\mathbb{F}$ be a finite field with $q := |\mathbb{F}|$ elements. Using a polynomial $i(t) \in \mathbb{F}[t]$, irreducible over $\mathbb{F}$, we generate an extension field $\mathbb{E} := \mathbb{F}[t]/i(t)$ of dimension n. This means we view elements of $\mathbb{E}$ as polynomials in t of degree less than n. Addition and multiplication are defined as for polynomials modulo $i(t)$. In addition, we can view elements from $\mathbb{E}$ as vectors over the vector-space $\mathbb{F}^n$. We will therefore view elements $a \in \mathbb{E}$ and $b \in \mathbb{F}^n$ as

$$a := \alpha_{n-1}t^{n-1} + \ldots + \alpha_1 t + \alpha_0 \text{ and } b := (\beta_1, \ldots, \beta_n)\,,$$

for $\alpha_{i-1}, \beta_i \in \mathbb{F}$ with $1 \leq i \leq n$. Moreover, we define the *canonical bijection* between $\mathbb{E}$ and $\mathbb{F}^n$ by identifying the coefficients $\alpha_{i-1} \leftrightarrow \beta_i$. We use both this bijection $\phi : \mathbb{E} \to \mathbb{F}^n$ and its inverse $\phi^{-1} : \mathbb{F}^n \to \mathbb{E}$.

2.2 Affine Transformations

In the context of affine transformations, the following lemma proves useful:

Lemma 2.4 *Let $\mathbb{F}$ be a finite field with $q := |\mathbb{F}|$ elements. Then we have $\prod_{i=0}^{n-1} q^n - q^i$ invertible $(n \times n)$-matrices over $\mathbb{F}$.*

Next, we recall some basic properties of affine transformations over the finite fields $\mathbb{F}$ and $\mathbb{E}$.

Definition 2.5 *Let $M_S \in \mathbb{F}^{n\times n}$ be an invertible $(n \times n)$ matrix and $v_s \in \mathbb{F}^n$ a vector and let $S(x) := M_S x + v_s$. We call this the "matrix representation" of the affine transformation S.*

Definition 2.6 *Moreover, let $s_1, \ldots, s_n$ be n polynomials of degree 1 at most over $\mathbb{F}$, i.e., $s_i(x_1, \ldots, x_n) := \beta_{i,1}x_1 + \ldots + \beta_{i,n}x_n + \alpha_i$ with $1 \leq i, j \leq n$ and $\alpha_i, \beta_{i,j} \in \mathbb{F}$. Let $S(x) := (s_1(x), \ldots, s_n(x))$ for $x := (x_1, \ldots, x_n)$ as a vector over $\mathbb{F}^n$. We call this the "multivariate representation" of the affine transformation S.*

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

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

DEFINITION 2.7 *Let $0 \le i < n$ and $A, B_i \in \mathbb{E}$. Moreover, let the polynomial $S(X) := \sum_{i=0}^{n-1} B_i X^{q^i} + A$ be an affine transformation. We call this the "univariate representation" of the affine transformation $S(X)$.*

Lemma 2.8 *An affine transformation in univariate representation can be transfered efficiently in multivariate representation and vice versa.*

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

3 Sustaining Transformations

In this section, we discuss several examples for sustaining transformations. In addition, we will consider their effect on the central transformation $\mathcal{P}'$. The authors are not convinced that the transformations stated here are the only ones possible but encourage the search for other and maybe more powerful sustaining transformations.

3.1 Additive Sustainer

For $n = m$, let $\sigma(X) := (X + A)$ and $\tau(X) := (X + A')$ for some elements $A, A' \in \mathbb{E}$. Moreover, as long as they keep the shape of the central equations $\mathcal{P}'$ invariant, they form sustaining transformations.

In particular, we are able to change the constant parts $v_s, v_t \in \mathbb{F}^n$ or $V_S, V_T \in \mathbb{E}$ of the two affine transformations $S, T \in \mathrm{Aff}^{-1}(\mathbb{F}^n)$ to zero, *i.e.*, to obtain a new key $(\hat{S}, \hat{\mathcal{P}}', \hat{T})$ with $\hat{S}, \hat{T} \in \mathrm{Hom}^{-1}(\mathbb{F}^n)$.
Remark. This is a very useful result for cryptanalysis as it allows us to "collect" the constant terms in the central equations $\mathcal{P}'$. For cryptanalytic purposes, we therefore need only to consider the case of linear transformations $S, T \in \mathrm{Hom}^{-1}(\mathbb{F}^n)$.

The additive sustainer also works if we interpret it over the vector space $\mathbb{F}^n$ rather than the extension field $\mathbb{E}$. In particular, we can also handle the case $n \neq m$ now. However, in this case it may happen that we have $a' \in \mathbb{F}^m$ and consequently $\tau : \mathbb{F}^m \to \mathbb{F}^m$. Nevertheless, we can still collect all constant terms in the central equations $\mathcal{P}'$.

