PERMUTATION POLYNOMIALS AND THEIR APPLICATIONS IN CRYPTOGRAPHY

by

Rajesh Pratap Singh

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY
GUWAHATI
GUWAHATI-781039, INDIA

January, 2010

PERMUTATION POLYNOMIALS AND THEIR APPLICATIONS IN CRYPTOGRAPHY

A Thesis Submitted

in Partial Fulfillment of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

by

Rajesh Pratap Singh

(Roll Number: 04612304)

to the

DEPARTMENT OF MATHEMATICS

INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI

January 2010

DECLARATION

It is certified that the work contained in the thesis titled **"Permutation Polynomials and Their Applications in Cryptography"** has done by me under the Supervision of Dr. Anupam Saikia and Prof. B. K. Sarma, Department of Mathematics, Indian Institute of Technology Guwahati, for the award of the degree of Doctor of Philosophy and this work has not been submitted elsewhere for a degree.

Rajesh Pratap Singh
(Roll no. 04612304)
Department of Mathematics
Indian Institute of Technology Guwahati

January, 2010

CERTIFICATE

It is certified that the work contained in the thesis titled **"Permutation Polynomials and their Applications in Cryptography"** by **Rajesh Pratap Singh**, a student in the Department of Mathematics, Indian Institute of Technology Guwahati for the award of the degree of Doctor of Philosophy has been carried out under our supervision and this work has not been submitted elsewhere for a degree.

(Prof. B. K. Sarma) **(Dr. Anupam Saikia)**

Department of Mathematics
Indian Institute of Technology Guwahati

Dedicated

to

My Mother

Acknowledgement

It is my pleasure to thank all who have helped me in realizing this thesis and for making my time at IIT Guwahati enjoyable. First, I would like to express my deep sense of gratitude to my thesis supervisors Dr. A. Saikia and Prof. B. K. Sarma for their support and meticulous supervision in guiding me throughout my research work. I am grateful to Dr. A. Saikia for agreeing to be my supervisor for this thesis. His continuous encouragement and intellectual discussions has been a driving force for me to excel in my work. I am very much thankful to Prof B. K. Sarma for his guidance and consistent support during my research period which has enabled me to reach this stage. His comments and great insight into my work have helped me immensely in improving my thesis. I am grateful to my doctoral committee members, Dr. S. Pati, Dr. K. V. Krishna and Dr. G. Sajith for reviewing my research work giving valuable suggestions for the improvements of my work. I would like to thank Dr. K. V. Krishna and Dr. Kalpesh Kapoor for valuable help in understanding complexity theory. I am thankful to Dr. K. V. Srikanth, Dr. Natesan Srinivasan, Dr. Vinay Wagh and Dr. Sriparna Bandopadhyay for their help and support. I am thankful to Prof. D. C. Dalal (former Head, Department of Mathematics, IIT Guwahati), Prof. R. Alam (former Head, Department of Mathematics, IIT Guwahati) and Prof. R. K. Sinha (Head, Department of Mathematics, IIT Guwahati) for providing me the necessary facilities in the Department for my research work.

I would like to thank Indian Institute of Technology Guwahati (IITG) for the facilities provided to me during my research work and to the Ministry of Human and Resource Development, Govt. of India, for offering me financial assistance for completion of my thesis work.

I would also like to express my gratitude to Dr. Soumen Maity, Indian Institute of Science Education and Research Pune, for introducing me into cryptography and motivating me to work in this area and guiding me in the initial phase of my PhD program. I am grateful to Prof. Rana Barua of Indian Statistical Institute Kolkata, for his help, encouragement and valuable suggestions. Discussions with Prof. Rana Barua have helped me a lot, when I was visiting ISI Kolkata.

I am grateful to Prof. Lei Hu of Chinese Academy of Science for his constructive suggestions on a part of thesis work which improved the chapter 5

of this thesis. I thank to Prof. Jintai Ding, University of Cincinnati USA and Prof. Rolf Oppliger, University of Zurich, Switzerland, for answering my queries related to cryptography.

I thank my seniors and friends Dr. Tara Kant Nayak, Dr. Safique Ahmad, Dr. Subhash Chandra Martha, Dr. Bhupen Deka Dr. Sasmita Barik, Dr. Madhsmita Tripati, Dr. Milan Nath, and Dr. Swapan Kumar Pandit for a lot of help and encouragement. I offer my thanks to Mr. Shantanu Majumdar, Jr. Technical Superintendent for technical support. Sridhar Samal, Manoj Boro of Department of Mathematics deserve special thanks for their assistance in all official matters.

I would also like to thank my friends I have at IIT Guwahati whose company provided academic help and a welcome distraction from academic works. Notably Raju, Rajendra, Manas, Bibhash, Atul, Prabhanjan, Kaushik, Gaurav, Narsingh, Sanjay, Sukhi, Sunil, Sandeep, Ravi, Shubham, Pushpendra, Murli, Jugal, Cosmika, Manideepa, Smruti, Suman Das, Namita, Late Achin, Akhilesh, Rupam, Debajit, Shuvam, Raj Bhawan, Biswajit, Dinesh, Pratibhamoy, Kalyan, as well as sundry others who have shared many lively moments with me. My friends at Haldwani, Rakesh, Narendra, K. B. Joshi, Veer Singh, Laxman, Navneet, Basant, Manju deserve a special thank for being with me all the time.

I thank to my parents and my younger brothers Kaptan and Rinku for their love and support.

Last but not the least, to my dear Deepika, who came along with me in every step of this journey and was always there for me whenever I needed her most.

January 2010 **(Rajesh Pratap Singh)**

Abstract

A polynomial over a finite ring R is called a *permutation polynomial* of R if it induces a bijection from R to R. Permutation polynomials over finite rings have several applications in combinatorics, coding theory and cryptography. For example, the RC6 block cipher uses the permutation polynomial $x + 2x^2$ over the finite ring $\mathbb{Z}_{2^n}$, where 2^n is the word size of machine. In 2001, Rivest found an exact characterization of permutation polynomials over finite rings $\mathbb{Z}_{2^n}$. However, using Rivest's technique it was difficult to characterize permutation polynomials over finite rings $\mathbb{Z}_m$, for $m = 3^n, 5^n$. In this thesis, we present some methods to characterize all permutation polynomials over finite rings $\mathbb{Z}_m$ for $m = 2^n, 3^n, 5^n$. In addition, we produce a new class of permutation binomials over the finite fields $\mathbb{Z}_p$. Moreover, we show that every polynomial over finite ring $\mathbb{Z}_{p^n}$ can be expressed as a triangular map over $\mathbb{Z}_p^n$. Using this representation, we obtain sufficient conditions for a polynomial over $\mathbb{Z}_{p^n}$ to be a permutation polynomial, for any prime p.

Next, we consider permutation polynomials over finite fields. Permutation polynomials over finite fields have been the subject of study for many years. There is a considerable interest in finding new classes of permutation polynomials over finite fields. However, only a handful of specific classes of permutation polynomials are known so far and very few of the known classes have permutation polynomials commuting with one another. We find certain new classes of permutation polynomials over finite fields. Some of these classes are commutative.

Multivariate public key cryptography is a branch of public key cryptography in which cryptosystems are based on the problem of solving nonlinear equations over finite fields. This problem is proven to be NP complete. MIC*, the first practical public key cryptosystem based on this problem, was proposed in 1988 by T. Matsumoto and H. Imai. This cryptosystem was more efficient than RSA and ECC (Elliptic curve cryptosystems). Unfortunately, this cryptosystem was broken by Patarin. In 1996 Patarin gave a generalization of MIC* cryptosystem called HFE. However, in HFE the secret key computation was not as efficient as in the original MIC* cryptosystem. The basic instance of HFE was broken in 1999. In recent years, designing a public key cryptosystem based on the problem of solving system of nonlinear equations has been a challenging area of research. In this thesis, we have designed two efficient multivariate public key cryptosystems using permutation polynomials over finite fields. We have shown that these cryptosystems are secure against all the known attacks.

Contents

Chapter 1

Introduction

1.1 Permutation Polynomials over Finite Rings

A polynomial $f(x) = \sum_{i=0}^{d} a_i x^i$ over a finite ring R is called a *permutation polynomial* of R if it induces a bijection from R to R. Permutation polynomials over finite rings have several applications in combinatorics, coding theory and cryptography, see ([60], [68]). The RC6 block cipher [68] uses the permutation polynomial $x+2x^2$ over the finite ring $\mathbb{Z}_{2^n}$, where 2^n is the word size of machine.

A ring R is said to be *polynomially complete* if any function from R into itself can be represented by a polynomial over R. Kempner [41] showed that the only residue class rings $\mathbb{Z}_m$ that are polynomially complete are the prime finite fields (see also Bernstein [6]). Heisler [39] proved more generally that finite fields are the only polynomially complete nonzero rings.

In 2001 [67] Rivest found an exact characterization of permutation polynomials over finite rings $\mathbb{Z}_{2^n}$ (Theorem 2.2.3). However, the technique used to prove this theorem was not helpful for characterizing permutation polynomials over finite rings $\mathbb{Z}_{p^n},\ p \geq 3$.

In the first part of Chapter 2, we provide a simple proof of Rivest's theorem using congruence. Our method enables us to obtain similar results for $Z_{p^n},\ p = 3, 5$. Further, we find a class of permutation binomials over the prime fields $\mathbb{Z}_p$.

Suppose $\mathbb{F}$ denotes a finite field and $\mathbb{F}^n$ denotes the set of all n-tuples in $\mathbb{F}$. A map $\phi : \mathbb{F}^n \mapsto \mathbb{F}^n$ defined by

$$\phi(x_1, x_2, \ldots, x_n) = \begin{pmatrix} f_1(x_1) \\ f_2(x_1, x_2) \\ f_3(x_1, x_2, x_3) \\ \vdots \\ f_n(x_1, x_2, \ldots, x_n) \end{pmatrix}^T$$

is called a *triangular mapping*. One well known family of invertible triangular maps is the set of de *Jonquières* maps. A map $G = \mathbb{F}^n \mapsto \mathbb{F}^n$ is a de *Jonquières* map if it is of the form:

$$\phi(x_1, x_2, \ldots, x_n) = \begin{pmatrix} x_1 \\ x_2 + g_1(x_1) \\ x_3 + g_2(x_1, x_2) \\ \vdots \\ x_n + g_{n-1}(x_1, x_2, \ldots, x_{n-1}) \end{pmatrix}^T$$

where $\mathbb{F}$ is any field, and $g_i \in \mathbb{F}[x_1, \ldots, x_n]$ are arbitrary polynomials.

Due to the very special structure of de *Jonquières* maps, the inverse can be easily computed. Moreover, because these maps are invertible, the closure of this set under composition forms a group. This group is called the group of *tame* transformations. Any invertible map which is not tame is called a *wild* transformation [26]. It is a highly nontrivial problem to find an example of a wild transformation, and the famous Nagata problem is such an example [62].

A triangular map of the form

$$F(x_1, x_2, \ldots, x_n) = \begin{pmatrix} x_1 \\ x_2.l_1(x_1) + g_1(x_1) \\ x_3.l_2(x_1, x_2) + g_2(x_1, x_2) \\ \vdots \\ x_n.l_{n-1}(x_1, x_2, \ldots, x_{n-1}) + g_{n-1}(x_n) \end{pmatrix}^T$$

where the functions $l_i \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ are linear (or affine) and the functions $g_i \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ are quadratic, was used in cryptography by Shamir [71]. Triangular mappings were also used by Moh [58] to construct a multivariate public key cryptosystem.

In the second part of Chapter 2, we show that every polynomial over a finite ring $\mathbb{Z}_{p^n}$ can be expressed as a triangular map over $\mathbb{Z}_p^n$. Using this representation of the polynomials, we give sufficient conditions for a polynomial over $\mathbb{Z}_{p^n}$ to be a permutation polynomial for any prime p.

1.2 Permutation Polynomials over Finite Fields

Throughout this section, $q = p^n$, where p is prime number and $\mathbb{F}_q$ is the finite field of order q. Almost all results in this section are cited from Lidl and Niederreiter's book [50].

Before we study permutation polynomials over $\mathbb{F}_q$, we observe that for every function $\varphi : \mathbb{F}_q \mapsto \mathbb{F}_q$, there is a unique polynomial function $f(x) \in \mathbb{F}_q[x]$ such that deg $f \leq q-1$ and $\varphi(a) = f(a)$ for all $a \in \mathbb{F}_q$. This polynomial $f(x)$ can be found by the Lagrange's Interpolation formula described in the next theorem.

Theorem 1.2.1. *(Lagrange's Interpolation Formula) Suppose $\mathbb{F}$ denotes an arbitrary field. For $n \geq 0$, let $a_0, a_1, \ldots, a_n$ be distinct elements of $\mathbb{F}$, and $b_0, b_1, \ldots, b_n$ arbitrary elements of $\mathbb{F}$. Then there exist exactly one polynomial $g \in \mathbb{F}[x]$ of degree less that or equal to n such that $f(a_i) = b_i$ for $i = 0, 1, \ldots, n$.*

This polynomial is given by

$$g(x) = \sum_{i=0}^{n} b_i \prod_{k=0,\ k\neq i}^{n} (a_i - a_k)^{-1}(x - a_k).$$

Thus, corresponding to a given function $\varphi : \mathbb{F}_q \mapsto \mathbb{F}_q$ one gets a polynomial

$$f(x) = \sum_{c\in\mathbb{F}_q} \varphi(c)\left(1 - (x-c)^{q-1}\right)$$

having the property that $\phi(a) = f(a)$ for all $a \in \mathbb{F}_q$.

We observe that a polynomial $f \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if one of the following conditions holds:

1. The function f is onto.
2. The function f is one-to-one.
3. The equation $f(x) = a$ has a solution in $\mathbb{F}_q$ for each $a \in \mathbb{F}_q$.
4. The equation $f(x) = a$ has a unique solution in $\mathbb{F}_q$ for each $a \in \mathbb{F}_q$.

In view of the above observation, we immediately have the following result.

Theorem 1.2.2. *(1) Every linear polynomial that is a polynomial of the form $ax + b$ with $a \neq 0$ over $\mathbb{F}_q$ is a permutation polynomial of $\mathbb{F}_q$.*
(2) The monomial x^k is a permutation polynomial of $\mathbb{F}_q$ if and only if $\gcd(k, q-1) = 1$.

For permutation polynomials of $\mathbb{F}_q$ we have three general characterizations which are mentioned below. The first one is almost obvious.

Theorem 1.2.3. *Let $f(x) \in \mathbb{F}_q[x]$. Write*

$$D(f) = \left\{ \frac{f(b) - f(a)}{a - b} \ : \ a \neq b \in \mathbb{F}_q \right\}$$

Then $f(x)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $0 \notin D(f)$.

The second characterization uses characters of the field $\mathbb{F}_q$. Let G be a finite abelian group. A *character* χ of G is a homomorphism from G into the

multiplicative group of complex numbers of absolute value 1. When we consider the finite field $\mathbb{F}_q$, we have two kinds of characters defined on $\mathbb{F}_q$: the *additive* characters defined on the additive group of $\mathbb{F}_q$ and the *multiplicative* characters defined on the multiplicative group $\mathbb{F}_q^*$. The additive character χ_0 of $\mathbb{F}_q$ satisfying $\chi_0(c) = 1$ for all $c \in \mathbb{F}_q$ is called the *trivial additive* character of $\mathbb{F}_q$.

Theorem 1.2.4. *The polynomial $f(x) \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $\sum_{c\in\mathbb{F}_q} \chi(f(c)) = 0$ for all nontrivial additive characters χ of $\mathbb{F}_q$.*

The third characterization of permutation polynomials over finite fields is the following.

Theorem 1.2.5. *(Hermite's criterion) A polynomial $f(x) \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if following two conditions hold:*
(1) $f(x)$ has only one root in $\mathbb{F}_q$; and
(2) for each integer t with $1 \le t \le q-2$ and $t \neq 0 \mod p$, the reduction of $f(x)^t \mod (x^q - x)$ has degree $\le q-2$.

The *reduction* of $f(x)^t \mod (x^q - x)$ is the polynomial $g(x) \in \mathbb{F}_q[x]$ such that $\deg g(x) \le q-1$ and $f(x)^t \equiv g(x) \mod (x^q - x)$. In fact, we have $f(c)^t = g(c)$ for all $c \in \mathbb{F}_q$, since $c^q = c$. As a consequence of Hermite's criterion, we get the following result.

Corollary 1.2.6. *If $d \ge 1$ is a divisor of $q-1$, then there is no permutation polynomials of $\mathbb{F}_q$ of degree d. In particular, for any odd prime p there is no permutation polynomial of over $\mathbb{Z}_p$ of degree $p-1$.*

Theoretically, the above three characterizations are interesting. However, it is not easy in practice to use them to check whether a given polynomial is a permutation polynomial or not. Permutation polynomials have been a subject of study for many years and determining new classes of permutation polynomials is still an open research problem, see [48] and [49]. Only a handful of classes of permutation polynomials are known so far. Some known results and known classes of permutation polynomials over finite fields are described below.

Theorem 1.2.7. *[50] Let $r \in \mathbb{N}$ with $\gcd(r, q-1) = 1$ and let s be a positive divisor of $q-1$. Let $g \in \mathbb{F}_q[x]$ be such that $g(x^s)$ has no nonzero root in $\mathbb{F}_q$. Then $f(x) = x^r \left(g((x^s))\right)^{(q-1)/s}$ is a permutation polynomial of $\mathbb{F}_q$.*

Theorem 1.2.8. *[50] For odd positive integer q, the polynomial $x^{(q+1)/2} + ax$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $\eta(a^2 - 1) = 1$, where η is the quadratic character of $\mathbb{F}_q$.*

A special class of polynomial was introduced by Dickson [21] (see also Dickson [22]). These polynomials, known as *Dickson polynomials of first kind*, have some interesting properties and they yield new examples of permutation polynomials. For $a \in \mathbb{F}_q$, the Dickson polynomial of first kind $g_k(x, a)$ is defined as

$$g_k(x, a) = \sum_{j=0}^{\lfloor k/2 \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-a)^j x^{k-j}.$$

These polynomials are important in connection with a celebrated conjecture of Schur which states that any $f \in \mathbb{Z}[x]$ which is a permutation polynomial of $\mathbb{F}_p$, when considered modulo p, for infinitely many primes p must be a composition of binomials $ax^n + b$ and Dickson polynomials. Schur proved the case when $\deg(f)$ is prime and Kurbatov [46] settled the case when $\deg(f)$ is a product of at most four distinct primes or a product of two odd prime powers. Finally, Schur's conjecture was proved completely by Fried [33]. Furthermore, it is shown that if $f \in \mathbb{Q}[x]$ is a composition of binomials $ax^n + b$ and Dickson polynomials and if $\deg(f)$ is coprime to 6, then f is a permutation polynomial of $\mathbb{F}_p$ for infinitely many primes p. Some more work related to this can also be found in Fried [34, 35]. The next theorem characterizes the permutation Dickson polynomials.

Theorem 1.2.9. *[50] The Dickson polynomial $g_k(x, a), a \in \mathbb{F}_q^*$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $\gcd(k, q^2 - 1) = 1$.*

Corollary 1.2.10. *If $a \in \mathbb{F}_q^*$ and $\gcd(k, q^2 - 1) = 1$, then*

$$\sum_{c \in \mathbb{F}_q} \chi\left(g_k(c, a)\right) = \sum_{c \in \mathbb{F}_q} \chi\left(c\right),$$

for every nontrivial additive or multiplicative character χ of $\mathbb{F}_q$.

For each k, the *Dickson polynomial of the second kind* $f_k(x)$ is defined by

$$f_k(x) = \sum_{j=0}^{\lfloor k/2 \rfloor} \binom{k-j}{j} (-a)^j x^{k-j}.$$

A class of permutation polynomials amongst the Dickson polynomials of second kind was obtained in [56]. Cohen [10] showed that in prime fields of odd order and in their degree 2 extensions these are the only examples of such polynomials. Some classes of permutation polynomials among the Dickson polynomials of second kind over finite fields of characteristic ≤ 5 can be found in [40]. Coulter and Matthews [13] expanded and simplified the known permutation behaviour of the Dickson polynomials of the second kind in characteristic 3 case. Some more results related to Dickson polynomials can be found in [11, 51].

Carlitz [7] found some permutation polynomials of the form $x^{m+1} + ax$ over finite fields $\mathbb{F}_q$. Wan and Lidl [74] considered the polynomials of the form $x^r f(x^{(q-1)/d})$ and gave a criterion for this type of polynomials to be a permutation polynomials over finite fields. Akbary and Wang [3] gave a general criterion for permutation polynomials of the form $x^r f(x^{(q-1)/l})$, where $r \geq 1, l \geq 1$ and $l \mid (q-1)$ and employed this criterion to characterize several classes of permutation polynomials of this form. In 2005, Yann Laigle-Chapuy [47] gave some classes of permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their applications in coding theory. Suppose p_1 is a prime number such that $p_1 \mid (q-1)$ and $b(x) = x^u(x^v + 1) \in \mathbb{F}_q[x]$, where u and v are positive integers and the $\gcd(v, q-1) = \frac{q-1}{p_1}$. Wang [75] characterized $b(x)$ as a permutation polynomial for $p_1 = 3, 5$. Later this result was generalized by Akbary and Wang [2] and was related to Lucas sequences. In 2007, Yuan and Ding [78] investigated four classes of permutation polynomials of the form $(x^2 + x + \delta)^s + x$. In 2008, Yuan, Ding, Wang and Piepryzyk [79] obtained several classes of permutation polynomials of the form $(x^p - x + \delta)^s + L(x)$, over the finite fields $\mathbb{F}_{p^m}$, $p = 2, 3$, where δ is an element of finite field with nonzero *trace* and $L(x)$ is a linearized polynomial over finite field as defined in Chapter 3. In 2009, Ding, Xiang, Yuan and Yuan [24] obtained six classes of linearized permutation polynomials and six classes of nonlinearized permutation polynomials over finite fields $\mathbb{F}_{3^{3m}}$. Charpin and Kyureghyan [8, 9] studied the permutation polynomials of the form $G(x) + \gamma Tr(H(x))$, where γ is an element of finite field and $Tr(H(x))$ denotes the *trace* of the polynomial $H(x)$ and gave some classes of permutation polynomials of this form. Some more classes of permutation polynomials over finite fields can be found in [12, 54, 1, 4].

Ribić [61] considered the problem of finding inverse of a permutation poly-

nomial and characterized the coefficients of the inverse polynomials of a known class of permutation polynomials. In 2009, Wang [77] gave an explicit formula of the inverse polynomial of a permutation polynomial of the form $x^r f(x^s)$ over F_q where $s \mid q-1$ and generalized Ribić's result.

In 2002, Das [18] related the number of permutation polynomials in $F_q[x]$ of degree $d \leq q-2$ to the solutions $x_1, x_2, \ldots, x_q$ of a system of linear equations over F_q, with the added restriction that $x_i \neq 0$ and $x_i \neq x_j$ whenever $i \neq j$. Using this he found an expression for the number of permutation polynomials of degree $p-2$ in $F_p[x]$ in terms of the permanent of a Vandermonde matrix whose entries are the primitive pth roots of unity. This leads to nontrivial bounds for the number of such permutation polynomials. Some more results related to to number of permutation polynomials of $\mathbb{F}_q[x]$ of given degree can be found in [45, 52, 53].

In Chapter 3 of this thesis, we generate some new classes of linearized as well as non linearized permutation polynomials over the finite fields $\mathbb{F}_{p^n}$ for $p = 2, 3$.

1.3 Multivariate Public Key Cryptography

The revolutionary idea of public key cryptography, which has fundamentally changed our modern communication systems, was discovered by Diffie and Hellmann [23]. Before public key cryptography, the traditional symmetric key cryptography used the same key for decryption and encryption. As a result, any two users of the system who want to communicate using symmetric key cryptosystem must have exchanged keys in a safe way. In contrast, a public key cryptosystem uses different keys for encryption and decryption. The encryption key is to be made public so that anyone can use this public key for encryption, while the decryption key is kept secret so that only the intended recipient can decrypt the secret message. Similarly, signature schemes based on public key cryptosystems use two different keys, one is a public key for verifying signature and other is a secret key to generate signatures. The first practical realization of public key cryptography was the famous RSA cryptosystem by Rivest, Shamir and Adlemann [69]. Public key cryptography is used in e-commerce for authentication and secure communication. The most widely used cryptosystems RSA and ECC

(elliptic curve cryptosystems) are based on the problems of integer factorization and discrete logarithm respectively. Improvements in factorization algorithm and computation power demands larger bit size in RSA key. At present the recommended key size is of 1024 bits which may still have to be increased to 4096 bits by 2015 [70]. Larger key size makes RSA less efficient for practical applications. ECC are more efficient as compared to RSA, but its shortest signature is of 320 bits which is still long for many applications [5]. Although RSA and ECC have these drawbacks, they are still not broken. But in 1999 Peter Shor [72] discovered the polynomial time algorithm for integer factorization and computation of discrete logarithm on quantum computers. Thus, once we have quantum computers the cryptosystems based on these problems can no longer be considered secure. So, there is a strong motivation to develop public key cryptosystems based on problems which are secure on both conventional and quantum computers. Multivariate cryptography can be a possible option applicable to both conventional and quantum computers [26]. In multivariate cryptography the public key cryptosystems are based on the problem of solving system of nonlinear equations which is proven to be NP-complete. MIC*, the first practical public key cryptosystem based on this problem was proposed in 1988 by T. Matsumoto and H. Imai [55]. The MIC* cryptosystem was based on the idea of hiding a monomial $x^{2^l}+1$ by two invertible affine transformations. This cryptosystem was more efficient than RSA and ECC. Unfortunately, this cryptosystem was broken by Patarin in 1995 [63]. In 1996, Patarin [65] gave a generalization of MIC* cryptosystem called HFE. However, in HFE the secret key computation was not as efficient as in the original MIC* cryptosystem. The basic instance of HFE was broken in 1999 [42]. The attack uses the simple fact that every homogeneous quadratic multivariate polynomial has a matrix representation. Using this representation a highly overdefined system of equations can be obtained and can be solved by a new technique called relinearization [42]. Other possible attacks on the HFE scheme can be found in [15, 16, 31]. Patarin [64] investigated whether it is possible to repair MIC* with the same kind of easy secret key computations. He designed some cryptosystems known as Dragons with multivariate polynomials of total degree 3 or 4 in public key (instead of 2) with enhanced security and with efficiency comparable to MIC*. In Dragon cryptosystems the public key was of mixed type of total degree 3 which

is quadratic in plaintext variables and linear in ciphertext variables. However, Patarin found [64] that Dragon scheme with one hidden monomial is insecure.

