Equivalent Keys in HFE, C*, and variations

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

Abstract

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

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

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

Date: 2005-01-28

1 Introduction

In the last 15 years, several schemes based on the problem of $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic equations have been proposed. The most important one certainly are C* [MI88] and Hidden Field Equations (HFE, [Pat96b]) plus their variations C^{*--}, HFE-, HFEv, and HFEv- [Pat96a, KPG99, Pat96b]. In all cases, the public key equations have the form

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

for $1 \le i \le m; 1 \le j \le k \le n$ and $\alpha_i, \beta_{i,j}, \gamma_{i,j,k} \in \mathbb{F}$ (constant, linear, and quadratic terms). We write the set of all such equations as $\mathcal{MQ}_m(\mathbb{F}^n)$. Moreover, the private key consists of the triple $(S, \mathcal{P}', T)$ where $S \in \mathrm{AGL}_n(\mathbb{F}), T \in \mathrm{AGL}_m(\mathbb{F})$ are affine transformations and $\mathcal{P}' \in \mathcal{MQ}_m(\mathbb{F}^n)$ is a polynomial-vector $\mathcal{P}' := (p'_1, \ldots, p'_m)$ with m components; each component is a polynomial in n variables $x'_1, \ldots, x'_n$. Throughout this paper, we will denote components of this private vector $\mathcal{P}'$ by a prime $'$. In contrast to the public polynomial vector $\mathcal{P} \in \mathcal{MQ}_m(\mathbb{F}^n)$, the private polynomial vector $\mathcal{P}'$ does allow an efficient computation of $x'_1, \ldots, x'_n$ for given $y'_1, \ldots, y'_m$. Hence, the goal of $\mathcal{MQ}$-schemes is that this should be hard if the public key $\mathcal{P}$ alone is given. The main difference between $\mathcal{MQ}$-schemes lies in their special construction of the central equations $\mathcal{P}'$ and consequently the trapdoor they embed into a specific class of $\mathcal{MQ}$-problems.

In this paper, we investigate the question of equivalent keys for selected $\mathcal{MQ}$-schemes. Due to space limitations, we concentrate on HFE, HFE-, HFEv, HFEv-, C*, and C^{*--}. However, we want to point out that the techniques outlined here are quite general and can also be applied to other schemes, cf [WP05] for a more detailed overview and also results on UOV.

2 Mathematical Background

After giving some basic definitions in the following section, we will move on to observations about affine transformations. See [WP05] for a more detailed introduction to the mathematical background.

2.1 Definitions

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

Definition 2.1 *We call two private keys*

$$(T, \mathcal{P}', S), (\tilde{T}, \tilde{\mathcal{P}}', \tilde{S}) \in AGL_m(\mathbb{F}) \times \mathcal{MQ}_m(\mathbb{F}^n) \times AGL_n(\mathbb{F})$$

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

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

for the two triples $(T, \mathcal{P}', S), (\tilde{T}, \tilde{\mathcal{P}}', \tilde{S})$ where $S, \tilde{S}$ are affine transformations over $\mathbb{F}^n$, $T, \tilde{T}$ are affine transformations over $\mathbb{F}^m$, and $\mathcal{P}, \tilde{\mathcal{P}}$ are systems of m multivariate quadratic equations with n input variables each.

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

Definition 2.2 *Let $(S, \mathcal{P}', T) \in AGL_m(\mathbb{F}) \times \mathcal{MQ}_m(\mathbb{F}^n) \times AGL_n(\mathbb{F})$ and $\sigma, \sigma^{-1} \in AGL_n(\mathbb{F})$ and $\tau, \tau^{-1} \in AGL_m(\mathbb{F})$. Moreover, let*

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

We call the pair $(\sigma, \tau) \in AGL_n(\mathbb{F}) \times AGL_m(\mathbb{F})$ sustaining transformations *for an $\mathcal{MQ}$-system if the* shape *of $\mathcal{P}'$ is invariant under the transformations σ and τ.*

Remark. In the above definition, the meaning of *shape* is still open. In fact, its meaning has to be defined for each $\mathcal{MQ}$-system individually, cf Sect. 4 for examples.

