

Equivalent Keys in Multivariate Quadratic Public Key Systems

Christopher Wolf and Bart Preneel

Communicated by ???

Abstract. Multivariate Quadratic public key schemes have been suggested as early as 1985 by Matsumoto and Imai as an alternative for the RSA scheme. Since then, several 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, *i.e.* the size of the set of possible private and hence public keys can be reduced. 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 Multivariate Quadratic public key systems, we see applications of our results both in cryptanalysis and in memory efficient implementations of \mathcal{MQ} -schemes.

Keywords. Multivariate Quadratic Polynomials, Public Key signature, Hidden Field Equations, Matsumoto-Imai scheme A, C^* , Unbalanced Oil and Vinegar, Stepwise Triangular Systems, Equivalent keys, Post-quantum cryptography.

2010 Mathematics Subject Classification. 14G50 94A60 14G15 11T71 14N10.

1 Outline

In the last 20 years, several schemes based on the problem of Multivariate Quadratic equations (or \mathcal{MQ} for short) have been proposed. The most important ones certainly are MIA / C^* [20] and Hidden Field Equations (HFE, [24]) plus their variations MIA- / C^{*-} , HFE-, HFEv, and HFEv- [16, 23, 24]. Both classes have been used to construct signature schemes for the European cryptography project NESSIE [22], namely the MIA- variation in Sflash [9], the HFEv- variation in

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 contracts IST-2002-507932 ECRYPT and ICT-2007-216676 Ecrypt II.

Quartz [7] and its tweaked version Quartz-7m [32]. Unbalanced Oil and Vinegar schemes [16] and Stepwise Triangular Schemes [31] 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 [36], Tractable Rational Maps [27], or Rainbow [10].

The aim of this article is to systematically study the question of equivalent keys of \mathcal{MQ} -schemes. Therefore, we will concentrate on the four basic classes Matsumoto-Imai Scheme A, Hidden Field Equations, Unbalanced Oil and Vinegar, and Stepwise Triangular System [30, 35]. 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 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 so 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 waste neither computation time nor storage space without any security benefit. The practical relevance of this work has been shown in [3]: even small changes in the \mathcal{MQ} -scheme can have a drastic effect on its running time.

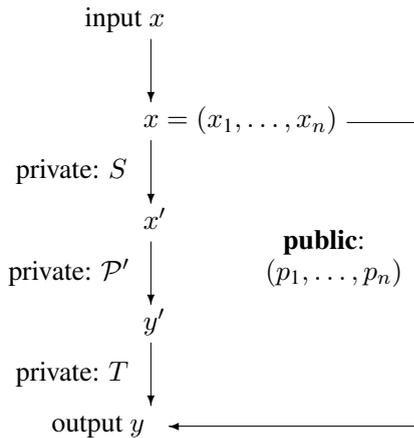


Figure 1. Graphical Representation of the \mathcal{MQ} -trapdoor (S, \mathcal{P}', T)

All systems based on \mathcal{MQ} -equations with $n \in \mathbb{Z}^+$ variables and $m \in \mathbb{Z}^+$ equations are based on finite field \mathbb{F} of size $q := |\mathbb{F}|$ and use a public key of the form

$$y_i := p_i(x_1, \dots, x_n) := \sum_{1 \leq j \leq k \leq n} \gamma_{i,j,k} x_j x_k + \sum_{j=1}^n \beta_{i,j} x_j + \alpha_i \quad (1.1)$$

for $1 \leq i \leq m; 1 \leq j \leq k \leq n$ and $\alpha_i, \beta_{i,j}, \gamma_{i,j,k} \in \mathbb{F}$ (constant, linear, and quadratic terms, respectively). We write the set of all such systems of polynomials as $\mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$. Following the notation of Figure 1, we write the private key as triple (S, \mathcal{P}', T) where $S \in \text{Aff}^{-1}(\mathbb{F}^n), T \in \text{Aff}^{-1}(\mathbb{F}^m)$ are bijective affine transformations. Details on affine transformation are given in Section 2.1. Denoting the binary function composition by \circ we can write the public key as $\mathcal{P} := T \circ \mathcal{P}' \circ S$ for a given private key $(S, \mathcal{P}', T) \in \text{Aff}^{-1}(\mathbb{F}^n) \times \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m) \times \text{Aff}^{-1}(\mathbb{F}^m)$. Changing the point of view, we have $\mathcal{P}' \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$ a polynomial-vector $\mathcal{P}' := (p'_1, \dots, p'_m)$ with m components; each component p'_i is a polynomial in n variables x'_1, \dots, x'_n . Throughout this paper, we will denote components of this private vector \mathcal{P}' by a prime $'$. Going into more detail:

$$y'_i := p'_i(x'_1, \dots, x'_n) := \sum_{1 \leq j \leq k \leq n} \gamma'_{i,j,k} x'_j x'_k + \sum_{j=1}^n \beta'_{i,j} x'_j + \alpha'_i. \quad (1.2)$$

for $1 \leq i \leq m$. Apparently, this is the same structure as for the public key equations (1.1). However, we note that the private key polynomials can be inverted efficiently, while the public key polynomials cannot. Actually, the goal of \mathcal{MQ} -schemes is that this inversion should be hard if the public key \mathcal{P} alone is given. The main difference between \mathcal{MQ} -schemes lies in their special construction of the central equations \mathcal{P}' and consequently the trapdoor they embed into a specific class of \mathcal{MQ} -problems. An introduction to Multivariate Quadratic public key systems is given in [30, 35]. We will cover the different basic classes in Section 4.

1.1 Related Work

In their cryptanalysis of HFE, Kipnis and Shamir report the existence of *isomorphic keys* [19]. A similar observation for Unbalanced Oil and Vinegar Schemes can be found in [16]. 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^* [23]—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 [26] but did not extend his result to other *Multivariate Quadratic* schemes. Additive sustainers will be introduced in Section 3.1. In the case of symmetric ciphers, [2] used a similar idea in the study of S-boxes. A different angle of the idea of equivalent keys can be found in [13] where the authors compute normal forms of the *public* key. Main reason here is to save some memory in the public but particularly in the private key. Using the techniques suggested in [13], the latter can be reduced by up to 50%.

This article is based on the two conference papers [33, 34] which deal with the classes MIA, HFE, and UOV. In this article, the proofs have been extended to the STS class. In addition, a tightness proof for the case of MIA is given.

1.2 Organisation of the Article

This article is organised 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, called *sustaining transformations*, which can be used to generate equivalent keys. These transformations are applied to different variations of *Multivariate Quadratic* 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 Initial 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 2: on the left hand side, you find the private key from Figure 1, on the right hand side, the idea of equivalent keys. In a nutshell, we will insert four affine transformations $\sigma, \sigma^{-1}, \tau, \tau^{-1}$ in between the two transformations S, T and the central polynomial \mathcal{P}' . The symbols σ, τ will be defined rigorously in Definition 2.1. Before continuing, we restrict ourselves to invertible affine and homomorphic transformations and denote them $\text{Aff}^{-1}(\mathbb{F}^n)$ and $\text{Hom}^{-1}(\mathbb{F}^n)$, respectively. Second, we do not only consider ground fields \mathbb{F} of size q but also their corresponding extension field \mathbb{E} of dimension n , i.e. $\mathbb{E} := \text{GF}(q^n)$ and \mathbb{E} is generated by the irreducible polynomial $i(t) \in \mathbb{F}[t]$ of degree n .

For convenience, we first fix an isomorphism between the extension field \mathbb{E} and the vector space \mathbb{F}^n . Both are used in the case of *Multivariate Quadratic* systems.

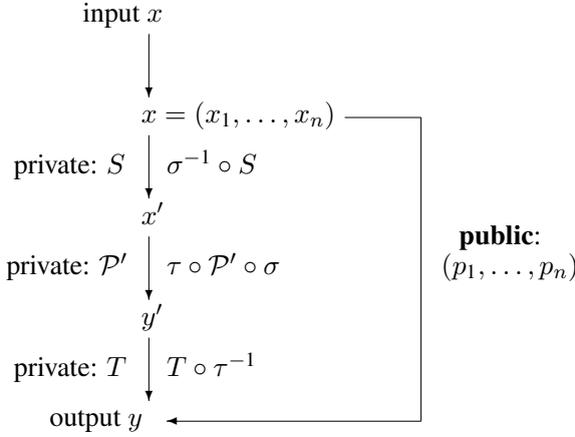


Figure 2. Equivalent private keys using affine transformations σ, τ

To this aim, we observe that all field elements $a \in \mathbb{E}$ have the form

$$a_{n-1}t^{n-1} + \dots + a_1t + a_0 \text{ with } a_i \in \mathbb{F}.$$

In addition, we see that a vector $b \in \mathbb{F}^n$ can be represented as (b_1, \dots, b_n) with $b_i \in \mathbb{F}$.

Definition 2.1. Let \mathbb{E} be an n^{th} degree extension of the ground field \mathbb{F} and \mathbb{F}^n the corresponding vector space. Then we call $\phi : \mathbb{E} \rightarrow \mathbb{F}^n$ with

$$\phi(a) := b \text{ and } b_i := a_{i-1} \text{ for } 1 \leq i \leq n$$

for $a_0, \dots, a_{n-1}, b_1, \dots, b_n \in \mathbb{F}$ as defined above the *canonical bijection* between \mathbb{E} and \mathbb{F}^n .

