On enumeration of polynomial equivalence classes and their application to MPKC

Dongdai Lin, Jean-Charles Faugère, Ludovic Perret, Tianze Wang

On Enumeration of Polynomial Equivalence Classes and Their Application to MPKC

Dongdai Lin[a], Jean-Charles Faugère[b], Ludovic Perret[b], Tianze Wang[a,c]

[a] *SKLOIS, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China*
[b] *LIP6, 104 avenue du Président Kennedy 75016 Paris, France*
[c] *Graduate University of Chinese Academy of Sciences, Beijing 100149, China*

Abstract

The Isomorphism of Polynomials (IP) is one of the most fundamental problems in multivariate public key cryptography (MPKC). In this paper, we introduce a new framework to study the counting problem associated to IP. Namely, we present tools of finite geometry allowing to investigate the counting problem associated to IP. Precisely, we focus on enumerating or estimating the number of isomorphism equivalence classes of homogeneous quadratic polynomial systems. These problems are equivalent to finding the scale of the key space of a multivariate cryptosystem and the total number of different multivariate cryptographic schemes respectively, which might impact the security and the potential capability of MPKC. We also consider their applications in the analysis of a specific multivariate public key cryptosystem. Our results not only answer how many cryptographic schemes can be derived from monomials and how big the key space is for a fixed scheme, but also show that quite many HFE cryptosystems are equivalent to a Matsumoto-Imai scheme.

Keywords: multivariate public key cryptography, polynomial isomorphism, finite geometry, equivalence classes, superfluous keys.

1. Introduction

Multivariate cryptography comprises all the cryptographic schemes using multivariate polynomials. The use of polynomial systems in cryptography dates back to the mid eighties with the design of C* [1], later followed by many other proposals [2, 3, 4, 5]. Schemes based on the hard problem of solving systems of multivariate equations over a finite field could be secure against the quantum computer threat, whereas it is well known that number theoretic-based schemes like RSA, DH, and ECDH are [6].

The general method of building multivariate public key schemes is to choose a system of quadratic polynomials, called central function F, and then hide this central function by using two invertible affine transformations T and L. The composition $T \circ F \circ L$ will be used as a public key and the pair (T, L) is considered as a secret key. We shall say that $T \circ F \circ L$ is a scheme *derived* from the central function F. We can see that the cryptographic scheme is uniquely determined by its central function and two secret affine transformations. But the converse is not true. Let us look at the following two examples.

Example 1. Let

$$F: \left\{ \begin{array}{lcl} u_1 & = & v_1^2 + \alpha^2 v_1 v_2 + \alpha v_1 v_3 + \alpha^2 v_2 v_3 + \alpha v_3^2 \\ u_2 & = & \alpha^2 v_1 v_2 + \alpha^2 v_2^2 + \alpha^2 v_2 v_3 + v_3^2 \\ u_3 & = & \alpha v_1 v_3 + \alpha v_2^2 + \alpha v_2 v_3 + \alpha v_3^2 \end{array} \right.$$

and

$$G: \left\{ \begin{array}{lcl} u_1 & = & v_1^2 + \alpha v_1 v_2 + \alpha^2 v_1 v_3 + \alpha^2 v_2 v_3 + v_3^2 \\ u_2 & = & \alpha v_1 v_2 + \alpha v_2^2 + \alpha v_2 v_3 + \alpha^2 v_3^2 \\ u_3 & = & \alpha^2 v_1 v_3 + \alpha^2 v_2^2 + \alpha^2 v_2 v_3 + \alpha^2 v_3^2 \end{array} \right. ,$$

where α is the defining element of $\mathbb{F}_4$ with $\alpha^2 + \alpha + 1 = 0$. One can check that, for

$$T_1: \left\{ \begin{array}{lcl} y_1 & = & \alpha^2 u_2 + \alpha^2 u_3 \\ y_2 & = & u_1 + \alpha^2 u_2 + \alpha u_3 \\ y_3 & = & u_1 + u_2 + u_3 \end{array} \right. \quad L_1: \left\{ \begin{array}{lcl} v_1 & = & \alpha x_1 + \alpha^2 x_3 \\ v_2 & = & \alpha x_1 \\ v_3 & = & \alpha x_1 + \alpha^2 x_2 \end{array} \right.$$

and

$$T_2: \left\{ \begin{array}{lcl} y_1 & = & \alpha^2 u_1 + u_3 \\ y_2 & = & u_1 + \alpha^2 u_2 \\ y_3 & = & u_1 + \alpha^2 u_2 + \alpha^2 u_3 \end{array} \right. \quad L_2: \left\{ \begin{array}{lcl} v_1 & = & x_1 + x_2 \\ v_2 & = & \alpha^2 x_1 + \alpha x_2 + \alpha^2 x_3 \\ v_3 & = & x_1 + \alpha x_3 \end{array} \right. ,$$

we have

$$T_1 \circ F \circ L_1 = T_2 \circ G \circ L_2.$$

In above example, different triples (T_1, F, L_1) and (T_2, G, L_2) lead to the same encryption mapping (i.e. public key). For this reason, we introduce the following definition.

Definition 1. Let F and G be two central functions. We shall say that the MPKC schemes derived from F and G are equivalent if there are two pairs (T_1, L_1) and (T_2, L_2) of invertible affine transformations such that

$$T_1 \circ F \circ L_1 = T_2 \circ G \circ L_2.$$

Example 2. Let F, T_1 and L_1 be as in Example 1. Let

$$T_3: \left\{ \begin{array}{lcl} y_1 & = & u_1 + u_3 \\ y_2 & = & \alpha u_1 + \alpha^2 u_2 + \alpha^2 u_3 \\ y_3 & = & \alpha^2 u_1 + u_2 + \alpha^2 u_3 \end{array} \right. \quad L_3: \left\{ \begin{array}{lcl} v_1 & = & x_1 + x_2 \\ v_2 & = & x_1 + \alpha^2 x_2 \\ v_3 & = & \alpha^2 x_1 + x_2 + \alpha^2 x_3 \end{array} \right. .$$

Then $T_1 \circ F \circ L_1 = T_3 \circ F \circ L_3$, i.e. (T_1, L_1) and (T_3, L_3) induce the same public key

$$\bar{F}: \left\{ \begin{array}{lcl} y_1 & = & \alpha^2 x_1^2 + \alpha x_1 x_2 + \alpha^2 x_1 x_3 + \alpha^2 x_2^2 + \alpha x_2 x_3 \\ y_2 & = & \alpha^2 x_1 x_2 + \alpha^2 x_2^2 + \alpha x_2 x_3 + \alpha x_3^2 \\ y_3 & = & \alpha x_1^2 + \alpha x_1 x_2 + \alpha x_2^2 + \alpha x_3^2 \end{array} \right. .$$

The above example shows that, for a fixed central function, different secret keys can lead to the same encryption mapping(i.e. public key). For this reason, we have

Definition 2. Let F be a central function, (T_1, L_1) and (T_2, L_2) be two different pairs of secret keys. We shall say that (T_1, L_1) and (T_2, L_2) are equivalent keys of the scheme derived from F if

$$T_1 \circ F \circ L_1 = T_2 \circ F \circ L_2.$$

The above two examples show that neither different central functions nor different secret pairs can guarantee leading to different encryption mappings. Equivalent schemes have the same set of encryption mappings, and so can be considered as the same scheme.

Having a large private (and consequently public) key space is a desirable property for any public key scheme. We emphasize that the existence of equivalent keys shrink the key space as only one equivalent key are useful and others are superfluous, and so it will have a smaller private and public key space than initially expected.

A similar notation of superfluous keys has been introduced by Wolf and Preneel in [7]. More precisely, superfluous keys in the Wolf-Preneel terminology are triples of central function and affine transformations that can induce the same encryption mappings. So, it is, in fact,the combination of equivalent schemes and equivalent keys in our framework, our approach is finer and more general.

Whilst the Multivariate Public Key Cryptosystems (MPKC) are considered to be a good candidate for the post-quantum era, the security of such schemes is still hard to establish. This is evidenced by the successful cryptanalysis of several pioneering schemes, namely C* [8], HFE [9] and SFLASH [10, 11]. Although there are several proposals of MPKC which are assumed to be secure (QUARTZ [4] and UOV [12] for instance), there is a global feeling of insecurity for such schemes. In this context, it is important to have a deeper understanding of MPKC. Up to now, most papers about MPKC analyze the security of a specific scheme, only few papers are related to the study of secret key size and the potentiality of MPKC schemes.

In this paper, we present a new framework for counting how many (non-equivalent) different schemes we can construct and how many equivalent keys (a.k.a. superfluous keys [7]) there are for a specific scheme. Clearly, both equivalent schemes and equivalent keys are tightly connected to the counting problem of the following mathematical problem:

Problem. *Given two polynomial systems F and G, to find, if any, a pair of invertible affine transformations (T, L) such that $T \circ F \circ L = G$.*

The above problem is called IP problem [13]. From an algorithmic point of view, IP and its variants have been thoroughly investigated, e.g. [14, 15, 16, 17]. The authors of [14] proposed the first efficient (i.e. allowing to solve cryptographic challenges) algorithm for solving random instances of IP. Recently, new algorithms for IP and its variants have been proposed [16]. These new algorithms combine (discrete) differential and Gröbner bases techniques permitting to further increase the number of instances of IP which can be solved efficiently. Interesting enough, it was observed experimentally in [14] that the difficulty of IP seems to be linked to the size of the automorphism group, which is related to the number of solutions of an IP instance.

In this paper, however, we consider the counting problem associated to IP. As we know, IP induces an equivalence relation among the polynomial systems, so a set of polynomial systems can be divided into disjoint union of equivalence classes, thus we can count both the cardinality of an equivalence class and the number of equivalence classes of

polynomial systems, which is equivalent to counting the number of "equivalent" secret keys in a multivariate scheme and the total number of different multivariate cryptographic schemes respectively.

To this end, we will extensively use tools of finite geometry [18, 19, 20, 21, 22]. Geometries over finite fields study in particular the standard form of quadratic form over finite fields under some linear transformation, which is related to the IP problem.