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

After these initial observations on equivalent keys, we concentrate on bijections between ground fields and their extension fields. Let $\mathbb{F}$ be a finite field with $q := |\mathbb{F}|$ elements and $\mathbb{E}$ its n-th degree extension $\mathbb{E} := \mathbb{F}[t]/i(t)$ for some irreducible, n-th degree polynomial $i(t)$ over $\mathbb{F}$. Moreover, we have the elements $a \in \mathbb{E}$ and $b \in \mathbb{F}^n$ as

$$a := \alpha_n t^{n-1} + \ldots + \alpha_2 t + \alpha_1 \text{ and } b := (\beta_1, \ldots, \beta_n)\,,$$

for $\alpha_i, \beta_i \in \mathbb{F}$ with $1 \leq i \leq n$. As elements in $\mathbb{E}$ also form a vector space, we define a bijection between $\mathbb{E}$ and $\mathbb{F}^n$ by identifying the coefficients $\alpha_i \leftrightarrow \beta_i$. We use this bijection throughout this paper.

2.2 Affine Transformations

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

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

Next, we introduce some definitions about the representation of affine transformations over the finite fields $\mathbb{F}$ and $\mathbb{E}$.

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

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

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

Remark. We can write any affine transformation either in univariate, multivariate or matrix representation. To transfer between these three, we need at most $O(n^2)$ steps, assuming uniform costs for operations in the ground field $\mathbb{F}$.

3 Sustaining Transformations

In this section, we give several examples for sustaining transformations. In addition, we will consider their effect on the central transformation $\mathcal{P}'$. See [WP05] for a more detailed overview.

3.1 Additive Sustainer

DEFINITION 3.1 *For $n = m$ and $A, A' \in \mathbb{E}$, we call $\sigma(X) := (X + A)$ and $\tau(X) := (X + A')$* additive transformations.

Moreover, as long as they keep the shape of the central equations $\mathcal{P}'$ invariant, they form sustaining transformations and are then called *additive sustainer*.

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

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

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

3.2 Big Sustainer

DEFINITION 3.2 *For $B, B' \in \mathbb{E}^*$, we call $\sigma(X) := (BX)$ and $\tau(X) := (B'X)$* big transformations.

The name is motivated as we work in the (big) extension field field $\mathbb{E}$. Again, we obtain a sustaining transformation *big sustainer* if this operation does not modify the shape of the central equations as $(BX), (B'X) \in \mathrm{AGL}_n(\mathbb{F})$.

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 $\mathcal{P}'$ over this extension field.

3.3 Small Sustainer

DEFINITION 3.3 *Let Diag(b) be the diagonal matrix on a vector $b \in \mathbb{F}^n$. Moreover, let the coefficients $b_1, \ldots, b_n, b'_1, \ldots, b'_m \in \mathbb{F}^*$. Then $\sigma(x) := Diag(b_1, \ldots, b_n)x$ and $\tau(x) := Diag(b'_1, \ldots, b'_m)x$ are called* small transformations.

The name is motivated as we work in the multiplicative group of the (small) ground field $\mathbb{F}$. If this leads to sustaining transformations, we call it the *small sustainer*.

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

3.4 Permutation Sustainer

DEFINITION 3.4 *Let $\sigma(x), \tau(x)$ be a permutation of the input vectors, i.e., permuting transformations.*

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

3.5 Gauss Sustainer

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

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

3.6 Frobenius Sustainer

DEFINITION 3.5 *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 $\mathbb{F}$. The following lemma establishes that they also form a group:

Lemma 3.6 *Frobenius transformations are a subgroup in $GL_n(\mathbb{F})$.*

PROOF. First, Frobenius transformations are linear transformations, so associativity is inherited from them. Second, the set H from Def. 3.5 is not empty for any given $\mathbb{F}$ and $n \in \mathbb{N}$. Hence, the corresponding set of Frobenius transformations is not empty either. So all left to show is that for any given Frobenius transformations σ, τ, the composition $\sigma \circ \tau^{-1}$ is also a Frobenius transformation.

