Equivalent Keys in $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic Public Key Systems

Christopher Wolf[1,2], and Bart Preneel[1]

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

[2]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

Abstract

$\mathcal{M}$ultivariate $\mathcal{Q}$uadratic public key schemes have been suggested back in 1985 by Matsumoto and Imai as an alternative for the RSA scheme. Since then, several other schemes have been proposed, for example Hidden Field Equations, Unbalanced Oil and Vinegar schemes, and Stepwise Triangular Schemes. All these schemes have a rather large key space for a secure choice of parameters. Surprisingly, the question of equivalent keys has not been discussed in the open literature until recently. In this article, we show that for all basic classes mentioned above, it is possible to reduce the private — and hence the public — key space by several orders of magnitude. For the Matsumoto-Imai scheme, we are even able to show that the reductions we found are the only ones possible, *i.e.*, that these reductions are tight. While the theorems developed in this article are of independent interest themselves as they broaden our understanding of $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic public key systems, we see applications of our results both in cryptanalysis and in memory efficient implementations of $\mathcal{MQ}$-schemes.

Keywords: $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic Polynomials, Public Key signature, Hidden Field Equations, Matsumoto-Imai scheme A, C*, Unbalanced Oil and Vinegar, Stepwise Triangular Systems

Date: 2005-12-22

1 Initial Considerations

In the last 20 years, several schemes based on the problem of $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic equations (or $\mathcal{MQ}$ for short) have been proposed. The most important ones certainly are MIA / C* [MI88] and Hidden Field Equations (HFE, [Pat96b]) plus their variations MIA- / C^{*--}, HFE-, HFEv, and HFEv- [KPG99, Pat96a, Pat96b]. Both classes have been used to construct signature schemes for the European cryptography project NESSIE [NES], namely the MIA- variation in Sflash [CGP03], the HFEv- variation in Quartz [CGP01] and the HFE- variation in the tweaked version Quartz-7m [WP04]. Unbalanced Oil and Vinegar schemes [KPG99] and Stepwise Triangular Schemes [WBP04] 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 [YC04], Tractable Rational Maps [WHL$^+$05], or Rainbow [DS05].

The aim of this paper is to systematically study 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 $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic 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 $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic schemes such that they do not have a large number of equivalent private keys but only a small number, preferable 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

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

with $n \in \mathbb{Z}^+$ variables and $m \in \mathbb{Z}^+$ equations. Moreover, we have $1 \le i \le m; 1 \le j \le k \le n$ 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 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 $S \in \mathrm{Aff}^{-1}(\mathbb{F}^n), T \in \mathrm{Aff}^{-1}(\mathbb{F}^m)$ are bijective affine transformations. Details on affine transformation are given in Section 2.1). Moreover, we have $\mathcal{P}' \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$ 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 $y'_1, \ldots, y'_m$. 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 $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic public key systems is given in [WP05c].

1.1 Related Work

In their cryptanalysis of HFE, Kipnis and Shamir report the existence of "isomorphic keys" [KS99]. A similar observation for Unbalanced Oil and Vinegar Schemes can be found in [KPG99]. In both cases, there has not been a systematic study of the structure of equivalent key classes. In addition, Patarin observed the existence of some equivalent keys for MIA / C* [Pat96a] — however, his method is different from the one presented in this article, as he concentrated on modifying the central monomial rather than using special affine transformations. Moreover, Toli observed that there exists an additive sustainer in the case of Hidden Field Equations [Tol03] but did not extend his result to other $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic schemes. Additive sustainers will be introduced in Section 3.1. In the case of symmetric ciphers, [BCBP03] used a similar idea in the study of S-boxes. A different angle of the idea of equivalent keys can be found in [HWyCL05] where the authors compute normal forms of the *public* key. Main reason here is to save some memory in the public but particularily in the private key. Using the techniques suggested in [HWyCL05], the latter can be reduced by up to 50%.

This article is based on the two conference papers [WP05b, WP05a] which deal with the classes MIA, HFE, and UOV. In this article, the proofs have been simplified and also extended to the STS class. In addition, a tightness proof for the case of MIA is given.

1.2 Outline

This paper is organized as follows: after this general introduction, we move on to the necessary mathematical background in Section 2. This includes particularly a definition of the term *equivalent keys*. In Section 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 Section 4. In Section 5, we give a tightness proof for the case of MIA/MIO. This paper concludes with Section 6.

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 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*

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

"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, $\mathrm{Aff}^{-1}(\cdot)$ denotes the class of bijective affine transformations. We give more details on affine transformations in Section 2.1. In order to find equivalent keys, we consider the following transformations:

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

$$
\begin{tikzcd}
\text{input } x \arrow[d] \\
x=(x_1,\ldots,x_n) \arrow[d, "\sigma^{-1}\circ S", "\text{private: } S"'] \arrow[ddd, bend left=60, "\textbf{public}: (p_1,\ldots,p_n)"] \\
x' \arrow[d, "\tau\circ\mathcal{P}'\circ\sigma", "\text{private: } \mathcal{P}'"'] \\
y' \arrow[d, "T\circ\tau^{-1}", "\text{private: } T"'] \\
\text{output } y
\end{tikzcd}
$$

Fig. 1: Equivalent private keys using affine transformations σ, τ

$(S, \mathcal{P}', T)$ for (2.2) and (σ, τ) sustaining transformations. This idea has already been outlined in Figure 1.

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 (cf Section 4.1), it is the bounding degree $d \in \mathbb{Z}^+$ of the polynomial $P'(X') \in \mathbb{E}[X']$. In the case of MIA, the "shape" is the fact that we have a single monomial with factor 1 as the central equation (cf Section 4.2). In general and 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 $\sigma = \tau = id$.

Lemma 2.3 *Let $\sigma \in \mathit{Aff}^{-1}(\mathbb{F}^n), \tau \in \mathit{Aff}^{-1}(\mathbb{F}^m)$ be sustaining transformations. If the two structures $G := (\sigma, \circ)$ 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 the subgroup G. Second, we also have symmetry as subgroups are closed under inversion. Third, we have transitivity as subgroups are closed under composition. Therefore, the subgroup G partitions the private key space into equivalence classes. The proof for the subgroup $H := (\tau, \circ)$ is analogous. □

Remark. We want to point out that the above proof does not use special properties of sustaining transformations, but the fact that we dealt with subgroups 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.