As the definition of equivalent keys is central for the remainder for this article, we start with an example, namely equivalent keys over the so-called Matsumoto-Imai Scheme A (MIA, see Section 4.1). Let $\mathbb{E} := \text{GF}(q^n)$ be the extension field of dimension n over the ground field \mathbb{F} . Then define the central equation \mathcal{P}' over \mathbb{E} by

$$Y' := X'^{q^\lambda + 1}$$

The rational behind this will become clear in Section 4.1. All we need to know for the moment is that this equation may not change, *i.e.* MIA is defined precisely by this equation—regardless which transformations S or T we choose.

Now consider two non-zero elements $B, C \in \mathbb{E}^*$ and define the corresponding maps $X' \rightarrow BX'$, $X' \rightarrow CX'$. Exploiting commutativity, we can rewrite the central equation of MIA as $C(BX')^{q^\lambda+1} = CB^{q^\lambda+1}X'^{q^\lambda+1}$. Having $C := B^{(q^\lambda+1) \cdot (-1)}$ we obtain $B^{(q^\lambda+1) \cdot (-1)}B^{q^\lambda+1}X'^{q^\lambda+1} = 1 \cdot X'^{q^\lambda+1}$, *i.e.* the two elements (or their corresponding affine transformations) cancel out. Therefore, all keys which are linked by some non-zero $B \in \mathbb{E}^*$ are equivalent. As $B^{(q^\lambda+1) \cdot (-1)}Y'$, BX' are affine transformations, they are readily absorbed into S, T , respectively. We capture the more general notion in the following definitions. Keep in mind that the “shape” of a Multivariate Quadratic system cannot be captured by one general definition. Our definition will therefore depend on the exact \mathcal{MQ} -system we are dealing with. This will become obvious when we deal with the different basic classes MIA, HFE, UOV, and STS in Section 4.

Definition 2.2. We call two private keys

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

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

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

A graphical representation of this idea has been given in Figure 2.

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

Definition 2.3. Let $(S, \mathcal{P}', T) \in \text{Aff}^{-1}(\mathbb{F}^n) \times \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m) \times \text{Aff}^{-1}(\mathbb{F}^m)$, be a private key and consider the four transformations $\sigma, \sigma^{-1} \in \text{Aff}^{-1}(\mathbb{F}^n)$ and $\tau, \tau^{-1} \in \text{Aff}^{-1}(\mathbb{F}^m)$. Moreover, let

$$\mathcal{P} = (T \circ \tau^{-1}) \circ (\tau \circ \mathcal{P}' \circ \sigma) \circ (\sigma^{-1} \circ S). \quad (2.1)$$

We call the pair $(\sigma, \tau) \in \text{Aff}^{-1}(\mathbb{F}^n) \times \text{Aff}^{-1}(\mathbb{F}^m)$ *sustaining transformations* for an \mathcal{MQ} -system if the “shape” of \mathcal{P}' is invariant under the pair (σ, τ) . Another way of saying this is to observe that \mathcal{P}' and $(\tau \circ \mathcal{P}' \circ \sigma)$ have the same “shape” and are hence central equations for the same class of Multivariate Quadratic systems of polynomials. For short, we write $(\sigma, \tau) \bullet (S, \mathcal{P}', T)$ for (2.1) and (σ, τ) sustaining transformations.

Remark 2.4. 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. In the case of MIA (see above), the “shape” is the fact that we have a single monomial with coefficient 1 as the central equation (cf. Section 4.1). In HFE (cf. Section 4.2), it is the bounding degree $d \in \mathbb{Z}^+$ of the polynomial $P'(X') \in \mathbb{E}[X']$. Similar, we can capture the invariant structure of the other Multivariate Quadratic classes UOV and STS, see Sections 4.3 and 4.4, respectively. In our above example, the pair $(BX, B^{-q^\lambda-1}X)$ for $B \in \mathbb{E}^*$ forms the sustaining transformation and hence we have $(BX, B^{-q^\lambda-1}X) \bullet (S, P', T)$. In general and for a pair (σ, τ) sustaining transformations, we are now able to produce equivalent keys for a given private key by $(\sigma, \tau) \bullet (S, P', T)$. A trivial example of sustaining transformations is the identity transformation, *i.e.* to set $\sigma = \tau = id$. This corresponds to the (trivial) fact that each key is equivalent to itself. However, in the general setting of \mathcal{MQ} -schemes, the definition is meaningful.

In some rare cases such as the UOV-class, we will be able to work only with one side, *i.e.* only σ, σ^{-1} or τ, τ^{-q} . This will be marked in the corresponding sections. To fit the above definition, we can think of the pair (σ, id) or (id, τ) instead.

2.1 Affine Transformations and Finite Fields

Given that our main tool to construct equivalent keys are special subclasses of affine transformations, we start with some general observations on them and connect them to the ground field \mathbb{F} and its n -dimensional extension field \mathbb{E} . As we only deal with bijective affine transformations $\text{Aff}^{-1}(\cdot)$ and bijective linear transformations $\text{Hom}^{-1}(\cdot)$ in this article, the following well-known lemma proves useful:

Lemma 2.5. *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} .*

Proof. We observe that we have full choice for the first row vector of our matrix—except the zero-vector. With an inductive argument we see that we have full choice for each consecutive row vector—except the span of the previous row vectors. Hence, we have $(q^n - q^{j-1})$ independent choices for the j^{th} row vector. \square

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

Definition 2.6. Let $M_S \in \mathbb{F}^{n \times n}$ be an $(n \times n)$ matrix and $v_S \in \mathbb{F}^n$ a vector and for $x \in \mathbb{F}^n$ define $S(x) := M_S x + v_S$. We call this the *matrix representation* of the affine transformation S .

Definition 2.7. 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 $1 \leq i, j \leq n$ 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 in \mathbb{F}^n . We call this the *multivariate representation* of the affine transformation S .

Remark 2.8. 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 $1 \leq i, j \leq n$. 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 so-called *univariate representation* over the extension field \mathbb{E} of the transformation S .

Definition 2.9. Let $0 \leq i < n$ and $A, B_i \in \mathbb{E}$. Moreover, let the polynomial $S(X) := \sum_{i=0}^{n-1} B_i X^{q^i} + A$ over \mathbb{E} be an affine transformation. We call this the *univariate representation* of the affine transformation $S(X)$.

The important point here is that $x \rightarrow x^q$ is a linear mapping in the finite field \mathbb{F} and also its extension field \mathbb{E} . Hence, all sums which have only powers of the form x^{q^i} for $0 \leq i < n$ in \mathbb{E} are also linear mappings. A proof of this statement can be found, e.g. in [19]. A more constructive proof is given in the following lemma.

Lemma 2.10. *An affine transformation in univariate representation can be transferred efficiently in multivariate representation and vice versa.*

Proof. As we already know that both the univariate and the matrix representation exist, it is sufficient to give an algorithm to transfer an affine transformation given in one of these representations to the other representation.

We start with the univariate polynomial $P(X) := \sum_{i=0}^{n-1} B_i X^{q^i} + A$ for given $B_i, A \in \mathbb{E}$ and compute a corresponding matrix $M \in \mathbb{F}^{n \times n}$ and a vector $v \in \mathbb{F}^n$. For this purpose, we define $\eta_0 \in \mathbb{F}^n$ the all-zero vector, and $\eta_i \in \mathbb{F}^n : 1 \leq i \leq n$, a vector with its i^{th} coefficient 1, the others 0. Moreover, we use the canonical bijection $\phi : \mathbb{E} \rightarrow \mathbb{F}^n$, cf. Definition 2.1. Now, we compute $v := \phi(P(\phi^{-1}(\eta_0)))$, and $M_i := \phi(P(\phi^{-1}(\eta_i)))$ where the vector $M_i \in \mathbb{F}^n$ denotes the i^{th} column of the matrix M . By construction, we have $\phi(P(X)) = M \cdot \phi(X) + v$ for all $X \in \mathbb{E}$.

The converse computation, i.e. to obtain a polynomial $P \in \mathbb{E}[x]$ of the required form for given matrix $M \in \mathbb{F}^{n \times n}$ and a vector $v \in \mathbb{F}^n$ is a little more difficult. Note that the polynomial P is very sparse as it has only $(n + 1)$ non-zero coefficients. We start with the observation $\phi^{-1}(M \cdot 0 + v) = P(0) = A$, i.e. we have $A := \phi^{-1}(v)$. For the coefficients $B_0, \dots, B_{n-1} \in \mathbb{E}$, it is sufficient to solve the

following matrix equation for given $X_i \in \mathbb{E}, 1 \leq i \leq \lambda$ and $\lambda \geq n$ over the extension field \mathbb{E} :

$$\begin{pmatrix} X_1^{q^0} & X_1^{q^1} & \dots & X_1^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ X_i^{q^0} & X_i^{q^1} & \dots & X_i^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ X_\lambda^{q^0} & X_\lambda^{q^1} & \dots & X_\lambda^{q^{n-1}} \end{pmatrix} \begin{pmatrix} B_0 \\ B_1 \\ \vdots \\ \vdots \\ B_{n-1} \end{pmatrix} = \begin{pmatrix} M.\phi(X_1) \\ M.\phi(X_2) \\ M.\phi(X_3) \\ \vdots \\ \vdots \\ M.\phi(X_\lambda) \end{pmatrix} \quad (2.2)$$

To obtain a unique solution, we need the rank of the above matrix to be equal to n . As it is a $(\lambda \times n)$ -matrix, we can be sure that the rank will not exceed n . Moreover, if the rank is smaller than n , we increase the value of λ , until the matrix has full rank and we obtain a unique solution. This is possible as we have full control on X and hence can make sure that they form a matrix of maximal rank. \square

We note that all computations in this proof can be done in polynomial time: we need matrix multiplications in the ground field \mathbb{F} , and Gauss operations in the extension field \mathbb{E} to solve the above linear equation. Hence, we can transfer efficiently between both representations. Moreover, we do not expect $\lambda \gg n$ in practice; this was confirmed through simulations.