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

So we can write $\sigma(X) \circ \tau^{-1}(X) = X^{q^{a+b'}}$. If $a + b' < n$ we are done. Otherwise $n \leq a + b' < 2n$, 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 $\sigma \circ \tau^{-1}$ is also a Frobenius transformation. This completes the proof that all Frobenius transformations form a group. □

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

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

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

3.7 Reduction Sustainer

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

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

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

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

When applying the reduction sustainer together with other sustainers, we have to make sure that we do not count the same transformation twice. We will deal with this problem in the corresponding sections.

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

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

4.1 Hidden Field Equations

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

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

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

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

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

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

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

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

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

PROOF (sketch). We use the additive sustainer and the big sustainer on both sides, *i.e.*, for S and T. In addition, we apply the Frobenius sustainer from one side and cancel it from the other side to keep the degree d untouched. □

A weaker version of this theorem can be found in [WP05, Thm. 1].
Remark. To the knowledge of the authors, the additive sustainer for HFE has first been reported in [Tol03] and used there for reducing the affine transformations to linear ones.

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

4.1.1 HFE-

The class HFE- is the original HFE-class with the reduction modification (cf Sect. 3.7).

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

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

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

PROOF (sketch). We apply the additive sustainer and the big sustainer to S. In addition, we apply the Frobenius sustainer to either S or T. To avoid double counting, we only consider the upper $n-r$ rows of T and apply both the additive sustainer and the multiplicative sustainer. In addition, we apply the reduction sustainer to T. □

For $q = 2, r = 7$ and $n = 107$, the number of equivalent keys for each private key is $\approx 2^{2129}$. In comparison, the number of choices for S and T is $\approx 2^{23,108}$. This special choice of parameters has been used in the repaired version Quartz-7m of Quartz [CGP01, WP04a].

4.1.2 HFEv

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

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

$$P_{z_1,\ldots,z_v}(X) := \sum_{\substack{0 \le i,j \le d \\ q^i + q^j \le d}} C_{i,j} X^{q^i+q^j} + \sum_{\substack{0 \le k \le d \\ q^k \le d}} B_k(z_1, \ldots, z_v) X^{q^k} + A(z_1, \ldots, z_v)$$

$$\text{where} \begin{cases} C_{i,j} X^{q^i+q^j} & \text{for } C_{i,j} \in \mathbb{E} \text{ are the quadratic terms,} \\ B_k(z_1, \ldots, z_v) X^{q^k} & \text{for } B_k(z_1, \ldots, z_v) \text{ depending linearly on } z_1, \ldots, z_v \text{ and} \\ A(z_1, \ldots, z_v) & \text{for } A(z_1, \ldots, z_v) \text{ depending quadratically on } z_1, \ldots, z_v \end{cases}$$

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

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

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

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

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

PROOF (sketch). First, we apply the additive sustainer on S, T and have hence linear transformations in both cases. This reduces by $q^n \cdot q^m$. To make sure that we do not count the same linear transformation twice, we consider a normal form for the (linear) transformation S

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

In the above definition, we also have I_v the identity matrix in $\mathbb{F}^{v \times v}$. For each invertible matrix M_S, we have a unique matrix

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

which transfers M_S to the normal form from above. Again, I_m is an identity matrix in $\mathbb{F}^{m\times m}$. This way, we obtain $\prod_{i=0}^{v-1}(q^v - q^i)$ equivalent keys in the "v" modification alone.