2.1 Affine Transformations

Given that our main tool to construct equivalent keys are special subclasses of affine transformations, we start with some general observations on them. As we only deal with bijective affine transformations $\mathrm{Aff}^{-1}(\cdot)$ and bijective linear transformations $\mathrm{Hom}^{-1}(\cdot)$ in this article, 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* $s_1, \dots, s_n$ *be* n *polynomials of degree 1 at most over* $\mathbb{F}$, *i.e.*, $s_i(x_1, \dots, x_n) := \beta_{i,1}x_1 + \dots + \beta_{i,n}x_n + \alpha_i$ *with* $1 \le i, j \le n$ *and* $\alpha_i, \beta_{i,j} \in \mathbb{F}$. *Let* $S(x) := (s_1(x), \dots, s_n(x))$ *for* $x := (x_1, \dots, x_n)$ *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 $1 \le i, j \le n$. However, the first is useful in the context of matrix equations while the latter is preferable when dealing with affine transformations in the context of term substitution.

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. A more elaborated proof can be found in [Wol05, Lemma 2.2.7]. □

3 Sustaining Transformations

In this section, we discuss several examples of sustaining transformations. In particular, we consider their effect on the central transformation $\mathcal{P}'$.

3.1 Additive Sustainer

For $n = m$, *i.e.*, the number of equations is equal to the number of variables, let $\sigma(X) := (X + A)$ and $\tau(X) := (X + A')$ for some elements $A, A' \in \mathbb{E}$. As long as the transformations σ, τ 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 $S, T \in \text{Aff}^{-1}(\mathbb{F}^n)$ to zero, *i.e.*, to obtain a new key $(\hat{S}, \hat{\mathcal{P}}', \hat{T})$ with $\hat{S}, \hat{T} \in \text{Hom}^{-1}(\mathbb{F}^n)$. The constant terms of S, T have now been moved to the central equation $\mathcal{P}'$ and as a result, $\hat{S}, \hat{T}$ are now linear rather than affine transformations over $\mathbb{F}^n$.
Remark. This result is very useful for cryptanalysis as it allows us to "collect" the constant terms in the central equations $\mathcal{P}'$. For cryptanalytic purposes, we therefore only need to consider the case of linear transformations $S, T \in \text{Hom}^{-1}(\mathbb{F}^n)$.

The additive sustainer also works if we interpret it over the vector space $\mathbb{F}^n$ rather than the extension field $\mathbb{E}$. To distinguish this case from the setting above, we write $a \in \mathbb{F}^n, a' \in \mathbb{F}^m$ here. In particular, we can also handle the case $n \ne m$ 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 $(BX), (B'X) \in \text{Aff}^{-1}(\mathbb{F}^n)$.

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. Note that we only allow non-zero elements of the extension field $\mathbb{E}$ for B, B' as $BX, B'X$ are not invertible otherwise.

3.3 Small Sustainer

We now consider vector-matrix multiplication 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 non-zero coefficients $b_1, \ldots, b_n, b'_1, \ldots, b'_m \in \mathbb{F}^*$ and $Diag(b), Diag(b')$ the diagonal matrices on both vectors $b \in \mathbb{F}^n$ 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 $(p'_1, \ldots, p'_m)$. As for the big sustainer, we require non-zero elements, *i.e.*, we have $b_i, b'_i \in \mathbb{F}^*$.

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.

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 the ground field $\mathbb{F}$. 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 Definition 3.1 is not empty for any given $\mathbb{F}$ and $n \in \mathbb{Z}^+$. Hence, the corresponding set of Frobenius transformations is not empty either. In particular, we notice that the Frobenius transformation X^{q^0} coincides with the neutral element of the group of linear transformations $(\mathrm{Hom}^{-1}(\mathbb{F}^n), \circ)$.

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

So all left to show is that for any given Frobenius transformations σ, τ, the composition $\sigma \circ \tau$ is also a Frobenius transformation, *i.e.*, that we have closure.

Let $\sigma(X) := X^{q^a}$ and $\tau(X) := X^{q^b}$ for some $a, b \in H$. So we can write $\sigma(X) \circ \tau(X) = X^{q^{a+b}}$. 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 $\sigma \circ \tau$ is also a Frobenius transformation. This completes the proof that all Frobenius transformations form a group. □

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). Fore a given extension field $\mathbb{E}$, there are n Frobenius sustainers.

It is tempting to extend this result to the case of powers of the characteristic of $\mathbb{F}$. However, this is not possible as $x^{\mathrm{char}\mathbb{F}}$ is not a linear transformation in $\mathbb{F}$ for $q \ne p$ where p denotes the characteristic of the finite field $\mathbb{F}$ and $q := |\mathbb{F}|$ the number of its elements.

Remark. All six sustainers presented so far form groups and hence partition the private key space into equivalence classes. The relation between partitions and groups has been previously discussed in 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* while $S, \mathcal{P}', T$ have the same meaning as before, *i.e.*, they are affine invertible transformations and a system of $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic polynomials, respectively. 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 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 $\mathcal{P}$). Therefore, 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. We will show how to deal with this difficulty in the corresponding proofs.

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

Having all necessary tools at hand, we show now how to apply suitable sustaining transformations to the $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic schemes. We want to stress that the reductions in size we achieve in this section represent lower rather than upper bounds: additional sustaining transformations may further reduce the key space of these schemes. The only exception for this rule are the MIA/MIO class: due to the tightness proof in Section 5, we know that only the big sustainer and the Frobenius sustainer can be applied here. Unfortunately, the details of this tightness proof are cumbersome and we do not see how it can be extended to the other schemes discussed in this section.

4.1 Hidden Field Equations

We start with the HFE class as the overall proof ideas can be demonstrated most clearly here. In fact, we will use some of these ideas again for the MIA class. The Hidden Field Equations (HFE) have been proposed by Patarin [Pat96b]. Its main characteristic is the exceptional low degree of the central polynomial $P'(X') \in \mathbb{E}[X']$.