A public key scheme based on the composition of tame transformation methods (TTM) was proposed in 1999 [58]. This scheme has been broken in 2000 [37], where the cryptanalysis is reduced to an instance of the Min-Rank problem that can be solved within a reasonable time. In 2004 Ding [25] proposed a perturbed variant of MIC* cryptosystem called PMI. PMI cryptosystem attempts to increase the complexity of the secret key computations in order to increase security, using a system of r arbitrary quadratic equations over $\mathbb{F}_q$ with the assumption that $r \ll n$, where n is the bit size. PMI cryptosystem was broken by Fouque, Granboulan and Stern [32]. The trick of the attack on PMI is to use differential cryptanalysis to reduce the PMI system to the MIC* system. A cryptosystem called Medium Field Equation (MFE) was proposed in 2006 [76] and was broken by Ding in 2007 [27] using high order linearization equation attack. A multivariate public key cryptosystem based on paraunitary matrices can be found in [20]. A detailed introduction of multivariate public key cryptography is available in the book by Ding *et. al.* [26]. An interesting introduction of hidden monomial cryptosystems can be found in reference [44]. Designing secure and efficient multivariate public key cryptosystem continues to be a challenging area of research in recent years. In Chapter 4 and Chapter 5 of this thesis, using permutation polynomials over finite fields, we present new methods for designing efficient multivariate public key cryptosystems by overcoming all the known attacks. We give a brief review of some multivariate public key cryptosystems. The following constructions are used by each of these crystosystems.

Suppose $\mathbb{F}_{q^n}$ is a finite field, where q is a power of 2. Suppose $\mathbb{B} = \{\vartheta_1, \vartheta_2, \ldots, \vartheta_n\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Using the basis $\mathbb{B}$, $\mathbb{F}_{q^n}$ can be identified with $\mathbb{F}_q^n$, the set of all n-tuples of $\mathbb{F}_q$, by the standard isomorphism $\phi : \mathbb{F}_{q^n} \mapsto \mathbb{F}_q^n$ defined by $\phi(a_1\vartheta_1 + a_2\vartheta_2 + \ldots, a_n\vartheta_n) = (a_1, a_2, \ldots, a_n)$.

Given a polynomial $f \in \mathbb{F}_{q^n}[x]$, let $\bar{f}$ be the map on $\mathbb{F}_q^n$ defined by

$$\bar{f}(x_1, x_2, \ldots, x_n) = \phi \circ f \circ \phi^{-1}(x_1, x_2, \ldots, x_n) = (\bar{f}_1, \bar{f}_2, \ldots, \bar{f}_1), \tag{1.1}$$

where $\bar{f}_1, \ldots, \bar{f}_n \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$. Suppose L_1 and L_2 are two invertible

affine transformation of $\mathbb{F}_q^n$. Define a map on $\mathbb{F}_q^n$ by

$$F(x_1, \ldots, x_n) = L_2 \circ \bar{f} \circ L_1(x_1, \ldots, x_n) = (f_1, \ldots, f_n) \tag{1.2}$$

where $f_1, \ldots, f_n \in \mathbb{F}_q[x_1, \ldots, x_n]$.

1.3.1 The Cryptosystem MIC*

Matsumoto-Imai public key cryptosystem MIC* chooses integer θ so that $0 < \theta < n$ and $\gcd(q^\theta + 1, q^n - 1) = 1$. It uses the polynomial map on $\mathbb{F}_{q^n}$ given by $f(x) = x^{q^\theta+1}$. From Theorem 1.2.2 it is clear that f is a bijection and its inverse map is given by x^t, where $t(q^\theta+1) \equiv 1 \mod (q^n-1)$. Moreover, we note that, because of the monomial $x^{q^\theta+1}$ used for obtaining them, the polynomials $f_1, \ldots, f_n$ are quadratic.

The Public Key

The public key of MIC* includes the following

1.) The field $\mathbb{F}_q$ including its additive and multiplicative structure

2.) The n quadratic polynomials $f_1, \ldots, f_n \in \mathbb{F}_q[x_1, \ldots, x_n]$.

The Private Key

The private key includes the two invertible affine transformation L_1 and L_2. There are only a few choices for the parameter θ and we can assume that θ is known.

Encryption

If somebody wants to send a plaintext message $x = (x_1, \ldots, x_n)$, he substitutes x_i in public equations and find the y_j. The $y = (y_1, \ldots, y_n)$ is the required ciphertext.

Decryption

One can decrypt the ciphertext by executing the following steps

1) First compute $(w_1, \ldots, w_2) = L_2^{-1}(y_1, \ldots, y_n)$;

2) Then compute $(z_1, \ldots, z_n) = \phi \circ f^{-1} \circ \phi^{-1}(w_1, \ldots, w_n)$;
3) Finally compute $(x_1, \ldots, x_n) = L_1^{-1}(z_1, \ldots, z_n)$.

Patarin's Attack on MIC* Patarin [63] showed how to break the MIC* cryptosystem. Suppose $u = \phi^{-1} \circ L_1(x_1, \ldots, x_n)$ and $v = \phi^{-1} \circ L_2^{-1}(y_1, \ldots, y_n)$. The relation between plaintext and ciphertext is $v = u^{q^\theta+1}$. Now raising power $(q^\theta - 1)$-st power, and multiplying both sides by uv, one can get the equation

$$u.v^{q^\theta} = u^{q^{2\theta}}. \tag{1.3}$$

Note that v^{q^θ} and $u^{q^{2\theta}}$ are linear maps of $\mathbb{F}_{q^n}$. Now substituting $u = \phi^{-1} \circ L_1(x_1, \ldots, x_n)$ and $v = \phi^{-1} \circ L_2^{-1}(y_1, \ldots, y_n)$, where L_1 and L_2 are unknown linear transformations of $\mathbb{F}_{q^n}$, and taking the n-tuple representation using the basis $\mathbb{B}$, one can get the n equations of the form

$$\left(\sum_{1 \le i,j \le n} a_{ijl} x_i y_j\right) + \left(\sum_{i \le i \le n} (b_{il} x_i + c_{il} y_i)\right) + d_l = 0, \tag{1.4}$$

$l = 1, 2, \ldots, n$. The coefficients a_{ijl}, b_{il}, c_{il} and d_l are unknown. Using the public key one can generate a large number of plaintext and ciphertext pairs. Substituting these plaintext and ciphertext pairs in (1.4) one can get the linear equations in the unknowns coefficients $a_{ijl}, b_{il}, c_{il}, d_l$ and these linear equations can be solved to find these unknown coefficients. Once we know all the equations (1.4) satisfied by all the ciphertext-plaintext pairs, after substituting the given ciphertext, we get linear equations in plaintext variables x_i which can be solved efficiently by Gaussian elimination method. Detail description of this attack can be found in [63] and [44].

1.3.2 The Cryptosystem HFE

The cryptosystem HFE (Hidden Field Equations) uses the map on $\mathbb{F}_{q^n}$ given by

$$f(x) = \sum_{i=0}^{r_2-1} \sum_{j=0}^{i} a_{ij} x^{q^i+q^j} + \sum_{i=0}^{r_1-1} b_i x^{q^i} + c, \tag{1.5}$$

where the coefficients $a_{ij}, b_i, c \in \mathbb{F}_{q^n}$ are randomly chosen, and r_1, r_2 are chosen so that the degree of f is less than some parameter d. Then, the polynomials $f_1, \ldots, f_n$ obtained as in (1.2) are quadratic polynomials over the finite field $\mathbb{F}_q$.

Public Key

The public key includes the following information:

1) The field $\mathbb{F}_q$, including its additive and multiplicative structure

2) The multivariate quadratic polynomials $f_1, \ldots, f_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$.

Private Key

The private key includes the following information:

1) The polynomial $f(x)$

2) The invertible affine transformations L_1 and L_2.

Encryption

Encryption is done by evaluating the public polynomials $f_i(x_1, \ldots, x_n)$ at message $x = (x_1, \ldots, x_n)$. If $y_i = f_i$, then corresponding ciphertext is $y = (y_1, \ldots, y_n)$.

Decryption

Given the ciphertext $y = (y_1, \ldots, y_n)$, decryption includes the following steps:

1) Compute $(z_1, \ldots, z_n) = L_2^{-1}(y_1, \ldots, y_n)$.

2) Let $z = \phi^{-1}(z_1, \ldots, z_n)$. Compute the set

$$\mathcal{Z} = \{\mathfrak{u} \in \mathbb{F}_{q^n} | f(\mathfrak{u}) = z\}.$$

To compute $\mathcal{Z}$ we may use Berlekamp algorithm, a root finding algorithm over finite fields. Roots finding algorithms are polynomial in the degree of the polynomials so the degree of $f(x)$ should not be too large, otherwise the decryption process is inefficient. Equivalently, we must not choose r_1, r_2 too large.

3) For each element $\mathfrak{u}_\mathfrak{i} \in \mathcal{Z}$, compute

$$(x_{i1}, \ldots, x_{in}) = L_1^{-1} \circ \phi(\mathfrak{u}_\mathfrak{i})$$

Although we would like that $f(x)$ is one to one map of finite field $\mathbb{F}_{q^n}$; that is there is only one element in $\mathcal{Z}$, it is possible that $\mathcal{Z}$ has multiple elements. In this case we can use one of several techniques (hash functions, plus method, etc.) to detect the plaintext among the solutions.

1.3.3 The Cryptosystem Little Dragon

In the Little Dragon cryptosystem, the exponent of the monomial x^h has slightly different form than in MIC*, namely, the exponent h, $0 < h < q^n$, such that $h+1$ is a sum of two different powers of q, that is, $h = q^\theta + q^\varphi - 1$. We choose θ and φ from the set $\{1, \ldots, n-1\}$ such that $\gcd(h, q^n - 1) = 1$. Suppose $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ denotes the plaintext variable and $y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$ denotes the cipher text variables. For the invertible linear transformation L_1 and L_2 of $\mathbb{F}_q^n$, $L_1(x_1, \ldots, x_n)$ and $L_2(y_1, \ldots, y_n)$ are first computed. Suppose $u = \phi^{-1} \circ L_1(x_1, \ldots, x_n)$ and $v = \phi^{-1} \circ L_2(y_1, \ldots, y_n)$. Now the relation between plaintext variables and ciphertext variables is

$$v = u^{q^\theta + q^\varphi - 1} \tag{1.6}$$

Note that if $x \neq 0$ then $u \neq 0$ in field $\mathbb{F}_{q^n}$. From (1.6) we obtain the following relation between the plaintext and the ciphertext:

$$vu = u^{q^\theta}.u^{q^\varphi} \tag{1.7}$$

Note that u^{q^θ} and u^{q^φ} are linear maps of $\mathbb{F}_{q^n}$. Now substituting $u = \phi^{-1} \circ L_1(x_1, \ldots, x_n)$ and $v = \phi^{-1} \circ L_2^{-1}(y_1, \ldots, y_n)$, and taking n-tuple representation using the basis $\mathbb{B}$, one can get the n equations of the form

$$\sum_{1 \leq i,j \leq n} a_{ijl} x_i y_j + \sum_{i \leq i \leq n} b_{ijl} x_i x_j = 0, \tag{1.8}$$

$l = 1, 2, \ldots, n$.

Public Key

Public key key is the n equations described in (1.8).

Private Key

The private key is the invertible affine transformations L_1 and L_2.

Encryption

The encryption is done as follows: 1) First, put the plaintext $(x_1, \ldots, x_n)$ in (1.8) and obtain n linear equations in the ciphertext variables y_i.
2) Solve these linear equations by Gaussian elimination method to get the required ciphertext $(y_1, \ldots, y_n)$.

Decryption

The decryption process includes the following steps:
1) First, compute $v = \phi^{-1} \circ L_2(y_1, \ldots, y_n)$.
2) Next, compute $z = v^t$, where $t(q^\theta + q^\varphi - 1) \equiv 1 \mod (q^n - 1)$.
3) Finally, compute $x = L_1^{-1}(\phi(z))$. Then, $x = (x_1, \ldots, x_n)$ is the required plaintext.

Patarin and Coopersmith [64] later found that the Little Dragon cryptosystem is not secure. The attack on little Dragon cryptosystem can also be found in [44].

1.3.4 The Cryptosystem Big Dragon

In Big Dragon cryptosystem the exponent of the monomial x^h is an integer of the form

$$h = q^{\theta_1} + q^{\theta_2} - q^{\varphi_1} - q^{\varphi_2}$$

such that $\gcd(h, q^n - 1) = 1$. Take a linear map ψ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ such that $\frac{\psi(v)}{v}$ is one-to-one map on the set $\mathbb{F}_{q^n}^*$ of nonzero elements of $\mathbb{F}_{q^n}$. The relation between the plaintext and the ciphertext variables is

$$u^h = \frac{\psi(v)}{v}. \tag{1.9}$$

Equivalently, we have the following relation between plaintext and ciphertext variables:

$$u^{q_1^\theta + q_2^\theta} v + u^{q_1^\varphi + q_2^\varphi} \psi(v) = 0. \tag{1.10}$$

Now substituting $u = \phi^{-1} \circ L_1(x_1, \ldots, x_n)$ and $v = \phi^{-1} \circ L_2^{-1}(y_1, \ldots, y_n)$, and taking the n-tuple representation using the basis $\mathbb{B}$, one can get n equations containing terms of the form $a_{ijk} x_i x_j y_k$, and there might also be terms of the forms $x_i y_k$, $x_i x_j$, y_k, etc. These n equations will be the public key of the cryptosystem. Note that the public equations are quadratic in plaintext variables x_i and linear in ciphertext variables y_j. One substitutes the plaintext in the public key and solves the resulting system of linear equations by Gaussian elimination method to get the ciphertext. Given a ciphertext the public equations are non-linear in the plaintext variables. To decrypt a message one uses the private key L_1, L_2, ψ and the relation (1.9).

Unfortunately, as explained in Patarin's expanded version of the paper [64], the Big Dragon is often vulnerable to the same type of attacks as in the case of the Little Dragon, at least when the function $\psi(v)$ is publicly known [64, 44]. However if $\psi(v)$ is kept secret, there is no known attack on the Big Dragon.

In Chapter 4 and Chapter 5 of this thesis, we have designed two efficient multivariate public key cryptosystems. Like Big Dragon Cryptosystem, the public key is mixed type of total degree three; two in plaintext variables and one in ciphertext variables. However it is possible to reduce the public key size by writing it as two sets of quadratic equations.

Chapter 2

Permutation Polynomials over the Finite Ring $\mathbb{Z}_m$

2.1 Introduction

In this chapter, we consider the problem of characterizing permutation polynomials over finite ring $\mathbb{Z}_{p^n}$. For any positive integer m, $\mathbb{Z}_m$ denotes the ring of integers modulo m. We seek necessary and sufficient conditions on the coefficients of a polynomial for it to be a permutation polynomial. In Section 2 of this chapter, we characterize permutation polynomial over finite ring $\mathbb{Z}_{p^n}$ for $p = 2, 3, 5$ and give a class of permutation binomials over finite field $\mathbb{Z}_p$. In Section 3, we show that every polynomial over $\mathbb{Z}_{p^n}$ can be represented by a triangular mapping over $\mathbb{Z}_p^n$ and using this representation, we find sufficient conditions for a polynomial to be a permutation polynomial over $\mathbb{Z}_{p^n}$. Consider the congruences

$$f(x) \equiv 0 \bmod p^n, \tag{2.1}$$

$$f(x) \equiv 0 \bmod p^{n-1}, \tag{2.2}$$

where $f(x)$ is any integral polynomial, p is prime and $n > 1$. Then the following result on solutions of the above congruences is well-known.

Theorem 2.1.1. *(Hardy & Wright [38]) The number of solutions of (2.1) corresponding to a solution ξ of (2.2) is*

(a) none, if $f'(\xi) \equiv 0 \bmod p$ and ξ is not a solution of (2.1);

(b) one, if $f'(\xi) \not\equiv 0 \bmod p$;

(c) p, if $f'(\xi) \equiv 0 \bmod p$ and ξ is a solution of (2.1).

The solutions of (2.1) corresponding to ξ may be derived from ξ, in case (b) holds, the solution is $\xi (\bmod p^n)$, and in case (c) holds, the solutions are by $\xi + kp^{n-1} (\bmod p^n)$, $0 \leq k \leq p-1$.

We will use this classical result extensively to study permutation polynomials over the finite ring $\mathbb{Z}_{p^n}$, where p is a prime.

2.2 Congruences modulo prime powers and permutation polynomials of finite rings $\mathbb{Z}_{p^n}$

As a consequence of the Theorem 2.1.1, we have the following result.

Proposition 2.2.1. *Let p be a prime. Then $f(x)$ is permutation polynomial of $\mathbb{Z}_{p^n}$ $(n > 1)$ if and only if it is permutation polynomial of $\mathbb{Z}_p$ and $f'(a) \not\equiv 0 \bmod p$ for all $a \in \mathbb{Z}_p$.*

Proof. First suppose that $f(x)$ is a permutation polynomial of $\mathbb{Z}_{p^n}$. Take any $\tilde{b} \in \mathbb{Z}_p$. Suppose $b \in \mathbb{Z}_{p^n}$ such that, b modulo $p = \tilde{b}$. There exist $a \in \mathbb{Z}_{p^n}$ such that $f(a) = b$. We can take, a modulo $p = \tilde{a}$ such that $f(\tilde{a}) = \tilde{b}$. This proves that $f(x)$ is a permutation polynomial of $\mathbb{Z}_p$. Since $g(x) = f(x) - f(a)$ has only one solution, therefore by the Theorem 2.1.1, we have $g^{'}(x) = f^{'}(x) \neq 0$ modulo p. For the converse part, take any $b \in \mathbb{Z}_{p^n}$. Suppose $g(x) = f(x) - b$. Then we have $g(x) = 0$ modulo p has one solution and $g^{'}(x) = f^{'}(x) \neq 0$ modulo p. Therefore by The Theorem 2.1.1, we have that $g(x) = 0$ modulo p^2 has a solution. Repeating the argument, we can say that $g(x) = 0$ modulo p^n has a solution, that is, $f(x)$ is a permutation of $\mathbb{Z}_{p^n}$. □

In this section we give necessary and sufficient conditions on the coefficients $a_0, a_1, \ldots, a_d$ for $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$ to be permutation polynomial modulo p^n, for $p = 2, 3, 5$. A characterization of permutation polynomials modulo 2^n was given in [67]. Rivest [67] proved that $f(x)$ is a permutation polynomial if and only if a_1 is odd, $(a_2+a_4+a_6+\ldots)$ is even, and $(a_3+a_5+a_7+\ldots)$ is even. We first give a very short and simple proof of the above characterization. We also give new characterization of permutation polynomials modulo p^n for $p = 3, 5$, and $n > 1$. A simple characterization of permutation polynomial modulo 2^n, $n > 1$, is given in Theorem 2.2.3 of this section. The theorem requires the following lemma.

Lemma 2.2.2. *A polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$ with integral coefficients is a permutation polynomial modulo 2 if and only if $(a_1+a_2+\ldots+a_d)$ is odd.*

Proof: Since $0^i = 0$ and $1^i = 1$ modulo 2 for $i \geq 1$, we can write $f(x) = a_0 + (a_1 + a_2 + \cdots + a_d)x \bmod 2$. Clearly $f(x)$ is a permutation polynomial modulo 2 if and only if $(a_1+a_2+\cdots+a_d) \not\equiv 0 \bmod 2$, that is, $(a_1+a_2+\cdots+a_d)$ is odd. □

Theorem 2.2.3. *(Rivest [67]) A polynomial $f(x) = a_0+a_1x+a_2x^2+\cdots+a_dx^d$ with integral coefficients is a permutation polynomial modulo 2^n, $n > 1$, if and only if a_1 is odd, $(a_2 + a_4 + a_6 + \ldots)$ is even, and $(a_3 + a_5 + a_7 + \ldots)$ is even.*

Proof: The proof given here is different from that of Rivest [67] and is relevant to the proof of theorems to follow. The theorem is proved by making use of Proposition 2.2.1 and Lemma 2.2.2. By Proposition 2.2.1, $f(x)$ is a permutation polynomial modulo 2^n if and only if it is a permutation polynomial modulo 2 and $f'(x) \not\equiv 0 \bmod 2$ for every integer $x \in \mathbb{Z}_2$. By Lemma 2.2.2, $f(x)$ is a permutation polynomial modulo 2 if and only if $(a_1 + a_2 + \ldots + a_d)$ is odd. It is easy to cheek that $f'(x) = a_1 + (a_3 + a_5 + \ldots)x \bmod 2$. The condition $f'(x) \not\equiv 0 \bmod 2$ with $x = 0$ gives a_1 is odd. The condition $f'(x) \not\equiv 0 \bmod 2$ with $x = 1$ gives $(a_1 + a_3 + a_5 + \ldots)$ is odd. Hence the theorem follows. □

Example 2.2.4. The following are all permutation polynomials modulo 2^2 of degree at most 3 and the coefficients are from $\mathbb{Z}_4$: x, $3x$, $x + 2x^2$, $3x + 2x^2$, $x + 2x^3$, $3x + 2x^3$, $x + 2x + 2x^3$ and $3x + 2x^2 + 2x^3$.

Lemma 2.2.5. *A polynomial* $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$ *with integral coefficients is a permutation polynomial modulo* 3 *if and only if* $(a_1 + a_3 + \ldots) \not\equiv 0 \bmod 3$ *and* $(a_2 + a_4 + \ldots) \equiv 0 \bmod 3$.

Proof: Since $x^{2k+1} = x \bmod 3$ and $x^{2k} = x^2 \bmod 3$ for $k \geq 1$, we can write $f(x) = a_0 + (a_1 + a_3 + \ldots)x + (a_2 + a_4 + \ldots)x^2 \bmod 3$. Letting $A = (a_1 + a_3 + \ldots) \bmod 3$ and $B = (a_2 + a_4 + \ldots) \bmod 3$, we can write $f(x)$ more compactly as $f(x) = a_0 + Ax + Bx^2$. It follows from Corollary 1.2.6 that no permutation polynomial over Z_3 can have degree 2. Therefore, we have $B \equiv 0 \bmod 3$. Thus $f(x)$ is a permutation polynomial modulo 3 if and only if $(a_1 + a_3 + \ldots) \not\equiv 0 \bmod 3$ and $(a_2 + a_4 + \ldots) \equiv 0 \bmod 3$. □

Theorem 2.2.6. *A polynomial* $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$ *with integral coefficients is a permutation polynomial modulo* 3^n, $n > 1$, *if and only if*

(a) $a_1 \not\equiv 0 \bmod 3$,

(b) $(a_1 + a_3 + \ldots) \not\equiv 0 \bmod 3$,

(c) $(a_2 + a_4 + \ldots) \equiv 0 \bmod 3$,

(d) $(a_1 + a_4 + a_7 + a_{10} + \ldots) + 2(a_2 + a_5 + a_8 + a_{11} + \ldots) \not\equiv 0 \bmod 3$, *and*

(e) $(a_1 + a_2 + a_7 + a_8 + \ldots) + 2(a_4 + a_5 + a_{10} + a_{11} + \ldots) \not\equiv 0 \bmod 3$.