Organization of the Paper. In Section 2, we recall the definition of IP and introduce the connection between IP and the matrices congruence problem . This is the key point of the paper. In Section 3, we study the enumeration problem of polynomial isomorphism classes in two different cases: $\mathrm{char}(\mathbb{F}_q) \neq 2$ and $\mathrm{char}(\mathbb{F}_q) = 2$. In each case, we provide a lower bound on the total number of (linearly) equivalence classes. Finally, in Section 4 we will give some basic results for this enumeration problem and consider their application to some specific multivariate cryptographic system (C^* and HFE). In particular, we provide a partial answer about how many different cryptographic schemes can be derived from a monomial central function, and how many pairs of secret keys we can choose for a fixed scheme/central function, which is the real scale of its private key space.

2. Preliminary

In this section, we recall the definition of IP problem introduced in [13] and a useful theorem given by Kipnis and Shamir in [23] (restated by Ding in his book [24]) which is about the relation between polynomials system and univariate polynomial over extension field. We also introduce a new notation called *friendly mapping*. Both the theorem and friendly mapping provide the key ingredient to connect our new tool to IP problem.

2.1. Isomorphism of Polynomials

Let $\mathbb{F}_q$ be a finite field with q elements and $\mathbb{F}_q[x_1, \ldots, x_n]$ be the ring of polynomials in $n \geq 1$ indeterminates over $\mathbb{F}_q$.

Definition 3. We denote by $\mathcal{P}$ the set of all the transformations $F : (x_1, \ldots, x_n) \mapsto (f_1, \ldots, f_n)$ from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$, where $f_i = \sum_{s=1}^{n} \sum_{t=1}^{s} c_{i,st} x_s x_t \in \mathbb{F}_q[x_1, \cdots, x_n]$. We say that $F_1 \in \mathcal{P}$ and $F_2 \in \mathcal{P}$ are equivalent if there exist two invertible linear transformations $(T, L) \in GL_n(\mathbb{F}_q) \times GL_n(\mathbb{F}_q)$ such that $F_2 = T \circ F_1 \circ L$.

Clearly, the above relation is an equivalence relation on the elements of $\mathcal{P}$. Thus, $\mathcal{P}$ can be written as a disjoint union of different equivalence classes. The problem of recovering the transformations T and L is known as IP with two secrets. A restricted problem called IP with one secret (IP1S)(see [13]) involves only one transformation on the variables, namely to find $L \in GL_n(\mathbb{F}_q)$ such that $F_2 = F_1 \circ L$. Generally, this simplification will induce more equivalence classes. Indeed, linear transformation T mixes some classes together.

Remark 1. Note that, in the case of $q = 2$, it holds that $x_k^2 = x_k$. As as a consequence, the f_i's in Definition 3 are not always homogeneous. They are, in fact, quadratic polynomials without constant terms. For simplicity and by abuse of language, we still refer to such polynomials as homogeneous in this paper.

IP (as well as IP1S) can also be interpreted as a group action. Let $\mathcal{G} = GL_n(\mathbb{F}_q) \times GL_n(\mathbb{F}_q)$ be the direct product of $GL_n(\mathbb{F}_q)$ and $GL_n(\mathbb{F}_q)$, then $\mathcal{G}$ forms a group under the operation: $(T_1, L_1) \cdot (T_2, L_2) = (T_1 \circ T_2, L_2 \circ L_1)$. Considering $\mathcal{G}$ acting on the set $\mathcal{P}$, we can define the invariant group of $F \in \mathcal{P}$ as follows:

$$H = \{(T, L) : T \circ F \circ L = F\}.$$

Then $T_1 \circ F \circ L_1 = T_2 \circ F \circ L_2$ iff $(T_1^{-1} \circ T_2) \circ F \circ (L_2 \circ L_1^{-1}) = F$, hence $(T_1^{-1} \circ T_2, L_2 \circ L_1^{-1}) \in H$. This means that in order to study equivalent keys, it suffices to study the invariant group H of F. H is a subgroup of $\mathcal{G}$ and each coset of this subgroup corresponds to a non-equivalent private key. Different cryptographic schemes are just the orbits of this group action [14].

Alternatively, we can view IP from a geometric point of view: thinking the indeterminates $x_1, x_2, \ldots, x_n$ as the coordinates of a point in some coordinate system. The linear transformation can be considered as a coordinate transformation of the coordinate system. The polynomial equivalence problem can then be considered as the study of geometric object defined by the polynomial system under the coordinate transformation. In this paper, we follow the geometric way and adopt results/techniques of finite geometry (or geometries over finite fields) to study IP and IP1S

2.2. Considering IP over Extension Fields

Let $g(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree n over $\mathbb{F}_q$, then $\mathbb{F}_{q^n} \simeq \mathbb{F}_q[x]/(g(x))$. Let $\phi : \mathbb{F}_{q^n} \to \mathbb{F}_q^n$ be the map defined by:

$$\phi(\alpha_0 + \alpha_1 x + \ldots + \alpha_{n-1} x^{n-1}) = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}). \tag{1}$$

It is easy to check that ϕ is a $\mathbb{F}_q$-vector space isomorphism between $\mathbb{F}_{q^n}$ and $\mathbb{F}_q^n$. The following lemma is from literature (we refer the reader to [23] and [24] for its proofs).

Lemma 1. *1) Let L be a linear transformation of $\mathbb{F}_q^n$, then $\phi^{-1} \circ L \circ \phi$ is of the form:*

$$\phi^{-1} \circ L \circ \phi(X) = \sum\nolimits_{i=0}^{n-1} \alpha_i X^{q^i}, \text{ where } \alpha_i \in \mathbb{F}_{q^n}. \tag{2}$$

2) Let $F \in \mathcal{P}$ as in Definition 3, then $\phi^{-1} \circ F \circ \phi$ is of the form:

$$\phi^{-1} \circ F \circ \phi(X) = \sum\nolimits_{i=0}^{n-1} \sum\nolimits_{j=0}^{i} \alpha_{ij} X^{q^i + q^j}, \text{where } \alpha_{ij} \in \mathbb{F}_{q^n}. \tag{3}$$

The converse of the results is also true.

We shall say that (2) *(resp.* (3)*) is the univariate representations of the corresponding maps.*

From above lemma, we can see that there is a 1-1 correspondence between the polynomial mappings of $\mathcal{P}$ (resp. linear transformations) and the univariate representation (3) (resp. (2)). Thus, we sometimes identify $\phi^{-1} \circ F \circ \phi$ (resp. $\phi^{-1} \circ L \circ \phi$) with F (resp. L).

Hereafter, we will use $\mathcal{F}$ to denote the set of mappings represented by (3) and use $\mathcal{L}$ to denote the set of invertible mappings represented by (2). Then $\mathcal{F} = \phi^{-1} \circ \mathcal{P} \circ \phi$ and the definition of IP1S can be restated in univariate representation over extension field as follows:

Definition 4. Let $F(X) = \sum_{i=0}^{n-1}\sum_{j=0}^{i} a_{ij}X^{q^i+q^j}, G(X) = \sum_{i=0}^{n-1}\sum_{j=0}^{i} b_{ij}X^{q^i+q^j} \in \mathcal{F}$. We say that F and G are *linearly equivalent* if and only if there exists $L(X) = \sum_{i=0}^{n-1} a_i X^{q^i} \in \mathcal{L}$ such that $F\big(L(X)\big) = G(X)$, for all $X \in \mathbb{F}_{q^n}$.

Let $L(X) = \sum_{i=0}^{n-1} a_i X^{q^i}$ be a polynomial over $\mathbb{F}_{q^n}$. We associate a matrix $\hat{L}$ over $\mathbb{F}_{q^n}$ to L as follows:

$$\hat{L} = \begin{pmatrix} a_0 & a_{n-1}^q & \dots & a_1^{q^{n-1}} \\ a_1 & a_0^q & \dots & a_2^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2}^q & \dots & a_0^{q^{n-1}} \end{pmatrix}_{n\times n}. \tag{4}$$

It holds that:

Lemma 2. *Let $L(X) = \sum_{i=0}^{n-1} a_i X^{q^i}$ be a polynomial over $\mathbb{F}_{q^n}$. Then $L \in \mathcal{L}$ if and only if the matrix $\hat{L}$ associated to L is invertible. Let $\mathcal{B}$ denote the set of all such invertible matrices of the form (4), then $\mathcal{B}$ is a subgroup of $GL_n(\mathbb{F}_{q^n})$ and is isomorphic to $GL_n(\mathbb{F}_q)$.*

Proof. Please refer to the discussion on page 361-362 of [25]. □

Definition 5. Let $\mathcal{M}_{n\times n}(\mathbb{F}_{q^n})$ be the set of all $n \times n$ matrices over $\mathbb{F}_{q^n}$. A mapping Ψ from $\mathcal{F}$ to $\mathcal{M}_{n\times n}(\mathbb{F}_{q^n})$ is called *friendly mapping* if for every $L \in \mathcal{L}$ and $F \in \mathcal{F}$:

$$\Psi(F \circ L) = \hat{L}\Psi(F)\hat{L}^{\mathrm{T}},$$

where superscript "T" means the transpose of a matrix.

The definition of "friendly mapping" is in fact a method to connect IP over the extension field to the transformations of matrices. Under friendly mapping, the IP problem can be viewed as a congruence problem on matrices. A natural candidate of friendly mapping is given below:

Lemma 3. *Let $\mathbb{F}_{q^n}$ be a finite field with q^n elements. For any $F = \sum_{i=0}^{n-1}\sum_{j=0}^{i} a_{ij}X^{q^i+q^j} \in \mathcal{F}$, we define $\Psi_1(F) \in \mathcal{M}_{n\times n}(\mathbb{F}_{q^n})$ as*

$$\Psi_1(F) = \begin{pmatrix} 2a_{00} & a_{10} & \dots & a_{n-1,0} \\ a_{10} & 2a_{11} & \dots & a_{n-1,1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1,0} & a_{n-1,1} & \dots & 2a_{n-1,n-1} \end{pmatrix}.$$

Then Ψ_1 is a friendly mapping.