The above lemma is based on [19, Lemmata 3.1 and 3.2] and extends from the linear to the affine case. In addition, the lemma given in [19] does not make use of a probabilistic algorithm to compute the univariate representation from the multivariate one. A more elaborated proof can be found in [30, Lemma 2.2.7].

3 Sustaining Transformations

In this section, we discuss several candidates of sustaining transformations—or actions over \mathbb{F}^n or \mathbb{E} . In particular, we consider their effect on the central transformation \mathcal{P}' .

Before introducing the different sustainers we want to point out that they are all special cases of two different points of views—both justified by Lemma 2.10. In a nutshell, we will deal with affine transformations in univariate or matrix $(S, T, \text{respectively})$.

$$S(X) := \sum_{i=0}^{n-1} B_i X^{q^i} + A \text{ with } A, B_i \in \mathbb{E} \text{ and}$$

$$T(x) := Mx + v \text{ with } M \in \text{Hom}^{-1}(\mathbb{F}^n), v \in \mathbb{F}^n.$$

In both cases, we need the transformation to be invertible. Otherwise, we would violate the corresponding condition on the private key (S, \mathcal{P}', T) .

In the sequel, we will specialise these two transformations and investigate under which circumstances we can use them with specific \mathcal{MQ} -schemes.

The reader may consider this section as a kind of “tool-box”: all transformations here will be used in Section 4. We could have started with explaining the different \mathcal{MQ} -schemes, first. However, this is also circular, as we need to think about the different sustainers before using them in concrete schemes. Hence, we have decided to give one small appetiser on MIA in the previous section, now present all sustainers, and then come to the concrete schemes in Section 4. However, we will point out for each sustainer in which case it can be used.

3.1 Additive Sustainer

For $n = m$, *i.e.* the number of equations is equal to the number of variables, we call the sustaining transformations (σ, τ) *additive sustainers* if we have $\sigma(X) := (X + A)$ and $\tau(X) := (X + A')$ for some elements $A, A' \in \mathbb{E}$. We need $n = m$ as the extension field \mathbb{E} in between S, T will require that the two affine transformations S, T are of equal dimension. To be sustainers, the transformations σ, τ need to keep the shape of the central equations \mathcal{P}' invariant. This is the case for HFE, UOV and STS.

Using the additive sustainer, 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 —or the other way around, depending on our needs.

Remark 3.1. 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 $n \neq m$ now. However, in this case it may happen that we have $a' \in \mathbb{F}^m$ and consequently

$\tau : \mathbb{F}^m \rightarrow \mathbb{F}^m$. Nevertheless, we can still collect all constant terms in the central equations \mathcal{P}' . In particular, this is the case for UOV and STS.

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 $1 \leq i \leq m$ and $1 \leq j \leq n$, both for UOV and STS. 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 $0 \leq i < n$ in HFE.

3.2 Big Sustainer

We now consider multiplication in the (big) extension field \mathbb{E} , *i.e.* we have the actions $\sigma(X) := (BX)$ and $\tau(X) := (B'X)$ for $B, B' \in \mathbb{E}^*$ and call the corresponding sustaining transformations (σ, τ) *big sustainer*. Their effect is to multiply a non-zero element on a field element X and X' , respectively. 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. In particular, we will use the big sustainer for HFE and MIA.

3.3 Small Sustainer

We now consider vector-matrix multiplication over the (small) ground field \mathbb{F} , *i.e.* we define the *small sustainer* as $\sigma(x) := \text{Diag}(b_1, \dots, b_n)x$ and $\tau(x) := \text{Diag}(b'_1, \dots, b'_m)x$ for the non-zero coefficients $b_1, \dots, b_n, b'_1, \dots, b'_m \in \mathbb{F}^*$ and $\text{Diag}(b), \text{Diag}(b')$ 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, \dots, p'_m) . As for the big sustainer, we require non-zero elements, *i.e.* we have $b_i, b'_i \in \mathbb{F}^*$. Not surprisingly, we will use the small sustainer for UOV and STS.

3.4 Permutation Sustainer

For the transformation σ , the *permutation sustainer* permutes input-variables of the central equations while for the transformation τ , it permutes the polynomials of the central equations themselves. We write the corresponding sets of permutations

as S_n and S_m , respectively. 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. It will become useful for STS and UOV—but also for HFEv, *i.e.* Hidden Field Equations with the so-called *vinegar modification*.

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 multiplicative group \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. We call the corresponding sustainer (σ, τ) the *Gauss sustainer*.

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, in particular STS, UOV, and HFEv.

3.6 Frobenius Sustainer

The *Frobenius sustainer* is very useful in the case of HFE and MIA, *i.e.* schemes which combine the vector space \mathbb{F}^n with the extension field \mathbb{E} . We start with a formal definition.

Definition 3.2. Let \mathbb{F} be a finite field with $q := |\mathbb{F}|$ elements and \mathbb{E} its n -dimensional extension. Moreover, let $H := \{i \in \mathbb{Z} : 0 \leq i < n\}$. 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 3.3. *Frobenius transformations are a subgroup in $\text{Hom}^{-1}(\mathbb{F}^n)$. Moreover, they are isomorphic to $(\mathbb{Z}_n, +)$ where $\mathbb{Z}_n := \{0, \dots, n-1\}$ are integers modulo n and "+" is integer addition modulo n .*

Proof. First, Frobenius transformations are linear transformations, so associativity is inherited from them. Second, the set H from Definition 3.2 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

$(\text{Hom}^{-1}(\mathbb{F}^n), \circ)$. In particular, this also corresponds to 0, *i.e.* the neutral element of $(\mathbb{Z}_n, +)$.

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 $a' \in H$. This corresponds to $b \equiv n - a \pmod{n}$ being the additive inverse of $a \in \mathbb{Z}_n$.

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. This is equivalent to the additive closure $c \equiv a + b \pmod{n}$ in \mathbb{Z}_n .

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 $n \leq a + b < 2n$, 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. Moreover, we see that they act like operations in the additive group $(\mathbb{Z}_n, +)$. \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) . For 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 $x^{\text{char}\mathbb{F}}$ is not a linear transformation in \mathbb{F} for $q \neq p$ where p denotes the characteristic of the finite field \mathbb{F} and $q := |\mathbb{F}|$ the number of its elements.

Before moving on, we will investigate the roll of sustaining transformations a bit further, namely by linking them with equivalence relations.

Lemma 3.4. *Let $\sigma \in \text{Aff}^{-1}(\mathbb{F}^n), \tau \in \text{Aff}^{-1}(\mathbb{F}^m)$ be sustaining transformations and two private key pairs $(T, \mathcal{P}', S), (\tilde{T}, \tilde{\mathcal{P}}', \tilde{S}) \in \text{Aff}^{-1}(\mathbb{F}^n) \times \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m) \times \text{Aff}^{-1}(\mathbb{F}^m)$ with $\tilde{T} := T \circ \tau^{-1}, \tilde{\mathcal{P}}' := \tau \circ \mathcal{P}' \circ \sigma$, and $\tilde{S} := \sigma^{-1} \circ S$. We denote with \circ composition of two affine transformations. Consider the subgroups $G \subset \text{Aff}^{-1}(\mathbb{F}^n)$ and $H \subset \text{Aff}^{-1}(\mathbb{F}^m)$ consisting of all sustaining transformations σ and τ , respectively. Now the pair (G, H) produces equivalence relations within the private key space, *i.e.* we have $(T, \mathcal{P}', S) \sim (\tilde{T}, \tilde{\mathcal{P}}', \tilde{S})$ for \sim the equivalence relation with reflexivity, symmetry and transitivity.*

Proof. First, we have reflexivity as the identity transformation is contained in both subgroups (G, H) . Second, we also have symmetry as subgroups are closed under inversion. Third, we have transitivity as subgroups are closed under composition. Therefore, the pair (G, H) partitions the private key space into equivalence classes. \square

Remark 3.5. (i) 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 3.4.

- (ii) In addition, we want to point out that taking a sustainer as a pair $(\sigma, \tau) \in \text{Aff}^{-1}(\mathbb{F}^n) \times \text{Aff}^{-1}(\mathbb{F}^m)$ of transformations is mandatory for some sustainers (e.g. Frobenius sustainer), while other sustainers (e.g. Gauss sustainers) can be used on either side—independent from the other.

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} . Therefore, we are in a case where we may not consider the transformations σ, τ , but only τ . In this new construction, we define the public key equations as $\mathcal{P} := R \circ T \circ \mathcal{P}' \circ S$ where $R : \mathbb{F}^n \rightarrow \mathbb{F}^{n-r}$ 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 Multivariate Quadratic polynomials, respectively. Less loosely speaking, we consider the function $R(x_1, \dots, x_n) := (x_1, \dots, x_{n-r})$, i.e. we neglect the last r components of the vector (x_1, \dots, x_n) . Although this modification looks rather easy, it proves powerful to defeat a wide class of cryptographic attacks against several MQ-schemes, including HFE, e.g. the attack introduced in [11].