Proof: By Proposition 2.2.1, $f(x)$ is a permutation polynomial modulo 3^n if and only if it is a permutation polynomial modulo 3 and $f'(x) \not\equiv 0 \bmod 3$ for every integer $x \in Z_3$. It is easy to verify that $f'(x) = a_1 + (2a_2 + a_4 + 2a_8 + a_{10} + 2a_{14} + a_{16} + \ldots)x + (2a_5 + a_7 + 2a_{11} + a_{13} + 2a_{17} + a_{19} + \ldots)x^2 \bmod 3$. The condition $f'(x) \not\equiv 0 \bmod 3$ with $x = 0$ gives $a_1 \not\equiv 0 \bmod 3$. The condition $f'(x) \not\equiv 0 \bmod 3$ with $x = 1$ gives $a_1 + (2a_2 + a_4 + 2a_8 + a_{10} + 2a_{14} + a_{16} + \ldots) + (2a_5 + a_7 + 2a_{11} + a_{13} + 2a_{17} + a_{19} + \ldots) \not\equiv 0 \bmod 3$. The condition $f'(x) \not\equiv 0 \bmod 3$ with $x = 2$ gives $a_1 + (a_2 + 2a_4 + a_8 + 2a_{10} + a_{14} + 2a_{16} + \ldots) + (2a_5 + a_7 + 2a_{11} + a_{13} + 2a_{17} + a_{19} + \ldots) \not\equiv 0 \bmod 3$. Now the theorem directly follows by combining above conditions and Lemma 2.2.5. □

Example 2.2.7. The following are some permutation polynomials modulo 9 of degree 5 and the coefficients are from $\mathbb{Z}_9$: $7x + x^3 + 8x^5$, $x + x^2 + 8x^3 + 8x^4 + 7x^5$,

$7x + 6x^2 + 8x^3 + 8x^5$ and $x + 7x^2 + 8x^3 + 8x^4 + 7x^5$. There are total 3888 permutation polynomials modulo 9 of degree at most 5 and the coefficients are from $\mathbb{Z}_9$.

Theorem 2.2.8. (Mollin & Small [59]) *Let p be a prime different from 3 such that $p \equiv 2 \bmod 3$. Then $f(x) = ax^3 + bx^2 + cx + d$ $(a \neq 0)$ permutes $\mathbb{Z}_p$ if and only if $b^2 = 3ac$.*

Lemma 2.2.9. *A polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$ with integral coefficients is a permutation polynomial modulo 5 if and only if $(a_4 + a_8 + a_{12} \ldots) \equiv 0 \bmod 5$ and*

$$(a_2 + a_6 + a_{10} + \ldots)^2 \equiv 3(a_1 + a_5 + a_9 + \ldots)(a_3 + a_7 + a_{11} + \ldots) \bmod 5.$$

Proof: Since $x^{4k+1} = x \bmod 5$, $x^{4k+2} = x^2 \bmod 5$, $x^{4k+3} = x^3 \bmod 5$, and $x^{4k} = x^4 \bmod 5$ for $k \geq 1$, we can write $f(x) = a_0 + (a_1 + a_5 + \ldots)x + (a_2 + a_6 + \ldots)x^2 + (a_3 + a_7 + \ldots)x^3 + (a_4 + a_8 + \ldots)x^4 \bmod 5$. Letting $A = (a_1 + a_5 + \ldots)$, $B = (a_2 + a_6 + \ldots)$, $C = (a_3 + a_7 + \ldots)$ and $D = (a_4 + a_8 + \ldots)$ we can write $f(x) = a_0 + Ax + Bx^2 + Cx^3 + Dx^4 \bmod 5$. By corollary 1.2.6, no polynomial of degree 4 can be a permutation polynomial modulo 5, so $D \equiv 0 \bmod 5$. Now $f(x) = a_0 + Ax + Bx^2 + Cx^3 \bmod 5$ and we are in the situation of Theorem 2.2.8. Hence, f is a permutation if and only if $B^2 = 3AC$. □

Example 2.2.10. The permutation binomials modulo 5 of degree at most 3 are: x, x^3, $2x + x^2 + x^3$, $3x + 2x^2 + x^3$, $3x + 3x^2 + x^3$, and $2x + 4x^2 + x^3$.

Theorem 2.2.11. *A polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$ with integral coefficients is a permutation polynomial modulo 5^n if and only if*

(a) $a_1 \not\equiv 0 \bmod 5$,

(b) $(a_4 + a_8 + a_{12} \ldots) \equiv 0 \bmod 5$,

(c) $(a_2 + a_6 + a_{10} + \ldots)^2 \equiv 3(a_1 + a_5 + a_9 + \ldots)(a_3 + a_7 + a_{11} + \ldots) \bmod 5$,

(d) $(a_1 + a_6 + a_{11} + \ldots) + 2(a_2 + a_7 + a_{12} + \ldots) + 3(a_3 + a_8 + a_{13} + \ldots) + 4(a_4 + a_9 + a_{14} + \ldots) \not\equiv 0 \bmod 5$,

(e) $(a_1 + 2a_6 + 4a_{11} + 3a_{16} + a_{21} + \ldots) + 2(2a_2 + 4a_7 + 3a_{12} + a_{17} + 2a_{22} + \ldots)$ $+3(4a_3+3a_8+a_{13}+2a_{18}+4a_{23}+\ldots)+4(3a_4+a_9+2a_{14}+4a_{19}+3a_{24}+\ldots) \not\equiv$ $0 \bmod 5$,

(f) $(a_1 + 3a_6 + 4a_{11} + 2a_{16} + a_{21} + \ldots) + 2(3a_2 + 4a_7 + 2a_{12} + a_{17} + 3a_{22} + \ldots)$ $+3(4a_3+2a_8+a_{13}+3a_{18}+4a_{23}+\ldots)+4(2a_4+a_9+3a_{14}+4a_{19}+2a_{24}+\ldots) \not\equiv$ $0 \bmod 5$, *and*

(g) $(a_1 + 4a_6 + a_{11} + 4a_{16} + a_{21} + \ldots) + 2(4a_2 + a_7 + 4a_{12} + a_{17} + 4a_{22} + \ldots)$ $+3(a_3+4a_8+a_{13}+4a_{18}+a_{23}+\ldots)+4(4a_4+a_9+4a_{14}+a_{19}+4a_{24}+\ldots) \not\equiv$ $0 \bmod 5$.

Proof. By Proposition 2.2.1, $f(x)$ is a permutation polynomial modulo 5^n if and only if it is a permutation polynomial modulo 5 and $f'(x) \not\equiv 0 \bmod 5$ for every integer $x \in \mathbb{Z}_5$. We obtain

$$\begin{aligned} f'(x) &= a_1 + \sum_k (4k+2)a_{4k+2}x + \sum_k (4k+3)a_{4k+3}x^2 + \sum_k (4k)a_{4k}x^3 \\ &\quad + \sum_k (4k+1)a_{4k+1}x^4 \\ &\equiv a_1 + (2a_2 + a_6 + 4a_{14} + 3a_{18} + 2a_{22} + \ldots)\, x \\ &\quad + (3a_3 + 2a_7 + a_{11} + 4a_{19} + 3a_{23} + \ldots)\, x^2 \\ &\quad + (4a_4 + 3a_8 + 2a_{12} + a_{16} + 4a_{24} + \ldots)\, x^3 \\ &\quad + (4a_9 + 3a_{13} + 2a_{17} + a_{21} + 4a_{29} + \ldots)\, x^4 \bmod 5 \end{aligned}$$

Observe that $f'(0) \not\equiv 0 \bmod 5$ means $a_1 \not\equiv 0 \bmod 5$;
$f'(1) \not\equiv 0 \bmod 5$ gives $(a_1 + a_6 + a_{11} + \ldots) + 2(a_2 + a_7 + a_{12} + \ldots) + 3(a_3 + a_8 + a_{13} + \ldots) + 4(a_4 + a_9 + a_{14} + \ldots) \not\equiv 0 \bmod 5$;
$f'(2) \not\equiv 0 \bmod 5$ gives $(a_1 + 2a_6 + 4a_{11} + 3a_{16} + a_{21} + \ldots) + 2(2a_2 + 4a_7 + 3a_{12} + a_{17} + 2a_{22} + \ldots)$ $+3(4a_3 + 3a_8 + a_{13} + 2a_{18} + 4a_{23} + \ldots) + 4(3a_4 + a_9 + 2a_{14} + 4a_{19} + 3a_{24} + \ldots) \not\equiv 0 \bmod 5$;
$f'(3) \not\equiv 0 \bmod 5$ gives $(a_1 + 3a_6 + 4a_{11} + 2a_{16} + a_{21} + \ldots) + 2(3a_2 + 4a_7 + 2a_{12} + a_{17} + 3a_{22} + \ldots)$ $+3(4a_3 + 2a_8 + a_{13} + 3a_{18} + 4a_{23} + \ldots) + 4(2a_4 + a_9 + 3a_{14} + 4a_{19} + 2a_{24} + \ldots) \not\equiv 0 \bmod 5$; and
$f'(4) \not\equiv 0 \bmod 5$ gives $(a_1+4a_6+a_{11}+4a_{16}+a_{21}+\ldots)+2(4a_2+a_7+4a_{12}+a_{17}+4a_{22}+\ldots)$ $+3(a_3+4a_8+a_{13}+4a_{18}+a_{23}+\ldots)+4(4a_4+a_9+4a_{14}+a_{19}+4a_{24}+\ldots) \not\equiv$

0 mod 5. Now the theorem directly follows by combining above conditions and Lemma 2.2.9. □

We give one example of a permutation polynomial over $\mathbb{Z}_{5^n}$, $n \geq 1$.

Example 2.2.12. Consider the polynomial $f(x) = x + x^2 + 2x^3 + 2x^4 + x^5 + x^6 + 4x^7 + 3x^8 + x^9 + x^{10}$. It can be easily shown that the conditions (a)-(g) of Theorem 2.2.11 are satisfied by the coefficients of $f(x)$. Thus $f(x)$ is a permutation polynomial of $\mathbb{Z}_{5^n}$, $n \geq 1$.

2.2.1 A new class of permutation binomials over $\mathbb{Z}_p$

Suppose p is an odd prime and a is an integer. a is defined to be a *quadratic residue* modulo p if $a \not\equiv 0 \pmod{p}$ and the congruence $y^2 \equiv a \pmod{p}$ has a solution $y \in \mathbb{F}_p$. a is defined to be a *quadratic non-residue* modulo p if $a \not\equiv 0 \pmod{p}$ and a is not a quadratic residue modulo p.

Theorem 2.2.13. (Euler's Criterion) *An integer a is a quadratic residue modulo p if and only if $a^{\frac{p-1}{2}} \equiv 1 \bmod p$.*

Theorem 2.2.14. *Let p be a prime and $f(x) = x^u(x^{\frac{p-1}{2}} + a)$, where u is an integer such that $(u, p-1) = 1$ and a is a non-zero element in $\mathbb{Z}_p$. Then $f(x)$ is a permutation binomial over $\mathbb{Z}_p$ if and only if $(a^2-1)^{\frac{p-1}{2}} = 1 \bmod p$.*

Proof: It is known that the monomial x^u is a permutation polynomial of $\mathbb{Z}_p$ if and only if $\gcd(u, p-1) = 1$. Using Euler's criteria we can rewrite

$$f(x) = \begin{cases} 0, & \text{if } x = 0; \\ x^u(a+1), & \text{if } x \text{ is quadratic residue;} \\ x^u(a-1), & \text{if } x \text{ is quadratic non-residue.} \end{cases}$$

There are $\frac{1}{2}(p-1)$ residues and $\frac{1}{2}(p-1)$ non-residues of an odd prime p. The product of two residues, or of two non-residues, is a residue, while the product of a residue and a non-residue is a non-residue. Since u is odd, x^u is residue (resp. non-residue) if x is residue (resp. non-residue). If both $a+1$ and $a-1$ are residues, then $f(x)$ maps residues to residues and non-residues to non-residues and if both $a+1$ and $a-1$ are non-residues, then $f(x)$ maps residues

to non-residues and non-residues to residues. On the other hand, if $a+1$ is residue and $a-1$ is non-residue then $f(x)$ maps all the non-zero elements to residues and if $a+1$ is non-residue and $a-1$ is residue then $f(x)$ maps all the non-zero elements to non-residues. Since x^u is a permutation polynomial, therefore $f(x)$ is a permutation polynomial if and only if both $a+1$ and $a-1$ are either quadratic residues or quadratic non residues. In other words, $f(x)$ is a permutation polynomial over $\mathbb{Z}_p$ if and only if $(a^2-1)^{\frac{p-1}{2}} = 1 \bmod p$. □

It may be noted that if the degree $u+\frac{p-1}{2}$ of binomial $f(x)$ of Theorem 2.2.14 is greater than $p-1$ for some values of u, then the polynomial is reduced modulo $x^p - x$ to obtain a permutation binomial. We now generate some permutation binomials of $\mathbb{Z}_p$ using Theorem 2.2.14. We list these examples in the table below.

p	u	a	$f(x)$
7	1	3	$x(x^3+3)$
7	1	4	$x(x^3+4)$
7	5	3	$x^2(x^3+5)$
7	5	4	$x^2(x^3+2)$
11	1	2	$x(x^5+2)$
11	3	4	$x^3(x^5+2)$
11	7	4	$x^2(x^5+3)$
11	9	9	$x^4(x^5+5)$
11	9	2	$x^4(x^5+6)$
11	9	4	$x^4(x^5+3)$
11	9	7	$x^4(x^5+8)$

Table 2.1: Some Permutation Binomials

2.3 Polynomials over the ring $\mathbb{Z}_{p^n}$ and Triangular mappings over $\mathbb{Z}_p^n$

Klimov *et. al.* [43] showed that every polynomial over $\mathbb{Z}_{2^n}$ can be expressed as a triangular mapping on $\mathbb{Z}_2^n$. In this section, generalizing this result we show that every polynomial over $\mathbb{Z}_{p^n}$ can be represented by a triangular mapping over $\mathbb{Z}_p^n$. An element $x \in \mathbb{Z}_{p^n}$ can be uniquely expressed as $x = \sum_{i=1}^{n} x_i p^{i-1}$, where $x_i \in \mathbb{Z}_p$. Let $\theta : \mathbb{Z}_{p^n} \mapsto \mathbb{Z}_p^n$ be the isomorphism of $\mathbb{Z}_{p^n}$ onto $\mathbb{Z}_p^n$ defined by $\theta(x) = (x_1, x_2, \ldots, x_n)$. We identify x by the n-tuple $(x_1, x_2, \ldots, x_n)$ in $\mathbb{Z}_p^n$. For a polynomial $f(x)$ over $\mathbb{Z}_{p^n}$, we have $\theta(f(x)) = (f_1, f_2, \ldots, f_n)$, where each f_i is function of $x_1, x_2, \ldots, x_n$. We will denote the i-th coordinate $f_i(x)$ of $f(x)$ by $(f(x))_i$.

Lemma 2.3.1. *Let $x, y \in \mathbb{Z}_{p^n}$ and $x_i, y_i, (x+y)_i$ and $(xy)_i$ respectively denote the i-th coordinates in the n-tuple representation of $x, y, x+y$ and xy over $\mathbb{Z}_p^n$. Then*

(i) $(x+y)_1 = (x_1 + y_1) \bmod p$.

(ii) for $i \geq 2$, $(x+y)_i = (x_i + y_i + \alpha_i) \bmod p$, *where α_i is a function of the coordinates $x_1, x_2, \ldots, x_{i-1}, y_1, y_2, \ldots, y_{i-1}$.*

(iii) for $i \geq 2$, $(xy)_i = (x_i y_1 + x_1 y_i + \beta_i) \bmod p$, *where β_i is a function of the coordinates $x_1, x_2, \ldots, x_{i-1}, y_1, y_2, \ldots, y_{i-1}$.*

(iv) for any integer $m \geq 2$, $(x^m)_1 = (x_1)^m \bmod p$ *and* $(x^m)_i = (m x_i (x_1)^{m-1} + \gamma_i) \bmod p$, *if $i \geq 2$, where γ_i is a function of the coordinates $x_1, x_2, \ldots, x_{i-1}$.*

Proof. We have $x = \sum_{i=1}^{n} x_i p^{i-1}$ and $y = (y_1, y_2, \ldots, y_n) = \sum_{i=1}^{n} y_i p^{i-1}$. The first assertion in trivial. In (ii) α_i is the carry over from the previous coordinates in the sum, so depends only on the coordinates $x_1, x_2, \ldots, x_{i-1}$, $y_1, y_2, \ldots, y_{i-1}$. For (iii) we note that $xy = x_1 y_1 + (x_1 y_2 + y_1 x_2)p + \cdots + (x_i y_1 + y_i x_1 + x_{i-1} y_2 + \cdots + x_2 y_{i-1})p^{i-1} + \cdots + (x_n y_1 + x_{n-1} y_2 + \cdots + x_1 y_n)p^{n-1}$. from which it follows that $(xy)_i$ is the sum modulo p of the coefficient of p^{i-1} and the carry over from the previous coordinates. Finally, the second part of (iv) follows easily from (iii) by induction on m. □

Remark 2.3.2. *The result (iv) of the above lemma shows that if $f(x)$ is a monomial $x^l, l \geq 1$, then $\theta(f(x)) = ((f(x))_1, (f(x))_2, \ldots, (f(x))_n)$ is a triangular mapping from $\mathbb{Z}_p^n$ to $\mathbb{Z}_p^n$.*

Lemma 2.3.3. *Let $x = \sum_{i=1}^{n} x_i p^{i-1}$, $k \geq 1$, $1 \leq r \leq p-1$. Then for $i \geq 2$*

(i) $\left(x^{pk}\right)_i = \alpha_i \ mod\ p$,

(ii) $\left(x^{pk+r}\right)_i = r x_i (x_1)^{pk+r-1} + \beta_i \ mod\ p$,

where α_i, β_i are functions of $x_1, x_2, \ldots, x_{i-1}$.

Proof. The results follows from (iv) of Lemma 2.3.1. □

Next, we give some examples of triangular mappings obtained from monomials.

Example 2.3.4. Consider the monomials x, x^2, x^3 over $\mathbb{Z}_{2^3}$. For $x = x_1 + x_2.2 + x_3.2^2$, we have

$$\begin{aligned} \theta(x) &= (x_1, x_2, x_3), \\ \theta(x^2) &= (x_1, 0, x_2 + x_1x_2), \quad \text{and} \\ \theta(x^3) &= (x_1, x_1x_2, x_1x_3). \end{aligned}$$

Example 2.3.5. Consider the monomials x, x^2, x^3 over $\mathbb{Z}_{3^3}$. For $x = x_1 + x_2.3 + x_3.3^2$, we have

$$\begin{aligned} \theta(x) &= (x_1, x_2, x_3), \\ \theta(x^2) &= (x_1^2, 2x_1x_2, x_2^2 + 2x_1x_3), \quad \text{and} \\ \theta(x^3) &= (x_1^3, 0, x_1^2x_2). \end{aligned}$$

Example 2.3.6. Consider the monomials x, x^2, x^4, x^5 over $\mathbb{Z}_{5^4}$. For $x = x_1 + x_2.5 + x_3.5^2 + x_4.5^3$, we have

$$\begin{aligned} \theta(x^2) &= (x_1^2, 2x_1x_2, x_2^2 + 2x_1x_3, 2x_1x_4 + 2x_2x_3), \\ \theta(x^4) &= (x_1^4, 4x_1^3x_2, 4x_1^3x_3, x_1^2x_2^2, 4x_1^3x_4 + 2x_1) \quad \text{and} \\ \theta(x^5) &= (x_1^5, 0, x_1^4x_2, x_1^4x_3 + 2x_1^3x_2^2). \end{aligned}$$

Theorem 2.3.7. *Let $f(x) = \sum_{i=0}^{d} a_i x^i$ be a polynomial of degree d over $\mathbb{Z}_{p^n}$. Suppose $\theta(f(x)) = (f_1, f_2, \ldots, f_n)$. Then $\theta(f(x))$ is a triangular mapping from $\mathbb{Z}_p^n$ to $\mathbb{Z}_p^n$.*

Proof. By (i) of Lemma 2.3.1, we have $f_1 = (f(x))_1 = \sum_{i=0}^{d} (a_i)_1 (x_1)^i \mod p$. Similarly using Lemmas 2.3.1 and 2.3.3 it is easy to see that for $i \geq 1$ $(f(x))_i = f_i(x_1, x_2, \ldots, x_i)$ that is i-th coordinate of $f(x)$ is function of first i coordinates of x. □

Example 2.3.8. Suppose $f(x) = x + 2x^2 + x^3 + 4x^4 + x^5$ is a polynomial over $\mathbb{Z}_{2^3}$, then $\theta(f(x)) = (x_1, x_2, x_3 + x_1 x_2)$.

In view of Theorem 2.3.7 we have the following result.

Proposition 2.3.9. *Let $f(x) = \sum_{i=0}^{d} a_i x^i$ be a polynomial over $\mathbb{Z}_{p^n}$. Then $f(x)$ is a permutation polynomial of $\mathbb{Z}_{p^n}$ if and only if the corresponding triangular mapping $\theta(f(x))$ is permutation of $\mathbb{Z}_p^n$.*

Lemma 2.3.10. *Suppose $\psi(x_1, x_2, \ldots, x_n) = \begin{pmatrix} f_1(x_1) \\ f_2(x_1, x_2) \\ f_3(x_1, x_2, x_3) \\ \vdots \\ f_n(x_1, x_2, \ldots, x_n) \end{pmatrix}^T$. Then ψ is an invertible mapping from $\mathbb{Z}_p^n$ to $\mathbb{Z}_p^n$ if and only if each f_i as a function of x_i is invertible over $\mathbb{Z}_p$ for fixed x_j, $j < i$.*

Proof. First suppose that ψ is invertible over $\mathbb{Z}_p^n$, that is, given any $y \in \mathbb{Z}_p^n$ where $y = (y_1, y_2, \ldots, y_n)$ there exists $x = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_p^n$ such that $\psi(x) = y$. Thus we can write $f_1(x_1) = y_1$, $f_2(x_1, x_2) = y_2, \ldots, f_n(x_1, x_2, \ldots, x_n) = y_n$. Note that given $y_1 \in \mathbb{Z}_p$ there exist $x_1 \in \mathbb{Z}_p$ such that $f_1(x_1) = y_1$ or equivalently we can say that f_1 is invertible over $\mathbb{Z}_p$. Now fixing $x_1 = \alpha_1$,we have $f_2(\alpha_1, x_2) = y_2$. Thus given $y_2 \in \mathbb{Z}_p$ there is $x_2 \in \mathbb{Z}_p$ such that $f_2(\alpha_1, x_2) = y_2$ or in other word we can say that $f_2(\alpha_1, x_2)$ is invertible over $\mathbb{Z}_p$. In a similar way we can prove that each f_i as a function of x_i is invertible over $\mathbb{Z}_p$ for fixed x_j, $j < i$. It is easy to see the converse. □

In the following section we give sufficient conditions to be a permutation polynomial over finite ring $\mathbb{Z}_{p^n}$ for all prime number p.

Now, we use the triangular mapping method to give sufficient conditions for a polynomial over the ring $\mathbb{Z}_{p^n}$, $n \geq 1$, to be a permutation polynomial.

Theorem 2.3.11. *Let p be a prime and $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$ be a polynomial with integral coefficients. Then $f(x)$ is a permutation polynomial over $\mathbb{Z}_{p^n}$, $n \geq 1$, if*

$$\sum_{k=1} a_{k(p-1)+1} \neq 0 \bmod p, \tag{2.3}$$

$$\sum_{k=1} a_{k(p-1)+r} = 0 \bmod p, \quad \textit{for } r = 0, 2, 3, \ldots, p-2, \textit{ and} \tag{2.4}$$

$$\sum_{r=1}^{p-1} \sum_{k=0}^{\lfloor \frac{d-r}{p} \rfloor} r a_{pk+r} \ell^{pk+r-1} \neq 0 \bmod p \quad \textit{for } \ell = 0, 1, 2, \ldots, p-1. \tag{2.5}$$

Proof. Consider the triangular mapping $\theta(f(x))$ and let $(f(x))_i$ denote its i-th coordinate function. We show that each $(f(x))_i$, as a function of x_i and for fixed x_j, $j < i$, is invertible. For $i = 1$ we note that $\left(x^k\right)_1 = (x_1)^k \bmod p$ and $(x_1)^{k(p-1)+r} = (x_1)^r \bmod p$, for $1 \leq r \leq p-2$. Therefore, we get

$$\begin{aligned}
(f(x))_1 &= \left(a_0 + a_1x + a_2x^2 + \cdots + a_dx^d\right)_1 \\
&= (a_0)_1 + (a_1)_1x_1 + (a_2)_1(x_1)^2 + (a_3)_1(x_1)^3 + \cdots + (a_d)_1(x_1)^d \bmod p \\
&= (a_0)_1 + \sum_{k=1} \left(a_{k(p-1)}\right)_1 (x_1)^{k(p-1)} + \sum_{k=1} \left(a_{k(p-1)+1}\right)_1 (x_1)^{k(p-1)+1} + \cdots \\
&\quad + \sum_{k=1} \left(a_{k(p-1)+p-2}\right)_1 (x_1)^{k(p-1)+p-2} \bmod p \\
&= (a_0)_1 + \left(\sum_{k=1} \left(a_{k(p-1)}\right)_1\right) (x_1)^{k(p-1)} + \left(\sum_{k=1} \left(a_{k(p-1)+1}\right)_1\right) x_1 + \cdots \\
&\quad + \left(\sum_{k=1} \left(a_{k(p-1)+p-2}\right)_1\right) (x_1)^{p-2} \qquad \bmod p.
\end{aligned} \tag{2.6}$$

If $\sum_{k=1} \left(a_{k(p-1)+1}\right)_1 \neq 0 \bmod p$ and $\sum_{k=1} \left(a_{k(p-1)+r}\right)_1 = 0 \bmod p$ for $r = 0, 2, 3 \ldots\ldots p-2$, then the mapping in equation (2.6) will be invertible.