For the HFE component, we apply the big sustainer both to S, T and obtain a factor of $(q^{n'}-1)^2$. In addition, we apply the Frobenius sustainer to the HFE component, which yields an additional factor of n'. □

For the case $q = 2, v = 7$ and $n = 107$, the number of equivalent keys for each private is $\approx 2^{460}$. In comparison, the number of choices for S and T is $\approx 2^{21,652}$.

4.1.3 HFEv-

Here, we use the HFEv modification from the previous section and apply the reduction modification from Sect. 3.7 to it.

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

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

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

Proof (sketch). This proof is a combination of the two cases HFEv and HFE-. □

For the case $q = 2, r = 3, v = 4$ and $n = 107, n' := 100$, the number of redundant keys is $\approx 2^{690}$. In comparison, the number of choices for S and T is $\approx 2^{22,261}$. This special choice of parameters has been used in the original version of Quartz [CGP01], as submitted to NESSIE [NES].

4.2 Class of C* Schemes

As HFE, the scheme C^*, due to Matsumoto and Imai [MI88], uses a finite field $\mathbb{F}$ and an extension field $\mathbb{E}$. However, the choice of the central equation is far more restricted than in HFE as we only have one monomial here.

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

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

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

Theorem 4.8 *For $K := (S, P, T) \in AGL_n(\mathbb{F}) \times \mathbb{E}[X] \times AGL_n(\mathbb{F})$ a private key in C^* we have*

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

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

PROOF (sketch). We use the big sustainer and the Frobenius sustainer on one side, *i.e.*, either for S or T, and cancel it out from the other side to preserve the C*-monomial $P(X)$. □

A weaker version of this theorem can be found in [WP05, Thm. 2].

Although we cannot apply the additive sustainer, the constant part of the affine transformations in C* do not seem to add to the overall security of the system, cf [GSB01].

For $q = 128$ and $n = 67$, we obtain $\approx 2^{469}$ equivalent private keys per class. The number of choices for S, T is $\approx 2^{63,784}$ in this case.

4.2.1 C*−−

As in the case of HFE and HFE-, we use the original C* scheme and apply the reduction modification from Sect. 3.7.

Theorem 4.9 *For $K := (S, P, T) \in AGL_n(\mathbb{F}) \times \mathbb{E}[X] \times AGL_n(\mathbb{F})$ a private key in C* and a reduction number $r \in \mathbb{N}$ we have*

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

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

PROOF (sketch). We use the big sustainer and the Frobenius sustainer on one side, *i.e.*, either for S or T, and cancel it out from the other side to preserve the C*-monomial $P(X)$. To avoid double counting, we can only consider the upper $n - r$ rows of the affine part of $(S, \mathcal{P}', T)$. In addition, we apply the reduction sustainer on the lower r rows of T. □

For $q = 128, r = 11$ and $n = 67$, we obtain $\approx 2^{6173}$ equivalent private keys per class. The number of choices for S, T is $\approx 2^{63,784}$ in this case. This particular choice of parameters has been used in Sflash^{v3} [CGP03].

5 Conclusions

In this paper, we showed through the examples of Hidden Field Equations (HFE) and C* that $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic systems allow many equivalent private keys and hence have a lot of redundancy in this key space, cf Table 1 and Table 2 for numerical examples; the symbols used in Table 1 are explained in the corresponding sections. The $\mathcal{MQ}$-scheme Unbalanced Oil and Vinegar (UOV) has been discussed in [WP05, Sect. 4.3].