Proof. It is easy to see from Lemma 2.4.1 of [24]. □

From the definition of Ψ_1, we can see that Ψ_1 maps polynomials in $\mathcal{F}$ into symmetric matrices. When $\mathrm{char}(\mathbb{F}_{q^n}) = 2$, these matrices are not only symmetric matrices, but also anti-symmetric matrices whose diagonal elements are all 0. This kind of matrices has a particular name:

Definition 6. Let K be a $n \times n$ matrix over $\mathbb{F}_{q^n}$, if $K^{\mathrm{T}} = -K$, then K is called anti-symmetric matrix. Anti-symmetric matrices with all diagonal elements equal to 0 are called *alternative matrices*.

When $\mathrm{char}(\mathbb{F}_{q^n}) = 2$, Ψ_1 maps polynomials in $\mathcal{F}$ to alternative matrices, and no entry in the matrix reflects the terms of the form aX^{2q^i}. It is somehow unreasonable to allow a friendly mapping to throw away the terms of the form aX^{2q^i}. But this does not affect much on the analysis of corresponding scheme as already shown in the book [24]. In order to keep these terms and get a finer classification, one can choose other friendly mapping such as the mapping to the residue classes of coefficient matrices modulo alternative group.

3. Some Bounds on the Number of IP Classes

In this section, we use finite geometry to investigate the number of equivalence classes.

3.1. Isomorphism Equivalence Classes when $\mathrm{char}(\mathbb{F}_q) = 2$

Here, we discuss the IP problem for a field $\mathbb{F}_q$ of characteristic 2. Thanks to the friendly mapping Ψ_1, introduced in the previous section, we have a correspondence between polynomials in $\mathcal{F}$ and the set of $n \times n$ matrices. Hence, we can shift from a functional point of view to a matrix point of view. According to the definition of friendly mapping Ψ_1, we know that the matrices associated to the polynomials in $\mathcal{F}$ are alternative matrices. Thus, if two polynomials of $\mathcal{F}$ are linearly equivalent, then their associated alternative matrices are congruent. Note that the congruence considered is not under the general linear group $GL_n(\mathbb{F}_{q^n})$ as usual but under its subgroup $\mathcal{B}$ (as defined in Lemma 2).

Definition 7. Let $\mathcal{A}_n$ be the set of alternative matrices of order n over $\mathbb{F}_{q^n}$. We say that $S_1 \in \mathcal{A}_n$ and $S_2 \in \mathcal{A}_n$ are linearly equivalent if there exits $M \in \mathcal{B}$ such that $S_2 = MS_1M^{\mathrm{T}}$.

As $\mathcal{B}$ forms a group under the matrix multiplication, the linear equivalence is indeed an equivalence relation. Hence, the set $\mathcal{A}_n$ can be written as a disjoint union of linear equivalence classes, namely

$$\mathcal{A}_n = L_1 \dot{\cup}\ L_2 \dot{\cup} \cdots \dot{\cup} L_m, \tag{5}$$

where m is the total number of linear equivalence classes. Our goal is to find the number m as well as the number of matrices in each class. To address this enumeration problem, we first determine the congruent equivalence classes of $\mathcal{A}_n$ under the group action of the general linear group $GL_n(\mathbb{F}_{q^n})$. We then try to partition these congruent classes into disjoint union of linear equivalence classes.

Lemma 4. *Let $\mathbb{F}_q$ be a finite field with q elements, K be an $n \times n$ alternative matrix over $\mathbb{F}_q$, then the rank of K must be even. Conversely, if* $\mathrm{Rank(K)} = 2\nu$*, then K must be congruent under $GL_n(\mathbb{F}_q)$ to a matrix of the following form:*

$$\begin{pmatrix} 0^{(\nu)} & I^{(\nu)} & \\ -I^{(\nu)} & 0^{(\nu)} & \\ & & 0^{(n-2\nu)} \end{pmatrix}.$$

Two $n \times n$ alternative matrices are congruent if and only if they have the same rank.

PROOF. See Page 107, Theorem 3.1 of [22]. □

Using the congruent equivalence relation under $GL_n(\mathbb{F}_{q^n})$, we can divide $\mathcal{A}_n$ into $\left(\lfloor \frac{n}{2} \rfloor + 1\right)$ partitions, i.e. $\left(\lfloor \frac{n}{2} \rfloor + 1\right)$ congruent equivalence classes, each class contains alternative matrices having the same rank. Suppose these equivalence classes are $G_0 = \{O_{n\times n}\}, G_2, \cdots, G_{2\lfloor \frac{n}{2} \rfloor}$, where G_t contains alternative matrices with rank t. Then

$$\mathcal{A}_n = G_0 \cup G_2 \cup \cdots \cup G_{2\lfloor \frac{n}{2} \rfloor}.$$

Usually, we do not consider the class G_0.

In the terminology of group theory, $\mathcal{A}_n$ is the target set and $GL_n(\mathbb{F}_{q^n})$ is the group acting on $\mathcal{A}_n$. Every set G_t is an orbit under this group action. We know then the total number of orbits is $\left(\lfloor \frac{n}{2} \rfloor + 1\right)$. Next, we want to determine the length of each orbit. Namely, we try to count how many elements there are in each congruent equivalence class. To do this, we introduce the concept of extended symplectic group.

Definition 8. Let $K_e = \begin{pmatrix} K & 0^{2\nu\times(n-2\nu)} \\ 0^{(n-2\nu)\times 2\nu} & 0^{(n-2\nu)} \end{pmatrix}$ be an alternative matrix over $\mathbb{F}_q$, where $K = \begin{pmatrix} 0^{(\nu)} & I^{(\nu)} \\ -I^{(\nu)} & 0^{(\nu)} \end{pmatrix}$. The extended symplectic group $Sp_{n,\nu}(\mathbb{F}_q)$ is the set of all non-singular $n \times n$ matrices T satisfying $TK_eT^{\mathrm{T}} = K_e$.

Matrices in the extended symplectic group are of the following form.

Lemma 5. *$Sp_{n,\nu}(\mathbb{F}_q)$ consists of matrices of the form:*

$$\begin{pmatrix} T_{11} & T_{12} \\ 0^{(n-2\nu)\times 2\nu} & T_{22} \end{pmatrix}$$

with the requirement that $T_{11}KT_{11}^{\mathrm{T}} = K$ and T_{22} is an invertible matrix of order $n - 2\nu$, where K is as in Definition 8.

This will be used in Section 4. The following well known facts (for instance, you can see in [22]) will be also useful.

Lemma 6. *1) The number of invertible $n \times n$ matrices over $\mathbb{F}_q$ is*

$$|GL_n(\mathbb{F}_q)| = q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n}(q^i - 1).$$

2) The number of matrices in the extended symplectic group $Sp_{n,\nu}(\mathbb{F}_q)$ is

$$|Sp_{n,\nu}(\mathbb{F}_q)| = \prod_{i=1}^{\nu}(q^{2i} - 1) \prod_{i=1}^{\ell}(q^i - 1) q^{\nu^2 + 2\nu\ell + \frac{\ell(\ell-1)}{2}},$$

where $\ell = n - 2\nu$.

Now, we are ready to compute the length of the orbit $G_{2\nu}$.

Theorem 1. *The number of different elements in $G_{2\nu}$ is*

$$\frac{|GL_n(\mathbb{F}_{q^n})|}{|Sp_{n,\nu}(\mathbb{F}_{q^n})|} = \frac{\prod_{i=1}^{n}(q^{ni}-1)q^{\frac{n^2(n-1)}{2}}}{\prod_{i=1}^{\nu}(q^{2ni}-1)\prod_{i=1}^{\ell}(q^{ni}-1)q^{n(\nu^2+2\nu\ell+\frac{\ell(\ell-1)}{2})}},$$

where $\ell = n - 2\nu$.

Proof. According to Lemma 4, every matrix in $G_{2\nu}$ must be congruent to an alternative $n \times n$ matrix K_e as defined in Definition 8. Thus, each matrix in $G_{2\nu}$ has the form of MK_eM^{T}, where M is an invertible $n \times n$ matrix over $\mathbb{F}_{q^n}$. Therefore, if two elements $M_1K_eM_1^{\mathrm{T}} = M_2K_eM_2^{\mathrm{T}}$, it follows that $K_e = (M_1^{-1}M_2)K_e(M_1^{-1}M_2)^{\mathrm{T}}$, hence $M_1^{-1}M_2 \in Sp_{n,\nu}(\mathbb{F}_{q^n})$. Then the number of different elements in $G_{2\nu}$ is $|GL_n(\mathbb{F}_{q^n})|/|Sp_{n,\nu}(\mathbb{F}_{q^n})|$. □

We now consider the partition of (5). As $\mathcal{B}$ is a subgroup of $GL_n(\mathbb{F}_{q^n})$, every L_i must be contained in some G_j. This means that each G_j must be a disjoint union of some L_i's. Suppose that G_t has m_t partitions, i.e.

$$G_t = L_{t,1} \dot{\cup} L_{t,2} \dot{\cup} \cdots \dot{\cup} L_{t,m_t}.$$

Then, $m = m_0 + m_2 + \cdots + m_{2\lfloor \frac{n}{2} \rfloor}$. Now, we try to estimate the value of m_t. We provide a lower bound of m_t and then derive a lower bound of m.