Now for the ith coordinate $i > 1$, using the part (ii) of Lemma 2.3.1 recursively, we have

$$\begin{aligned}(f(x))_i &= (a_0 + a_1x + a_2x^2 + \ldots + a_dx^d)_i \\ &= \left(a_0 + \sum_{k=1}^{\lfloor \frac{d}{p} \rfloor} a_{pk}x^{pk} + \sum_{r=1}^{p-1}\sum_{k=0}^{\lfloor \frac{d-r}{p} \rfloor} a_{pk+r}x^{pk+r}\right)_i \\ &= \sum_{k=1}^{\lfloor \frac{d}{p} \rfloor} \left(a_{pk}x^{pk}\right)_i + \sum_{r=1}^{p-1}\sum_{k=0}^{\lfloor \frac{d-r}{p} \rfloor} \left(a_{pk+r}x^{pk+r}\right)_i + \beta_1 \qquad \mod p.\end{aligned}$$

where β_1 is a function of first $i-1$ coordinates of x. Using Lemma 2.3.1 and Lemma 2.3.3 we get

$$\begin{aligned}\left(a_{pk}x^{pk}\right)_i &= (a_{pk})_i \left(x^{pk}\right)_1 + (a_{pk})_1 \left(x^{pk}\right)_i + \beta_2 \qquad \mod p \\ &= \beta',\end{aligned}$$

where β' is a function of first $i-1$ coordinates of x. For the powers of x, that are of the form $r \pmod p$, we get

$$\begin{aligned}(a_{pk+r}x^{pk+r})_i &= (a_{pk+r})_i(x^{pk+r})_1 + (a_{pk+r})_1(x^{pk+r})_i + \beta_3 \qquad \mod p \\ &= (a_{pk+r})_i(x^{pk+r})_1 + (a_{pk+r})_1\left(r(x_1)^{pk+r-1}x_i + \beta_4\right) + \beta_3 \qquad \mod p \\ &= r(a_{pk+r})_1(x_1)^{pk+r-1}x_i + \gamma' \qquad \mod p,\end{aligned}$$

where β_3, β_4 and γ' are functions of first $i-1$ coordinates of x. Note that $\gamma' = (a_{pk+r})_i(x^{pk+r})_1 + (a_{pk+r})_1\beta_4 + \beta_3$. Bringing them all together, we have

$$\begin{aligned}(f(x))_i &= \sum_{r=1}^{p-1}\sum_{k=0}^{\lfloor \frac{d-r}{p} \rfloor} r(a_{pk+r})_1(x_1)^{pk+r-1}x_i + \beta^\star \qquad \mod p \\ &= x_i\sum_{r=1}^{p-1}\sum_{k=0}^{\lfloor \frac{d-r}{p} \rfloor} r(a_{pk+r})_1(x_1)^{pk+r-1} + \beta^\star \qquad \mod p,\end{aligned}$$

where $\beta^\star$ is function of first $i-1$ coordinates of x. For $f(x)$ to be permutation

polynomial this mapping should be invertible for all values of x_1. Thus we get the conditions

$$\sum_{r=1}^{p-1} \sum_{k=0}^{\lfloor \frac{d-r}{p} \rfloor} r(a_{pk+r})_1 (x_1)^{pk+r-1} \neq 0 \bmod p$$

Suppose $\ell = x_1$, then we can rewrite it in the form

$$\sum_{r=1}^{p-1} \sum_{k=0}^{\lfloor \frac{d-r}{p} \rfloor} r a_{pk+r} \ell^{pk+r-1} \neq 0 \mod p$$

for $\ell = 0, 1, \ldots, p-1$. □

Example 2.3.12. We give an example of a permutation polynomial satisfying the conditions given in Theorem 2.3.11. Consider the polynomial $f(x) = x + 11x^2 + 7x^3 + 11x^{10} + 2x^{11} + 4x^{13} + 6x^{21}$. It can be seen easily that the coefficients of $f(x)$ satisfy (2.3) and (2.4). Moreover, the condition (2.5) amounts to

$$1 + 2.11\, l + 3.7\, l^2 + 10.11\, l^9 + 2.4\, l^{13} + 10.6\, l^{20} \not\equiv 0 \mod 11,$$

for $l = 0, 1, \ldots, 10$. This can be easily verified to be true, noting that $l^{10} \equiv 1 \mod 11$ for $1 \leq l \leq 10$. Hence, $f(x)$ is a permutation polynomial of $\mathbb{Z}_{11^n}$ for all $n \geq 1$.

Chapter 3

Permutation Polynomials over Finite Fields

3.1 Introduction

Let q be a prime power and let $\mathbb{F}_q$ denote the finite field of order q. We will denote an extension of $\mathbb{F}_q$ of degree m by $\mathbb{F}_{q^m}$. An element $\vartheta \in \mathbb{F}_{q^m}$ is said to be normal over $\mathbb{F}_q$ if the elements $\vartheta, \vartheta^q, \ldots, \vartheta^{q^{m-1}}$ form a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. In that case the set $\mathbb{B} = \{\vartheta, \vartheta^q, \ldots, \vartheta^{q^{m-1}}\}$ is called a normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Any element x of $\mathbb{F}_{q^m}$ can be expressed as $x = \sum_{i=0}^{m-1} x_i \vartheta^{q^i}$ where $x_i \in \mathbb{F}_q$. Thus $\mathbb{F}_{q^m}$ can be identified by $\mathbb{F}_q^m$, the set of all m-tuples over $\mathbb{F}_q$, and $x \in \mathbb{F}_{q^m}$ can be written as $(x_0, x_1, \ldots x_{m-1})$. If $q = 2$, then $x_i \in \{0, 1\}$ and in this case the weight of x is defined to be the number of 1's in $(x_0, x_1, \ldots, x_{m-1})$, and denote it by $w(x)$.

A polynomial $L(x) \in \mathbb{F}_{q^m}[x]$ is called a *linearized polynomial* or *p- polynomial* over $\mathbb{F}_q$ if

$$L(x) = \sum_{i=0}^{k} \alpha_i x^{q^i}. \tag{3.1}$$

See [50]. The linearized polynomial $L(x)$ satisfies the following: $L(\beta + \gamma) = L(\beta) + L(\gamma)$ and $L(a\beta) = aL(\beta)$ for all $\beta, \gamma \in \mathbb{F}_{q^m}$ and $a \in \mathbb{F}_q$. Thus, $L(x)$ is a linear operator of the vector space $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Consequently, $L(x)$ is a

permutation polynomial of $\mathbb{F}_{q^m}$ if and only if the only root of $L(x)$ in $\mathbb{F}_{q^m}$ is 0.

Corresponding to an element $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{m-1})$ of finite field $\mathbb{F}_{q^m}$, we define a polynomial function L_α on $\mathbb{F}_{q^m}$ as

$$L_\alpha(x) = \sum_{i=0}^{m-1} \alpha_i x^{q^i}. \tag{3.2}$$

Since each function on $\mathbb{F}_{q^m}$ is given by a unique polynomial of degree at most $q^m - 1$ and because the polynomial $L_\alpha(x)$ is of degree at most q^{m-1}, the distinct polynomials $L_\alpha(x)$ are all distinct as functions on $\mathbb{F}_{q^m}$. Note that $L_\alpha(x)$ are linearized or p-polynomials in finite fields $\mathbb{F}_{q^m}$.

"Convolution" operation is well known. In the next definition we define the convolution of finite fields elements which will be needed in the sequel.

Definition 3.1.1. Suppose $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{m-1})$ and $\beta = (\beta_0, \beta_1, \ldots, \beta_{m-1})$, $\alpha_i, \beta_i \in \mathbb{F}_q$, are two elements of finite fields $\mathbb{F}_{q^m}$. The *convolution* $\alpha * \beta$ of α and β is defined by

$$\alpha * \beta = (\gamma_0, \gamma_1, \ldots, \gamma_{m-1}), \quad \textit{where } \gamma_k = \sum_{i=0}^{m-1} \alpha_i \beta_{(k-i) \bmod m}. \tag{3.3}$$

Definition 3.1.2. A polynomial $f(x) \in \mathbb{F}_{q^m}[x]$ which is not linearized is called a nonlinear polynomial.

In Section 2 of this chapter we characterize a group of linearized permutation polynomials and give some classes of linearized permutation polynomials. In Section 3 we generate two classes of permutation polynomials, which are not linearized.

3.2 Some Classes of Linearized Permutation Polynomials of $\mathbb{F}_{q^m}$.

Let p be a prime and q is a power of p. To prove our results systematically first we need a lemma.

Lemma 3.2.1. *Suppose $L_\alpha \circ L_\beta$ denotes the composition of linearized polynomials $L_\alpha(x)$ and $L_\beta(x)$. Then $L_\alpha \circ L_\beta = L_{\alpha * \beta}$.*

Proof. For $\alpha = (\alpha_0, \ldots, \alpha_{m-1})$ and $\beta = (\beta_0, \ldots, \beta_{m-1})$, we have $L_\alpha(x) = \sum_{i=0}^{m-1} \alpha_i x^{q^i}$, and $L_\beta(x) = \sum_{j=0}^{m-1} \beta_j x^{q^j}$. Now we have

$$\begin{aligned} L_\alpha \circ L_\beta &= L_\alpha(L_\beta) \\ &= \sum_{i=0}^{m-1} \alpha_i \left(\sum_{j=0}^{m-1} \beta_j x^{q^j} \right)^{q^i} \\ &= \sum_{i=0}^{m-1} \alpha_i \left(\sum_{j=0}^{m-1} \beta_j x^{q^{i+j}} \right) \\ &= \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \alpha_i \beta_j x^{q^{i+j}} \end{aligned}$$

Suppose $i+j = k$, that is, $j = k-i$, we have $L_\alpha \circ L_\beta = \sum_{k=0}^{m-1} \left(\sum_{i=0}^{m-1} \alpha_i \beta_{k-i} \right) x^{q^k}$. Note that $x^{q^m} = x = x^{q^0}$, therefore the suffix $k-i$ will be under modulo m. Thus in view of equation (3.3), we have $L_\alpha \circ L_\beta = L_{\alpha * \beta}$. □

In view of above lemma we conclude that the linearized polynomials $L_\alpha(x)$ form a semigroup with identity. Let $\mathcal{L}(m)$ denote the group of all invertible linearized polynomials $L_\alpha(x)$ over $\mathbb{F}_{q^m}$. We will identify $\mathcal{L}(m)$ with an appropriate subgroup of the general linear group $GL(m, \mathbb{F}_q)$. Moreover we will characterize elements of $\mathcal{L}(m)$ for certain values of m and thereby show that the groups $\mathcal{L}(m)$ are quite large.

3.2.1 Characterization of the group $\mathcal{L}(m)$, for $m = p^k$.

A characterization of a linearized polynomial to be a permutation was given by Dickson [21], which is as follows:

Theorem 3.2.2. [21] *The linearized polynomial*

$$L(x) = \sum_{s=0}^{m-1} c_s x^{q^s} \in \mathbb{F}_{q^m}[x]$$

is a permutation polynomial of $\mathbb{F}_{q^m}$ *if and only if*

$$\begin{vmatrix} c_0 & c_{m-1}^{q} & c_{m-2}^{q^2} & \cdots & c_1^{q^{m-1}} \\ c_1 & c_0^{q} & c_{m-1}^{q^2} & \cdots & c_2^{q^{m-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{m-1} & c_{m-2}^{q} & c_{m-3}^{q^2} & \cdots & c_0^{q^{m-1}} \end{vmatrix} \neq 0. \tag{3.4}$$

An $m \times m$ matrix A over a field $\mathbb{F}$ is said to be *circulant* if it has the form

$$A = \begin{pmatrix} c_0 & c_{m-1} & c_{m-2} & \cdots & c_1 \\ c_1 & c_0 & c_{m-1} & \cdots & c_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{m-1} & c_{m-2} & c_{m-3} & \cdots & c_0 \end{pmatrix}. \tag{3.5}$$

Let e_k denote the k^{th} column of the identity matrix I and R be the matrix $(e_2, e_3, \ldots, e_m, e_1)$. Clearly, m is the least positive integer such that $R^m = I$. Let c denote the vector $(c_0, c_1, \ldots, c_{m-1})^T$ and A the circulant matrix as in equation (3.5). Then we have

$$A = (c, Rc, R^2c, \ldots, R^{m-1}c) \tag{3.6}$$

$$= c_0 I + c_1 R + c_2 R^2 +, \ldots, c_{m-1} R^{m-1}. \tag{3.7}$$

We will denote the circulant matrix A by $\mathrm{cir}(c_0, c_1, \ldots, c_{m-1})$. The product of any two circulant matrices $A = \mathrm{cir}(a_0, a_1, a_2, \ldots, a_{m-1})$ and $B = \mathrm{cir}(b_0, b_1, b_2, \ldots,$

b_{m-1}) is circulant and is given by

$$AB = \text{cir}(c_0, c_1, c_2, \ldots, c_{m-1}), \text{where } \; c_k = \sum_{i=0}^{m-1} a_i b_{(k-i)(\text{mod } m)}. \tag{3.8}$$

It is known that the inverse of a nonsingular circulant matrix is circulant (see [19]). Thus the nonsingular circulant matrices over a field $\mathbb{F}$ form a subgroup of the general linear group of $\mathbb{F}$. In view of equation (3.7), we note that this group is abelian. We denote this group by $\mathcal{C}(\mathbb{F}, m)$.

Lemma 3.2.3. *For $m \geq 1$, the groups $\mathcal{C}(\mathbb{F}_q, m)$ and $\mathcal{L}(m)$ are isomorphic.*

Proof. We define a mapping $\phi : \mathcal{L}(m) \to \mathcal{C}(\mathbb{F}_q, m)$ as follows: for $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{m-1})$

$$\phi(L_\alpha(x)) = \text{cir}(\alpha_0, \alpha_1, \ldots, \alpha_{m-1})$$

Since $\alpha_i \in \mathbb{F}_q$ in Theorem 3.2.2, the determinant in (3.4) is that of the circulant matrix $\text{cir}(\alpha_0, \alpha_1, \ldots, \alpha_{m-1})$. Thus L_α is invertible if and only if the circulant matrix $\text{cir}(\alpha_0, \alpha_1, \ldots, \alpha_{m-1})$ is nonsingular. In other words, ϕ is a bijection. It follows from Lemma 3.2.1 and equation (3.8) that ϕ is a group homomorphism. □

Proposition 3.2.4. *Let $\alpha = (\alpha_0, \ldots, \alpha_{m-1}) \in \mathbb{F}_{q^m}$. If the polynomial $L_\alpha(x)$ is a permutation of $\mathbb{F}_{q^m}$ then $\sum_{i=0}^{m-1} \alpha_i \neq 0$ in $\mathbb{F}_q$. The converse is also true if $m = p^k$ $(k \geq 1)$*

Proof. Let $L_\alpha = \sum_{i=0}^{m-1} \alpha_i x^{q^i}$. If $\sum_{i=0}^{m-1} \alpha_i = 0$, then $L_\alpha(x)$ has both 0 and 1 as roots, and therefore is not a permutation. Next suppose that $\sum_{i=0}^{m-1} \alpha_i \neq 0$ in $\mathbb{F}_q$. Then

$$\begin{aligned} \text{cir}(\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{m-1})^{p^k} &= (\alpha_0 I + \alpha_1 R + \alpha_2 R^2, \ldots + \alpha_{m-1} R^{m-1})^{p^k} \\ &= \alpha_0 I + \alpha_1 R^m + \alpha_2 (R^m)^2 + \ldots + \alpha_{m-1} (R^m)^{m-1} \\ &= \alpha_0 I + \alpha_1 I + \alpha_2 I + \ldots + \alpha_{m-1} I = \left(\sum_{i=0}^{m-1} \alpha_i \right) I. \end{aligned}$$

This implies that $\text{cir}(\alpha_0, \alpha_1, \ldots, \alpha_{m-1})$ is invertible and therefore in view of Lemma 3.2.3, $L_\alpha(x)$ is a permutation polynomial. □

In view of above proposition we immediately have the following corollaries:

Corollary 3.2.5. *If $m = p^k$, then $\#\mathcal{C}(\mathbb{F}_q, m) = \#\mathcal{L}(m) = q^m - q^{m-1}$, where $\#\mathcal{L}(m)$ denotes the cardinality of the group $\mathcal{L}(m)$.*

Corollary 3.2.6. *If $m = 2^k$ for some $k \geq 0$ and $\alpha = (\alpha_0, \ldots, \alpha_{m-1}) \in \mathbb{F}_{2^m}$. Then the polynomial $L_\alpha(x)$ is a permutation of $\mathbb{F}_{2^m}$ if and only if $w(\alpha)$ is odd.*

Corollary 3.2.7. *Let $\mathbb{F}_{q^m}$ is a finite field, with $m = q^k$, $k \geq 0$. Let $L_\alpha^j(x)$ denote the jth times composition of $L_\alpha(x)$ with itself. If $L_\alpha(x)$ is permutation polynomial of $\mathbb{F}_{q^m}$, then the inverse polynomial of $L_\alpha(x)$ is $L_\alpha^{q^k-1}(x)$.*

Proof. The result follows by noting that $(cir(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}))^{q^k} = I$. □

Corollary 3.2.8. *Let $\mathbb{F}_{q^m}$ is a finite field, with $m = q^k$, $k \geq 0$. Suppose we are taking normal basis representation of finite field elements with respect to normal basis $\mathbb{B} = \{\vartheta, \vartheta^q, \ldots, \vartheta^{q^{m-1}}\}$. Suppose $\alpha = (\alpha_0, \ldots, \alpha_{m-1}) \in \mathbb{F}_{q^m}$ such that $\sum_{i=0}^{m-1} \alpha_i \neq 0$ in $\mathbb{F}_q$. Then we have $L_\alpha^m(x) = L_\vartheta(x)$*

Proof. First note that $L_\vartheta = x$, since $\vartheta = (1, 0, 0, \ldots, 0)$. By Proposition 3.2.4, $L_\alpha(x)$ is permutation polynomial of $\mathbb{F}_{q^m}$ and from Proposition 3.2.4 and the Lemma 3.2.3, we have $L_\alpha^m(x) = x$, the identity of the group $\mathcal{L}(m)$. Thus the proof follows. □

Remark 3.2.9. We note that $\vartheta = (1, 0, 0, \ldots, 0)$ is the identity of convolution, that is, $\alpha * \vartheta = \alpha$, for all $\alpha \in \mathbb{F}_{2^m}$. Moreover, since $L_{(\alpha)^m}(x) = L_\alpha^m(x) = L_\vartheta(x)$, we have $(\alpha)^m = \vartheta$.

Lemma 3.2.3 implies, in particular, that the group $\mathcal{L}(m)$ is abelian. Since there are 2^{m-1} different α with odd weight, $\mathcal{L}(m)$ has order 2^{m-1} when $m = 2^k$. For $q = 2$, the converse of Proposition 3.2.4 is true and can be seen in the following Proposition.

Proposition 3.2.10. *Let the integer m be such that $L_\alpha(x), \alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{m-1})$, is a permutation polynomial over $\mathbb{F}_{2^m}$ whenever $w(\alpha)$ is odd. Then $m = 2^k$ for some $k \geq 0$.*

Proof. Since $L_\alpha(x)$ is not a permutation polynomial when $w(\alpha)$ is even, we have 2^{m-1} as the order of $\mathcal{L}(m)$ and therefore that of $\mathcal{C}(\mathbb{F}_2, m)$.
Now $R = (e_2, e_3, \ldots, e_m, e_1)$ is an element of $\mathcal{C}(\mathbb{F}_2, m)$ of order m. Thus m divides 2^{m-1} and has the required form. □
Here we give some examples of linearized permutation polynomials and their inverses. We list these examples in the table given below.

Field	α	$L_\alpha(x)$	$L_\alpha^{-1}(x)$
$\mathbb{F}_{2^4}$	$(1,1,1,0)$	$x + x^2 + x^4$	$x + x^4 + x^8$
$\mathbb{F}_{2^4}$	$(1,1,0,1)$	$x + x^2 + x^8$	$x + x^2 + x^8$
$\mathbb{F}_{2^4}$	$(0,1,1,1)$	$x^2 + x^4 + x^8$	$x^2 + x^4 + x^8$
$\mathbb{F}_{2^8}$	$(1,1,1,0,0,0,0,0)$	$x + x^2 + x^4$	$x^2 + x^4 + x^{16} + x^{32} + x^{128}$
$\mathbb{F}_{2^8}$	$(1,1,0,1,0,0,0,0)$	$x + x^2 + x^8$	$x + x^4 + x^{32} + x^{64} + x^{128}$
$\mathbb{F}_{2^8}$	$(1,1,1,1,1,0,0,0)$	$x + x^2 + x^4 + x^8 + x^{16}$	$x^2 + x^8 + x^{64}$

Table 3.1: Some Linearized Permutation Polynomials and their inverses.

Lemma 3.2.11. *If we take the normal basis representation of finite fields elements and let* $\alpha = (\alpha_0, \ldots, \alpha_{m-1})$, $\beta = (\beta_0, \ldots, \beta_{m-1}) \in \mathbb{F}_{q^m}$. *Then* $L_\alpha(\beta) = \left(cir(\alpha_0, \ldots, \alpha_{m-1})\beta^T\right)^T$.

Proof. Since we are taking the normal basis representation, therefore we have $\beta^q = (\beta_{m-1}, \beta_0, \ldots, \beta_{m-2})$, $\beta^{q^2} = (\beta_{m-2}, \beta_{m-1}, \beta_0, \ldots, \beta_{m-3})$ and so on. Thus we have

$$\begin{aligned} L_\alpha(\beta) &= \sum_{i=0}^{m-1} \alpha_i \beta^{q^i} \\ &= \alpha_0(\beta_0, \ldots, \beta_{m-1}) + \alpha_1(\beta_{m-1}, \beta_0, \ldots, \beta_{m-2}) + \ldots \\ &+ \alpha_{m-1}(\beta_1, \beta_2, \ldots, \beta_{m-1}\beta_0) \\ &= \left(cir(\alpha_0, \ldots, \alpha_{m-1})\beta^T\right)^T \quad \square \end{aligned}$$

Lemma 3.2.12. *Let $\alpha, \beta \in \mathbb{F}_{q^m}$. Then $L_\alpha(\beta) = L_\beta(\alpha)$.*

Proof. Let $\alpha = (\alpha_0, \ldots, \alpha_{m-1})$, $\beta = (\beta_0, \ldots, \beta_{m-1})$. Then

$$\begin{aligned} L_\alpha(\beta) &= \left(cir(\alpha_0, \ldots, \alpha_{m-1})\beta^T\right)^T \\ &= \left(cir(\beta_0, \ldots, \beta_{m-1})\alpha^T\right)^T \\ &= L_\beta(\alpha) \quad \square \end{aligned}$$

Proposition 3.2.13. *An element α of $\mathbb{F}_{q^m}$ is a normal element of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ if and only if $L_\alpha(x)$ is a permutation polynomial of $\mathbb{F}_{q^m}$.*

Proof. Suppose α is a normal element of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Let $y \in \mathbb{F}_{q^m}$. Then $y = \sum_{i=0}^{m-1} y_i \alpha^{q^i}$ for some $y_i \in \mathbb{F}_q$. If $z = \sum_{i=0}^{m-1} y_i \vartheta^{q^i}$, where $\mathbb{B} = \{\vartheta, \vartheta^q, \ldots, \vartheta^{q^{m-1}}\}$ is the fixed normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Then $y = L_z(\alpha) = L_\alpha(z)$. Thus L_α is surjective and therefore $L_\alpha(x)$ is permutation polynomial of $\mathbb{F}_{q^m}$. Conversely suppose that $L_\alpha(x)$ is permutation of $\mathbb{F}_{q^m}$. Then $L_\alpha(x) = L_x(\alpha) = y$ has a unique solution for all $y \in \mathbb{F}_{q^m}$. This implies that α is a normal element of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. $\square$

Thus we see that there is a one-one correspondence between normal elements of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and the linear permutation polynomials of the form $L_\alpha(x)$. Using the above proposition we can easily count the normal elements of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

Corollary 3.2.14. *Let $\mathbb{F}_{q^m}$ is a finite field, with $m = p^k$, $k \geq 0$. Then total number of normal elements of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ is $q^m - q^{m-1}$. In particular, when $q = 2$ and $m = 2^k$, the number of normal elements is 2^{m-1}.* $\square$

Lemma 3.2.15. *Suppose $L_\beta \in \mathfrak{L}(m)$. If α is a normal element of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, then so is $L_\beta(\alpha)$.*

Proof. The set $\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Since L_β is an invertible linear operator of $\mathbb{F}_{q^m}$, therefore the set $\{L_\beta(\alpha), L_\beta(\alpha^q), \ldots, L_\beta(\alpha^{q^{m-1}})\}$ is also a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. The proof is complete by noting the fact that $L_\beta(\alpha^{q^i}) = (L_\beta(\alpha))^{q^i}$.

In view of above Lemma and Proposition 3.2.13, we immediately have the following Proposition.

