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*
{ddlin,wangtz83}@is.iscas.ac.cn

[b] *LIP6, 104 avenue du Président Kennedy 75016 Paris, France*
jean-charles.faugere@inria.fr, ludovic.perret@lip6.fr

[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, 6, 7]. Schemes based on the hard problem of solving systems of multivariate equations over a finite field are not concerned with the quantum computer threat, whereas it is well known that number theoretic-based schemes like RSA, DH, and ECDH are [8].

The basic idea of a multivariate public-key scheme is to generate a highly structured set of polynomials which can be easily inverted. In order to hide the structure, the multivariate polynomials are composed with bijective affine transformations. The resulting set of multivariate polynomials is then the public-key. To encrypt (resp. verify a signature), one simply evaluates the message (resp. signature) on the polynomials of the public-key.

To decrypt (resp. sign), one only has to invert the bijective affine transformations and an easy algebraic system.

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 subject to doubt. This is due to the successful cryptanalysis of pioneering schemes, namely C* [9], HFE [10] and SFLASH [11, 12]. Although there are several proposals of MPKC which are assumed to be secure (QUARTZ [4] and UOV [13] 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. In this paper, we present a new framework for counting the number of different schemes and equivalent keys, a.k.a. superfluous keys[14, 6]. In other words, we want to know how many "different" MPKC schemes can be constructed.

This type of problem is tightly related to the Isomorphism of Polynomials (IP)[15]: a basic hard problem on which multivariate cryptography relies. Briefly speaking, this problem consists of recovering the affine transformations between two sets of multivariate polynomials (this problem is also know as IP with two secrets (IP2S)). It is equivalent to recovering the secret-key from the public-key.

From an algorithmic point of view, IP and its variants have been thoroughly investigated, e.g. [16, 17, 18, 19]. The authors of [16] 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 [18]. 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 [16] 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, we consider the counting problem associated to IP. Namely, we focus on the problem of counting the number of solutions of IP and the problem of counting the number of equivalence classes of polynomial systems. These problems are equivalent to counting the number of "equivalent" secret keys in a multivariate scheme and the total number of different multivariate cryptographic schemes respectively, which might impact the security and the potential capability of multivariate public key cryptography.

To this end, we will extensively use tools of finite geometry [20]. 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.

1.1. Overview of the Results.

We present a new framework to study the enumeration problem related to IP. In [16], it has been shown that IP can be interpreted in terms of group action and orbit. Thus, IP induces an equivalence relation on the polynomials systems [16]. The set of algebraic polynomials can be divided into different disjoint equivalence classes. Thus, the counting problem associated to IP consists of counting the cardinality of each equivalence class and counting the number of equivalence classes. The former problem corresponds to counting "equivalent" secret keys in a multivariate scheme. The latter one allows to enumerate the number of different multivariate schemes. More precisely, we focus on the enumeration problem associated to an important special case of IP, i.e. IP with one secret (IP1S). On the theoretical side, IP1S is known to be at least as difficult as Graph Isomorphsim (GI) [21]. On the practical side, identification scheme was proposed based on IP1S [15]. In what follows, the equivalence relation induced by IP1S is called "*linear equivalence*". Note that the equivalence classes induced by IP are obtained by merging some linear equivalence classes together using a linear combination. From a technical point of view, the study of the enumeration problem related to IP1S is easier than the one associated to IP.

We have connected IP1S with the matrix congruence problem using the so-called "*friendly mapping*" introduced in this paper. Once this bridge established, we can use basic results from finite geometry and give a lower bound on the total number of linear equivalence classes.

After that, we present some basic results for this enumeration problem and apply the results to MI-type schemes. We computed the cardinalities of linear equivalence classes containing a monomial and the number of such linear equivalence classes. Roughly speaking, we obtain that there are precisely $\sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \frac{|\mathbb{F}_{q^n}^*|}{|\mathcal{R}(X^{q^k+1})|}$ linear equivalence classes containing a monomial of the form $aX^{q^u+q^v} \in \mathbb{F}_{q^n}[X]$, with $0 \leq v < u \leq n-1$. In each class, there are $\frac{|GL_n(\mathbb{F}_q)|}{|\ker(X^{q^{u-v}+1})|}$ (resp. $\frac{|GL_n(\mathbb{F}_q)|}{2|\ker(X^{q^{u-v}+1})|}$) different polynomials when $u-v \neq \frac{n}{2}$ (resp. $u-v = \frac{n}{2}$), where $\mathcal{R}(X^{q^i+1})$ denote the range of X^{q^i+1} as a function from $\mathbb{F}_{q^n}^*$ to $\mathbb{F}_{q^n}^*$. We also prove that $\frac{n+1}{2}|GL_n(\mathbb{F}_q)|$ polynomials of the form $\sum a_{ij}X^{q^i+q^j} \in \mathbb{F}_{q^n}[X]$ are linearly equivalent to a monomial of the form $aX^{q^s+q^t}(0 \leq t \leq s \leq n-1)$.

From a cryptographic point of view, these results indicate that some HFE instances (whose central functions contain more than one term) can be equivalent to a cryptographic scheme whose central function is a monomial. Thus the security of these HFE instances is weak as Patarin's bi-linear attack [9] can be obviously applied.

