

4-2016

Some Algebraic Aspect and Applications of a Family Of Functions over Finite Fields

Shaima Ahmed Thabet

Follow this and additional works at: https://scholarworks.uaeu.ac.ae/all_theses

Part of the [Mathematics Commons](#)

Recommended Citation

Thabet, Shaima Ahmed, "Some Algebraic Aspect and Applications of a Family Of Functions over Finite Fields" (2016). *Theses*. 454.
https://scholarworks.uaeu.ac.ae/all_theses/454

This Thesis is brought to you for free and open access by the Electronic Theses and Dissertations at Scholarworks@UAEU. It has been accepted for inclusion in Theses by an authorized administrator of Scholarworks@UAEU. For more information, please contact fadl.musa@uaeu.ac.ae.



United Arab Emirates University

College of Science

Department of Mathematical Sciences

SOME ALGABRAIC ASPECT AND APPLICATIONS OF A FAMILY
OF FUNCTIONS OVER FINITE FIELDS

Shaima Ahmed Thabet

This thesis is submitted in partial fulfillment of the requirements for the degree of
Master of Science in Mathematics

Under the Supervision of Dr. Adama Diene

April 2016

Declaration of Original Work

I, Shaima Ahmed Thabet, the undersigned, a graduate student at the United Arab Emirates University (UAEU), and the author of this thesis entitled “*Some Algebraic Aspect and Applications of a Family of Functions over Finite Fields*”, hereby, solemnly declare that this thesis is my own original research work that has been done and prepared by me under the supervision of Dr. Adama Diene, in the College of Science at UAEU. This work has not previously been presented or published, or formed the basis for the award of any academic degree, diploma or a similar title at this or any other university. Any materials borrowed from other sources (whether published or unpublished) and relied upon or included in my thesis have been properly cited and acknowledged in accordance with appropriate academic conventions. I further declare that there is no potential conflict of interest with respect to the research, data collection, authorship, presentation and/or publication of this thesis.

Student Signature: Sb

Date: 7-12-2016

Copyright© 2016 Shaima Ahmed Thabet
All Rights Reserved

Approval of the Master Thesis

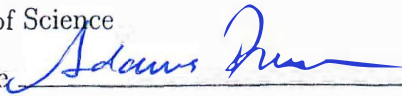
This Master Thesis is approved by the following Examining Committee Members:

1) Advisor (Committee Chair): Dr. Adama Diene

Title: Associate Professor

Department of Mathematical Sciences

College of Science

Signature  Date 1-05-2016

2) Member: Dr. Kanat Abdukhalikov

Title: Associate Professor

Department of Mathematical Sciences

College of Science

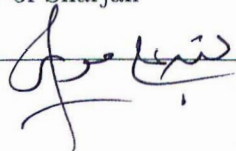
Signature  Date 1.05.2016

3) Member (External Examiner): Dr. Moussa Benoumhani

Title: Associate Professor

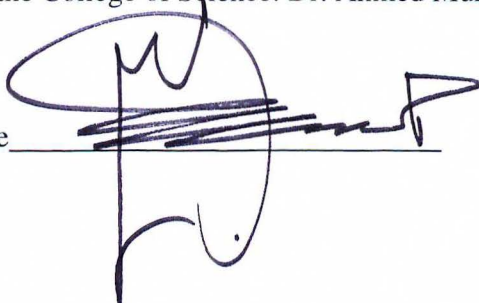
Department of Mathematics

Institution: University of Sharjah

Signature  Date 5-1-2016

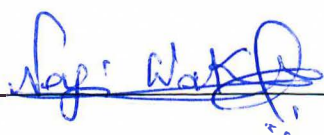
This Master Thesis is accepted by:

Dean of the College of Science: Dr. Ahmed Murad

Signature 

Date 8/12/2016

Dean of the College of the Graduate Studies: Professor Nagi T. Wakim

Signature 

Date 13/12/2016

Abstract

We study two families of functions over finite fields; the Multivalued Threshold Functions and the Multivariate Polynomials. Recent advances made in our conception and our understanding of Boolean Threshold Functions and Multivalued Threshold Functions have considerably increased the importance of the role that they play in our days in areas like cryptography, circuit complexity, learning theory, social choice, quantum complexity, and in many other areas. Theoretical aspects of Threshold Functions were first studied by Bovdi and Geche who gave an algebraic approach of Boolean Threshold Functions using group ring theory. We will present some algebraic properties of Boolean threshold functions. For the family of Multivariate Polynomials, it was first used by Matsumoto and Imai to design a cryptosystem. Many others researchers followed their steps with a design of new post quantum multivariate cryptosystems. Unfortunately, many of them have been proven insecure. We introduce in this thesis a new multivariate cryptosystem that supposes to resist quantum computers attacks.

Keywords: Multivalued Threshold Functions, Boolean Threshold Functions, Cryptosystem.

Title and Abstract (in Arabic)

بعض الجوانب الجبرية وتطبيقاتها على المجموعات المحدودة

الملخص

سوف ندرس عائلتين من الوظائف على المجموعات المحدودة. أولاً وظائف العتبة المتعددة القيم وكثيرات الحدود. مؤخرًا في تصورنا وفهمنا للمنطقية وظائف عتبة ومتعددة القيم وظائف عتبة ارتفعت بشكل ملحوظ على أهمية الدور الذي تقوم به في أيامنا هذه في مجالات مثل التشفير، دائرة التعقيد، نظرية التعلم، واختيار الاجتماعي والتعقيد الكمي، وفي العديد من المجالات الأخرى.

تمت دراسة الجوانب النظرية من وظائف عتبة أولاً من بوفي و Geche الذي قدم نهج جبري من وظائف عتبة منطقية باستخدام نظرية المجموعة. وسوف نقدم بعض نتائجها إلى وظائف عتبة متعددة القيم. العائلة متعدد المتغيرات، وقد تم استخدامها لأول مرة من قبل ماتسوموتو وايماي لتصميم نظام تشفير. يتبع العديد من الباحثين الآخرين خطواتهم مع تصميم نظم الترميز الجديدة متعدد المتغيرات. ولكن للأسف، وكثيراً منهم قد اثبت انها غير آمنة. ونحن نقدم في هذا العمل نظام تشفير متعدد المتغيرات الجديدة التي يفترض أن تقاوم الهجمات أجهزة الكمبيوتر.

مفاهيم البحث الرئيسية: المجموعات المحدودة، المجموعات كثيرات الحدود، التشفير.

Acknowledgements

My thanks go to Dr. Adama Diene whose enthusiasm about and introduction to Algebra got me started.

I would like to thank my committee for their guidance, support, and assistance throughout my preparation of this thesis. I would like to thank the chair and all members of the Department of Mathematics at the United Arab Emirates University for assisting me all over my studies and research. My special thanks are extended to the Library Research Desk for providing me with the relevant reference materials.

Special thanks go to my father, mother, husband, brother, and sisters who helped me along the way. I am sure they suspected it was endless.

Dedication

To my beloved parents and family

Table of Contents

Title	i
Declaration of Original Work	ii
Copyright	iii
Approval of the Master Thesis	iv
Abstract	vi
Title and Abstract (in Arabic)	vii
Acknowledgements	viii
Dedication	ix
Table of Contents	x
Chapter 1: Introduction	1
Chapter 2: Preliminaries.....	4
2.1 Finite Field	4
2.1.1 Definitions and Examples	4
2.1.2 Basic Properties of Finite Fields	5
2.1.3 Construction of Finite Fields.....	9
2.2 Functions from F_q^n to F_q	10
2.3 Multivariate Cryptosystems	11
2.4 The Matsumoto-Imai Cryptosystem	12
2.5 Patarin Linearization Equations Attack on the <i>MI</i> Cryptosystem.....	17
2.6 Oil-Vinegar Scheme.....	18
2.7 Polynomial Type of Oil-Vinegar	21
Chapter 3: Some Algebraic Aspects of Threshold Functions	29
3.1 Group Ring.....	29
3.2 Threshold Functions.....	29
Chapter 4: Conclusion.....	34
References	35

Chapter 1: Introduction

Let p be a prime, $q = p^e$ for some integer e , F_q the finite field with q elements, and F_{q^n} an extension of degree n of F_q . It is well-known that any function $f: F_{q^n} \rightarrow F_q$ is a polynomial function. More precisely, every function from F_{q^n} to F_q (or from F_q^n to F_q) can be uniquely represented as a polynomial in $F_q[x_1, \dots, x_n]$ in which the degree of each x_i is at most $q - 1$. In particular, every function from F_{q^n} to F_q is uniquely represented by a polynomial of degree $q - 1$ in $F_q[X]$. Functions or polynomials over finite fields have many important applications in today's life. In this thesis, we will study two families of functions or polynomials over finite fields: the multivariate polynomials and the threshold functions. Both families of polynomials play a very important role in nowadays in area like cryptography, circuit complexity leaning theory, and many other areas.

The first part (section 3) of this thesis deals with the family of multivariate polynomials over finite fields and their applications to cryptography known as Multivariate Quadratic Cryptosystem. This family of cryptosystem was first introduced in 1988 by Matsumoto and Imai with their milestone scheme named *MI* or C^* [14] cryptosystem. *MI* was known to be very efficient with a lot of potential practical applications and an alternative to number theory based cryptosystems such as RSA, El Gamal, and others. Unfortunately, it was broken by Patarin linearization equations attack in 1995. But the ideas used in designing *MI* and its good potentiality for storage and efficiency attracted many researchers to explore this new family of cryptosystems. That is how, shortly after proving the insecurity of *MI*, Patarin designed a new scheme called Hidden Field Equation cryptosystem (HFE) [15] in 1996. Unluckily, HFE was also proven insecure by the Kipnis-Shamir method [12]. In 1997 Patarin explored the idea of linearization equations attack to design a signature algorithm named (balanced) Oil-Vinegar scheme (OV) [16]. But in 1998 Kipnis and Shamir introduced the separation method to prove OV insecure and soon after, in 1999 they proposed a modified scheme of OV called Unbalanced Oil-Vinegar signature scheme (UOV) [13]. UOV is still considered today secure if parameters are

chosen carefully. It is proven very vulnerable to some attacks for many choices of parameters. Many other schemes obtained by modifying the UOV, *MI* and HFE were after proposed. We can name Sflash [1], C[18], PMI [4], PMI+ [5], HFE[15], IPHFE [7], HFE_v [7, 18] and Quartz [17] among this family of cryptosystems.

The most important thing of building Multivariate Public Key Cryptosystem (MPKC) is how to find a good polynomial system F that makes the cryptosystem secure and efficient. The security of MPKC is based on the knowledge that solving a set of multivariate polynomial equations over finite field is in general proven to be an NP-hard problem. However, this fact does not guarantee the security and most of these schemes based on Multivariable Quadratic Equations (MQE) over finite fields suggested in the last three decades were broken (see [25]). Apparently, the broken systems were based on some hidden structure, which on one hand enabled the efficient invertibility of the system, but on the other hand was found to be vulnerable to algebraic attacks. Almost all the MQE based encryption schemes proved to be insecure share the common defect that some quadratic forms associated to their central maps have low rank (see [20]) and therefore are vulnerable to the Min-Rank Attack (see [11]). On the other hand, the belief that random quadratic systems are hard to solve on average (see [1], [14] and references therein), points towards designing trap-door primitives based on randomness, which raises difficulties in designing immune invertible primitives. Little was done in this direction in the context of asymmetric public-key cryptography (see [14]).

Recently, researchers propose some new multivariate cryptosystems, such as Huang-Liu-Yang-2012 scheme [11], Yasuda-Takagi-Sakurai-2013 scheme [23], Gao-Heindl-2013 scheme [22], ABC [20], matrix-based Rainbow [21], Zhang-Tan-2014 scheme [26], NT-Rainbow [23], Yasuda-Takagi-Sakurai-2014 scheme [24], cubic-ABC [6] and ZHFE [19]. However, we need more time to verify their securities.

In this thesis, we introduce a polynomial type of the OV schemes which has a much higher security as its construction is completely based on randomly chosen multivariate polynomials. In general, Multivariate Public Key Cryptosystems have the following structure. Let k be a finite field with q elements. A public key is a map \bar{F} :

$k^n \longrightarrow k^n$ constructed as $\bar{F} = L_1 \circ F \circ L_2$, where L_1 and L_2 are two random invertible transformations over k^m and k^n respectively. The central map $F : k^n \longrightarrow k^m$ is nonlinear multivariate polynomial map that has the property of being invertible computation-wise.