If we look at the central equations as multivariate polynomials, the additive sustainer will affect the constants α_i and $\beta_{i,j} \in \mathbb{F}$ for $1 \le i \le m$ and $1 \le j \le n$. A similar observation is true for central equations over the extension field $\mathbb{E}$: in this case, the additive sustainer affects the additive constant $A \in \mathbb{E}$ and the linear factors $B_i \in \mathbb{E}$ for $0 \le i < n$.

3.2 Big Sustainer

We now consider multiplication in the (big) extension field $\mathbb{E}$, *i.e.*, we have $\sigma(X) := (BX)$ and $\tau(X) := (B'X)$ for $B, B' \in \mathbb{E}^*$. Again, we obtain a sustaining transformation if this operation does not modify the shape of the central equations as $(BX), (B'X) \in \mathrm{Aff}^{-1}(\mathbb{F}^n)$.

The big sustainer is useful if we consider schemes defined over extension fields as it does not affect the overall degree of the central equations over this extension field.

3.3 Small Sustainer

We now consider multiplications over the (small) ground field $\mathbb{F}$, *i.e.*, we have $\sigma(x) := Diag(b_1, \ldots, b_n)x$ and $\tau(x) := Diag(b'_1, \ldots, b'_m)x$ for the coefficients $b_1, \ldots, b_n, b'_1, \ldots, b'_m \in \mathbb{F}^*$ and $Diag(b)$ the diagonal matrix on a vector $b \in \mathbb{F}^n$ and $b' \in \mathbb{F}^m$, respectively.

In contrast to the big sustainer, the small sustainer is useful if we consider schemes which define the central equations over the ground field $\mathbb{F}$ as it only introduces a scalar factor in the polynomials $(p'_1, \dots, p'_m)$.

3.4 Permutation Sustainer

For the transformation σ, this sustainer permutes input-variables of the central equations while for the transformation τ, it permutes the polynomials of the central equations themselves. As each permutation has a corresponding, invertible permutation-matrix, both $\sigma \in S_n$ and $\tau \in S_m$ are also affine transformations. The effect of the central equations is limited to a permutation of these equations and their input variables, respectively.

3.5 Gauss Sustainer

Here, we consider Gauss operations on matrices, *i.e.*, row and column permutations, multiplication of rows and columns by scalars from the ground field $\mathbb{F}$, and the addition of two rows/columns. As all these operations can be performed by invertible matrices; they form a subgroup of the affine transformations and are hence a candidate for a sustaining transformation.

The effect of the Gauss Sustainer is similar to the permutation sustainer and the small sustainer. In addition, it allows the addition of multivariate quadratic polynomials. This will not affect the shape of some $\mathcal{MQ}$-schemes.

The sustainers given so far have been already outlined in [WP05b]. To the knowledge of the authors, the following sustainers are new and to the knowledge to the authors have not been considered previously in the literature.

3.6 Frobenius Sustainer

Definition 3.1 *Let $\mathbb{F}$ be a finite field with $q := |\mathbb{F}|$ elements and $\mathbb{E}$ its n-dimensional extension. Moreover, let $H := \{i \in \mathbb{Z} : 0 \le i < n\}$. For $a, b \in H$ we call $\sigma(X) := X^{q^a}$ and $\tau(X) := X^{q^b}$* Frobenius transformations.

Obviously, Frobenius transformations are linear transformations with respect to $\mathbb{F}$. The following lemma establishes that they also form a group:

Lemma 3.2 *Frobenius transformations are a subgroup in $Hom^{-1}(\mathbb{F}^n)$.*

Proof. First, Frobenius transformations are linear transformations, so associativity is inherited from them. Second, the set H from Def. 3.1 is not empty for any given $\mathbb{F}$ and $n \in \mathbb{N}$. Hence, the corresponding set of Frobenius transformations is not empty either. So all left to show is that for any given Frobenius transformations σ, τ, the composition $\sigma \circ \tau^{-1}$ is also a Frobenius transformation.

Let $\sigma(X) := X^{q^a}$ and $\tau(X) := X^{q^b}$ for some $a, b \in H$. Working in the multiplicative group $\mathbb{E}^*$ we observe that we need $q^b \cdot B' \equiv 1 \pmod{q^n - 1}$ for B' to obtain the inverse function of τ. We notice that $B' := q^{b'}$ for $b' := n - b \pmod{n}$ yields the required and moreover $\tau^{-1} := X^{q^{b'}}$ is a Frobenius transformation as $b' \in H$.

So we can write $\sigma(X) \circ \tau^{-1}(X) = X^{q^{a+b'}}$. If $a + b' < n$ we are done. Otherwise $n \le a + b' < 2n$, so we can write $q^{a+b'} = q^{n+s}$ for some $s \in H$. Again, working in the multiplicative group E^* yields $q^{n+s} \equiv q^s \pmod{q^n - 1}$ and hence, we established that $\sigma \circ \tau^{-1}$ is also a Frobenius transformation. This completes the proof that all Frobenius transformations form a group. $\square$

Frobenius transformations usually change the degree of the central equation $\mathcal{P}'$. But taking $\tau := \sigma^{-1}$ cancels this effect and hence preserves the degree of $\mathcal{P}'$. Therefore, we can speak of a Frobenius sustainer (σ, τ). So there are n Frobenius sustainers for a given extension field $\mathbb{E}$.