Proposition 3.2.16. *Suppose for $\alpha \in \mathbb{F}_{q^m}$, $L_\alpha(x)$ is permutation polynomial of $\mathbb{F}_{q^m}$ and $f \in \mathcal{L}(m)$ is any arbitrary element, then $L_{f(\alpha)}(x)$ is also a permutation polynomial of $\mathbb{F}_{q^m}$.*

3.2.2 Two more classes of linearized permutation polynomials

In this section we will give two more classes of linearized polynomials over finite field $\mathbb{F}_{q^m}$ for $q = 2, 3$. Two prove our results systematically first we give a definition from [50].

Definition 3.2.17. *For $\alpha \in \mathbb{F}_{q^m}$, the* trace *$Tr(\alpha)$ of α over $\mathbb{F}_q$ is defined as*

$$Tr(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{m-1}}$$

.

It is easy to see that $Tr(x)$ is a linear function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$, and also note that $Tr(\alpha^{q^i}) = Tr(\alpha)$ (see chapter 3 of [50]). The following Lemma will be used in the proof of Theorem 3.2.19.

Lemma 3.2.18. *If $L_\alpha(x) \in \mathcal{L}(m)$, then $Tr(L_\alpha(\beta)) = Tr(\beta)$ for all $\beta \in \mathbb{F}_{2^m}$.*

Proof. For $\beta \in \mathbb{F}_{2^m}$, $Tr(\beta) = \beta + \beta^2 + \ldots + \beta^{2^{m-1}}$. Suppose $\alpha = (\alpha_0, \ldots, \alpha_{m-1})$, where $\alpha_i \in \mathbb{F}_2$. Then $L_\alpha(\beta) = \sum_{i=0}^{m-1} \alpha_i \beta^{2^i}$. Now $Tr\left(L_\alpha(\beta)\right) = Tr\left(\sum_{i=0}^{m-1} \alpha_i \beta^{2^i}\right)$. Since $Tr(x)$ is a linear function, we have $Tr\left(L_\alpha(\beta)\right) = \sum_{i=0}^{m-1} \alpha_i Tr(\beta^{2^i})$. Since $Tr(\beta^{2^i}) = Tr(\beta)$, we have $Tr\left(L_\alpha(\beta)\right) = w(\alpha)Tr(\beta) = Tr(\beta)$, as $w(\alpha)$ is odd. □

Theorem 3.2.19. *If $L_\alpha(x)$ is a permutation polynomial of F_{2^m} and a is an element of $\mathbb{F}_{2^m}$, with $Tr(a) = 0$ then*

$$f(x) = L_\alpha(x) + aTr(x)$$

is a permutation polynomial of F_{2^m} .

Proof. Let β, γ be two distinct elements of $\mathbb{F}_{2^m}$ such that $f(\beta) = f(\gamma)$, since $L_\alpha(\beta) \neq L_\alpha(\gamma)$, we have $Tr(\beta) \neq Tr(\gamma)$. Without loss of generality assume that $Tr(\beta) = 0$ and $Tr(\gamma) = 1$. Then $f(\beta) = f(\gamma)$ implies that

$$L_\alpha(\beta) = L_\alpha(\gamma) + a$$

that is,

$$L_\alpha(\beta + \gamma) = a$$

By Lemma 3.2.18, this implies that

$$Tr(\beta + \gamma) = Tr(L_\alpha(\beta + \gamma)) = Tr(a) = 0$$

that is

$$Tr(\beta) = Tr(\gamma)$$

Which is a contradiction. Hence the result follows. □

Here we generate one example for the above class of linearized permutation polynomial.

Example 3.2.20. *The polynomial $x^4 + x + 1$ is irreducible over $\mathbb{F}_2$. Suppose β is a root of $x^4 + x + 1$ in the splitting field of $\mathbb{F}_2$. Then $\mathbb{F}_{2^4} = \{a + b\beta + c\beta^2 + d\beta^3 | a, b, c \in \mathbb{F}_2, \beta^4 + \beta + 1 = 0\}$ We take $a = \beta + \beta^2 \in \mathbb{F}_{2^4}$ as $Tr(\beta + \beta^2) = 0$ and $L_\alpha(x) = x + x^2 + x^4$. Then $x + x^2 + x^4 + (\beta + \beta^2)(x + x^2 + x^4 + x^8) = (1 + \beta + \beta^2)x + (1 + \beta + \beta^2)x^2 + (1 + \beta + \beta^2)x^4 + (\beta + \beta^2)x^8$ is a permutation polynomial of $\mathbb{F}_{2^4}$.*

Theorem 3.2.21. *Suppose $\mathbb{F}_{3^m}$ is a finite field and k is a positive integer such that $gcd(k, m) = 1$ and suppose $\alpha \in \{0, 1, 2\}$. Suppose k, α, and m are positive integers such that $k + \alpha m$ is not multiple of 3. Then*

$$f(x) = \sum_{i=0}^{k-1} x^{3^i} + \alpha Tr(x)$$

is permutation polynomial of F_{3^m}.

Proof. First note that $gcd(3^k - 1, 3^m - 1) = 3^{gcd(k,m)} - 1 = 2$. We have

$f(x)^3 - f(x) = x^{3^k} - x$. We note that, 0 and 1 are always roots of $f(x)^3 - f(x)$. Moreover, any root of $f(x)$ is a root of $f(x)^3 - f(x)$. If β is root of $f(x)^3 - f(x)$ other than 0 and 1, then we have $\beta^{3^k-1} = 1$. Suppose a denotes the order of β in $\mathbb{F}_{3^m}^*$, where $\mathbb{F}_{3^m}^*$ denotes the group of nonzero elements of finite field F_{3^m}. Then a divides $3^k - 1$ and also a divides $3^m - 1$, that is, a divides 2 or $a = 2$. This implies that $\beta = -1$. Thus 0, 1 and -1 are the only roots of $f(x)^3 - f(x)$. But 1 and -1 are not the roots of $f(x)$ since 3 does not divide $k + \alpha m$. Thus 0 is the only root of $f(x)$. Hence the result follows. □

3.3 Some Classes of Nonlinear Permutation Polynomials

Theorem 3.3.1. *Let m be an odd positive integer, and $\beta = (\beta_0, \ldots, \beta_{m-1})$ be an element of F_{2^m} such that $\omega(\beta)$ is even and that 0 and 1 are the only roots of $L_\beta(x)$ in $\mathbb{F}_{2^m}$. Suppose k_1 and k_2 are non negative integers such that $\gcd(2^{k_1} + 2^{k_2}, 2^m - 1) = 1$. Let ℓ be any positive integer with $(2^{k_1} + 2^{k_2}).\ell \equiv 1 \bmod 2^m - 1$ and γ be an element of $\mathbb{F}_{2^m}$ with $Tr(\gamma) = 1$. Then*

$$f(x) = (L_\beta(x) + \gamma)^\ell + Tr(x)$$

is a permutation polynomial of F_{2^m}.

Proof. First note that $Tr(L_\beta(x)) = 0$ and hence $Tr(L_\beta(x) + \gamma) = Tr(\gamma) = 1$. Thus $L_\beta(x) + \gamma \neq 0$ in $\mathbb{F}_{2^m}$.

Suppose, if possible, x and y are distinct elements of F_{2^m} such that $f(x) = f(y)$. First, suppose that $Tr(x) = Tr(y)$. Then $f(x) = f(y)$ gives

$$(L_\beta(x) + \gamma)^\ell = (L_\beta(y) + \gamma)^\ell.$$

Raising each of the two sides to the power $2^{k_1} + 2^{k_2}$, we get

$$L_\beta(x) + \gamma = L_\beta(y) + \gamma$$

that is $L_\beta(x+y)=0$. Since 0 and 1 are the only roots of $L_\beta(x)$, and because $x \neq y$,we get $x+y=1$. Then $Tr(x+y)=Tr(1)=1$, since m is odd. That is $Tr(x) \neq Tr(y)$, a contradiction.

Without loss of generality assume that $Tr(x)=0$ and $Tr(y)=1$. Then $f(x)=f(y)$ implies that

$$(L_\beta(x)+\gamma)^\ell = (L_\beta(y)+\gamma)^\ell + 1$$

and therefore

$$\begin{aligned} L_\beta(x)+\gamma &= [(L_\beta(y)+\gamma)^\ell+1]^{2^{k_1}+2^{k_2}} \\ &= \left((L_\beta(y)+\gamma)^{\ell.2^{k_1}}+1\right)\left((L_\beta(y)+\gamma)^{\ell.2^{k_2}}+1\right) \\ &= (L_\beta(y)+\gamma)^{\ell(2^{k_1}+2^{k_2})} + (L_\beta(y)+\gamma)^{\ell.2^{k_1}} + (L_\beta(y)+\gamma)^{\ell.2^{k_2}} + 1 \\ &= L_\beta(y)+\gamma+(L_\beta(y)+\gamma)^{\ell.2^{k_1}} + (L_\beta(y)+\gamma)^{\ell.2^{k_2}} + 1, \end{aligned}$$

since $(2^{k_1}+2^{k_2}).\ell \equiv 1 \bmod 2^m-1$. Further, $Tr(L_\beta(x))=0$ and $Tr\left((L_\beta(y)+\gamma)^{\ell.2^{k_1}}\right) = Tr\left((L_\beta(y)+\gamma)^{\ell.2^{k_2}}\right) = Tr\left((L_\beta(y)+\gamma)^{\ell}\right)$. Now applying the trace function to both sides of the above equation, we get

$$Tr(\gamma) = Tr(\gamma) + Tr(1),$$

which implies that $Tr(1)=0$, a contradiction since m is odd. □

Now we generate some examples for the above class of permutation polynomial.

Example 3.3.2. The polynomial x^2+x has only roots 0 and 1 in $\mathbb{F}_{2^m}$, so we are taking $L_\beta(x)=x^2+x$. We take $\gamma=1$, $m=3$, $k_2=0$, $k_1=1$, this gives $2^{k_1}+2^{k_2}=3$ and $\ell=5$. Thus $(x^2+x+1)^7+Tr(x)$ is a permutation polynomial of $\mathbb{F}_{2^3}$.

It is easy to see that 0 and 1 are the only roots of $x^{2^k}+x$ in $\mathbb{F}_{2^m}$ if and only if k and m are relatively prime. In the next lemma, we construct another linearized polynomial having only roots 0 and 1 in $\mathbb{F}_{2^m}$.

Lemma 3.3.3. *Let k be an even integer, with $\gcd(k, m) = 1$. Then, 0 and 1 are the only roots of $h(x) = \sum_{i=0}^{k-1} x^{2^i}$ in F_{2^m}.*

Proof. Consider $h_1(x) = h(x)^2 + h(x) = h(x)(h(x) + 1)$. Clearly, each root of $h(x)$ is a root of $h_1(x)$. Moreover, $h_1(x) = x^{2^k} + x$ and has 0 and 1 as its only roots. □

Example 3.3.4. We consider the field $\mathbb{F}_{2^3}$ and $k = 4$, then from above lemma $x + x^2 + x^4 + x^8$ has only roots $0, 1$ in the finite field $\mathbb{F}_{2^3}$. Now suppose $L_\beta(x) = x+x^2+x^4+x^8$. We take $k_2 = 0, k_1 = 2$, this gives $2^{k_1} + 2^{k_2} = 5$ and $\ell = 3, \gamma = 1$. Thus by Theorem 3.3.1, $(1 + x + x^2 + x^4 + x^8)^3 + Tr(x)$ is permutation of $\mathbb{F}_{2^3}$.

Lemma 3.3.5. *The polynomial $f(x) = x^{2^{k2^r}+2^r} + x^{2^{k2^r}} + x^{2^r}$, where r and k are positive integers, is a permutation polynomial of $\mathbb{F}_{2^m}$ if and only if $2^{k2^r} + 2^r$ and $2^m - 1$ are co-prime.*

Proof. First, note that there exist integers r and k such that $2^{2^r k}+2^r$ and 2^m-1 are co-prime. It is known that composition of two polynomials is a permutation polynomial if and only if both the polynomials are permutation polynomials (see chapter 7 of [50]). It is easy to check that $f(x + 1) = x^{2^{k2^r}+2^r} + 1$. By Theorem 1.2.2, $f(x + 1)$ is a permutation polynomial if and only if $2^{2^r k} + 2^r$ and $2^m - 1$ are co-prime. Since $x + 1$ is always a permutation of $\mathbb{F}_{2^m}$, therefore $f(x)$ is a permutation polynomial of $\mathbb{F}_{2^m}$ if and only if $2^{k2^r} + 2^r$ and $2^m - 1$ are co-prime.

As a consequence of above lemma we have the following result.

Theorem 3.3.6. *The polynomial $g(x) = (x^{2^{k2^r}} + x^{2^r} + \alpha)^l + x$ is permutation polynomial of $\mathbb{F}_{2^m}$ if $Tr(\alpha) = 1$ and $(2^{k2^r} + 2^r).l = 1 \ mod\ 2^m - 1$.*

Proof. Since $Tr(x^{2^{k2^r}} + x^{2^r} + \alpha) = Tr(\alpha) = 1$, $x^{2^{k2^r}} + x^{2^r} + \alpha \neq 0$ for all $x \in \mathbb{F}_{2^m}$. Let β be an element of $\mathbb{F}_{2^m}$. Then $g(x) = \beta$ implies

$$(x^{2^{k2^r}} + x^{2^r} + \alpha)^l = x + \beta.$$

Raising both sides to the power $2^{k2^r} + 2^r$, we get

$$(x^{2^{k2^r}} + x^{2^r} + \alpha) = (x + \beta)^{2^{k2^r}+2^r},$$

$$\text{i.e.,} \quad (x^{2^{k2^r}} + x^{2^r} + \alpha) + (x+\beta)^{2^{k2^r}+2^r} = 0.$$

Suppose $h(x) = (x^{2^{k2^r}} + x^{2^r} + \alpha) + (x+\beta)^{2^{k2^r}+2^r}$. It is enough to show that for any $\beta \in \mathbb{F}_{2^m}$ the equation $h(x) = 0$ has a unique solution. Note that $h(x) = 0$ and $h(x+\beta) = 0$ have the same number of solutions. Now $h(x+\beta) = 0$ is equivalent to

$$x^{2^{k2^r}+2^r} + x^{2^{k2^r}} + x^{2^r} + \beta^{2^{k2^r}} + \beta^{2^r} + \alpha = 0.$$

By Lemma 3.3.5, $x^{2^{k2^r}+2^r} + x^{2^{k2^r}} + x^{2^r}$ is a permutation polynomial of $\mathbb{F}_{2^m}$. Hence the equation $h(x+\beta) = 0$ has a unique solution for any $\beta \in \mathbb{F}_{2^m}$. □

Example 3.3.7. We consider the finite field $\mathbb{F}_{2^3}$. We take $r = 0, k = 2$, $\alpha = 1$, this gives $2^{k2^r} + 2^r = 5$ and $l = 3$. Then we have, $(x^{2^{k2^r}} + x^{2^r} + \alpha)^l + x = x^7 + x^5 + x^4 + x^3 + x + 1$. Thus the polynomial $x^7 + x^5 + x^4 + x^3 + x + 1$ is a permutation polynomial of $\mathbb{F}_{2^3}$.

Chapter 4

Public Key Cryptography Using Permutation p-Polynomials

4.1 Introduction

In this chapter we propose an efficient multivariate public key cryptosystem based on permutation p-polynomials over finite fields. We will use the group $\mathcal{L}(m)$ of permutation p-polynomials which we introduced in Chapter 3. We construct nonlinear trapdoor function based on the problem of solving nonlinear equations. The complexity of encryption in our public key cryptosystem is $O(m^3)$ multiplications which is equivalent to those of other multivariate public key cryptosystems. But the decryption in our proposed cryptosystem is much faster than in the other such existing cryptosystems. For decryption we need $O(m^2)$ left cyclic shifts and $O(m^2)$ xor operations. In Section 2, we present our public key cryptosystem and in Section 3 we give its security analysis. In Section 4 we discuss the efficiency of our public key cryptosystem and in Section 5 we compare our public key cryptosystem with HFE. Finally, in Section 6 we give a toy example of our cryptosystem.

4.2 Public key Cryptosystem

In this section we present our multivariate public key cryptosystem using some results from the previous chapter. Suppose $\mathbb{B} = \{\vartheta, \vartheta^q, \ldots, \vartheta^{q^{m-1}}\}$ is a normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Using the representation with respect to this basis, suppose $x = (x_0, x_1, \ldots x_{m-1}) \in \mathbb{F}_{q^m}$, where $x_i \in \mathbb{F}_q$. Then, the operation $x \mapsto x^q$ transforms x to $(x_{m-1}, x_0, \ldots, x_{m-2})$ which is just one left cyclic shift of $(x_0, x_1, \ldots, x_{m-1})$. Hence the cost of exponentiating by q is negligible. From now on we will take the normal basis representation of the elements of the finite field $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ with respect to the fixed normal basis $\mathbb{B}$. Though the cryptosystem we are proposing will work in any finite field $\mathbb{F}_{q^m}$, $m = p^k$, for practical point of view we consider $q = 2$ and $m = 2^k$. To obtain quadratic polynomials we use convolution of bits. We have seen in Chapter 3 that convolution of binary bits is equivalent to the composition of corresponding p-polynomials. Moreover, composition of two permutation p-polynomials is a permutation p-polynomial. For $x \in \mathbb{F}_{2^m}$ let $(x)^t$ denote the t times convolution of x with itself. From now on words we will denote the linearized polynomials $L_\alpha(x)$ by simply L_α. Let the set of all odd weight element of $\mathbb{F}_2^m$ be denoted by $O\mathbb{F}_2^m$. To describe our cryptosystem systematically, we need a few results which are discussed below.

Lemma 4.2.1. *For $\alpha = (\alpha_0, \ldots, \alpha_{m-1}) \in \mathbb{F}_{2^m}$, if $(\alpha)^2 = (\beta_0, \ldots, \beta_{m-1})$, then $\beta_{2i+1} = 0$ and $\beta_{2i} = \alpha_i + \alpha_{(m/2)+i}$, where $0 \le i \le (m-2)/2$.*

Proof. We have, $\beta_k = \sum_{i=0}^{m-1} \alpha_i.\alpha_{k-i}$, where the suffices will be modulo m. For $0 \le i \le (m-2)/2$, we have $\beta_{2i+1} = \alpha_0\alpha_{2i+1} + \alpha_1\alpha_{2i} + \ldots + \alpha_{2i+1}\alpha_0 + \alpha_{2i+2}\alpha_{m-1} + \ldots + \alpha_{m-1}\alpha_{2i+2}$. All the terms will be canceled out in pairs, so we have $\beta_{2i+1} = 0$. In a similar manner $\beta_{2i} = \alpha_0\alpha_{2i} + \alpha_1\alpha_{2i-1} + \ldots + \alpha_i\alpha_i + \ldots + \alpha_{2i}\alpha_0 + \alpha_{2i+1}\alpha_{m-1} + \ldots + \alpha_{m/2+i}\alpha_{m/2+i} + \ldots + \alpha_{m-1}\alpha_{2i+1} = \alpha_i^2 + \alpha_{(m/2)+i}^2 = \alpha_i + \alpha_{(m/2)+i}$, as $x_i^2 = x_i$ for $x_i \in \mathbb{F}_2$. □

Above lemma implies that $(x)^2$ is a linear function on the finite field $\mathbb{F}_{2^m}$. In general, it can be proved that $(x)^{2^k}$ is a linear function on $\mathbb{F}_{2^m}$.

Lemma 4.2.2. *Suppose $x = (x_0, x_1, \ldots, x_{m-1})$ is an element of $\mathbb{F}_2^m$. If $(x)^t = (h_0, h_1, \ldots, h_{m-1})$, then each h_i is a nonlinear function of x_i of degree $w(t)$, where $w(t)$ denotes the weight of t.*

Proof: Suppose $G = (g_0, g_1, \ldots, g_{m-1})$, where each g_i is a linear polynomial in variables x_i and suppose $(G)^{2^l} = (g_0^{'}, g_1^{'}, \ldots, g_{m-1}^{'})$ and $(G)^{2^{l+2^k}} = (g_0^{''}, g_1^{''}, \ldots, g_{m-1}^{''})$, where $k > l \geq 1$. Then by lemma 4.2.1, degrees of $g_i^{'}$ and $g_i^{''}$ are 1 and 2, respectively. This proves the lemma. □

Lemma 4.2.3. *The function defined by $h(x) = (x)^t$, where t is co-prime to m, is a bijection from $O\mathbb{F}_2^m$ onto $O\mathbb{F}_2^m$.*

Proof. Since $(x)^t$ is of odd weight whenever x is so, $h(x)$ is a function from $O\mathbb{F}_2^m$ into $O\mathbb{F}_2^m$. Now, since t and m are co-prime, there exist positive integers r and k such that $tk = 1 + rm$. Let $y \in O\mathbb{F}_2^m$. Consider $x = (y)^k$. Then $x \in O\mathbb{F}_2^m$. Moreover,

$$L_{(x)^t} = L_{(y)^{kt}} = L_{(y)}^{kt} = L_{(y)}^{1+rm} = L_y,$$

Since by the Lemma 3.2.1, we have $L_{(y)^{kt}} = L_{(y)}^{kt}$ and from the Corollary 3.2.8, $L_y^m = L_\vartheta$. This implies that $h(x) = (x)^t = y$. Thus, $h(x)$ is surjective, and the result follows. □

Lemma 4.2.4. *Convolution is distributive over addition in finite fields, that is, $\alpha * (\beta + \gamma) = \alpha * \beta + \alpha * \gamma$, for all $\alpha, \beta, \gamma \in \mathbb{F}_{2^m}$.*

Proof. Suppose $\alpha = (\alpha_0, \ldots, \alpha_{m-1})$, $\beta = (\beta_0, \ldots, \beta_{m-1})$ and $\gamma = (\gamma_0, \ldots, \gamma_{m-1})$. Then, $\beta + \gamma = (\beta_0 + \gamma_0, \ldots, \beta_{m-1} + \gamma_{m-1})$. Now, we have

$$\alpha * (\beta + \gamma) = \sum_{i=0}^{m-1} \alpha_i \left(\beta_{(k-i) \bmod m} + \gamma_{(k-i) \bmod m}\right),$$

or equivalently we can write

$$\alpha * (\beta + \gamma) = \sum_{i=0}^{m-1} \left(\alpha_i \beta_{(k-i) \bmod m} + \alpha_i \gamma_{(k-i) \bmod m}\right),$$

that is,

$$\alpha * (\beta + \gamma) = \alpha * \beta + \alpha * \gamma.$$

□

Lemma 4.2.5. *If $m = 2^k, k \geq 1$ and $\alpha, \beta \in O\mathbb{F}_2^m$, then $\alpha * \beta \in O\mathbb{F}_2^m$, that is, if the bit size is a power of 2 then the convolution of two odd weight binary strings is an odd weight binary string.*

Proof. By Corollary 3.2.6, the linearized polynomials L_α and L_β are permutation of $\mathbb{F}_{2^m}$. Since the composition of two permutation polynomials is a permutation polynomial, therefore $L_\alpha \circ L_\beta$ is a permutation of $\mathbb{F}_{2^m}$. But by Lemma 3.2.1, $L_\alpha \circ L_\beta = L_{\alpha * \beta}$, therefore $L_{\alpha*\beta}$ is a permutation of $\mathbb{F}_{2^m}$. Now the result follows by Corollary 3.2.6.