In the second part of this thesis (section 4), we will study the family of threshold functions over a finite field. It was initially studied by Bovdi and Geche who gave an algebraic approach of boolean threshold functions using group ring theory. A threshold function is a Boolean function $f: \{0,1\} \longrightarrow \{0,1\}$ such that there exist real numbers w_1, w_2, \dots, w_n and A , satisfying:

$$f(x_1, x_2, \dots, x_n) = 1 \text{ if and only if } \sum_{i=1}^n w_i x_i \geq A.$$

vector $\vec{w} = \langle w_1, w_2, \dots, w_n \rangle$ is called weight vector and A is the threshold value. A threshold function can be easily extended to multivalued threshold functions

follows: $f : \mathbb{Z}_p^n \longrightarrow \mathbb{Z}_p$

$$f(x) = \begin{cases} 0 & X \cdot w^T < A_1 \\ 1 & A_1 \leq X \cdot w^T < A_2 \\ \cdot & \cdot \\ \cdot & \cdot \\ p-1 & X \cdot w^T > A_{p-1} \end{cases}$$

Different aspects of threshold functions have been studied extensively, many but the first algebraic approach was done in [13], where the authors established a connection between threshold functions and fundamental ideals of group rings. Then in [13], the authors determine the invariance groups of threshold functions and in some lattices induced by threshold functions are introduced. We will revisit these findings for boolean threshold functions in chapter 3.

Chapter 2: Preliminaries

2.1 Finite Field

2.1.1 Definitions and Examples

Definition 2.1.1 Let F be a set with two binary operations, addition denoted by $+$ and multiplication denoted by \cdot , F is called a field with respect to the addition and the multiplication if the following hold:

F1 $(F, +)$ is an abelian group.

F2 (F^*, \cdot) is an abelian group, where $F^* = F \setminus \{0\}$ and 0 is the zero of the group $(F, +)$.

F3 $a(b + c) = ab + ac$ for all $a, b, c \in F$.

We also say that $(F; +, \cdot)$ is a field. $(F, +)$ is called the additive group of the field and (F^*, \cdot) is called the multiplicative group of F .

A field with finitely many elements is called a finite field. We denote a finite field with q elements by F_q .

The identity of $(F, +)$ is denoted by 0 and the identity of (F^*, \cdot) by 1 .

Example 2.1.2 Z_p , where p is prime, consists of p residue classes

$$\bar{a} = a + p\mathbb{Z}_p = \{a + pk : k \in \mathbb{Z}\}, \quad a = 0, 1, 2, \dots, p - 1.$$

The addition and the multiplication are defined by: for any $\bar{a}, \bar{b}, \bar{c} \in Z_p$, we have

$$\bar{a} + \bar{b} = \overline{a + b},$$

$$\bar{a} \cdot \bar{b} = \overline{ab}$$

$(Z_p, +)$ and (Z_p^*, \cdot) are both abelian groups and for any $\bar{a}, \bar{b}, \bar{c} \in Z_p$, we have

$$\bar{a}(\bar{b} + \bar{c}) = \overline{a(\bar{b} + \bar{c})} = \overline{a(b + c)}$$

$$= \overline{ab} + \overline{ac} = \bar{a}\bar{b} + \bar{a}\bar{c}.$$

Thus, F1, F2, and F3 are satisfied and Z_p is a finite field.

2.1.2 Basic Properties of Finite Fields

The proof of the following theorem can be found in [30].

Theorem 2.1.3 *Let F_q be a finite field with q elements. Then $a^{q-1} = 1$ for all $a \in F_q^*$.*

Corollary 2.1.4 *Let F_q be a finite field with q elements and E be a finite field which contains F_q as a subfield. Then $a^q = a$ for all $a \in F_q$ and moreover, for any $\alpha \in E$, $\alpha^q = \alpha$ implies $\alpha \in F_q$.*

Proof. It follows from Theorem 2.1.3 that $a^q = a$ for all $a \in F_q$. Since $x^q - x$ has at most q roots in E , the q elements of F_q are all the roots of $x^q - x$ in E . Now if $\alpha^q = \alpha$ for all $\alpha \in E$, α is a root of $x^q - x$. Therefore α must be one of the elements of F_q , i.e., $\alpha \in F_q$. ■

Theorem 2.1.5 *The multiplicative group F_q^* of any finite field F_q is cyclic. A generator of F_q^* is called a primitive element of F_q .*

Proof. Let F_q be a finite field with q elements and F_q^* be its multiplicative group. F_q^* is of order $q-1$. We know that the order of every element of F_q^* is a divisor of $q-1$. Let d be a positive divisor of $q-1$. Denote by $\varphi(d)$ the number of elements of order d in F_q^* . Clearly,

$$\sum_{d|(q-1), d > 0} \varphi(d) = q - 1. \quad (1)$$

Assume that $\varphi(d) > 0$, then there is an element of order d in F_q^* . Let a be such an element, then the cyclic group $\langle a \rangle$ generated by a is of order d and every element in $\langle a \rangle$ satisfies the polynomial $x^d - 1 = 0$. Let b be any element of order d in F_q^* , then b satisfies also $x^d - 1 = 0$. Since the number of distinct roots of $x^d - 1$ in F_q is at most d , we must have $b = a^i$ for some i , $1 \leq i \leq d-1$. Thus $b \in \langle a \rangle$. Since the number of elements of order d in $\langle a \rangle$ is $\phi(d)$, where ϕ is the Euler function. We have

proved that

$$\varphi(d) = 0 \text{ or } \phi(d). \quad (2)$$

By Theorem 2.1.5,

$$\sum_{d|(q-1)} \phi(d) = q - 1. \quad (3)$$

From (1) (2) and (3) we deduce $\varphi(d) = \phi(d)$ for all positive divisors d of $q - 1$. In particular, $\varphi(q - 1) = \phi(q - 1) > 0$. That is, there is an element of order $q - 1$ in F_q^* . Hence F_q^* is cyclic. ■

Definition 2.1.6 *Let F be a field and n be a positive integer such that $nx = 0$ for all $x \in F$, we call the least such integer the characteristic of F and we write $\text{Char}F = n$, and we say F has positive characteristic. On the other hand if $nx \neq 0$ for all n , we say that $\text{Char}F = 0$.*

The proof of the next theorem can be found in [30].

Theorem 2.1.7 *Let F_q be a finite field of characteristic p , then the number of elements of F must be a power of p .*

Theorem 2.1.8 *Let F be a finite field which contains a subfield F_q with q elements, then the number of elements of F must be a power of q .*

Proof. Rewrite F_q as F_1 . If $F = F_1$, then F is a finite field containing exactly q elements. Hence our theorem holds. If $F \neq F_1$, then F will contain e_2 and $e_2 \notin F_1$. Let $F_2 = \{a_1 + a_2e_2 : a_1, a_2 \in F_1\}$. We will prove: if $a_1 + a_2e_2 = b_1 + b_2e_2$ with $a_1, a_2, b_1, b_2 \in F_1$, then $a_1 = b_1, a_2 = b_2$. In fact, from this equation it follows that $(a_2 - b_2)e_2 = b_1 - a_1$. If $a_2 \neq b_2$ then $e_2 = (a_2 - b_2)^{-1}(b_1 - a_1) \in F$. A contradiction follows. Hence we must have $a_1 = b_1$ and $a_2 = b_2$. Therefore F_2 contains exactly q^2 distinct elements. If $F = F_2$, then F is a finite field with exactly

q^2 elements. So our theorem holds. If $F \neq F_2$, then F will contain e_3 and $e_3 \notin F_2$. Let $F_3 = \{a_1 + a_2e_2 + a_3e_3 : a_1, a_2, a_3 \in F_1\}$. Assume that

$$a_1 + a_2e_2 + a_3e_3 = b_1 + b_2e_2 + b_3e_3 \text{ with } a_1, a_2, a_3, b_1, b_2, b_3 \in F_1.$$

Then

$$(a_3 - b_3)e_3 = (b_1 - a_1) + (b_2 - a_2)e_2.$$

If $a_3 \neq b_3$, then

$$e_3 = (a_3 - b_3)^{-1}(b_1 - a_1) + (a_3 - b_3)^{-1}(b_2 - a_2)e_2 \in F_2.$$

This is contradiction. Hence we must have $a_3 = b_3$. Then we have $a_1 + a_2e_2 = b_1 + b_2e_2$, which, by the above proof, yields $a_1 = b_1, a_2 = b_2$. Therefore, we conclude that F_3 contains exactly q^3 distinct elements. If $F = F_3$, then F is a finite field with exactly q^3 elements. So our theorem holds. If $F \neq F_3$, then F will contain e_4 and $e_4 \notin F_3$. Let $F_4 = \{a_1 + a_2e_2 + a_3e_3 + a_4e_4 : a_1, a_2, a_3, a_4 \in F_1\}$. Similarity it can be proved that F_4 contains exactly q^4 distinct elements. Continue in this way. If the number of elements in F is N and $q^n \leq N < q^{n+1}$, then a sequence of subset $F_1, F_2, F_3, \dots, F_n$ is obtained, where $F_i = \{a_1 + a_2e_2 + \dots + a_ie_i : a_1, a_2, \dots, a_i \in F_1\}$. $e_2 \notin F_1, e_3 \notin F_2, \dots, e_n \notin F_{n-1}$, and $F_i (1 \leq i \leq n)$ contains exactly q^i distinct elements. If $F \neq F_n$, then F will contain an element e_{n+1} and $e_{n+1} \notin F_n$. Let $F_{n+1} = \{a_1 + a_2e_2 + \dots + a_n e_n : a_1, a_2, \dots, a_n \in F_n\}$. In similar way one can prove that F_{n+1} contains exactly q^{n+1} distinct elements. But $F_{n+1} \subset F$, the number of elements in F is N , and $N < q^{n+1}$. this is impossible. Hence $F = F_n$. So F is a finite field which contains exactly q^n elements. ■

Theorem 2.1.9 *Let p be a prime number and n be a positive integer, then there exists a finite field which contains exactly p^n elements.*

Proof. Let $\Phi_{p,n}$ be the product of all monic irreducible polynomials of degree n in $F_p[x]$. If p is a prime number and n a positive integer, then $\Phi_{p,n} > 0$. Thus there always exists a monic irreducible polynomial of degree n over the prime field

Z_p with p elements. Let $p(x)$ be one of them. Then $Z_p[x]/(p(x))$ is a finite field with p^n elements. ■

Let q be a power of a prime p and n a positive integer. We may view F_q as a subfield of F_{q^n} . The map $\sigma : \alpha \mapsto \alpha^q$ from F_{q^n} to itself is an automorphism, which leaves every element of F_q fixed, i.e., $\sigma(\alpha) = \alpha$ for every $\alpha \in F_q$. We call σ the Frobenius automorphism of F_{q^n} over F_q . If we denote by σ^2 the composition $\sigma \circ \sigma$, then $\sigma^n = 1, \sigma^k \neq 1$ for $1 \leq k < n$, and $\sigma^0 = 1, \sigma^1 = \sigma, \dots, \sigma^{n-1}$ are n distinct automorphisms of F_{q^n} over F_q .

Theorem 2.1.10 *Let σ be the Frobenius automorphism of F_{q^n} over F_q and $\tilde{\sigma}$ be an extended automorphism of σ to the polynomial ring $F_{q^n}[x]$. Let $f(x) \in F_{q^n}[x]$. If $\tilde{\sigma}(f(x)) = f(x)$, then $f(x) \in F_q[x]$.*

Proof. Let $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \dots + \alpha_m x^m$. Then $\tilde{\sigma}(f(x)) = \sigma(\alpha_0) + \sigma(\alpha_1)x + \sigma(\alpha_2)x^2 + \dots + \sigma(\alpha_m)x^m$. From $\tilde{\sigma}(f(x)) = f(x)$. We deduce $\sigma(\alpha_i) = \alpha_i$ for $i = 0, 1, 2, \dots, m$. But we also have $\sigma(\alpha_i) = \alpha_i^q$. Therefore $\alpha_i^q = \alpha_i$ and $\alpha_i \in F_q$ for $i = 0, 1, 2, \dots, m$. Hence $f(x) \in F_q[x]$. ■

Theorem 2.1.11 *$\text{Gal}(F_{q^n}/F_q) = \langle \sigma \rangle$. More precisely, $\sigma^0 = 1, \sigma^1 = \sigma, \dots, \sigma^{n-1}$ are all automorphisms of F_{q^n} over F_q .*

Proof. Let ξ be a primitive element of F_{q^n} and let

$$\begin{aligned} f(x) &= (x - \xi)((x - \sigma(\xi)) \dots (x - \sigma^{n-1}(\xi))) \\ &= x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n, \end{aligned}$$

Clearly,

$$\tilde{\sigma}(x - \sigma^i(\xi)) = x - \sigma^{i+1}(\xi) \text{ for } i = 0, 1, 2, \dots, n-2$$

and $\tilde{\sigma}(x - \sigma^{n-1}(\xi)) = x - \sigma^n(\xi) = x - \xi$. Thus $\tilde{\sigma}(f(x)) = f(x)$. From the above theorem, $f(x) \in F_q[x]$, i.e., $a_k \in F_q$ for $k = 0, 1, 2, \dots, n$.