In Table 1, we summarize the main results of this paper. "Nb. of classes" denotes the number of linear equivalence classes containing the monomial in the "Monomial" column; "Cardinality" is the total number of polynomials in the linear equivalence class containing that monomial; "Nb. of HFE instances" is the number of HFE instances, i.e. polynomials with more than one term, in the linear equivalence class containing that monomial.

Table 1: Summary of the results

Monomial	Condition	Nb. of classes	Cardinality	Nb. of HFE instances
$aX^{q^u+q^v}$ $(u \neq v)$	$u - v \neq \frac{n}{2}$	$\frac{\lvert\mathbb{F}_{q^n}^*\rvert}{\lvert\mathcal{R}(X^{q^{u-v}+1})\rvert}$	$\frac{\lvert GL_n(\mathbb{F}_q)\rvert}{\lvert\ker(X^{q^{u-v}+1})\rvert}$	$\frac{\lvert GL_n(\mathbb{F}_q)\rvert}{\lvert\ker(X^{q^{u-v}+1})\rvert} - n\lvert\mathcal{R}(X^{q^{u-v}+1})\rvert$
	$u - v = \frac{n}{2}$	$\frac{\lvert\mathbb{F}_{q^n}^*\rvert}{\lvert\mathcal{R}(X^{q^{\frac{n}{2}}+1})\rvert}$	$\frac{\lvert GL_n(\mathbb{F}_q)\rvert}{2\lvert\ker(X^{q^{\frac{n}{2}}+1})\rvert}$	$\frac{\lvert GL_n(\mathbb{F}_q)\rvert}{2\lvert\ker(X^{q^{u-v}+1})\rvert} - \frac{n\lvert\mathcal{R}(X^{q^{u-v}+1})\rvert}{2}$
aX^{2q^i} $(q > 2)$	$\mathrm{char}(\mathbb{F}_q) = 2$	1	$\lvert GL_n(\mathbb{F}_q)\rvert$	$\prod_{k=1}^{n}(q^k-1)q^{\frac{1}{2}n(n-1)} - (q^n-1)n$
	$\mathrm{char}(\mathbb{F}_q) \neq 2$	2	$\frac{1}{2}\lvert GL_n(\mathbb{F}_q)\rvert$	$\prod_{k=1}^{n}\frac{1}{2}(q^k-1)q^{\frac{1}{2}n(n-1)} - \frac{(q^n-1)n}{2}$

1.2. Organization of the Paper.

After this introduction this paper is organized as follows. 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. We also recall the connection between IP and equivalent keys in MPKC. In Section 3 we study the enumeration problems of polynomial isomorphism classes in two different cases: $\text{char}(\mathbb{F}_q) \neq 2$ and $\text{char}(\mathbb{F}_q) = 2$. In each case, we provide a lower bound on the total number of (linear) 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 the key space for a fixed scheme.

2. Preliminary

In this section, we recall the definition of the IP problem introduced in [15], the structure of MPKC schemes and a useful theorem given by Kipnis and Shamir in [22] (restated by Ding in his book [23]). This theorem is the key ingredient to connect our new tool to IP. Then, we recall some basic theorems in group theory about the orbit. We give those theorems without proof and refer the reader to the original papers.

2.1. Isomorphism of Polynomials

Let $\mathbb{F}_q$ be a finite field with q elements and $\mathbb{F}_q[\bar{x}] = \mathbb{F}_q[x_1, \ldots, x_n]$ be the ring of polynomials in $n \geq 1$ indeterminates over $\mathbb{F}_q$. Let $u > 1$ and $A = \{a_1(\bar{x}), \ldots, a_u(\bar{x})\}, B = \{b_1(\bar{x}), \ldots, b_u(\bar{x})\} \in \mathbb{F}_q[\bar{x}]^u$ be two systems of quadratic polynomials. We say that A and B are *isomorphic* if there exist two invertible affine transformations $L \in GL_n(\mathbb{F}_q) \times \mathbb{F}_q^n, S \in GL_u(\mathbb{F}_q) \times \mathbb{F}_q^u$ such that $B = S \circ A \circ L$.

The problem of recovering the transformations is known as IP with two secrets. A restricted problem called IP with one secret (IP1S)(see [15]) involves only one affine transformation on the variables, namely L.

In this paper, we consider for simplicity IP with two secrets with the restrictions that the number of polynomials in A (or B) equals the number of indeterminates, i.e. $u = n$. We also suppose that the polynomials in A and B are quadratic and homogeneous, and, S and T are invertible linear transformations. We can then restate the problem as follows.

Definition 1. We denote by $\mathcal{F}$ 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 $F_1 \in \mathcal{F}$ and $F_2 \in \mathcal{F}$ are equivalent if there exist two invertible linear transformations $(L, S) \in GL_n(\mathbb{F}_q) \times GL_n(\mathbb{F}_q)$ such that

$$F_2 = S \circ F_1 \circ L.$$

The above relation is an equivalence relation on the elements of $\mathcal{F}$. Thus, $\mathcal{F}$ can be written as a disjoint union of different equivalence classes.

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 1 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 $GL_n(\mathbb{F}_q)$, and η the map from $\mathcal{G} \times \mathcal{F}$ to $\mathcal{F}$ such that $\eta\big((S, L), F\big) = S \circ F \circ L$. Under the function η, we can say that G acts on the set $\mathcal{F}$. The equivalence classes are just the orbits of this group action [16].