Theorem 2. *The number of elements in $L_{t,j}$ is upper bounded by the order of $\mathcal{B}$, i.e.*

$$|L_{t,j}| \leq \prod_{i=1}^{n}(q^i-1)q^{\frac{n(n-1)}{2}}.$$

Proof. The orbit equation yields $|L_{t,j}| = [\mathcal{B} : T_{t,j}]$, where $T_{t,j}$ is the stabilizer of some matrix in $L_{t,j}$ under the group action of $\mathcal{B}$. Obviously $|T_{t,j}| \geq 1$, and thus $|L_{t,j}| \leq |\mathcal{B}|$. From Lemma 2, $\mathcal{B} \cong GL_n(\mathbb{F}_q)$ and we conclude by using 1) of Lemma 6. □

In the proof, the number of elements in $L_{t,j}$ are obtained using the stabilizer of some matrix in $L_{t,j}$ under the group action of $\mathcal{B}$. This is somewhat the core difficulty of enumeration problems in general. By combining Theorem 1 and Theorem 2, we get:

Theorem 3. *It holds that $m_{2\nu}$ is at least $\frac{|G_{2\nu}|}{|GL_n(\mathbb{F}_q)|}$ for $1 \leq \nu \leq \lfloor \frac{n}{2} \rfloor$, i.e.*

$$m_{2\nu} \geq \frac{\prod_{i=1}^{n}(q^{ni}-1)q^{\frac{n^2(n-1)}{2}}}{\prod_{i=1}^{\nu}(q^{2ni}-1)\prod_{i=1}^{\ell}(q^{ni}-1)q^{n(\nu^2+2\nu\ell+\frac{\ell(\ell-1)}{2})}\prod_{i=1}^{n}(q^i-1)q^{\frac{n(n-1)}{2}}},$$

where $\ell = n - 2\nu$.

PROOF. Since $G_{2\nu} = L_{2\nu,1} \dot\cup L_{2\nu,2} \dot\cup \cdots \dot\cup L_{2\nu,m_{2\nu}}$, Theorem 2 yields

$$|G_{2\nu}| = \sum_{i=1}^{m_{2\nu}} |L_{2\nu,i}| \leq \sum_{i=1}^{m_{2\nu}} |\mathcal{B}| = m_{2\nu}|\mathcal{B}|.$$

□

Corollary 1. *A lower bound for the number of linear equivalence classes is*

$$\sum_{\nu=1}^{\lfloor \frac{n}{2} \rfloor} \frac{\prod_{i=1}^{n}(q^{ni}-1)q^{\frac{n^2(n-1)}{2}}}{\prod_{i=1}^{\nu}(q^{2ni}-1)\prod_{i=1}^{\ell}(q^{ni}-1)q^{n(\nu^2+2\nu\ell+\frac{\ell(\ell-1)}{2})}\prod_{i=1}^{n}(q^i-1)q^{\frac{n(n-1)}{2}}} + 1,$$

where $\ell = n - 2\nu$.

3.2. Isomorphism Equivalence Classes when $\mathrm{char}(\mathbb{F}_q) \neq 2$

We suppose here that the characteristic of $\mathbb{F}_q$ is odd. As in the previous subsection, we try to get a lower bound on the number of all linear equivalence classes. Here, we use orthogonal geometry over finite fields. Let S be a non-singular symmetric matrix over $\mathbb{F}_q$. We shall say that an invertible matrix T is an orthogonal matrix with respect to S if $TST^{\mathrm{T}} = S$. The set of all orthogonal matrices forms a group under matrix multiplication. We call this group orthogonal group of order n with respect to S. It will be denoted by $O_n(\mathbb{F}_q, S)$.

Lemma 7. *Every symmetric matrix over* $\mathbb{F}_q$ *is congruent to exactly one of the following matrices:*

$$M(n,2\nu,\nu) = \begin{pmatrix} S & \\ & 0^{(n-2\nu)} \end{pmatrix}, \qquad M(n+1,2\nu+1,\nu,1) = \begin{pmatrix} S & & \\ & 1 & \\ & & 0^{(n-2\nu)} \end{pmatrix},$$

$$M(n+1,2\nu+1,\nu,z) = \begin{pmatrix} S & & \\ & z & \\ & & 0^{(n-2\nu)} \end{pmatrix}, \quad M(n+2,2\nu+2,\nu) = \begin{pmatrix} S & & & \\ & 1 & & \\ & & -z & \\ & & & 0^{(n-2\nu)} \end{pmatrix},$$

where $S = \begin{pmatrix} 0^{(\nu)} & I^{(\nu)} \\ I^{(\nu)} & 0^{(\nu)} \end{pmatrix}$ *and* z *is a fixed non-square element in* $\mathbb{F}_q^*$.

For the proof, we refer again to [22].

Let $\mathcal{S}$ be the set of all symmetric matrices of order n over $\mathbb{F}_{q^n}$. According to Lemma 7, we can divide $\mathcal{S}$ into $2n+1$ congruent equivalence classes under the general linear group $GL_n(\mathbb{F}_{q^n})$. We have to compute how many linear equivalence classes are in each congruent equivalence class and how many different matrices in each linear equivalence class.

Let $S_e = \begin{pmatrix} S & 0_{(2\nu+\delta)\times\ell} \\ 0_{\ell\times(2\nu+\delta)} & 0^{(\ell)} \end{pmatrix}$, where $S = M(2\nu+\delta, 2\nu+\delta, \nu, \Delta)$ is the canonical form as defined in Lemma 7 and Δ represents the definite fixed part of the corresponding form. The set of all $(2\nu+\delta+\ell) \times (2\nu+\delta+\ell)$ invertible matrices T such that $TS_eT^{\mathrm{T}} = S_e$ forms a group. This group is the extended orthogonal group, written as $O_{2\nu+\delta+\ell,2\nu+\delta,\nu,\Delta}(\mathbb{F}_q)$ or $O_{2\nu+\delta+\ell,\Delta}(\mathbb{F}_q)$ in short. The general form of such matrices is given below:

Lemma 8. *$O_{2\nu+\delta+\ell,\Delta}(\mathbb{F}_q)$ consists of matrices of the form:*

$$\begin{pmatrix} T_{11} & T_{12} \\ 0_{\ell\times(2\nu+\delta)} & T_{22} \end{pmatrix}$$

with the requirement that $T_{11}ST_{11}^{\mathrm{T}} = S$ and T_{22} is an invertible matrix of order ℓ, where $S = M(2\nu+\delta, 2\nu+\delta, \nu, \Delta)$.

Lemma 9. *The order of $O_{2\nu+\delta+\ell,\Delta}(\mathbb{F}_q)$ is*

$$|O_{2\nu+\delta+\ell,\Delta}(\mathbb{F}_q)| = \prod_{i=1}^{\nu}(q^i-1)\prod_{i=0}^{\nu+\delta-1}(q^i+1)\prod_{i=1}^{\ell}(q^i-1)q^{\nu(\nu+\delta-1)+\ell(2\nu+\delta)+\frac{\ell(\ell-1)}{2}}.$$

Again, we refer to [22] for a proof.

Corollary 2. *Let $\mathcal{S}_{n,2\nu+\delta,\nu,\Delta}(\mathbb{F}_{q^n})$ be the set of all symmetric matrices congruent to $M(n, 2\nu+\delta, \nu, \Delta)$, then*

$$|\mathcal{S}_{n,2\nu+\delta,\nu,\Delta}(\mathbb{F}_{q^n})| = \frac{|GL_n(\mathbb{F}_{q^n})|}{|O_{2\nu+\delta+\ell,\Delta}(\mathbb{F}_{q^n})|}.$$

According to Theorem 2, each congruent class must be a disjoint union of some linear equivalence classes, and each one contains at most $|GL_n(\mathbb{F}_q)|$ different elements. Thus:

Theorem 4. *The number of linear equivalence classes contained in $\mathcal{S}_{n,2\nu+\delta,\nu,\Delta}(\mathbb{F}_q)$ is lower bounded by:*

$$\frac{|GL_n(\mathbb{F}_{q^n})|}{(|O_{2\nu+\delta+\ell,\Delta}(\mathbb{F}_{q^n})|)(|GL_n(\mathbb{F}_q)|)},$$

where $\ell = n-2\nu-\delta$.

Finally, by running on all the possibilities of choices of ν, δ and Δ, we get:

Corollary 3. *A lower bound of the number of linear equivalence classes is:*

$$\sum_{i=1}^{\lfloor\frac{n}{2}\rfloor}\left(\frac{|GL_n(\mathbb{F}_{q^n})|}{(|O_{2i+0+(n-2i),\Delta}(\mathbb{F}_{q^n})|)(|GL_n(\mathbb{F}_q)|)} + \frac{|GL_n(\mathbb{F}_{q^n})|}{(|O_{2(i-1)+2+(n-2i),\Delta}(\mathbb{F}_{q^n})|)(|GL_n(\mathbb{F}_q)|)}\right) + \sum_{i=0}^{\lceil\frac{n}{2}\rceil-1}\frac{2|GL_n(\mathbb{F}_{q^n})|}{(|O_{2i+1+(n-2i-1),1}(\mathbb{F}_{q^n})|)(|GL_n(\mathbb{F}_q)|)} + 1.$$

3.3. Tightness of the bounds

The lower bounds given in this section are very rough. When $\mathrm{char}(\mathbb{F}_q) = 2$, Ψ_1 throws away the terms of the form X^{2q^i}. Thus the target set $\mathcal{A}_n$ is much smaller than the original target set $\mathcal{F}$. We actually estimate the lower bound of number of linear equivalence class of polynomials of the form $\sum_{i=0}^{n-1}\alpha_{ij}X^{q^i+q^j}$ with $i \neq j$, but this does not affect much on the analysis of corresponding scheme as already shown in the book [24].

Another reason for the untightness is that we roughly use the order of $GL_n(\mathbb{F}_q)$ as the cardinality of each linear equivalence class. Actually, different equivalence classes may have different cardinalities, that means there may be many linear equivalence classes whose cardinalities are much smaller than $|GL_n(\mathbb{F}_q)|$. As an example, please see Corollary 4 and Corollary 5 of Section 4. As a result, even if we can compute the exact size of some equivalence classes, we still can not take advantage of the results to compute the sizes of other classes.

The size of each equivalence class depends much on the properties of the polynomials of the class. We note that the size of the equivalence class containing permutation polynomials must be exactly $|GL_n(\mathbb{F}_q)|$, but for some non-permutation polynomials, its orbit can also contain $|GL_n(\mathbb{F}_q)|$ elements. How to characterize such polynomials is still an open problem.

From the viewpoint of finite geometry, the IP problem is related to identifying the standard form of alternative matrices (resp. symmetric matrices) when $\mathrm{char}(\mathbb{F}_q) = 2$ (resp. $\mathrm{char}(\mathbb{F}_q) \neq 2$) under the congruence action of special group $\mathcal{B}$ (see Lemma 2). As some elementary matrices are not in $\mathcal{B}$, such problem become difficult and many classical results of finite geometry are not appliable in such cases.