Let τ be an automorphism of F_{q^n} over F_q and suppose that $\tau(\xi) = \xi^i$ where $1 \leq i \leq q^n - 2$. Clearly, $f(\xi) = 0$, i.e., $\xi^n + a_1 \xi^{n-1} + \dots + a_{n-1} \xi + a_n = 0$. Applying

the automorphism τ to the above equation we obtain

$$(\xi^i)^n + a_1(\xi^i)^{n-1} + \dots + a_{n-1}\xi^i + a_n = 0,$$

i.e., $f(\xi^i) = 0$. But $f(x)$ has n roots $\xi, \sigma(\xi), \dots, \sigma^{n-1}(\xi)$ in F_{q^n} . Thus ξ^i must be one of them. Say $\xi^i = \sigma^j(\xi), 0 \leq j \leq n-1$, then $\tau(\xi) = \xi^i = \sigma^j(\xi)$, which implies $\tau(\alpha) = \sigma^j(\alpha)$ for all $\alpha \in F_{q^n}$. Hence $\tau = \sigma^j$. ■

2.1.3 Construction of Finite Fields

Theorem 2.1.12 *Let E be a field, F be a subfield of E , and α be any element of E . Then $F[\alpha]$ is a subring of E and is an integral domain; moreover, $F(\alpha)$ is a subfield of E .*

Proof. Let $f(x), g(x) \in F[x]$, then $f(x) - g(x), f(x)g(x) \in F[x]$. It follows that $f(\alpha) - g(\alpha), f(\alpha)g(\alpha) \in F[\alpha]$. Clearly, $1 \in F[\alpha]$. Therefore $F[\alpha]$ is a subring of E . Since F is a subfield of E , $F[\alpha]$ is an integral domain. Similarly, we can show that $F(\alpha)$ is a subfield of E . ■

The proof of the following theorem can be found in [30]

Theorem 2.1.13 *Let E be a field, F be a subfield of E , and α be any element of E . If $p(x)$ is an irreducible polynomial of degree n over F satisfying $p(\alpha) = 0$. Then $F(\alpha)$ is a subfield of E .*

Theorem 2.1.14 *Let F be a field and $p(x)$ is an irreducible polynomial of degree n over F . If we denote the residue class of $x \pmod{p(x)}$ by α . Then*

$$F[x]/(p(x)) \cong F[\alpha] = F(\alpha)$$

Moreover, if F is a finite field with q elements then $|F[x]/(p(x))| = q^n$.

Example 2.1.15 Consider $F_2 = \{0, 1\}$, and $f(x) = x^2 + x + 1$. Since the degree of f is 2 and since $f(0) = 1 \neq 0$ and $f(1) = 1 \neq 0$, f has no root in F_2 . Therefore f is irreducible in F_2 . So $F_2[x]/(f(x))$ is a field. If α is a root of f we know that $F_2[x]/(f(x))$ is isomorphic to $F_2(\alpha)$ and the degree $[F_2(\alpha) : F_2] = \deg f = 2$. We have $F_2[x]/(f(x)) = F_2(\alpha) = \{a + b\alpha : a, b \in F_2\} = \{0, 1, \alpha, \alpha^2 = 1 + \alpha\}$ which is a field of 4 elements. We can identify it with F_4 , i.e., $F_2(\alpha) \cong F_4$. The tables of addition and multiplication are as follows:

+	0	1	α	$\alpha + 1$
0	0	1	α	$\alpha + 1$
1	1	0	$\alpha + 1$	α
α	α	$\alpha + 1$	0	1
$\alpha + 1$	$\alpha + 1$	α	1	0

*	0	1	α	$\alpha + 1$
0	0	0	0	0
1	0	1	α	$\alpha + 1$
α	0	α	$\alpha + 1$	1
$\alpha + 1$	0	$\alpha + 1$	1	α

2.2 Functions from F_q^n to F_q

Let $n \geq 0$ be an integer and let $F(F_q^n, F_q)$ denote the set of all functions from F_q^n to F_q . Clearly, $F(F_q^n, F_q)$ is an F_q -algebra. A property particular to finite fields is that every function in $F(F_q^n, F_q)$ is a polynomial function. Let $F_q[X_1, \dots, X_n]$ be the polynomial ring in X_1, \dots, X_n over F_q . Each element $f(X_1, \dots, X_n) \in F_q[X_1, \dots, X_n]$ gives rise to a function

$$\begin{aligned} \bar{f}: F_q^n &\longrightarrow F_q \\ (a_1, \dots, a_n) &\longrightarrow f(a_1, \dots, a_n) \end{aligned}$$

Clearly, $\bar{(\)} : f \mapsto \bar{f}$ is an F_q -algebra homomorphism from $F_q[X_1, \dots, X_n]$ to $F(F_q^n, F_q)$. The homomorphism $\bar{(\)} : F_q[X_1, \dots, X_n] \longrightarrow F(F_q^n, F_q)$ is onto. This claim follows from the Lagrange interpolation. For each $(a_1, \dots, a_n) \in F_q^n$, define

$$f(a_1, \dots, a_n) = \prod_{i=1}^n \prod_{b \in F_q \setminus \{a_i\}} \frac{X_i - b}{a_i - b} \in F_q[X_1, \dots, X_n].$$

$$\bar{f}_{(a_1, \dots, a_n)}(b_1, \dots, b_n) = \begin{cases} 1 & \text{if } (b_1, \dots, b_n) = (a_1, \dots, a_n), \\ 0 & \text{if } (b_1, \dots, b_n) \neq (a_1, \dots, a_n), \end{cases}$$

So, $\bar{f}_{(a_1, \dots, a_n)}, (a_1, \dots, a_n) \in F_q^n$, form a basis of $F(F_q^n, F_q)$. Consequently, $\bar{()}: F_q[X_1, \dots, X_n] \longrightarrow F(F_q^n, F_q)$ is onto.

Theorem 2.2.1 *The homomorphism $\bar{()}: F_q[X_1, \dots, X_n] \longrightarrow F(F_q^n, F_q)$ induces an F_q -algebra isomorphism $F_q[X_1, \dots, X_n]/(X_i^q - X_i, \dots, X_n^q - X_n) \cong F(F_q^n, F_q)$, where $(X_i^q - X_i, \dots, X_n^q - X_n)$ is the ideal of $F_q[X_1, \dots, X_n]$ generated by $X_i^q - X_i, \dots, X_n^q - X_n$.*

Proof. Since $a^q - a = 0$ for all $a \in F_q$, it is clear that $(X_i^q - X_i, \dots, X_n^q - X_n) \subset \text{Ker}(\bar{()})$. Thus $\bar{()}$ induces an onto homomorphism

$$\theta: F_q[X_1, \dots, X_n]/(X_i^q - X_i, \dots, X_n^q - X_n) \longrightarrow F(F_q^n, F_q).$$

However, $\dim_{F_q} F_q[X_1, \dots, X_n]/(X_i^q - X_i, \dots, X_n^q - X_n) = q^n = \dim_{F_q} F(F_q^n, F_q)$. (The first equal sign holds in the above since $X_1^{e_1} \dots X_n^{e_n}$, $0 \leq e_i \leq q-1$, $1 \leq i \leq n$, form a basis of $F_q[X_1, \dots, X_n]/(X_i^q - X_i, \dots, X_n^q - X_n)$. Therefore θ is an isomorphism.

■

The concrete meaning of the theorem is that every function from F_q^n to F_q can be uniquely represented as a polynomial in $F_q[X_1, \dots, X_n]$ in which the degree of each X_i is at most $q-1$. In particular, every function from F_q to F_q is uniquely represented by a polynomial of degree $q-1$, in $F_q[X]$.

2.3 Multivariate Cryptosystems

The first such new idea was proposed by Matsumoto and Imai [Matsumoto and Imai, 1988]. Their key idea was to utilize both the vector space and the hidden field structure of k^n , where k is a finite field. More specifically, instead of searching for invertible maps over the vector space k^n directly, they looked for invertible maps on a field K , a degree n field extension of k , which can also be identified as an n -dimensional vector space over k . This map could then be transformed into an invertible

map over k^n . This cryptosystem, known as C^* or MI , attracted a lot of attention due to its high efficiency and potential use in practical applications. Unfortunately, MI was broken later in 1995 by Jacques Patarin using an algebraic attack that utilizes linearization equations. This method takes advantage of certain specific hidden algebraic structures in MI . But the new ideas used in its design opened the door to researchers to explore a new family of cryptosystem called Multivariate Quadratic Cryptosystems (MQC). Many new variants of the MI cryptosystems including the Sflash signature scheme [Akkar et al., 2003; Patarin et al., 2001], which was accepted in 2004 as one of the final selections for the New European Schemes for Signatures, Integrity, and Encryption project [NESSIE, 1999] for use in low cost smart cards were then proposed. Indeed, the work of Matsumoto and Imai has played a critical role as a catalyst in this new area and has stimulated the subsequent development. In this chapter, we will present the MI cryptosystem in detail, Patarin's cryptanalysis of MI , the family Oil-Vinegar signature scheme and some potential attacks. We will also introduce a new cryptosystem called Polynomial Type Oil Vinegar signature scheme; which can be conriveded as a generalization of the the OV schemes.

2.4 The Matsumoto-Imai Cryptosystem

Let k be a finite field with 2^e elements, for some positive integer e . Let $g(x)$ be an irreducible polynomial of degree n over k . Then $K = k[x]/g(x)$ is an extension of degree n of k . If we write

$$p(x) = \sum_{i=0}^{n-1} a_i x^i \quad \text{and} \quad \alpha \equiv x \pmod{p(x)},$$

then, as a vector space over k , K consists of all polynomials of degree $\leq n - 1$ in α with coefficients in k ; *i.e.*,

$$K = \left\{ \sum_{i=0}^{n-1} \alpha_i \alpha^i \mid \alpha_0, \alpha_1, \dots, \alpha_{n-1} \in k \right\}$$

Lemma 2.4.1 *The map $K \longrightarrow K$ defined by $X \longmapsto X^{2^e}$ is k -linear. And therefore*

the map $X \mapsto X^{2^{e\theta}+1}$ is quadratic.

Proof. Let X and Y be two elements of K , and a and b be two elements of k . Since $|k| = 2^q$, $a^{2^q} = a$ and $b^{2^q} = b$. Therefore

$$(aX + bY)^{2^{q\theta}} = (aX)^{2^{q\theta}} + (bY)^{2^{q\theta}} = a(X)^{2^{q\theta}} + b(Y)^{2^{q\theta}}. \blacksquare$$

Let $\phi : K \rightarrow k^n$ be defined by

$$\phi\left(\sum_{i=0}^{n-1} \alpha_i X^i\right) = (\alpha_0, \alpha_1, \dots, \alpha_{n-1})$$

Note that $\phi(a) = \phi(a, 0, \dots, 0) \quad \forall a \in k$ and ϕ is a k -linear map if we treat k as a subfield in K . Now choose θ such that $0 < \theta < n$ and $\gcd(2^{q\theta} + 1, 2^{qn} - 1) = 1$ where $\gcd(a, b)$ represents the greatest common divisor of a and b , and let $F : K \rightarrow K$ be defined by

$$F(X) = X^{2^{e\theta}+1}.$$

F is called the Matsumoto-Imai function. F is invertible if and only if $\gcd(2^{q\theta} + 1, 2^{qn} - 1) = 1$. In this case, $F^{-1} : K \rightarrow K$ is defined by

$$F^{-1}(X) = X^t$$

where t satisfies

$$t(2^{q\theta} + 1) \equiv 1 \pmod{(2^{qn} - 1)}.$$

We define $\tilde{F} : k^n \rightarrow k^n$ by

$$\tilde{F} = \phi \circ F \circ \phi^{-1} = (f_1, \dots, f_n), \quad \text{where } f_1, \dots, f_n \in k[x_1, \dots, x_n].$$

