HFE BASED MULTI-VARIATE QUADRATIC CRYPTOSYSTEMS AND DEMBOWSKI OSTROM POLYNOMIALS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

BILAL ALAM

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
IN
CRYPTOGRAPHY

MAY 2013

Approval of the thesis:

HFE BASED MULTI-VARIATE QUADRATIC CRYPTOSYSTEMS AND DEMBOWSKI OSTROM POLYNOMIALS

submitted by **BILAL ALAM** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy in Department of Cryptography, Middle East Technical University** by,

Prof. Dr. Bülent Karasözen
Director, Graduate School of **Applied Mathematics** _____

Prof. Dr. Ferruh Özbudak
Head of Department, **Cryptography** _____

Prof. Dr. Ferruh Özbudak
Supervisor, **Cryptography, METU** _____

Dr. Oğuz Yayla
Co-supervisor, **Cryptography, METU** _____

Examining Committee Members:

Prof. Dr. Ersan Akyıldız
Cryptography,IAM METU _____

Prof. Dr. Ferruh Özbudak
Cryptography,IAM METU _____

Assoc. Prof. Dr. Ali Doğanaksoy
Cryptography,IAM METU _____

Asst. Prof. Dr. Zülfükar Saygı
Mathematics,Tobb University Of Economics And Technology _____

Dr. Çağdaş Çalık
Cryptography,IAM METU _____

Date: _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: BILAL ALAM

Signature :

ABSTRACT

HFE BASED MULTI-VARIATE QUADRATIC CRYPTOSYSTEMS AND DEMBOWSKI OSTROM POLYNOMIALS

Alam, Bilal

Ph.D., Department of Cryptography

Supervisor : Prof. Dr. Ferruh Özbudak

Co-Supervisor : Dr. Oğuz Yayla

May 2013, 73 pages

Harayama and Friesen proposed linearised binomial attack for multivariate quadratic cryptosystems and introduced weak Dembowski Ostrom(DO) polynomials in this framework over the finite field $\mathbb{F}_2$. They conjecture about the existence of infinite class of weak DO polynomials and presented the open problem of enumerating their classes. We extend linearised binomial attack to multivariate quadratic cryptosystems over $\mathbb{F}_p$ for any prime p and redefine the weak DO polynomials for general case. We identify an infinite class of weak Dembowski Ostrom polynomials for these systems by considering highly degenerate quadratic forms over algebraic function fields and Artin-Schreir type curves to achieve our results. This thesis also presents a comprehensive survey of HFE based multivariate quadratic public key cryptosystems and discusses some recent cryptanalytic attacks involving Gröbner bases and matrix/vector operations by reducing the involved problem to related MinRank and IP problem. We also mention a possible connection among Ore's p-polynomials and HFE cryptosystems identified in the work of Coulter.

Keywords: linearised binomial attack, weak Dembowski Ostrom polynomials, Hidden Field Equations Cryptosystems, Multivariate Quadratic Cryptosystems

ÖZ

HFE TABANLİ İKINCI DERECEDEN ÇOK DEĞIŞKENLI KRIPTOSISTEMLER VE DEMBOWSKI OSTROM POLINOMLAR

Alam, Bilal

Doktora, Uygulamalı Matematik Enstitüsü

Tez Yöneticisi : Prof. Dr. Ferruh Özbudak

Ortak Tez Yöneticisi : Dr. Oğuz Yayla

Mayis 2013, 73 sayfa

Harayama ve Friesen, ikinci dereceden çok-değişkenli kriptosistemlerine doğrusal binom atağını sunmuşlardır ve sonlu cisim $\mathbb{F}_2$ üzerindeki bu sistemler için zayıf Dembowski Ostrom(DO) polinomlarını tanımlamışlardır. Sonsuz elemanlı zayıf DO polinom sınıflarının olduğu varsayımını öne sürmüşlerdir ve bu sınıfların sıralanmasını açık problem olarak sunmuşlardır. Çalışmamızda, doğrusal binom atağını, herhangi bir asal p karakteristiğine sahip sonlu cisim $\mathbb{F}_p$ üzerindeki ikinci dereceden çok-değişkenli kriptosistemlere genelleştiriyoruz ve genel durum için zayıf DO polinomlarını yeniden tanımlıyoruz. Bu genel sistemler için sonsuz elemanlı zayıf DO polinom sınıfını, cebirsel fonksiyon cisimleri üzerindeki oldukça bozuk ikinci dereceden formları ve Artin-Schreir eğrilerini kullanarak sunuyoruz. Bu tezde ayrıca HFE tabanlı ikinci dereceden çok-değişkenli kriptosistemler hakkında detaylı bir inceleme sunulmaktadır ve bu problemin ilgili MinRank ve IP problemlerine dönüştürülmesi ile Gröbner bazları ve matris/vektör işlemleri içeren yakın zamanda sunulan bazı ataklar tartışılmaktadır. HFE kirptosistemleri ile Ore polinomlarının bağlantılarına da değinilmiştir.

Anahtar Kelimeler: doğrusal binom atak, zayif Dembowski Ostrom Polinomlar, Saklı Cisim Denklemleri, İkinci Dereceden Çok Değişkenli Kriptosistemler

To my Dearest Father and Mother
Best Friend and Wonderful Partner Saba
Zaim, Zeyn And Family

ACKNOWLEDGMENTS

I owe the successful completion of my research presented in this thesis to the valuable guidance from my supervisor Prof. Dr. Ferruh Özbudak and co-supervisor Dr. Oğuz Yayla. Their enthusiastic encouragement and insight to the understanding of this problem paved the way to its solution and my success. I am extremely indebted to them for contributing their efforts in terms of time and knowledge towards the completion of this work.

I would specially like to acknowledge the support of Dr. Oğuz Yayla in drafting this work and educating me at each step during the course.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

Introduction

Cryptography can be broadly considered as the mathematics of encrypting and decrypting data. It enables to store vital information and also to communicate the same across an insecure channel to the intended recipient. Contrary to this, cryptanalysis is the mathematics of extracting secured vital information and analysing/breaking the security embedded to vital information being communicated. It involves application of variety of mathematical tools as well as some analytic approach to pattern extraction. Cryptanalysts are often termed as attackers. Cryptology embraces both cryptographers and cryptanalysts.

Cryptography involves the design of basic primitives that are algorithms with sound mathematical properties and related in complexity to hard mathematical problems. More sophisticated and complex cryptographic tools or cryptosystems are then developed by employing these basic cryptographic primitives to address the high level security requirements in practice. A cryptosystem is generally considered as 5-tuple$(\mathcal{P}, \mathcal{K}, \mathcal{C}, \mathcal{E}, \mathcal{D})$ package as follow:

1. $\mathcal{P}$ refers to set of plain information referred as *Plaintext*.
2. $\mathcal{C}$ refers to set of secured information referred as *Ciphertext*.
3. $\mathcal{K}$ refers to set of possible keys referred as *Key-space*.
4. Corresponding to each $K \in \mathcal{K}$ there is an *Encryption-rule* $E \in \mathcal{E}$ such that it transforms given plaintext $P \in \mathcal{P}$ to ciphertext $C \in \mathcal{C}$ i.e. $E : P \to C$ and also there is a *Decryption-Rule* $D \in \mathcal{D}$ to retrieve the plaintext from ciphertext i.e. $D : C \to P$.

Broadly speaking, there are two models of cryptography i.e. *Symmetric-Key Model* and *Asymmetric-Key Model*. In Symmetric-Key model, one key is used for both encryptions and decryption. Data Encryption Standard (DES) and Advanced Encryption Standard (AES) represent this model. Figure 1.1 illustrates symmetric key cryptography model.

Key agreement is thus a natural question in terms of symmetric-key cryptography model. The only option other than physically exchanging the key is to transmit

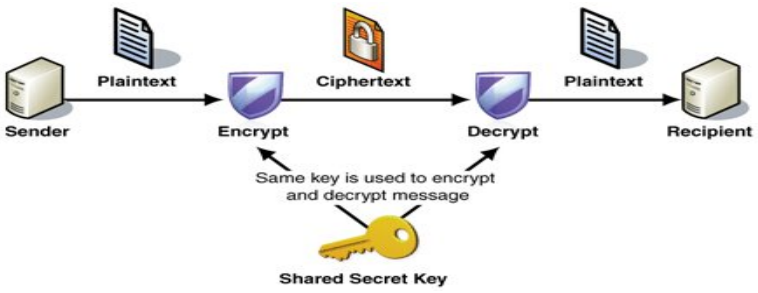

Figure 1.1: Symmetric-key Cryptography Model

it securely over an insecure channel. Asymmetric-Key model is an answer to this problem of key transfer.

Public-key or Asymmetric cryptography model was introduced by Whitfield Diffie and Martin Hellman in [24]. Asymmetric cryptography model employs a pair of keys termed as a *Public key* that encrypts the information and a corresponding *Private key* that decrypts the encrypted information. Public key is published to the world and private key is kept secret. The sender of vital information encrypts using the public key of intended recepient without even prior interaction. Though necessarily related, retrieving private key from published public key is considerd computationally infeasible. Encryption only requires knowldege of recipient's public key while decryption by the intended recepient involves only private key operations. Figure 1.2 illustrates asymmetric cryptography model. Public key cryptography model facilitates secure information exchange over insecure model without the trouble of key agreement or key transfer. Elgamal, RSA and Elliptic-curves are well known asymmetric cryptosystems.

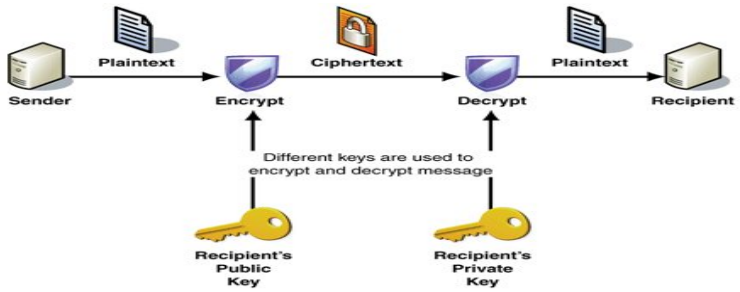

Figure 1.2: Asymmetric-key / Public Key Cryptography Model

Asymmetric cryptographic algorithms are often based on the computational complexity of hard mathematical problems from number theory. The integer factorization problem is the basis of RSA while the complexity of solving discrete logarithm is related to Diffie - Hellman and DSA. Elliptic curve cryptography is developed around number theoretic problems involving elliptic curves. The main strong assumption is computational infeasibility of constructing one key from the other, even though they are necessarily related. This indirectly effects the choice

of mathematical problems for asymmetric cryptography as well.

The advent of quantum computers and development of polynomial time algorithm like Shor′s algorithm for integer factorization has raised serious questions about viability of number theoretic problems and cryptographic tools based on mathematical hardness of these problems. As a consequence to this cryptographic and mathematical community is investing huge amount of time and resources in development of credible tools in terms of security for the prospective era of quantum computers. Research in this field is tagged as Post Quantum Cryptography(PQC) [21] and research till date in PQC can be divided in the following domains

1. Hash Based Cryptography
2. Code Based Cryptography
3. Lattice Based Cryptography
4. Multivariate Quadratic Equations Cryptography
5. Secret Key Cryptography

Multivariate cryptography is an asymmetric cryptographic primitive based on multivariate polynomials over a finite field. Multivariate public key cryptosystems (MPKCs for short) employ a set of multivariate polynomials as the public key. The NP-hardness of the problem to solve these non-linear equations over a finite field [49] formulates the main security assumption of the resultant cryptosystems. There has been intensive research performed on MPKCs in the last few decades rendering some constructions are not as secure as initially claimed. Many MPKCs, however, are still viable. In practice, quadratic polynomials are usually used in MPKCs, and hence, in this study we consider only multivariate quadratic (MQ) systems.

With the advent of quantum computers and it's potential towards applications in ubiquitous computing devices, we can find some very recent results for MPKCs [21]. The idea to strengthen HFE based MQ cryptosystems using field of odd characteristics [5, 19] is a proof of this fact. Public key cryptosystems can be considered as instance of *trapdoor one-way functions* [24]. This function and the mathematical structure behind it determines the essential characteristics of the public key cryptosystem. MPKCs are also instance of a trapdoor one way function involving the inversion of a set of quadratic equations over finite field termed as an **MQ Problem**. Given a system of m quadratic polynomial equations $P_1(x) = P_2(x) = \cdots = P_m(x) = 0$ in n variables $x = (x_1, \cdots, x_n)$ over a finite field $\mathbb{F}_q$. The MQ-problem involves computing the inverse map x for a given $y = (y_1, \cdots, y_m)$.

For a random set of quadratic equations the corresponding MQ problem is an NP-hard problem in general [49]. But MPKCs are not designed with random set of quadratic equations but those related to specific trapdoor function. Thus, the NP-hardness of MQ problem does not guarantee the security of MQ cryptosystem but

the trapdoor function being the main vulnerable entity in the design determines the overall strength of the systems. There are effective attacks proposed against many trapdoor designs and the theory of MPKCs thus evolves as more and more insight is developed about designing secure multivariate trapdoors.

1.1 Our Contribution

An MQ cryptosystem defined over finite field $\mathbb{F}_q$ of cardinality q when used in digital signature scheme usually gives short signatures of size q^m for some integer m. Thus, the birthday attack is generally applicable to the underlying MQ system at complexity $O(q^{m/2})$ [12].

T. Harayama and K. Friesen in a recent work [34], proposed a linearized binomial attack (LBA) for MQ systems over $\mathbb{F}_2$ with $n = m$ as a customized birthday attack under some restrictions on the univariate representation of public polynomials over $\mathbb{F}_{2^n}$. They observed experimentally that the LBA can be asymptotically better by at least a factor of $2^{n/8}$ than the generic birthday attack for MQ signature schemes that have univariate public key polynomial belonging to certain classes of Dembowski Ostrom(DO) polynomials over $\mathbb{F}_{2^n}$. They termed these polynomials as *Weak DO Polynomials* and conjectured about the existence of an infinite class of these polynomials over $\mathbb{F}_{2^n}$ of the form $g(x) = x^{2^{n/4}+1} + x^{2^{3n/4}+1} \in \mathbb{F}_{2^n}[x]$. They also posed an open question to enumerate other such classes of weak DO polynomials.