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. Connection to MPKC

In this part, we explain the relation between IP and MPKC and introduce some notations. The general method of building multivariate public key schemes is to choose a special central function $F \in \mathcal{F}$, a system of quadratic polynomials, and then hide this central function by using two invertible affine transformation S and L. The public key of the system is $S \circ F \circ L$; S and L are considered to be the secret keys.

We shall say that $S \circ F \circ L$ is a scheme *derived* from the central function F. It is easy to see that the cryptographic scheme is uniquely determined by its central function and the two secret affine transformations. But the converse is not true, namely, for two different central functions F_1 and F_2, we may have secret keys (S_1, L_1) and (S_2, L_2) such that $S_1 \circ F_1 \circ L_1 = S_2 \circ F_2 \circ L_2$. In this case, (S_1, F_1, L_1) and (S_2, F_2, L_2) lead to the same encryption (resp. decryption) mapping. For this reason, we introduce the following definition.

Definition 2. Let F_1 and F_2 be two central functions. We shall say that the MPKC schemes derived from F_1 and F_2 are equivalent if there are two distinct pairs (S_1, L_1) and (S_2, L_2) of invertible affine transformations such that:

$$S_1 \circ F_1 \circ L_1 = S_2 \circ F_2 \circ L_2.$$

Obviously, equivalent polynomials define the same cryptosystem. Namely, equivalent polynomials can lead to the same encryption map by suitably choosing secret keys. Thus, schemes derived from equivalent polynomials will have the same key space and the same set of encryption/decryption maps. On the other hand, polynomials from different equivalence classes will define different cryptosystems. The number of equivalence classes will reflect how many different MPKC schems can be derived from polynomial systems.

Polynomial systems in the same equivalence class only differ on the pair of affine transformations, which corresponds to the secret key. In the same equivalence class, generally different pairs of affine transformations lead to different encryption/decryption maps. But this is not always the case. We mention that from a fixed central function ($F_1 = F_2$) and different pairs of secret keys, we can also derive the same encryption (resp. decryption) mapping. Such pairs will be called equivalent keys as formalized below.

Definition 3. Let F be a central function, (S_1, L_1) and (S_2, L_2) be two different pairs of secret keys. We shall say that (S_1, L_1) and (S_2, L_2) are equivalent keys of the scheme derived from F if:

$$S_1 \circ F \circ L_1 = S_2 \circ F \circ L_2.$$

It is worth to mention that only one equivalent key are useful and others are superfluous. A similar notation of superfluous keys has been introduced by Wolf and Preneel in [14]. More precisely, superfluous keys in the Wolf-Preneel terminology [14] are in fact the combination of equivalent schemes and equivalent keys in our framework. In [14], the authors restricted their equivalent keys to "sustain" the form of the central function. Our approach is finer and more general. In the last part of Section 4, we will see that there exist some pairs of secret keys which do not sustain the form of central functions whilst deriving the same encryption (resp. decryption) mapping.

The cardinality of an equivalence class corresponds to the number of encryption mapping that we can get by choosing different pairs of affine transformations. This reflects how many pairs of affine transformations can derive the same encryption map, i.e. how many equivalent keys we would have for a specific scheme. The number of different polynomial systems in an equivalence class represents the number of different secret keys which can be chosen. We emphasize that the existence of equivalent keys shrink the key space.

2.3. 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 [22] and [23] 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:*

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

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

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

The converse of the results is also true.

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

From the above lemma, we can see that there is a 1-1 correspondence between the polynomial mappings of $\mathcal{F}$ (resp. linear transformations) and the univariate representation (3) (resp. (2)). Thus, we will identify $\phi^{-1} \circ F \circ \phi$ (resp. $\phi^{-1} \circ L \circ \phi$) with F (resp. L) hereafter. We use again $\mathcal{F}$ to denote the set of mappings represented by (3) and use $\mathcal{L}$ to denote the set of invertible mappings represented by (2). Hence, Definition 1 of IP can be restated over the extension field as follows:

Definition 4. Let $F(X) = \sum\limits_{i=0}^{n-1} \sum\limits_{j=0}^{i} a_{ij} X^{q^i+q^j} \in \mathcal{F}$, and $G(X) = \sum\limits_{i=0}^{n-1} \sum\limits_{j=0}^{i} b_{ij} X^{q^i+q^j} \in \mathcal{F}$. We shall say that F and G are equivalent if and only if there exist $L(X) = \sum\limits_{i=0}^{n-1} a_i X^{q^i}$, and $S(X) = \sum\limits_{i=0}^{n-1} b_i X^{q^i} \in \mathcal{L}$ such that:

$$S \circ F \circ L(X) = S\big(F(L(X))\big) = G(X), \text{ for all } X \in \mathbb{F}_{q^n}.$$

From now on, we will ignore the mapping S and consider only the impact of invertible linear transformation L. Generally, this simplification will induce more equivalence classes. Indeed, linear transformation S mixes some classes together. In other words, we consider the IP1S problem.