4. Applications to Multivariate Public-Key Crytptography

In this section, we count the number of different schemes and equivalent keys that can be derived from monomials over extension field. This kind of schemes is a generalization of Matsumoto–Imai scheme (a.k.a. C* scheme) whose central function is of the form X^{q^t+1} with $\gcd(q^n-1, q^t+1) = 1$ [1]. We call such generalization *MI-type schemes*.

Definition 9. Let $\mathbb{F}_q$ be finite field with q elements and n be a positive integer. We shall say that $L_1 \circ F \circ L_2$ is a MI-type scheme if L_1 and L_2 are invertible linear transformations over $\mathbb{F}_q^n$ and F is a monomial over $\mathbb{F}_{q^n}$ of the form $aX^{q^i+q^j}$, for $i, j, 0 \leq i, j \leq n-1$ and $a \in \mathbb{F}_{q^n}^*$.

For such schemes, our goal is to identify all its equivalence classes and count the number of elements in each class. We emphasize that the purpose of the generalization is not to increase the security of the scheme. The basic Patarin's bi-linear attack [8] against C* still works for MI-type schemes.

Let $\mathcal{F}$ be as defined in Section 2. Under the linear equivalence relation, $\mathcal{F}$ can be divided into disjoint equivalence classes. In the sequel, we call a monomial of $\mathcal{F}$ a "*monomial point*" and the equivalence class an "*orbit*".

For all $f \in \mathbb{F}_{q^n}[X]$, we can associate a polynomial mapping $f : c \mapsto f(c)$ from $\mathbb{F}_{q^n}$ into $\mathbb{F}_{q^n}$. Let $\mathcal{R}(f) = \{f(c) | c \in \mathbb{F}_{q^n}^*\}$ and $\ker(f) = \{c \in \mathbb{F}_{q^n}^* | f(c) = 1\}$, here we use f to denote both the polynomial and the associated mapping. Then $\mathcal{R}(X^{q^{i+t}+q^t}) = \mathcal{R}(X^{q^i+1})$ and $|\mathcal{R}(X^{q^{i+t}+q^t})| = |\mathcal{R}(X^{q^i+1})| = \frac{q^n-1}{\gcd(q^i+1, q^n-1)}$ for any $t, 0 \leq t \leq n-1$.

4.1. Number of Orbits Containing Monomials

In this subsection, we determine how many equivalence classes contain monomials. Before stating the main results of this part, we give several intermediate results which will be used through this section.

Hereafter, we will use $E_i(c)$ to denote the elementary matrix obtained by multiplying the i-th row of identity matrix by c, E_{ij} the elementary matrix obtained by interchanging the i-th row and j-th row of identity matrix, and $E_{ij}(c)$ the elementary matrix obtained by adding the i-th row multiplied by c to the j-th row of identity matrix.

Lemma 10. *Let $a, b \in \mathbb{F}_{q^n}^*$ and $0 \leq i \leq n-1$. The monomial aX^{2q^i} can not be linearly equivalent to $bX^{q^u+q^v}$ for any $u \neq v$.*

PROOF. By contradiction, assume there exists an invertible linear transformation $L(X)$ such that $aX^{2q^i} \circ L(X) = bX^{q^u+q^v}$. By the definition of Ψ_1, we have $\hat{L}\Psi_1(aX^{2q^i})\hat{L}^{\mathrm{T}} = \Psi_1(bX^{q^u+q^v})$. It follows

$$\mathrm{Rank}\big(\hat{L}\Psi_1(aX^{2q^i})\hat{L}^{\mathrm{T}}\big) = \mathrm{Rank}\big(\Psi_1(bX^{q^u+q^v})\big).$$

But $\mathrm{Rank}\big(\Psi_1(bX^{q^u+q^v})\big) = 2$. On the other hand:

$$\mathrm{Rank}(\hat{L}\Psi_1(aX^{2q^i})\hat{L}^{\mathrm{T}}) = \mathrm{Rank}(\Psi_1(aX^{2q^i})) = \begin{cases} 0 & , \quad \mathrm{char}(\mathbb{F}_q) = 2, \\ 1 & , \quad \mathrm{char}(\mathbb{F}_q) \neq 2, \end{cases}$$

which leads to a contradiction. Thus the lemma is proved. □

Lemma 11. *Let $0 \leq i, j \leq n-1$ and $L(X)$ be a linear transformation:*

(i) *$L(X)$ is a monomial if and only if $X^{q^i} \circ L(X) \circ X^{q^j}$ is a monomial;*
(ii) *$L(X)$ is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if $X^{q^i} \circ L(X) \circ X^{q^j}$ is a permutation polynomial of $\mathbb{F}_{q^n}$.*

PROOF. This lemma is trivial from the truth that X^{q^i} and X^{q^j} are both permutation polynomials over $\mathbb{F}_{q^n}$ and their inverse polynomials are also monomials. □

Lemma 12. *If there exists an invertible linear transformation $L(X) = \sum_{k=0}^{n-1} c_k X^{q^k}$ such that $aX^{2q^i} \circ L(X) = bX^{2q^j}$ with $0 \leq i, j \leq (n-1)$ and $a, b \in \mathbb{F}_{q^n}^*$, then $L(X)$ must be a monomial.*

PROOF. When $\mathrm{char}(\mathbb{F}_q) = 2$:

$$bX^{2q^j} = aX^{2q^i} \circ L(X) = a\left(\sum_{k=0}^{n-1} c_k X^{q^k}\right)^{2q^i} = \sum_{k=0}^{n-1} a c_k^{2q^i} X^{2q^{k+i}}.$$

Thus $c_{j-i}^{2q^i} = a^{-1}b$ and the others coefficients of $L(X)$ must be zero, where the index of c_i is computed modulo n.

When $\mathrm{char}(\mathbb{F}_q) \neq 2$: by assumption, we have

$$aX^{2q^i} \circ L(X) = bX^{2q^j} \Leftrightarrow X^2 \circ (X^{q^i} \circ L(X) \circ X^{q^{n-j}}) = a^{-1}bX^2.$$

By Lemma 11, it is sufficient to prove that if there exists an invertible linear transformation $L(X)$ such that $X^2 \circ L(X) = cX^2$, then $L(X)$ must be a monomial.

By the very definition of Ψ_1, we have that $\hat{L}\Psi_1(X^2)\hat{L}^{\mathrm{T}} = \Psi_1(cX^2)$, where $\hat{L}$ is the associated matrix to $L(X)$ and thus $\hat{L} \in \mathcal{B}$ as in Lemma 2. By letting $X = 1$ in $X^2 \circ L(X) = cX^2$ it follows that $c = (L(1))^2$. Thus c must be a square element of $\mathbb{F}_{q^n}$. Now, let $c = \alpha^2$, we have

$$\begin{pmatrix} \alpha & \\ & I^{(n-1)} \end{pmatrix} \begin{pmatrix} 2 & \\ & I^{(n-1)} \end{pmatrix} \begin{pmatrix} \alpha & \\ & I^{(n-1)} \end{pmatrix} = \begin{pmatrix} 2c & \\ & I^{(n-1)} \end{pmatrix},$$

i.e. $E_1(\alpha)\Psi_1(X^2)E_1(\alpha)^{\mathrm{T}} = \Psi_1(cX^2)$. Thus

$$\hat{L}\Psi_1(X^2)\hat{L}^{\mathrm{T}} = E_1(\alpha)\Psi_1(X^2)E_1(\alpha)^{\mathrm{T}}, \quad (E_1(\alpha)^{-1}\hat{L})\Psi_1(X^2)(E_1(\alpha)^{-1}\hat{L})^{\mathrm{T}} = \Psi_1(X^2).$$

Therefore $\hat{L} \in E_1(\alpha)O_n\big(\mathbb{F}_{q^n}, \Psi_1(X^2)\big)$. By Lemma 8, $\hat{L} \in E_1\big(\alpha)O_n(\mathbb{F}_{q^n}, \Psi_1(X^2)\big)$ must be in the following form:

$$\begin{pmatrix} \alpha a_{11} & \alpha T_{12} \\ 0_{(n-1)\times 1} & T_{22} \end{pmatrix}.$$

with $a_{11}^2 = 1$ and T_{22} invertible. The fact that $\hat{L} \in \mathcal{B}$ implies that $\hat{L}$ is a diagonal matrix. Hence, the linear polynomial $L(X)$ corresponding to $\hat{L}$ is a monomial. □

The following result is about the monomial $bX^{q^u+q^v}$, with $u \neq v$.

Lemma 13. *If there exists an invertible linear transformation $L(X) = \sum_{k=0}^{n-1} c_k X^{q^k}$ such that $aX^{q^s+q^t} \circ L(X) = bX^{q^u+q^v}$ with $s \neq t, u \neq v$, then $L(X)$ must be a monomial.*

Proof. Clearly, by Lemma 11, it is sufficient to prove that if there exists an invertible linear transformation $L(X)$ such that $X^{q^i+1} \circ L(X) = cX^{q^j+1}$ where $1 \leq i, j \leq n-1$, then $L(X)$ must be a monomial. Without loss of generality we can suppose that $1 \leq i \leq j \leq n-1$. Now we first consider the case $\mathrm{char}(\mathbb{F}_q) = 2$.