4.2.1 Public key generation

Consider a message of $m-1$ bit string $(x_0, x_1, \ldots, x_{m-2})$, where m is of the form 2^k. We are adjoining one more bit x_{m-1} to make the weight odd. After decryption one needs to remove the last bit x_{m-1}. So we can assume that message $X = (x_0, x_1, \ldots, x_{m-1})$ is an m bit odd weight element of the finite field $\mathbb{F}_{2^m}$. Suppose $L_\alpha, L_\beta, L_\gamma, L_\delta, L_\eta$ are elements of the group $\mathfrak{L}(m)$ and L_ξ, L_ζ are elements of the group $\mathfrak{L}(2m)$. Let π_1,π_2, π_3, π_4, π_5 are random permutations of $\{0, 1, 2, \ldots, m-1\}$ and π_6, π_7 are random permutations of $\{0, 1, 2, \ldots, 2m-1\}$. Now compute $T_1^{'} = L_\alpha \circ \pi_1$, $T_2^{'} = L_\beta \circ \pi_2$, $T_3^{'} = L_\gamma \circ \pi_3$, $T_4^{'} = L_\delta \circ \pi_4$, $T_5^{'} = L_\eta \circ \pi_5$ and $T_6^{'} = L_\xi \circ \pi_6$, $T_7^{'} = L_\zeta \circ \pi_7$, where $\circ$ denotes the composition of mappings. Now, define the affine transformation $T_r(X) = T_r^{'}(X) + \sigma_r$ for $1 \leq r \leq 7$, where σ_r for $1 \leq r \leq 5$ is an even weight element of $\mathbb{F}_{2^m}$ and σ_6, σ_7 are even weight element of $\mathbb{F}_{2^{2m}}$. We note that if X is an odd weight element of $\mathbb{F}_{2^m}$, then $T_r^{'}(X)$ and $T_r(X)$ are odd weight element of $\mathbb{F}_{2^m}$. Thus, $T_r(X)$ is a bijection of $O\mathbb{F}_{2^m}$. Next, compute $X^{'} = T_1(X)$, $X^{''} = T_2(X)$. Again, compute $T_3\left((X^{'})^2 * X^{''}\right)$ and $T_4\left(X^{'} * X^{''}\right) + T_5\left((X^{'})^2 * X^{''}\right)$. Suppose the quadratic polynomials f_i and f_{m+i} denote the i^{th} bits of $T_3\left((X^{'})^2 * X^{''}\right)$ and $T_4\left(X^{'} * X^{''}\right) + T_5\left((X^{'})^2 * X^{''}\right)$, respectively, in their normal basis representations. Suppose $\vartheta^{'}$ is the normal element of $\mathbb{F}_{2^{2m}}$ and $\mathbb{B}^{'}$ denotes the normal basis of $\mathbb{F}_{2^{2m}}$ over $\mathbb{F}_2$ corresponding to $\vartheta^{'}$. Now, consider the $2m$ bits $(f_0, f_1, \ldots, f_{2m-1})$ as an element of $\mathbb{F}_{2^{2m}}$ corresponding to the basis $\mathbb{B}^{'}$. Suppose $Y = (y_0, y_1, \ldots, y_{2m-1},)$ is the ciphertext which is to be computed using the algorithm described in the sequel. Let $Z = T_6(Y)$ and suppose λ and σ are elements of $\mathbb{F}_{2^{2m}}$ of even and odd weights,

respectively. Then, by Lemma 4.2.3 the function $\lambda + \sigma * (Z)^{2m-1}$ is a bijection of $O\mathbb{F}_{2^{2m}}$. The relation between the plaintext and the ciphertext is:

$$T_7\left(f_0, f_1, \ldots, f_{2m-1}\right) = \lambda + \sigma * (Z)^{2m-1} \tag{4.1}$$

We note that the ciphertext Y is an odd weight element of $\mathbb{F}_{2^{2m}}$. It follows from Remark 3.2.9 that $(Z)^{2m} = \vartheta'$, the identity of convolution. Taking convolution with Z of each of the two sides of (4.1) and using Lemma 4.2.4, we have the following relation between the plaintext and the ciphertext:

$$T_7\left(f_0, f_1, \ldots, f_{2m-1}\right) * Z + \lambda * Z + \sigma = 0 \tag{4.2}$$

Equation (4.2) gives the $2m$ polynomial equations of total degree 3 in variables $x_0, x_1, \ldots, x_{m-1}$; $y_0, y_1, \ldots, y_{2m-1}$, but of degree 1 in variables y_i. Thus, we get $2m$ equations of the form

$$\sum a_{ijk}x_i x_j y_k + \sum b_{ij}x_i y_j + \sum c_{ij}x_i x_j + \sum d_k y_k + \sum e_k x_k + f_l = 0. \tag{4.3}$$

The terms $a_{ijkl}x_i x_j y_k$, $b_{ijl}x_i y_j$ and $d_k y_k$ will always have nonzero coefficients in the above equation. Each of the equations is of degree three with $O(m^3)$ terms. Since we have $2m$ equations, number of terms in the system will be of $O(m^4)$, which is large. However, it is possible to reduce the number of terms in the polynomial equations (4.3) up to $O(m^3)$ by writing it as a two sets of public polynomials containing only quadratic terms without changing the security, since this can be done in polynomial time (see [64]). Thus, the public key will be two sets of $2m$ quadratic equations of the form:

$$\sum g_k y_k + \sum b_{ij}x_i y_j + \sum d_k y_k + \sum e_k x_k + f_l = 0$$

where

$$g_k = \sum h_{ijk}x_i x_j.$$

The results in Section 3.2 are true for any arbitrary prime power q. Therefore, the public key size can be further reduced by taking m not too large (for example

$m = 32$) and q not too small.

4.2.2 Secret key

The linear transformations $(T_1, T_2, T_3, T_4, T_5, T_6, T_7)$ and finite fields elements (λ, σ) are the required secret keys.

4.2.3 Encryption

For encrypting a plaintext $M = (x_0, x_1, \ldots, x_{m-1})$, one substitutes the plaintext vector in the public key and solves the resulting linear equations for the ciphertext $Y = (y_0, y_1, \ldots, y_{2m-1})$. One will get a unique ciphertext because our encryption function is injective. Given a ciphertext Y, the public equations are nonlinear in x_i. It follows from equation (4.1) that the encryption function is given by

$$E(X) = Y = T_6^{-1}\left(\left((F(X) + \lambda) * (\sigma)^{2m-1}\right)^{2m-1}\right),$$

where $F(X) = T_7(f_0, f_1, \ldots, f_{2m-1})$.

Theorem 4.2.6. *The encryption function E is well defined and bijective from $O\mathbb{F}_{2^m}$ to $E(O\mathbb{F}_{2^m})$, where $E(O\mathbb{F}_{2^m})$ denotes the range of E in $O\mathbb{F}_{2^{2m}}$.*

Proof. Suppose $X_1, X_2 \in O\mathbb{F}_{2^m}$. It is easy to verify that $X_1 = X_2$ implies $E(X_1) = E(X_2)$. Now, we assume that $E(X_1) = E(X_2)$, that is,

$$T_6^{-1}\left(\left((F(X_1) + \lambda) * (\sigma)^{2m-1}\right)^{2m-1}\right) = T_6^{-1}\left(\left((F(X_2) + \lambda) * (\sigma)^{2m-1}\right)^{2m-1}\right).$$

Therefore

$$\left((F(X_1) + \lambda) * (\sigma)^{2m-1}\right)^{2m-1} = \left((F(X_2) + \lambda) * (\sigma)^{2m-1}\right)^{2m-1}.$$

Since $(F(X_1) + \lambda) * (\sigma)^{2m-1}$ and $(F(X_2) + \lambda) * (\sigma)^{2m-1}$ are elements of $O\mathbb{F}_{2^{2m}}$,

so by Lemma 4.2.3 we have

$$(F(X_1) + \lambda) * (\sigma)^{2m-1} = (F(X_2) + \lambda) * (\sigma)^{2m-1}.$$

Now, taking the convolution of both sides with σ and noting that $(\sigma)^{2m} = \vartheta'$ we have $F(X_1) = F(X_2)$, which implies

$$T_3\left((X_1^{'})^2 * X_1^{''}\right) = T_3\left((X_1^{'})^2 * X_1^{''}\right),$$

and

$$T_4\left(X_1^{'} * X_1^{''}\right) + T_5\left((X_1^{'})^2 * X_1^{''}\right) = T_4\left(X_2^{'} * X_2^{''}\right) + T_5\left((X_2^{'})^2 * X_2^{''}\right).$$

From the above two relations, we have

$$(X_1^{'})^2 * X_1^{''} = (X_2^{'})^2 * X_2^{''} \quad \text{and} \quad X_1^{'} * X_1^{''} = X_2^{'} * X_2^{''},$$

that is,

$$X_1 * X_2^{'} * X_2^{''} = (X_2^{'})^2 * X_2^{''}.$$

This implies $X_1 = X_2$. □

4.2.4 Decryption

The decryption algorithm for the cryptosystem is as follows.

Input: Ciphertext $Y = (y_0, \ldots, y_{m-1})$ and secret parameters $(T_1, T_2, T_3, T_4, T_5, T_6, T_7, \lambda, \sigma)$ and an element of $\alpha \in F_{2^{2m}}$ such that $w(\alpha)$ is odd.

Output: Message X

1: $Z \leftarrow T_6(Y)$.
2: $(Z)^{2m-1} \leftarrow L_\alpha^{-1}\left(L_Z^{2m-1}(\alpha)\right)$.
3: $Z^{'} \leftarrow \lambda + \sigma * (Z)^{2m-1}$.
4: $\triangle \leftarrow T_7^{-1}(Z^{'})$.
5: $(\delta_0, \ldots, \delta_{2m-1}) \leftarrow \triangle$.
6: $\triangle_1 \leftarrow (\delta_0, \ldots, \delta_{m-1})$ and $\triangle_2 \leftarrow (\delta_m, \ldots, \delta_{2m-1})$.

7: $\triangle_3 \leftarrow T_3^{-1}(\triangle_1)$ and $\triangle_4 \leftarrow T_5(\triangle_3)$.
8: $\triangle_5 \leftarrow \triangle_2 + \triangle_4$.
9: $\triangle_6 \leftarrow T_4^{-1}(\triangle_5)$.
10: $\triangle_7 \leftarrow L_{\triangle_6}(\alpha)$.
11: $\triangle_8 \leftarrow L_{\triangle_3}(\alpha)$.
12: $\triangle_9 \leftarrow L_{\triangle_7}^{m-1}(\triangle_8)$.
13: $X \leftarrow T_1^{-1}(\triangle_9)$.
14: Return X.

We now prove that the above algorithm gives valid plaintext X as the output for a ciphertext Y.

Theorem 4.2.7. *Given ciphertext Y, the output X given by the decryption algorithm is a valid plaintext.*

Proof. Using the Lemma 3.2.1 and 3.2.12, first note that

$$\begin{aligned} L_\alpha^{-1}\left(L_Z^{2m-1}(\alpha)\right) &= L_\alpha^{-1}\left(L_{(Z)^{2m-1}}(\alpha)\right) \\ &= L_\alpha^{-1}\left(L_\alpha\left((Z)^{2m-1}\right)\right) \\ &= (Z^{2m-1}) \end{aligned}$$

where $Z = T_6(Y)$. Now suppose $Z' = \lambda + \sigma * (Z)^{2m-1}$. Now from relation 4.1, we have

$$T_7(f_0, \ldots, f_{2m-1}) = \lambda + \sigma * (Z)^{2m-1} = Z'.$$

that is,

$$(f_0, \ldots, f_{2m-1}) = T_7^{-1}(Z') = \triangle = (\delta_0, \ldots, \delta_{2m-1}).$$

This implies,

$$(f_0, \ldots, f_{m-1}) = (\delta_0, \ldots, \delta_{m-1}) \quad \text{and} \quad (f_m, \ldots, f_{2m-1}) = (\delta_m, \ldots, \delta_{2m-1})$$

that is, we have,

$$T_3\left((X')^2 * X''\right) = \triangle_1 \tag{4.4}$$

and

$$T_4\left(X' * X''\right) + T_5\left((X')^2 * X''\right) = \triangle_2 \tag{4.5}$$

From relation (4.4), we have

$$(X^{'})^2 * X^{''} = T_3^{-1}(\triangle 1) = \triangle_3 \tag{4.6}$$

and

$$T_5\left((X^{'})^2 * X^{''}\right) = T_5(\triangle_3) = \triangle_4 \tag{4.7}$$

Adding relation (4.5) and (4.7), we get $T_4(X^{'} * X^{''}) = \triangle_2 + \triangle_4 = \triangle_5$ or equivalently, we have

$$X^{'} * X^{''} = T_4^{-1}(\triangle_2 + \triangle_4) = \triangle_6. \tag{4.8}$$

Suppose α is an odd weight element of $\mathbb{F}_{2^m}$. Now from relation (4.8) and (4.6), we have $L_{X^{'}*X^{''}}(\alpha) = L_{\triangle}(\alpha) = \triangle_7$ and $L_{(X^{'})^2*X^{''}}(\alpha) = L_{\triangle_3}(\alpha) = \triangle_8$. Now from the Lemma 3.2.1, we have $L_{(X^{'})^2*X^{''}}(\alpha) = L_{X^{'}}\left(L_{X^{'}*X^{''}}(\alpha)\right)$. Thus we have $L_{X^{'}}(\triangle_7) = \triangle_8$. Since by the Lemma 3.2.12, $L_{X^{'}}(\triangle_7) = L_{\triangle_7}\left(X^{'}\right)$, therefore we have $X^{'} = L_{\triangle_7}^{-1}(\triangle_8)$. Since by Corollary 3.2.7, we know that $L_{\triangle_7}^{-1} = L_{\triangle_7}^{m-1}$, therefore we have $X^{'} = L_{\triangle_7}^{m-1}(\triangle_8) = \triangle_9$. Thus we have $X = T_1^{-1}(\triangle_9)$. □

4.3 Security of the proposed cryptosystem

In this section we discuss the security of the proposed cryptosystem. In general it is very difficult to prove the security of a public key cryptosystem [57], [73]. For example if the public modulus of RSA is decomposed into its prime factors then RSA is broken. However, it is not proved that breaking RSA is equivalent to factoring its modulus, see [36]. In this section we will give some security arguments and evidence that our cryptosystem is secure. Most of the multivariate public key cryptosystems use the structure $t(f(s(x)))$, where t and s are secret invertible linear transformation and $f(x)$ is a quadratic nonlinear function. Hiding $f(x)$ by two linear transformations does not work very effectively (see the attack of Kipnis and Shamir on HFE [42]). We are using a different structure and we will prove that our structure is at least as secure as the $t(f(s(x)))$ structure. In our cryptosystem the function $f(x)$ is $(x*x*x, x*x+x*x*x)$ so $t(f(s(x))) = t\left(s(x)*s(x)*s(x),\ s(x)*s(x)+s(x)*s(x)*s(x)\right)$. We take the simpler case,

suppose we are not using the transformations T_3, T_4 and T_5. Then, our structure is $T_7\left(T_1(x) * T_1(x) * T_2(x),\ T_1(x) * T_2(x) + T_1(x) * T_1(x) * T_2(x)\right)$. It is clear that if $T_1 = T_2$, then our structure is equivalent to $t(f(s(x)))$ structure. Thus, if it is possible to attack our structure, then it is also possible to attack $t(f(s(x)))$ structure. This proves that our structure is at least as secure as the commonly used structures $t(f(s(x)))$ in multivariate cryptography. Moreover, our quadratic part of the plaintext is hidden, because in this case the public polynomials are the m bit representation of $F(X) * Z + \lambda * Z + \sigma$, where $F(X) = T_7(f_0, f_1, \ldots, f_{2m-1})$ and $Z = T_6(Y)$. From $F(X) * Z + \lambda * Z + \sigma$ it is not possible to compute either $F(X)$, Z, λ or σ, because $F(X) * Z$ is equivalent to the composition of corresponding p-polynomials and in general it is very difficult to decompose the composition of two functions. We are using affine transformations, so the bitwise representation of $F(X) * Z$ will also give the terms of the form $d_k y_k + c_k$. So it is not possible to find λ and σ from the public key. In the rest of this section, we discuss some known attacks developed for multivariate cryptosystems and we will show that those attacks are not applicable to our cryptosystem. The attacks discussed in this section are Gröbner basis, univariate polynomial representation, Linearization, Relinearization, XL and FXL algorithms.

4.3.1 Linearization equation attacks.

Let $F = \{f_0, f_1, \ldots, f_{m-1}\}$ be any set of m polynomials in $\mathbb{F}_q[x_0, x_1, \ldots, x_{m-1}]$. A linearization equation for F is any polynomial in $\mathbb{F}_q[x_0, x_1, \ldots, x_{m-1}, y_0, y_1, \ldots, y_{m-1}]$ of the form

$$\sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_{ijl}x_i y_j + \sum_{i=0}^{m-1} b_{il}x_i + \sum_{j=0}^{m-1} c_{jl}y_j + d_l \tag{4.9}$$

where $l = 0, 1, \ldots, m-1$, where $y_j = f_j$.

Linear equation attack was first successfully applied by Patarin in [63] to break the cryptosystem MIC* [55]. The idea of Patarin was to notice that if a function is defined as $F : x \rightarrow x^{q^i+1}$, then a relation between the plaintext $(x_0, x_1, \ldots, x_{m-1})$ and the ciphertext $(y_0, y_1, \ldots, y_{m-1})$ of the form shown in

equations (4.9) can be established, where a_{ij}, b_i, c_j and d_l are unknown coefficients. By taking at least $(m+1)^2$ different plaintext-ciphertext pairs a linear system of equations can be established and solved.

Ou cryptosystem does not use any function of the form x^{q^i+1}. Moreover, here the plaintext and the ciphertext are connected by the relation (4.1), and T_6, λ and σ are secrets. So, in this case it is not possible to obtain a relation of the form (4.9). One may try to find a relation which is linear in x_i and nonlinear in y_j. However, this line of attack is not possible as the degree of the inverse function is very high. From the relation (4.1) we have $(f_0, f_1, \ldots, f_{2m-1}) = T_7^{-1}(Z')$. Note that $Z' = \lambda + \sigma * (Z)^{2m-1}$ and $Z = T_6(Y)$ so $T_7^{-1}(Z')$ will give nonlinear polynomials of degree $w(2m-1)$ in the ciphertext variables. Suppose $T_7^{-1}(Z') = (Z_0, Z_1, \ldots, Z_{2m-1})$. Then we have the following relations between the plaintext and the ciphertext

$$T_3\left(X' * X' * X''\right) = (Z_0, Z_1, \ldots, Z_{m-1})$$

and

$$T_4\left(X' * X''\right) + T_5\left(X' * X' * X''\right) = (Z_m, Z_{m+1}, \ldots, Z_{2m-1}).$$

Using these two relations one can get the following relation between the plaintext and the ciphertext:

$$X' * T_4^{-1} \circ T_5\left(Z'\right) + T_4^{-1}(Z_m, Z_{m+1}, \ldots, Z_{2m-1}) = Z'', \tag{4.10}$$

where $X' = T_1(X)$, $Z'' = T_3^{-1}(Z_0, Z-1, \ldots, Z_{m-1})$ and $T_1, T_2, T_3, T_4, T_5, T_6$ are unknown linear transformations. Note that the relation (4.10) is of total degree $w(2m-1)+1$; of degree $w(2m-1)$ degree in the ciphertext variables and of degree one degree in the plaintext variable. Most crucially, the degree of relation (4.10) is not constant but a function of m. Thus, to attack the cryptosystem one will need Gaussisn reduction on $O(m^{w(2m-1)+1})$ terms, which is impractical for the bit size 64 or more, because for $m = 64$, $w(2m-1)+1 = 8$.

4.3.2 Attacks with Differential Cryptanalysis

Differential cryptanalysis has been successfully used earlier to attack the symmetric cryptosystem. In recent years differential cryptanalysis has emerged as a powerful tool to attack the multivariate public key cryptosystems too. In 2005 [32] Fouque, Granboulan and Sterm used differential cryptanalysis to attack the multivariate cryptosystems. The key point of this attack is that in case of quadratic polynomials the differential of public key is a linear map and its kernel or its rank can be analyzed to get some information on the secret key. For any multivariate quadratic function $G : \mathbb{F}_q^n \to \mathbb{F}_q^m$ the differential operator between any two points $x, k \in \mathbb{F}_q^n$ can be expressed as $L_{G,k}G(x+k)-G(x)-G(k)+G(0)$ and in fact that operator is a bilinear function. By knowing the public key of a given multivariate quadratic scheme and by knowing the information about the nonlinear part (x^{q^i+1}) they showed that for certain parameters it is possible to recover the kernel of $L_{G,k}$. This attack was successfully applied on Ding's cryptosystem [25] and afterwards using the same technique Dubois, Fouque, Shamir and Sterm in 2007 [28] have completely broken all versions of the SFLASH signature scheme proposed by Patarin, Courtois, and Goubin [66]. In our cryptosystem we are not using any polynomial of the form x^{q^i+1}. Moreover the public key in our system is not quadratic but of total degree 3, quadratic in plaintext variables and degree one in ciphertext variables. Substituting the ciphertext gives quadratic plaintext variables but in that case it will be different for different ciphertexts. So to attack our cryptosystem by the methods of [32] and [28] is not feasible.

4.3.3 Attacks using the univariate polynomial representation of multivariate public polynomials

The fact that any function from a finite field into itself can be represented by a univariate polynomial is sometime used to attack multivariate cryptosystem (see [26] for example). In our case, the encryption function is from the finite field $\mathbb{F}_{2^m}$ to the finite field $\mathbb{F}_{2^{2m}}$, and therefore we cannot represent the encryption function by a polynomial directly. It is possible to have such a representation by introducing dummy variables $x_m, x_{m+1}, \ldots, x_{2m}$. In our cryptosystem the

relation between the plaintext and ciphertext is $F(X) = \lambda + \sigma * (Z)^{2m-1}$, where $F(X) = T_7(f_0, f_1, \ldots, f_{2m-1})$. Suppose $G(X) = ((F(X) + \lambda) * \sigma^{2m-1})^{2m-1}$. Then, we have $Y = T_6^{-1}(G(X))$. Note that $F(X)$ is nonlinear of degree 2, so that $T_6^{-1}(G(X))$ will give $2m$ multivariate polynomials of degree $2.w(2m-1)$. By Lemma 3.3 of [42], the degree of the univariate polynomial representation is not constant but it is function of m. Thus, the degree and the number of nonzero terms of the univariate polynomial representation of encryption function are both $O(m^m)$. The complexity of root finding algorithms, Berlekamp algorithm for example, is polynomial in the degree of the polynomial. This results in an exponential time algorithm to find the roots of univariate polynomial. Therefore, this approach is less efficient than the exhaustive search.

4.3.4 Gröbner basis attacks

After substituting the ciphertext in the public key, one can get $2m$ quadratic equations in m variables and then Gröbner basis techniques can be applied to solve the system. The classical algorithms for solving systems of multivariate equations is Buchberger's algorithm for constructing Gröbner basis (see [17]). Theoretically, it can solve all the multivariate quadratic equations. However, its complexity is exponential in the number of variables, although there is no closed-form formula for it. In the worst case the Buchberger's algorithm is known to run in double exponential time and on average its running time seems to be single exponential (see [14]). There are some efficient variants F_4 and F_5 of Buchberger's algorithm given by Jean-Charles Faugere (see [29] and [30]). The complexity of computing a Gröbner basis for the public polynomials of the basic HFE scheme is not feasible using Buchberger's algorithm. However, it is completely feasible using the algorithm F_5. The complexities of solving the public polynomials of several instances of the HFE using the algorithm F_5 are provided in [31]. Moreover, it has been expressed in [31], "A crucial point in the cryptanalysis of HFE is the ability to distinguish a randomly algebraic system from an algebraic system coming from HFE". Instead of using any polynomial of special form we are using convolution operation to construct the public polynomials. Moreover our public key is of mixed type, this means, for different ciphertexts we will get different system of quadratic polynomial

equations, so in our public key the quadratic polynomials look random. We have already seen that the degree of the univariate polynomial representation of the encryption function is proportional to m. It is explained in [31] that in this case there does not seem to exist polynomial time algorithm to compute the Gröbner basis. Hence, attack on our cryptosystem by Gröbner basis method is not feasible.

4.3.5 Relinearization, XL and FXL Algorithms

Relinearization, XL or FXL algorithm are some techniques to solve the quadratic equations directly. The relinearization technique is developed in [42] for solving an overdefined system of quadratic equations. However, it is shown in [14] that the Relinearization technique is not as efficient as one may expect since many of newly generated equations are dependent. Therefore, a technique called XL (extended relinearization) has been proposed in [14]. It is claimed to be the best algorithm for solving overdefined multivariate equations. However, when the number of equations is $m + r$ for some $1 \leq r \leq m$, then it is proved in [14] that XL has exponential complexity. A variant of the XL algorithm called FXL, was introduced in [14]. In this algorithm some variables are guessed to make the system slightly overdefined. Then the XL algorithm is applied. The main question is how many variables must be guessed. Although more guesses make the system more unbalanced, they add to the complexity of the algorithm. The optimum number of guesses is provided in [14].

One will find it difficult to attack our cryptosystem by solving the quadratic equations directly with the help of the above techniques, because our public key is of mixed type, which means that for different ciphertexts one will have to solve different systems of quadratic nonlinear equations.

In case of applying XL, $r = m$ for our cryptosystem. Hence, XL algorithm cannot be used directly to attack our cryptosystem, since it has exponential complexity.

Even using the optimum value for the number of variables guessed in the nonlinear equation, FXL has the exponential complexity for solving the system of public polynomials in the proposed cryptosystem. Hence, the FXL algorithm is not applicable to our cryptosystem.

4.4 Complexity and number of operations for encryption and decryption

In this section we discuss the complexities of the encryption and the decryption of our cryptosystem.

4.4.1 Encryption

The public key in our cryptosystem consists of 2m equations of the form (4.3). There are $O(m^2)$ terms of the form $x_i x_j$ in each of the $2m$ equations of the public key. So the complexity of evaluating public key at message block $x_0, x_1, \ldots, x_{m-1}$ is $O(m^3)$. The next step of encryption is to solve the $2m$ linear equation in $2m$ ciphertext variables $y_0, y_1, \ldots, y_{2m-1}$. This can be done efficiently by Gaussian elimination with $O(m^3)$ complexity. Hence, the total complexity of encryption is $O(m^3)$.

4.4.2 Decryption

In our cryptosystem decryption is very fast. For decryption we are using the following operations: permutation of bits, xor and left cyclic shifts of bits. We count the total number of operations to describe the exact efficiency of our cryptosystem. To operate T_i or T_i^{-1}, $0 \leq i \leq 5$ on a m bit string we need one permutation on bits and at most $m-2$ left cyclic shifts and m xor operations. To operate T_i or T_i^{-1}, for $i = 6, 7$ on a $2m$ bit string we need one permutation on $2m$ bits and at most $2m-2$ left cyclic shifts and $2m$ xor operations. To compute $(Z)^{2m-1}$, where Z is a $2m$ bit string, we need at most $(2m-1)(2m-2)+2m-2$ left cyclic shifts and at most $(2m-1)^2+2m-1$ xor operations. Thus, to compute L_θ^{-1} where θ is m bit binary string we need at most $(m-1)(m-2)+m-2$ left cyclic shifts and at most $(m-1)^2+m-1$ xor operations. Thus, we see that for decryption we need $O(m^2)$ xor operations and $O(m^2)$ left cyclic shifts operations.