Definition 5. Let $F(X) = \sum\limits_{i=0}^{n-1} \sum\limits_{j=0}^{i} a_{ij} X^{q^i+q^j} \in \mathcal{F}$, and $G(X) = \sum\limits_{i=0}^{n-1} \sum\limits_{j=0}^{i} b_{ij} X^{q^i+q^j} \in \mathcal{F}$. We say that F and G are *linearly equivalent* if and only if there exists $L(X) = \sum\limits_{i=0}^{n-1} a_i X^{q^i} \in \mathcal{L}$ such that $F\big(L(X)\big) = G(X)$, for all $X \in \mathbb{F}_{q^n}$.

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

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

It holds that:

Lemma 2. *Let $L(X) = \sum\limits_{i=0}^{n-1} a_i X^{q^i}$ 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 [24]. □

Definition 6. 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:

Definition 7. 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

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

Sometimes, we also call $\Psi_1(F)$ the matrix associated to F.

It is easy to see that Ψ_1 is a friendly mapping (Lemma 2.4.1 of [23]). 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 all diagonal elements are 0. This kind of matrices has a particular name:

Definition 8. 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 term of the form X^{2q^i}. It is somehow unreasonable to allow a friendly mapping to throw away the terms of the form X^{2q^i}. This in fact does not affect much on the analysis of corresponding scheme as already shown in the book [23]. 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 9. Let $\mathcal{A}_n$ be the set of all 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 3. *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* Rank(K) $= 2\nu$*, then K must be congruent 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 [20]. □

Using the congruent equivalence relation under general group $GL_n(\mathbb{F}_{q^n})$, 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. Next, we want to determine the length of each orbit. Namely, we try to count how many elements are in each congruent equivalence class. To do this, we introduce the concept of extended symplectic group.

Definition 10. 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 4. *Any matrix in $Sp_{n,\nu}(\mathbb{F}_q)$ is 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 10.

This will be used in Section 4. The following well known facts (for instance, you can see in [20]) will be also useful.

Lemma 5. *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 3, every matrix in $G_{2\nu}$ must be congruent to an alternative $n \times n$ matrix K_e as defined in Definition 10. 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), namely:

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

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.

In the terminology of group theory, the group $\mathcal{B}$ acts on the target set G_t. We aim at determining all the orbits under this group action (the total number and the length).

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 5. □

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 equal to $\frac{|G_{2\nu}|}{|GL_n(\mathbb{F}_q)|}$ 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

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

□

Finally:

Corollary 1. *The lower bound of 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 6. *The symmetric matrices over $\mathbb{F}_q$ is congruent to one and only 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 [20].

Let $\mathcal{S}$ be the set of all symmetric matrices of order n over $\mathbb{F}_{q^n}$. According to Lemma 6, 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 6 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 7. *Matrices in $O_{2\nu+\delta+\ell,\Delta}(\mathbb{F}_q)$ are such that*

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

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 8. *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 [20] 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 $M(n,2\nu+\delta,\nu,\Delta)$, it holds that:*

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

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:*

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

4. Applications to Multivariate Public-Key Crytptography

In this part, we count the number of different schemes and equivalent keys that can be derived from the classical Matsumoto–Imai scheme (a.k.a. C* schem). In [1], they described the famous multivariate public key scheme called C*.This cryptosystem uses a finite field $\mathbb{F}_q$ and an extension field $\mathbb{F}_{q^n}$. The choice of the central function is restricted to a monomial of the form X^{q^t+1}, with $\gcd(q^n - 1, q^t + 1) = 1$.

For our analysis, we generalize C* schemes to so-called *MI-type schemes.*

Definition 11. 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 $F \in \mathcal{F}$ 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. Surprisingly enough, we will see that although the central function is restricted to a monomial, its equivalent schemes can also be as in HFE, 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 C*.

We emphasize that the purpose of the generalization is not to increase the security of the scheme. The basic Patarin's bi-linear attack [9] against C* still works for MI-type schemes. On the other hand, by identifying equivalent schemes, we can rule out several HFE schemes from a possible use.

Let $\mathcal{F}$ be as defined in Section 2. Under the linear equivalence relation, $\mathcal{F}$ can be divided into disjoint equivalence classes. Our goal is to identify all classes containing a monomial and compute the cardinalities of these 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 $\mathbb{F}_{q^n}$. Here, we use f to denote both the polynomial and the associated mapping. Finally, we denote by $\mathcal{R}(f) = \{f(c)|c \in \mathbb{F}_{q^n}^*\}$ and $\ker(f) = \{c \in \mathbb{F}_{q^n}^*|f(c) = 1\}$. We have the following simple result.

Theorem 5. *For any $t, 0 \le t \le n-1$, $\mathcal{R}(X^{q^{i+t}+q^t}) = \mathcal{R}(X^{q^i+1})$. Thus:*

$$|\mathcal{R}(X^{q^{i+t}+q^t})| = |\mathcal{R}(X^{q^i+1})| = \frac{q^n-1}{\gcd(q^i+1, q^n-1)}.$$

Proof. It holds that:

$$\mathcal{R}(X^{q^{i+t}+q^t}) = \left\{c^{q^{i+t}+q^t}|c \in \mathbb{F}_{q^n}^*\right\} = \left\{(c^{q^t})^{q^i+1}|c \in \mathbb{F}_{q^n}^*\right\} = \left\{a^{q^i+1}|a \in \mathcal{R}(X^{q^t})\right\}.$$