In this thesis we address this conjecture. We prove the existence of conjectured class of weak DO polynomials in Corollary 4.7 and identify the general class to which this class belongs in Theorem 4.6. As our first contribution using results in [43] we extend the LBA in [34] to MQ cryptosystems over $\mathbb{F}_p$ with p any odd prime. This allowed us to redefine weak DO polynomials for finite fields of characteristic any prime p in Definition 4.1. Our second contribution is identification of a general class of these weak DO polynomials of the form $g'(x) = \sum_{i=1}^{k} A_i x^{p^{(2i-1)n/2k}+1} \in \mathbb{F}_{p^n}[X]$ in Theorem 4.8. We use theory of algebraic function fields to prove the existence of our general class of weak DO polynomials and also show that the conjectured class in [34] is a subclass of our general class. Many infinite subclasses can be extracted from our general class and thus can be considered as an answer to enumeration problem stated in [34]. But we do observe that many other classes can still be derived following our approach and hence we regard the enumeration problem partially resolved.

Christropher Wolf in his PhD dissertation [56] provided an extensive survey of the MPKCs discussing the design methods as well as cryptanalytic attacks on such systems. The HFE (Hidden Field Equations) MQ cryptosystems were one of the few focussed multivariate cryptosystem designs proposed almost a decade ago by Patarin [48] and were observed to withstand major attacks otherwise successful against other multivariate schemes. Many polynomial time proposed

attacks against HFE cryptosystems have been recently proved theoretically or conjectured to be sub-exponential based on simulation results. In this thesis, we devote a complete section to the study of HFE cryptosystems discussing few important variations and significant cryptanalytic attacks proposed till date for HFE designs. Coulter, Havas and Henderson [10] reported a connection between cryptanalysis of HFE cryptosystems and decomposition of p-polynomials proposed by Ore [44] as early as 1930's. We also discuss their work at the end of this thesis.

1.2 Outline of Thesis

The thesis is organised as follows: In Chapter 2 we cover some necessary mathematical tools required to develop a clear understanding of the material presented later in this thesis. Chapter 3 introduces MQ cryptosystems with few important concepts involved. In Chapter 4, after reviewing the work of Harayama and Friesen [34, 35] we discuss LBA over even characteristic MPKCs and its extension to the odd prime p case. Later after redefining the weak DO polynomials we present proof of the existence of the conjectured class [34, 35] and our general class of weak DO polynomials. At the end of this thesis, in Chapter 5 we provide a comprehensive survey of design variations and major cryptanalytic attacks on HFE based MQ cryptosystems till date concluding with the discussion on connection between Ore's decomposition of p-polynomials and cryptanalysis of HFE cryptosystems.

CHAPTER 2

MATHEMATICAL BACKGROUND

In order to facilitate the readers to understand the results presented in this thesis, it would be more systematic to start with discussion of few fundamental mathematical concepts and to introduce the properties and notations useful to this thesis. This would improve clarity and comprehension of the subjects under discussion in various sections and in general the theory of *Multivariate Quadratic* public key cryptography.

2.1 Birthday Problem

The birthday problem is a very simple problem in statistics of computing the probability of coincidence among the birthdays in a group of people. Mathematically, it can be defined as computing the probability that two out of n people share their birthdays.

Assuming P_s as the probability of one such coincidence and P_d as it's complement i.e. the probability of not having any such coincidence. With these two as the only involved cases, we have $P_s = 1 - P_d$, because the possibilities are mutually exclusive.

The occurrence of birthday's of individuals on any particular day of an year are independent events. Hence, considering a uniform distribution for such a problem, the resultant probability P_d can be expressed as

$$\begin{aligned} P_d &= \frac{365}{365} \times \frac{364}{365} \times \frac{363}{365} \times \cdots \\ &= (1/365) \times (365 \times 364 \times 363 \times \cdots) \end{aligned}$$

Considering the probability for a group of 23 people, it can be estimated as:

$$\begin{aligned} P_d &= \frac{365}{365} \times \frac{364}{365} \times \frac{363}{365} \times \cdots \times \frac{343}{365} \\ &= (1/365) \times (365 \times 364 \times 363 \times \cdots \times 343) \\ &= 0.493 \end{aligned}$$

Therefore, $P_s \approx 1 - 0.493 = 0.507(50.7\%)$. Generalize the problem for a group of n people. With $P_s(n)$ as the probability of at least one coincidence among the birthdays of n people and $P_d(n)$ as the probability of all n birthdays being different. Based on the pigeonhole principle, $P_d(n)$ is zero when $n > 365$. When $n \leq 365$

$$P_d(n) = 1 \times (1 - \frac{1}{365}) \times (1 - \frac{2}{365}) \times \cdots \times (1 - \frac{n-1}{365}). \tag{2.1}$$

The above statement is a representation of first birthday being different from others with probability 1. The second birthday different from first with probability $1 - \frac{1}{365}$ and so on each subsequent birthday different from previous ones. The complementary event of observing at least two of the n persons having the same birthday can be calculated as

$$P_s(n) = 1 - P_d(n).$$

To express, this generalization mathematically we use Taylor Series expansion of the exponential function (the constant $e \approx 2.718281828$).

$$e^x = 1 + x + \frac{x^2}{2!} + \cdots$$

which can be considered as first-order approximation of e^x. For $x \ll 1$

$$e^x \approx 1 + x.$$

Applying this approximation to $P_d(n)$, let $x = -i/365$. i.e.

$$e^{-i/365} \approx 1 - \frac{i}{365}.$$

Replacing i with non-negative integers for each term in the formula of $P_d(n)$ until $i = n - 1$, for e.g. with $i = 2$

$$e^{-2/365} \approx 1 - \frac{2}{365}$$

The expression derived earlier for $P_d(n)$ can be approximated as

$$\begin{aligned} P_d(n) &\approx 1 \times e^{-1/365} \times e^{-2/365} \cdots e^{-(n-1)/365} \\ &= 1 \times e^{-(1+2+\cdots+(n-1))/365} \\ &= e^{-(n(n-1)/2)/365} \end{aligned}$$

Therefore,

$$P_s(n) = 1 - P_d(n) \approx 1 - e^{-n(n-1)/(2\times 365)} \tag{2.2}$$

And further approximation gives

$$P_s(n) \approx 1 - e^{-n^2/(2\times 365)}. \tag{2.3}$$

Further generalizing the birthday problem to any number of persons and days. Lets take m as the number of persons and n as the number of days. With $m \ll n$,

the same approach applied to this general case gives $P_s(m, n)$ i.e. the probability that at least two out of m people share the same birthday from a set of n available days.

$$P_s(m, n) \approx 1 - e^{-m^2/2n}. \tag{2.4}$$

In cryptography, the birthday problem finds its application in an attack known as *Birthday Attack*. This attacks exploits the mathematics involved in resolving birthday problem as a probability result. Overall the attack looks for collision among outputs of a mathematical function with certain number of random inputs, based on the theory of pigeonhole principle involved in birthday problem/paradox.

Given $f(x)$ any function with x as input. A collision is defined as $f(x_1) = f(x_2)$ i.e. same output with two given inputs $x_1 \neq x_2$. Birthday problem has direct application in computing the probability of such an occurrence for any mathematical function. To observe this, let n be the cardinality of the output set and m be the number of random inputs. Then the probability of observing a collision is directly given as

$$P_{(m,n)} \approx 1 - e^{-m^2/2n}. \tag{2.5}$$

In birthday attack, we go one step further and compute the minimum number of random inputs N_P required to observe a collision with probability p. It can be trivially observed as

$$N_P \approx \sqrt{2n \ln \frac{1}{1-p}}$$

Taking the success probability p as 50% or 0.5, we get

$$N_P \approx 1.1774\sqrt{n} \approx \sqrt{\frac{\pi}{2}n}$$

which is the expected number of random inputs required to obtain a collision with a success probability 0.5 or 50%.

2.2 Finite Fields

Modern cryptography (in general) is based on theory of finite fields. So, we would like to review certain fundamentals of theory of finite fields from lectures on Finite Fields and Galois Rings by Wan [54].

Definition 2.1. Finite Field $\mathbb{F}$ is any group of elements with two binary operations: (1) Addition $+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ and (2) Multiplication $. : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$. The definition itself implies closure with respect to both these operations. We call (F, +, .) a finite field *if* it satisfies the following set of rules called Axioms of fields. $\mathbb{F}$ is an additive abelian group $(F, +)$ such that

1. Associativity: $\forall a, b, c \in \mathbb{F} \ : \ ((a + b) + c) = (a + (b + c))$.

2. Identity element: $\exists\, e \in \mathbb{F}\ : \forall a \in \mathbb{F} : a + e = a$.
3. Inverse: $\forall a \in \mathbb{F}\ \exists\ -a \in \mathbb{F} : a + (-a) = (-a) + a = e$.
4. Commutativity: $\forall a, b \in \mathbb{F} : a + b = b + a$.

$\mathbb{F}$ is a multiplicative abelian group $(F, .)$ such that

1. Associativity: $\forall a, b, c \in \mathbb{F}\ :\ ((a\ .\ b)\ .\ c) = (a\ .\ (b\ .\ c))$.
2. Identity element: $\exists\, e \in \mathbb{F}\ : \forall a \in \mathbb{F} : a\ .\ e = a$.
3. Inverse: $\forall$ non-zero $a \in \mathbb{F}\ \exists\, a^{-1} \in \mathbb{F} : a\ .\ a^{-1} = a^{-1}\ .\ a = e$.
4. Commutativity: $\forall a, b \in \mathbb{F} : a\ .\ b = b\ .\ a$.

Distributivity: $\forall a, b, c \in \mathbb{F} : a\ .\ (b + c) = a\ .\ b + a\ .\ c$.

Remark 2.1. In this thesis for any finite field $\mathbb{F}$, we will take the additive identity as '0' and multiplicative identity as '1'. And, briefly we write ab instead of $a.b$.

Definition 2.2. Let $\mathbb{Z}_p$ be the set of integers modulo integer p. If p is any prime number, then the set $\mathbb{Z}_p = \{0, 1, 2, \cdots, p-1\}$ is an additive abelian group denoted as $(\mathbb{Z}_p, +)$ and the set $Z_p^* = \{1, 2, \cdots, p-1\}$ is a multiplicative abelian group $(\mathbb{Z}_p^*, .)$. Hence, Z_p is a finite field.

Definition 2.3. Let $\mathbb{F}_s$ be any subset of finite field $\mathbb{F}$. If F_s is itself a field with the two binary operations of addition and multiplication, i.e. $\forall a, b \in \mathbb{F}_s$ we have $a - b \in \mathbb{F}_s$ and also $ab^{-1} \in \mathbb{F}_s$ such that $b \neq 0$. Then $\mathbb{F}_s$ is termed as subfield of $\mathbb{F}$ and $\mathbb{F}$ is called the Extension field of $\mathbb{F}_s$.

Definition 2.4. Let $\mathbb{F}, \mathbb{F}'$ be any two fields. If there exists a bijective map from $\mathbb{F} \to \mathbb{F}'$

$$\begin{aligned} \sigma : \mathbb{F} &\to \mathbb{F}' \\ a &\to \sigma(a) \end{aligned}$$

such that the field operations of addition and multiplication are preserved i.e. $\forall a, b \in \mathbb{F}$, we have

$$\begin{aligned} \sigma(a + b) &= \sigma(a) + \sigma(b) \\ \sigma(ab) &= \sigma(a)\sigma(b). \end{aligned}$$

We say that $\mathbb{F}$ is isomorphic $\mathbb{F}'$, denoted as $\mathbb{F} \cong \mathbb{F}'$. Any isomorphism of a field with itself is termed as Automorphism. e.g. any field with prime number of elements p, denoted as $\mathbb{F}_p$ is isomorphic to $\mathbb{Z}_p$.

Definition 2.5. For any finite field $\mathbb{F}$, if there exists any positive integer m such that $me = 0$, where e is the multiplicative identity element. Then m is termed as the *characteristic* of $\mathbb{F}$. If there exists no positive integer m such that $me = 0$, then the characterisitic is taken as 0. For any finite field $\mathbb{F}_p$, $\mathbb{F}_{p^n}$ (where $n \geq 1$ any positive integer) is an extension field with p^n elements. Characteristic of any $\mathbb{F}_{p^n}$ is p.

Theorem 2.1. *[54, Theorem 3.10] For any isomorphic fields $\mathbb{F}$ and $\mathbb{F}'$, the characteristic of $\mathbb{F}$ and $\mathbb{F}'$ must be equal.*

Theorem 2.2. *[54, Corollary 3.17] For any finite field $\mathbb{F}$ of characteristic p, with $p \neq 0$ and any two elements $a, b \in \mathbb{F}_p$, we have*

$$(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}$$

where n is any non-negative integer.

Corollary 2.3. *[54, Corollary 3.18] For any finite field $\mathbb{F}$ of characteristic p, with $p \neq 0$ and a non-negative integer n, there exists an automorphism of $\mathbb{F}$ of the form*

$$\sigma_n : a \to a^{p^n} \ (a \in \mathbb{F}).$$

Any sum of *monomials* of the form

$$a_i x^i \qquad ; \ a_i \in \mathbb{F}$$

of degree i in the inderterminate x is termed as a *polynomial* in x over the field $\mathbb{F}$. i.e. a formal sum of the form

$$a_0 + a_1 x + \cdots + a_n x^n; \ a_i \in \mathbb{F}.$$

Let $\mathbb{F}[x]$ be the set of polynomials in x over $\mathbb{F}$. $\mathbb{F}[x]$ is infact a *ring of polynomials* in the indeterminate x over the field $\mathbb{F}$ or *polynomial ring* in x over $\mathbb{F}$, as per usual polynomial addition and multiplication operations. The 0 is the zero of $\mathbb{F}[x]$ and 1 is the identity of $\mathbb{F}[x]$.

Definition 2.6. [54, Definition 5.2] For any finite field $\mathbb{F}_p$ and a polynomial ring $\mathbb{F}_p[x]$ in the indeterminate x over $\mathbb{F}_p$. Let $p(x)$ be an irreducible polynomial in $\mathbb{F}_p[x]$. Then $\mathbb{F}_p[x]/p(x)$ is a field. Also known as the Residue Class Field of the polynomial ring $\mathbb{F}_p[x]$ modulo the irreducible polynomial $p(x)$, with additions and multiplications performed modulo irreducible polynomial $p(x)$. If $p(x)$ is of degree n, then $\mathbb{F}_p[x]/p(x)$ defines an n-th degree extension of $\mathbb{F}_p$ termed as $\mathbb{F}_{p^n}$ and all the elements of $\mathbb{F}_p[x]/p(x)$ can be expressed as

$$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \ with \ a_i \in \mathbb{F}_p.$$

We can also define a vector space $\mathbb{F}_p^n$ of dimension n over finite field $\mathbb{F}_p$ where each element corresponds to a vector with n co-ordinates over $\mathbb{F}_p$ i.e. $\forall b \in \mathbb{F}_p^n$ we have $b = (b_0, b_1, \cdots, b_{n-1})$ with $b_i \in \mathbb{F}_p$ for $0 \leq i \leq n-1$.