To finish the description of the construction of MI , let

$$\bar{F}(x_1, \dots, x_n) = L_1 \circ F \circ L_2(x_1, \dots, x_n) = (\bar{f}_1(x_1, \dots, x_n), \dots, \bar{f}_n(x_1, \dots, x_n)),$$

where $\bar{f}_1, \dots, \bar{f}_n \in k[x_1, \dots, x_n]$ and L_1, L_2 are invertible transformations over k^n . We can summarize the construction of MI with the following diagram.

$$k^n \xrightarrow{L_2} k^n \xrightarrow{\phi^{-1}} K \xrightarrow{\tilde{F}} K \xrightarrow{\phi} k^n \xrightarrow{L_1} k^n.$$

The Public Key

The public key of the MI consists of the following:

1. The field k including its additive and multiplicative structure
2. The n polynomials $\bar{f}_1, \dots, \bar{f}_n \in k[x_1, \dots, x_n]$

The Private key

The private key of the MI consists of the following:

1. L_1 and L_2 .
2. θ .

To encrypt a plaintext $\phi(X) = (x_1, x_2, \dots, x_n)$, we apply $\bar{f}_1, \dots, \bar{f}_n$ and obtain the ciphertext $\phi(Y) = (y_1, y_2, \dots, y_n)$. To decrypt, we use the two affine linear maps L_1 and L_2 , and we invert the composition map above and apply it to the ciphertext $\phi(Y) = (y_1, y_2, \dots, y_n)$ to get the plaintext $\phi(X) = (x_1, x_2, \dots, x_n)$. If the 2 affine linear maps L_1 and L_2 , are unknown, one must solve a system of n quadratic equations in n unknowns (x_1, x_2, \dots, x_n) . Since solving a system of n quadratic equations in n variables is believed to be an NP-hard problem, we conclude that for a large n encryption is an easy and fast process, while decryption without the secret key seems to be extremely hard. Therefore, the MI scheme was assumed to be a secure cryptosystem. Unfortunately, Patarin proved that this scheme is insecure under an algebraic attack [P] using the notion of linearization equations. We can summarize the encryption and decryption processes as follows:

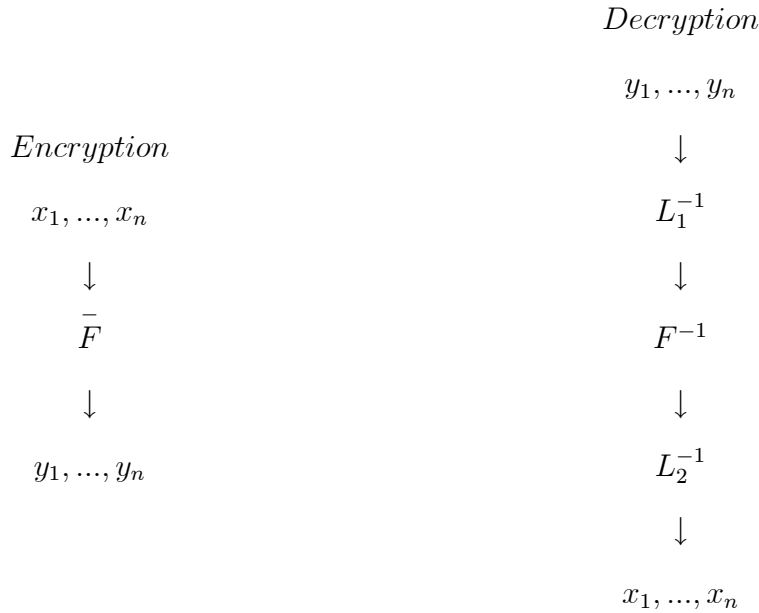
Encryption

Take the plaintext message (x_1, \dots, x_n) and find the associated ciphertext $(y_1, \dots, y_n) = \bar{f}_i(x_1, \dots, x_n)$, for $i = 1, \dots, n$

Decryption

We can decrypt the ciphertext (y_1, \dots, y_n) by executing the following steps:

1. First compute $(z_1, \dots, z_n) = L_1^{-1}(y_1, \dots, y_n)$;
2. Second compute $(\bar{z}_1, \dots, \bar{z}_n) = \phi \circ \tilde{F} \circ \phi^{-1}(z_1, \dots, z_n)$;
3. Finally compute $(x_1, \dots, x_n) = L_2^{-1}(\bar{z}_1, \dots, \bar{z}_n)$.



Example 2.4.2 Let $F_q = F_{2^2} = \{0, 1, \alpha, \alpha^2\}$, and $n=3$ an irreducible polynomial $f(x) = x^3+x+1$ over F_{2^2} . Let α be a root of $f \implies \alpha^3+\alpha+1 = 0$.

Next we choose θ such that $(2^\theta + 1, 2^n - 1) = 1$. We may choose $\theta = 2$. which implies $(2^\theta + 1, 2^3 - 1) = (5, 7) = 1$.

map \tilde{F} and its inverse are given by

$$\tilde{F}(X) = X^{1+4^2} \quad \text{and} \quad \tilde{F}^{-1}(X) = X^{2^6}.$$

Let L_1 and L_2 be given by

$$L_1(x_1, x_2, x_3) = \begin{pmatrix} \alpha^2 & \alpha & \alpha \\ \alpha & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ \alpha \end{pmatrix}$$

$$L_2(x_1, x_2, x_3) = \begin{pmatrix} 1 & 0 & \alpha \\ 0 & 1 & \alpha \\ 1 & \alpha & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} \alpha \\ \alpha^2 \\ \alpha^2 \end{pmatrix}$$

To derive the public key polynomial using the plaintext message variables x_1, x_2, x_3 we begin by computing $\phi^{-1} \circ L_2(x_1, x_2, x_3)$, which we find to be $(\alpha + x_1 + \alpha x_3) + (\alpha^2 + x_2 + \alpha x_3)\alpha + (\alpha^2 + x_1 + \alpha x_2)\alpha^2$. If we denote this expression by $X = (x_2 + x_3 + 1) + (x_1 + x_3 + 1)\alpha + (x_1 + x_2 + x_3 + 1)\alpha^2$. Then we compute $\tilde{F}(X) = X^{17}$, where $X^{17} = [(x_2 + x_3 + 1) + (x_1 + x_3 + 1)\alpha + (x_1 + x_2 + x_3 + 1)\alpha^2]^{17}$. $\tilde{F}(X) = 1 + \alpha^2 x_1 + \alpha x_2 + x_3 + x_1 x_2 + \alpha x_1 x_3 + \alpha^2 x_2 x_3 + (\alpha + \alpha x_1 + x_2 + \alpha^2 x_3 + x_1^2 + \alpha^2 x_1 x_2 + x_2^2 + x_2 x_3)x + (\alpha^2 + \alpha^2 x_1 + \alpha x_2 + \alpha x_2 + \alpha x_3 + x_1^2 + x_1 x_2 + \alpha x_1 x_3 + \alpha^2 x_2^2 + \alpha x_2 x_3 + \alpha^2 x_3^2)x^2$.

we compute $L_1 \circ \phi(X)$ to get the public key polynomials

$$\bar{f}_1(x_1, x_2, x_3) = 1 + x_3 + \alpha x_1 x_3 + \alpha^2 x_2^2 + \alpha^2 x_2^2 + \alpha^2 x_2 x_3 + x_3^2$$

$$\bar{f}_2(x_1, x_2, x_3) = 1 + \alpha^2 x_1 + \alpha x_2 + x_3 + x_1^2 + x_1 x_2 + \alpha^2 x_1 x_3 + x_2^2$$

$$\bar{f}_3(x_1, x_2, x_3) = \alpha^2 x_3 + x_1^2 + \alpha^2 x_2^2 + x_2 x_3 + \alpha^2 x_3^2,$$

Now, for the plaintext $(x'_1, x'_2, x'_3) = (1, \alpha, \alpha^2)$; we have

$$y'_1 = \bar{f}_1(1, \alpha, \alpha^2) = 0$$

$$y'_2 = \bar{f}_2(1, \alpha, \alpha^2) = 0$$

$$y'_3 = \bar{f}_3(1, \alpha, \alpha^2) = 1$$

Therefore, the corresponding ciphertext is $(0, 0, 1)$.

To decrypt, we first compute $L_1^{-1}(y'_1, y'_2, y'_3)$ and $\tilde{F}^{-1}(X)$. In deed, we have

$$L_1^{-1}(y'_1, y'_2, y'_3) = \begin{pmatrix} \alpha^2 & 1 & 1 \\ 1 & \alpha^2 & \alpha \\ \alpha^2 & 1 & 0 \end{pmatrix} \begin{pmatrix} y'_1 - 0 \\ y'_2 - 1 \\ y'_3 - \alpha \end{pmatrix}$$

Now if we apply the decryption algorithm, we obtain:

$$L_1^{-1}(0, 0, 1) = \begin{pmatrix} \alpha \\ \alpha \\ 1 \end{pmatrix}$$

$$X = \alpha + \alpha x + x^2$$

$$\text{and } \tilde{F}^{-1}(X) = X^t = X^{2^6} = \alpha + x^2$$

Now we have $(\bar{z}_1, \bar{z}_2, \bar{z}_3) = (\alpha, 0, 1)$

$$L_2^{-1}(y_1, y_2, y_3) = \begin{pmatrix} \alpha^2 & \alpha^2 & \alpha \\ \alpha & \alpha & \alpha \\ 1 & \alpha & 1 \end{pmatrix} \begin{pmatrix} y_1' - \alpha \\ y_2' - \alpha^2 \\ y_3' - \alpha^2 \end{pmatrix}$$

$$L_2^{-1}(\alpha, 0, 1) = (1, \alpha, \alpha^2)^T \text{ which is the plaintext } X.$$

2.5 Patarin Linearization Equations Attack on the MI Cryptosystem

Recall that for $X = \sum_{i=0}^{n-1} a_i x^i$, the central map of MI is given by $M : K \rightarrow K$

defined by $X \mapsto X^{2^{e\theta}}$. Assume that $M(X) = Y = \sum_{i=0}^{n-1} b_i y^i$, then we have

$$Y = X^{2^{e\theta}+1}.$$

By composing on each side of this equation with $g : X \mapsto X^{2^{e\theta}-1}$, we obtain

$$Y^{2^{e\theta}-1} = X^{2^{2e\theta}-1}.$$

Multiplying both sides by XY yield

$$XY^{2^{e\theta}} = YX^{2^{2e\theta}}.$$

$$XY^{2^{e\theta}} - YX^{2^{2e\theta}} = 0.$$

Now using $\phi(X) = (x_1, x_2, \dots, x_n)$, and $\phi(Y) = (y_1, y_2, \dots, y_n)$, and the fact that $X \mapsto X^{2^{e\theta}}$ and $Y \mapsto Y^{2^{e\theta}}$ are linear, we obtain

$$\sum_{i=0}^{n-1} a_i x_i + \sum_{i=0}^{n-1} b_i y_i + \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} c_{ij} x_i y_j + d = 0$$

Definition 2.5.1 For $X = \sum_{i=0}^{n-1} a_i x^i$ and $M : K \rightarrow K$ defined by $X \mapsto X^{2^{e\theta}}$, If

$M(X) = Y = \sum_{i=0}^{n-1} b_i y^i$, with $\phi(X) = (x_1, x_2, \dots, x_n)$, and $\phi(Y) = (y_1, y_2, \dots, y_n)$, an equation of the form

$$\sum_{i=0}^{n-1} a_i x_i + \sum_{i=0}^{n-1} b_i y_i + \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} c_{ij} x_i y_j + d = 0,$$

where a_i, b_i, c_{ij} , and d are in k is called a linearization equation for the y'_i s.

If enough plaintext-ciphertext (X, Y) are substituted in the linearization equations, we obtain a system of linear equations in $(n + 1)^2$ variables a_i, b_i, c_{ij} , and d that can be solved using Gaussian elimination to find the coefficients a_i, b_i, c_{ij} , and d . Knowing these coefficients, we can find any plaintext X given a ciphertext Y .

2.6 Oil-Vinegar Scheme

After defeating the proposed *MI* cryptosystem, Patarin exploited in 1997 the structure of the linearization equations attack to design a new signature scheme called Oil-Vinegar signature (OV). The basic building block for an OV scheme is the Oil-Vinegar polynomial. An Oil-Vinegar polynomial is a quadratic multivariate polynomial having $o + v = n$ variables, where o represents the number of oil variables and v the number of vinegar variables. The nonlinear terms occur only in the following two cases: between vinegar variables, or with one vinegar variable and one oil variable. In another words, there is no quadratic term with oil variables only. More precisely, we have the following definition.