It is tempting to extend this result to the case of powers of the characteristic of $\mathbb{F}$. However, this is not possible as $x^{\text{char}\mathbb{F}}$ is not a linear transformation in $\mathbb{F}$ for $q \neq p$.

Remark. We want to point out that all six sustainers presented so far form groups and hence partition the private key space into equivalence classes (cf Lemma 2.3).

3.7 Reduction Sustainer

Reduction sustainers are quite different from the transformations studied so far, because they are applied with a different construction of the trapdoor of $\mathcal{P}$. In this new construction, we define the public key equations as $\mathcal{P} := R \circ T \circ \mathcal{P}' \circ S$ where $R : \mathbb{F}^n \to \mathbb{F}^{n-r}$ denotes a *reduction* or *projection*. In addition, we have $S, T \in \text{Aff}^{-1}(\mathbb{F}^n)$ and $\mathcal{P}' \in \mathcal{MQ}(\mathbb{F}^n)$. Less loosely speaking, we consider the function $R(x_1, \ldots, x_n) := (x_1, \ldots, x_{n-r})$, *i.e.*, we neglect the last r components of the vector $(x_1, \ldots, x_n)$. Although this modification looks rather easy, it proves powerful to defeat a wide class of cryptographic attacks against several $\mathcal{MQ}$-schemes, including HFE and C* / MIA, *e.g.*, the attack introduced in [FJ03].

For the corresponding sustainer, we consider the affine transformation T in matrix representation, *i.e.*, we have $T(x) := Mx + v$ for some invertible matrix $M \in \mathbb{F}^{m \times m}$ and a vector $v \in \mathbb{F}^m$. We observe that any change in the last r columns of M or v does not affect the result of R (and hence $\mathcal{P}$). Hence, we can choose these last r columns without affecting the public key. Inspecting Lemma 2.4, we see that this gives us a total of

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

choices for v and M, respectively, that do not affect the public key equations $\mathcal{P}$.

When applying the reduction sustainer together with other sustainers, we have to make sure that we do not count the same transformation twice, cf the corresponding proofs.

4 Application to $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic Schemes

In this section, we show how to apply the sustainers from the previous section to several $\mathcal{MQ}$-schemes. Due to space limitations in this paper, we will only outline some central properties of each scheme and sketch the corresponding proofs. We want to stress that the reductions in size we achieve represent only lower, no upper bounds: additional sustaining transformations can reduce the key space of these schemes further.

4.1 Hidden Field Equations

The Hidden Field Equations (HFE) have been proposed by Patarin [Pat96b].

Definition 4.1 *Let $\mathbb{E}$ be a finite field and $P(X)$ a polynomial over $\mathbb{E}$. For*

$$P(X) := \sum_{\substack{0 \le i,j \le d \\ q^i + q^j \le d}} C_{i,j} X^{q^i + q^j} + \sum_{\substack{0 \le k \le d \\ q^k \le d}} B_k X^{q^k} + A$$

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

and a degree $d \in \mathbb{N}$, we say the central equations $\mathcal{P}'$ are in HFE-shape.

Due to the special form of $P(X)$, we can express it as a $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic equation $\mathcal{P}'$ over $\mathbb{F}$, cf [Pat96b]. Moreover, as the degree of the polynomial P is bounded by d, this allows efficient inversion of the equation $P(X) = Y$ for given $Y \in \mathbb{E}$. So the *shape* of HFE is in particular this degree d of the private polynomial P. Moreover, we observe that there are no restrictions on its coefficients $C_{i,j}, B_k, A \in \mathbb{E}$ for $i, j, k \in \mathbb{N}$ and $q^i, q^i + q^j \leq d$. Hence, we can apply both the additive and the big sustainer (cf sect. 3.1 and 3.2) without changing the shape of this central equation.

Theorem 4.2 *For $K := (S, P, T) \in Aff^{-1}(\mathbb{F}^n) \times \mathbb{E}[X] \times Aff^{-1}(\mathbb{F}^n)$ a private key in HFE, we have*

$$n.q^{2n}(q^n - 1)^2$$

equivalent keys.