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

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

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

and a degree $d \in \mathbb{Z}^+$, 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 $\mathbb{F}$. A proof of this fact for the case $\mathbb{F}$ =GF(2) can be found in [MIHM85]. It has been elaborated and further extended in [Wol05, Section 2.4]. Polynomials of cubic and higher degree have been discussed in [KS99, Lemma 3.3]. The bound of the degree of the polynomial $P'(X')$ has a different motivation: this allows efficient inversion of the equation $P(X) = Y$ for given $Y \in \mathbb{E}$ and is hence necessary to obtain efficient schemes. 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 $i, j, k \in \mathbb{Z}^+$ and $q^i, q^i + q^j \leq d$. Hence, we can apply both the additive and the big sustainer from sections 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 theorem, 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 $\hat{S} : \mathbb{E} \rightarrow \mathbb{E}$ 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 after the Frobenius sustainer has been applied. Now we pick an element $C \in \mathbb{E} \backslash \{0, 1\}$ for which $g := \overline{S}(C)$ 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 surjective 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 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 authors, the additive sustainer for HFE has first been reported in [Tol03]; it was 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 from Section 3.7 applied. 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 $K := (S, P, T) \in Aff^{-1}(\mathbb{F}^n) \times \mathbb{E}[X] \times Aff^{-1}(\mathbb{F}^n)$ a private key in HFE and a reduction parameter $r \in \mathbb{Z}^+$ 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 can 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 $\tilde{T}$ allows for $q^r \prod_{i=n-r-1}^{n-1}(q^n - q^i)$ 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 $q^{n-r} \cdot q^r \cdot (q^{n-r}-1) \cdot \prod_{i=n-r-1}^{n-1}(q^n - q^i)$ 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 Quartz-7m [WP04].

4.1.2 HFEv

Another important variation of Hidden Field Equations is HFEv. In particular, it was used in the signature scheme Quartz [CGP01]. HFEv was introduced in [KPG99]. The HFEv scheme is characterized in the following definition.

DEFINITION 4.4 *Let $\mathbb{E}$ be a finite field with degree n' over $\mathbb{F}$, $v \in \mathbb{Z}^+$ the number of vinegar variables, 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*

$$
\begin{aligned}
P'_{z'_1,\ldots,z'_v}(X') \quad := \quad & \sum_{\substack{0\le i,j\le d \\ q^i+q^j\le d}} C_{i,j} X'^{q^i+q^j} + \sum_{\substack{0\le k\le d \\ q^k\le d}} B_k(z_1,\ldots,z_v) X'^{q^k} \\
& + A'(z'_1,\ldots,z'_v) \\
& \text{where} \begin{cases} C'_{i,j} X'^{q^i+q^j} & \text{for } C'_{i,j} \in \mathbb{E} \text{ are the quadratic terms,} \\ B'_k(z'_1,\ldots,z'_v) X'^{q^k} & \text{for } B'_k(z'_1,\ldots,z'_v) \text{ depending linearly on } z'_1,\ldots,z'_v \text{ and} \\ A'(z'_1,\ldots,z'_v) & \text{for } A'(z'_1,\ldots,z'_v) \text{ depending quadratically on } z'_1,\ldots,z'_v \end{cases}
\end{aligned}
$$

and a degree $d \in \mathbb{Z}^+$, 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 $K := (S, P', T) \in \mathit{Aff}^{-1}(\mathbb{F}^n) \times \mathbb{E}[X'] \times \mathit{Aff}^{-1}(\mathbb{F}^m)$ a private key in HFEv, $v \in \mathbb{Z}^+$ 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 $q^m \cdot (q^m - 1) = q^{n'} \cdot (q^{n'} - 1)$ 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. In order 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. In order 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 stated 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 $B'_k(z'_1,\dots,z'_v)$ and $A'(z'_1,\dots,z'_v)$.

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 $P_{z_1,\dots,z_v}(X)$. 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 [CGP01] was of this type.

Theorem 4.6 *For $K := (S, P', T) \in Aff^{-1}(\mathbb{F}^n) \times \mathbb{E}[X'] \times Aff^{-1}(\mathbb{F}^{m+v}, \mathbb{F}^{m+r})$ a private key in HFEv-, $v \in \mathbb{Z}^+$ vinegar variables, a reduction parameter $r \in \mathbb{Z}^+$ 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

As HFE, the MIA class uses a finite field $\mathbb{F}$ and an extension field $\mathbb{E}$. However, the choice of the central equation is far more restrictive than in HFE as we only have one monomial here.

Definition 4.7 *Let $\mathbb{E}$ be an extension field of dimension n over the finite field $\mathbb{F}$ with even characteristic and $\lambda \in \mathbb{Z}^+$ 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. As we will see in Section 5, the only sustainers suitable here are the big sustainer, see Section 3.2, and the Frobenius sustainer from Section 3.6.

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 "new" scheme C* coincides with the previously suggested "Scheme A" from [IM85]. To acknowledge this historical development, we decided to come back to the earlier notation and call the scheme presented in this section "MIA" for "Matsumoto-Imai Scheme A". This has been previously suggested in [WP05c].

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 Input 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

$$\begin{aligned}\mathcal{P} &= T \circ \tau^{-1} \circ \tau \circ P' \circ \sigma \circ \sigma^{-1} \circ S\\ &= \tilde{T} \circ (B^{(q^\lambda+1)\cdot(-1)}.B^{q^\lambda+1}.X'^{q^\lambda+1}) \circ \tilde{S}\\ &= \tilde{T} \circ P' \circ \tilde{S}\,,\end{aligned}$$

where $\tilde{S}$ is in normal form. In contrast to HFE in 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 to 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

$$(BX^{q^c}, B^{-q^\lambda-1}X^{q^{n-c}}) \bullet (S, P', T) \text{ where } B \in \mathbb{E}^* \text{ and } 0 \le c < n \text{ for } c \in \mathbb{N}\,,$$

which leads to a total of $n \cdot (q^n-1)$ 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. □

We want to point out that there is also a variation of MIA defined over *odd* characteristic. This variation has been suggested in [WP05c, Sect. 7.1] and uses exactly the same structure for the private key. For technical reasons, the condition on the gcd is replaced by $\gcd(q^n-1, q^\lambda+1) = 2$. However, this is irrelevant for our purpose and we have hence the following corollary.

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 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 proved 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 article 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 Geiselmann *et al.* showed how to reveal the constant parts of these transformations [GSB01]. Hence, having S, T affine instead of linear does not 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.

4.2.1 MIA-

We want to point out that MIA itself is insecure, due to a very efficient attack by Patarin [Pat95]. However, for well-chosen parameters q, r, its variation MIA- (also known as C^{*--}) is believed to be secure: as in the case of HFE and HFE-, we use the original MIA scheme and apply the minus modification from Section 3.7.