Remark that $\gcd(q^t, q^n-1) = 1$. Thus, X^{q^t} is a permutation polynomial of $\mathbb{F}_{q^n}$, and $\mathcal{R}(X^{q^t}) = \mathbb{F}_{q^n}^*$. Therefore, it holds that:

$$\mathcal{R}(X^{q^{i+t}+q^t}) = \left\{a^{q^i+1}|a \in \mathbb{F}_{q^n}^*\right\} = \mathcal{R}(X^{q^i+1}).$$

Note that X^{q^i+1} is a homomorphism from $\mathbb{F}_{q^n}^*$ into $\mathbb{F}_{q^n}^*$, we have $\mathbb{F}_{q^n}^*/\ker(X^{q^i+1}) \simeq \mathcal{R}(X^{q^i+1})$ and then:

$$|\mathcal{R}(X^{q^{i+t}+q^t})| = |\mathcal{R}(X^{q^i+1})| = \frac{|\mathbb{F}_{q^n}^*|}{|\ker(X^{q^i+1})|} = \frac{q^n-1}{\gcd(q^i+1, q^n-1)}.$$

□

4.1. Number of Orbits Containing Monomials

As already explained, different equivalence classes correspond to different cryptographic schemes. The number of equivalence classes is in fact the number of different cryptographic schemes which can be derived from different central functions or different central polynomials. 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 9. *Let $a, b \in \mathbb{F}_{q^n}^*$ and $0 \le i \le n-1$. 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 that aX^{2q^i} and $bX^{q^u+q^v}(u \neq v)$ are linearly equivalent, i.e. there exists an invertible linear transformation $L(X)$ such that $aX^{2q^i} \circ L(X) = bX^{q^u+q^v}$. By the very definition of friendly mapping Ψ_1, this leads to:

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

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:

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

leading to a contradiction. Thus, aX^{2q^i} and $bX^{q^u+q^v}(u \neq v)$ can not be linearly equivalent. □

Lemma 10. *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. *(i)* We denote $X^{q^i} \circ L(X) \circ X^{q^j}$ by $L'(X)$ and suppose that $L(X) = \sum_{k=0}^{n-1} c_k X^{q^k}$. It follows that

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

Thus, $L'(X)$ is a monomial if and only if there is one and only one nonzero coefficient c_k, for $k, 0 \leq k \leq n-1$, i.e. $L(X)$ is a monomial.

(ii) As $\gcd(q^k, q^n - 1) = 1$ for $0 \leq k \leq n-1$, X^{q^i} and X^{q^j} are both permutation polynomials of $\mathbb{F}_{q^n}$. Now, we set $L' = X^{q^i} \circ L \circ X^{q^j}$. if L is a permutation polynomial, then it immediately follows that L' is a permutation polynomial. The converse is obvious if we notice that $L = X^{q^{n-i}} \circ L' \circ X^{q^{n-j}}$. □

By Lemma 9, the monomials can be roughly classified into two types: aX^{2q^i} and $bX^{q^u+q^v}$ with $u \neq v$. For the type of monomials aX^{2q^i}, we have

Lemma 11. *Let $0 \leq i, j \leq (n-1)$ and $a, b \in \mathbb{F}_{q^n}^*$. If there exists an invertible linear transformation $L(X) = \sum_{k=0}^{n-1} c_k X^{q^k}$ such that $aX^{2q^i} \circ L(X) = bX^{2q^j}$, then $L(X)$ must be a monomial.*

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

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

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.

Assume now $\mathrm{char}(\mathbb{F}_q) \neq 2$:

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

By Lemma 10, 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 friendly mapping Ψ_1:

$$\hat{L}\Psi_1(X^2)\hat{L}^{\mathrm{T}} = \Psi_1(cX^2),$$

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

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

Therefore

$$\hat{L} \in E_1(\alpha)O_n\big(\mathbb{F}_{q^n}, \Psi_1(X^2)\big).$$

By Lemma 7, a matrix in $O_n\big(\mathbb{F}_{q^n}, \Psi_1(X^2)\big)$ is of the form

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

with $a_{11}^2 = 1$ and T_{22} invertible. Hence $\hat{L} \in E_1\big(\alpha)O_n(\mathbb{F}_{q^n}, \Psi_1(X^2)\big)$ must be in the following form:

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

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. □

From above lemma, we deduce:

Corollary 4. *For any $a, b \in \mathbb{F}_{q^n}^*$ and $0 \leq i, j \leq n-1$, aX^{2q^i} and bX^{2q^j} are linearly equivalent if and only if $a^{-1}b$ is a square element.*

Proof. If aX^{2q^i} and bX^{2q^j} are linearly equivalent, then there exists a $L(X)$ such that $aX^{2q^i} \circ L(X) = bX^{2q^j}$. By Lemma 11, $L(X) = cX^{q^k}$. Then we have that $aX^{2q^i} \circ \left(cX^{q^k}\right) = bX^{2q^j}$, i.e. $ac^{2q^i}X^{2q^{i+k}} = bX^{2q^j}$. Hence, $ac^{2q^i} = b$, i.e. $a^{-1}b = c^{2q^i}$ which is a square element.
Conversely, if $a^{-1}b = c^2$, then $aX^{2q^i} \circ \left(c^{q^{n-i}}X^{q^{j-i}}\right) = ac^2X^{2q^j} = bX^{2q^j}$, which implies that aX^{2q^i} and bX^{2q^j} are linearly equivalent. □