For the corresponding sustainer, we consider the sustainer τ and 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 rows of M or v does not affect the result of R (and hence \mathcal{P}). Therefore, we can choose these last r rows without affecting the public key. Inspecting Lemma 2.5, 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} . The corresponding sustainers are in fact all pairs of matrices/vectors changing *only* the last r rows of $M \in \mathbb{F}^{m \times m}$ and $v \in \mathbb{F}^m$.

Table 1. Summary of the Sustaining Transformations

Name	Form	From	Choices
Additive Sustainer	$X + A$ $x + a$	$A \in \mathbb{E}$ $a \in \mathbb{F}^n$	q^n
Big Sustainer	BX	$B \in \mathbb{E}^*$	$q^n - 1$
Small Sustainer	$\text{Diag}(b_1, \dots, b_n)x$	$x \in \mathbb{F}^n$, $b_1, \dots, b_n \in \mathbb{F}^*$	$(q - 1)^n$
Permutation Sustainer	$\pi(x)$	$x \in \mathbb{F}^n$, $\pi \in S_n$	$n!$
Frobenius Sustainer	X^{q^i}	$X \in \mathbb{E}$, $0 \leq i < n$	n
Reduction Sustainer	$R(x) \rightarrow (x_1, \dots, x_{n-1})$	$x \in \mathbb{F}^n$, $0 < r \leq n$	$q^r \prod_{i=n-r-1}^{n-1} (q^n - q^i)$

In a slight abuse of notation, we will write $R \in \text{Aff}^{-1}(\mathbb{F}^n, \mathbb{F}^{n-r})$ to capture the fact that the matrix M has full rank.

When applying the reduction sustainer τ 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 for MIA-, and HFE-.

3.8 Summary of Sustainers

After having introduced all different sustainer classes, we will quickly summarise them (except the Gauss Sustainer, cf. Table 1). In particular, we will point out, how many choices they give us individually and in which scheme we can use them.

4 Application to Multivariate Quadratic Schemes

Having all necessary tools at hand, we now show how to apply suitable sustaining transformations to the Multivariate Quadratic 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 4.1, we know that only the big sustainer and the Frobenius sustainer can be applied here.

4.1 Matsumoto-Imai Scheme A

We start with the Matsumoto-Imai Scheme A class (MIA) as it allows for the easiest proofs. In particular, we have already used MIA as a short example in Section 1. We recall that MIA uses both a finite field \mathbb{F} and an extension field \mathbb{E} . However, the choice of the central equation is quite restrictive as we only have one monomial here.

Definition 4.1. 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, we have to preserve the coefficient of the monomial $X'^{q^\lambda + 1}$, i.e. we are not allowed to change it to some other element of the extension field \mathbb{E} . As we will see in Section 4.1, the only sustainers suitable here are the big sustainer, see Section 3.2, and the Frobenius sustainer from Section 3.6.

Remark 4.2. In the paper [20], MIA was introduced under the name C^* . Moreover, it used the branching modifier [35, 4.4] by default. As branching has been attacked very successfully, C^* has been used without this modification for any later construction, e.g. [5, 6, 8, 9]. However, without the branching condition, the “new” scheme C^* coincides with the previously suggested “Scheme A” from [14]. 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 [35].

Theorem 4.3. For $K := (S, P', T) \in \text{Aff}^{-1}(\mathbb{F}^n) \times \mathbb{E}[X'] \times \text{Aff}^{-1}(\mathbb{F}^n)$ a private key in MIA we have at least

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

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 starting with S in univariate representation. Without loss of generality, let $B := S(1)$ be a non-zero coefficient with 1 being the one-element of the extension field \mathbb{E} . If $B = 0$ set $B := S(0)$ with 0 being the zero-element of the extension field \mathbb{E} . As $S(\cdot)$

is a bijection, at least one of these values must be non-zero. Applying $\sigma^{-1}(X) := B^{-1}X$ will lead to 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

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

where \tilde{S} is in normal form. Note that we cannot choose the transformations σ and τ independently: each choice of σ implies a particular τ and vice versa.

Next step is to apply the Frobenius sustainer and to compute one special normal form of S . Therefore, fix the transformation \tilde{S} in matrix form, and consider the following n applications of the Frobenius sustainer: $\mathfrak{S} := \{\tilde{S}^{q^0}, \tilde{S}^{q^1}, \dots, \tilde{S}^{q^{(n-1)}}\}$. We now need to do two things: First we need to show that we have indeed n distinct elements and second, we need to single out one of them as normal form. For the first, we consider $\tilde{S}^{q^a}, \tilde{S}^{q^b} \in \mathfrak{S}$ and assume $\tilde{S}^{q^a} = \tilde{S}^{q^b}$. This leads to $\tilde{S} = \tilde{S}^{q^b/q^a} = \tilde{S}^{q^{b-a}}$ and hence $q^0 = q^{b-a} \Rightarrow b = a$. Hence, all n elements are distinct. For the second, use a bijection between $\mathbb{F}^n \leftrightarrow \{0, \dots, q^n - 1\}$ and usual ordering in the integers. We can now pick the maximal \tilde{S}^{q^c} for $0 \leq c < n$ from the set \mathfrak{S} by interpreting each element as vector in \mathbb{Z}^n . Therefore, we have computed one distinct normal form for the initial transformation S . Again, we need to “repair” $X'^{q^\lambda+1}$ by applying an inverse Frobenius sustainer to T and hence have

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

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

We want to point out that there is also a variation of MIA defined over *odd* characteristic. This variation has been suggested in [35, 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, so the above proof also applies to MIO.

Remark 4.4. Patarin observed that it is possible to derive equivalent keys by changing the monomial P' [23]. 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 [34]; 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 [12]. Hence, having S, T affine instead of linear does not enhance the overall security of MIA.

For $q = 128$ and $n = 67$, we obtain $\approx 2^{475}$ equivalent private keys per class. The number of choices for S, T is $\approx 2^{63,784}$ in this case.

Tightness for MIA and MIO

All theorems in this 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 prove that for the MIA/MIO class from above, the big sustainer and the Frobenius sustainer are actually the *only* possible way to achieve equivalent keys for MIA and MIO—as long as we keep the value of λ fixed. As λ is a system parameter and cannot be changed by the user, this restriction is justified. 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 2.2 restricts us to affine transformations to transfer one private key into another. Hence we have the following equation:

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

which we can rewrite as

$$X^{q^\lambda+1} \circ S^{-1} = T \circ X^{q^\lambda+1}. \quad (4.1)$$

We know from Section 2.1 that affine transformations form a group. Moreover, we can use Definition 2.9 to obtain a univariate representation for any given affine transformation. We can hence express (4.1) 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 [19] or the proof of Lemma 2.10. This yields

$$\begin{pmatrix} A^{q^\lambda+1} & AB_0^{q^\lambda} X^{q^\lambda} & AB_1^{q^\lambda} X^{q^\lambda+1} & \dots & AB_{n-1}^{q^\lambda} X^{q^\lambda+n-1} \\ B_0 A^{q^\lambda} X & B_0^{q^\lambda+1} X^{q^\lambda+1} & B_0 B_1^{q^\lambda} X^{q^\lambda+1+1} & & B_0 B_{n-1}^{q^\lambda} X^{q^\lambda+n-1+1} \\ B_1 A^{q^\lambda} X^q & B_1 B_0^{q^\lambda} X^{q^\lambda+q} & B_1^{q^\lambda+1} X^{q^\lambda+1+q} & \dots & B_1 B_{n-1}^{q^\lambda} X^{q^\lambda+n-1+q} \\ \vdots & & \vdots & \ddots & \vdots \\ B_{n-1} A^{q^\lambda} X^{q^{n-1}} & B_{n-1} B_0^{q^\lambda} X^{q^\lambda+q^{n-1}} & B_{n-1} B_1^{q^\lambda} X^{q^\lambda+1+q^{n-1}} & \dots & B_{n-1}^{q^\lambda+1} X^{q^\lambda+n-1+q^{n-1}} \end{pmatrix} \\ \equiv \begin{pmatrix} \tilde{A} & 0 & \dots & 0 \\ 0 & \tilde{B}_0 X^{q^\lambda+1} & 0 & 0 \\ & 0 & \tilde{B}_1 X^{q^\lambda+1+q} & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \tilde{B}_{n-1} X^{q^\lambda+n-1+q^{n-1}} \end{pmatrix} (*)$$

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 $(q^n - 1)$. Therefore, the above equation is modulo X^{q^n-1} . This is expressed by the “ \equiv ” sign.

In addition, we will not use the matrix equation above directly. Instead, we will combine them according to the powers of X . For example, $AB_0^\lambda X^{q^\lambda} = 0$ and $A^{q^\lambda} B_\lambda X^{q^\lambda} X^{q^\lambda} = 0$ are combined into one equation $AB_0^{q^\lambda} X^{q^\lambda} + A^{q^\lambda} B_\lambda X^{q^\lambda} = 0$. Technically, we collect terms of same powers of X . The structure of the matrix shows, that this will only happen twice for each given power of X (once each row and once each column).

Lemma 4.5. *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 $0 \leq i < n$ except one are zero. Note that $B_0 = \dots = B_{n-1} = 0$ implies $S(X) = A$ for any input $X \in \mathbb{E}$ and some fixed $A \in \mathbb{E}$. Hence we need some $B_i \neq 0$ as $S(X) = A$ is not a bijection anymore and this violates our initial assumption about S . 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 $n \geq 2$.