Definition 2.7. [56, Definition 2.16] For any finite field $\mathbb{F}_p$, we have a canonical bijective map ϕ between its n-th degree extension $\mathbb{F}_{p^n}$ and n-dimensional vector space $\mathbb{F}_p^n$. i.e.

$$\begin{aligned} \phi : \mathbb{F}_{p^n} &\to \mathbb{F}_p^n \\ \phi(a) &\to b \\ a_i &\to b_i \qquad \text{for} \quad 0 \leq i \leq n-1. \end{aligned}$$

Hence we can say that $\mathbb{F}_{p^n}$ is isomorphic to $\mathbb{F}_p^n$ i.e. $\mathbb{F}_{p^n} \cong \mathbb{F}_p^n$.

Definition 2.8. Let $\mathbb{F}_{p^n}$ be an n-th degree extension of finite field $\mathbb{F}_p$ with characteristic prime p. Then for any element $\alpha \in \mathbb{F}_{p^n}$, the elements $\alpha, \alpha^p, \alpha^{p^2}, \cdots, \alpha^{p^{n-1}}$ are called the *conjugates* of α over $\mathbb{F}_p$.

Definition 2.9. [54, Definition 7.5] For any element $\alpha \in \mathbb{E} := \mathbb{F}_{p^n}$ and $\mathbb{F} := \mathbb{F}_p$, the trace $Tr_{\mathbb{E}/\mathbb{F}}(\alpha)$ of α over $\mathbb{F}$ is defined as the sum of its conjugates over $\mathbb{F}$ i.e.

$$Tr_{\mathbb{E}/\mathbb{F}}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{n-1}}.$$

Theorem 2.4. *[54, Theorem 7.12] For any element $\alpha, \beta \in \mathbb{E} := \mathbb{F}_{p^n}$ and $c \in \mathbb{F} := \mathbb{F}_{p^s}$ such that $s|n$, the trace $Tr_{\mathbb{E}/\mathbb{F}}$ function satisfies the following axioms*

1. $Tr_{\mathbb{E}/\mathbb{F}}(\alpha + \beta) = Tr_{\mathbb{E}/\mathbb{F}}(\alpha) + Tr_{\mathbb{E}/\mathbb{F}}(\beta)$
2. $Tr_{\mathbb{E}/\mathbb{F}}(c\alpha) = cTr_{\mathbb{E}/\mathbb{F}}(\alpha)$
3. $Tr_{\mathbb{E}/\mathbb{F}}(c) = nc$
4. $Tr_{\mathbb{E}/\mathbb{F}}(\alpha^p) = Tr_{\mathbb{E}/\mathbb{F}}(\alpha)$

if $\mathbb{F}$ is the smallest prime subfield of $\mathbb{F}_{p^n}$, then the trace $Tr_{\mathbb{E}/\mathbb{F}}(\alpha)$ is termed as the Absolute Trace of α and denoted as $Tr_E(\alpha)$.

2.3 Characters and Character Sums

Considering $\mathbb{F}_p$ as a finite abelian group of order p with identity element 1. *Character* χ of $\mathbb{F}_p$ is defined as a homomorphism from $\mathbb{F}_p$ to a multiplicative group $\mathbb{C}$ of complex numbers of absolute value 1. The homomorphism is defined as

$$\chi(\gamma_1\gamma_2) = \chi(\gamma_1)\chi(\gamma_2) \qquad \forall \gamma_1, \gamma_2 \in \mathbb{F}_p.$$

For any finite cyclic group $\mathbb{F}_{p^n}$ of order p^n, let α be the generator of $\mathbb{F}_{p^n}$ such that every element can be expressed as a power j of α with $0 \leq j \leq p^n - 1$, the function

$$\chi_j(\alpha^k) = e^{2\pi ijk/p^n} \qquad k = 0, 1, \cdots, p^n - 1$$

define the character of $\mathbb{F}_{p^n}$. In other words, if χ is any character of $\mathbb{F}_{p^n}$ then $\chi(\alpha)$ is an p^n-th root of unity, i.e. $\chi(\alpha) = e^{2\pi ij/p^n}$ for some j with $0 \leq j \leq p^n - 1$. To each character $\chi(\alpha)$, there is associated a complex conjugate character $\bar{\chi}(\alpha) = \overline{\chi(\alpha)}$ for any $\alpha \in \mathbb{F}_{p^n}$. Let $\mathbb{F}_{p^n}$ represent an additive abelian group with prime field $\mathbb{F}_p$. If $Tr : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is the absolute trace from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, the function defined by

$$\chi_1(\alpha) = e^{2\pi iTr(\alpha)/p} \qquad \forall \alpha \in \mathbb{F}_{p^n} \tag{2.6}$$

is called the *canonical additive character* of $\mathbb{F}_{p^n}$, since

$$\chi_1(\alpha_1 + \alpha_2) = \chi_1(\alpha_1)\chi_1(\alpha_2) \qquad \forall \alpha_1, \alpha_2 \in \mathbb{F}_{p^n}.$$

All the additive characters of $\mathbb{F}_{p^n}$ can be expressed in terms of χ_1 e.g. for any $\beta \in \mathbb{F}_{p^n}$, we can write

$$\chi_\beta(\alpha) = \chi_1(\beta\alpha).$$

Using property of trace map, it is trivial to observe that for additive characters we have

$$\chi_1(\alpha^p) = \chi_1(\alpha).$$

Definition 2.10. [39, Section 5.4] Let χ be a non-trivial additive character of $\mathbb{E} := \mathbb{F}_{p^n}$ and $f(x)$ be a polynomial of positive degree over $\mathbb{E}$. Weil sum of the $f(x)$ is defined as:

$$\sum_{x\in\mathbb{E}} \chi(f(x)).$$

We would like to mention few results before considering the usefulness of Weil Sum for our purpose.

Theorem 2.5. *[39, Theorem 5.4] Let χ be a character of finite abelian group G and $\alpha \in G$, then:*

$$\sum_{\alpha\in G} \chi(\alpha) = 0$$

if $\alpha \neq 1$ and $\chi \in G'$ (group of characters of G), then

$$\sum_{\chi\in G'} \chi(\alpha) = 0$$

Theorem 2.6. *[39, Theorem 5.5] The cardinality of characters of finite abelian group G is equal to $|G|$.*

Following directly from Theorem 2.5 and Theorem 2.6, we have following *Orthogonality Relations* for charcters

1. Let χ and ζ be character of G, then

$$\frac{1}{|G|}\sum_{\alpha\in G} \chi(\alpha)\overline{\zeta(\alpha)} = \begin{cases} 0 & \text{for} \quad \chi \neq \zeta \\ 1 & \text{for} \quad \chi = \zeta \end{cases}$$

2. Let α_1, α_2 be elements of G, then

$$\frac{1}{|G|}\sum_{\chi\in G'} \chi(\alpha_1)\overline{\chi(\alpha_2)} = \begin{cases} 0 & \text{for} \quad \alpha_1 \neq \alpha_2 \\ 1 & \text{for} \quad \alpha_1 = \alpha_2 \end{cases}$$

Now, in order to determine the number of solutions of any arbitrary map $f : G \times \cdots \times \mathbb{G} \to G$, we can use orthogonality relations of character of G and Weil sum of f. For fixed $\gamma \in G$, the number $N(\gamma)$ of n-tuples $(x_1, \cdots, x_n) \in G^n$ such that $f(x_1, \cdots, x_n) = \gamma$ is given by:

$$N(\gamma) = \frac{1}{|G|}\sum_{x_1\in G} \cdots \sum_{x_n\in G}\sum_{\chi\in G'} \chi(f(x_1, \cdots, x_n))\overline{\chi(\gamma)}. \tag{2.7}$$

2.4 NP-Completeness

Definition 2.11. [38, Definition 4.2] A given Decision problem belongs to the class-NP if, any instance of this problem can be answered by an adversary possesing unlimited computing power. Adversary can also provide a Polynomial time Certificate in case of answer *YES*, as an evidence.

Definition 2.12. [38, Definition 4.3] Given $\mathbb{P}_1, \mathbb{P}_2$ two decision problems, we say that $\mathbb{P}_1$ reduces to $\mathbb{P}_2$ (in polynomial time) if there exists an algorithm, polynomial in input length of $\mathbb{P}_1$ such that one can construct an instance P_2 of $\mathbb{P}_2$ from given instance P_1 of $\mathbb{P}_1$. And that the answer for P_1 is the same as the answer for P_2.

Definition 2.13. [38, Definition 4.6] A decision problem D in NP is said to be NP-Complete if every other problem O in NP can be reduced to D in polynomial time.

CHAPTER 3

Multivariate Public Key Cryptography

Multivariate quadratic cryptography is considered as one of the secure building block in post quantum era. Many constructions have been presented in this domain and the researchers have devoted reasonable resources to develop secure cryptosystems based on multivariate equations solving problem. Quite a few basic constructions have been successfully attacked at least theoretically, however many still remain viable. The theory of multivariate quadratic (MQ) cryptography is still evolving as more and more insight is developed about its trapdoor design and the security of resultant cryptosystem. The scrutiny of the time complexity of successful attacks also continues and debate is still on. In this chapter we will introduce the mathematical problem of MQ cryptography. The information presented in this chapter is based on the taxonomy of such schemes presented by C.Wolf and B.Preneel in [55]

3.1 Multivariate System of Equations

Let $x_1, x_2, \ldots, x_n$ be the variables over $\mathbb{F}$. For given $n, d, m \in \mathbb{N}$ where n is the number of variables, d is the degree value of highest degree term and m is the number of polynomials, we define the system P of m polynomial equations in n variables with maximum degree d i.e. $P := (P_1, P_2, \ldots, P_m)$ with each P_i having the following form

$$P_i(x_1, x_2, \ldots, x_n) := \sum_{k \in \mathcal{K}} \alpha_{i,k} \prod_{j=1}^{d} x_{k_j} \qquad \text{for} \quad 1 \leq i \leq m \tag{3.1}$$

where $\mathcal{K}$ is a d-dimensional vector defined as: $k := (k_1, k_2, \ldots, k_d)$ for $k \in \mathcal{K}$ s.t each $k_i \in \{1, \ldots, n\}$ for $d \geq 1$. For $d = 0$, we have $k = 0$ with $x_0 = 1$ as a convention. Following the definition above the problem of solving multivariate system of equations over F is defined as follows:

Definition 3.1. Let $\mathcal{M}$ be a map from $\mathbb{F}^n$ to $\mathbb{F}^m$ defined as $F : P_i(x_1, \ldots, x_n) = y_i$ where $x := (x_1, \ldots, x_n) \in \mathbb{F}^n$ and $y := (y_1, \ldots, y_m) \in \mathbb{F}^m$ and each P_i for $1 \leq i \leq m$ be as defined in (3.1). Then solving multivariate system of equations over $\mathbb{F}$ is equivalent to inverting the map $\mathcal{M}$ i.e. for given $y \in \mathbb{F}^m$ finding a solution $x \in \mathbb{F}^n$.

One of the important parameters is the resultant key length if such map $\mathcal{M}$ has to be used as a public key primitive. First step is to compute the number of terms in n variables of degree d over the finite field F.

$$\mathcal{T}_d(\mathbb{F}^n) := \begin{cases} \sum_i^{min(|\mathbb{F}|-1,d)} \binom{n}{i} & \text{for} \quad d > 0 \\ 1 & \text{for} \quad d = 0 \end{cases}$$

since $x^{|\mathbb{F}|-1} = 1 \quad \forall x \in \mathbb{F}$. The total number of terms in a single polynomial over $\mathbb{F}$ of maximum degree d in n variables as

$$\mathcal{T}^d(\mathbb{F}^n) := \sum_{i=0}^{d} \mathcal{T}_i(\mathbb{F}^n).$$

Overall public key-length $\mathcal{L}$ for this system of m equations can be stated as

$$\mathcal{L}(\mathbb{F}, n, m, d) := m\mathcal{T}^d(\mathbb{F}^n) log_2|\mathbb{F}| = O(mn^d). \tag{3.2}$$

3.2 Multivariate Quadratic System of Equations

Any mathematical structure when used as a cryptographic primitive has to address certain fundamental issues, in order to be practicable. One such concern is of resultant key size. As mentioned in the last section, multivariate system of equations when used as a building block in any cryptographic system gives the resultant key size as $O(mn^d)$ or $O(n^{d+1})$ for $m = n$. Hence, key size is exponential in terms of maximum degree d of polynomials. In order to be used as cryptographic primitive we want this d to be as small as possible. In quadratic system of polynomial equations, we have this $d = 2$ and even inversion of MQ polynomial maps over $\mathbb{F}$ have been proven $\mathcal{NP}$-complete(*cf.* Section 2.4) [47]. This makes quadratic system of polynomial equations, a viable candidate for public key cryptosystems. This field of cryptography is termed as *Multivariate Quadratic (MQ) Cryptography* and the fundamental problem in Definition 3.1 for this case is termed as an *MQ-Problem.*

3.3 Multivariate Quadratic Cryptosystems

MQ cryptosystems are public key cryptosystems with separate public and private keys that are non-trivially related but extracting the private key from the public key is considered computationally infeasible.

3.3.1 Public Key

In MQ public key cryptosystems the public key is represented by a system of quadratic polynomial equations and can be defined as follows

Definition 3.2. Let $\mathcal{P} := (P_1, \ldots, P_m)$ be a polynomial vector with each P_i defined as a quadratic polynomial over $\mathbb{F}$ in n variables for $1 \leq i \leq m$. Then the map $\mathcal{P} : \mathbb{F}^n \to \mathbb{F}^m$ defined as

$$\begin{aligned} P_1(x_1, \ldots, x_n) : &= \sum_{1 \leq j,k \leq n} \alpha_{1,j,k} x_j x_k + \sum_{1 \leq j \leq n} \beta_{1,j} x_j + \gamma_1 \\ &\vdots \\ P_m(x_1, \ldots, x_n) : &= \sum_{1 \leq j,k \leq n} \alpha_{m,j,k} x_j x_k + \sum_{1 \leq j \leq n} \beta_{m,j} x_j + \gamma_m \end{aligned}$$

where $\alpha_{i,j,k}, \beta_{i,j}, \gamma_i \in \mathbb{F}$, represents the public key of the MQ cryptosystem.

We would like to mention an important observation made initially by Kipnis and Shamir [36] in their attack on MQ cryptosystems and later by C.Wolf and B.Preneel [55]. They termed the above mentioned Definition (3.2) as multivariate representation for public key of the MQ cryptosystem over $\mathbb{F}$ and stated the following equivalent univariate representation.