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

Lemma 12. *If there exists an invertible linear transformation $L(X) = \sum_{k=0}^{n-1} c_kX^{q^k}$ such that $aX^{q^s+q^t} \circ L(X) = bX^{q^u+q^v}$, with $s \neq t$ and $u \neq v$, then $L(X)$ must be a monomial.*

Proof. Without loss of generality we can suppose that $0 \leq t < s \leq n-1$ and $0 \leq v < u \leq n-1$. By assumption, we have

$$\begin{aligned} & aX^{q^s+q^t} \circ L(X) = bX^{q^u+q^v} \\ \Leftrightarrow\ & (aX \circ X^{q^{s-t}+1} \circ X^{q^t}) \circ L(X) = bX^{q^{u-v}+1} \circ X^{q^v} \\ \Leftrightarrow\ & X^{q^{s-t}+1} \circ X^{q^t} \circ L(X) \circ X^{q^{n-v}} = a^{-1}X \circ bX^{q^{u-v}+1} \\ \Leftrightarrow\ & X^{q^{s-t}+1} \circ (X^{q^t} \circ L(X) \circ X^{q^{n-v}}) = a^{-1}bX^{q^{u-v}+1}. \end{aligned}$$

By Lemma 10, 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 assume that $\mathrm{char}(\mathbb{F}_q) = 2$. By definition of Ψ_1,

$$\hat{L}\Psi_1(X^{q^i+1})\hat{L}^{\mathrm{T}} = \Psi_1(cX^{q^j+1}).$$

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

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

Now we determine the general form of matrix in $Sp_n(\mathbb{F}_{q^n}, \Psi_1(X^{q^i+1}))$. From

$$E_{2,i+1}\Psi_1(X^{q^i+1})E_{2,i+1}^{\mathrm{T}} = \Psi_1(X^{q+1}),$$

we have

$$\begin{aligned} Sp_n\big(\mathbb{F}_{q^n}, \Psi_1(X^{q^i+1})\big) &= E_{2,i+1}^{-1} Sp_n\big(\mathbb{F}_{q^n}, \Psi_1(X^{q+1})\big) E_{2,i+1} \\ &= E_{2,i+1} Sp_n\big(\mathbb{F}_{q^n}, \Psi_1(X^{q+1})\big) E_{2,i+1}. \end{aligned}$$

According to Lemma 4, a matrix in $Sp_n\big(\mathbb{F}_{q^n}, \Psi_1(X^{q+1})\big)$ is of the form

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ 0 & 0 & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & a_{n3} & \cdots & a_{nn} \end{pmatrix} = \begin{pmatrix} T_{11} & T_{12} \\ 0_{(n-2)\times 2} & T_{22} \end{pmatrix}$$

with

$$T_{11} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} T_{11}^{\mathrm{T}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

and T_{22} invertible. Thus, a matrix in $Sp_n\big(\mathbb{F}_{q^n}, \Psi_1(X^{q^i+1})\big)$ must be as:

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

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 $j \not\in \{i, n-i\}$, then $\hat{L}$ is a zero matrix since there is a zero on each circulant diagonal.
- If $j = i$, then the only nonzero circulant diagonal of $\hat{L}$ is the main diagonal. Thus $L(X) = a_{11}X$.
- If $j = n-i$, then the only nonzero circulant 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 circulant diagonal.
- If $j = \frac{n}{2}$, then there are two nonzero circulant 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

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

  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 combining Lemma 11 and Lemma 12, we get the following important result.

Theorem 6. *Let $L(X) = \sum_{i=0}^{n-1} c_iX^{q^i}$ be an invertible linear transformation such that $aX^{q^i+q^j} \circ L(X) = bX^{q^u+q^v}$ for $a, b \in \mathbb{F}_{q^n}^*$, and $0 \leq i, j \leq n-1$, $0 \leq u, v \leq n-1$, then $L(X)$ must be a monomial.*

By Lemma 9, 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 13. *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 Theorem 6, 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 $k_1 \equiv \frac{n}{2} + k_2 (\text{mod} n)$. 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 7. *The number of monomials in the orbit containing a fixed monomial* $aX^{q^u+q^v}$ $(0 \leq v < u \leq n-1)$ *is* $n|\mathcal{R}(X^{q^{u-v}+1})|$ *when* $u - v \neq \frac{n}{2}$ *or* $\frac{n}{2}|\mathcal{R}(X^{q^{u-v}+1})|$ *otherwise.*

Proof. Since $aX^{q^u+q^v} = aX^{q^{u-v}+1} \circ X^{q^v}$, $aX^{q^u+q^v}$ is linearly equivalent to $aX^{q^{u-v}+1}$, i.e. $aX^{q^u+q^v}$ and $aX^{q^{u-v}+1}$ are in the same orbit. Then the result follows immediately from Lemma 13. □

Lemma 14. *For a fixed integer* $1 \leq i \leq n-1$, *all monomials of the form* aX^{q^i+1} *are distributed in* $|\mathbb{F}^*_{q^n}/\mathcal{R}(X^{q^i+1})|$ *different orbits.*

Proof. If αX^{q^i+1} is linearly equivalent to βX^{q^i+1}, then there exists a $L(X)$ such that $\alpha X^{q^i+1} = \beta X^{q^i+1} \circ L(X)$. From Theorem 6 it follows that $L(X) = cX^{q^k}$. Thus we have that $\alpha = \beta c^{q^i+1}$, i.e. α and β are in the same coset of $\mathcal{R}(X^{q^i+1})$ in the group $\mathbb{F}^*_{q^n}$.