By the definition of Ψ_1, we have $\hat{L}\Psi_1(X^{q^i+1})\hat{L}^{\mathrm{T}} = \Psi_1(cX^{q^j+1})$, where $\hat{L} \in \mathcal{B}$ is the matrix associated to L as in Lemma 2. Since

$$E_{j+1}(c)E_{i+1,j+1}\Psi_1(X^{q^i+1})E_{i+1,j+1}^{\mathrm{T}}E_{j+1}(c)^{\mathrm{T}} = \Psi_1(cX^{q^j+1}),$$

we have

$$\hat{L} \in E_{j+1}(c)E_{i+1,j+1}Sp_n(\mathbb{F}_{q^n}, \Psi_1(X^{q^i+1})).$$

Since $Sp_n\big(\mathbb{F}_{q^n}, \Psi_1(X^{q^i+1})\big) = E_{2,i+1}Sp_n\big(\mathbb{F}_{q^n}, \Psi_1(X^{q+1})\big)E_{2,i+1}$, so, by Lemma 5, a matrix in $Sp_n\big(\mathbb{F}_{q^n}, \Psi_1(X^{q^i+1})\big)$ must be of the form:

$$\begin{pmatrix}
a_{11} & a_{1,i+1} & a_{13} & \dots & a_{1i} & a_{12} & a_{1,i+2} & \dots & a_{1n} \\
0 & a_{i+1,i+1} & a_{i+1,3} & \dots & a_{i+1,i} & 0 & a_{i+1,i+2} & \dots & a_{i+1,n} \\
0 & a_{3,i+1} & a_{33} & \dots & a_{3i} & 0 & a_{3,i+2} & \dots & a_{3n} \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\
0 & a_{i,i+1} & a_{i3} & \dots & a_{ii} & 0 & a_{i,i+2} & \dots & a_{in} \\
a_{21} & a_{2,i+1} & a_{23} & \dots & a_{2i} & a_{22} & a_{2,i+2} & \dots & a_{2n} \\
0 & a_{i+2,i+1} & a_{i+2,3} & \dots & a_{i+2,i} & 0 & a_{i+2,i+2} & \dots & a_{i+2,n} \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\
0 & a_{n,i+1} & a_{n3} & \dots & a_{ni} & 0 & a_{n,i+2} & \dots & a_{nn}
\end{pmatrix}.$$

with

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } \left| \begin{pmatrix} a_{33} & \cdots & a_{3n} \\ \vdots & \ddots & \vdots \\ a_{n3} & \cdots & a_{nn} \end{pmatrix} \right| \neq 0.$$

Thus, $\hat{L} \in E_{j+1}(c)E_{i+1,j+1}Sp_n\big(\mathbb{F}_{q^n}, \Psi_1(X^{q^i+1})\big)$ is of the form

$$\begin{pmatrix} a_{11} & a_{1,i+1} & a_{13} & \dots & a_{1i} & a_{12} & a_{1,i+2} & \dots & a_{1n} \\ 0 & a_{i+1,i+1} & a_{i+1,3} & \dots & a_{i+1,i} & 0 & a_{i+1,i+2} & \dots & a_{i+1,n} \\ 0 & a_{3,i+1} & a_{33} & \dots & a_{3i} & 0 & a_{3,i+2} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & a_{i,i+1} & a_{i3} & \dots & a_{ii} & 0 & a_{i,i+2} & \dots & a_{in} \\ 0 & a_{j+1,i+1} & a_{j+1,3} & \dots & a_{j+1,i} & 0 & a_{j+1,i+2} & \dots & a_{j+1,n} \\ 0 & a_{i+2,i+1} & a_{i+2,3} & \dots & a_{i+2,i} & 0 & a_{i+2,i+2} & \dots & a_{i+2,n} \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ ca_{21} & ca_{2,i+1} & ca_{23} & \dots & ca_{2i} & ca_{22} & ca_{2,i+2} & \dots & ca_{2n} \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & a_{n,i+1} & a_{n3} & \dots & a_{ni} & 0 & a_{n,i+2} & \dots & a_{nn} \end{pmatrix}.$$

Note that $\hat{L} \in \mathcal{B}$ and any diagonal of a matrix in $\mathcal{B}$ is of the form $\{\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}\}$ with some $\alpha \in \mathbb{F}_{q^n}$. Hence, there are at most two diagonals in $\hat{L}$ whose elements all are not zeros and elements in other diagonals are all zeros. These two non-zero diagonals are diagonals containing a_{11} and ca_{21} respectively. Now we investigate $\hat{L}$ in two cases:
Case 1. $i \neq \frac{n}{2}$, i.e. $i \neq n-i$.

- If $j \notin \{i, n-i\}$, then $\hat{L}$ is a zero matrix since there is a zero on each diagonal.
- If $j = i$, then the only nonzero diagonal is the main diagonal. Thus $L(X) = a_{11}X$.
- If $j = n-i$, then the only nonzero diagonal of $\hat{L}$ is the one containing ca_{21}. Thus $L(X) = ca_{21}X^{q^{n-i}}$.

Case 2. $i = \frac{n}{2}$, i.e. $i = n-i$.

- If $j \neq \frac{n}{2}$, then $\hat{L}$ is a zero matrix since there is no non-zero diagonal.
- If $j = \frac{n}{2}$, then there are two nonzero diagonals of $\hat{L}$. One is the main diagonal, the other is the one containing ca_{21}. Thus $L(X) = c_1X + c_2X^{q^{\frac{n}{2}}}$. By hypothesis that $X^{q^i+1} \circ L(X) = cX^{q^j+1}$, i.e. $X^{q^{\frac{n}{2}}+1} \circ L(X) = cX^{q^{\frac{n}{2}}+1}$, we have

$$\begin{aligned} cX^{q^{\frac{n}{2}}+1} &= X^{q^{\frac{n}{2}}+1} \circ L(X) = (c_1X + c_2X^{q^{\frac{n}{2}}})^{q^{\frac{n}{2}}+1} \\ &= (c_1^{q^{\frac{n}{2}}+1} + c_2^{q^{\frac{n}{2}}+1})X^{q^{\frac{n}{2}}+1} + c_1c_2^{q^{\frac{n}{2}}}X^2 + c_1^{q^{\frac{n}{2}}}c_2X^{2q^{\frac{n}{2}}}. \end{aligned}$$

Thus $c_1^{q^{\frac{n}{2}}+1} + c_2^{q^{\frac{n}{2}}+1} = c$ and $c_1c_2^{q^{\frac{n}{2}}} = c_1^{q^{\frac{n}{2}}}c_2 = 0$, which implies that $c_1 = 0$ or $c_2 = 0$, i.e. $L(X)$ is c_1X or $c_2X^{q^{\frac{n}{2}}}$.

For the case of $\mathrm{char}(\mathbb{F}_q) \neq 2$, the analysis is similar but we need replacing the extended symplectic group with the extended orthogonal group. □

By Lemma 10, we know that $\alpha X^{q^u+q^v}(u \neq v)$ and βX^{2q^i} can not be in the same orbit, so in the following of this section, we will study the two types of monomials seperately. First we will show the number of orbits containing some monomial of the form $aX^{q^u+q^v}$ $(u \neq v)$ and the number of monomials in each of these orbits.

Lemma 14. *The number of monomials in the orbit containing a fixed monomial* aX^{q^i+1} $(1 \leq i \leq n-1)$ *is* $n|\mathcal{R}(X^{q^i+1})|$ *when* $i \neq \frac{n}{2}$ *or* $\frac{n}{2}|\mathcal{R}(X^{q^i+1})|$ *otherwise.*

Proof. The number of monomials in the orbit containing a fixed monomial aX^{q^i+1} is exactly the number of monomials linearly equivalent to aX^{q^i+1}. If a monomial $bX^{q^s+q^t}$ is linearly equivalent to aX^{q^i+1}, then there exists a $L(X)$ such that $bX^{q^s+q^t} = aX^{q^i+1} \circ L(X)$. From Lemma 12 and Lemma 13, it follows that $L(X) = cX^{q^k}$. Thus all monomials linearly equivalent to aX^{q^i+1} come from $aX^{q^i+1} \circ cX^{q^k}$. Let

$$\begin{aligned}\mathcal{S} &= \{aX^{q^i+1} \circ cX^{q^k} | c \in \mathbb{F}_{q^n}^*, 0 \leq k \leq (n-1)\},\\ \mathcal{S}_k &= \{aX^{q^i+1} \circ cX^{q^k} | c \in \mathbb{F}_{q^n}^*\}\\ &= \{ac^{q^i+1}X^{q^{(i+k)}+q^k} | c \in \mathbb{F}_{q^n}^*\},\ 0 \leq k \leq (n-1).\end{aligned}$$

Then $\mathcal{S} = \bigcup_k \mathcal{S}_k$ and the coefficients of monomials in $\mathcal{S}_k$ are exactly a coset of $\mathcal{R}(X^{q^i+1})$ in the group $\mathbb{F}_{q^n}^*$, thus $|\mathcal{S}_k| = |\mathcal{R}(X^{q^i+1})|$ for $0 \leq k \leq (n-1)$. Now let us consider when $\mathcal{S}_{k_1} = \mathcal{S}_{k_2}$. It is east to see that the degrees of monomials in $\mathcal{S}_k$ are all $(q^{i+k}+q^k)$ mod (q^n-1), hence for $0 \leq k_1, k_2 \leq n-1$, if $\mathcal{S}_{k_1} = \mathcal{S}_{k_2}$, then $q^{i+k_1}+q^{k_1} \equiv q^{i+k_2}+q^{k_2}$ mod (q^n-1), i.e.

$$\text{(I)} \quad \begin{cases} i+k_1 \equiv i+k_2 \pmod n \\ k_1 \equiv k_2 \pmod n \end{cases} \quad \text{or} \quad \text{(II)} \quad \begin{cases} i+k_1 \equiv k_2 \pmod n \\ k_1 \equiv i+k_2 \pmod n \end{cases}$$

From (I), we get that $k_1 = k_2$. From (II), we get that $i = \frac{n}{2}$ and $k_1 \equiv \frac{n}{2} + k_2 (\mathrm{mod} n)$. So it follows that:
When $i \neq \frac{n}{2}$, $\mathcal{S}_0, \cdots, \mathcal{S}_{n-1}$ is a partition of $\mathcal{S}$. Hence $|\mathcal{S}| = n|\mathcal{R}(X^{q^i+1})|$.
When $i = \frac{n}{2}$, $\mathcal{S}_k = \mathcal{S}_{k+\frac{n}{2}}$ for $0 \leq k \leq \frac{n}{2}-1$. $\mathcal{S}_0, \cdots, \mathcal{S}_{\frac{n}{2}-1}$ is a partition of $\mathcal{S}$. Hence $|\mathcal{S}| = \frac{n}{2}|\mathcal{R}(X^{q^i+1})|$. □