Theorem 3.1. *([55, Theorem 2.16]) Let $n, m \in \mathbb{N}$ with $k := max\{n, m\}$. Let $\mathbb{E}$ be a k-dimensional extension of $\mathbb{F}$ such that $q := |F|$. For a given public system ($\mathcal{P}$) of MQ polynomial equations over $\mathbb{F}[x_1, \ldots, x_n]$ as in Definition (3.2) there exists a unique univariate polynomial ($\mathcal{P}'$) over $\mathbb{E}[X]$ of the form*

$$\mathcal{P}'(X) := \sum_{0 \leq i \leq D} A_i X^{q^{\alpha_i} + q^{\beta_i}} + \sum_{0 \leq j \leq L} B_j X^{q^{\gamma_j}} + C$$

with $A_i, B_j, C \in \mathbb{E}$, $D, L < q^k - 1 \in \mathbb{N}$ and $\alpha_i \geq \beta_i$, $q^{\alpha_i} + q^{\beta_i} \leq D$, $q^{\gamma_j} \leq L$ that computes the same function as $\mathcal{P}$ i.e.

$$\mathcal{P}'(X) = \phi^{-1}(\mathcal{P}(R(\phi(X)))) \; \forall X \in \mathbb{E} \tag{3.3}$$

and conversely

$$\mathcal{P}(x) = R(\phi(\mathcal{P}'(\phi^{-1}(x)))) \; \forall x \in \mathbb{F}^k \tag{3.4}$$

where ϕ is the canonical bijective map from $\mathbb{E}$ to $\mathbb{F}^k$ i.e. k-dimensional vector space over $\mathbb{F}$ and its inverse canonical bijective map ϕ^{-1} is from $\mathbb{F}^k$ to $\mathbb{E}$. And R is the reduction/projection map from $\mathbb{F}^n$ to $\mathbb{F}^m$ if $n > m$ or $\mathbb{F}^m$ to $\mathbb{F}^n$ if $m > n$. The converse is also true.

Proof. A detailed proof can be found in [55] however we will just mention the sketch of the proof for completeness. Initially we take the homogeneous case $m = n$. Given a multivariate polynomial vector $\mathcal{P} \in (\mathbb{F}[x_1, \ldots, x_n])^n$ as in Definition 3.2, we use the counting argument to observe that total number of terms in a single polynomial are $\binom{n}{2} + n + n + 1 = \frac{n(n+3)}{2} + 1$ over $\mathbb{F} \neq GF(2)$ and $\binom{n}{2} + n + 1 = \frac{n(n+1)}{2} + 1$ over $\mathbb{F} = GF(2)$ which correspond to monomials of the form $x_j x_k, x_j, \gamma_i$ for $1 \leq i, j, k \leq n$. In characteristic 2, we have $x_i^2 = x_i$. Overall, total number of choices for these quadratic polynomials over $\mathbb{F} \neq GF(2)$ are $q^{n(\frac{n(n+3)}{2}+1)}$ and over

$\mathbb{F} = GF(2)$ are $q^{n(\frac{n(n+1)}{2}+1)}$. Similarly count for univariate polynomials $\mathcal{P}'$ can be evaluated by counting the quadratic, linear and constant terms to observe the equality with the earlier count of multivariate representation. Uniqueness can be observed from the fact that these polynomials are mappings from $\mathbb{F}^n$ to $\mathbb{F}^n$ in multivariate or $\mathbb{E}$ to $\mathbb{E}$ in univariate representation and the canonical bijection ϕ can easily be extended to polynomial rings $\mathbb{E}[X]$ and $\mathbb{F}[x_1, \ldots, x_n]$. Two different mappings with same polynomial representation or vice versa is not an option. For the heterogeneous case $m \neq n$ assuming $n > m$, we use the reduction map $R : F^n \to F^m$ as stated in the statement of theorem. The reduction map can be defined as follows:

$$R(x_1, x_2, \ldots, x_m, x_{m+1}, \ldots, x_n) := (x_1, \ldots, x_m)$$

and its inverse

$$R^{-1}(x_1, \ldots, x_m) = (x_1, x_2, \ldots, x_m, 0, \ldots, 0).$$

For $m > n$, the reduction/projection map can be defined converse to the mentioned case. The remaining proof follows. □

Using the Kipnis and Shamir ideas [36] in addition with/without the reduction (projection) maps explained in Theorem 3.1 one can obtain the univariate representation from multivariate representation (3.3) and multivariate from univariate representation (3.4) for heterogeneous / homogeneous quadratic system of polynomial equations. C.Wolf [57] also explains that using polynomial interpolation with evaluations at $n(n+1)(n+2)/2$ points, a multivariate representation from a given univariate representation for the quadratic system of polynomial equations can be obtained.

3.3.2 Private Key

For a given MQ public key as above which in general can be considered as a one-way map $\mathcal{P} : \mathbb{F}^n \to \mathbb{F}^m$, the equivalent private key termed as the *MQ-trapdoor* is defined as follows:

Definition 3.3. Let $\mathcal{P}$ be a given public key as in Definition (3.2) for an MQ cryptosystem over $\mathbb{F}$, the corresponding private key is given by a composition of three invertible maps $(S, P, T) \in (\text{Aff}^{-1}(\mathbb{F}^n)) \times \text{MQ}(\mathbb{F}^n, \mathbb{F}^m) \times (\text{Aff}^{-1}(\mathbb{F}^m))$ evaluated from right to left. Here $\text{Aff}^{-1}(\mathbb{F}^n)$ is an invertible affine map from $\mathbb{F}^n$ to $\mathbb{F}^n$, $\text{Aff}^{-1}(\mathbb{F}^m)$ is an invertible affine map from $\mathbb{F}^m$ to $\mathbb{F}^m$ and $\text{MQ}(\mathbb{F}^n, \mathbb{F}^m)$ is a MQ map from $\mathbb{F}^n$ to $\mathbb{F}^m$ defined by a quadratic polynomial (or system of quadratic polynomials) over $\mathbb{F}$.

The affine transformations in Definitions (3.3) can be defined as follows

Definition 3.4. Let $a_1, \ldots, a_n$ be n polynomials of maximum degree 1 over $\mathbb{F}$, i.e. $a_i := \alpha_{i,1}x_1 + \ldots + \alpha_{i,n}x_n + \beta_i \ \forall 1 \leq i, j \leq n$ with $\alpha_{i,j}, \ \beta_i \in \mathbb{F}$. Let

$A_{mv}(x) := (a_1(x), \ldots, a_n(x))$ for $x := (x_1, \ldots, x_n) \in \mathbb{F}^n$ (i.e. n-dimensional vector space over $\mathbb{F}$). Then $A_{mv}(x)$ is a multivariate representation of an affine transformation from $\mathbb{F}^n$ to $\mathbb{F}^n$. Moreover, for $0 \leq i \leq n$ let $A_i, B \in \mathbb{E}$ (i.e. an n-dimensional extension of $\mathbb{F}$) . Then $A_u(x) := \sum_{i=0}^{n-1} A_i X^{q^i} + B$ for $X \in \mathbb{E}$ is the univariate representation of an affine transformation from $\mathbb{E}$ to $\mathbb{E}$.

Definition 3.5. Let $S_a \in \mathbb{F}^{n \times n}$ be an $(n \times n)$ matrix over $\mathbb{F}$ and $s_v := (s_1, \ldots, s_n) \in \mathbb{F}^n$ be an n-dimensional vector over $\mathbb{F}$. Then the matrix representation $A_m(x)$ of an affine transformation for $x := (x_1, \ldots, x_n) \in \mathbb{F}^n$ can be expressed as:

$$A_m(x) = S_a x + s_v.$$

It can be observed that co-efficients $\alpha_{i,j}$ and β_i in the multivariate representation correspond to the (i, j)-th element and s_i in equivalent matrix representation in definitions above. Hence, multivariate representation can be trivially extracted from matrix representation and vice versa.

Transformation of these representations from univariate to multivariate (matrix) representation and vice versa, is important from the perspective of cryptanalysis of these systems as we will see later in attacks on HFE MQ cryptosystems. Using these representations the problem of recovering the private key can be transformed to solving a related algebraic problem of MinRank. In order to transfer the affine transformation in univariate representation to matrix (multivariate representation) we have the following result from [55].

Lemma 3.2. *[55, Lemma 2.2.7] There exists an efficient algorithm to transfer an affine transformation from univariate to matrix(or multivariate) representation and vice versa.*

Proof. Given an affine transformation in univariate representation as $A_u(x) := \sum_{i=0}^{n-1} A_i X^{q^i} + B$ for $A_i, B, X \in \mathbb{E}$. In order to obtain the corresponding matrix representation $A_m(x) = S_a x + s_v$ for $S_a \in \mathbb{F}^{n \times n}$ and $s_v \in \mathbb{F}^n$, we use the following equality by construction:

$$\phi(A_u(X)) = S_a(\phi(X)) + s_v$$

where ϕ is the canonical bijection from $\mathbb{E}$ to $\mathbb{F}^n$ and ϕ^{-1} is its inverse from $\mathbb{F}^n$ to $\mathbb{E}$. Let $\gamma_i \in \mathbb{F}^n$ for $1 \leq i \leq n$ with i-th component of the vector as 1 with remaining as 0 and γ_0 be the all zero n-dimensional vector over $\mathbb{F}$. It is observed that $S_a(\gamma_0) + s_v = s_v$ and similarly $S_a(\gamma_i) = S_{a_i}$ where S_{a_i} is the i-th column of S_a. Hence, directly from the construction, we can evaluate the matrix representation A_m from univariate representation A_u as follows

$$\begin{aligned} S_{a_i} &: = \phi(A_u(\phi^{-1}(\gamma_i))) \\ s_v &: = \phi(A_u(\phi^{-1}(\gamma_0))) \end{aligned}$$

For the converse, we have a given matrix representation $A_m(x) = S_a x + s_v$ for the affine transformation and we need to extract the equivalent univariate representation $A_u(x) := \sum_{i=0}^{n-1} A_i X^{q^i} + B$. Now again by construction, we have

$S_a(\gamma_0) + s_v = A_u(0) = B$. To determine the co-efficients A_i for $0 \leq i \leq n-1$, we equate this problem to solving system of linear equations such that the corresponding matrix of linear transformation is of full rank n in this case. For given $X_i \in \mathbb{E}$ with $1 \leq i \leq j$ and $j \geq n$, we solve the following matrix equation for A_i where $1 \leq i \leq n$.

$$M_X A = S$$

$$\begin{pmatrix} X_1^{q^0} & X_1^{q^1} & \cdots & X_1^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ X_i^{q^0} & X_i^{q^1} & \cdots & X_i^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ X_j^{q^0} & X_j^{q^1} & \cdots & X_j^{q^{n-1}} \end{pmatrix} \begin{pmatrix} A_0 \\ \vdots \\ A_i \\ \vdots \\ A_{n-1} \end{pmatrix} = \begin{pmatrix} S_a(\phi(X_0)) \\ \vdots \\ S_a(\phi(X_i)) \\ \vdots \\ S_a(\phi(X_j)) \end{pmatrix}$$

To obtain a unique solution we need the matrix M_X to be of full rank. Obtaining such a full rank matrix can be performed in polynomial time by increasing j and reducing via Gauss reduction until we get a matrix of full rank n. The rank of $j \times n$ matrix is upper bounded by number of columns n. □

3.3.3 MQ Trapdoors

Based on the design of private key 3-tuple (S, P, T), especially the central invertible quadratic map $P \in \mathrm{MQ}(\mathbb{F}^n, \mathbb{F}^m)$, C.Wolf and B.Preneel [55] classified the MQ cryptosystems in the following four general blocks.

3.3.3.1 Unbalanced Oil and Vinegar Schemes (UOV)

Kipnis, Patarin and Goubin [37] introduced *Unbalanced Oil and Vinegar* schemes as a generalisation of original *Oil and Vinegar* scheme by Patarin [51].

Definition 3.6. Let $\mathbb{F}$ be a finite field and $n, m \in \mathbb{N}$ with $m < n$. The system of quadratic polynomial equations $P := (P_1, \ldots, P_n) \in (\mathbb{F}[x_1, \ldots, x_n])^n$ s.t.

$$P_i(x_1, \ldots, x_n) := \sum_{k=1}^{n-m} \sum_{l=1}^{n} \alpha_{i,j,k} x_k x_l + \sum_{k=1}^{n} \beta_{i,k} x_k + \gamma_i$$

where $\alpha_{i,j,k}, \beta_{i,k}, \gamma_i \in \mathbb{F}$ is an UOV shaped central trapdoor for the MQ cryptosystem. Here x_j for $1 \leq j \leq n-m$ are termed as vinegar variables and x_j for $n-m \leq j \leq n$ are termed as oil variables.

The main consideration in this scheme is that vinegar variables are combined quadratically with other vinegar variables , however oil variables are only combined quadratically with other vinegar variables. To construct the private key, random values are first assigned to vinegar variables and the resultant system

of linear equations in oil variables is solved using methods like Gaussian elimination. So private key construction is not as complex as it seems. In addition, unbalanced oil and vinegar schemes also use one affine transformation S instead of two (S, T) as in general case, to hide the central quadratic map P. The other affine transformation T can be taken as an identity transformation.

3.3.3.2 Stepwise Triangular Systems (STS)

In *Stepwise Triangular* MQ systems, the central quadratic polynomial map P is defined over $\mathbb{F}$ like Unbalance Oil and Vinegar schemes. The scheme was introduced by C.Wolf, An Braeken, and B.Preneel [58].

Definition 3.7. Let $P := (P_1, \ldots, P_r, \ldots, P_{(m-1)r+1}, \ldots, P_{mr})$ be system of polynomial equation over $\mathbb{F}$ such that the step-wise polynomials are defined as: where

$$
\begin{array}{ll}
\textit{Step } 1 \left\{ \right. & P_1(x_1, \ldots, x_r) \\
 & \vdots \\
 & P_r(x_1, \ldots, x_r) \\
\vdots & \\
\textit{Step } s' \left\{ \right. & P_{(s'-1)r+1}(x_1, \ldots, x_r, \ldots, x_{(s'-1)r+1}, \ldots, x_{s'r}) \\
 & \vdots \\
 & P_{s'r}(x_1, \ldots, x_r, \ldots, x_{(s'-1)r+1}, \ldots, x_{s'r}) \\
\vdots & \\
\textit{Step } s \left\{ \right. & P_{(s-1)r+1}(x_1, \ldots, x_r, \ldots, x_{(s'-1)r+1}, \ldots, x_{s'r}, \ldots, x_{n-r+1}, \ldots, x_n) \\
 & \vdots \\
 & P_{sr}(x_1, \ldots, x_r, \ldots, x_{(s'-1)r+1}, \ldots, x_{s'r}, \ldots, x_{n-r+1}, \ldots, x_n)
\end{array}
$$

Figure 3.1: Stepwise Triangular Systems

r controls the step-width(number of new variables) and step-height(number of new equations) of the system of quadratic equations. The n variables are divided in steps $r_1, \ldots, r_s$ such that $n = \sum_i^s r_i$ and m equations are divided in steps $m_1, \ldots, m_s$ such that $m = \sum_i^s m_i$. In each step i for $1 \leq i \leq s$, r_i new variables are added to r_{i-1} variables in step $i-1$ for m_i new equations. This system of quadratic polynomial map over $\mathbb{F}$ defines central quadratic polynomial map P in STS type MQ system.