Proof. To prove this lemma, we consider normal forms of private keys: let $\tilde{S} \in \mathrm{Aff}^{-1}(\mathbb{F}^n)$ being the affine transformation we start with. First we compute $\hat{S}(X) := \tilde{S}(X) - \tilde{S}(0)$, *i.e.*, we apply the additive sustainer. Obviously, we have $\hat{S}(0) = 0$ after this transformation and hence a special fix-point. Second we define $\overline{S}(X) := \hat{S}(X).\hat{S}(1)^{-1}$, *i.e.*, we apply the big sustainer. As the transformation $\hat{S} : \mathbb{E} \to \mathbb{E}$ is a bijection and we have $\hat{S}(0) = 0$, we know that $\hat{S}(1)$ must be non-zero. Hence, we have $\overline{S}(1) = 1$, *i.e.*, we add a new fix-point but still keep the old fix-point as we have $\overline{S}(0) = \hat{S}(0) = 0$. Similar we can compute an affine transformation $\overline{T}(X)$ with $\overline{T}(0) = 0$ and $\overline{T}(1) = 1$ as a normal form of the affine transformation $\tilde{T} \in \mathrm{Aff}^{-1}(\mathbb{F}^n)$. Note that both the additive sustainer and the big sustainer keep the degree of the central polynomial $P(X)$ so we can apply both sustainers on both sides without changing the "shape" of $P(X)$.

Applying the Frobenius sustainer is a little more technical. First we observe that this sustainer keeps the fix-points $\overline{S}(0) = \overline{T}(0) = 0$ and $\overline{S}(1) = \overline{T}(1) = 1$ so we are sure we still deal with equivalence classes, *i.e.*, each given private key has a unique normal form, even with the Frobenius sustainer applied. Now we pick an element $C \in \mathbb{E}\backslash\{0, 1\}$ with $g := \overline{S}(C)$ is a generator of $\mathbb{E}^*$, *i.e.*, we have $\mathbb{E}^* = \{g^i \mid 0 \leq i < q^n\}$. As $\mathbb{E}$ is a finite field we know that such a generator g exists. Given that $\overline{S}$ is injective we know that we can find the corresponding $C \in \mathbb{E}\backslash\{0, 1\}$. Now we compute $g_i := \overline{S}(C)^{q^i}$ for $0 \leq i < n$. Using any total ordering "<", we obtain $g_c := \min\{g_0, \ldots, g_{n-1}\}$ for some $c \in \mathbb{N}$ as the smallest element of this set. One example of such a total ordering would be to use a bijection between the sets $\mathbb{E} \leftrightarrow \{0, \ldots, q^n - 1\}$ and then exploiting the ordering of the natural numbers to derive an ordering on the elements of the extension field $\mathbb{E}$. Finally, we define $S(X) := [\overline{S}(X)]^{q^c}$ as new affine transformation. To cancel the effect of the Frobenius sustainer, we moreover define $T(X) := [\overline{T}(X)]^{q^{n-c}}$.

Hence, we have now computed a unique normal form for a given private key. Moreover, we can "reverse" these computations and derive an equivalence class of size $n.q^{2n}.(q^n - 1)^2$ this way as we have

$$(BX^{q^c} + A, B'X^{q^{n-c}} + A') \bullet (S, \mathcal{P}', T) \text{ for } B, B' \in \mathbb{E}^*, A, A' \in \mathbb{E} \text{ and } 0 \leq c < n\,.$$

□

Remark. To the knowledge of the author, the additive sustainer for HFE has first been reported in [Tol03] and used there for reducing the affine transformations to linear ones. In addition, a weaker version of the above theorem can be found in [WP05b].

For $q = 2$ and $n = 80$, the number of equivalent keys per private key is $\approx 2^{326}$. In comparison, the number of choices for S and T is $\approx 2^{12,056}$. This special choice of parameters has been used in HFE Challenge 1 [Pat96b].

4.1.1 HFE-

We recall that HFE- is the original HFE-class with the minus modification (cf Section 3.7). In particular, this means that the "shape" of the central polynomial $P'(X')$ is still the same, *i.e.*, all considerations from the previous theorem also apply to HFE-.

Theorem 4.3 *For $K := (S, P, T) \in \mathit{Aff}^{-1}(\mathbb{F}^n) \times \mathbb{E}[X] \times \mathit{Aff}^{-1}(\mathbb{F}^n)$ a private key in HFE and a reduction parameter $r \in \mathbb{N}$ we have*

$$n.q^{2n}(q^n - 1)(q^{n-r} - 1) \prod_{i=n-r-1}^{n-1} (q^n - q^i)$$

equivalent keys. Hence, the key-space of HFE- can be reduced by this number.

Proof. This proof uses the same ideas as the proof of Theorem. 4.2 to obtain a normal form of the affine transformation S, *i.e.*, applying the additive sustainer, the big sustainer and the Frobenius sustainer on this side. Hence, we have a reduction by $n.q^n(q^n - 1)$ keys here.