Theorem 5. *The number of orbits containing some monomial* $aX^{q^u+q^v}$ $(0 \leq v < u \leq n-1)$ *is* $\sum_{k=1}^{\frac{1}{2}(n-1)} \frac{|\mathbb{F}_{q^n}^*|}{|\mathcal{R}(X^{q^k+1})|}$ *if* n *is odd or* $\sum_{k=1}^{\frac{n}{2}} \frac{|\mathbb{F}_{q^n}^*|}{|\mathcal{R}(X^{q^k+1})|}$ *if* n *is even.*

Proof. Since $aX^{q^u+q^v} = aX^{q^{u-v}+1} \circ X^{q^v}$, any monomial $aX^{q^u+q^v}$ is linearly equivalent to $aX^{q^{u-v}+1}$. It is then sufficient to determine the number of orbits that contains some monomials of the form aX^{q^k+1}. Let

$$\begin{aligned}\mathcal{M} &= \{aX^{q^k+1} | a \in \mathbb{F}_{q^n}^*,\ 1 \leq k \leq n-1\},\\ \mathcal{M}_k &= \{aX^{q^k+1} | a \in \mathbb{F}_{q^n}^*\},\ 1 \leq k \leq n-1.\end{aligned}$$

Then $\mathcal{M} = \bigcup_{k=1}^{n-1} \mathcal{M}_k$. From Lemma 13, we have αX^{q^i+1} and βX^{q^i+1} are linearly equivalent iff α and β are in the same coset of $\mathcal{R}(X^{q^i+1})$ in the group $\mathbb{F}_{q^n}^*$, therefore $\mathcal{M}_k$ is distributed in $|\mathbb{F}_{q^n}^*/\mathcal{R}(X^{q^k+1})|$ different orbits. Since $aX^{q^k+1} \circ X^{q^{n-k}} = aX^{q^{n-k}+1}$, aX^{q^k+1} and $aX^{q^{n-k}+1}$ are in the same orbit . Thus the orbits containing monomials in $\mathcal{M}_k$ also contains monomials in $\mathcal{M}_{n-k}$, i.e. monomials in $\mathcal{M}_k$ and $\mathcal{M}_{n-k}$ are distributed in $|\mathbb{F}_{q^n}^*/\mathcal{R}(X^{q^k+1})|$ $(= |\mathbb{F}_{q^n}^*/\mathcal{R}(X^{q^{n-k}+1})|)$ different orbits. Therefore

- When n is odd, $\mathcal{M}_1, \cdots, \mathcal{M}_{\frac{n-1}{2}}$ is a partition of $\mathcal{M}$, thus $\mathcal{M}$ is distributed in $\sum_{k=1}^{\frac{1}{2}(n-1)} \frac{|\mathbb{F}_{q^n}^*|}{|\mathcal{R}(X^{q^k+1})|}$ different orbits.
- When n is even, $\mathcal{M}_1, \cdots, \mathcal{M}_{\frac{n-2}{2}}, \mathcal{M}_{\frac{n}{2}}$ is a partition of $\mathcal{M}$, thus $\mathcal{M}$ is distributed in
$$\sum_{k=1}^{\frac{1}{2}(n-2)} \frac{|\mathbb{F}_{q^n}^*|}{|\mathcal{R}(X^{q^k+1})|} + \frac{|\mathbb{F}_{q^n}^*|}{|\mathcal{R}(X^{q^{n/2}+1})|} = \sum_{k=1}^{\frac{n}{2}} \frac{|\mathbb{F}_{q^n}^*|}{|\mathcal{R}(X^{q^k+1})|}$$
different orbits. □

For monomials of the form aX^{2q^i}, we have:

Theorem 6. *When* $\mathrm{char}(\mathbb{F}_q) = 2$*, all monomials of the form* aX^{2q^i} *are in one orbit, in which there are* $n(q^n-1)$ *monomials. When* $\mathrm{char}(\mathbb{F}_q) \neq 2$*, all monomials of the form* aX^{2q^i} *are in two orbits, in each of them there are exact* $\frac{1}{2}n(q^n-1)$ *monomials.*

Proof. From Lemma 12, we can deduce that two monomials αX^{2q^u} and βX^{2q^v} are in the same orbit if and only if $\alpha^{-1}\beta$ is a square element of $\mathbb{F}_{q^n}$.
When $\mathrm{char}(\mathbb{F}_q) = 2$, all elements of $\mathbb{F}_{q^n}^*$ are square elements. Hence two arbitrary monomials αX^{2q^u} and βX^{2q^v} are in the same orbit since $\alpha^{-1}\beta$ is always a square element. And therefore there are $n(q^n-1)$ monomials of the form aX^{2q^i} in the orbit.
When $\mathrm{char}(\mathbb{F}_q) \neq 2$, there are exact $\frac{1}{2}(q^n-1)$ square elements and $\frac{1}{2}(q^n-1)$ non-square elements of $\mathbb{F}_{q^n}^*$. For two elements α and β, $\alpha^{-1}\beta$ is a square element if and only if both α and β are square elements or non-square elements simultaneously. Thus all monomials aX^{2q^i} whose coefficients are square elements (resp. non-square elements) are in the same orbits. Then the conclusion follows immediately. □

To summarize:

Theorem 7. *The number of orbits containing monomial points is:*

$$\begin{cases} \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \frac{|\mathbb{F}_{q^n}^*|}{|\mathcal{R}(X^{q^k+1})|} + 1, & \text{if } \mathrm{char}(\mathbb{F}_q) = 2, \\ \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \frac{|\mathbb{F}_{q^n}^*|}{|\mathcal{R}(X^{q^k+1})|} + 2, & \text{if } \mathrm{char}(\mathbb{F}_q) \neq 2. \end{cases}$$

Proof. The proof is obtained thanks to Theorem 5 and Theorem 6. □

In the formulae of Theorem 7, $\sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \frac{|\mathbb{F}_{q^n}^*|}{|\mathcal{R}(X^{q^k+1})|}$ represents the number of orbits containing monomial of the form $aX^{q^u+q^v}(u \neq v)$. The rest part represents the number of orbits containing monomial of the form aX^{2q^i} in function of the characteristic.

4.2. Length of Orbits Containing Monomial Points

We compute here the length of orbits containing monomial points. As already pointed out, this is equivalent to describe non-equivalent keys of a MPKC scheme. In particular, we show that some HFE instances, i.e. with more than one monomial occurring in the central function, can be equivalent to MI-type schemes. Thus, considering the insecurity of MI-type schemes, we have of course to avoid such weak instances. To compute the length of an orbit, we have to identify the stabilizer of such monomial under the action of invertible linear transformations.

Definition 10. The stabilizer of $F \in \mathcal{F}$ is defined as the set of all invertible linear transformation $L(X) \in \mathcal{L}$ defined in Section 2.3 such that $F \circ L(X) = F$.

Clearly, the stabilizer of F is a subgroup of $\mathcal{L}$ which is isomorphic to $GL_n(\mathbb{F}_q)$. If the mapping induced by F is bijective, then the stabilizer of F has only one element, i.e. X. For a monomial point, we can describe its stabilizer as follows.

Theorem 8. *Let $1 \leq i \leq n-1$ and $a \in \mathbb{F}_{q^n}^*$. The stabilizer of aX^{q^i+1} is $\{cX | c^{q^i+1} = 1, c \in \mathbb{F}_{q^n}^*\}$ when $i \neq \frac{n}{2}$ and $\{cX^{q^t} | c^{q^i+1} = 1, c \in \mathbb{F}_{q^n}^*$ and $t = 0$ or $\frac{n}{2}\}$ when $i = \frac{n}{2}$.*

Proof. By definition, the stabilizer of aX^{q^i+1} is the set of all invertible linear transformation $L(X)$ such that $aX^{q^i+1} \circ L(X) = aX^{q^i+1}$. From Lemma 12 and Lemma 13, it follows that $L(X) = cX^{q^k}$. We have then

$$aX^{q^i+1} = aX^{q^i+1} \circ L(X) = aX^{q^i+1} \circ cX^{q^k} = ac^{q^i+1}X^{q^{i+k}+q^k}.$$

This leads to the following equivalent conditions : $c^{q^i+1} = 1$ and two systems of congruence equations:

$$\text{(I)} \quad \begin{cases} i + k \equiv i \pmod{n} \\ k \equiv 0 \pmod{n} \end{cases} \quad \text{or} \quad \text{(II)} \quad \begin{cases} i + k \equiv 0 \pmod{n} \\ k \equiv i \pmod{n} \end{cases}$$

From (I), we get that $k = 0$. From (II), we see that $i = k = \frac{n}{2}$. This mean that when $i \neq \frac{n}{2}$ the stabilizer is $\{cX | c^{q^i+1} = 1, c \in \mathbb{F}_{q^n}^*\}$. On the other hand, when $i = \frac{n}{2}$, the stabilizer is $\{cX^{q^t} | c^{q^{\frac{n}{2}}+1} = 1, c \in \mathbb{F}_{q^n}^*$ and $t = 0$ or $\frac{n}{2}\}$. □

By noticing that the order of the stabilizer of aX^{q^i+1} is $|\ker(X^{q^i+1})|$ for $i \neq \frac{n}{2}$ and $2|\ker(X^{q^i+1})|$ when $i = \frac{n}{2}$, we get:

Corollary 4. *Let $1 \leq i \leq n-1$ and $a \in \mathbb{F}_{q^n}^*$. The length of the orbit containing the monomial point aX^{q^i+1} is $\frac{|GL_n(\mathbb{F}_q)|}{|\ker(X^{q^i+1})|}$ when $i \neq \frac{n}{2}$ and $\frac{|GL_n(\mathbb{F}_q)|}{2|\ker(X^{q^i+1})|}$ when $i = \frac{n}{2}$.*

In the special case of $F(X) = aX^{2q^i}$, we have:

Theorem 9. *Let $0 \leq i \leq n-1$ and $a \in \mathbb{F}_{q^n}^*$. The stabilizer of aX^{2q^i} is reduced to X when $\mathrm{char}(\mathbb{F}_q) = 2$ and $\pm X$ when $\mathrm{char}(\mathbb{F}_q) \neq 2$.*

PROOF. As in the proof of Theorem 8, we can suppose that $L(X) = cX^{q^k}$. This leads to $aX^{2q^i} = aX^{2q^i} \circ cX^{q^k} = ac^{2q^i} X^{2q^{i+k}}$. Then, we have $c^{2q^i} = 1$ and $i + k \equiv i \pmod{n}$. It follows that $k = 0$, $c = 1$ when $\mathrm{char}(\mathbb{F}_q) = 2$ and $c = \pm 1$ when $\mathrm{char}(\mathbb{F}_q) \neq 2$. □

Corollary 5. *Let $0 \leq i \leq n-1$ and $a \in \mathbb{F}_{q^n}^*$. The length of the orbit containing the monomial point aX^{2q^i} is $|GL_n(\mathbb{F}_q)|$ for $\mathrm{char}(\mathbb{F}_q) = 2$ and $\frac{|GL_n(\mathbb{F}_q)|}{2}$ for $\mathrm{char}(\mathbb{F}_q) \neq 2$.*

According to Corollary 4 and Corollary 5, the number of equivalent keys of a scheme derived from a monomial $aX^{q^u+q^v}$ is related to the kernel of $X^{q^u+q^v}$. If the monomial induces a permutation, then there is no equivalent keys at all. This means that for a fixed central function, different keys will lead to different encryption maps.