Generally, STS is used in the settings of regular STS schemes where each $r_i = r = m_i$ i.e. r new equations and r new variables are introduced at each step i. In practice this becomes a bijective structure in each level with q^r possible new vectors $(x_{(i-1)r+1}, \ldots, x_{ir})$ which satisfy the r new equations over $\mathbb{F}$ with

$|\mathbb{F}| = q$ and hence inversion gives a unique solution making the overall regular STS scheme very efficient, especially useful in signature schemes based on regular STS.

3.3.3.3 Matsumoto-Imai Scheme (MIA)

The scheme was introduced by Matsumoto and Imai [40]. This scheme uses two different finite fields for its trapdoor quadratic polynomial map.

Definition 3.8. Let $\mathbb{F}$ be a finite field and $\mathbb{E}$ be its n degree extension such that $|\mathbb{F}| := q$. Let $h \in \mathbb{N}$ such that $gcd(q^n - 1, q^h + 1) = 1$, then the permutation polynomial

$$P(X) := (X)^{q^h+1} \qquad \forall \quad X \in \mathbb{E}$$

defines the central quadratic polynomial map P for the MIA scheme. We may write this univariate quadratic polynomial in the form of system of multivariate quadratic equations over $\mathbb{F}$ as $P' := \phi \circ P \circ \phi^{-1}(x)$ for $x = (x_1, \ldots, x_n) \in \mathbb{F}^n$ where ϕ is the canonical bijection between the extension field $\mathbb{E}$ and n-dimensional vector space $\mathbb{F}^n$ over $\mathbb{F}$.

The construction is simple from the perspective of computing private key inversion as it only requires evaluating inverse of $q^h + 1$ modulo $q^n - 1$ which can be precomputed. In addition being a permutation map, we have a unique solution for all Y such that $P(X) = Y$. From the attacker's perspective the design has an inherent weakness since such permutations are limited in number. But the author in [40] claims that the hardness of the MIA scheme does not rely in determining P but on the difficulty of determining the two affine maps S, T for given public($\mathcal{P}$) and private(P) quadratic polynomial maps respectively.

3.3.3.4 Hidden Field Equations (HFE)

Patarin [51] successfully attacked the MIA scheme and later gave a generalisation of the MIA scheme in [48] using a univariate quadratic polynomial over finite field $\mathbb{E}$ i.e. n degree extension of $\mathbb{F}$, instead of a monomial q^h+1 used as a permutation map in MIA.

Definition 3.9. Let $\mathbb{F}$ be a finite field and $\mathbb{E}$ its n degree extension such that $|\mathbb{F}| := q$, then

$$P(X) = \sum_{i,j} A_{i,j} X^{q^i+q^j} + \sum_{0 \leq k \leq D} B_k q^k + C \qquad \forall \quad X \in \mathbb{E}$$

such $q^i + q^j, q^k \leq D$ and co-efficients $A_{i,j}, B_i, C \in \mathbb{E}$ define the central quadratic polynomial map P for the HFE scheme. We may write this univariate quadratic polynomial in the form of system of multivariate quadratic equations over $\mathbb{F}$ as $P' := \phi \circ P \circ \phi^{-1}(x)$ for $x = (x_1, \ldots, x_n) \in \mathbb{F}^n$ using canonical bijective map ϕ as in Definition 3.8.

The degree of the polynomial P is upper bounded by D to allow efficient inversion of the equation $P(X) = Y$ for given $Y \in \mathbb{E}$. There are deterministic algorithms for this inversion in time polynomial in D and the dimension n of extension field $\mathbb{E}$ over $\mathbb{F}$. Thus, for the efficiency both are kept small. Unlike MIA, for HFE this map is not surjective and requires random redundancy bits to allow inversion.

Apart form these basic types of trapdoors for the central polynomial map P in MQ cryptosystems, there are many other variants of these schemes which are discussed in [55]. However, we shall only be discussing the HFE variants in last part of this thesis.

3.4 Equivalent Keys

The MQ cryptosystems are generally constructed by first choosing the private central quadratic polynomial P, and then computing the resultant polynomial map after mixing with the two affine maps S, T. The public key $\mathcal{P}$ is the multivariate representation of this resultant quadratic polynomial map. So, in general, there is a large key space for these schemes. However, C.Wolf and B.Preneel [59] identified the equivalence among these keys based on the concept of sustainers which allow the variations in private key without altering the shape of trapdoor and giving the same resultant public key. We shall be introducing the concept of equivalent keys, however for interested readers we refer to [59].

Definition 3.10. We call two private keys (S, P, T) and (S', P', T') equivalent if:

$$(S, P, T) = \mathcal{P} = (S', P', T')$$

where $S, S' \in \mathrm{Aff}^{-1}(\mathbb{F}^n)$, $T, T' \in \mathrm{Aff}^{-1}(\mathbb{F}^m)$ and $P, P' \in \mathrm{MQ}(\mathbb{F}^n, \mathbb{F}^m)$ i.e. they lead to the same public key $\mathcal{P}$

The existence of equivalent keys is founded on the concept of sustaining transformation that was defined by Wolf [59] as follows.

Definition 3.11. Given a private key $(S, P, T) \in \mathrm{Aff}^{-1}(\mathbb{F}^n) \times \mathrm{MQ}(\mathbb{F}^n, \mathbb{F}^m) \times \mathrm{Aff}^{-1}(\mathbb{F}^m)$, the sustaining transformations are the transformation pairs of the form $(\lambda, \mu) \in \mathrm{Aff}^{-1}(\mathbb{F}^n) \times \mathrm{Aff}^{-1}(\mathbb{F}^m)$ such that when applied to private key tuple (S, P, T) like

$$\mathcal{P} = (T \circ \mu^{-1}) \circ (\mu \circ P \circ \lambda) \circ (\lambda^{-1} \circ S)$$

does not alter the shape of the central quadratic polynomial map P.

We shall be mentioning briefly few notable sustaining transformations identified in context of MQ cryptosystems in [59]. Corresponding equivalent keys can be trivially derived using these sustaining transformations.

3.4.1 Sustaining Transformations

3.4.1.1 Additive Sustainer

The additive sustainer is applicable to homogeneous MQ cryptosystems i.e. $m = n$ with equal number of variables and equations. Additive sustainers are defined as transformation pairs (λ, μ) such that

$$\begin{aligned} \lambda(X) &:= X + A \qquad A \in \mathbb{E} \\ \mu(X) &:= X + A' \qquad A' \in \mathbb{E}. \end{aligned}$$

In cryptanalysis, these additive sustainers play important role by allowing the adversary to consider only linear transformations S', T' instead of affine transformations S, T as the constant terms are absorbed into central quadratic polynomial map using additive sustainers.

3.4.1.2 Big Sustainer

These sustainers are considered in terms of trapdoor schemes where we consider big field $\mathbb{E}$ operations instead of the small field $\mathbb{F}$. Hence, MIA and HFE are good candidates for these big sustainers. Big sustainers are defined as transformation pairs (λ, μ) such that

$$\begin{aligned} \lambda(X) &:= AX \qquad A \in \mathbb{E} \\ \mu(X) &:= A'X \qquad A' \in \mathbb{E}. \end{aligned}$$

3.4.1.3 Small Sustainer

In contrary to big sustainers, small sustainers consider small field $\mathbb{F}$ vector multiplications such that the resultant central quadratic polynomial map P still belongs to the same class of trapdoors. Hence, UOV and STS are eligible candidates for these schemes. Small sustainers are defined as transformation pairs (λ, μ) such that

$$\begin{aligned} \lambda(x) &:= Diag(\lambda_1, \ldots, \lambda_n)x \qquad x \in \mathbb{F}^n \\ \mu(x) &:= Diag(\mu_1, \ldots, \mu_m)x \qquad x \in \mathbb{F}^m \end{aligned}$$

where $Diag(\lambda_1, \ldots, \lambda_n), Diag(\mu_1, \ldots, \mu_n)$ are the diagonal matrices with co-efficients $\lambda_i, \mu_j \in \mathbb{F}^*$ for $1 \leq i \leq n$ and $1 \leq j \leq m$.

3.4.1.4 Permutation Sustainer

Permutation maps are naturally bijective and invertible, permutation sustainers however have to be carefully applied as the permutations for each affine transformation performs different kind of permutation. The permutation sustainer pair

(λ, μ) is defined as

$\lambda(x) := (x'_1, \ldots, x'_n)\ ;\ x = (x_1, \ldots, x_n) \in \mathbb{F}^n$

$\mu(x) := (P'_1(T(x)), \ldots, P'_m(T(x)))\ ;\ P = (P_1(T(x), \ldots, P_m(T(x))) \in (\mathbb{F}[x_1, \ldots, x_n])^m$

where $(x'_1, \ldots, x'_n)$ represents the permutation of input variables $(x_1, \ldots, x_n)$ and $(P'_1, \ldots, P'_m)$ is the permutation of quadratic polynomial equations $(P_1, \ldots, P_m)$ applied to result of affine transformation T. UOV, STS and HFEv (an HFE variant) are good candidates for this sustainer.

3.4.1.5 Gauss Sustainer

As mentioned earlier for the affine transformations, the quadratic polynomial system of equations can also be represented by matrices over $\mathbb{F}$ using the multivariate representation for quadratic polynomial equations. Gauss sustainers consider the Gauss operations on these matrices i.e. row and column permutations, multiplication of rows and columns by scalars from $\mathbb{F}$ and addition of two rows/columns. All these operations are invertible and hence form a group of sustainers termed as Gauss sustainers.

3.4.1.6 Frobenius Sustainer

Frobenius sustainers consider a class of automorphisms over the extension field $\mathbb{E}$ called Frobenius transformations. They are normally considered for MIA and HFE schemes. In case of MIA the Frobenius mappings are considered over vector space $\mathbb{F}^n$. Frobenius sustainers are defined as:

Definition 3.12. Let $\mathbb{E}$ be an n-dimensional extension of the finite field $\mathbb{F}$ such that $|\mathbb{F}| := q$. The Frobenius sustainer pair (λ, μ) is

$$\lambda(X) := X^{q^i} \qquad \text{for } X \in \mathbb{E} \text{ and } 0 \leq i < n$$
$$\mu(X) := X^{q^j} \qquad \text{for } X \in \mathbb{E} \text{ and } 0 \leq j < n$$

Frobenius transformations are linear maps and invertible. Thus form a group of sustainer termed as Frobenius sustainers.

3.5 Related Problems

In general, inverting a MQ map termed as an *MQ Problem* is considered NP-complete (*cf.* Section 2.4) over finite fields [48]. However, there are few related mathematical problems that are solvable in polynomial or sub-exponential time depending on choice of finite field. In cryptanalytic attacks on MQ systems, the attackers try to reduce in polynomial time the given MQ problem to an instance of these related problems to obtain the solution. Two very related problems are thus of great significance.

3.5.1 Isomorphism of Polynomials (IP)

The IP problem was critical to design of MIA and many other MQ cryptosystems.

Definition 3.13. Given a public key quadratic polynomial map $\mathcal{P}$ and private key quadratic polynomial map P over finite field $\mathbb{F}$ or its finite extension $\mathbb{E}$. The problem of determining the affine transformations $S, T \in \text{Aff}^{-1}(\mathbb{F}^n) \times \text{Aff}^{-1}(\mathbb{F}^m)$ such that $\mathcal{P} := S \circ P \circ T$ is termed as an IP-problem.

The security of IP-problem is discussed in detain in [48, 31] where they discuss the IP-problem with one secret affine map involved i.e the other map can be taken as identity map. There is another recent attack [3] on HFE cryptosystems where the adversary reduces in polynomial time the MQ problem to an instance of IP problem in order to identify family of weak public keys in the design.

3.5.2 Minimum Rank Problem (MinRank)

Multivariate quadratic cryptosystems in their multivariate representation over $\mathbb{F}$ or matrix representation, allow the adversary to reduce the problem of key inversion to solution of another algebraic problem termed as MinRank problem.

Definition 3.14. Let $(A_1, \ldots, A_m) \in \mathbb{F}^{n \times n}$ be the $n \times n$ invertible matrices over $\mathbb{F}$ and $r, m \in \mathbb{N}$. The problem of finding a linear combination of these matrices i.e $\lambda \in \mathbb{F}^m$ such that

$$\text{Rank}(\sum_{i=1}^{m} \lambda_i A_i) \leq r \tag{3.5}$$

Kipnis and Shamir [36] exploited this idea in their attack on HFE type MQ cryptosystems. Later Bettale, J.C Faugere and L. Perret [1] used the similar approach in their latest attack on variants of HFE and multi-HFE.

CHAPTER 4

Linearized Binomial Attack

MQ cryptosystems do not employ random set of quadratic equations in public keys but those which correspond to specifically designed private key MQ trapdoors. This allows easy and efficient inversions in the private key operations. Hence, the security of these cryptosystems is no more guaranteed by NP-hardness of MQ problem. There exist specific weaknesses inherent to the design strategy that can be exploited to launch cryptanalytic attacks. Several major methods have been developed to attack the MQ cryptosystems. Structural attacks rely solely on the specific structure of the trapdoor involved. General attacks use various methods of solving set of multivariate polynomial equations e.g Gröbner basis method and its improvements. One similar general attack has been proposed in [34] by Harayama and Friesen in which they exploit the equivalent univariate representation of the public key polynomial map. Broadly, their attack is an existential forgery attack against the MQ signature schemes to find one valid forged message and signature pair. We shall be mentioning details of there attack in first part of this chapter and later we will give details of our observations regarding their attack and also our contribution to the problem after generalising the work in [34].