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 $r \in \mathbb{Z}^+$ 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 $n \cdot (q^n - 1)$ 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 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^{v3} [CGP03].

4.3 Unbalanced Oil and Vinegar Schemes

In contrast to the two schemes before, we now consider a class of $\mathcal{MQ}$-schemes which does not mix operations over two different fields $\mathbb{E}$ and $\mathbb{F}$ but only performs computations over the ground field $\mathbb{F}$. Moreover, Unbalanced Oil and Vinegar schemes (UOV) omit the affine transformation T but use $S \in \mathrm{Aff}^{-1}(\mathbb{F}^n)$. To fit in our framework, we set it to be the identity transformation, *i.e.*, we have $T := \tau := id$. UOV were proposed in [KPG99].

Definition 4.11 *Let $\mathbb{F}$ be a finite field and $n, m \in \mathbb{Z}^+$ with $n \geq 2m$. Moreover, let $\alpha'_i, \beta'_{i,j}, \gamma'_{i,j,k} \in \mathbb{F}$. We say that the polynomials below are central equations in UOV-shape:*

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

In this context, the variables x'_i for $1 \leq i \leq m$ are called the "vinegar" variables and x'_i for $m < i \leq n$ the "oil" variables. Note that the vinegar variables are combined quadratically while the oil variables are only combined with vinegar variables in a quadratic way. Therefore, assigning random values to the vinegar variables, results in a system of linear equations in the oil variables which can than be solved, *e.g.*, using Gaussian elimination. So the "shape" of UOV is the fact that a system in the oil variables alone is linear. Hence, we may not mix oil variables and vinegar variables in our analysis but may perform affine transformations within one set of these variables. So for UOV, we can apply the additive sustainer and also the Gauss sustainer, introduced in sections 3.1 and 3.5. However, in order to ensure that the shape of the central equations does not change, we have to ensure that the Gauss sustainer influences the vinegar and oil variables separately.

Theorem 4.12 *Let $K := (S, \mathcal{P}', id) \in \mathit{Aff}^{-1}(\mathbb{F}^n) \times \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m) \times \mathit{Aff}^{-1}(\mathbb{F}^m)$ be a private key in UOV. Then we have*

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

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

Proof. As in the case of the schemes before, we compute a normal form for a given private key. First, applying the additive sustainer reduces the affine transformation S to a linear transformation. This results in a factor of q^n in terms of equivalent keys. Second, applying the Gauss sustainer separately within vinegar and oil variables, we can enforce the following structure, denoted $R \in \mathbb{F}^{n \times n}$, on the matrix $M_S \in \mathbb{F}^{n \times n}$ of the (now only) linear transformation S:

$$R := \begin{pmatrix} I_m & 0 & A_m \\ 0 & I_{n-2m} & B_m^{n-2m} \\ 0 & 0 & I_m \end{pmatrix}.$$

In this context, the matrices I_m, I_{n-2m} are the identity elements of $\mathbb{F}^{m \times m}$ and $\mathbb{F}^{(n-2m)\times(n-2m)}$, respectively. Moreover, we have the matrices $A_m \in \mathbb{F}^{m \times m}$ and $B_m^{n-2m} \in \mathbb{F}^{(n-2m)\times m}$. For a given central equation $\mathcal{P}'$, each possible matrix R leads to the same number of equivalent keys. Let

$$E := \begin{pmatrix} F_{n-m} & 0 \\ G_{n-m}^m & H_m \end{pmatrix}$$

be an $(n \times n)$-matrix. Here, we require that the matrices $F_{n-m} \in \mathbb{F}^{(n-m)\times(n-m)}$ and $H_m \in \mathbb{F}^{m \times m}$ are invertible and hence the counting from Lemma 2.4 applies. For $G_{n-m}^m \in \mathbb{F}^{m \times (n-m)}$, we have no restrictions. This way, we define the transformation $\sigma(x) := Ex$ where $x \in \mathbb{F}^n$. Note that these transformations σ form a subgroup within the affine transformations. So we have

$$(Ex + a, id) \bullet (S, \mathcal{P}', id) \text{ for } a \in \mathbb{F}^n \text{ and } E \text{ as defined above.}$$

As this choice of σ partitions the private key space into equivalence classes of equal size, and due to the restrictions on E, we reduced the size of the private key space by an additional factor of $q^{mn} \prod_{i=0}^{n-m-1}(q^{n-m} - q^i) \prod_{i=0}^{m-1}(q^m - q^i)$. □

For $q = 2, m = 64, n = 192$, we obtain $2^{32{,}956}$ equivalent keys per key — in comparison to $2^{37{,}054}$ choices for S. If we increase the number of variables to $n = 256$, we obtain $2^{57{,}596}$ and $2^{65{,}790}$, respectively. Both choices of parameter have been used in [KPG03].

4.4 Stepwise-Triangular Systems

Unbalanced Oil and Vinegar schemes and Stepwise-Triangular Systems (STS) are quite similar as both are defined over small ground fields rather than ground fields and extension fields. In addition, they enforce a special structure on the input variables. In the case of UOV we have two sets of variables while we use $L \in \mathbb{Z}^+$ such sets in the case of STS, each forming one *layer* or *step*. These layers form a generalized triangular structure, hence the name of these schemes. We capture this intuition more formally below. Stepwise Triangular Schemes were introduced in [WBP04].

Definition 4.13 *Let $n_1, \ldots, n_L \in \mathbb{Z}^+$ be L integers such that $n_1 + \cdots + n_L = n$, the number of variables, and $m_1, \ldots, m_L \in \mathbb{Z}^+$ such that $m_1 + \cdots + m_L = m$, the number of equations. Here n_l represents the number of new variables (step-width) and m_l the number of equations (step-height), both in Step l for $1 \le l \le L$. By convention, we set $n_0 := m_0 := 0$. Now let $\mathcal{P}' \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$ be a system of $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic polynomials such that the m_l private quadratic polynomials $p'_{m_0+\ldots+m_{l-1}+1}, \ldots, p'_{m_l}$ of each layer l contain only the variables x'_k with $k \le \sum_{j=1}^{l} n_j$, i.e., only the variables defined in all previous steps plus n_l new ones. Then we call $(S, \mathcal{P}', T,) \in \mathit{Aff}^{-1}(\mathbb{F}^n) \times \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m) \times \mathit{Aff}^{-1}(\mathbb{F}^m)$ a private key in* Stepwise Triangular System *shape. If $n_1 = \ldots = n_L = m_1 = \ldots = m_L = r$ for some $r \in \mathbb{Z}^+$, we call this a* regular *Stepwise Triangular System.*

We want to stress in this context that we do not assume any additional structure for the private polynomials $p'_1, \ldots, p'_m$ here. In particular, all coefficients $\gamma'_{i,j,k}, \beta'_{i,j}, \alpha'_i \in \mathbb{F}$ for these polynomials may be chosen at random.