Definition 2.6.1 Let k be a finite field with q elements, x_1, x_2, \dots, x_o be the o oil variables and x'_1, x'_2, \dots, x'_v the v vinegar variables. An Oil-Vinegar polynomial is

any total degree two polynomial $f \in k[x_1, x_2, \dots, x_o, x'_1, x'_2, \dots, x'_v]$ of the form

$$f = \sum_{i=1}^o \sum_{j=1}^v a_{ij} x_i x'_j + \sum_{i=1}^v \sum_{j=1}^v b_{ij} x'_i x'_j + \sum_{i=1}^o c_i x_i + \sum_{j=1}^v d_j x'_j + e$$

where $a_{ij}, b_{ij}, c_i, d_j, e \in k$.

Example 2.6.2 $f(x, y, z) = xy + 2xz + 3y^2 + 4yz + 5z^2 + 6x + 7y + 8z + 9$

is an oil and vinegar polynomial over the finite field F_{11} with the oil variable x and vinegar variables y, z . In this case, $o = 1, v = 2$ and $n = o + v = 3$. There is no quadratic term of the form x^2 . The nonlinear terms are $xy, 2xz, 3y^2, 4yz$ and $5z^2$. For these nonlinear terms, $3y^2, 4yz, 5z^2$ are among the first case with only with vinegar variable related. The remaining $xy, 2xz$ are among the second case with one vinegar variable and one oil variable. We can also represent f in a matricial form as following, Let

$$A = \begin{pmatrix} 0 & 1 & 2 & 6 \\ 0 & 3 & 4 & 7 \\ 0 & 0 & 5 & 8 \\ 0 & 0 & 0 & 9 \end{pmatrix}, \quad X = \begin{pmatrix} x \\ y \\ z \\ 1 \end{pmatrix}$$

the polynomial $f(x, y, z)$ can be rewritten as $X^T A X$.

Note 1: it is also called an unbalanced oil and vinegar polynomial over F_{11} , as $o < v$.

Note 2: it also can be viewed as an oil and vinegar polynomial over the real field

Definition 2.6.3 A polynomial map $F : k^n \longrightarrow k^o$ of the form

$$F(x_1, \dots, x_o, x'_1, \dots, x'_v) = (f_1, f_2, \dots, f_o),$$

where $f_1, f_2, \dots, f_o \in k[x_1, x_2, \dots, x_o, x'_1, x'_2, \dots, x'_v]$ are Oil-Vinegar polynomials is called an Oil-Vinegar map.

The public key for the OV schemes is a map $\bar{F} = F \circ L$, where F is an Oil-Vinegar map and L is an invertible linear map. The composition by L is done in order to mix the oil and the vinegar variables together. The private key is L . There is no need to compose with a second linear transformation on the left for the OV. These schemes are designed only for signature. They are not suitable for encryption.

To sign a message $Y = (y_1, y_2, \dots, y_o)$, we need to find a vector $W = (w_1, w_2, \dots, w_n)$

such that $\bar{F}(W) = Y$. To do so, we first choose v random values for the vinegar variables x'_1, x'_2, \dots, x'_v , and we substitute in the system to get o linear equations in the o variables x_1, x_2, \dots, x_o . This linear system has a high probability of having a solution. If it does not, we change the values of the vinegar variables x'_1, x'_2, \dots, x'_v and we try again until a solution in k^o is found. Then we apply L^{-1} . To verify if W is a signature for Y , it suffices to check if $\bar{F}(W) = Y$.

Example 2.6.4 Let $k = F_2 = (\{0; 1\}; +; \times)$,

$$o = 2, v = 2$$

The polynomial mapping $F = (f_1, f_2, f_3, f_4)$ is the following,

$$\begin{aligned} f_1(x_1, x_2, \bar{x}_1, \bar{x}_2) &= \bar{x}_1^2 + \bar{x}_1\bar{x}_2 + \bar{x}_2^2 + x_1\bar{x}_1 + x_2\bar{x}_1 + x_2\bar{x}_2 + x_1 + \bar{x}_2 \\ f_2(x_1, x_2, \bar{x}_1, \bar{x}_2) &= \bar{x}_1^2 + x_1\bar{x}_1 + x_2\bar{x}_1 + x_1 + x_2 + \bar{x}_1 + 1 \\ f_3(x_1, x_2, \bar{x}_1, \bar{x}_2) &= \bar{x}_1^2 + \bar{x}_1\bar{x}_2 + x_1\bar{x}_1 + x_2 + x_1 + x_2\bar{x}_2 \\ f_4(x_1, x_2, \bar{x}_1, \bar{x}_2) &= \bar{x}_1 + x_1\bar{x}_1 + \bar{x}_2 + x_2 + \bar{x}_2^2 \end{aligned}$$

The public key is $\{f_1, f_2, f_3, f_4\}$. To sign a document (y_1, y_2, y_3, y_4) we need to assign to vinegar variable arbitrary value ($\bar{x}_1 = 0, \bar{x}_2 = 1$), and solve the linear system

$$\begin{cases} x_1 + x_2 = y_1 \\ x_2 + 1 = y_2 \\ x_1 = y_3 \\ x_2 = y_4 \end{cases}$$

The solution of the system is $x_1 = 1, x_2 = 1$

Therefore the signature of the message $(0, 0, 1, 1)$, is $(1, 1)$.

2.7 Polynomial Type of Oil-Vinegar

In this section, we introduced a new multivariate signature called polynomial oil-vinegar. It can be viewed as generalization of the OV schemes. Let $n, m, s \in \mathbb{Z}$ be positive integers satisfying $m = s^2$ and $n = 2m$. For a given integer s , let k^s denote the set of all s -tuples of elements of k . We denote the plaintext by $(x_1, x_2, \dots, x_n) \in k^n$ and the ciphertext by $(y_1, y_2, \dots, y_m) \in k^m$. The polynomial ring with n variables in k will be denoted by $k[x_1, \dots, x_n]$. Let $L_1 : k^n \rightarrow k^n$ and $L_2 : k^m \rightarrow k^m$ be two linear transformations, i.e.

$$\mathcal{L}_1(x) = L_1x \quad \text{and} \quad \mathcal{L}_2(y) = L_2y,$$

where L_1 and L_2 are respectively an $n \times n$ matrix and an $m \times m$ matrix with entries in k , $x = (x_1, x_2, \dots, x_n)^t$, $y = (y_1, y_2, \dots, y_m)^t$, and t denote the matrix transposition.

The Central map Let

$$P = \begin{pmatrix} p_1(x)p'_1(x) & p_2(x)p'_2(x) & \dots & p_s(x)p'_s(x) \\ p_{s+1}(x)p'_{s+1}(x) & p_{s+2}(x)p'_{s+2}(x) & \dots & p_{2s}(x)p'_{2s}(x) \\ \vdots & \vdots & \ddots & \vdots \\ p_{(s-1)s+1}(x)p'_{(s-1)s+1}(x) & p_{(s-1)s+2}(x)p'_{(s-1)s+2}(x) & \dots & p_{s^2}(x)p'_{s^2}(x) \end{pmatrix}; \quad M = \begin{pmatrix} A_{2 \times 2} & B_{2 \times k} \\ C_{l \times 2} & D_{l \times k} \end{pmatrix};$$

and $N = \begin{pmatrix} n_1 & \dots & n_s \\ n_{s+1} & n_{2s} & \\ \vdots & \vdots & \ddots & \vdots \\ n_{(s-1)s+1} & n_{(s-1)s+2} & \dots & n_{s^2} \end{pmatrix}$ be three $s \times s$ matrices,

where $p_i, p'_i \in k[x_1, \dots, x_n]$ are affine and are randomly chosen, N is an invertible matrix with scalar entries, and M is a block matrix such that B and C have only scalar entries and A and D have multivariate polynomials linear affine entries. Furthermore, A is invertible.

Assume that

$$A = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix};$$

with $A_1A_4 - A_2A_3 = a \in k$

Let $D = CA^{-1}B + E$, where E is an invertible matrix with entries in k .

Define $H = MPN$, and let $f_{ij} \in k[x_1, \dots, x_n]$ be the (i, j) element of H .

Then we obtain with this notation $s^2 = m$ polynomials

$f_{11}, f_{12}, \dots, f_{1s}, f_{21}, f_{22}, \dots, f_{2s}, \dots, f_{s1}, f_{s2}, \dots, f_{ss}$ that can be renumerated as f_1, f_2, \dots, f_m . We define the central map to be

$$F(x_1, \dots, x_n) = (f_1(x_1, x_2, \dots, x_n), \dots, f_m(x_1, x_2, \dots, x_n))$$

and

$$\bar{F} = \mathcal{L}_2 \circ \mathcal{F} \circ \mathcal{L}_1 = (\bar{f}_1, \bar{f}_2, \dots, \bar{f}_m),$$

where $L_1 : k^n \rightarrow k^n$ and $L_2 : k^m \rightarrow k^m$ are as above, $\bar{f}_i \in k[x_1, \dots, x_n]$ are m multivariate polynomials of degree three. The secret key and the public key are given by:

Secret Key The secret key is made of the following two parts:

- 1) The invertible linear transformations L_1, L_2 .
- 2) The matrices M, N , and P .

Public Key The public key is made of the following two parts:

- 1) The field k , including the additive and multiplicative structure;
- 2) The maps \bar{F} or equivalently, its m total degree two components

$$\bar{f}_1(x_1, x_2, \dots, x_n), \dots, \bar{f}_m(x_1, x_2, \dots, x_n) \in k[x_1, \dots, x_n].$$

Signing A signer will sign a message y_1, \dots, y_m with x_1, \dots, x_n satisfying

$$(y_1, y_2, \dots, y_m) = \bar{F}(x_1, x_2, \dots, x_n).$$

To find x_1, \dots, x_n ,

- 1 Compute $(\bar{y}_1, \bar{y}_2, \dots, \bar{y}_n) = L_2^{-1}(y_1, y_2, \dots, y_m)$.

- 2 Put $H = \begin{pmatrix} \bar{y}_1 & \bar{y}_2 & \dots & \bar{y}_s \\ \bar{y}_{s+1} & \bar{y}_{s+2} & \dots & \bar{y}_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{y}_{(s-1)s+1} & \bar{y}_{(s-1)s+2} & \dots & \bar{y}_{s^2} \end{pmatrix}$;

Since $H = MPN$, we have $P = M^{-1}HN^{-1}$. Notice here that M and N are invertible polynomial matrices and M^{-1} and N^{-1} can be easily found.

3 Assign arbitrary value to each $p'_i(x), i = 1, 2, \dots, s^2$.

4 Solve the new linear system $P = M^{-1}HN^{-1}$ for x_1, \dots, x_n . If there is no solution, we choose new values for the $p'_i(x), i = 1, 2, \dots, s^2$ and we repeat step

4. Let $(\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n)$ be the solution.

5 Compute $(x_1, x_2, \dots, x_n) = L_1^{-1}(\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n)$. The signature is (x_1, x_2, \dots, x_n)

Verification

Anyone can verify the signature by computing $(y_1, y_2, \dots, y_m) = \bar{F}(x_1, x_2, \dots, x_n)$.

If true we accept. Otherwise we reject.

Example 2.7.1 let $m = s^2, n = 2m$, and $s = 3$, so $m = 9, n = 18$.