For the affine transformation T, we also have to take the reduction sustainer into account: we use $\tilde{T}(X) : \mathbb{F}^n \to \mathbb{F}^{n-r}$ and fix $\tilde{T}(0) = 0$ by applying the additive sustainer and $\tilde{T}(1) = 1$ by applying the big sustainer, which gives us q^{n-r} and $q^{n-r} - 1$ choices, respectively. To avoid double counting with the reduction sustainer, all computations were performed in $\tilde{\mathbb{E}} := \mathrm{GF}(q^{n-r})$ rather than $\mathbb{E}$. Again, we are able to compute a normal form for a given private key and reverse these computations to obtain the full equivalence class for any given private key in normal form. Moreover, we observe that the resulting transformation $\tilde{T}$ actually allows for $q^r \prod_{i=n-r-1}^{n-1}(q^n - q^i)$ possible choices for the original transformation $T : \mathbb{F}^n \to \mathbb{F}^n$ without affecting the output of $\tilde{T}$ and hence, keeping the two fix points $\tilde{T}(0) = 0$ and $\tilde{T}(1) = 1$. Therefore, there are a total of $q^{n-r}.q^r.(q^{n-r} - 1). \prod_{i=n-r-1}^{n-1}(q^n - q^i)$ possibilities for the transformation T without changing the public key equations. Multiplying out the intermediate results for S and T yields the theorem. □

For $q = 2, r = 7$ and $n = 107$, the number of equivalent keys for each private key is $\approx 2^{2129}$. In comparison, the number of choices for S and T is $\approx 2^{23,108}$. This special choice of parameters has been used in the repaired version Quartz-7m of Quartz [CGP01, WP04].

4.1.2 HFEv

The following modification, due to [KPG99], uses a different form for the central equations $\mathcal{P}'$.

Definition 4.4 *Let $\mathbb{E}$ be a finite field with degree n' over $\mathbb{F}$, the number of vinegar variables $v \in \mathbb{N}$, and $P(X)$ a polynomial over $\mathbb{E}$. Moreover, let $(z_1, \ldots, z_v) := s_{n-v+1}(x_1, \ldots, x_n), \ldots, s_n(x_1, \ldots, x_n)$ for s_i the polynomials of $S(x)$ in multivariate representation and $X' := \phi^{-1}(x'_1, \ldots, x'_{n'})$, using the canonical bijection $\phi^{-1} : \mathbb{F}^n \to \mathbb{E}$ and $x'_i := s_i(x_1, \ldots, x_n)$ for $1 \le i \le n'$ as hidden variables. Then define the central equation as*

$$\begin{aligned} P'_{z_1,\ldots,z_v}(X') &:= \sum_{\substack{0 \le i,j \le d \\ q^i + q^j \le d}} C_{i,j} X'^{q^i + q^j} + \sum_{\substack{0 \le k \le d \\ q^k \le d}} B_k(z_1, \ldots, z_v) X'^{q^k} \\ &\quad + A(z_1, \ldots, z_v) \\ &\quad \text{where} \begin{cases} C_{i,j} X'^{q^i + q^j} & \text{for } C_{i,j} \in \mathbb{E} \text{ are the quadratic terms,} \\ B_k(z_1, \ldots, z_v) X'^{q^k} & \text{for } B_k(z_1, \ldots, z_v) \text{ depending linearly on } z_1, \ldots, z_v \text{ and} \\ A(z_1, \ldots, z_v) & \text{for } A(z_1, \ldots, z_v) \text{ depending quadratically on } z_1, \ldots, z_v \end{cases} \end{aligned}$$

and a degree $d \in \mathbb{N}$, we say the central equations $\mathcal{P}'$ are in HFEv-shape.

The condition that the $B_k(z_1, \ldots, z_v)$ are affine functions (*i.e.*, of degree 1 in the z_i at most) and $A(z_1, \ldots, z_v)$ is a quadratic function over $\mathbb{F}$ ensures that the public key is still quadratic over $\mathbb{F}$.

Theorem 4.5 *For $K := (S, P, T) \in Aff^{-1}(\mathbb{F}^n) \times \mathbb{E}[X] \times Aff^{-1}(\mathbb{F}^m)$ a private key in HFEv, $v \in \mathbb{N}$ the number of vinegar variables, $\mathbb{E}$ an n'-dimensional extension of $\mathbb{F}$ where $n' := n - v = m$ we have*

$$n' q^{n+n'+vm}(q^{n'} - 1)^2 \prod_{i=0}^{v-1}(q^v - q^i)$$

equivalent keys. Hence, the key-space of HFEv can be reduced by this number.

Proof. In contrast to HFE-, the difficulty now lies in the computation of a normal form for the affine transformation S rather than the affine transformation T. For the latter, we can still apply the big sustainer and the additive sustainer and obtain a total of $q^m.(q^m - 1) = q^{n'}.(q^{n'} - 1)$ equivalent keys for a given transformation T. Moreover, the HFEv modification does not change the "absorbing behaviour" of the central polynomial P and hence, the proof from Theorem. 4.2 is still applicable.