As STS and UOV are based on a similar concept, the following proof on Stepwise Triangular Schemes uses the same ideas as the proof for the UOV class. As for UOV we exploit the fact that we can use Gauss operations within any given layer — and use again the fact that equations of Layer l depend on all variables of the layers $1, \ldots, l$, *i.e.*, we may also perform Gauss operations on these previous layers, as long as the result only affects the given Layer l.

Theorem 4.14 *Let $\mathbb{F}$ be a finite field with $q := |\mathbb{F}|$ elements, $n \in \mathbb{Z}^+$ the number of variables, $m \in \mathbb{Z}^+$ the number of equations and $L \in \mathbb{Z}^+$ the number of layers. Moreover, let $(n_1, \ldots, n_L) \in$*

$(\mathbb{Z}^+)^L$ *be a vector of integers such that* $n_1 + \ldots + n_L = n$ *and* $m_1, \ldots, m_L \in \mathbb{Z}^+$ *integers such that* $m_1 + \ldots + m_L = m$. *Then for* $K := (S, \mathcal{P}', T) \in \mathit{Aff}^{-1}(\mathbb{F}^n) \times \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m) \times \mathit{Aff}^{-1}(\mathbb{F}^m)$ *a private key in STS we have*

$$q^{m+n} \prod_{i=1}^{L} \left(q^{n_i(n - \sum_{j=1}^{i} n_j)} \prod_{j=0}^{n_i - 1} (q^{n_i} - q^j) \right) \prod_{i=1}^{L} \left(q^{m_i(m - \sum_{j=1}^{i} m_j)} \prod_{j=0}^{m_i - 1} (q^{m_i} - q^j) \right)$$

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

Proof. For this proof, we apply both the additive sustainer and the Gauss sustainer. The latter is applied independently on each layer.

First, we observe that we can apply the additive sustainer both to the transformation $S \in \mathrm{Aff}^{-1}(\mathbb{F}^n)$ and $T \in \mathrm{Aff}^{-1}(\mathbb{F}^m)$ to obtain the fix point $S(0) = T(0) = 0$. As a result, we obtain a factor of q^{m+n} and may assume $S \in \mathrm{Hom}^{-1}(\mathbb{F}^n)$ and $T \in \mathrm{Hom}^{-1}(\mathbb{F}^m)$ for the remainder of this proof.

As in the proof of Theorem 4.12, we impose a special structure on the linear transformation S. Therefore, we consider the matrix

$$M_S := \begin{pmatrix} I_{n_1} & * & * & \cdots & & * & * \\ 0 & I_{n_2} & * & & & & * \\ 0 & 0 & I_{n_3} & & & & \\ \vdots & & & \ddots & & & \vdots \\ & & & & I_{n_{L-2}} & * & * \\ 0 & & & & 0 & I_{n_{L-1}} & * \\ 0 & 0 & & \cdots & 0 & 0 & I_{n_L} \end{pmatrix}$$

In $M_S \in \mathbb{F}^{n \times n}$, sub-matrices I_{n_i} are identity matrices in $\mathbb{F}^{n_i \times n_i}$ for $1 \leq i \leq n$. The left lower portion of M_S is zero while the upper right portion of M_S consists of elements of $\mathbb{F}$. To obtain this matrix M_S, we make use of

$$E := \begin{pmatrix} A_{n_1} & 0 & 0 & \cdots & & 0 & 0 \\ * & A_{n_2} & 0 & & & & 0 \\ * & * & A_{n_3} & & & & \\ \vdots & & & \ddots & & & \vdots \\ & & & & A_{n_{L-2}} & 0 & 0 \\ * & & & & * & A_{n_{L-1}} & 0 \\ * & * & & \cdots & * & * & A_{n_L} \end{pmatrix}$$

In this matrix $E \in \mathbb{F}^{n \times n}$, we have invertible components $A_{n_i} \in \mathbb{F}^{n_i \times n_i}$ for $1 \leq i \leq L$. Moreover, the upper right portion of the matrix E is zero while the left lower portion of E consists of elements of $\mathbb{F}$. We see that the above matrix is sufficient to impose this special structure on M_S. Moreover, for each choice of E, we obtain another linear transformation S and hence, M_S is a normal form of S.

Using Lemma 2.4, we can now count the number of possible matrices E and obtain

$$\prod_{i=1}^{L} \left(q^{n_i(n - \sum_{j=1}^{i} n_j)} \prod_{j=0}^{n_i - 1} (q^{n_i} - q^j) \right)$$

for the number of possibilities. To see the correctness of the above computation, we specialise it for n_1: here we have the term $\prod_{j=0}^{n_1 - 1} (q^{n_1 - q^j})$ which computes the number of choices for the matrix A_{n_1} while $q^{n_1(n-n_1)}$ gives the number of choices in the $(n_1 \times (n - n_1))$ column over $\mathbb{F}$ below the matrix A_{n_1}. By induction on n_i we obtain the above formula for $1 \leq i \leq L$. In particular, as M_S is in normal form, there exists exactly one matrix E of the above form for any given $S \in \mathrm{Hom}^{-1}(\mathbb{F}^n)$. Hence, we have established the existence of an equivalence class of this size.