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

$0 \leq a, b, c, d, \lambda < n$ in the sequel. We collect coefficients of monomials of the same degree and distinguish the following three types of equations from (*):

- (i) Equations of the form $AB_a^{q^\lambda} + B_bA^{q^\lambda} = 0$ 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 $0 \leq b < n$.
- (ii) Equations of the form $B_a^{q^\lambda}B_b = 0$ 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 $0 \leq b < n$. As we have $q > 2$ there is no reduction of the power here.
- (iii) Equations of the form $B_a^{q^\lambda}B_b + B_c^{q^\lambda}B_d = 0$ with the following conditions on their powers: first, we have $a \neq b, c \neq d$, 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 symmetric, i.e. (c, d) is the dual of (a, b) . We call these *equations of type B*.

There is a subtle point in the analysis above: We need to make sure that our distinction between the three kind of equations is actually "tight" in a sense that they do not mix. We will therefore inspect them one by one and determine why they cannot mix. In a nutshell, we therefore need to concentrate on the exponents of X .

First, we see that *equations of type A* always have an exponent of the form q^a for $0 \leq a < n$. Obviously, this makes them distinct from *equations of type B*, where we have an exponent of the form $q^b + q^c$ for $0 \leq b, c < n$ and $b \neq c$. As we reduce both by $(q^n - 1)$, we cannot mix these exponents. Second, we inspect the *equations of Hamming weight 1*. Here, we have exponents of the form $2q^d$ for $0 \leq d < n$, which obviously brings them very close to an *equation of type B*. However, as we have $q > 2$, there is no pair $(a, d) \in \mathbb{N}^2$ with $0 \leq a, d < n$ and $q^a = 2q^d$. Moreover, we cannot bring them in a form $q^b + q^c$ as we have $b \neq c$ for *equations of type B*. Hence, we see that the three cases are clearly distinct.

In addition, 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.

We know from the argument above that there must be at least one non-zero coefficient in $S(x)$. Without loss of generality, we assume that this is B_0 . Our goal is now to show that all coefficients B_i for $1 < i < n$ are zero, as is $A = 0$. We start with inspecting the equation $B_0^{q^\lambda} B_\lambda = 0$ of *Hamming weight 1* and we see that it implies $B_\lambda = 0$ as we have $B_0 \neq 0$ (see above). In addition, this implies $A = 0$ as we have $AB_0^{q^\lambda} + B_\lambda A^{q^\lambda} = 0$ as an equation of type A. For $n = 2$, we are done. For $n \geq 3$, we can now use all *equations of type B* of the form $B_0^{q^\lambda} B_b + B_c^{q^\lambda} B_\lambda = 0$. We notice that we need to meet the following conditions: $b \neq 0, \lambda$ and $c \neq 0, \lambda$ but $c + \lambda \equiv b \pmod{n}$. We see that we can construct pairs (b, c) meeting these conditions for all $b \in \mathbb{Z}/n\mathbb{Z} \setminus \{0, \lambda, 2\lambda\}$ with $0 < b < n$. Using the above equation we have established that all coefficients $B_b = 0$ as $B_0 \neq 0$ and $B_\lambda = 0$. Note that $\lambda \not\equiv 2\lambda \pmod{n}$ as we have $0 < \lambda < n$. Moreover, $2\lambda \equiv 0 \pmod{n}$ 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. In fact, this is even true for any even multiple of lambda, *i.e.* we can exclude all cases $2k\lambda \equiv 0 \pmod{n}$ for $k \in \mathbb{N}$. We use the condition $\gcd(q^n - 1, q^\lambda + 1) = 1$ for MIA and $\gcd(q^n - 1, q^\lambda + 1) = 2$ for MIO to show that $2k\lambda = n$ is impossible. To this aim we observe that $(q^{2k\lambda} - 1) = (q^\lambda + 1) \sum_{i=0}^{2k-1} ((-1)^{i+1} q^{i\lambda})$, *i.e.* the gcd condition is violated for $n = 2k\lambda$.

All left to show is that the coefficient $B_{2\lambda}$ is also equal to zero. To this aim, we use the equation $B_\lambda^{q^\lambda} B_{2\lambda} = 0$ of *type Hamming weight 1*. As we have $B_\lambda \neq 0$, this implies $B_{2\lambda} = 0$.

We have now established that all coefficients $A = B_1 = \dots = B_{n-1} = 0$. Using the equations on the diagonal, these conditions also propagate through to the coefficients of the affine transformation T . It is tempting to conclude that $\tilde{B}_0 \neq 0$. However, this is not true in general as the matrix on the right hand side may have been rotated by a constant $r \in \mathbb{Z}^+$ with $0 \leq r < n$. This is equivalent to the application of a Frobenius transformation. Still, we established that S, T may have only one non-zero coefficient each in their univariate representation. Therefore, we know that the big sustainer and the Frobenius sustainer are the only two sustainers applicable to Multivariate Quadratic systems of the MIA and the MIO type. \square

From a cryptographic point of view, we are done. To the knowledge of the authors, no scheme with $q = 2$ has ever been suggested in the context of MIA. Typical choices for q are 128, 256 or $65536=2^{16}$. Hence, it is enough that the above proof deals only with the case $q > 2$. However, from a mathematical point of view this is not satisfactory as the case $q = 2$ is technically allowed for MIA. The reason that the above proof fails is that equations of type A and Hamming weight 1 are

mapped to one type of equation, namely $AB_a^{q^\lambda} + B_bA^{q^\lambda} + B_{a-1}^{q^\lambda}B_{b-1} = 0$ 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 4.6. *For $q = 2$, the affine transformation S in univariate representation either has all coefficients A, B_0, \dots, 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 $\tilde{A}, \tilde{B}_0, \dots, \tilde{B}_{n-1}$ of the transformation T .*

Alas, we are not able to prove a general statement for $q = 2$ as the following counter example shows. Let $n > 3$ and $B_i = c$ for some $c \in \mathbb{E}^*$ and $0 \leq i < n$. This implies that the equations of Hamming weight 2 are trivially true. Now all equations of type A and Hamming weight 1 become true for $A \in \mathbb{E}$ with

$$A^{2^\lambda}c + Ac^{2^\lambda} + c^{2^\lambda+1} = 0.$$

These equations become possible as we do no longer have a clear distinction between the three types of equations for $q = 2$.

Note that this tightness proof is the *only* tightness proof we are aware of for the number of equivalent keys of \mathcal{MQ} -schemes. In particular, the equations for all other schemes (see below) become far too complicated and are hence not useful to construct similar implication chains as above.

MIA-

The following section deals with MIA-, *i.e.* the original MIA scheme and apply the minus modification from Section 3.7. For example, this has been used in the Sflash scheme.

Theorem 4.7. *Let $r \in \mathbb{Z}^+$ be the reduction number and $K := (S, P', T) \in \text{Aff}^{-1}(\mathbb{F}^n) \times \mathbb{E}[X] \times \text{Aff}^{-1}(\mathbb{F}^n)$ a private key in MIA. Then we have*

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

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. \square

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} [9].

4.2 Hidden Field Equations

We continue with the Hidden Field Equations class (HFE) as it is very similar to MIA. The Hidden Field Equations (HFE) have been proposed by Patarin [24]. Its main characteristic is the exceptional low degree of the central polynomial $P'(X') \in \mathbb{E}[X']$. In contrast to MIA, we do not have a degree in the range of q^n but some $d \ll q^n$. In fact, this is the first part of the “shape” of HFE. The second part is to restrict the choice of $P'(X')$ to quadratic terms at most as we will see in the definition below.

Definition 4.8. Let \mathbb{E} be a finite field and $P'(X')$ a polynomial over \mathbb{E} . Moreover, let $i, j, k \in \mathbb{Z}^+$ and $i < j$ for $q = 2$ and $i \leq j$ otherwise. For

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

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

and a degree $d \in \mathbb{Z}^+$, 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 $\mathbb{F} = \text{GF}(2)$ can be found in [21].

It has been elaborated and further extended in [30, Section 2.4]. Polynomials of cubic and higher degree have been discussed in [19, 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 a private key of HFE is in particular this degree d of the private polynomial P' . In contrast, there are no restrictions on its coefficients $C'_{i,j}, B'_k, A' \in \mathbb{E}$ for $i, j, k \in \mathbb{Z}^+$ and $q^i + q^j, q^k \leq d$ as they are all drawn at random. 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. In addition, we can also apply the Frobenius sustainer here.

Theorem 4.9. *For $K := (S, P', T) \in \text{Aff}^{-1}(\mathbb{F}^n) \times \mathbb{E}[X'] \times \text{Aff}^{-1}(\mathbb{F}^n)$ a private key in HFE, we have*

$$n \cdot q^{2n} (q^n - 1)^2$$

equivalent keys.

Proof. To prove this theorem, we consider normal forms of the private keys by bringing the affine transformations $S, T \in \text{Aff}^{-1}(\mathbb{F}^n)$ into a special form. In the proof, we will do the following (sketch): first, we use the additive sustainer to transfer the constant parts of S, T to the central polynomial $P'(X')$. Second, we force the first column of the matrix in S, T to become the one-vector $(1, 0, \dots, 0) \in \mathbb{F}^n$ and third, we apply the Frobenius sustainer to shift the largest row vector in the matrix form of $S(X)$ into row 1.