Instead, we have to concentrate on the affine transformation S here. To simplify the following argument, we apply the additive sustainer on S and obtain a linear transformation. This reduces the key-space by q^n. To make sure that we do not count the same linear transformation twice, we consider a normal form for the now (linear) transformation S

$$\begin{pmatrix} E_m & F_v^m \\ 0 & I_v \end{pmatrix} \text{ with } E_m \in \mathbb{F}^{m \times m}, F_v^m \in \mathbb{F}^{m \times v}$$

In the above definition, we also have I_v the identity matrix in $\mathbb{F}^{v \times v}$. Moreover, the left-lower corner is the all-zero matrix in $\mathbb{F}^{v \times m}$. The reason for this non-symmetry: we may not introduce vinegar variables in the set of oil variables, but due to the form of the vinegar equations, we can introduce oil variables in the set of vinegar variables. This is done by the following matrix. In particular, for each invertible matrix M_S, we have a unique matrix

$$\begin{pmatrix} I_m & 0 \\ G_m^v & H_v \end{pmatrix} \text{ with an invertible matrix } H_v \in \mathbb{F}^{v \times v}.$$

which transfers M_S to the normal form from above. Again, I_m is an identity matrix in $\mathbb{F}^{m \times m}$. Moreover, we have some matrix $G_m^v \in \mathbb{F}^{v \times m}$. This way, we obtain $q^{vm} \prod_{i=0}^{v-1}(q^v - q^i)$ equivalent keys in the "v" modification alone. As said previously, the identity matrix I_m ensures that the input of the HFE component is unaltered. However, we do not have such a restriction on the input of the vinegar part and can hence introduce the two matrices G_m^v and H_v: they are "absorbed" into the random terms of the vinegar polynomials $B_k(z_1, \ldots, z_v)$ and $A(z_1, \ldots, z_v)$.

For the HFE component over $\mathbb{E}$, we can now apply the big sustainer to S and obtain a factor of $(q^{n'} - 1)$. In addition, we apply the Frobenius sustainer to the HFE component, which yields an additional factor of n'. Note that the Frobenius sustainer can be applied both to S and T, and hence, we can make sure that it cancels out and does not affect the degree of the central polynomial $P_{z_1,\ldots,z_v}(X)$. Again, we can reverse all computations and therefore, obtain equivalence classes of equal size for each given private key in normal form. □

For the case $q = 2, v = 7$ and $n = 107$, the number of equivalent keys for each private is $\approx 2^{1160}$. In comparison, the number of choices for S and T is $\approx 2^{21,652}$.

4.1.3 HFEv-

Here, we combine both the HFEv and the HFE- modification to obtain HFEv-. In fact, the original Quartz scheme was of this type.

Theorem 4.6 *For $K := (S, P, T) \in \mathit{Aff}^{-1}(\mathbb{F}^n) \times \mathbb{E}[X] \times \mathit{Aff}^{-1}(\mathbb{F}^{m+v}, \mathbb{F}^{m+r})$ a private key in HFEv, $v \in \mathbb{N}$ vinegar variables, a reduction parameter $r \in \mathbb{N}$ and $\mathbb{E}$ an n'-dimensional extension of $\mathbb{F}$ where $n' := n - v$ and $n' = m + r$ we have*

$$n' q^{r+2n'+vn'} (q^{n'} - 1)^2 \prod_{i=0}^{v-1} (q^v - q^i) \prod_{i=n'-r-1}^{n'-1} (q^{n'} - q^i)$$

equivalent keys. Hence, the key-space of HFEv can be reduced by this number.

Proof. This proof is a combination of the two cases HFEv and HFE-. Given that the difficulty for the HFE- modification was in the T-transformation while the difficulty of HFEv was in the S-transformation, we can safely combine the known sustainers without any double-counting. □

For the case $q = 2, r = 3, v = 4$ and $n = 107, n' := 103$, the number of redundant keys is $\approx 2^{1258}$. In comparison, the number of choices for S and T is $\approx 2^{22,261}$. This special choice of parameters has been used in the original version of Quartz [CGP01], as submitted to NESSIE [NES].

4.2 Matsumoto-Imai Scheme A

Definition 4.7 *Let $\mathbb{E}$ be an extension field of dimension n over the finite field $\mathbb{F}$ and $\lambda \in \mathbb{N}$ an integer with $\gcd(q^n - 1, q^\lambda + 1) = 1$. We then say that the following central equation is of MIA-shape:*

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

The restriction $\gcd(q^n - 1, q^\lambda + 1) = 1$ is necessary first to obtain a permutation polynomial and second to allow efficient inversion of $P'(X')$. In this setting, we cannot apply the additive sustainer, as this monomial does not allow any linear or constant terms. Moreover, the monomial requires a factor of one. Hence, we have to preserve this property. At present, the only sustainers suitable seem to be the big sustainer (cf Sect. 3.2) and the Frobenius sustainer (cf Sect. 3.6). We use both in the following

Remark. In the paper [MI88], MIA was introduced under the name C^*. Moreover, it used the branching modifier [WP05c, 4.4] by default. As branching has been attacked very successfully, C^* has been used without this modification for any later construction, *e.g.*, [CGP00b, CGP02, CGP00a, CGP03]. 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".

Theorem 4.8 *For $K := (S, P, T) \in \mathit{Aff}^{-1}(\mathbb{F}^n) \times \mathbb{E}[X] \times \mathit{Aff}^{-1}(\mathbb{F}^n)$ a private key in MIA we have*

$$n(q^n - 1)$$

equivalent keys. Hence, the key-space of MIA can be reduced by this number.