Let Central map be

$$P = \begin{pmatrix} p_1(x)p'_1(x) & p_2(x)p'_2(x) & p_3(x)p'_3(x) \\ p_4(x)p'_4(x) & p_5(x)p'_5(x) & p_6(x)p'_6(x) \\ p_7(x)p'_7(x) & p_8(x)p'_8(x) & p_9(x)p'_9(x) \end{pmatrix}$$

where $p_i, p'_i \in k[x_1, \dots, x_{18}], i = 1, \dots, 9$ are affine. We can assume

$$p_1 = x_1 + x_5, \quad p'_1 = x_1 + x_6,$$

$$p_2 = x_3 + x_5 + 1, \quad p'_2 = x_2 + x_5, \quad p_3 = x_1 + 1, \quad p'_3 = x_{12} + x_{13},$$

$$p_4 = x_{13} + 1, \quad p'_4 = x_{13} + x_{17},$$

$$p_5 = x_5 + x_{16} + 1, \quad p'_5 = x_5 + 1,$$

$$p_6 = x_{13} + x_{14} + x_{15}, \quad p'_6 = x_2 + x_4 + x_{13},$$

$$p_7 = x_{17} + 1, \quad p'_7 = x_{16} + x_{17},$$

$$p_8 = x_{15} + x_{18}, \quad p'_8 = x_{18} + 1,$$

$$p_9 = x_1 + 1, \quad p'_9 = x_1 + x_{18}.$$

We can write P as

$$P = \begin{pmatrix} A & B & C \\ D & E & F \\ G & H & I \end{pmatrix}$$

where

$$A = p_1(x)p_1'(x) = x_1^2 + x_1x_6 + x_1x_5 + x_5x_6.$$

$$B = p_2(x)p_2'(x) = x_2x_3 + x_3x_5 + x_2x_5 + x_5^2 + x_2 + x_5.$$

$$C = p_3(x)p_3'(x) = x_1x_{12} + x_1x_{13} + x_{12} + x_{13}.$$

$$D = p_4(x)p_4'(x) = x_{13}^2 + x_{13}x_{17} + x_{13} + x_{17}.$$

$$E = p_5(x)p_5'(x) = x_5^2 + x_5x_{16} + x_{16}.$$

$$F = p_6(x)p_6'(x) = x_2x_{13} + x_4x_{13} + x_{13}^2 + x_2x_{14} + x_4x_{14} + x_{13}x_{14} \\ + x_2x_{15} + x_4x_{15} + x_{13}x_{15}.$$

$$G = p_7(x)p_7'(x) = x_{16}x_{17} + x_{17}^2 + x_{16} + x_{17}.$$

$$H = p_8(x)p_8'(x) = x_{15} + x_{18} + x_{15} + x_{18}^2 + x_{18}.$$

$$I = p_9(x)p_9'(x) = x_1^2 + x_1x_{18} + x_1 + x_{18}.$$

Choose

$$N = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \quad \text{and} \quad M = \begin{pmatrix} A_{2 \times 2} & B_{2 \times k} \\ C_{L \times 2} & D_{L \times k} \end{pmatrix};$$

Where C, B are 1×1 matrices and A and D are multivariate affine polynomials given by

$$A = \begin{pmatrix} x_1 + x_3 & x_1 + x_3 + 1 \\ x_3 + x_1 + 1 & x_3 + x_1 \end{pmatrix};$$

Note that $(x_1 + x_3)(x_3 + x_1) - (x_1 + x_3 + 1)(x_3 + x_1 + 1) = 1 \neq 0$.

And

$$B = \begin{pmatrix} 1 \\ 0 \end{pmatrix};$$

$$C = \begin{pmatrix} 1 & 1 \end{pmatrix};$$

$$D = (x_3 + x_2).$$

We can rewrite M as:

$$M = \begin{pmatrix} A_1 & B_1 & C_1 \\ D_1 & E_1 & F_1 \\ G_1 & H_1 & I_1 \end{pmatrix};$$

where $A_1 = x_1 + x_3$, $B_1 = x_1 + x_3 + 1$, $C_1 = 1$, $D_1 = x_3 + x_1 + 1$, $E_1 = x_3 + 1$, $F_1 = 0$, $G_1 = 1$, $H_1 = 1$, $I_1 = x_3 + x_2$.

Define $H = MPN$. To calculate H , we first compute MP and obtain

$$MP = \begin{pmatrix} A' & B' & C' \\ D' & E' & F' \\ G' & H' & I' \end{pmatrix};$$

where

$$A' = x_1^3 + x_1^2x_6 + x_1^2x_5 + x_1x_6 + x_1^2x_3 + x_1x_3x_6 + x_3x_6 + x_2x_5^2 + x_3^2x_5 + x_2x_3x_5 + x_3x_5^2 \\ + x_1x_2x_3 + x_1x_2x_5 + x_1x_5^2 + x_1x_2 + x_1x_5 + x_2x_5 + x_5^2 + x_2 + x_5.$$

$$B' = x_1x_2x_3 + x_1x_3x_5 + x_1x_2x_5 + x_1x_5^2 + x_1x_2 + x_1x_5 + x_1x_{12} + x_1x_{13} + x_{12}x_{13}.$$

$$C' = x_1^2 + x_1x_6 + x_1x_5 + x_6 + x_1x_3x_{12} + x_1x_3x_{13} + x_3x_{12} + x_3x_{13} + x_1x_2x_{12} + \\ x_1x_2x_{13} + x_2x_{12} + x_2x_{13}.$$

$$D' = x_1x_{13}^2 + x_1x_{13}x_{17} + x_1x_{13} + x_1x_{17} + x_3x_{13}^2 + x_3x_{13}x_{17} + x_3x_{13} + x_3x_{17} + x_3x_5^2 \\ + x_3x_5x_{16} + x_3x_{16} + x_3 + x_1x_5^2 + x_1x_5x_{16} + x_1x_{16} + x_1 + x_5^2 + x_5x_{16} + x_{16} + 1.$$

$$E' = x_1x_{13}^2 + x_1x_{13}x_{17} + x_1x_{13} + x_1x_{17} + x_3x_{13}^2 + x_3x_{13}x_{17} + x_3x_{13} + x_3x_{17} + x_{13}^2 + \\ x_{13}x_{17} + x_{13} + x_{17} + x_3x_5^2 + x_3x_5x_{16} + x_3x_{16} + x_3 + x_5^2 + x_5x_{16} + x_{16} + 1 + \\ x_2x_{13} + x_4x_{13} + x_{13}^2 + x_2x_{14} + x_4x_{14} + x_{13}x_{14} + x_2x_{15} + x_4x_{15} + x_{13}x_{15}.$$

$$F' = x_{13}^2 + x_{13}x_{17} + x_{13} + x_{17} + x_2x_3x_{13} + x_3x_4x_{13} + x_3x_{13}^2 + x_2x_3x_{14} + x_3x_4x_{14} + \\ x_3x_{13}x_{14} + x_2x_3x_{15} + x_3x_4x_{15} + x_3x_{13}x_{15} + x_2^2x_{13} + x_2x_4x_{13} + x_2x_{13}^2 + x_2^2x_{14} + \\ x_2x_4x_{14} + x_2x_{13}x_{14} + x_2^2x_{15} + x_2x_4x_{15} + x_2x_{13}x_{15}.$$

$$G' = x_1x_{16}x_{17} + x_1x_{17}^2 + x_1x_{16} + x_1x_{17} + x_3x_{16}x_{17} + x_3x_{17}^2 + x_3x_{16} + x_3x_{17} +$$

$$\begin{aligned} & x_3x_{15}x_{18} + x_3x_{15} + x_3x_{18}^2 + x_3x_{18} + x_1x_{15}x_{18} + x_1x_{15} + x_1x_{18}^2 + x_1x_{18} + \\ & x_{15}x_{18} + x_{15} + x_{18}^2 + x_{18}. \end{aligned}$$

$$\begin{aligned} H' = & x_1x_{16}x_{17} + x_1x_{17}^2 + x_1x_{16} + x_1x_{17} + x_3x_{16}x_{17} + x_3x_{17}^2 + x_3x_{16} + x_3x_{17} + \\ & x_{16}x_{17} + x_{16} + x_3x_{15}x_{18} + x_3x_{15} + x_3x_{18}^2 + x_3x_{18} + x_{15}x_{18} + x_{15} + x_{18}^2 + \\ & x_{18}^2 + x_1^2 + x_1x_{18} + x_1 + x_{18}. \end{aligned}$$

$$\begin{aligned} I' = & x_{16}x_{17} + x_{17}^2 + x_{16} + x_{17} + x_1^2x_3 + x_1x_3x_{18} + x_1x_3 + x_3x_{18} + x_1^2x_2 + \\ & x_1x_2x_{18} + x_1x_2 + x_2x_{18}. \end{aligned}$$

Next, we compute $H = MPN$ to obtain

$$H = MPN = \begin{pmatrix} A' & B' & C' \\ D' & E' & F' \\ G' & H' & I' \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

So

$$H = \begin{pmatrix} A' + B' + C' & C' & B' + C' \\ D' + E' + F' & F' & E' + F' \\ G' + H' + I' & I' & H' + I' \end{pmatrix};$$

where

$$\begin{aligned} f_1 = & A' + B' + C' \\ = & x_1^3 + x_1^2x_6 + x_1^2x_5 + x_1^2x_3 + x_1x_3x_6 + x_3x_6 + x_2x_3^2 + x_3^2x_5 + x_2x_3x_5 + x_3x_5^2 + \\ & x_1x_5^2 + x_1x_2 + x_2x_5 + x_5^2 + x_2 + x_5 + x_1x_3x_5 + x_1x_5^2 + \\ & x_1x_2 + x_1x_{12} + x_1x_{13} + x_{12}x_{13} + x_1^2 + x_1x_5 + x_6 + x_1x_3x_{12} + x_1x_3x_{13} + x_3x_{12} + \\ & x_3x_{13} + x_1x_2x_{12} + x_1x_2x_{13} + x_2x_{12} + x_2x_{13}. \end{aligned}$$

$$\begin{aligned} f_2 = & C' \\ = & x_1^2 + x_1x_6 + x_1x_5 + x_6 + x_1x_3x_{12} + x_1x_3x_{13} + x_3x_{12} + x_3x_{13} + x_1x_2x_{12} + \\ & x_1x_2x_{13} + x_2x_{12} + x_2x_{13}. \end{aligned}$$

$$\begin{aligned} f_3 = & B' + C' \\ = & x_1x_2x_3 + x_1x_3x_5 + x_1x_2x_5 + x_1x_5^2 + x_1x_2 + x_1x_{12} + x_1x_{13} + x_{12}x_{13} + \\ & x_1^2 + x_1x_6 + x_6 + x_1x_3x_{12} + x_1x_3x_{13} + x_3x_{12} + x_3x_{13} + x_1x_2x_{12} + x_1x_2x_{13} + \\ & x_2x_{12} + x_2x_{13}. \end{aligned}$$

$$f_4 = D' + E' + F'$$

$$\begin{aligned} &= x_3x_5^2 + x_3x_5x_{16} + x_3x_{16} + x_1x_5^2 + x_1x_5x_{16} + x_1x_{16} + x_1 + x_5x_{16} + x_{16} + x_3x_5^2 + \\ &x_3x_5x_{16} + x_3x_{16} + x_5x_{16} + x_{16} + x_2x_{13} + x_4x_{13} + x_2x_{14} + x_4x_{14} + x_{13}x_{14} + x_2x_{15} + \\ &x_4x_{15} + x_{13}x_{15} + x_{13}^2 + x_2x_3x_{13} + x_3x_4x_{13} + x_3x_{13}^2 + x_2x_3x_{14} + x_3x_4x_{14} + x_3x_{13}x_{14} + \\ &x_3x_4x_{15} + x_3x_{13}x_{15} + x_2^2x_{13} + x_2x_4x_{13} + x_2x_{13}^2 + x_2^2x_{14} + x_2x_4x_{14} + x_2x_{13}x_{14} + \\ &x_2^2x_{15} + x_2x_4x_{15}. \end{aligned}$$

$$f_5 = F'$$

$$\begin{aligned} &= x_{13}^2 + x_{13}x_{17} + x_{13} + x_{17} + x_2x_3x_{13} + x_3x_4x_{13} + x_3x_{13}^2 + x_2x_3x_{14} + x_3x_4x_{14} + \\ &x_3x_{13}x_{14} + x_2x_3x_{15} + x_3x_4x_{15} + x_3x_{13}x_{15} + x_2^2x_{13} + x_2x_4x_{13} + x_2x_{13}^2 + x_2^2x_{14} + \\ &x_2x_4x_{14} + x_2x_{13}x_{14} + x_2^2x_{15} + x_2x_4x_{15} + x_2x_{13}x_{15}. \end{aligned}$$

$$f_6 = E' + F'$$

$$\begin{aligned} &= x_1x_{13}^2 + x_1x_{13}x_{17} + x_1x_{13} + x_1x_{17} + x_3x_{13}^2 + x_3x_{13}x_{17} + x_3x_{13} + x_3x_{17} + x_{13}x_{17} + \\ &x_3x_5^2 + x_3x_5x_{16} + x_3x_{16} + x_3 + x_5^2 + x_5x_{16} + \\ &x_{16} + 1 + x_2x_{13} + x_4x_{13} + x_{13}^2 + x_2x_{14} + x_4x_{14} + x_{13}x_{17} + x_2x_3x_{13} + x_3x_4x_{13} + x_3x_{13}^2 + \\ &x_2x_3x_{14} + x_3x_4x_{14} + x_3x_{13}x_{14} + x_2x_3x_{15} + \\ &x_3x_4x_{15} + x_3x_{13}x_{15} + x_2^2x_{13} + x_2x_4x_{13} + x_2x_{13}^2 + x_2^2x_{14} + x_2x_4x_{14} + x_2x_{13}x_{14} + \\ &x_2^2x_{15} + x_2x_4x_{15} + x_2x_{13}x_{15}. \end{aligned}$$

$$f_7 = G' + H' + I'$$

$$\begin{aligned} &= x_3x_{15}x_{18} + x_3x_{15} + x_3x_{18} + x_1x_{15}x_{18} + x_1x_{15} + x_1x_{18}^2 + x_1x_{18} + x_{15}x_{18} + x_{15} + x_{18}^2 + \\ &x_{16}x_{17} + x_{16} + x_3x_{15}x_{18} + x_3x_{15} + x_{15}x_{18} + x_{15} + \\ &x_1^2 + x_1x_{18} + x_1 + x_{16}x_{17} + x_{17}^2 + x_{16} + x_{17} + x_1^2x_3 + x_1x_3x_{18} + x_1x_3 + x_1^2x_2 + x_1x_2x_{18} + \\ &x_1x_2 + x_2x_{18}. \end{aligned}$$

$$f_8 = I'$$

$$\begin{aligned} &= x_{16}x_{17} + x_{17}^2 + x_{16} + x_{17} + x_1^2x_3 + x_1x_3x_{18} + x_1x_3 + x_3x_{18} + x_1^2x_2 + x_1x_2x_{18} + x_1x_2 + \\ &x_2x_{18}. \end{aligned}$$

$$f_9 = H' + I'$$

$$\begin{aligned} &= x_1x_{16}x_{17} + x_1x_{17}^2 + x_1x_{16} + x_1x_{17} + x_3x_{16}x_{17} + x_3x_{17}^2 + x_3x_{16} + x_3x_{17} + x_{16}x_{17} + \\ &x_3x_{15}x_{18} + x_3x_{15} + x_3x_{18}^2 + x_{15}x_{18} + x_{15} + x_1^2 + x_1x_{18} + x_1 + x_{18} + x_{16}x_{17} + x_{17}^2 + x_{17} \\ &+ x_1^2x_3 + x_1x_3x_{18} + x_1x_3 + x_1^2x_2 + x_1x_2x_{18} + x_1x_2 + x_2x_{18}. \end{aligned}$$