On the other hand, if α and β are in the same coset of $\mathcal{R}(X^{q^i+1})$, i.e. these exists $c \in \mathbb{F}^*_{q^n}$ such that $\alpha = \beta c^{q^i+1}$, then αX^{q^i+1} is linearly equivalent to βX^{q^i+1} as $\alpha X^{q^i+1} = \beta X^{q^i+1} \circ cX$.

Therefore α and β are in the same coset of $\mathcal{R}(X^{q^i+1})$ in the group $\mathbb{F}^*_{q^n}$ if and only if αX^{q^i+1} and βX^{q^i+1} are linearly equivalent i.e. they are in the same orbit. Thus the total $q^n - 1$ monomials of the form aX^{q^i+1} are distributed in $|\mathbb{F}^*_{q^n}/\mathcal{R}(X^{q^i+1})|$ different orbits. □

Theorem 8. *The number of orbits containing some monomial of the form* $aX^{q^u+q^v}$ $(0 \leq v < u \leq n-1)$ *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* $\sum_{k=1}^{\frac{n}{2}} \frac{|\mathbb{F}_{q^n}^*|}{|\mathcal{R}(X^{q^k+1})|}$ *otherwise.*

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

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

Then $\mathcal{M} = \bigcup_{k=1}^{n-1} \mathcal{M}_k$. By Lemma 14, $\mathcal{M}_k$ 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 9. *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 Corollary 4 it follows 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 10. *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 8 and Theorem 9. □

In the formulae of Theorem 10, $\sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \frac{|\mathbb{F}_{q^n}^*|}{|\mathcal{R}(X^{q^k+1})|}$ 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 12. 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 11. *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 $\frac{n}{2}\}$ otherwise, i.e. $i = \frac{n}{2}$.*

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 Theorem 6 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 5. *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 12. *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 11, we can suppose 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 $\mathrm{char}(\mathbb{F}_q) \neq 2$. □

Hence:

Corollary 6. *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 5 and Corollary 6, 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. Understanding the Results of this Section

In this section we will show that a portion of HFE schemes are equivalent to MI-type schemes, so are as weak as MI-type schemes. Precisely, by combining Lemma 13 and Corollary 5, we get:

Theorem 13. *Let $0 \leq v < u \leq n-1$ and $a \in \mathbb{F}^*_{q^n}$. The linear equivalence class of $aX^{q^u+q^v}$ contains $n|\mathcal{R}(X^{q^{u-v}+1})|$ different monomials for $u-v \neq \frac{n}{2}$ and $\frac{n}{2}|\mathcal{R}(X^{q^{u-v}+1})| = \frac{n}{2}|\mathcal{R}(X^{q^{\frac{n}{2}}+1})|$ different monomials if $u-v = \frac{n}{2}$. Therefore, there are $\frac{|GL_n(\mathbb{F}_q)|}{|\ker(X^{q^{u-v}+1})|} - n|\mathcal{R}(X^{q^{u-v}+1})|$ for $u-v \neq \frac{n}{2}$, 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.*

As we know, HFE has been introduced as an improvement of C* scheme by making the central function more complex. According to Theorem 13, we can see 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 than MI-type instances. Now we count how many HFE instances in total are linearly equivalent to MI-type instances.

Theorem 14. *There are $\frac{n+1}{2}|GL_n(\mathbb{F}_q)|$ different polynomials in $\mathcal{F}$ which are linearly equivalent to some monomial.*

Proof. From Theorem 9 we know that there is only 1 (resp. 2 when char$(\mathbb{F}_q) \neq 2$) orbit containing monomials of the form aX^{2q^i}. From Corollary 6, we have that each such orbit contains $|GL_n(\mathbb{F}_q)|$ (resp. $\frac{|GL_n(\mathbb{F}_q)|}{2}$) polynomials when char$(\mathbb{F}_q) = 2$ (resp. char$(\mathbb{F}_q) \neq 2$). Thus the number of polynomials linearly equivalent to some monomial of the form aX^{2q^i} is $|GL_n(\mathbb{F}_q)|$.

Now we compute the number of polynomials linear equivalent to a monomial of the form $aX^{q^u+q^v}$ $(u \neq v)$. We spit the discussion in two cases:

Case 1. We suppose that n is odd. From Theorem 8 it follows that $\sum_{k=1}^{\frac{1}{2}(n-1)} \frac{|\mathbb{F}_{q^n}^*|}{|\mathcal{R}(X^{q^k+1})|}$ orbits contain monomials of the form $aX^{q^u+q^v}$. Thanks to Corollary 5 each such orbit contains $\frac{|GL_n(\mathbb{F}_q)|}{|\ker(X^{q^k+1})|}$ polynomials. Thus the number of polynomials linearly equivalent to some monomial of the form $aX^{q^u+q^v}$ is

$$\sum_{k=1}^{\frac{1}{2}(n-1)} \frac{|\mathbb{F}_{q^n}^*|}{|\mathcal{R}(X^{q^k+1})|} \cdot \frac{|GL_n(\mathbb{F}_q)|}{|\ker(X^{q^k+1})|} = \sum_{k=1}^{\frac{1}{2}(n-1)} |GL_n(\mathbb{F}_q)| = \frac{1}{2}(n-1)|GL_n(\mathbb{F}_q)|.$$