The corresponding proof for the transformation T is analogous, so we can define matrix $E' \in \mathbb{F}^{m \times m}$ similar to matrix E. We only have to replace variables by equations here to reflect the different roles the transformations S and T play. Note that we are allowed to add equations of lower layers to equations of higher layers and hence, may perform the same Gauss operations on equations that we could apply on variables. So we have

$$(Ex + a, E'x + a') \bullet (S, \mathcal{P}', T) \text{ for } a \in \mathbb{F}^n, a' \in \mathbb{F}^m \text{ and } E, E' \text{ defined as above.}$$

As this choice of σ, τ partitions the private key space into equivalence classes of equal size, and due to the restrictions on E, E', we reduced the size of the private key space by the above number. □

Corollary 4.15 *For regular STS with step-width $r \in \mathbb{Z}^+$, $L \in \mathbb{Z}^+$ layers and $n := Lr$ variables, the above formula simplifies to*

$$q^{2n} \left(\prod_{l=1}^{L} q^{r(n-(l-1)r)} \prod_{i=0}^{r-1} (q^r - q^i)^L \right)^2 .$$

Choosing a regular STS scheme and $q = 2, r = 4, L = 25, n = 100$, we obtain $2^{11,315}$ equivalent keys for each given private key. For comparison: the number of choices for the two affine transformations S, T is $2^{20,096}$. Changing the number of layers to 20, and consequently having $r = 5$, we obtain a total of $2^{11,630}$ equivalent keys. These special choices of parameters have been suggested in [KS04].

5 Tightness for MIA and MIO

All theorems in the previous section suffer from the same problem: we do not know if the size-reductions are "tight", *i.e.*, if the sustainers applied are the only ones possible. In this section we proof that for the MIA/MIO class, the big sustainer and the Frobenius sustainer are actually the *only* possible way to achieve equivalent keys for MIA and MIO. We recall that both classes use a finite field $\mathbb{F}$ with $q := |\mathbb{F}|$ elements and an extension field $\mathbb{E}$ of dimension n over $\mathbb{F}$. Over $\mathbb{E}$, they use the monomial $Y' := X'^{q^\lambda+1}$ as central equation for $1 \leq \lambda < n$. While MIA needs q to be even, MIO is defined for q being odd. The proof for the MIA case is based on an unpublished observation by Dobbertin. Its extension to the MIO class is due to the authors.

The starting point of the proof is the following equation which needs to hold for any two equivalent keys for the MIA / MIO class. This is due to the fact that Definition 2.1 restricts us to affine transformations to transfer one private key into. Hence we have the following equation:

$$X^{q^\lambda+1} = T \circ X^{q^\lambda+1} \circ S ,$$

which we can rewrite as

$$X^{q^\lambda+1} \circ S^{-1} = T \circ X^{q^\lambda+1} . \tag{2}$$

We know from Section 2.1 that affine transformations form a group. Moreover, we can use Definition 2.7 to obtain a univariate representation for any given affine transformation. We can hence express (2) as

$$\left(\sum_{i=0}^{n-1} B_i X^{q^i} + A \right)^{q^\lambda+1} = \sum_{i=0}^{n-1} \tilde{B}_i \left(X^{q^\lambda+1} \right)^{q^i} + \tilde{A} ,$$

for some coefficients $A, \tilde{A}, B_i, \tilde{B}_i \in \mathbb{E}$. Note that we have $(A+B)^p = A^p + B^p$ in a finite field of characteristic p and consequently $(A+B)^q = A^q + B^q$ for $q = p^k$ and some $k \in \mathbb{Z}^+$. We now use a matrix representation of the above equation, similar to the matrix used by Kipnis and Shamir in their cryptanalysis of HFE [KS99]. This yields

$$\begin{pmatrix} A^{q^\lambda+1} & AB_0^{q^\lambda} X^{q^\lambda} & AB_1^{q^{\lambda+1}} X^{q^{\lambda+1}} & \dots & AB_{n-1}^{q^{\lambda+n-1}} X^{q^{\lambda+n-1}} \\ B_0 A^{q^\lambda} X & B_0^{q^\lambda+1} X^{q^\lambda+1} & B_0 B_1^{q^\lambda} X^{q^{\lambda+1}+1} & & B_0 B_{n-1}^{q^\lambda} X^{q^{\lambda+n-1}+1} \\ B_1 A^{q^\lambda} X^q & B_1 B_0^{q^\lambda} X^{q^\lambda+q} & B_1^{q^\lambda+1} X^{q^{\lambda+1}+q} & \dots & B_1 B_{n-1}^{q^\lambda} X^{q^{\lambda+n-1}+q} \\ \vdots & & \vdots & \ddots & \vdots \\ B_{n-1} A^{q^\lambda} X^{q^{n-1}} & B_{n-1} B_0^{q^\lambda} X^{q^\lambda+q^{n-1}} & B_{n-1} B_1^{q^\lambda} X^{q^{\lambda+1}+q^{n-1}} & \dots & B_{n-1}^{q^\lambda+1} X^{q^{\lambda+n-1}+q^{n-1}} \end{pmatrix}$$

$$= \begin{pmatrix} \tilde{A} & 0 & & \dots & 0 \\ 0 & \tilde{B}_0^{q^\lambda+1} X^{q^\lambda+1} & 0 & & 0 \\ & 0 & \tilde{B}_1^{q^{\lambda+1}+q} X^{q^{\lambda+1}+q} & & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \tilde{B}_{n-1}^{q^\lambda+(n-1)+q^{n-1}} X^{q^{\lambda+n-1}+q^{n-1}} \end{pmatrix} \quad (*)$$

As we work in $\mathbb{E}$ which has a multiplicative group of $q^n - 1$ elements, we can reduce all powers larger than or equal to q^n by $q^n - 1$.

Lemma 5.1 *For $\mathbb{F}$ a finite field with $q > 2$ elements, we can only use the big sustainer and the Frobenius sustainer to derive equivalent private keys within the MIA and the MIO class.*

Proof. For this proof we show that the equations given by $(*)$ imply that $A = 0$ and all B_i for $0 \le n < n$ except one are zero. Note that $B_0 = \ldots = B_{n-1} = 0$ implies that $S(X)$ is no bijection anymore but the transformation $S(X) = A$ for any input $X \in \mathbb{E}$ and fixed $A \in \mathbb{E}$. Hence, there must exist at least one non-zero coefficient B_i. W.l.o.g., we assume that B_0 is non-zero. Note that this lemma is trivially true for an extension field of degree $n = 1$. Hence, we assume that $\mathbb{E}$ is a proper extension of $\mathbb{F}$ and therefore $n \ge 2$.

For the proof, we make use of the fact that we can reduce all powers in $\mathbb{E}$ by $q^n - 1$. For powers of the form q^i this means that we can reduce the power i by n, *i.e.*, all computations are done in the ring $\mathbb{Z}/n\mathbb{Z}$ and we can hence assume $0 \le a, b, c, d < n$ in the sequel. Moreover, we can distinguish the following three types of equations in $(*)$:

1. Equations of the form $AB^{q^\lambda + a} + B_b^{q^b} A^{q^\lambda} = 0$ for $a + \lambda \equiv b \pmod n$. We call them *equations of type A*. Note that they are related to terms with monomial of the form X^{q^b} for $0 \le b < n$.