We first apply steps one and two to the affine transformation S . Let $\tilde{S}(X)$ be the affine transformation of the initial key. 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, as $\hat{S} : \mathbb{E} \rightarrow \mathbb{E}$ is a bijection, we observe that $\hat{S}(1)$ is non-zero, *i.e.* by applying the big sustainer, we can define $\bar{S}(X) := \hat{S}(X) \cdot \hat{S}(1)^{-1}$. Hence, we have $\bar{S}(1) = 1$, *i.e.* we add a new fix-point but still keep the old fix-point as we have $\bar{S}(0) = \hat{S}(0) = 0$. When viewing the affine transformation $\bar{S}(X)$ in matrix form, this is equivalent to fixing the first column to the one-vector. We apply the same steps to transformation T and obtain \bar{T} accordingly.

Third, we consider the Frobenius transformation $X \rightarrow X^{q^c}$ for $c = 0..(n-1)$ on $\bar{S}(X)$ and obtain the following n transformations $\{\bar{S}(X)^{q^0}, \dots, \bar{S}(X)^{q^{n-1}}\}$. Using a similar argument as in Theorem 4.3 we see that we derive n distinct matrices $\bar{S}(X)^{q^i}$ for $0 \leq i \leq n$. By interpreting the first *row* vector as an integer (*e.g.* as a bit-string for fields of even characteristic), we can identify the value i which leads to the *maximal* transformation $\bar{S}(X)^{q^i}$, using usual integer ordering. Denote

this transformation by $\dot{S}(X) := \overline{S}(X)^{q^i}$. To cancel the effect of the Frobenius sustainer, we define $\dot{T}(X) := \overline{T}(X)^{q^{n-i}}$.

There are two remarks to make: first, the maximal transformation $\overline{S}(X)^{q^i}$ is unique as $\overline{S}(X)$ is an invertible transformation. If two transformations had the same row vector, these row vectors would obviously be linearly dependent which violates invertibility of $\overline{S}(X)$. Second, we need to consider row vectors here instead of column vectors as the first column vector is fixed to one. Hence, we would never obtain the identity transformation $X \rightarrow X^{q^0}$ in this step and therefore obtain a (wrong) smaller count for the number of equivalent keys.

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 $n \cdot q^{2n} \cdot (q^n - 1)^2$ this way as we have

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

□

A weaker version of the above theorem can be found in [34].

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 [24].

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 4.10. *Let $r \in \mathbb{Z}^+$ be a reduction parameter and $K := (S, P', T) \in \text{Aff}^{-1}(\mathbb{F}^n) \times \mathbb{E}[X] \times \text{Aff}^{-1}(\mathbb{F}^n)$ a private key in HFE. Then we have*

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

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 4.9 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 $n \cdot q^n (q^n - 1)$ keys here.

For the affine transformation T , we also have to take the reduction sustainer into account: we use $\tilde{T}(X) : \mathbb{F}^n \rightarrow \mathbb{F}^{n-r}$ 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 $\tilde{\mathbb{E}} := \text{GF}(q^{n-r})$ 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 $T : \mathbb{F}^n \rightarrow \mathbb{F}^n$ 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. \square

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 [32].

HFEv

Another important variation of Hidden Field Equations is HFEv. In particular, it was used in the signature scheme Quartz [7]. HFEv was introduced in [16]. The HFEv scheme is characterised in the following definition.

Definition 4.11. 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 $(z'_1, \dots, z'_v) := s_{n-v+1}(x_1, \dots, x_n), \dots, s_n(x_1, \dots, x_n)$ be the vinegar variables for s_i the polynomials of $S(x)$ in multivariate representation and $X' := \phi^{-1}(x'_1, \dots, x'_{n'})$, using the canonical bijection $\phi^{-1} : \mathbb{F}^n \rightarrow \mathbb{E}$ and $x'_i := s_i(x_1, \dots, x_n)$ for $1 \leq i \leq n'$ as

hidden variables. Then define the central equation as

$$\begin{aligned}
 P'_{z'_1, \dots, z'_v}(X') &:= \sum_{\substack{0 \leq i, j \leq d \\ q^i + q^j \leq d}} C'_{i,j} X'^{q^i + q^j} + \sum_{\substack{0 \leq k \leq d \\ q^k \leq d}} B_k(z'_1, \dots, z'_v) X'^{q^k} \\
 &\quad + A'(z'_1, \dots, z'_v)
 \end{aligned}$$

for $C'_{i,j} \in \mathbb{E}$ are the
 quadratic terms,
 for $B'_k(z'_1, \dots, z'_v)$ depending
 linearly on z'_1, \dots, z'_v and
 for $A'(z'_1, \dots, z'_v)$ depending
 quadratically on z'_1, \dots, z'_v

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

The condition that the $B'_k(z'_1, \dots, z'_v)$ are affine functions (*i.e.* of degree 1 in the z'_i at most) and $A'(z'_1, \dots, z'_v)$ is a quadratic function over \mathbb{F} ensures that the public key is still quadratic over \mathbb{F} .

Theorem 4.12. *Let $v \in \mathbb{Z}^+$ be the number of vinegar variables, \mathbb{E} an \tilde{n} -dimensional extension of \mathbb{F} where $\tilde{n} := n - v = m$ and $K := (S, P', T) \in \text{Aff}^{-1}(\mathbb{F}^m) \times \mathbb{E}[X'] \times \text{Aff}^{-1}(\mathbb{F}^m)$ be a private key in HFEv. Then we have*

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

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 $q^m \cdot (q^m - 1) = q^{\tilde{n}} \cdot (q^{\tilde{n}} - 1)$ 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 4.9 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 $(q^{\tilde{n}} - 1)$. In addition, we apply the Frobenius sustainer to the HFE component, which yields an additional factor of \tilde{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. \square

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 $\approx 2^{21,652}$.

HFE_v-

Here, we combine both the HFE_v and the HFE- modification to obtain HFE_v-. In fact, the original Quartz scheme [7] was of this type.

Theorem 4.13. *Let $v \in \mathbb{Z}^+$ be vinegar variables, $r \in \mathbb{Z}^+$ a reduction parameter and \mathbb{E} an \tilde{n} -dimensional extension of \mathbb{F} where $\tilde{n} := n - v$ and $\tilde{n} = m + r$.*

Moreover, let $K := (S, P', T) \in \text{Aff}^{-1}(\mathbb{F}^n) \times \mathbb{E}[X'] \times \text{Aff}^{-1}(\mathbb{F}^{\tilde{n}}, \mathbb{F}^{\tilde{n}-r})$ be a private key in HFEv- shape. Then we have a total of

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

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-. In total, we obtain the following factors

- \tilde{n} for the Frobenius sustainer,
- $(q^{\tilde{n}} - 1)^2$ for two non-zero elements $A, B \in \mathbb{E}^*$ to be absorbed into S, T , respectively,
- $q^{2\tilde{n}+v\tilde{n}} \prod_{i=0}^{v-1} (q^v - q^i)$ for the vinegar variables (cf. Thm. 4.12), which are absorbed into the central equations, and
- $q^r \prod_{i=\tilde{n}-r-1}^{\tilde{n}-1} (q^{\tilde{n}} - q^i)$ for the minus modification (cf. Thm. 4.10)

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. \square

For the case $q = 2, r = 3, v = 4$ and $n = 107, \tilde{n} = 103$, 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 [7], as submitted to NESSIE [22].

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 $S \in \text{Aff}^{-1}(\mathbb{F}^n)$. To fit in our framework, we set it to be the identity transformation, *i.e.* we have $T := \tau := id$. UOV were proposed in [16].

Definition 4.14. 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:

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

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 then 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 does not mix vinegar variables into the oil variables.

Theorem 4.15. *Let $K := (S, \mathcal{P}', id) \in \text{Aff}^{-1}(\mathbb{F}^n) \times \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m) \times \text{Aff}^{-1}(\mathbb{F}^m)$ 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 :

$$R := \left(\begin{array}{cc|c} I_m & 0 & A_m \\ 0 & I_{n-2m} & B_m^{n-2m} \\ \hline 0 & 0 & I_m \end{array} \right).$$

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 $B_m^{n-2m} \in \mathbb{F}^{(n-2m) \times m}$. Note that the right column of R corresponds to the oil-space in UOV, *i.e.* a linear transformation that separates out the oil variables from the vinegar variables. If we can do this separation, we have broken UOV (*e.g.* with extended the Shamir-Kipnis attack). Hence, it is not surprising that we find this artefact in our study of equivalent keys.

In addition, we have an asymmetry between the oil- and the vinegar-space: While we can absorb the vectors generating the vinegar space into the coefficients

of the vinegar cross vinegar terms, we cannot do so for the vectors generating the oil space as the corresponding coefficients are zero. Hence, the matrix R is one big identity matrix for the vinegar variables (I_m and I_{n-2m}), and a set of m linearly independent vectors A_m, B_m^{n-2m}, I_m for the oil variables.

Now, each possible matrix R leads to the same number of equivalent keys for a central equation \mathcal{P}' in UOV shape. Let

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

be an $(n \times n)$ -matrix. Here, we require that the matrices $F_m \in \mathbb{F}^{m \times m}$ and $H_{n-m} \in \mathbb{F}^{(n-m) \times (n-m)}$ are invertible and hence the counting from Lemma 2.5 applies. For $G_{n-m}^m \in \mathbb{F}^{m \times (n-m)}$, we have no restrictions. As we used the equation $E \circ R = S$, we define the transformation as $\sigma(x) := E^{-1}x$ where $x \in \mathbb{F}^n$. Note that these transformations σ form a subgroup within the affine transformations. So we have

$$(E^{-1}x + a, id) \bullet (S, \mathcal{P}', id) \text{ for } a \in \mathbb{F}^n \text{ and } E \text{ as defined above.}$$

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

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 [17].