4.1 Existential Forgery

MQ cryptosystems are generally considered as a signature scheme. An MQ cryptosystem defined over finite field $\mathbb{F}_q$ of characteristic p, as a digital signature scheme usually give short signatures of size $\mathbb{F}_q^m$ for some integer m. Thus, the birthday attack is generally applicable to the underlying MQ system at the time complexity $O(q^{m/2})$ [12]. The classical way to compute a digital signature $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_n)$ is to first compute the hash $x = (x_1, x_2, \ldots, x_m) \in \mathbb{F}_q^m$ of a message $m \in \mathbb{F}_q^m$. The respective signature $\sigma \in \mathbb{F}_q^n$ is computed by using the inverse private key triple (S^{-1}, P^{-1}, T^{-1})

$$\sigma = \mathcal{P}^{-1}(x) = S^{-1}(P^{-1}(T^{-1}(x))).$$

In order to verify the signature for a received message and signature pair (m, σ), the recipient using public polynomial map $\mathcal{P} := (P_1, \ldots, P_m)$ checks the following

equalities

$$(x_1, \ldots, x_m) = (P_1(\sigma_1, \ldots, \sigma_n), \ldots, P_m(\sigma_1, \ldots, \sigma_n))$$

where x_i, σ_j are the i-th, j-th components of the hash of message m and signature σ respectively for each $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$. According to birthday paradox, a valid signature can be forged in the square root of exhaustive search (see Section 2.1). Adversary produces a list of $q^{m/2}$ evaluations $\mathcal{P}(\sigma)$ of arbitrary signatures σ using public key polynomial map $\mathcal{P}$ and a list of $q^{m/2}$ hash values of arbitrary messages m in the hash image space [12]. Then with probability greater than 50%, one can expect to produce at least one valid message and signature pair (m, σ), which is called *existential forgery*.

4.2 Customized Birthday Attack

T. Harayama and K. Friesen in a recent work [34], proposed a linearized binomial attack (LBA) for MQ systems over finite fields of characteristic 2. They termed the LBA as a customized birthday attack, however it is basically a meet-in-the middle attack [29] which is a variant of normal birthday attack. They observed experimentally that the linearized binomial attack can be asymptotically better by at least a factor of $2^{n/8}$ than the generic birthday attack for MQ signature schemes that have univariate public key polynomial belonging to certain classes of DO polynomials over $\mathbb{F}_{2^n}$. They termed these polynomials as *Weak DO Polynomials*.

Harayama and Friesen [34], only consider the homogeneous MQ signature scheme (i.e. for $m = n$) over $\mathbb{F}_2$ (i.e. $p = 2$) for their proposed LBA. However, we shall be discussing LBA for homogeneous MQ cryptosystems over $\mathbb{F}_p$ where p is any prime. We explain our motivation in Remark 4.1 and prove the validity of our results using Mills [43] and Remark 4.6.

Remark 4.1. Multivariate cryptography is not limited to finite fields of characteristic 2. However, major MQ signature schemes like Rainbow(28, 18, 12, 12)[20], PMI+(136, 6, 18, 8) Perturbed Matsumoto-Imai Plus[55], Quartz or HFEv-(2, 129, 103, 3, 4)[37]; all employ finite fields with characteristic 2. This is due to reduced computational complexity involved. Most of them have been subjected to algebraic(direct) attacks involving use of mathematical tools like Gröbner basis method, Min-Rank problem solving, relinearization etc. to solve a set of multivariate quadratic equations. These attacks are sub-exponential or polynomial time attacks mainly because they employ field equations dependent on field characteristic 2. If the ground field is chosen to be of any characteristic other than 2 then all these attacks become void or at least exponential in terms of time and memory required for solving new field equations[19]. This was our prime motivation in considering LBA for MQ cryptosystems not only over binary finite fields but also over finite fields of odd characteristic.

Let $\mathbb{F}_p$ be finite field with prime p elements and $\mathbb{F}_q$ be an n-dimensional extension of $\mathbb{F}_p$. In the LBA, they assume under the framework of adaptive chosen message

attack that the adversary can obtain messages whose hash values are in the image space of the linearized polynomial $L : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ i.e. $Im(L)$ where $L(y) = y^{p^\delta} - y$.

Similar to normal birthday attack, for LBA with hash space reduced to $p^{n-\delta}$, the adversary produces a list of $p^{(n-\delta)/2}$ evaluations $\mathcal{P}'(x) \in Im(L)$ of arbitrary signatures $x \in \mathbb{F}_{p^n}$ using public key polynomial map $\mathcal{P}'$ where $\mathcal{P}'$ is the univariate representation of public key polynomial map $\mathcal{P}$ (*cf.* Theorem 3.1). Adversary also produces a list of $p^{(n-\delta)/2}$ hashes $H(m) \in Im(L)$ of arbitrary messages $m \in \mathbb{F}_{p^n}$ by making $p^{(n-\delta)/2}$ adaptive chosen message queries to the hashing oracle. Therefore, we are looking for $x_0 \in \mathbb{F}_{p^n}$ values such that $\mathcal{P}'(x_0) = y_0^{p^\delta} - y_0$ for some $y_0 \in \mathbb{F}_{p^n}$. Let

$$h(x, y) = \mathcal{P}'(x) - y^{p^\delta} + y \tag{4.1}$$

where x is the randomly generated signature value, $\mathcal{P}'(x)$ is the evaluation through public polynomial map and $z = y^{p^\delta} - y$ defines the restricted hash space. In other words we are looking for solutions over $\mathbb{F}_{p^n}$ of the bivariate equation:

$$\begin{aligned} h(x, y) &= \mathcal{P}'(x) - y^{p^\delta} + y = 0 \\ &= \sum_{1 \le i \le D} a_i x^{p^{\alpha_i} + p^{\beta_i}} + \sum_{1 \le j \le L} b_j x^{p^{\gamma_j}} - y^{p^\delta} + y = 0. \end{aligned}$$

A major consideration is the complexity calculation of obtaining such a collision. A randomly generated signature $x \in \mathbb{F}_p^n$ maps to the restricted hash message space of cardinality $p^{n-\delta}$ with a probability $p^{n-\delta}/p^n$ and the complexity of obtaining $p^{(n-\delta)/2}$ signatures with corresponding evaluations in reduced hash space $Im(L)$ is $p^n/p^{n-\delta}\sqrt{p^{n-\delta}}$. The overall complexity of LBA can be observed as $\sqrt{\frac{\pi}{2}}p^n/p^{n-\delta}\sqrt{p^{n-\delta}}$ according to birthday paradox. This however, is always greater than that of normal birthday attack $\sqrt{\frac{\pi}{2}p^n}$.

This complexity of LBA needs to be improved in order to make it practical. Harayama and Friesen [34] used Mills [43] results for this purpose that we shall be discussing in the next few sections before returning to the LBA in section 4.2.4.

4.2.1 Equivalent Univariate Representation

Mills [43] in his work on Dembowski Ostrom polynomials obtained certain results that Harayama and Friesen [34] observed useful to the discussion of LBA on MQ cryptosystems. We shall be stating certain relevant results from Mills [43] over $\mathbb{F}_p$ such that p is an odd prime. These results were later extended by Harayama and Friesen [34, 35] to $p = 2$ case. Hence, all the results that we mention subsequent to this are valid for any prime p characteristic finite field $\mathbb{F}_p$ unless stated otherwise.

To evaluate the number of solutions of the bivariate equation in (4.1), one can use the theory of character sums over finite field $\mathbb{F}_p$.

Theorem 4.1. *Let $h(x,y) = \mathcal{P}'(x) - y^{p^\delta} + y = 0$ be a polynomial over $\mathbb{F}_q[x,y]$ with $q := p^n$, then the number of solutions of $h(x,y)$ are given by*

$$N = \frac{1}{|\mathbb{F}_q|} \sum_{\omega \in \mathbb{F}_q} \sum_{x,y \in \mathbb{F}_q} \chi_1(\omega h(x,y)) \tag{4.2}$$

where χ_1 is the canonical additive character over $\mathbb{F}_q$ as defined in (2.6) and $\chi_1(\omega h(x,y))$ is the Weil Sum of $h(x,y)$ over group of characters χ_ω of $\mathbb{F}_q$ such that $\chi_\omega = \chi_1(\omega)$

Proof. Follows directly from (2.7) using (2.6). □

Hence, the Weil Sums can be used to compute the number of solutions desired in LBA. Mills [43] obtained the following equivalent result for these computations of Weil Sum. His result was later extended to even characteristic finite field case by Harayama and Friesen in [34, 35].

Theorem 4.2. *([35, Theorem 2.1.1],[43, Theorem 1.4]) Let $S(a_1, \cdots, a_D, b_1, \cdots, b_L, c)$ be the Weil Sum of the following univariate polynomial*

$$\mathcal{P}'(x) = \sum_{1 \le i \le D} a_i x^{p^{\alpha_i} + p^{\beta_i}} + \sum_{1 \le j \le L} b_j x^{p^{\gamma_j}}.$$

where $D, L \in \mathbb{N}, a_i, b_j, c \in \mathbb{F}_q, \alpha_i \ge \beta_i, p^{\alpha_i} + p^{\beta_i}, p^{\gamma_j} \le p^n - 1$ for each $1 \le i \le D, 1 \le j \le L$. With the translation of co-efficients involved such that $A_i^{p^{t_i}} = a_i \in \mathbb{F}_q$ $(1 \le i \le D)$ and parameters $t_i, y_i, s_i \in \mathbb{Z}$ and $b \in \mathbb{F}_q$ such that $t_i \equiv \beta_i - \beta_1 \bmod n$ $(1 \le i \le D)$ and $y_i = n - s_i$ $(2 \le i \le D)$, $s_i = \alpha_i - \beta_i \ge 0$ $(1 \le i \le D)$ and $b = \sum_{1 \le j \le L} b_j^{p^{e-\gamma_j}}$. Then $S(a_1, \cdots, a_D, b_1, \cdots, b_L)$ can be equivalently expressed as

$$S = \sum_{x \in \mathbb{F}_q} \chi_1\Big(\sum_{i=1}^{D} A_i x^{p^{s_i}+1} + b^{p^{\beta_1}} x\Big). \tag{4.3}$$

*The polynomial $\sum_{i=1}^{D} A_i x^{p^{s_i}+1} + b^{p^{\beta_1}} x$ is the **simplified univariate representation** of $\mathcal{P}'(x)$ with $S(a_1, \cdots, a_D, b_1, \cdots, b_L) = S(A_1, \cdots, A_D, b_1, \cdots, b_L)$.*

Proof. We give the proof from [35] for completeness. Following directly from the statement of the theorem, the proof also involves the translation of co-efficients and exponents using properties of character sums mentioned in section 2.3. Let

the Weil sum of $\mathcal{P}'(x)$ be given as

$$\begin{aligned}
\sum_{x\in\mathbb{F}_q}\chi_1(\mathcal{P}'(x)) &= \sum_{x\in\mathbb{F}_q}\chi_1(\sum_{1\le i\le D}a_i x^{p^{\alpha_i}+p^{\beta_i}}+\sum_{1\le j\le L}b_j x^{p^{\gamma_j}})\\
&= \sum_{x\in\mathbb{F}_q}\chi_1(\sum_{1\le i\le D}a_i x^{p^{\alpha_i}+p^{\beta_i}})\chi_1(\sum_{1\le j\le L}b_j x^{p^{\gamma_j}})\\
&= \sum_{x\in\mathbb{F}_q}\chi_1(\sum_{1\le i\le D}a_i x^{p^{\alpha_i}+p^{\beta_i}})\prod_{1\le j\le L}\chi_1(b_j x^{p^{\gamma_j}})\\
&= \sum_{x\in\mathbb{F}_q}\chi_1(\sum_{1\le i\le D}a_i x^{p^{\alpha_i}+p^{\beta_i}})\prod_{1\le j\le L}\chi_1(b_j^{e-\gamma_j} x^{p^e})\\
&= \sum_{x\in\mathbb{F}_q}\chi_1(\sum_{1\le i\le D}a_i x^{p^{\alpha_i}+p^{\beta_i}})\prod_{1\le j\le L}\chi_1(b_j^{e-\gamma_j} x)\\
&= \sum_{x\in\mathbb{F}_q}\chi_1(\sum_{1\le i\le D}a_i x^{p^{\alpha_i}+p^{\beta_i}})\chi_1(\sum_{1\le j\le L}b_j^{e-\gamma_j} x)\\
&= \sum_{x\in\mathbb{F}_q}\chi_1(\sum_{1\le i\le D}a_i x^{p^{\alpha_i}+p^{\beta_i}})\chi_1(bx)\\
&= \sum_{x\in\mathbb{F}_q}\chi_1(\sum_{1\le i\le D}a_i x^{p^{\alpha_i}+p^{\beta_i}}+bx)
\end{aligned}$$

This reduces the linearized polynomial $\sum_{1\le j\le L}b_j x^{p^{\gamma_j}}$ into a monomial bx where $b=\sum_{1\le j\le L}b_j^{p^{e-\gamma_j}}$. Hence

$$S(a_1,\cdots,a_D,b_1,\cdots,b_L)=S(a_1,\cdots,a_D,b)$$

Similarly, we translate further the polynomial $S(a_1,\cdots,a_D,b)$ as follows:

$$\begin{aligned}
S(a_1,\cdots,a_D,b) &= \sum_{x\in\mathbb{F}_q}\chi_1(\sum_{1\le i\le D}a_i x^{p^{\alpha_i}+p^{\beta_i}}+bx)\\
&= \sum_{x\in\mathbb{F}_q}\prod_{1\le i\le D}\chi_1(a_i x^{p^{\alpha_i}+p^{\beta_i}})\chi_1(bx)\\
&= \sum_{x\in\mathbb{F}_q}\prod_{1\le i\le D}\chi_1(a_i x^{p_i^{\beta}(p^{s_i}+1)})\chi_1(bx)\\
&= \sum_{x\in\mathbb{F}_q}\prod_{1\le i\le D}\chi_1(A_i^{p^{t_i}}(x^{p^{\beta_1}})^{p^{t_i}(p^{s_i}+1)})\chi_1(b^{p^{\beta_1}}x^{p^{\beta_1}})\\
&= \sum_{x'\in\mathbb{F}_q}\prod_{1\le i\le D}\chi_1((A_i x'^{p^{s_i}+1})^{p^{t_i}})\chi_1(b^{p^{\beta_1}}x') \qquad ;\ x'=x^{p^{\beta_1}}\\
&= \sum_{x'\in\mathbb{F}_q}\prod_{1\le i\le D}\chi_1(A_i x'^{p^{s_i}+1})\chi_1(b^{p^{\beta_1}}x')\\
&= S(A_1,\cdots,A_D,b).
\end{aligned}$$

□

Using Theorem 4.2, bivariate equation (4.1) can be equivalently stated in terms of simplified univariate polynomial as

$$h(x,y) = \sum_{i=1}^{D} A_i x^{p^{s_i}+1} + b^{p^{\beta_1}} x - y^{p^\delta} + y = 0. \tag{4.4}$$

Remark 4.2. In [43, 34] the authors consider the simplified univariate representation for $\mathcal{P}'(x)$ with $b = 0$. The corresponding simplified polynomial $\sum_{i=1}^{D} A_i x^{p^{s_i}+1}$ belongs to a special class of polynomials termed as Dembowski Ostrom (DO) polynomials, defined independently in [18]. We shall also be considering only these polynomials in our subsequent discussion.