To complete the construction, we have define the cental map to be :

$$F(x_1, \dots, x_{18}) = (f_1(x_1, x_2, \dots, x_{18}), \dots, f_9(x_1, x_2, \dots, x_{18}))$$

Finally the public key $\bar{\mathcal{F}}$ will be obtained by performing the composition $\bar{\mathcal{F}} = L_2 \circ F \circ L_1$, where L_2 and L_1 are any two linear affine maps.

Chapter 3: Some Algebraic Aspects of Threshold Functions

In this chapter, we use the theory of group ring to derive some algebraic properties of threshold functions.

3.1 Group Ring

Definition 3.1.1 Let K be a field and G be an abelian group. We define the group ring KG to be the set of all formal sums of the form $\sum_{\alpha \in G} a_\alpha \cdot \alpha$ with $a_\alpha \in K$. The addition, the scalar multiplication, and the multiplication in KG are respectively defined as follow:

$$\left(\sum a_\alpha \cdot \alpha \right) + \left(\sum b_\alpha \cdot \alpha \right) = \sum (a_\alpha + b_\alpha) \alpha,$$

$$b \left(\sum a_\alpha \cdot \alpha \right) = \sum (ba_\alpha) \cdot \alpha,$$

$$\left(\sum a_\alpha \cdot \alpha \right) \left(\sum b_\alpha \cdot \alpha \right) = \sum (a_\alpha b_\alpha) \cdot \alpha.$$

The associative law in G guarantees the associativity of multiplication in KG . So KG is a ring.

3.2 Threshold Functions

In this section, we look in detail of the family to threshold functions from F_p^n to F_p .

Definition 3.2.1 Let $\mathbb{Z}_p = \{0, 1, 2, \dots, p-1\}$ and \mathbb{Z}_p^n the Cartesian power of \mathbb{Z}_p which $\mathbb{Z}_p^n = \{a_1, a_2, \dots, a_n\}$, where $a_1, a_2, \dots, a_n \in \mathbb{Z}_p$. A threshold function $f : \mathbb{Z}_p^n \rightarrow \mathbb{Z}_p$ is a

$$f(x) = \begin{cases} 0 & X \cdot w^T < A_1 \\ 1 & A_1 \leq X \cdot w^T < A_2 \\ \cdot & \cdot \\ \cdot & \cdot \\ p-1 & X \cdot w^T > A_{p-1} \end{cases}$$

where

1. $w = (w_1, \dots, w_n) \in \mathbb{R}^n$, is called weight.
2. A_1, A_2, \dots, A_p are a real numbers defining and satisfying the threshold ,and $A_1 < A_2 < \dots < A_p$.
3. T is the matrix transposition .

Example 3.2.2 Let $\mathbb{Z}_2 = \{0, 1\}$ and \mathbb{Z}_2^n the Cartesian power of \mathbb{Z}_2 which $\mathbb{Z}_2^n = \{(a_1, a_2, \dots, a_n), \text{ where } a_1, a_2, \dots, a_n \in \mathbb{Z}_2\}$. And $f: \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ we define by

$$f(X) = \begin{cases} 0 & X.w^T < A_1 \\ 1 & A_1 \leq X.w^T \end{cases} .$$

Let G be a finite group, and R be a field, or ring then

$$RG = \{u = \sum_{g \in G} \alpha_g g : g \in G, \text{ and } \alpha_g \in R\} \text{ is a group ring.}$$

Example 3.2.3 Let $G = \{a, b, c\}$ and $R = F_2 = \{\bar{0}, \bar{1}\}$

$$\text{then } RG = \{u = \sum_{g \in G} \alpha_g g = \alpha_a a + \alpha_b b + \alpha_c c : \text{where } \alpha_i = 0 \text{ or } 1\}$$

If we choose $G = \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2$ and RG to be the group ring over the real number \mathbb{R} , then every element $g \in G$ can be uniquely represented in the form $g = a_1^{x_1} \dots a_n^{x_n}$, where $(x_1, x_2, \dots, x_n) \in \mathbb{Z}_2^n$ and the a_i are such that $G = \langle a_1 \rangle \times \langle a_2 \rangle \times \dots \times \langle a_n \rangle$. Therefore each element $g = a_1^{x_1} \dots a_n^{x_n} \in G$ can be identified with the corresponding vector $(x_1, x_2, \dots, x_n) \in \mathbb{Z}_2^n$.

Definition 3.2.4 Let $u = \sum_{g \in G} \alpha_g g \in RG$. For $g = a_1^{x_1} \dots a_n^{x_n}$, we define $f_u : G \rightarrow R$ by $f(g) = f(x_1, x_2, \dots, x_n) = \alpha_g$. Denoted by F the set of all elements in RG whose coefficients are restricted to \mathbb{Z}_2 , then F is one-to-one correspondance with the set of all boolean functions. The correspondance is given by: $f \longleftrightarrow u$.

Remark 3.2.5 An element u of the RG is called P -element if f corresponding to u is threshold function.

Remark 3.2.6 If $u_1 \neq u_2 \implies \exists g \in G, \alpha_g(u_1) \neq \alpha_g(u_2) \implies f_{u_1} \neq f_{u_2}$.

let $\Omega = \{\bar{w} = \langle w_1, w_2, \dots, w_n \rangle : \bar{X}, \bar{Y} \in \mathbb{Z}_2^n \text{ and } \bar{X} \neq \bar{Y} \text{ where } \bar{X} = \langle x_1, x_2, \dots, x_n \rangle, \bar{Y} = \langle y_1, y_2, \dots, y_n \rangle\}$. Then $\bar{X} \cdot \bar{w} \neq \bar{Y} \cdot \bar{w}$.

$\rho(\bar{w}) = \{(\bar{X}, \bar{Y}) : \bar{X} = \langle x_1, x_2, \dots, x_n \rangle, \bar{Y} = \langle y_1, y_2, \dots, y_n \rangle, \text{ and } \bar{X} \cdot \bar{w}^T > \bar{Y} \cdot \bar{w}^T\}$.

Definition 3.2.7 for \bar{w}_1 and $\bar{w}_2 \in \Omega$, we say \bar{w}_1 is equivalent to \bar{w}_2 if $\rho(\bar{w}_1) = \rho(\bar{w}_2)$. we will say denote by $Q(\bar{w})$ the class of all threshold functions that can be realized with the vector \bar{w} .

Now we consider three operations conserving threshold property of Boolean function:

A- again we know $u = \sum_{g \in G} \alpha_g g \in GR$ (group ring), let f_u be a threshold function corresponding to u . And $f_u(g) = f(x_1, x_2, \dots, x_i, \dots, x_n) = \alpha_g$. Then we get a new threshold function: $f^1(x_1, x_2, \dots, \bar{x}_i, \dots, x_n)$, if $u \leftrightarrow f_u$. If f^1 is obtained from f_u (by inverting the i^{th} coordinate), then f^1 is a new threshold function associated to ua_i ($f^1 \leftrightarrow ua_i = u^1$), where $u^1 = a_i u = a_i \sum_{g \in G} \alpha_g g = \sum_{g \in G} (\alpha_g a_i) g$. The mapping $u \rightarrow a_i u$ is automorphism of the addition group of the group ring.

B- let φ be an automorphism of G . ($i, e \varphi : G \rightarrow G, \varphi(a_k) = a_k \forall k \neq i, j$) and $f_u(g) = f(x_1, x_2, \dots, x_i, \dots, x_j, \dots, x_n) = \alpha_g$. We get another threshold function: $f^2(x_1, x_2, \dots, x_j, \dots, x_i, \dots, x_n)$, if $u \leftrightarrow f_u$, and $f^2 \leftrightarrow f_u$, is obtained from the threshold function f by interchanging two input variables x_i, x_j . So $\varphi(a_i) = a_j$ and $\varphi(a_j) = a_i$.

C- Again $f_u(g) = f(x_1, x_2, \dots, x_i, \dots, x_j, \dots, x_n)$. Assume $f \longleftrightarrow u$, and $u = \sum_{g \in G} \alpha_g g$.

$\alpha_g g$. We get another threshold function:

$$f^4(x_1, x_2, \dots, x_n) = \overline{x_j \oplus f(x_1 \oplus x_j, x_2 \oplus x_j, \dots, x_{j-1} \oplus x_j, x_{j+1} \oplus x_j, \dots, x_n \oplus x_j)}$$

where \oplus is addition mod p . And let $H_j = \langle a_1 \rangle \times \dots \times \langle a_{j-1} \rangle \times \langle a_{j+1} \rangle \times \dots \times \langle a_n \rangle$. Then $f^4 \longleftrightarrow v$ with $v = \left(\sum_{g \in H_j} \alpha_g g \right) (a_1 a_2 \dots a_{j-1} a_{j+1} \dots a_n) + \sum_{g \in H_j} g + \sum_{g \in a_j H_j} \alpha_g g$.

Lemma 3.2.8 Let f be a Boolean function, and assume that f is a threshold function with $\bar{w}_1 \in \Omega$ and real number A . And if $\bar{w}_1 \sim \bar{w}_2$, then $\exists A \in \mathbb{R}$ such that \bar{w}_2 and A can realize also f .

Proof. We have $f(x) = \begin{cases} 0 & X \cdot w^T < A \\ 1 & X \cdot w^T \geq A \end{cases}$
Let $\bar{X} = \{f^{-1}(0)\} = \{X : f(X) = 0\}$ and $\bar{X}_1 = \{\bar{X} : \bar{X} \cdot w^T \text{ is the maximum}\}$.
Assume $\bar{w}_1 \sim \bar{w}_2 \implies \rho(\bar{w}_1) = \rho(\bar{w}_2)$, $\rho(\bar{w}_1) = \{(\bar{X}, \bar{Y}) : \bar{X} \cdot \bar{w}_1^T > \bar{Y} \cdot \bar{w}_1^T\}$
 $= \rho(\bar{w}_2)$ since $\rho(\bar{w}_1) = \rho(\bar{w}_2) \implies \bar{X}_1 = \{\bar{X} : X \cdot \bar{w}_1^T \text{ is the maximum}\}$
 $= \{\bar{X} : \bar{X} \cdot \bar{w}_2^T \text{ is the maximum}\}$. Let $X \in \bar{X}_1 \implies X \cdot \bar{w}_1^T = B < A \implies$
 $X \cdot \bar{w}_2^T = B_1 < A$ consider the interval $(B_1, \min\{x \cdot \bar{w}_2^T : f(X) = 1\}] = C_1$
and let A be any number between B_1 and C_1 . Then for any X such that
 $X \cdot \bar{w}_2^T < B_1 \implies X \cdot \bar{w}_2^T < A$, and any X such that $X \cdot \bar{w}_2^T \geq C_1 \implies X \cdot \bar{w}_2^T \geq A$
 $\implies f(x) = \begin{cases} 0 & X \cdot w^T < A \\ 1 & X \cdot w^T \geq A \end{cases} \implies [w_2, A]$ realize f as a threshold function.