Proof. To prove this statement, we consider normal forms of keys in MIA. In particular, we concentrate on a normal form of the affine transformation S where S is in univariate representation. As for HFE and w.l.o.g., let $B := S(1)$ be a non-zero coefficient on position 1. Unlike HFE we cannot enforce that $S(0) = 0$, so we may have $S(1) = 0$. However, in this case set $B := S(0)$. Applying $\sigma^{-1}(X) := B^{-1}X$ will ensure a normal form for S. In order to "repair" the monomial $P(X)$, we have to apply an inverse transformation to T. So let $\tau(X) := (B^{q^\lambda+1})^{-1}X$. This way we obtain

$$\begin{aligned}\mathcal{P} &= T \circ \tau^{-1} \circ \tau \circ P \circ \sigma \circ \sigma^{-1} \circ S \\ &= \tilde{T} \circ (B^{(q^\lambda+1).(-1)}.B^{q^\lambda+1}.X^{q^\lambda+1}) \circ \tilde{S} \\ &= \tilde{T} \circ P \circ \tilde{S}\,,\end{aligned}$$

where $\tilde{S}$ is in normal form. In contrast to HFE (cf Theorem. 4.2), we cannot chose the transformations σ and τ independently: each choice of σ implies a particular τ and vice versa. However, the fix point 1 is still preserved by the Frobenius sustainer and so we can apply this sustainer on the transformation S. As for HFE, we compute a normal form for a given generator and a total ordering of $\mathbb{E}$; again, we "repair" the monomial $X^{q^\lambda+1}$ by applying an inverse Frobenius sustainer to T and hence have

$$(BX^{q^c}, B^{-q^\lambda-1}X^{q^{n-c}}) \bullet (S, P, T) \text{ where } B \in \mathbb{E}^* \text{ and } 0 \leq c < n \text{ for } c \in \mathbb{N}$$

which leads to a total of $n(q^n - 1)$ equivalent keys for any given private key. Since all these keys form equivalence classes of equal size, we reduced the private key space of MIA by this factor. □

Corollary 4.9 *For $K := (S, P, T) \in \mathit{Aff}^{-1}(\mathbb{F}^n) \times \mathbb{E}[X] \times \mathit{Aff}^{-1}(\mathbb{F}^n)$ a private key in MIO [WP05c, Sect. 7.1] we have*

$$n(q^n - 1)$$

equivalent keys. Hence, the key-space of MIO can be reduced by this number.

The above corollary can be proven in exactly the same way as Theorem 4.8. In particular, the fact that MIO is defined over odd rather than even characteristic does not impose a restriction in this context.

Remark. Patarin observed that it is possible to derive equivalent keys by changing the monomial P [Pat96a]. As the aim of this chapter is the study of equivalent keys by chaining the affine transformations S, T alone, we did not make use of this property. A weaker version of the above theorem can be found in [WP05b]; in particular, it does not take the MIO class into account.

Moreover, we observed in this section that it is not possible for MIA to change the transformations S, T from affine to linear. But in [GSB01] Geiselmann *et al.* showed how to reveal the constant parts of these transformations. Hence, having S, T affine instead of linear does not seem to enhance the overall security of MIA.

For $q = 128$ and $n = 67$, we obtain $\approx 2^{469}$ equivalent private keys per class. The number of choices for S, T is $\approx 2^{63,784}$ in this case. This special choice of parameters has been used in Sflash^{v3}, cf [CGP03].

4.2.1 MIA-

As we recall from the cryptanalysis section, MIA itself is insecure, due to a very efficient attack by Patarin [Pat95]. However, for well-chosen parameters q, r, its variation MIA- (or C^{*--}) is actually secure: as in the case of HFE and HFE-, we use the original MIA scheme and apply the minus modification.

Theorem 4.10 *For $K := (S, P, T) \in \mathit{Aff}^{-1}(\mathbb{F}^n) \times \mathbb{E}[X] \times \mathit{Aff}^{-1}(\mathbb{F}^n)$ a private key in MIA and a reduction number $r \in \mathbb{N}$ we have*

$$n.(q^n - 1)q^r \prod_{i=n-r-1}^{n-1} (q^n - q^i)$$

equivalent keys. Hence, the key-space of MIA- can be reduced by this number.

PROOF. This proof is similar to the one of MIA, *i.e.*, we apply both the Frobenius and the big sustainer to S and the corresponding inverse sustainer to the transformation T. This way, we "repair" the change on the central monomial $X^{q^\lambda+1}$. All in all, we obtain a factor of $n.(q^n-1)$ equivalent keys for a given private key.

Next we observe that the reduction sustainer applied to the transformation T alone allows us to change the last r rows of the vector $v_T \in \mathbb{F}^n$ and also the last r rows of the matrix $M_T \in \mathbb{F}^{n\times n}$. This yields an additional factor of $q^r \prod_{i=n-r-1}^{n-1}(q^n-q^i)$ on this side.