4.2.2 Emulation Conditions

Mills [43] proved that by imposing certain restrictions on the exponents of these DO polynomials, the solutions of the corresponding bivariate equation in (4.4) can divided into equivalence classes. We term these conditions as *Emulation Conditions*. These conditions are defined as follows for $\delta = gcd(s_1, \cdots, s_D, n)$

n/δ is even,
$\delta = gcd(s_i, n)$ for each i,
s_i/δ is odd for each i, and
2δ *divides* $|s_i - s_j|$ for all $i \neq j$.

With these emulation conditions, the non-zero solutions to the above mentioned bivariate equation $h(x,y)$ are divided into T equivalence classes of size $p^\delta + 1$. This is proved in the following result in [34] for $p = 2$ case and [43] for any odd prime p.

Theorem 4.3. *[34, Lemma 2.2.1][43] Let $\mathcal{P}'(x)$ be a simplified univariate polynomial $\sum_{i=1}^{D} A_i x^{p^{s_i}+1}$ over $\mathbb{F}_q$ with s_i/δ odd for each $1 \leq i \leq D$ and $h(x,y) = \mathcal{P}'(x) - y^{p^\delta} + y$ is the bivariate polynomial over $\mathbb{F}_q \times \mathbb{F}_q$. Then the number of solutions $N = N(h(x,y))$ of the bivariate equation $h(x,y) = 0$ is congruently estimated as*

$$N \equiv -1 \; mod \; (p^\delta + 1). \tag{4.5}$$

Proof. By definition $\delta = gcd(s_1, \ldots, s_D)$. Hence, $p^{s_i} + 1$ is divisible by $p^\delta + 1$ for each s_i/δ odd. Let $(x,y) \in \mathbb{F}_q \times \mathbb{F}_q$ with $x \neq 0$ a solution of the equation $\sum_{i=1}^{D} A_i x^{p^{s_i}+1} = y^{p^\delta} - y$ over $\mathbb{F}_q \times \mathbb{F}_q$, then $(\omega x, y)$ is also a solution if $\omega^{p^\delta+1} = 1$. Thus, the solutions $(x,y) \in \mathbb{F}_q \times \mathbb{F}_q$ with $x \neq 0$ are grouped in T equivalence classes of size $p^\delta + 1$ i.e. $\{(\omega x, y) \in \mathbb{F}_q \times \mathbb{F}_q | \omega^{p^\delta+1} = 1, \omega \in \mathbb{F}_q\}$. Also for $x = 0$,

the linearized binomial $y^{p^\delta} - y = 0$ is satisfied by any $y \in \mathbb{F}_{p^\delta}$. So, the total number of solutions can be written as

$$\begin{aligned} N &= (p^\delta + 1)t + p^\delta \qquad t \in \mathbb{N} \\ &\equiv -1 \; mod \; (p^\delta + 1). \end{aligned}$$

□

In other words, one can pick arbitrary elements x in $\mathbb{F}^*_{p^n}$ so that they are mapped by $\mathcal{P}'(x)$ to reduced space of $\mathbb{F}_{p^{n-\delta}}$ with a high probability t/T(see [43, Lemma 3.4, 3.5, 3.6] and [34, Lemma 2.2.1]).

4.2.3 Number of Solutions and Weil Sum

Mills [43] observed that the number of solutions to the bivariate equation in (4.4) can also be expressed in terms of Weil Sum for the simplified univariate polynomial $\mathcal{P}'(x)$ using (2.7).

Theorem 4.4. *([43, Lemma 3.6][34, Theorem 2.2.3]) Let p be any prime and $q := p^n$. Let $\delta, n \in \mathbb{N}$ with n/δ even, and let N be the number of solutions $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ of the following bivariate equation*

$$\sum_{i=1}^{D} A_i x^{p^{s_i}+1} = y^{p^\delta} - y.$$

And let $\delta = gcd(s_i, n)$ for $1 \leq i \leq D$ for $D \in \mathbb{N}$ such that 2δ divides $|s_i - s_j|$ for all $i \neq j$. Then

$$N = q + (p^\delta - 1)S \tag{4.6}$$

where $S = S(A_1, \cdots, A_D)$ is the Weil Sum given by Theorem 4.2 (assuming $b = 0$).

Proof. Using (2.7) for given bivariate equation in (4.4), we have

$$\begin{aligned} N &= \frac{1}{q} \sum_{\omega \in \mathbb{F}_q} \sum_{x,y \in \mathbb{F}_q} \chi_1\bigg(\omega\bigg[\sum_{i=1}^{n} A_i x^{p^{s_i}+1} - y^{p^\delta} + y\bigg]\bigg) \\ qN &= q^2 + \sum_{\omega \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_q} \chi_1\bigg(\omega\bigg[\sum_{i=1}^{n} A_i x^{p^{s_i}+1}\bigg]\bigg) \sum_{y \in \mathbb{F}_q} \chi_1\bigg(\omega(y - y^{p^\delta})\bigg) \\ qN &= q^2 + \sum_{\omega \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_q} \chi_1\bigg(\omega\bigg[\sum_{i=1}^{n} A_i x^{p^{s_i}+1}\bigg]\bigg) \sum_{y \in \mathbb{F}_q} \chi_1\bigg(y^{p^\delta}(\omega^{p^\delta} - \omega)\bigg). \end{aligned}$$

The last sum is zero unless $\omega \in \mathbb{F}^*_{p^\delta}$. Hence

$$N = q + \sum_{\omega \in \mathbb{F}^*_{p^\delta}} \sum_{x \in \mathbb{F}_q} \chi_1\bigg(\omega\bigg[\sum_{i=1}^{n} A_i x^{p^{s_i}+1}\bigg]\bigg).$$

Since n/δ is even and $\delta = gcd(s_i, n)$ by construction and also 2δ divides $|s_i - s_j|$ for $i \neq j$. Thus $gcd(p^{s_i}+1, p^n-1) = p^\delta + 1$ and $p^\delta + 1$ divides $\frac{p^n-1}{p^\delta-1}$ for each i. Hence, it is observed that the equation $\omega z_\omega^{p^{s_i}+1} = 1, i = 1, \ldots, n$ is solvable for each i and the solutions $z_\omega \in \mathbb{F}^*_{p^{2\delta}}$. Thus

$$\begin{aligned} N &= q + \sum_{\omega \in \mathbb{F}^*_{p^\delta}} \sum_{x \in \mathbb{F}_q} \chi_1\Big(\omega\Big[\sum_{i=1}^{n} A_i x^{p^{s_i}+1}\Big]\Big) \\ &= q + \sum_{\omega \in \mathbb{F}^*_{p^\delta}} \sum_{x \in \mathbb{F}_q} \chi_1\Big(\Big[\sum_{i=1}^{n} A_i \omega (z_\omega x)^{p^{s_i}+1}\Big]\Big) \\ &= q + \sum_{\omega \in \mathbb{F}^*_{p^\delta}} \sum_{x \in \mathbb{F}_q} \chi_1\Big(\sum_{i=1}^{n} A_i x^{p^{s_i}+1}\Big) \\ &= q + (p^\delta - 1)S. \end{aligned}$$

□

Harayama and Friesen in [34, Theorem 2.3.1] made an observation regarding evaluating exact value of Weil Sum S in Theorem 4.4. We will state their result without proof as it can be verified using Theorem 4.3 and Theorem 4.4.

Theorem 4.5. *Let $\mathbb{F}_q$ be a finite field of order $q := 2^n$ and characteristic 2. Let $f(x)$ be a simplified univariate polynomial $\sum_{i=1}^{n} A_i x^{p^{s_i}+1}$ over $\mathbb{F}_{2^n}$ satisfying the emulation conditions in section 4.2.2. Also let $S = S(A_1, \cdots, A_D, b)$ be the Weil Sum of $f(x)$ with $|S|$ as its absolute value. Then we have*

$$S = \begin{cases} +|S| & \text{if } (1 - |S|) \equiv 0 \bmod (2^\delta + 1) \\ -|S| & \text{otherwise.} \end{cases}$$

No such observation can be made about odd prime case and the only estimate of S in Theorem 4.11 in that case can be made using [43, Theorem 1.4] as

$$S = \pm p^{\frac{n+l}{2}}$$

where l is the dimension of the linear subspace of $\mathbb{F}_{p^\epsilon}$ such that $\epsilon := gcd(2s_1, s_1 + s_i, s_1 + y_i, n)$ (*cf.* Theorem 4.2).

4.2.4 The Attack

LBA involves obtaining collision among the signature evaluations through public key polynomial map and hash values of messages in reduced image space of $Im(L)$. This was equivalent to finding solutions of bivariate equation $h(x, y)$ in (4.4). Thus, in order to improve the complexity of LBA Harayama and Friesen in [34] suggested to use simplified univariate public key polynomial in Theorem 4.2 for public key evaluations and subsequently emulation conditions to reduce the desire number of evaluations. The attack can be stated as follows

1. Let $\delta = gcd(s_1, \cdots, s_D, n)$. This δ allows the adversary to fix a linearized binomial $L(y) = y^{p^\delta} - y$ in $\mathbb{F}_{p^n}[y]$. We denote by $Im(L)$ the image of the mapping L over $\mathbb{F}_{p^n}$.
2. Generate $\frac{T}{t}p^{(n-\delta)/2}$ random elements $x \in \mathbb{F}_{p^n}$ and obtain the list
$$\{\mathcal{P}'(x_1), \mathcal{P}'(x_2), \cdots, \mathcal{P}'(x_{\frac{T}{t}p^{(n-\delta)/2}})\}.$$
3. Generate $p^{(n-\delta)/2}$ messages(m) with hash values $z \in Im(L)$ to obtain the list
$$\{z_1, z_2, \cdots, z_{p^{(n-\delta)/2}}\}.$$
4. Search for a coincidence $\mathcal{P}'(x_j) = z_i$ for some i, j in two lists.

Remark 4.3. Harayama and Friesen [34] assume the scenario in step (3) under the framework of adaptively chosen message attack. Also it is assumed not to incur any additional cost other than $O(p^{(n-\delta)/2})$. Although, in [34] the assumption is not explained but we believe it to be valid under the framework of fully programming random oracle model [30] where such reductions are allowed to the arbitrary chosen range values. And it is also proved fundamental to the security proof of a cryptographic construction under adaptive chosen message attack in the random oracle model.

The attack forms a case of existential forgery [41, Section 11.2.4] when successful. A valid (*message, signature*) pair can be forged in the total time complexity
$$O(\frac{T}{t}p^{(n-\delta)/2}). \tag{4.7}$$
When this complexity is smaller than that of birthday security parameter $p^{n/2}$, the LBA is successful against the MQ signature scheme in complexity less than normal birthday attack. The same can be equivalently stated in terms of number of solution N of the bivariate equation $h(x, y) = 0$ in (4.4). If
$$N > p^\delta + p^{-\delta/2}(p^n - 1) \tag{4.8}$$
then the complexity of LBA is better than normal birthday attack complexity $p^{n/2}$. We see an extension of this attack to heterogeneous MQ cryptosystems as we remark in Remark 4.4.

Remark 4.4. Harayama and Friesen [34] only consider the homogeneous MQ cryptosystems i.e. $m = n$. But we observe that it is easy to extend the ideas to heterogeneous case based on the existence of univariate polynomial in this case as mentioned in Theorem 3.1.

4.3 Weak Dembowski-Ostrom (DO) Polynomials

4.3.1 Definition

Harayama and Friesen in [34] based on LBA defined the weak DO polynomials as follows:

Definition 4.1. Let F_q be the n-th degree extension of finite field F_p. Let $f'(x) = \sum_{i=1}^{D} A_i x^{p^{s_i}+1}$ be a DO polynomial over F_q satisfying the following emulation conditions for $\delta = gcd(s_1, \cdots, s_D)$

$$n/\delta \text{ is even,}$$
$$s_i/\delta \text{ is odd for each } i.$$

If the number of solutions (N) over F_q of bivariate equation $f'(x) = y^{p^\delta} - y$ satisfy

$$N > p^\delta + p^{-\delta/2}(p^n - 1), \tag{4.9}$$

for the birthday security parameter $p^{n/2}$, then f' is called ***Weak DO polynomial***.

The MQ signature scheme having public polynomials with univariate representation in weak DO polynomials is subjected to LBA in complexity less than $p^{n/2}$. Our weak DO polynomial definition differs from the definition in [34]. We explain the difference of Definition 4.1 with the one given in [34] in Remark 4.5.

Remark 4.5. The above definition is a generalisation of the definition by Harayama and Friesen in [34] based on our observations already explained. The N-bound mentioned above is also slightly different than one observed in [34]. Since computing δ from equivalent univariate representation of public key is trivial, one does not need to search for δ in $\{1, 2, \ldots, n\}$. Moreover, authors in [34] ignored factor of $\pi/2$ in computing complexity of LBA and later in N-bound evaluation for weak DO polynomials. We also remove the emulation condition 2δ *divides* $|s_i - s_j|$ for all $i \neq j$ which evolves directly from s_i/δ is odd. The emulation condition $\delta = gcd(s_i, n)$ is also removed, which we will justify in Remark 4.6.

4.3.2 Conjecture About Existence

In [34], authors demonstrated the existence of weak DO polynomials for $D = 2$ with $n = 4i, s_1 = i, s_2 = 3i$ and $p = 2$ by taking $\delta = i = n/4$. Later, based on their simulation results they conjectured that

$$f'(x) = x^{2^{n/4}+1} + x^{2^{3n/4}+1} \in \mathbb{F}_{2^n}[x] \tag{4.10}$$

with $n = 4i$, $i \geq 2$ forms an infinite class of weak DO polynomials. They considered LBA for MQ signature schemes over $\mathbb{F}_2$ due to the fact that the exact value of Weil Sum for f' in Theorem 3([34, Theorem 2.3.1]) can only be determined when defined over $\mathbb{F}_{2^n}$. The Weil Sum value is used to compute the exact number of solutions N of the bivariate equation h in (4.4) using the equality

$$N = 2^n + (2^\delta - 1)S \tag{4.11}$$

where S is the exact value of Weil Sum for simplified univariate polynomial f' ([34, Theorem 2.2.3]). However, based on our observation in Remark 4.6 we identify a general class of *Weak DO* polynomials over finite fields of any prime characteristic.