2. Equations of the form $B_a^{q^{\lambda+a}} B_b^{q^b} = 0$ with the condition $a + \lambda \equiv b \pmod n$ on the powers. We call them *equations of Hamming weight 1* and say that they are *self-dual*. Note that each row / column in the above matrix contains exactly one equation of Hamming weight 1 and that they correspond to terms with a monomial of the form X^{2q^b} for $0 \le b > n$. As we have $q > 2$ there is no reduction of the power here.

3. Equations of the form $B_a^{q^{\lambda+a}} B_b^{q^b} + B_c^{q^{\lambda+c}} B_d^{q^d} = 0$ with the following conditions on their powers: first, we have $a \ne b, c \ne d$, as we otherwise would include equations from the diagonal. Obviously, we cannot make the assumption anymore that the right-hand side is equal to zero in this case. Second, we have $a + \lambda \not\equiv b \pmod n$ and $c + \lambda \not\equiv d \pmod n$ as we obtain equations of Hamming weight 1 otherwise. Third, we need $a + \lambda \equiv d \pmod n$ and $c + \lambda \equiv b \pmod n$ to ensure that the powers in the monomial $X^{q^b + q^d}$ actually match. We call the pair (a, b) the *dual* of the pair (c, d). Note that this relation is reflexive, *i.e.*, (c, d) is the dual of (a, b). We call these *equations of type B*.

Note that equations of type A and equations of Hamming weight 1 do not mix as we have $q > 2$. Moreover, equations of Hamming weight 1 may not lie on the diagonal as we would have $\lambda + a \equiv a \pmod n$ in this case and hence $\lambda \equiv 0 \pmod n$, but this violates $0 < \lambda < n$. So far, we did not include any equation from the diagonal in our analysis. We come back to them later.

Inspecting the equation $B_0^{q^\lambda} B_\lambda^{q^\lambda} = 0$ of Hamming weight 1, we see that it implies $B_\lambda = 0$ as we have $B_0 \ne 0$ (see above). In addition, this implies $A = 0$ as we have $AB_0^{q^\lambda} + B_\lambda^{q^\lambda} A^{q^\lambda} = 0$ as an equation of type A. For $n = 2$, we are done. For $n \ge 3$, we can now use all equations of type B of the form $B_0^{q^\lambda} B_b^{q^b} + B_c^{q^{\lambda+c}} B_\lambda^{q^\lambda} = 0$. We notice that we need to meet the following conditions: $b \ne 0, \lambda$ and $c \ne 0, \lambda$ but $c + \lambda \equiv b \pmod n$. We see that we can construct pairs (b, c) meeting this conditions for all $b \in \mathbb{Z}/n\mathbb{Z}\backslash\{0, \lambda, 2\lambda\}$ with $0 < b < n$. Using the above equation we have established that all coefficients $B_b = 0$ as $B_0 \ne 0$ and $B_\lambda = 0$. Note that $\lambda \not\equiv 2\lambda \pmod n$ as we have $0 < \lambda < n$. Moreover, $2\lambda \not\equiv 0 \pmod n$ is not true either, which we see with the following argument: due to the size condition on λ, we know that we need to have $2\lambda = n$ to make the above equation hold. We use the condition $\gcd(q^n - 1q^\lambda + 1) = 1$ for MIA and $\gcd(q^n - 1q^\lambda + 1) = 2$ for MIO to show that $2\lambda = n$ is impossible. Therefore we observe that $(q^{2\lambda} - 1) = (q^\lambda + 1)(q^\lambda - 1)$, *i.e.*, the gcd condition is violated for $n = 2\lambda$.

All left to show is that the coefficient $B_{2\lambda}$ is also equal to zero. To this end, we use the equation $B_{2\lambda}^{q^{3\lambda}} B_0^{q^0} + B_{-\lambda}^{q^0} B_{3\lambda}^{q^{3\lambda}} = 0$ of type B. In order to force the coefficient $B_{2\lambda}$ equal to zero, we need $B_{-\lambda} = 0$ or $B_{3\lambda} = 0$. Therefore, we use the equation $B_{-\lambda} q^0 B_0 q^0 = 0$ of type Hamming weight 1. As we have $B_0 \ne 0$, this implies $B_{-\lambda}$ and hence $B_{2\lambda} = 0$.

We have now established that all coefficients $A = B_1 = \ldots = B_{n-1} = 0$. Using the equations on the diagonal, these conditions also propagate through to the coefficients of the affine transformation T, *i.e.*, to $\tilde{A}, \tilde{B}_a$ for $0 < a < n$. Given that all coefficients but B_0 are zero, all equations which have terms of the form $B_a B_b$ for $a \ne 0, b \ne 0$ on the left hand side are now also zero, *i.e.*, they do not influence the equations of the form $B_i^{q^{\lambda+i}} B_i^{q^i} = \tilde{B}_j^{q^{\lambda+j}} \tilde{B}_j^{q^j}$ for some i, j with $0 \le i, j < n$. We can not assume $i = j$ here as the matrix on the right hand side may have been rotated by a constant

$r \in \mathbb{Z}^+$ with $0 \le r < n$. This is equivalent to the application of a Frobenius transformation. Still, we established that S, T may have only one non-zero coefficient in their univariate representation. Therefore, we know that the big sustainer and the Frobenius sustainer are the only two sustainers applicable to $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic systems of the MIA and the MIO type. □

Unfortunately, the above proof is not valid in the case $q = 2$. The reason is that the equations of type A and Hamming weight 1 are mapped to one type of equation, namely $AB_a^{q^{\lambda+a}} + B_b^{q^b} A^{q^\lambda} + B_{a-1}^{q^{\lambda+a-1}} B_{b-1}^{q^{b-1}} = 0$ for $a + \lambda \equiv b \pmod{n}$. All other powers are also reduced $\pmod{n}$. However, as soon as we assume $A = 0$, the above equation collapses to the original equation of Hamming weight 1, and the rest of the proof is again applicable. Alternatively, we could assume that any $B_i = 0$, and derive a similar proof starting with equations of type B. This leads to the following

Corollary 5.2 *For $q = 2$, the affine transformation S in univariate representation either has all coefficients $A, B_0, \ldots, B_{n-1}$ not equal to zero or exactly one coefficient B_i non-equal to zero and all other coefficients equal to zero. The same condition holds for the coefficients $\tilde{A}, \tilde{B}_0, \ldots, \tilde{B}_{n-1}$ of the transformation T.*

Still, we were not able to derive a contradiction with the assumption that all of the above values are non-equal to zero, so we have to leave the proof for the case $q = 2$ as an open problem. However, due to the very high number of equations of $O(n^2)$ compared to only $O(n)$ free variables, we conjecture that the above lemma also holds for $q = 2$ although we expect a far more technical proof in this case.