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 generalised triangular structure, hence the name of these schemes. We capture this intuition more formally below. Stepwise Triangular Schemes were introduced in [31].

Definition 4.16. Let $n_1, \dots, n_L \in \mathbb{Z}^+$ be L integers such that $n_1 + \dots + n_L = n$, the number of variables, and $m_1, \dots, m_L \in \mathbb{Z}^+$ such that $m_1 + \dots + m_L = m$, 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 $1 \leq \ell \leq L$. 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 Multivariate Quadratic polynomials such that the m_ℓ private quadratic polynomials $p'_{m_0+\dots+m_{\ell-1}+1}, \dots, p'_{m_0+\dots+m_\ell}$ of each layer ℓ contain only the variables x'_k with $k \leq \sum_{j=1}^{\ell} n_j$, i.e. only the variables defined in all previous steps plus n_ℓ new ones. Then we call $(S, \mathcal{P}', T) \in \text{Aff}^{-1}(\mathbb{F}^n) \times \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m) \times \text{Aff}^{-1}(\mathbb{F}^m)$ a private key in *Stepwise Triangular System* shape. If $n_1 = \dots = n_L = m_1 = \dots = m_L = r$ 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, \dots, 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 $1, \dots, \ell$, i.e. we may also perform Gauss operations on these previous layers, as long as the result only affects the given layer ℓ .

Theorem 4.17. *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 $(n_1, \dots, n_L) \in (\mathbb{Z}^+)^L$ be a vector of integers such that $n_1 + \dots + n_L = n$ and $m_1, \dots, m_L \in \mathbb{Z}^+$ integers such that $m_1 + \dots + m_L = m$. Then for $K := (S, \mathcal{P}', T) \in \text{Aff}^{-1}(\mathbb{F}^n) \times \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m) \times \text{Aff}^{-1}(\mathbb{F}^m)$ 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 $S \in \text{Aff}^{-1}(\mathbb{F}^n)$ and $T \in \text{Aff}^{-1}(\mathbb{F}^m)$ to obtain the fix point $S(0) = T(0) = 0$. As a result, we obtain a factor of q^{m+n} and may assume $S \in \text{Hom}^{-1}(\mathbb{F}^n)$ and $T \in \text{Hom}^{-1}(\mathbb{F}^m)$ for the remainder of this proof.

As in the proof of Theorem 4.15, we impose a special structure on the linear

transformation S . Therefore, we consider the matrix

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

as normal form. 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 , *i.e.* by choosing the A_{n_i} accordingly, we obtain M_S as defined above for a given matrix E . Moreover, for each choice of E , we obtain another linear transformation S and hence, M_S is a normal form of S .

Using Lemma 2.5, 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 $S \in \text{Hom}^{-1}(\mathbb{F}^n)$. 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. \square

Corollary 4.18. *For regular STS with step-width $r \in \mathbb{Z}^+$, $L \in \mathbb{Z}^+$ layers and $n := Lr$ variables, the above formula simplifies to*

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

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 [15].

4.5 Effects on the Public Key Space

Obviously, the reductions given above have an effect on the *private* key space, *i.e.* the number of private keys. In a slight abuse of notation, the size can be expressed as

$$q^n \prod_{i=0}^{n-1} (q^n - q^i) \cdot |\mathcal{P}'| \cdot q^m \prod_{i=0}^{m-1} (q^m - q^i) \quad (4.2)$$

for the number of invertible affine transformations over $\mathbb{F}^n, \mathbb{F}^m$ and the number of possible central equations keys written as $|\mathcal{P}'|$. Note that the number of different private keys \mathcal{P}' depends on the actual scheme. For example for MIA, we only have one specific \mathcal{P}' for each given parameter $\lambda \in \mathbb{N}$ —and λ is supposed to be publicly known. In case of HFE, and with a total of $c \in \mathbb{N}$ non-zero coefficients, we have $|\mathcal{P}'| = q^n c$ as we can pick random elements from the extension field \mathbb{E} for all monomials of the form $X^{q^i+q^j}, X^{q^i}, 1$ up to a certain degree $d \in \mathbb{N}$.

When computing the size of the *public* key space, *i.e.* the number of different elements of $\mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$, we need to remember that each public key is computed as

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

Hence, computing $|\mathcal{P}|$ is at first glance equivalent to (4.2). However, taking the idea of equivalent keys into account we see that this is actually wrong: as each public key could have been computed by $\rho \in \mathbb{N}$ different private keys. So to avoid double counting, we need to reformulate (4.2) using a reduction factor ρ .

$$q^n \prod_{i=0}^{n-1} (q^n - q^i) \cdot |\mathcal{P}'| \cdot q^m \prod_{i=0}^{m-1} (q^m - q^i) / \rho. \quad (4.3)$$

Hence, both the private *and* the public key space are reduced by ρ . This is still true, even when assuming that an attacker will only obtain a copy of the public key $\mathcal{P} \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$. Given that all reductions given in this article are *equivalence relations*, we do not need to distinguish different cases and can actually divide by only one factor ρ per scheme. Moreover, the result of (4.3) is an integer.

5 Conclusions

In this article, we showed through the examples of Matsumoto-Imai Scheme A (MIA), Hidden Field Equations (HFE), Unbalanced Oil and Vinegar schemes (UOV), and Stepwise-Triangular Systems (STS) that Multivariate Quadratic systems allow many equivalent private keys and hence have a lot of redundancy in their key spaces. These results have been summarised in tables 2 and 3. The first gives an overview on the formulae achieved while the latter features some numerical examples. The symbols used in Table 2 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} , $v \in \mathbb{Z}^+$ the number of vinegar variables, $\tilde{n} \in \mathbb{Z}^+$ the number of equations including vinegar variables, L the number of layers for STS, and n_i, m_i for $1 \leq i \leq L$ the number of new variables and equations, respectively.

Table 3 allows us to get a feeling for the significance of the work: While AES with 256 key bits is considered secure, the *reduction* for MIA alone, *i.e.* the scheme

Table 2. Summary of the reduction results of this article

Scheme (<i>Section</i>)	Reduction
MIA (4.1)	$n(q^n - 1)$
MIA- (4.1)	$n(q^n - 1)q^r \prod_{i=n-r-1}^{n-1} (q^n - q^i)$
HFE (4.2)	$nq^{2n}(q^n - 1)^2$
HFE- (4.2)	$nq^{2n}(q^n - 1)(q^{n-r} - 1) \prod_{i=n-r-1}^{n-1} (q^n - q^i)$
HFEv (4.2)	$\tilde{n}q^{n+\tilde{n}+vm}(q^{\tilde{n}} - 1)^2 \prod_{i=0}^{v-1} (q^v - q^i)$
HFEv- (4.2)	$\tilde{n}q^{r+2\tilde{n}+v\tilde{n}}(q^{\tilde{n}} - 1)^2 \prod_{i=0}^{v-1} (q^v - q^i) \prod_{i=\tilde{n}-r-1}^{\tilde{n}-1} (q^{\tilde{n}} - q^i)$
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)	$q^{m+n} \prod_{i=1}^L \left(q^{n_i(n - \sum_{j=1}^i n_j)} \prod_{j=0}^{n_i-1} (q^{n_i} - q^j) \right)$ $\prod_{i=1}^L \left(q^{m_i(m - \sum_{j=1}^i m_j)} \prod_{j=0}^{m_i-1} (q^{m_i} - q^j) \right)$

with the smallest number of equivalent keys, is already in the range of 469 bits. Equivalently, we can save a full row of transformation S in implementation—allowing the corresponding saving in time and memory. For lightweight implementations, even reductions in the range of a few percent are significant. In the case of UOV or STS, the savings are even larger. As a nice side-result, this memory-efficient implementation does *not* jeopardise the security of these schemes. However, in general we advocate the construction of schemes which do not allow for equivalent private keys and are hence efficient by construction. Second, the results of this article 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 scheme should be simplified accordingly. In addition, recent cryptanalytic results such as [1] become much easier when equivalent private key forms can be dismissed rather early in the cryptanalytic process. The same is also true for older work as [18, 19]. Third, constructors of new schemes should keep these sustaining transformations in mind (see above): there is no point in having a large private key space—if it can be reduced immediately by an attacker who can just apply some sustainers. Moreover, the results obtained in this 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

Table 3. Numerical examples for the reduction results of this article

Scheme	Parameters	Choices for S, T (in \log_2)	Reduction (in \log_2)
MIA	$q = 128, n = 67$	63,784	469
MIA-	$q = 128, r = 11, n = 67$	63,784	6180
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
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

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} . Last but not least equivalent keys allow a tighter evaluation of the effective public key space: when we can already discard a large fraction of the private key space as equivalent, this subsequently means that we also reach a much smaller fraction of the public key space as initially expected.

We want to stress that the sustainers from Section 3 are probably not the only ones possible. 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 4.1. 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. However, having concentrated on the basic schemes, we are confident that we have provided the most necessary tools to evaluate these schemes, too.