Note that the changes on the side of the transformation S and the changes on the side of the transformation T actually are independent: the first computes a normal form for S while the second computes a normal form on T. Hence, we may multiply both factors to obtain the overall number of independent keys. □

For $q=128, r=11$ and $n=67$, we obtain $\approx 2^{6180}$ equivalent private keys per class. The number of choices for S,T is $\approx 2^{63,784}$ in this case. This particular choice of parameters has been used in Sflash$^{\text{v3}}$ [CGP03].

5 Conclusions

In this paper, we showed through the examples of Hidden Field Equations (HFE) and MIA that $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic systems allow many equivalent private keys and hence have a lot of redundancy in this key space, cf Table 1 and Table 2 for numerical examples; the symbols used in Table 1 are explained in the corresponding sections. The $\mathcal{MQ}$-scheme Unbalanced Oil and Vinegar (UOV) has been discussed in [WP05b, Sect. 4.3]. A general overview of $\mathcal{MQ}$-schemes can be found in [WP05c].

Table 1: Summary of the Reduction Results of this Paper

Scheme (*Section*)	Reduction
MIA (*4.2*)	$n(q^n-1)$
MIA- (*4.2.1*)	$n(q^{n-r}-1)q^r \prod_{i=n-r-1}^{n-1}(q^n-q^i)$
HFE (*4.1*)	$nq^{2n}(q^n-1)^2$
HFE- (*4.1.1*)	$nq^n(q^n-1)q^{n-r}(q^{n-r}-1)\prod_{i=n-r-1}^{n-1}(q^n-q^i)$
HFEv (*4.1.2*)	$n'q^{n+n'+vm}(q^{n'}-1)^2\prod_{i=0}^{v-1}(q^v-q^i)$
HFEv- (*4.1.3*)	$n'q^{r+2n'vn'}(q^{n'}-1)^2\prod_{i=0}^{v-1}(q^v-q^i)\prod_{i=n'-r-1}^{n'-1}(q^{n'}-q^i)$

We see applications of our results in different contexts. First, they can be used for memory efficient implementations of the above schemes: using the normal forms outlined in this paper, the memory requirements for the private key can be reduced without jeopardising the security of these schemes. Second, they apply to cryptanalysis as they allow to concentrate on special forms of the private key: an immediate consequence from Sect. 3.1 (additive sustainers) is that HFE does not gain any additional strength from the use of affine rather than linear transformations. Hence, this system should be simplified accordingly. Third, the constructors of new schemes may want to keep these sustaining transformations in mind: there is no point in having a large private key space — if it can be reduced immediately by applying sustainers.

We want to stress that the sustainers from Sect. 3 may not be the only ones possible. We therefore invite other researchers to look for even more powerful transformations. In addition, there are other

Table 2: Numerical Examples for the Reduction Results of this Paper

Scheme	Parameters	Choices for S, T (in $\log_2$)	Reduction (in $\log_2$)
HFE	$q = 2, n = 80$	12,056	326
HFE-	$q = 2, r = 7, n = 107$	23,108	2129
HFEv	$q = 2, v = 7, n = 107$	21,652	1160
HFEv-	$q = 2, n = 107$	22,261	1258
MIA	$q = 128, n = 67$	63,784	469
MIA	$q = 128, n = 67$	63,784	6173

multivariate schemes which have not been discussed in this paper, due to space and time limitations. These schemes include (non-exhaustive list) enTTS [YC04], STS [WBP04]), and PMI [Din04]. We also invite to apply the techniques used in this paper to these schemes to compare the effect of these sustainers to different classes of $\mathcal{MQ}$-schemes.

Acknowledgements

We want to thank Patrick Fitzpatrick (BCRI, University College Cork, Ireland) for encouraging this direction of research. In addition, we want to thank An Braeken (COSIC) who pointed out the existence of Frobenius sustainers (cf Sect. 3.6) for fields of even characteristic; in addition we want to thank her for helpful remarks. Moreover, we want to thank Magnus Daum (CTSC, Ruhr-University Bochum, Germany) for comments on some early results presented in this paper.

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.

Disclaimer

References

[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.ac.be/nessie/workshop/submissions/flash.zip`, 9 pages.

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

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

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

[CGP03] Nicolas Courtois, Louis Goubin, and Jacques Patarin. *SFlash^{v3}, a fast asymmetric signature scheme — Revised Specificatoin of SFlash, version 3.0*, October 17$^{\text{th}}$ 2003. ePrint Report 2003/211, `http://eprint.iacr.org/`, 14 pages.

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

[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.

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

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

[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`.

[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.

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

[Pat95] Jacques Patarin. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88. In *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`.

[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.

[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. Knörzer, 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 $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic 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.

[YC04] Bo-Yin Yang and Jiun-Ming Chen. Rank attacks and defence in Tame-like multivariate PKC's. Cryptology ePrint Archive, Report 2004/061, 29rd September 2004. `http://eprint.iacr.org/`, 21 pages.