■

Example 3.2.9 Let $n = 3$, and $f : \mathbb{Z}_2^3 \longrightarrow \mathbb{Z}_2$.

since $\mathbb{Z}_2^3 = \{x_1 = (0, 0, 0), x_2 = (0, 0, 1), x_3 = (0, 1, 0), x_4 = (0, 1, 1),$
 $x_5 = (1, 0, 0), x_6 = (1, 0, 1), x_7 = (1, 1, 0), x_8 = (1, 1, 1)\}$.

Choose $w_1 = (1, 3, 5)$ and $A = 5$.

Find - $\rho(w_1) = \{(\bar{X}, \bar{Y}) : \bar{X} \cdot \bar{w}_1^T > \bar{Y} \cdot \bar{w}_1^T\}$, where $\bar{X}, \bar{Y} \in \mathbb{Z}_2^3$.

The values of $x_i \cdot \bar{w}_1^T$ are given by:

$$x_1 \cdot w_1^T = (0 \ 0 \ 0)(1 \ 3 \ 5)^T = 0$$

$$x_2 \cdot w_1^T = (0 \ 0 \ 1)(1 \ 3 \ 5)^T = 5$$

$$x_3 \cdot w_1^T = (0 \ 1 \ 0)(1 \ 3 \ 5)^T = 3$$

$$x_4 \cdot w_1^T = (0 \ 1 \ 1)(1 \ 3 \ 5)^T = 8$$

$$x_5 \cdot w_1^T = (1 \ 0 \ 0)(1 \ 3 \ 5)^T = 1$$

$$x_6 \cdot w_1^T = (1 \ 0 \ 1)(1 \ 3 \ 5)^T = 6$$

$$x_7 \cdot w_1^T = (1 \ 1 \ 0)(1 \ 3 \ 5)^T = 4$$

$$x_8 \cdot w_1^T = (1 \ 1 \ 1)(1 \ 3 \ 5)^T = 9$$

Using the definition of $\rho(w)$ we obtain;

$$\begin{aligned} \rho(w_1) = & \{(x_2, x_1), (x_3, x_1), (x_4, x_1), (x_5, x_1), (x_6, x_1), (x_7, x_1), (x_8, x_1) \\ & (x_2, x_3), (x_4, x_2), (x_2, x_5), (x_6, x_2), (x_8, x_2), (x_4, x_3), (x_3, x_5), (x_6, x_3) \\ & (x_7, x_3), (x_8, x_3), (x_4, x_5), (x_4, x_6), (x_4, x_7), (x_8, x_4), (x_6, x_5), (x_7, x_5) \\ & (x_8, x_5), (x_6, x_7), (x_8, x_6), (x_8, x_7)\} \end{aligned}$$

If we choose $w_2 = (2, 3, 4)$, then the $x_i.w_2^T$ are given by:

$$x_2.w_2^T = (0 \ 0 \ 0)(2 \ 3 \ 4)^T = 0$$

$$x_3.w_2^T = (0 \ 0 \ 1)(2 \ 3 \ 4)^T = 4$$

$$x_4.w_2^T = (0 \ 1 \ 0)(2 \ 3 \ 4)^T = 3$$

$$x_5.w_2^T = (0 \ 1 \ 1)(2 \ 3 \ 4)^T = 7$$

$$x_6.w_2^T = (1 \ 0 \ 0)(2 \ 3 \ 4)^T = 2$$

$$x_7.w_2^T = (1 \ 0 \ 1)(2 \ 3 \ 4)^T = 6$$

$$x_8.w_2^T = (1 \ 1 \ 0)(2 \ 3 \ 4)^T = 5$$

$$x_8.w_2^T = (1 \ 1 \ 1)(2 \ 3 \ 4)^T = 9$$

$$\begin{aligned} \text{Therefore } \rho(w_2) = & \{(x_2, x_1), (x_3, x_1), (x_4, x_1), (x_5, x_1), (x_6, x_1), (x_7, x_1), (x_8, x_1) \\ & (x_2, x_3), (x_4, x_2), (x_2, x_5), (x_6, x_2), (x_8, x_2), (x_4, x_3), (x_3, x_5), (x_6, x_3) \\ & (x_7, x_3), (x_8, x_3), (x_4, x_5), (x_4, x_6), (x_4, x_7), (x_8, x_4), (x_6, x_5), (x_7, x_5) \\ & (x_8, x_5), (x_6, x_7), (x_8, x_6), (x_8, x_7)\} \end{aligned}$$

Notice that $\rho(w_1) = \rho(w_2)$.

$$\text{Now we find } \bar{X} = \{x \in \mathbb{Z}_2^3 : f(x) = 0\} \text{ such that } f(x) = \begin{cases} 0 & x.w_1^T < A_1 \\ 1 & x.w_1^T \geq A_1 \end{cases},$$

for $A_1 = 5$, to find A_2 we first compute:

$$\bar{X}_1 = \{x \in \bar{X} : x.w^T \text{ is maximum}\}, \text{ i.e. } \bar{X}_1 = x_6.$$

Then, we have $B_1 = \{x_6.w_2^T \text{ is also the maximum}\}$, i.e. $B_1 = 6$.

Also $C_1 = \min \{x.w_2^T : f(x)=1\}$. Choose A_2 such that $B_1 < A_2 \leq C_1$, we

can choose $A = 6$.

$$f(x_1) = \begin{cases} 0 & x.w_2^T < A_2 \\ 1 & x.w_2^T \geq A_2 \end{cases}, \quad \bar{X}_2 = \{x \in \mathbb{Z}_2^3 : f(x_1) = 0\},$$

so $\bar{X}_2 = \{x_1, x_2, x_3, x_5, x_6, x_7\}$. Hence $w_1 \sim w_2$.

Chapter 4: Conclusion

We conducted the analysis of Multivalued threshold function and the Multivariate polynomials which present the two main families over finite fields that have been studied over this thesis. Both of these families play essential role in present areas such as cryptography, circuit complexity, learning theory, social choice, quantum complexity, and many other aspects. Many other researchers had worked on establishing in new design of quantum multivariate cryptosystems which most of them seem to be insecure. The aim of this thesis is to introduce new cryptosystem that suppose to resist quantum computers attacks. In this thesis four chapters have been presented. The first chapter describes an introduction about the finite field and cryptosystem include their histories. Definition, properties, and construction in addition to multivariate cryptosystem and oil-vinegar have been discussed in the second chapter of this thesis. the third chapter include description to some aspects of threshold function and group ring.

References

- [1] Akkar, M.-L., Courtois, N. T., Duteuil, R., and Goubin, L., A Fast and Secure Implementation of Sash, Public Key Cryptography-PKC 2003, pp. 267-278. Springer, 2003.
- [2] N. N. Aizenberg, A. A. Bovdi, E. I. Gergo, F. E. Gech, Algebraic aspects of threshold logic, *Cybernetics* 16 (1980) 118-193.
- [3] Bini D. A., B. Iannazzo and B. Meini., Numerical Solution of Algebraic Riccati Equations, *Fundamentals of Algorithms*. SIAM, Philadelphia, 2012.
- [4] A. Casson and D. Jungreis, Convergence groups and Seifert bered 3-manifolds, *Invent.Math.* 118 (1994) 441-456.
- [5] Ding, J., A New Variant of the Matsumoto- Imai Cryptosystem through Perturbation, Public Key Cryptography PKC 2004, pp. 305-318. Springer, 2004.
- [6] Ding, J. Gower, J. and Schmidt, D. Multivariate Public Key Cryptosystems, *Advances in information security*, spring, 2006.
- [7] Ding, J. and Gower, J. E., Inoculating Multivariate Schemes against Deferential Attacks, Public Key Cryptography-PKC 2006, pp. 290-301. Springer, 2006.
- [8] Ding, J., Petzoldt, A., and Wang, L.-C., The Cubic Simple Matrix Encryption Scheme, In Mosca, M. (ed.), *Post-Quantum Cryptography*, Lecture Notes in Computer Science, 8772, pp. 76-87. Springer International Publishing, 2014.
- [9] Ding, J. and Schmidt, D., Cryptanalysis of HFEv and Internal Perturbation of HFE, In Vaudenay, S. (ed.), *Public Key Cryptography-PKC 2005*, Lecture Notes in Computer Science, 3386, pp. 288-301. Springer Berlin Heidelberg, 2005.
- [10] Ding J. and Yang B. Y., *Post Quantum Cryptography*, chapter Multivariate Public Key Cryptography, pages 193-234. Springer-Verlag Berlin Heidelberg, 2009.
- [11] Gao, S. and Heindl, R., Multivariate Public Key Cryptosystems from Diophantine Equations, *Designs, Codes and Cryptography*, 67, 1-18, 2013.
- [12] Huang, Y.-J., Liu, F.-H., and Yang, B.-Y., Public-Key Cryptography from New Multivariate Quadratic Assumptions, *Public Key Cryptography. PKC 2012*, pp. 190-205. Springer 2012.
- [13] E. K. Horvath. Invariance groups of threshold functions, *Acta Cybernetica* 11(1994), 325-332.

- [14] Kipnis, A. and Shamir, A. , Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization, Advances in cryptology-CRYPTOGRAPHY99, pp. 19-30. Springer, 1999.
- [15] Kipnis, A., Patarin, J., and Goubin, L., Unbalanced Oil and Vinegar Signature Schemes, Advances in Cryptology-EUROCRYPT-99, pp. 206-222. Springer, 1999. prensice Hall , 2000.
- [16] Matsumoto, T. and Imai, H., Public Quadratic Polynomial-Tuples for Efficient Signature-Verication and Message-Encryption, EUROCRYPT88, pp. 419-453. Springer, 1988.
- [17] S. Muroga, Threshold logic and its applications, Wiley-Interscience (1971).
- [18] Patarin, J., Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms, In Maurer, U. (ed.), Advances in Cryptology-EUROCRYPT96, Lecture Notes in Computer Science, 1070, pp. 33-48. Springer Berlin Heidelberg, 1996.
- [19] Patarin, J., The Oil and Vinegar Signature Scheme, Dagstuhl Workshop on Cryptography, 1997.
- [20] Patarin, J., Courtois, N., and Goubin, L., Quartz, 128-Bit Long Digital Signatures, Topics in Cryptology-CT-RSA 2001, pp. 282-297. Springer, 2001.
- [21] Patarin, J., Goubin, L., and Courtois, N., Câà.âà. + and HM: Variations Around Two Schemes of T. Matsumoto and H. Imai, IAdvances in Cryptology-ASIACRYPT98, pp. 35-50. Springer, 1998.
- [22] D. S. Passman. The Algebraic structure of Group Ring. Robert E. Krieger Publishing Company. John Willey & Son, Inc. 1985.
- [23] Porras, J., Baena, J., and Ding, J., ZHFE, a New Multivariate Public Key Encryption Scheme., Post- Quantum Cryptography, pp. 229-245. Springer, 2014.
- [24] Tao, C., Diene, A., Tang, S., and Ding, J., Simple Matrix Scheme for Encryption, Post-Quantum Cryptography, pp. 231-242. Springer, 2013.
- [25] Yasuda, T., Ding, J., Takagi, T., and Sakurai, K., A Variant of Rainbow with Shorter Secret Key and Faster Signature Generation , Proceedings of the first ACM workshop on Asia public-key cryptography, pp. 57-62. ACM, 2013.
- [26] Yasuda, T., Takagi, T., and Sakurai, K., Multivariate Signature Scheme Using Quadratic Forms , Post-Quantum Cryptography, pp. 243-258. Springer, 2013.
- [27] Yasuda, T., Takagi, T., and Sakurai, K., Efficient Variant of Rainbow without Triangular Matrix Representation , Information and Communication Technology, pp. 532-541. Springer 2014.

- [28] Yasuda, T., Takagi, T., and Sakurai, K., Efficient Variant of Rainbow Using Sparse Secret Keys, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 5, 3-13, 2014.
- [29] Wolf C., Preneel B., Taxonomy of Public-Key Schemes based on the Problem of Multivariate Quadratic Equations, Cryptology ePrint Archive, Report 2005/077, 2005, <http://eprint.iacr.org/>.
- [30] Wan, Z., Finite Fields and Galois Rings, world scientific, 2003.
- [31] Zhang, W. and Tan, C. H., A New Perturbed Matsumoto-Imai Signature Scheme, Proceedings of the 2nd ACM workshop on ASIA public-key cryptography, pp. 43-48. ACM, 2014.