4.5 Comparison with HFE

In our cryptosystem the complexity of encryption is $O(m^3)$, i.e., equivalent to that of HFE. But the decryption is faster than HFE. In HFE the decryption is slow because one needs to compute the roots of a polynomial. The decryption complexity of HFE is $O(n^4 d^2 log(d))$, where d is the degree of the HFE polynomial. Note that for security reasons one cannot take smaller degree. Due to this the decryption process in HFE is slow. In our cryptosystem we are using left cyclic shifts and xor operations resulting much faster decryption process. In our cryptosystem we need $O(m^2)$ left cyclic shifts and $O(m^2)$ xor operations to decrypt a message. Public key size of HFE is of $O(m^3)$ terms. In our cryptosystem public key size is bigger than HFE but it is also of $O(m^3)$ terms as it is possible to write the public key as two sets of quadratic public polynomials. Secret key generation in our public key cryptosystem is faster than HFE, because for secret keys we have to select random odd weight and even weight binary strings and random permutations only.

4.6 A toy example of cryptosystem

Example 4.6.1. We consider finite field $\mathbb{F}_{2^4}$, $\lambda = 0$ and $\sigma = (1,0,0,0,0,$ $0,0,0)$. Suppose ϑ' is the normal element of $\mathbb{F}_{2^8}$ and we take the normal basis representation of $\mathbb{F}_{2^8}$ with respect to ϑ'. Suppose $T_1 = \pi_1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 3 & 1 \end{pmatrix}$ and $T_2 = \pi_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \end{pmatrix}$ and T_3, T_4, T_5 are $x + x^2 + x^4$, $x^2 + x^4 + x^8$, $x + x^2 + x^8$ respectively, $T_6 = \pi_6 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 5 & 0 & 4 & 2 & 6 & 7 \end{pmatrix}$ and $T_7 = \pi_7 \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 7 & 2 & 1 & 0 & 4 & 6 \end{pmatrix}$. Message $M = (x_0, x_1, x_2, x_3)$, $T_1(M) = M' = (x_2, x_0, x_3, x_1)$ and $T_2(M) = M' = (x_3, x_2, x_0, x_1)$. We compute all the bits of $M' * M''$. Suppose $[M' * M'']_i$ denotes the ith bit of $M' * M''$. We obtain, $[M' * M'']_0 = x_2x_3 + x_0 + x_3x_1 + x_1x_2$, $[M' * M'']_1 = x_2 + x_1$, $[M' * M'']_2 =$

$x_3 + x_1x_0 + x_2x_1 + x_0x_2$, $[M' * M'']_3 = x_2x_0 + x_0x_1 + x_2x_3 + x_1x_3$. Now compute all the bits $M' * M' * M''$. The bits of $M' * M' * M''$ are $[M' * M' * M'']_0 = x_2x_3 + x_0x_1 + x_3 + x_1$, $[M' * M' * M'']_1 = x_0 + x_2 + x_0x_1 + x_2x_3$, $[M' * M' * M'']_2 = x_0x_3 + x_1x_2$, $[M' * M' * M'']_3 = x_0x_3 + x_1x_2$. (f_0, f_1, f_2, f_3) denotes the bits of $T_3(M' * M' * M'')$ and (f_4, f_5, f_6, f_7) denotes the bits of $T_4(M' * M'') + T_5(M' * M' * M'')$, we have $f_0 = x_3x_2 + x_0x_1 + x_3 + x_1$, $f_1 = 1 + x_0x_3 + x_1x_2$, $f_2 = 1 + x_0x_3 + x_0x_1$, $f_3 = x_0 + x_2 + x_3x_2 + x_1x_2$, $f_4 = x_0 + x_0x_3 + x_3x_2 + x_1x_3$, $f_5 = 1 + x_0 + x_2x_3 + x_3x_0$, $f_6 = x_3 + x_2x_0 + x_1x_2 + x_0x_1$, $f_7 = 1 + x_0x_1 + x_0x_2 + x_3x_1 + x_2x_3$. Ciphertext $Y = (y_0, y_1, y_2, y_3, y_4, y_5, y_6, y_7)$ is an element of $\mathbb{F}_{2^{2m}}$. $T_6(Y) = Z = (y_3, y_1, y_5, y_0, y_4, y_2, y_6, y_7)$. Note that $\vartheta' = (1, 0, 0, 0, 0, 0, 0, 0)$. Suppose $P_0, P_1, P_2, P_3, P_4, P_5, P_6, P_7$ denote the bits of $T_7(f_0, f_1, f_2, f_3, f_4, f_5, f_6, f_7) * Z + \vartheta'$. We compute all the P_i, so the required public key is :

$P_0 = 1 + y_0(x_0x_1 + x_1x_2) + y_1(x_0x_2) + y_2(x_0x_3 + x_2x_3) + y_3(x_2x_3 + x_0x_3) + y_4(x_0x_3 + x_1x_3) + y_5(x_2x_3 + x_0x_3 + x_1x_3) + y_6(x_1x_2 + x_2x_3 + x_1x_3) + y_7(x_0x_1 + x_1x_3)x_0y_3 + x_1y_3 + x_0y_7 + x_2y_7 + x_2y_6 + x_0y_6 + y_2 + y_4 + x_1y_0 + x_3y_0 + x_0y_5 + x_1y_1$

$P_1 = y_0(x_2x_3 + x_0x_3 + x_1x_3) + y_1(x_0x_3 + x_2x_3) + y_2(x_0x_3 + x_1x_3) + y_3(x_0x_1 + x_1x_2) + y_4(x_0x_1 + x_1x_2) + y_5(x_0x_2) + y_6(x_0x_3 + x_2x_3) + y_7(x_2x_3 + x_1x_2 + x_0x_2 + x_1x_3) + x_0y_0 + x_0y_1 + x_0y_3 + x_0y_7 + x_1y_1 + x_1y_4 + x_1y_5 + x_2y_3 + x_2y_7 + x_3y_4 + y_2 + y_6$

$P_2 = y_0(x_0x_2) + y_1(x_0x_1 + x_1x_2) + y_2(x_0x_1 + x_1x_2) + y_3(x_2x_3 + x_1x_3 + x_0x_2 + x_1x_2) + y_4(x_0x_3 + x_2x_3 + x_1x_3) + y_5(x_2x_3 + x_0x_3) + y_6(x_0x_3 + x_1x_3) + y_7(x_0x_3 + x_2x_3) + x_0y_1 + x_0y_3 + x_0y_4 + x_0y_5 + x_1y_0 + x_1y_2 + x_1y_5 + x_2y_1 + x_2y_3 + x_3y_2 + y_6 + y_7$

$P_3 = y_0(x_0x_3 + x_2x_3) + y_1(x_0x_2 + x_1x_2 + x_2x_3) + y_2(x_0x_3 + x_2x_3 + x_1x_3) + y_3(x_2x_3 + x_0x_3) + y_4(x_0x_2) + y_5(x_0x_1 + x_1x_2) + y_6(x_0x_1 + x_1x_2) + y_7(x_0x_3 + x_1x_3) + x_0y_0 + x_0y_1 + x_0y_2 + x_0y_5 + x_1y_0 + x_1y_4 + x_1y_6 + x_2y_1 + x_2y_5 + x_3y_6 + y_3 + y_7$

$P_4 = y_0(x_0x_1 + x_1x_2) + y_1(x_2x_3 + x_0x_3) + y_2(x_0x_2) + y_3(x_1x_3 + x_0x_3) + y_4(x_0x_3 + x_2x_3) + y_5(x_2x_3 + x_0x_2 + x_1x_3 + x_1x_2) + y_6(x_1x_3 + x_2x_3 + x_0x_3) + y_7(x_0x_3 + x_2x_3) + x_0y_0 + x_0y_4 + x_0y_5 + x_0y_6 + x_1y_4 + x_1y_2 + x_1y_7 + x_2y_0 + x_2y_5 + x_3y_7 + y_1 + y_3$

$P_5 = y_0(x_0x_2 + x_1x_2 + x_1x_3 + x_2x_3) + y_1(x_0x_3 + x_1x_3) + y_2(x_0x_3 + x_2x_3) + y_3(x_0x_1 + x_1x_2) + y_4(x_0x_1 + x_1x_2) + y_5(x_2x_3 + x_0x_3) + y_6(x_0x_2) + y_7(x_2x_3 + x_0x_3 + x_1x_3) + x_0y_0 + x_0y_2 + x_0y_4 + x_0y_7 + x_1y_2 + x_1y_3 + x_1y_6 + x_2y_0 + x_2y_4 + x_3y_3 + y_1 + y_5$

$P_6 = y_0(x_0x_3 + x_2x_3) + y_1(x_0x_1 + x_1x_2) + y_2(x_0x_1 + x_1x_2) + y_3(x_2x_3 + x_0x_3 + x_1x_3) + y_4(x_0x_2 + x_1x_3 + x_2x_3 + x_1x_2) + y_5(x_0x_3 + x_1x_3) + y_6(x_0x_3 + x_2x_3) + y_7(x_0x_2) + x_0y_2 + x_0y_3 + x_0y_4 + x_0y_6 + x_1y_1 + x_1y_6 + x_1y_7 + x_2y_2 + x_2y_4 + x_3y_1 + y_0 + y_5$

$P_7 = y_0(x_0x_3 + x_1x_3) + y_1(x_0x_3 + x_1x_3 + x_2x_3) + y_2(x_0x_2 + x_2x_3 + x_1x_2 + x_1x_3) + y_3(x_0x_2) + y_4(x_2x_3 + x_0x_3 + x_0x_2) + y_5(x_1x_2 + x_0x_1) + y_6(x_0x_1 + x_1x_2) + y_7(x_2x_3 + x_0x_3) + x_0y_1 + x_0y_2 + x_0y_6 + x_0y_7 + x_1y_3 + x_1y_5 + x_1y_7 + x_2y_2 + x_2y_6 + x_3y_5 + y_0 + y_4$

The public key looks large, however it is possible to reduce the size of public key containing only quadratic terms. The public key can be written as two sets of public polynomials containing only quadratic terms. We have

$P_0' = 1 + y_0g_1 + y_1g_0 + y_2g_4 + y_3g_4 + y_4g_5 + y_5g_3 + y_6b + y_7g_5 + x_0y_3 + x_1y_3 + x_0y_7 + x_2y_7 + x_2y_6 + x_0y_6 + y_2 + y_4 + x_1y_0 + x_3y_0 + x_0y_5 + x_1y_1$

$P_1' = y_0g_3 + y_1g_4 + y_2g_5 + y_3g_1 + y_4g_1 + y_5g_0 + y_6g_4 + y_7g_2 + x_0y_0 + x_0y_1 + x_0y_3 + x_0y_7 + x_1y_1 + x_1y_4 + x_1y_5 + x_2y_3 + x_2y_7 + x_3y_4 + y_2 + y_6$

$P_2' = y_0g_0 + y_1g_1 + y_2g_1 + y_3g_2 + y_4g_3 + y_5g_4 + y_6g_5 + y_7g_4 + x_0y_1 + x_0y_3 + x_0y_4 + x_0y_5 + x_1y_0 + x_1y_2 + x_1y_5 + x_2y_1 + x_2y_3 + x_3y_2 + y_6 + y_7$

$P_3' = y_0g_4 + y_1g_6 + y_2g_3 + y_3g_4 + y_4g_0 + y_5g_1 + y_6g_1 + y_7g_5 + x_0y_0 + x_0y_1 + x_0y_2 + x_0y_5 + x_1y_0 + x_1y_4 + x_1y_6 + x_2y_1 + x_2y_5 + x_3y_6 + y_3 + y_7$

$P_4' = y_0g_1 + y_1g_4 + y_2g_0 + y_3g_5 + y_4g_4 + y_5g_2 + y_6g_3 + y_7g_4 + x_0y_0 + x_0y_4 + x_0y_5 + x_0y_6 + x_1y_4 + x_1y_2 + x_1y_7 + x_2y_0 + x_2y_5 + x_3y_7 + y_1 + y_3$

$P_5' = y_0g_2 + y_1g_5 + y_2g_4 + y_3g_1 + y_4g_1 + y_5g_4 + y_6g_0 + y_7g_3 + x_0y_0 + x_0y_2 + x_0y_4 + x_0y_7 + x_1y_2 + x_1y_3 + x_1y_6 + x_2y_0 + x_2y_4 + x_3y_3 + y_1 + y_5$

$P_6' = y_0g_4 + y_1g_1 + y_2g_1 + y_3g_3 + y_4g_2 + y_5g_5 + y_6g_4 + y_7a_0 + x_0y_2 + x_0y_3 + x_0y_4 + x_0y_6 + x_1y_1 + x_1y_6 + x_1y_7 + x_2y_2 + x_2y_4 + x_3y_1 + y_0 + y_5$

$P_7' = y_0g_5 + y_1g_3 + y_2g_2 + y_3g_0 + y_4g_7 + y_5g_1 + y_6g_1 + y_7g_4 + x_0y_1 + x_0y_2 + x_0y_6 + x_0y_7 + x_1y_3 + x_1y_5 + x_1y_7 + x_2y_2 + x_2y_6 + x_3y_5 + y_0 + y_4$

Where $g_0 = x_0x_2$, $g_1 = x_0x_1 + x_1x_2$, $g_2 = x_2x_3 + x_1x_2 + x_0x_2 + x_1x_3$, $g_3 = x_2x_3 + x_0x_3 + x_1x_3$, $g_4 = x_2x_3 + x_0x_3$, $g_5 = x_0x_3 + x_1x_3$, $g_6 = x_2x_3 + x_1x_2 + x_0x_2$, $g_7 = x_2x_3 + x_0x_3 + x_0x_2$ and $b = g_0 + g_2$. Suppose $M = (0, 0, 0, 1)$ is the plaintext message. Substituting this in above public equation we get linear equations, $y_2 + y_4 + y_0 = 1$, $y_2 + y_4 + y_6 = 0$, $y_2 + y_6 + y_7 = 0$, $y_3 + y_6 + y_7 = 0$, $y_1 + y_3 + y_7 = 0$, $y_1 + y_3 + y_5 = 0$, $y_0 + y_1 + y_5 = 0$, $y_0 + y_4 + y_5 = 0$. Solving these linear equations by Gaussian-elimination we get $(y_0, y_1, y_2, y_3, y_4, y_5, y_6, y_7) = (0, 1, 0, 0, 1, 1, 1, 1)$, which is the required ciphertext.

Chapter 5

Poly-Dragon: An Efficient Multivariate Public Key Cryptosystem

5.1 Intrduction

In this chapter we propose another multivariate public key cryptosystem. The public key of our cryptosystem contains polynomials of total degree three in plaintext and ciphertext variables, two in plaintext variables and one in ciphertext variables. However, it is possible to reduce the public key size by writing it as two sets of quadratic multivariate polynomials. The complexity of encryption in this public key cryptosystem is $O(m^3)$, where m is bit size, equivalent to other multivariate public key cryptosystems. For decryption we need only four exponentiations in the binary field. The public key algorithm is bijective and can be used for encryption as well as for signatures. We will use nonlinear permutation polynomials from Chapter 3. In Section 2 of this chapter we present the cryptosystem and in Section 3, we give a toy example of the cryptosystem. In Section 4, we give the security analysis and in Section 5 we discuss the efficiency of the cryptosystem.

5.2 The Cryptosystem Poly-Dragon

5.2.1 Public key generation.

For the public key cryptosystem we will use permutation polynomials $g(x) = (x^{2^{k2^r}} + x^{2^r} + \alpha)^l + x$ and $f(x) = (L_\beta(x) + \gamma)^\ell + Tr(x)$ obtained in Theorem 3.3.1 and Theorem 3.3.6. For quadratic public key size, we cannot take all the permutation polynomials of the form $(x^{2^{k2^r}} + x^{2^r} + \alpha)^l + x$. But the permutation polynomials in which l is of the form $2^t + 1$ or $2^t - 1$ can be used to design the multivariate public key cryptosystem with quadratic public key size. For l is of the form $2^t + 1$ it is not clear whether $g(x)$ is a permutation polynomial or not. But, for $r = 0$, $m = 2n - 1$, $k = n$, $k_2 = n$, $k_1 = 0$, $l = 2^n - 1$ and $\ell = 2^n - 1$, $g(x)$ and $f(x)$ are permutation polynomials because in this case $2^{2^r k} + 2^r = 2^n + 1$, $2^{k_1} + 2^{k_2} = 2^n + 1$ and $(2^n - 1)(2^n + 1) = 1 \bmod 2^m - 1$. So, for public key generation we will take $g(x) = (x^{2^n} + x + \alpha)^{2^n - 1} + x$ and $f(x) = (L_\beta(x) + \gamma)^{2^n - 1} + Tr(x)$, where α, β, γ are secret. Suppose s and t are two invertible affine transformations. The relation between the plaintext and the ciphertext is $g(s(x)) = f(t(y))$, where variable x denotes the plaintext and y the ciphertext. Suppose $s(x) = u$ and $t(y) = v$. Thus we have the following relation between plaintext and ciphertext: $(u^{2^n} + u + \alpha)^{2^n - 1} + u = (L_\beta(v) + \gamma)^{2^n - 1} + Tr(v)$. Since $u^{2^n} + u + \alpha$ and $L_\beta(v) + \gamma$ are nonzero in the field $\mathbb{F}_{2^m}$, this relation gives

$$\begin{aligned}(u^{2^n} + u + \alpha)^{2^n}(L_\beta(v) + \gamma) + u(u^{2^n} + u + \alpha)(L_\beta(v) + \gamma)\\ +(u^{2^n} + u + \alpha)(L_\beta(v) + \gamma)^{2^n} + Tr(v)(u^{2^n} + u + \alpha)(L_\beta(v) + \gamma) &= 0.\end{aligned}$$

Suppose $Tr(v) = \zeta_y \in \{0, 1\}$. Using a fixed basis $\mathbb{B} = \{\vartheta_0, \ldots, \vartheta_{m-1}\}$ of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$, we identify the field $\mathbb{F}_{2^m}$ by $\mathbb{F}_2^m$. Substituting $u = s(x)$ and $v = t(y)$, where $x = (x_0, \ldots, x_{m-1})$ and $y = (y_0, \ldots, y_{m-1})$, we get m nonlinear polynomial equations of the form

$$\begin{aligned}\sum a_{ijk} x_i x_j y_k + \sum b_{ij} x_i x_j + \sum (c_{ij} + \zeta_y) x_i y_j\\ + \sum (d_k + \zeta_y) y_k + \sum (e_k + \zeta_y) x_k + f_l &= 0, \qquad (5.1)\end{aligned}$$

where $a_{ij}, b_{ij}, c_k, d_k, e_k \in \mathbb{F}_2$. These equations are of degree three and therefore each of them contains $O(m^3)$ terms. Since we have m equations, total size will be of $O(m^4)$, which is large. It is possible to reduce the size of polynomial equations (5.1) to $O(m^3)$ by writing it as two sets of public polynomials containing only quadratic terms without changing the security since this can be done in polynomial time (see [64]). Thus, the public key will be two sets of m quadratic equations of the form:

$$\sum g_k y_k + \sum (b_{ij} + \zeta_y) x_i y_j + \sum (d_k + \zeta_y) y_k + \sum (e_k + \zeta_y) x_k + f_l = 0,$$

where $g_k = \sum h_{ijk} x_i x_j$.

5.2.2 Secret Key

The invertible affine transformations (s, t) and the field elements α, β, γ are the secret keys.

5.2.3 Encryption

If Bob wants to send a plaintext message $x = (x_0, \ldots, x_{m-1})$ to Alice, he does the following:

1. Bob substitutes the plaintext $(x_0, \ldots, x_{m-1})$ and $\zeta_y = 0$ in public key and gets n linear equations in ciphertext variables $y_0, \ldots, y_{m-1}$. Bob solve these linear equations by Gaussian elimination and gets $y^{'} = (y_0, \ldots, y_{m-1})$

2. In the second step of encryption Bob substitutes the plaintext $(x_0, \ldots, x_{m-1})$ and $\zeta_y = 1$ in public key and gets m linear equations in ciphertext variables $y_0, \ldots, y_{m-1}$. Now Bob solve these linear equations by Gaussian elimination method to gets $y^{''} = (y_0, \ldots, y_{m-1})$.

3. The ordered pair $(y^{'}, y^{''})$ is the required ciphertext.

5.2.4 Decryption

The decryption algorithm of the cryptosystem is as follows.

Input: Ciphertext $(y^{'}, y^{''})$ and secret parameters $(s, t, \alpha, \beta, \gamma)$.

Output: Message $(x_0, \ldots, x_{m-1})$.

1: $v_1 \leftarrow t(y^{'})$ and $v_2 \leftarrow t(y^{''})$.
2: $z_1 \leftarrow L_\beta(v_1) + \gamma$ and $z_2 \leftarrow L_\beta(v_2) + \gamma$.
3: $z_3^{'} \leftarrow (z_1)^{2^m-1}$ and $z_4^{'} \leftarrow (z_2)^{2^m-1}$.
4: $z_3 \leftarrow z_3^{'} + Tr(v_1)$ and $z_4 \leftarrow z_4^{'} + Tr(v_2)$.
5: $z_5 \leftarrow z_3^{2^m} + z_3 + \alpha + 1$ and $z_6 \leftarrow z_4^{2^m} + z_4 + \alpha + 1$.
6: $z_7 \leftarrow z_5^{2^m-1}$ and $z_8 \leftarrow z_6^{2^m-1}$.
7: $X_1 \leftarrow s^{-1}(z_3 + 1)$, $X_2 \leftarrow s^{-1}(z_4 + 1)$, $X_3 \leftarrow s^{-1}(z_3 + z_7 + 1)$ and $X_4 \leftarrow s^{-1}(z_4 + z_8 + 1)$.
8: Return (X_1, X_2, X_3, X_4).

Out of X_1, X_2, X_3, X_4, one will be the correct message. There are only four choices for the message, and it will be easy to identify the correct one.