Case 2. Now, we consider n even. Theorem 8 states that there are in total $\sum_{k=1}^{\frac{n}{2}} \frac{|\mathbb{F}_{q^n}^*|}{|\mathcal{R}(X^{q^k+1})|}$ orbits containing monomials of the form $aX^{q^u+q^v}$. Due to Corollary 5 we have that each corresponding orbit contains $\frac{|GL_n(\mathbb{F}_q)|}{|\ker(X^{q^k+1})|}$ (resp. $\frac{|GL_n(\mathbb{F}_q)|}{2|\ker(X^{q^k+1})|}$) polynomials when $k \neq \frac{n}{2}$ (resp. $k = \frac{n}{2}$). Thus the number of polynomials linearly equivalent to some $aX^{q^u+q^v}$ is

$$\begin{aligned}
&\sum_{k=1}^{\frac{1}{2}(n-2)} \frac{|\mathbb{F}_{q^n}^*|}{|\mathcal{R}(X^{q^k+1})|} \cdot \frac{|GL_n(\mathbb{F}_q)|}{|\ker(X^{q^k+1})|} + \frac{|\mathbb{F}_{q^n}^*|}{|\mathcal{R}(X^{q^{\frac{n}{2}}+1})|} \cdot \frac{|GL_n(\mathbb{F}_q)|}{2|\ker(X^{q^{\frac{n}{2}}+1})|} \\
&= \frac{1}{2}(n-2)|GL_n(\mathbb{F}_q)| + \frac{1}{2}|GL_n(\mathbb{F}_q)| \\
&= \frac{1}{2}(n-1)|GL_n(\mathbb{F}_q)|.
\end{aligned}$$

To sum up, there are $\frac{1}{2}(n+1)|GL_n(\mathbb{F}_q)|$ different polynomials in $\mathcal{F}$ which are linearly equivalent to some monomial, either of the form aX^{2q^i} or of the form $aX^{q^u+q^v}$ with $u \neq v$. □

Remark 2. When $q > 2$, polynomials in $\mathcal{F}$ are all quadratic. However when $q = 2$, monomials of the form aX^{2q^k} are linear as $aX^{2q^k} = aX^{q^{k+1}}$. Hence, the polynomials in $\mathcal{F}$ which are linearly equivalent to some monomial of the form aX^{2q^k} are all linear.

By Theorem 14, we know that the number of quadratic polynomials in $\mathcal{F}$ linearly equivalent to some monomial is $\frac{n+1}{2}|GL_n(\mathbb{F}_q)|$ (resp. $\frac{n-1}{2}|GL_n(\mathbb{F}_q)|$) when $q > 2$ (resp. $q = 2$), among which 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

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

Table 2 shows the numerical value of the above formula for some specific parameters. We can see that there are huge number of HFE instances linearly equivalent to some monomial.

Table 2: Numerical values

q	n	Nb. of HFE instances ($\log_2$)
2	80	> 6325
2	100	> 9905
2	128	> 16261
2^8	80	> 51204
2^8	100	> 80005
2^8	128	> 131077

In summary, the results of this section not only answer how many cryptographic schemes at most we can derive from monomials (Theorem 10) but also show that quite many HFE cryptosystems are equivalent to MI-type schemes (Theorem 14). 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 related to equivalent keys and equivalent schemes of multivariate 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.

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] Neal Koblitz. *Algebraic Aspects of Cryptography.*, volume 3 of *Algorithms and Computation in Mathematics*. Springer-Verlag, 1998.

[6] 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/.

[7] Zhiping Wu, Jintai Ding, Jason E. Gower, and Dingfeng Ye. Perturbed hidden matrix cryptosystems. In *ICCSA (2)*, pages 595–602, 2005.

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

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

[10] 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.

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

[12] 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.

[13] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes. In *EUROCRYPT*, pages 206–222, 1999.

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

[15] Jacques Patarin. Hidden fields equations (hfe) and isomorphisms of polynomials (ip): Two new families of asymmetric algorithms. In *EUROCRYPT*, pages 33–48, 1996.

[16] Jean-Charles Faugère and Ludovic Perret. Polynomial equivalence problems: Algorithmic and theoretical aspects. In *EUROCRYPT*, pages 30–47, 2006.

[17] 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.

[18] 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.

[19] 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.

[20] Zhexian Wan. Geometry of classical groups over finite fields. *Student litterature, Lund*, 1993.

[21] Jacques Patarin, Louis Goubin, and Nicolas Courtois. Improved algorithms for isomorphisms of polynomials. In *EUROCRYPT*, pages 184–200, 1998.

[22] Aviad Kipnis and Adi Shamir. Cryptanalysis of the hfe public key cryptosystem by relinearization. In *CRYPTO*, pages 19–30, 1999.

[23] 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.

[24] Rudolf Lidl and Harald Niederreiter. *Finite fields.* Cambridge University Press, 1997.