4.3. Implication of the Results of this Section

Comparing with MI scheme whose central function has only one term in its univariate representation, HFE schemes have several terms in order to avoid the linearized attacks that MI schemes suffer from. Surprisingly enough, the results of this section show that although the central function is restricted to a monomial in MI-type scheme, its equivalent schemes can be in HFE category, i.e. with more than one monomial occuring in the central function. In other words, we show that HFE is not always more secure than MI schemes which is supposed to be.

In fact, by Lemma 14 and Corollary 4, the linear equivalence class of $aX^{q^u+q^v}$ contains $n|\mathcal{R}(X^{q^{u-v}+1})|$ different monomials if $u - v \neq \frac{n}{2}$ and $\frac{n}{2}|\mathcal{R}(X^{q^{\frac{n}{2}}+1})|$ different monomials if $u - v = \frac{n}{2}$. Therefore, there are $\frac{|GL_n(\mathbb{F}_q)|}{|ker(X^{q^{u-v}+1})|} - n|\mathcal{R}(X^{q^{u-v}+1})|$ if $u - v \neq \frac{n}{2}$, and $\frac{|GL_n(\mathbb{F}_q)|}{2|ker(X^{q^{u-v}+1})|} - \frac{n}{2}|\mathcal{R}(X^{q^{u-v}+1})|$ if $u - v = \frac{n}{2}$, polynomials containing more than one term and so belonging to the HFE category.

The above arguments show that, in each class containing monomial, quite portion of the polynomials contain more than one term. This implies that, in each class, there are several HFE instances – seemingly complex and hard to solve – which are actually as easy as MI-type instances.

Precisely, there are $\frac{n+1}{2}|GL_n(\mathbb{F}_q)|$ different polynomials in $\mathcal{F}$ which are linearly equivalent to some monomials. Note that $\mathcal{F}$ contains some linear polynomials of the form aX^{2q^k} when $q = 2$, the number of quadratic polynomials in $\mathcal{F}$ linearly equivalent to some monomial is exactly $\frac{n+1}{2}|GL_n(\mathbb{F}_q)|$ (resp. $\frac{n-1}{2}|GL_n(\mathbb{F}_q)|$) when $q > 2$ (resp. $q = 2$), among them there are $\frac{1}{2}n(n+1)(q^n-1)$ $\big($resp. $\frac{1}{2}n(n-1)(q^n-1)\big)$ monomials. Thus the number of all HFE instances, i.e. quadratic polynomials which has more than two terms, linearly equivalent to some monomial is

$$\begin{cases} \frac{n+1}{2}|GL_n(\mathbb{F}_q)| - \frac{1}{2}n(n+1)(q^n-1), & \text{for } q > 2, \\ \frac{n-1}{2}|GL_n(\mathbb{F}_q)| - \frac{1}{2}n(n-1)(q^n-1), & \text{for } q = 2. \end{cases}$$

In summary, the results of this section not only answer how many cryptographic schemes at most we can derive from monomials (Theorem 7) but also show that quite many HFE cryptosystems are equivalent to MI-type schemes. In such way, by identifying equivalent schemes, we can rule out several HFE schemes from possible use. However, it is not clear how to decide efficiently if a HFE scheme is equivalent to a MI-type scheme.

5. Conclusion and Future works

In this article, we brought a new question related to the IP problem, i.e. to determine the number of all the isomorphism equivalence classes of quadratic homogeneous polynomial systems. This question is equivalent to counting the equivalent keys and equivalent schemes of multivariate cryptography. In terms of cryptography, more equivalent keys exist means smaller key space and the number of equivalence classes means the number of different schemes we can have with same parameter, both of them are very important in practice as having a large number of private keys and more choices of instances of cryptographic schemes is always desirable properties for public key cryptography. By adopting a new tool of finite geometry, we have provided a framework for approaching to the question. Though determining all the equivalence classes is still an open problem, it seems that finite geometry is a good language to study it.

Acknowledgement

The authors would like to thank anonymous referees and Shuhong Gao for their valuable comments and discussions. This work was supported by the National 973 Program of China under Grant 2011CB302400, the National Natural Science Foundation of China under Grant 60970152, the Grand Project of Institute of Software under Grant YOCX285056.

References

[1] 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 *LNCS*, pages 419–453. Springer–Verlag, 1988.

[2] Jacques Patarin. The Oil and Vinegar signature scheme. presented at the Dagstuhl Workshop on Cryptography, 1997.

[3] Jacques Patarin, Louis Goubin, and Nicolas Courtois. $C^* - +$ and hm: Variations around two schemes of t.matsumoto and h.imai. In *Advances in Cryptology - Asiacrypt'98*, volume 1514, pages 35–49. Springer, 1998.

[4] Jacques Patarin, Nicolas Courtois, and Louis Goubin. Quartz, 128-bit long digital signatures. In *CT-RSA'01*, volume 2020, pages 282–297. Springer, 2001.

[5] Christopher Wolf and Bart Preneel. Taxonomy of Public Key Schemes based on the problem of Multivariate Quadratic equations. Cryptology ePrint Archive, Report 2005/077, 2005. http://eprint.iacr.org/.

[6] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[7] Christopher Wolf and Bart Preneel. Large superfluous keys in multivariate quadratic asymmetric systems. In *Public Key Cryptography*, pages 275–287, 2005.

[8] Jacques Patarin. Cryptoanalysis of the matsumoto and imai public key scheme of eurocrypt'88. In *CRYPTO*, pages 248–261, 1995.

[9] Jean-Charles Faugère and Antoine Joux. Algebraic cryptanalysis of Hidden Field Equation (HFE) cryptosystems using Gröbner bases. In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003*, volume 2729 of *LNCS*, pages 44–60. Springer, 2003.

[10] Vivien Dubois, Pierre-Alain Fouque, and Jacques Stern. Cryptanalysis of sflash with slightly modified parameters. In *EUROCRYPT*, pages 264–275, 2007.

[11] Vivien Dubois, Pierre-Alain Fouque, Adi Shamir, and Jacques Stern. Practical cryptanalysis of sflash. In Alfred Menezes, editor, *CRYPTO*, volume 4622 of *Lecture Notes in Computer Science*, pages 1–12. Springer, 2007.

[12] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes. In *EUROCRYPT*, pages 206–222, 1999.
[13] Jacques Patarin. Hidden fields equations (hfe) and isomorphisms of polynomials (ip): Two new families of asymmetric algorithms. In *EUROCRYPT*, pages 33–48, 1996.
[14] Jean-Charles Faugère and Ludovic Perret. Polynomial equivalence problems: Algorithmic and theoretical aspects. In *EUROCRYPT*, pages 30–47, 2006.
[15] Françoise Levy dit Vehel and Ludovic Perret. Polynomial equivalence problems and applications to multivariate cryptosystems. In Thomas Johansson and Subhamoy Maitra, editors, *INDOCRYPT*, volume 2904 of *Lecture Notes in Computer Science*, pages 235–251. Springer, 2003.
[16] Jean-Charles Faugère Pierre-Alain Fouque Charles Bouillaguet and Ludovic Perret. Practical cryptanalysis of the identification scheme based on the isomorphism of polynomial with one secret problem. In *Public Key Cryptography*, page to appear, 2011.
[17] Pierre-Alain Fouque, Gilles Macario-Rat, and Jacques Stern. Key recovery on hidden monomial multivariate schemes. In Nigel P. Smart, editor, *EUROCRYPT*, volume 4965 of *Lecture Notes in Computer Science*, pages 19–30. Springer, 2008.
[18] Zhexian Wan. On the symplectic invariants of a subspace of a vector space. *Acta Mathematica Scientia*, 11:251–253, 1991.
[19] Zhexian Wan. On the orthogonal invariants of a subspace of a vector space over a finite field of odd characteristic. *Linear Algebra and Its Applications*, 184:123–133, 1993.
[20] Zhexian Wan. Anzahl theorems in finite singular symplectic, unitary and orthogonal geometries. *Discrete Mathematics*, 123:131–150, 1993.
[21] Zhexian Wan. Further studies of singular symplectic, unitary and orthogonal geometries over finite fields. *Southeast Asian Bulletin of Mathematics*, 17:177–196, 1993.
[22] Zhexian Wan. *Geometry of classical groups over finite fields.* Science Press, 1993.
[23] Aviad Kipnis and Adi Shamir. Cryptanalysis of the hfe public key cryptosystem by relinearization. In *CRYPTO*, pages 19–30, 1999.
[24] Jintai Ding, Jason E. Gower, and Dieter Schmidt. *Multivariate Public Key Cryptosystems (Advances in Information Security).* Springer-Verlag New York, Inc. Secaucus, NJ, USA, 2006.
[25] Rudolf Lidl and Harald Niederreiter. *Finite fields.* Cambridge University Press, 1997.