Table 1: Summary of the Reduction Results of this Paper

Scheme (*Section*)	Reduction
Hidden Field Equations (*4.1*)	$nq^{2n}(q^n-1)^2$
HFE Minus (*4.1.1*)	$nq^n(q^n-1)q^{n-r}(q^{n-r}-1)\prod_{i=n-r-1}^{n-1}(q^n-q^i)$
HFE Vinegar (*4.1.2*)	$n'q^nq^{n'}(q^{n'}-1)^2\prod_{i=0}^{v-1}(q^v-q^i)$
HFE Vinegar Minus (*4.1.3*)	$n'q^rq^{2n'}(q^{n'}-1)^2\prod_{i=0}^{v-1}(q^v-q^i)\prod_{i=n-r-1}^{n-1}(q^n-q^i)$
C* (*4.2*)	$n(q^n-1)$
C* Minus Minus (*4.2.1*)	$n(q^{n-r}-1)q^r\prod_{i=n-r-1}^{n-1}(q^n-q^i)$

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

We want to stress that the sustainers from Sect. 3 are certainly not the only ones possible. We therefore invite other researchers to look for even more powerful transformations. In addition, there are other multivariate schemes which have not been discussed in this paper or [WP05], due to space and time limitations. These schemes include (non-exhaustive list) enTTS [YC04], STS [WBP04]), and PMI [Din04]. We also invite to apply the techniques used in this paper to these schemes.

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

Scheme	Parameters	Choices for S,T (in $\log_2$)	Reduction (in $\log_2$)
HFE	$q=2, n=80$	12,056	326
HFE-	$q=2, r=7, n=107$	23,108	2129
HFEv	$q=2, v=7, n=107$	21,652	460
HFEv-	$q=2, n=107$	22,261	690
C*	$q=128, n=67$	63,784	469
C*−−	$q=128, n=67$	63,784	6173

Acknowledgements

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

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

Disclaimer

The information in this document reflects only the authors' views, is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

References

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

[CGP01] Nicolas Courtois, Louis Goubin, and Jacques Patarin. *Quartz: Primitive specification (second revised version)*, October 2001. `https://www.cosic.esat.kuleuven.ac.be/nessie/workshop/submissions/quar%tzv21-b.zip`, 18 pages.

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

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

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

[KPG99] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced Oil and Vinegar signature schemes. In *Advances in Cryptology — EUROCRYPT 1999*, volume 1592 of *Lecture Notes in Computer Science*, pages 206–222. Jacques Stern, editor, Springer, 1999.

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

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

[Pat96a] Jacques Patarin. Asymmetric cryptography with a hidden monomial. In *Advances in Cryptology — CRYPTO 1996*, volume 1109 of *Lecture Notes in Computer Science*, pages 45–60. Neal Koblitz, editor, Springer, 1996.

[Pat96b] Jacques Patarin. Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms. In *Advances in Cryptology — EUROCRYPT 1996*, volume 1070 of *Lecture Notes in Computer Science*, pages 33–48. Ueli Maurer, editor, Springer, 1996. Extended Version: http://www.minrank.org/hfe.pdf.

[Tol03] Ilia Toli. Cryptanalysis of HFE, June 2003. arXiv preprint server, http://arxiv.org/abs/cs.CR/0305034, 7 pages.

[WBP04] Christopher Wolf, An Braeken, and Bart Preneel. Efficient cryptanalysis of RSE(2)PKC and RSSE(2)PKC. In *Conference on Security in Communication Networks — SCN 2004*, Lecture Notes in Computer Science, pages 145–151, September 8–10 2004. extended version: http://eprint.iacr.org/2004/237.

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

[WP04a] Christopher Wolf and Bart Preneel. 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/.

[WP04b] Christopher Wolf and Bart Preneel. Equivalent keys in HFE, C^*, and variations. Cryptology ePrint Archive, Report 2004/360, 2004. http://eprint.iacr.org/2004/360/, 12 pages.

[WP05] Christopher Wolf and Bart Preneel. Superfluous keys in $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic asymmetric systems. In *Public Key Cryptography — PKC 2005*, volume 3386 of *Lecture Notes in Computer Science*, pages 275–287. Serge Vaudenay, editor, Springer, 2005. extended version http://eprint.iacr.org/2004/361/.

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