Acknowledgments. 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. Section 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) for comments on some early results presented in this paper. Finally, we are in debt to Enrico Thomae (CITS, Ruhr-University Bochum) for fruitful discussions and helpful comments on the manuscript. In particular, he supplied the counter example for $q = 2$ in the MIA section.

Bibliography

- [1] Olivier Billet and Gilles Macario-Rat, Cryptanalysis of the Square Cryptosystems, in: *ASIACRYPT*, Lecture Notes in Computer Science 5912, Mitsuru Matsui, editor, pp. 451–468, Springer, 2009, ISBN 978-3-642-10365-0.
- [2] 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*, Lecture Notes in Computer Science 2656, Eli Biham, editor, pp. 33–50, Springer, 2003.
- [3] Andrey Bogdanov, Thomas Eisenbarth, Andy Rupp and Christopher Wolf, Time-Area Optimized Public-Key Engines: -Cryptosystems as Replacement for Elliptic Curves?, in: *CHES* (Elisabeth Oswald and Pankaj Rohatgi, eds.), Lecture Notes in Computer Science 5154, pp. 45–61, Springer, 2008.
- [4] An Braeken, Christopher Wolf and Bart Preneel, A Study of the Security of Unbalanced Oil and Vinegar Signature Schemes, in: *The Cryptographer's Track at RSA Conference 2005*, Lecture Notes in Computer Science 3376, Alfred J. Menezes, editor, Springer, 2005, 13 pages, cf <http://eprint.iacr.org/2004/222/>.
- [5] Nicolas Courtois, Louis Goubin and Jacques Patarin, *Flash: Primitive specification and supporting documentation*, 2000, <https://www.cosic.esat.kuleuven.be/nessie>, submissions, 9 pages.
- [6] 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.
- [7] 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.
- [8] 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.
- [9] Nicolas Courtois, Louis Goubin and Jacques Patarin, *Sflash^{v3}, a fast asymmetric signature scheme — Revised Specification of Sflash, version 3.0*, October 17th 2003, ePrint Report 2003/211, <http://eprint.iacr.org/>, 14 pages.
- [10] Jintai Ding and Dieter Schmidt, Rainbow, a New Multivariable Polynomial Signature Scheme, in: *Conference on Applied Cryptography and Network Security — ACNS 2005*, Lecture Notes in Computer Science 3531, pp. 164–175, Springer, 2005.

-
- [11] Jean-Charles Faugère and Antoine Joux, Algebraic cryptanalysis of Hidden Field Equations (HFE) Using Gröbner Bases, in: *Advances in Cryptology — CRYPTO 2003*, Lecture Notes in Computer Science 2729, Dan Boneh, editor, pp. 44–60, Springer, 2003.
- [12] W. Geiselmann, R. Steinwandt and Th. Beth, Attacking the Affine Parts of SFlash, in: *Cryptography and Coding - 8th IMA International Conference*, Lecture Notes in Computer Science 2260, B. Honary, editor, pp. 355–359, Springer, 2001, Extended version: <http://eprint.iacr.org/2003/220/>.
- [13] Yuh-Hua Hu, Lih-Chung Wang, Chun yen Chou and Feipei Lai, Similar Keys of Multivariate Quadratic Public Key Cryptosystems, in: *Cryptology and Network Security, 4th International Conference, CANS 2005, Xiamen, China, December 14-16, 2005, Proceedings* (Yvo Desmedt, Huaxiong Wang, Yi Mu and Yongqing Li, eds.), Lecture Notes in Computer Science 3810, pp. 211–222, Springer, 2005.
- [14] 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*, Lecture Notes in Computer Science 229, Jacques Calmet, editor, pp. 108–119, Springer, 1985.
- [15] Masao Kasahara and Ryuichi Sakai, A Construction of Public Key Cryptosystem for Realizing Ciphertext of Size 100 Bit and Digital Signature Scheme, *IE-ICE Trans. Fundamentals* **E87-A** (2004), 102–109, Electronic version: <http://search.ieice.org/2004/files/e000a01.htm#e87-a,1,102>.
- [16] Aviad Kipnis, Jacques Patarin and Louis Goubin, Unbalanced Oil and Vinegar Signature Schemes, in: *Advances in Cryptology — EUROCRYPT 1999*, Lecture Notes in Computer Science 1592, Jacques Stern, editor, pp. 206–222, Springer, 1999.
- [17] Aviad Kipnis, Jacques Patarin and Louis Goubin, *Unbalanced Oil and Vinegar Signature Schemes — Extended Version*, 2003, 17 pages, citeseer/231623.html, 2003-06-11.
- [18] Aviad Kipnis and Adi Shamir, Cryptanalysis of the Oil and Vinegar Signature Scheme, in: *Advances in Cryptology — CRYPTO 1998*, Lecture Notes in Computer Science 1462, Hugo Krawczyk, editor, pp. 257–266, Springer, 1998.
- [19] Aviad Kipnis and Adi Shamir, Cryptanalysis of the HFE public key cryptosystem, in: *Advances in Cryptology — CRYPTO 1999*, Lecture Notes in Computer Science 1666, Michael Wiener, editor, pp. 19–30, Springer, 1999, <http://www.minrank.org/hfesubreg.ps> or <http://citeseer.nj.nec.com/kipnis99cryptanalysis.html>.
- [20] Tsutomu Matsumoto and Hideki Imai, Public Quadratic Polynomial-Tuples for Efficient Signature Verification and Message-Encryption, in: *Advances in Cryptology — EUROCRYPT 1988*, Lecture Notes in Computer Science 330, Christoph G. Günther, editor, pp. 419–545, Springer, 1988.

-
- [21] 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** (1985), 139–146.
- [22] *NESSIE: New European Schemes for Signatures, Integrity, and Encryption. Information Society Technologies Programme of the European Commission (IST-1999-12324)*, <http://www.cryptoneessie.org/>.
- [23] Jacques Patarin, Asymmetric Cryptography with a Hidden Monomial, in: *Advances in Cryptology — CRYPTO 1996*, Lecture Notes in Computer Science 1109, Neal Koblitz, editor, pp. 45–60, Springer, 1996.
- [24] Jacques Patarin, Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): two new Families of Asymmetric Algorithms, in: *Advances in Cryptology — EUROCRYPT 1996*, Lecture Notes in Computer Science 1070, Ueli Maurer, editor, pp. 33–48, Springer, 1996, Extended Version: <http://www.minrank.org/hfe.pdf>.
- [25] Serge Vaudenay, editor, *Public Key Cryptography — PKC 2005*, Lecture Notes in Computer Science 3386, Springer, 2005, ISBN 3-540-24454-9.
- [26] Iia Toli, *Cryptanalysis of HFE*, June 2003, arXiv preprint server, <http://arxiv.org/abs/cs.CR/0305034>, 7 pages.
- [27] Lih-Chung Wang, Yuh-Hua Hu, Feipei Lai, Chun-Yen Chou and Bo-Yin Yang, Tractable Rational Map Signature, in PKC [25].
- [28] Christopher Wolf, Hidden Field Equations (HFE) - *Variations and Attacks*, Diplomarbeit, Universität Ulm, December 2002, <http://www.christopher-wolf.de/dp1>, 87 pages.
- [29] Christopher Wolf, Efficient Public Key Generation for HFE and Variations, in: *Cryptographic Algorithms and Their Uses 2004*, Dawson, Klimm, editors, pp. 78–93, QUT University, 2004.
- [30] Christopher Wolf, *Multivariate Quadratic Polynomials in Public Key Cryptography*, Ph.D. thesis, Katholieke Universiteit Leuven, Belgium, November 2005, <http://hdl.handle.net/1979/148>, 156+xxiv pages.
- [31] Christopher Wolf, An Braeken and Bart Preneel, Efficient Cryptanalysis of RSE(2)PKC and RSSE(2)PKC, in: *Conference on Security in Communication Networks — SCN 2004*, Lecture Notes in Computer Science 3352, pp. 294–309, Springer, September 8–10 2004, Extended version: <http://eprint.iacr.org/2004/237>.
- [32] 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/>.

- [33] Christopher Wolf and Bart Preneel, Equivalent Keys in HFE, C^* , and variations, in: *Proceedings of Mycrypt 2005*, Lecture Notes in Computer Science 3715, Serge Vaudenay, editor, pp. 33–49, Springer, 2005, Extended version <http://eprint.iacr.org/2004/360/>, 15 pages.
- [34] Christopher Wolf and Bart Preneel, Superfluous Keys in Multivariate Quadratic Asymmetric Systems, in PKC [25], Extended version <http://eprint.iacr.org/2004/361/>.
- [35] 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.
- [36] Bo-Yin Yang and Jiun-Ming Chen, *Rank Attacks and Defence in Tame-Like Multivariate PKC's*, Cryptology ePrint Archive, Report 2004/061, 29th September 2004, <http://eprint.iacr.org/>, 21 pages.

Received ???.

Author information

Christopher Wolf, K.U.Leuven, ESAT-COSIC, Kasteelpark Arenberg 10, BE-3001 Leuven-Heverlee, Belgium and Horst Görtz Institute for IT-Security, Building NA 5/69, Ruhr-University Bochum, DE-44780 Bochum, Belgium.
E-mail: chris@Christopher-Wolf.de, Christopher.Wolf@rub.de

Bart Preneel, K.U.Leuven, ESAT-COSIC, Kasteelpark Arenberg 10, BE-3001 Leuven-Heverlee, Belgium, Belgium.
E-mail: Bart.Preneel@esat.kuleuven.be