Theorem 5.2.1. *Given ciphertext, the decryption algorithm outputs a valid plaintext.*

Proof. We prove that the procedure described above outputs a valid plaintext. The relation between the plaintext and the ciphertext is $(u^{2^n} + u + \alpha)^{2^n-1} + u = (L_\beta(v) + \gamma)^{2^n-1} + Tr(v)$, or equivalently, $u^{2^n} + u + \alpha = (u + z)^{2^n+1}$, where $z = (L_\beta(v) + \gamma)^{2^n-1} + Tr(v)$, and this can be converted to the form $(u + z + 1)^{2^n+1} + z + z^{2^n} + \alpha + 1 = 0$. There are only two possibilities: either $u = z + 1$ or $u \neq z + 1$. If $u = z + 1$, then $x = s^{-1}(z + 1)$. If $u \neq z + 1$, then raising both sides to power $2^m - 1$ in the relation $(u + z + 1)^{2^n+1} = z + z^{2^n} + \alpha + 1$, we get $(u + z + 1) = (z + z^{2^n} + \alpha + 1)^{2^n-1}$ or $u = z + 1 + (z + z^{2^n} + \alpha + 1)^{2^n-1}$, which implies $x = s^{-1}\left(z + 1 + \left(z + z^{2^n} + \alpha + 1\right)^{2^n-1}\right)$. □

5.3 A Toy Example

Here is a toy example for our cryptosystem. We consider the finite field $\mathbb{F}_{2^3}$, that is, $n = 2$ and $m = 3$. The polynomial $x^3 + x + 1$ is irreducible over $\mathbb{F}_2$. Suppose ϑ is the root of this polynomial in the extension field of $\mathbb{F}_2$, i.e.,

$\vartheta^3+\vartheta+1=0$. Using the basis $\{1,\vartheta,\vartheta^2\}$ the finite field $\mathbb{F}_{2^3}$ can be expressed as $\mathbb{F}_{2^3}=\{0,1,\vartheta,\vartheta^2,1+\vartheta,1+\vartheta^2,\vartheta+\vartheta^2,1+\vartheta+\vartheta^2\}$. We are taking $\alpha=\gamma=1+\vartheta+\vartheta^2$, as $tr(1+\vartheta+\vartheta^2)\neq 0$, and $\beta=1+\vartheta$. Corresponding to $\beta=1+\vartheta=(1,1,0)$, $L_\beta=x+x^2$. We are taking invertible transformation $s(x)=A_1x+c_1$ and $t(x)=A_2x+c_2$, where

$$A_1=\begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}, A_2=\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix},\ c_1=(1,0,1)^T \text{ and } \quad c_2=(0,1,0)^T.$$

Suppose $x\in\mathbb{F}_{2^3}$, then x can be expressed as $x=x_0+x_1\vartheta+x_2\vartheta^2$, where $x_i\in\mathbb{F}_2$. Taking $x=(x_0,x_1,x_2)^T$, we have $A_1x+c_1=(x_0+x_1+1,x_1+x_2,x_2+1)^T$ and $A_2x+c_2=(x_0+x_1+x_2,x_1+x_2+1,x_2)^T$. For the plaintext variable $x=(x_0,x_1,x_2)$ the corresponding ciphertext variable is $y=(y_0,y_1,y_2)$. We have $u=(x_0+x_1+1)+(x_1+x_2)\vartheta+(x_2+1)\vartheta^2$ and $v=(y_0+y_1+y_2)+(y_1+y_2+1)\vartheta+y_2\vartheta^2$. The relation between the plaintext and the ciphertext is

$$\begin{aligned}(u^{2^n}+u+\alpha)^{2^n}(L_\beta(v)+\gamma)+u(u^{2^n}+u+\alpha)(L_\beta(v)+\gamma)\\ +(u^{2^n}+u+\alpha)(L_\beta(v)+\gamma)^{2^n}+Tr(v)(u^{2^n}+u+\alpha)(L_\beta(v)+\gamma) &= 0.\end{aligned}$$

Substituting u and v and $\alpha=\gamma=1+\vartheta+\vartheta^2$, and $L_\beta(x)=x+x^2$ and $Tr(v)=\zeta_y$ we have the following relation between the plaintext and the ciphertext:

$$\begin{aligned}&\{1+\zeta_y+(1+\zeta_y)x_2y_2+(1+\zeta_y)x_2y_1+\zeta_yx_1y_1+x_0+y_1+x_1x_2+x_0x_1y_1+\\ &x_0x_2y_1+x_0x_2y_2\}+\vartheta\{x_1+(\zeta_y+1)y_1+y_2+\zeta_yx_2+\zeta_yx_2y_1+(\zeta_y+1)x_2y_2+\\ &\zeta_yx_1y_2+x_0x_2+x_0y_1+x_0x_2y_2+x_0x_1y_1+x_1y_1+x_1x_2y_2\}+\\ &\vartheta^2\{1+x_2+(\zeta_y+1)y_2+\zeta_yx_1+\zeta_yy_1+(\zeta_y+1)x_1y_1+\zeta_yx_1y_2+(\zeta_y+1)x_2y_1+\\ &x_2y_2+x_0x_1+x_0y_1+x_0y_2+x_0x_1y_1+x_0x_1y_2+x_0x_2y_1+x_1x_2y_1\}=0,\end{aligned}$$

or, equivalently,

$$
\begin{aligned}
1+\zeta_y+(1+\zeta_y)x_2y_2+(1+\zeta_y)x_2y_1+\zeta_y x_1y_1+ & \\
x_0+y_1+x_1x_2+x_0x_1y_1+x_0x_2y_1+x_0x_2y_2 &= 0,\\
x_1+(\zeta_y+1)y_1+y_2+\zeta_y x_2+\zeta_y x_2y_1+(\zeta_y+1)x_2y_2+\zeta_y x_1y_2+ & \\
x_0x_2+x_0y_1+x_0x_2y_2+x_0x_1y_1+x_1y_1+x_1x_2y_2 &= 0,\\
1+x_2+(\zeta_y+1)y_2+\zeta_y x_1+\zeta_y y_1+(\zeta_y+1)x_1y_1+\zeta_y x_1y_2+(\zeta_y+1)x_2y_1 & \\
+x_2y_2+x_0x_1+x_0y_1+x_0y_2+x_0x_1y_1+x_0x_1y_2+x_0x_2y_1+x_1x_2y_1 &= 0.
\end{aligned}
$$

Above equations represent the required public key. Note that the above equations are nonlinear in the plaintext variables (x_0, x_1, x_2) and linear in the ciphertext variables (y_0, y_1, y_2).

5.4 Security of the proposed Cryptosystem

In this section, we discuss the security of the proposed cryptosystem. We give some security arguments and evidence that our cryptosystem is secure. We are using the polynomials $(x^{2^m}+x+\alpha)^{2^m-1}+x$, and $(L_\beta(x)+\gamma)^{2^m-1}+Tr(x)$ where α, β and γ are secret. Thus, if we write the polynomial $(x^{2^m}+x+\alpha)^{2^m-1}+x$ in the form $\sum_{i=0}^{d} p_i x^i$ then some of coefficients will be 0 and 1 and the rest will be some functions of α. Since α is secret, most of the coefficients of this polynomial are also secret. Similarly, if we write the polynomial $(L_\beta(x)+\gamma)^{2^m-1}+Tr(x)$ in the form $\sum_{i=0}^{d} p_i' x^i$ then all the coefficients of this polynomial are secret because β and γ both are secret. One important point is that the degrees of these polynomials are not constant but are functions of n, as $m=(n+1)/2$. The Coppersmith-Patarin attack on Little Dragon cryptosystem [44] is due to the use of the monomial x^n to design the Little Dragon cryptosystem, so this attack is not applicable to our cryptosystem. Here we discuss some known attacks developed for multivariate cryptosystems and we will show that those attacks are not applicable to our cryptosystem. The attacks discussed in this section are Linearization equation, Gröbner basis, univariate polynomial representation, Differential cryptanalysis, Relinearization, XL and FXL algorithms attacks.

5.4.1 Linearization Equation Attacks

We are not using the monomial x^{q^i+1}. Moreover, in our cryptosystem the plaintext and ciphertext are connected by the relation $(u^{2^m} + u + \alpha)^{2^m-1} + u = (L_\beta(v) + \gamma)^{2^m-1} + Tr(v)$ where α, β, γ are secret. So, in this case it is not possible to obtain a relation of the form (4.9). However, one can try to find a relation which is linear in x_i and nonlinear in y_j. We will prove that this line of attack is not possible as the degree of the inverse function is very high. Suppose $(L_\beta(v)+\gamma)^{2^m-1}+Tr(v) = z$, then our relation between plaintext and ciphertext is $(u^{2^m}+u+\alpha)^{2^m-1}+u = z$ or equivalently we have $(u^{2^m}+u+\alpha) = (z+u)^{2^m+1}$ which is further equivalent to $(z+u+1)^{2^m+1} = z^{2^m}+z+\alpha+1$. If $z+u+1 \neq 0$ then raising both sides to the power 2^m-1 we get $(z+u+1) = (z^{2^m}+z+\alpha+1)^{2^m-1}$. If $z^{2^m} + z + \alpha + 1 \neq 0$, then we have the following relation between plaintext and ciphertext $(z + u + 1)(z^{2^m} + z + \alpha + 1) + (z^{2^m} + z + \alpha + 1)^{2^m} = 0$. This relation gives equations which are linear in plaintext variables x_i and non-linear in ciphertext variables y_i. Note that $z = (L_\beta(v) + \gamma)^{2^m-1} + Tr(v)$ will give non linear equations of degree $w(2^m - 1)$, where $w(2^m - 1)$ denotes the weight of $2^m - 1$ so the relation $(z+u+1)(z^{2^m}+z+\alpha+1)+(z^{2^m}+z+\alpha+1)^{2^m} = 0$ gives equations of non linear degree $2w(2^m - 1)$ in ciphertext variables y_i. Thus, this line of attack is completely infeasible.

5.4.2 Attacks with Differential Cryptanalysis

We are using the polynomials $(x^{2^m} + x + \alpha)^{2^m-1} + x$ and $(L_\beta(v) + \gamma)^{2^m-1} + Tr(v)$, where α, β, γ are secret. Clearly the degree of these polynomial are not quadratic. Moreover, the public key in our cryptosystem is of mixed type. Substituting the ciphertext gives quadratic equations in plaintext variables but in that case, they will be different for different ciphertexts. So, attacking our cryptosystem by the methods of [32] and [28] is not feasible.

5.4.3 Gröbner Basis Attacks

Our public key is of mixed type, this mean for different ciphertexts we will get different system of quadratic polynomial equations, so in our public key the quadratic polynomials look random. We are using a polynomial which has

degree proportional to n. It is explained in [31] that in this case there does not seem to exist polynomial time algorithm to compute the Gröbner basis. Hence, Gröbner basis attacks on our cryptosystem are not feasible.

5.4.4 Relinearization, XL and FXL Algorithms.

Our polynomials are not quadratic. Moreover, the degrees of our polynomials are not constant, but are functions of m. So, the attack as given in [42] is not feasible to our cryptosystem. Adversary can not use directly Relinearization, XL or FXL algorithms to attack our cryptosystem, because when the number of equations is equal to the number of variables, the complexities of these algorithms is 2^m.

5.5 Efficiency of the proposed cryptosystem

In this section we discuss complexities of the encryption and decryption of our cryptosystem.

5.5.1 Encryption

There are $O(m^2)$ terms of the form $x_i x_j$ in each m equations of the public key. So the complexity of evaluating public key at message block $x_0, \ldots, x_{m-1}$ is $O(m^3)$. The next step of encryption is to solve the m linear equations in m ciphertext variables $y_0, \ldots, y_{m-1}$. This can be done efficiently by Gaussian elimination with complexity $O(m^3)$. Hence the complexity of encryption is $O(m^3)$.

5.5.2 Decryption

For decryption in the proposed cryptosystem we need four exponentiations namely $z_3' \leftarrow (z_1)^{2^n-1}$, $z_4' \leftarrow (z_2)^{2^n-1}$, $z_7 \leftarrow z_5^{2^n-1}$ and $z_8 \leftarrow z_6^{2^n-1}$. So the complexity of decryption is equivalent to Dragon cryptosystems [44], [64]. Note that for exponentiation in finite fields $\mathbb{F}_{2^m}$, there are several efficient algorithms, so the exponentiation can be performed very efficiently. The exact complexity of exponentiation will depend on the algorithm used for exponentiation.

Chapter 6

Conclusion

In the thesis we have studied permutation polynomials over finite rings $\mathbb{Z}_{p^n}$ and finite fields, and obtained some new results. We have used permutation polynomials over finite fields to design two efficient multivariate public key cryptosystems which we have shown to be secure against all the known attacks.

We have characterized permutation polynomials over finite ring $\mathbb{Z}_{p^n}$, for $p = 2, 3, 5$. Moreover, we have given sufficient conditions for a polynomial over $\mathbb{Z}_{p^n}$ for any p to be a permutation polynomial. However, it is not clear at this stage how to characterize permutation polynomials over finite rings $\mathbb{Z}_{p^n}$ for primes $p \geq 7$. From our results, it is clear that the main difficulty arises in the case $n = 1$.

We have found some new classes of permutation polynomials over finite fields $\mathbb{F}_{p^m}$, for $p = 2,\ 3$. In particular, we have introduced and characterized $\mathcal{L}(m)$, a commutative group of linearized permutation polynomials over finite fields $\mathbb{F}_{2^m}$. Computations with the group $\mathcal{L}(m)$ are efficient, which makes it suitable for cryptographic applications. We have constructed nonlinear trapdoor function using the group $\mathcal{L}(m)$. However, we believe that the group $\mathcal{L}(m)$ is of independent interest. We have also obtained some classes of nonlinear permutation polynomials and have used them to design another efficient multivariate public key cryptosystem. Like in Big Dragon Cryptosystem, the public key in our cryptosystems is of mixed type with total degree three; two in plaintext variables and one in ciphertext variables. The public key size can be reduced by writing it as two sets of quadratic equations. The efficiency of encryption in both the cryptosystems is equivalent to those of other multivariate public key

cryptosystems, that is, $O(m^3)$, where m is the bit size. The decryption in both the cryptosystem is more efficient than any other existing multivariate public key cryptosystem. We have shown that our cryptosystems are secure against all the known attacks.

It is not clear at this stage how to design a secure Little Dragon type cryptosystems having public key of mixed type but quadratic. It will be an interesting topic of future work to investigate how one can use permutation polynomials over finite fields to devise such cryptosystems.

List of Publications

1. Rajesh P. Singh, A. Saikia and B. K. Sarma, *Little-Dragon Two: An efficient Multivariate Public Key Cryptosystem,* "International journal of network security and its applications", 2(2) 2010.

2. Rajesh P. Singh and Soumen Maity, *Permutation Polynomials Modulo P^n*, International conference in number theory and combinatorics (ICNTC-2006).

3. Rajesh P. Singh, B. K. Sarma and A. Saikia, *Public Key Cryptography Using Permutation P-Polynomials over Finite Fields*, "Applicable Algebra in Communications and Engineering," Springer, Under revision preprint http://eprint.iacr.org/2009/208.

4. Rajesh P. Singh, A. Saikia and B. K. Sarma, *Poly-Dragon: An efficient Multivariate Public Key Cryptosystem,* communicated to the "Journal of Mathematical Cryptology,"
preprint http://eprint.iacr.org/2009/587.

5. *"Permutation Polynomials and Triangular Mappings over Finite Fields",* under preparation.

Bibliography

[1] Abhyankar, S. S., *Symplectic groups and permutation polynomials, part II*, Finite Fields and Their Applications **8** (2002), 233–255.

[2] Akbary, A. and Wang, Q., *A generalised Lucas sequence and permutation binomials*, Proceedings of the American Mathematical Society **134** (2005), no. 1, 15–22.

[3] _____, *On Polynomials of the Form $x^r f(x^{(q-1)/l})$*, International Journal of Mathematics and Mathematical Sciences, Hindawi Publishing Corporation (doi:10.1155/2007/23408).

[4] Akbary, A., Ghioca, D., Wang, Q., *On permutation polynomials of prescribed shape*, Finite Fields and Their Applications **15** (2009), 195–206.

[5] American National Standards Institute, *The elliptic curve digital signature algorithm (ECDSA)*, ANSI X9.62, 1998.

[6] Bernstein, B. A., *Modular representation of finite algebras*, Proc. International Math. Congress **22** (1924), no. 1, 207–216.

[7] Carlitz, L., *Some theorems on permutation polynomials*, Bull. Amer. Math. Soc. **68** (1962), 120–122.

[8] Charpin, P. and Kyureghyan, G. M., *On a class of permutation polynomials over $\mathbb{F}_{2^m}$*, SETA 2008, LNCS 5203 (2008), 368–376.

[9] _____, *When does $g(x)+\gamma tr(h(x))$ permute $\mathbb{F}_{p^n}$?*, Finite Fields and Their Applications **15** (2009), 615–632.

[10] Cohen, S. D., *Dickson polynomials of the second kind that are permutations*, Canad. J. Math **46** (1994), 225–238.

[11] _____, *Dickson permutations,in "number-theoretic and algebraic methods in computer science (moscow, 1993)*, World Scientific Publishing, River Edge, NJ (1995).

[12] Coulter, R., Henderson, M. and Matthews, R., *A note on constructing permutation polynomials*, Finite Fields and Their Applications **15** (2009), 519–530.

[13] Coulter, R. S. and Matthews, Rex W., *On the permutation behavior of dickson polynomials of second kind*, Finite Fields and Their Applications **8** (2002), 519–530.

[14] Courtois, N., Klimov, A., Patarin, J., and Shamir, A., *Efficient Algorithm for Solving Overdefined System of Multivariate Polynomial Equations*, EUROCRYPT '2000, LNCS **1807** (2000), 392–407.

[15] Courtois, N. T., *The security of hidden field equations (HFE)*, CT-RSA'01, LNCS **2020** (2001), 266–281.

[16] Courtois, N. T., Daum, M., and Felke, P., *On the security of HFE, HFEv- and Quartz*, PKC '2003, LNCS **2567** (2003), 337–350.

[17] Cox, D., Little, J., and OShea, D., *Ideals, varieties, and algorithms: An introduction to computational algebraic geometry and commutative algebra*, Undergraduate Texts in Mathematics, Springer, 1997.

[18] Das, P., *The number of permutation polynomials of a given degree over a finite field*, Finite Fields and Their Applications **8** (2002), 478–490.

[19] Davis, P. J., *Circulant matrices*, American Mathematical Society, 1994.

[20] Delgosha, F., and Fekri, F., *Public-Key Cryptography Using Paraunitary Matrices*, IEEE TRANSACTIONS ON SIGNAL PROCESSING **54** (2006), no. 9.

[21] Dickson, L. E., *The analytic representation of substitution on a power of a prime number of letters with a discussion of the linear group*, Ann. of Math. **11** (1931), 65–120.

[22] ———, *Linear Groups with an Exposition of the Galois Field Theory*, Teubner, Leipzig, 1901; Dover New York (1958).

[23] Diffie, W., Hellman, M. E., *New directions in cryptography*, IEEE Trans. Information Theory **22** (1976), 644–654.

[24] Ding, C. , Xiang, Q., Yuan, J., Yuan, P., *Explicit classes of permutation polynomials of* $\mathbb{F}_{3^{3m}}$, Science in China Series A: Mathematics **53** (2009), 639–647.

[25] Ding, J., *A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation*, PKC 04, LNCS **2947** (2004), 305–318.

[26] Ding, J., Gower, J. E. and Schmidt, D. S., *Multivariate public key cryptosystems*, Springer, 2006.

[27] Ding, J., Hu, L., Nie, X., Li, J., and Wagner, J., *High Order Linearization Equation (HOLE) Attack on Multivariate Public Key Cryptosystems*, PKC 2007, LNCS **4450** (2007), 223–248.

[28] Dubois, V., Fouque, P., Shamir, A., Sterm, J., *Practical Cryptanalysis of Sflash*, Advances in Cryptology-Crypto '2007, LNCS **4622** (2007), 1–12.

[29] Faugere, J. C., *A New efficient algorithm for computing Grobner bases (F_4)*, Journal of Pure and Applied Algebra **139** (2002), 61–88.

[30] ———, *A New efficient algorithm for computing Grobner bases without reduction to zero (F_5)*, International Symposium on Symbolic and Algebraic Computation - ISSAC '2002, ACM PRESS (2002), 75–83.

[31] Faugere, J. C. and Joux, A., *Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Grobner Basis*, CRYPTO '2003, LNCS **2729** (2003), 44–60.

[32] Fouque, P. A., Granboulan, L., and Sterm, J., *Differential Cryptanalysis for Multivariate Schemes*, EUROCRYPT 2005, LNCS **3494** (2005), 341–353.

[33] Fried, M., *On a conjecture of Schur*, Michigan Math. J. **17** (1970), 41–55.

[34] ———, *On a theorem of MacCluer*, Acta Arith. **25** (1974), 121–126.

[35] ———, *Arithmatical properties of function fields (II). The generalised schur problem*, Acta Arith. **25** (1974), 225–258.

[36] Goldwasser, S. and Bellare, M., *Lecture notes on cryptography [online]*, Available: http://www.cs.ucsd.edu/users/mihir/papers/ gb.html, 2001.

[37] Goubin, L. and Courtois, N. T., *Cryptanalysis of the TTM cryptosystem*, Adv. Cryptol.-ASIACRYPT 00, LNCS **1976** (2000), 44–57.

[38] Hardy, G. H. and Wright, E. M., *An introduction to the theory of numbers*, Oxford Science Publications, 1979.

[39] Heisler, J., *A characterization of finite fields*, Amer. Math. Monthly **74** (1967), 537–538.

[40] Henderson, M. and Matthews, R., *Dickson polynomials of the second kind which are permutation polynomials over a finite field*, New Zealand J. Math **27** (1998), 227–244.

[41] Kempner, A. J., *Polynomials and their residue systems*, Trans. Amer. Math. Soc. **22** (1921), 240–288.

[42] Kipnis, A. and Shamir, A., *Cryptanalysis of the HFE public key cryptosystem by relinearization*, CRYPTO '99, LNCS **1666** (1999), 19–30.

[43] Klimov, A. and Shamir, A., *A New Class of Invertible Mappings*, CHES 2002, LNCS **2523** (2003), 470–483.

[44] Koblitz, N., *Algebraic aspects of cryptography*, Algorithm and Computation in Mathematics, Springer., vol. 3, 1998.

[45] Konyagin, S., Pappalardi, F., *Enumerating permutation polynomials over finite fields by degree*, Finite Fields and Their Applications **8** (2002), 548–553.

[46] Kurbatov, V.A., *On the monodromy group of an algebraic function*, Amer. Math. Soc. **36** (1964), no. 2, 17–62.

[47] Laigle-Chapuy, Y., *Permutation polynomials and applications to coding theory*, Finite Fields and Their Applications **13** (2007), 207–213.

[48] Lidl, R. and Mullen, G.L., *When does a polynomial over a finite field permute the elements of the field?*, Amer. Math. Monthly **95** (1988), no. 3, 243–246.

[49] ———, *When does a polynomial over a finite field permute the elements of the field? II*, The American Math. Monthly **100** (1993), no. 1, 71–74.

[50] Lidl, R. and Niederreiter, H., *Finite fields*, Cambridge University Press, 1997.

[51] Lidl, R., Mullen, G. L., and Turnwald, G., *Dickson polynomials*, Pitman Monographs and Surveys in Pure and Applied Mathematics, Longman Scientific and Technical, Essex, England **65** (1993).

[52] Malvenuto, C., Pappalardi, F., *Enumerating permutation polynomials i:permutations with non-maximal degree*, Finite Fields and Their Applications **8** (2002), 531–547.

[53] ———, *Enumerating permutation polynomials II: k cycles with minimal degree*, Finite Fields and Their Applications **10** (2004), 72–96.

[54] Marcos, J. E., *Specific permutation polynomials over finite fields*, Finite Fields and Their Applications **in press** (2009).

[55] Matsumoto, T. and Imai, H., *Public quadratic polynomial-tuples for efficient signature-verification and message-encryption*, Eurocrypt '88, springer-verlag (1989), 419–453.

[56] Matthews, Rex W., *Permutation polynomials in one and several variables*, PhD Thesis, University of Tasamania (1982).

[57] Menezes, A. J., van Oorschot, P. C., and Vanstone, S. A., *Handbook of applied cryptography*, New York: CRC Press, 1997.

[58] Moh, T. T., *A public key system with signature and master key functions*, Commun. Algebra, **27** (1999), no. 5, 2207–2222.

[59] Mollin, R. A. and Small, C., *On permutation polynomials over finite fields*, Internat. J. Math. & Math. Sci. **10** (1987), no. 3, 535–544.

[60] Mullen, G. L., *Permutation polynomials and nonsingular feedback shift registers over finite fields*, IEEE Trans. Information Theory **35** (1989), no. 4, 900–902.

[61] Muratović-Ribić, A., *A note on the coefficients of inverse polynomials*, Finite Fields and Their Applications **13** (2007), 977–980.

[62] Nagata, M., *On automorphism group of k[x,y]*, Lectures on Mathematics. Kyoto University, Kinokuniya, Tokyo, vol. 5, 1972.

[63] Patarin, J., *Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt '88,*, Advances in Cryptology-Crypto '95, springer-verlag (1996), 248–261.

[64] _____, *Asymmetric cryptography with a hidden monomial*, Advances in Cryptology-Crypto '96, Springer-verlag (1997), 45–60.

[65] _____, *Hidden field equations (HFE) and isomorphism of polynomials (IP): two new families of asymetric algorithms*, Advances in cryptology-Eurocrypt '96, Springer-verlag (1997), 33–48.

[66] Patarin, J., Courtois, N. T., and Goubin, L., *FLASH, a fast multivariate signature algorithm*, CT-RSA 01, LNCS **2020** (2001), 298–307.

[67] Rivest, R.L., *Permutation polynomials modulo* 2^w, Finite Fields and Their Applications **7** (2001), 287–292.

[68] Rivest, R.L., Robshaw, M. J. B., Sidney, R., and Yin, Y. L., *The RC6 block cipher*, http://theory.lcs.mit.edu/ rivest/rc6.pdf or http://csrc.nist.gov/encryption/aes/.

[69] Rivest, R.L., Shamir, A., Adleman, L., *A method for obtaining digital signatures and public key cryptosystem*, Communications of the ACM **21** (1978).

[70] Schneier, B., *Applied cryptography: Protocols, algorithms, and source code in c*, New York, Wiley, 1997.

[71] Shamir, A., *Efficient signature schemes based on birational permutations*, Adv. Cryptol.-CRYPTO 93, LNCS **773** (1994), 1–12.

[72] Shor, P., *Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM Journal on Scientific Computing **26** (1997).

[73] Stinson, D. R., *Cryptography: Theory and Practice*, Boca Raton, FL: CRC Press, The CRC Series on Discrete Mathematics and Its Applications, 1995.

[74] Wan, D. Q. and Lidl, R., *Permutation polynomials of the form* $x^r f(x^{(q-1)/d})$ *and their group structure*, Monatshefte fur Mathematik **112** (1991), 149–163.

[75] Wang, L., *On permutation polynomials*, Finite Fields and their Applications **8** (2002), no. 1, 311–322.

[76] Wang, L. C., Yang, B., Hu, Y. and Lai, F., *A Medium- Field Multivariate Public key Encryption Scheme*, CT-RSA 2006: The Cryptographers Track at the RSA Conference 2006, LNCS **3860** (2006), 132–149.

[77] Wang, Q., *On inverse permutation polynomials*, Finite Fields and Their Applications **15** (2009), 58–70.

[78] Yuan, J., Ding, C., *Four classes of permutation polynomials of* $\mathbb{F}_{2^m}$, Finite Fields and Their Applications **13** (2007), 869–876.

[79] Yuan, J., Ding, C., Wang, H. , Pieprzyk, J., *Permutation polynomials of the form* $(x^p - x + \delta)^s + L(x)$, Finite Fields and Their Applications **14** (2007), 482–493.