6 Conclusions

In this article, we showed through the examples of Hidden Field Equations (HFE), Matsumoto-Imai Scheme A (MIA), Unbalanced Oil and Vinegar schemes (UOV), and Stepwise-Triangular Systems (STS) that $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic systems allow many equivalent private keys and hence have a lot of redundancy in their key spaces. These results have been summarized in tables 1 and 2. The

Table 1: Summary of the reduction results of this article

Scheme (*Section*)	Reduction
UOV (*4.3*)	$q^{n+mn} \prod_{i=0}^{n-m-1}(q^{n-m} - q^i) \prod_{i=0}^{m-1}(q^m - q^i)$
STS (*4.4*)	$q^{m+n} \prod_{i=1}^{L} \left(q^{n_i(n-\sum_{j=1}^{i} n_j)} \prod_{j=0}^{n_i-1}(q^{n_i} - q^j)\right)$ $\prod_{i=1}^{L} \left(q^{m_i(n-\sum_{j=1}^{i} m_j)} \prod_{j=0}^{m_i-1}(q^{m_i} - q^j)\right)$
MIA (*4.2*)	$n(q^n - 1)$
MIA- (*4.2.1*)	$n(q^n - 1)q^r \prod_{i=n-r-1}^{n-1}(q^n - q^i)$
HFE (*4.1*)	$nq^{2n}(q^n - 1)^2$
HFE- (*4.1.1*)	$nq^{2n}(q^n - 1)(q^{n-r} - 1) \prod_{i=n-r-1}^{n-1}(q^n - q^i)$
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*)	$n'q^{r+2n'vn'}(q^{n'} - 1)^2 \prod_{i=0}^{v-1}(q^v - q^i) \prod_{i=n'-r-1}^{n'-1}(q^{n'} - q^i)$

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 $1 \le l \le L$ the number of new variables and equations, respectively.

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 chapter, 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 the existence of the additive sustainers from Section 3.1 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, constructors of new schemes should keep these sustaining transformations in mind: there is no point in having a

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
HFEv	$q = 2, v = 7, n = 107$	21,652	1160
HFEv-	$q = 2, r = 3, v = 4, n = 107$	22,261	1258
MIA	$q = 128, n = 67$	63,784	469
MIA-	$q = 128, r = 11, n = 67$	63,784	6180

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 article 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 $\mathcal{P}$.

We want to stress that the sustainers from Section 3 are probably not the only ones possible. We therefore state as an open problem to look for even more powerful transformations. The only case where we know for certain that we found all sustainers possible, is the MIO/MIA class. The corresponding proof can be found in Section 5. We also state as an open problem to find such proofs for the other schemes discussed in this article. In addition, there are other multivariate schemes which could not be discussed in this article, due to space limitations. We are confident that they can be analysed using similar techniques as outlined in this article but have to leave the concrete proof as an open problem.

References

[BCBP03] Alex Biryukov, Christophe De Cannière, An Braeken, and Bart Preneel. A toolbox for cryptanalysis: Linear and affine equivalence algorithms. In *Advances in Cryptology — EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 33–50. Eli Biham, editor, Springer, 2003.

[BWP05] An Braeken, Christopher Wolf, and Bart Preneel. A study of the security of Unbalanced Oil and Vinegar signature schemes. In *The Cryptographer's Track at RSA Conference 2005*, volume 3376 of *Lecture Notes in Computer Science*. Alfred J. Menezes, editor, Springer, 2005. 13 pages, cf `http://eprint.iacr.org/2004/222/`.

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

[CGP00b] Nicolas Courtois, Louis Goubin, and Jacques Patarin. *Sflash: Primitive specification and supporting documentation*, 2000. `https://www.cosic.esat.kuleuven.be/nessie`, submissions, Sflash, 10 pages.

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

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

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

[DS05] Jintai Ding and Dieter Schmidt. Rainbow, a new multivariable polynomial signature scheme. In *Conference on Applied Cryptography and Network Security — ACNS 2005*, volume 3531 of *Lecture Notes in Computer Science*, pages 164–175. Springer, 2005.

[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/`.

[HWyCL05] Yuh-Hua Hu, Lih-Chung Wang, Chun yen Chou, and Feipei Lai. Similar keys of multivariate quadratic public key cryptosystems. In Yvo Desmedt, Huaxiong Wang, Yi Mu, and Yongqing Li, editors, *Cryptology and Network Security, 4th International Conference, CANS 2005, Xiamen, China, December 14-16, 2005, Proceedings*, volume 3810 of *Lecture Notes in Computer Science*, pages 211–222. Springer, 2005.

[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.

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

[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`.

[KS04] Masao Kasahara and Ryuichi Sakai. A construction of public key cryptosystem for realizing ciphtertext of size 100 bit and digital signature scheme. *IEICE Trans. Fundamentals*, E87-A(1):102–109, January 2004. Electronic version: `http://search.ieice.org/2004/files/e000a01.htm\#e87-a,1,102`.

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

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

[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`.

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

[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`.

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

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

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

[Wol05] Christopher Wolf. *$\mathcal{M}$ultivariate $\mathcal{Q}$uadratic Polynomials in Public Key Cryptography*. Ph.D. thesis, Katholieke Universiteit Leuven, Belgium, November 2005. `http://hdl.handle.net/1979/148`, 156+xxiv pages.

[WP04] Christopher Wolf and Bart Preneel. Asymmetric cryptography: Hidden Field Equations. In *European Congress on Computational Methods in Applied Sciences and Engineering 2004*. P. Neittaanmäki, T. Rossi, S. Korotov, E. Oñate, J. Périaux, and D. 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 PKC [PKC05], pages 275–287. 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.