Remark 4.6. We note that if the bivariate equation happens to be equivalent to certain type of algebraic curve, then the number of points can be easily determined using [39, Theorem 6.32] in terms of standard classification of quadratic forms, without resolving the sign of the Weil Sum of f'. This also allows us to remove the emulation condition of $\delta = gcd(s_i, n)$ which is required to obtain number N of solutions over F_q in terms of Weil Sum S as in (4.11). The same should affect the choice of δ in LBA.

4.3.3 Classes of Weak Dembowski Ostrom Polynomials

The conjecture by Harayama and Friesen in [34] based on our observation in Remark 4.6 relates to proving existence of certain classes of Artin-Schrier type algebraic curves over $\mathbb{F}_p[x, y]$ with many rational places ignoring the genus. In fact, the desired rational places are at least greater than bound in (4.8). This allows us to approach the problem from the theory of algebraic functions fields where there are already many results that could assist in solving this problem. It can be observed that the bivariate equation in (4.4) actually resembles the Artin-Schrier type algebraic function field over $\mathbb{F}_{p^n}[x, y]$ in [17] constructed using quadratic forms. Çakçak and Özbudak [17] characterize certain Artin-Schrier type algebraic function fields with prescribed genus and number of rational places using theory of quadratic forms. This approach proved useful in solution of our problem.

4.3.3.1 Quadratic Forms

Let Q_s be a quadratic form over $\mathbb{F}_q$ defined as

$$\begin{aligned} Q_s \ : \ \mathbb{F}_{q^{2k}} \ &\rightarrow \ \mathbb{F}_q \\ a \ &\rightarrowtail \ Tr(aS(a)) \end{aligned}$$

and

$$S(X) = \alpha_0 X + \alpha_1 X^q + \cdots + \alpha_h X^{q^h} \ \in \mathbb{F}_{q^{2k}}[X] \tag{4.12}$$

be an $\mathbb{F}_q$-linearized polynomial of degree q^h in $\mathbb{F}_{q^{2k}}[X]$ for $k \geq 1, h \geq 0$. Let F be the algebraic function field over $\mathbb{F}_{q^{2k}}$ given as

$$F \ = \ \mathbb{F}_{q^{2k}}(u, v) \ \text{ with } v^q - v \ = \ uS(u) \tag{4.13}$$

such that $Tr(.)$ denotes the trace map from $\mathbb{F}_{q^{2k}}$ to $\mathbb{F}_q$, i.e. for $a \in \mathbb{F}_{q^{2k}}$, $Tr(a) = a + a^q + \cdots + a^{q^{2k-1}}$. Let V_s be the subset of $\mathbb{F}_{q^{2k}}$ defined as

$$V_s \ = \ \{a \in \mathbb{F}_{q^{2k}} \ : \ Q_s(a) \ = \ 0\}.$$

For an Artin-Schrier type algebraic function field given in (4.13), there is only one rational point in F over the point at infinity of the function field $\mathbb{F}_{q^{2k}}(u)$. The other rational points of F correspond to the elements $a \in \mathbb{F}_{q^{2k}}$ satisfying

$Tr(aS(a)) = 0$. Moreover for each $a \in \mathbb{F}_{q^{2k}}$ with $Q_s(a) = Tr(aS(a)) = 0$, there are q rational points in F, so that the total number of rational points is given by

$$N(F) \ = \ 1 + q|V_s| \tag{4.14}$$

([62, Proposition 6.4.1]).

4.3.3.2 Classification of Weak DO Polynomials

Enumerating weak DO polynomials satisfying emulation conditions in Definition 4.1 can be indirectly achieved using theory of quadratic forms and counting number of rational points on the Artin-Schreier type algebraic curves, that we briefly mention in section 4.3.3.1. Following the notations in section 4.3.3.1, we define an Artin-Schreier type algebraic curve as follows

$$F \ = \ \mathbb{F}_{p^n}(x, y) \quad \text{with } y^q - y = xS(x) \ ; \ q = p^{n/2k} \tag{4.15}$$

with

$$S(X) = \alpha_0 X + \alpha_1 X^q + \cdots + \alpha_h X^{q^h} \ \in \mathbb{F}_{p^n}[X] \qquad ; \ 0 \leq h \leq n-1. \tag{4.16}$$

It is observed that the number of $\mathbb{F}_{p^n}$ rational points (4.14) of the algebraic function field in (4.15) is greater than the N-bound defined in (4.8) if $|V_s| \ = \ p^n$ which correspond to cardinality of $\mathbb{F}_{p^n}$. This is verified by using MAGMA [4]. Hence, we are looking for class of polynomials S that have

$$|V_s| \ = \ \{a \in \mathbb{F}_{p^n} \ : \ Q_s(a) \ = \ Tr(aS(a)) \ = 0\} \ = \ p^n. \tag{4.17}$$

We first prove the existence of a simple class of weak DO polynomials in Theorem 4.6. Corollary 1 to Theorem 4.6 will directly show the correctness of the conjecture in [34] (see the equation (6)). Then we will prove a general class of weak DO polynomials in Theorem 4.8. And we also verify our computations using MAGMA [4].

Theorem 4.6. *Let p be any prime and $n, k \in \mathbb{Z}^+$ such that $2k|n$. Let $s_1 = jn/2k$ and $s_2 = (2k-j)n/2k$ for some j in $\{1, 2, \ldots, (2k-1)\}$ such that $gcd(j, 2k-j) = 1$. Let $A_1, A_2 \in \mathbb{F}_{p^n}$ such that $A_1^{p^{s_2}} + A_2 = 0$ then*

$$f(x) = A_1 x^{p^{s_1}+1} + A_2 x^{p^{s_2}+1} \in \mathbb{F}_{p^n}[x]$$

forms an infinite class of weak DO polynomials.

Proof. First we examine $f(x)$ for emulation conditions. By definition

$$\begin{aligned} f(x) = &= A_1 x^{p^{s_1}+1} + A_2 x^{p^{s_2}+1} \\ &= A_1 x^{p^{jn/2k}+1} + A_2 x^{p^{(2k-j)n/2k}+1} \ \in \mathbb{F}_{p^n}[x] \end{aligned}$$

where $j \in \{1, 2, \ldots, (2k-1)\}$ such that $gcd(j, 2k-j) = 1$ and $\delta = gcd(s_1, s_2) = n/2k$. If $gcd(j, 2k-j) = 1$ then w.l.o.g j can be considered odd and hence with

$s_1 = jn/2k$ and $s_2 = (2k-j)n/2k$, we have emulation conditions in Definition 4.1 satisfied with n/δ even and s_i/δ odd for $i \in \{1,2\}$ and $k, n \in \mathbb{Z}^+$ such that $2k|n$.

Let the trace map Tr be from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^\delta}$. To verify the condition in (4.17), we need to prove the following

$$Tr(f(x)) = Tr(A_1 x^{p^{jn/2k}+1} + A_2 x^{p^{(2k-j)n/2k}+1}) = 0 \text{ for all } x \in \mathbb{F}_{p^n} \tag{4.18}$$

Each $x \in \mathbb{F}_{p^n}$ has $2k-1$ conjugates over $\mathbb{F}_{p^\delta}$. Each conjugate is of the form $x^{p^{in/2k}}$ for $1 \leq i \leq 2k-1$. Hence for $i = 2k-j$ we get

$$\begin{aligned}(A_1 x^{p^{jn/2k}+1})^{p^{n(2k-j)/2k}} &= A_1^{p^{n(2k-j)/2k}} x^{p^n + p^{(2k-j)n/2k}} \\ &= A_1^{p^{s_2}} x^{p^{(2k-j)n/2k}+1} \\ &= -A_2 x^{p^{(2k-j)n/2k}+1}.\end{aligned}$$

Hence the trace $Tr(f(x))$ in (4.18) sums to 0 under the condition $A_1^{p^{s_2}} + A_2 = 0$ over $\mathbb{F}_{p^n}$ for all $x \in \mathbb{F}_{p^n}$. Now, we consider the following Artin - Schrier type curve

$$F = \mathbb{F}_{p^n}(x,y) \quad \text{with } y^q - y = xS(x) \qquad \text{where } q = p^{n/2k} \tag{4.19}$$

with

$$S(X) = A_1 x^{q^j} + A_2 x^{q^{2k-j}} \in \mathbb{F}_{p^n}[X]$$

where $j \in \{1, 2, \ldots, 2k-1\}$ such that $gcd(j, 2k-j) = 1$. Using theory of algebraic function fields the number of points($N(F)$) on this Artin-Schrier type curve can be evaluated using (4.14). As mentioned in section 4.3.3.2 it is observed that $N(F)$ for Artin-Schrier type curve in (4.19) such that $n, k \in \mathbb{Z}^+$ and $2k|n$, is greater than bound for weak DO polynomials in (4.8). Hence for a particular choice of k we get infinite classes of weak DO polynomials i.e. over various extensions $\mathbb{F}_{p^n}$ of $\mathbb{F}_p$ such that $2k|n$. Table 4.2 mentions such choices of n for particular k. □

Remark 4.7. Moreover, we observed that the classes of weak DO polynomials for $j \in \{1, 2, \ldots, 2k-1\}$ with $gcd(j, 2k-j) = d > 1$ can also be represented by Theorem 4.6 for $s_1 = j'n/2k'$ and $s_2 = (2k'-j')n/2k'$ where $j = j'd$ and $k = k'd$ such that $gcd(j', 2k'-j') = 1$. Hence we do not mention those redundant classes.

We present few example weak DO class polynomials satisfying Theorem 4.6 in Table 4.1 with parameters list. In Table 4.2, for $k = 2, 3, 4$ and $p = 2, 3, 5$, we consider few initial n values and define weak DO class polynomials satisfying Theorem 4.6 with $\delta = 1, 2, 3$. We also mention the corresponding N-bound (*cf.* (4.8)) and N-observed (*cf.* (4.14)) values calculated using (4.8) and (4.14).

Corollary 4.7. *Let $n, k \in \mathbb{Z}^+$ such that $2k|n$. Let $s_1 = jn/2k$ and $s_2 = (2k-j)n/2k$ for some j in $\{1, 2, \ldots, (2k-1)\}$ such that $gcd(j, 2k-j) = 1$. Let $A_1, A_2 \in \mathbb{F}_{2^n}$ such that $A_1^{2^{s_2}} + A_2 = 0$ then*

$$f(x) = A_1 x^{2^{s_1}+1} + A_2 x^{2^{s_2}+1} \in \mathbb{F}_{2^n}[x]$$

forms an infinite class of weak DO polynomials.

Table 4.1: Parameter list: $D = 2$ with $A_1^{p^{s_2}} + A_2 = 0$ over $\mathbb{F}_{p^n}$

k	j	$s_1 = jn/2k$	$s_2 = (2k-j)n/2k$	$\delta = gcd(s_1, s_2)$	Class Polynomial
2	1	$n/4$	$3n/4$	$n/4$	$A_1 x^{p^{n/4}+1} + A_2 x^{p^{3n/4}+1}$
3	1	$n/6$	$5n/6$	$n/6$	$A_1 x^{p^{n/6}+1} + A_2 x^{p^{5n/6}+1}$
4	1	$n/8$	$7n/8$	$n/8$	$A_1 x^{p^{n/8}+1} + A_2 x^{p^{7n/8}+1}$
4	3	$3n/8$	$5n/8$	$n/8$	$A_1 x^{p^{3n/8}+1} + A_2 x^{p^{5n/8}+1}$
5	1	$n/10$	$9n/10$	$n/10$	$A_1 x^{p^{n/10}+1} + A_2 x^{p^{9n/10}+1}$
5	3	$3n/10$	$7n/10$	$n/10$	$A_1 x^{p^{3n/10}+1} + A_2 x^{p^{7n/10}+1}$
6	1	$n/12$	$11n/12$	$n/12$	$A_1 x^{p^{n/12}+1} + A_2 x^{p^{11n/12}+1}$
6	5	$5n/12$	$7n/12$	$n/12$	$A_1 x^{p^{5n/12}+1} + A_2 x^{p^{7n/12}+1}$
⋮	⋮	⋮	⋮	⋮	⋮

Table 4.2: Weak DO Polynomials (*cf.* Theorem 4.6 with $j = 1$, $k = 2, 3, 4$)

k	n	(s_1, s_2)	δ	N-bound			N-observed		
				$p=2$	$p=3$	$p=5$	$p=2$	$p=3$	$p=5$
Class Polynomial: $A_1 x^{p^{n/4}+1} + A_2 x^{p^{3n/4}+1}$ such that $A_1^{p^{3n/4}} + A_2 = 0$ over $\mathbb{F}_{p^n}$									
2	4	(1,3)	1	12	49	284	33	244	3126
	8	(2,6)	2	131	2195	78149	1025	59050	9765626
	12	(3,9)	3	1455	102302	21836726	32769	14348908	30517578126
Class Polynomial: $A_1 x^{p^{n/6}+1} + A_2 x^{p^{5n/6}+1}$ such that $A_1^{p^{5n/6}} + A_2 = 0$ over $\mathbb{F}_{p^n}$									
3	6	(1,5)	1	46	423	6992	129	2188	78126
	12	(2,10)	2	2051	177155	48828149	16385	4782970	6103515626
	18	(3,15)	3	92689	74559134	341196896105	2097153	10460353204	476837158203126
Class Polynomial: $A_1 x^{p^{n/8}+1} + A_2 x^{p^{7n/8}+1}$ such that $A_1^{p^{7n/8}} + A_2 = 0$ over $\mathbb{F}_{p^n}$									
4	8	(1,7)	1	182	3790	174697	513	19684	1953126
	16	(2,14)	2	32771	14348915	30517578149	262145	387420490	3814697265626
	24	(3,21)	3	5931649	54353589664	5331201499700169	134217729	7625597484988	7450580596923828126

The conjecture in [34] (see the equation (6)) is a special case of the class given in Corollary 1 for $j = 1$ and $k = 2$ with $A_1, A_2 \in \mathbb{F}_2$.

Theorem 4.8. *Let p be any prime and $n, k \in \mathbb{Z}^+$ such that $2k|n$. Let $s_i = \alpha_i n/2k$ with $\alpha_i = (2i-1)$ for $1 \le i \le k$ where $A_i \in \mathbb{F}_{p^n}$ such that $A_i + A_{k+1-i}^{p^{s_i}} = 0$. Then*

$$f(x) = \sum_{i=1}^{k} A_i x^{p^{s_i}+1} \ \in \mathbb{F}_{p^n}[X] \tag{4.20}$$

forms an infinite class of weak DO polynomials.

Proof. Similar to Theorem 2.5, first we examine $f(x)$ for emulation conditions in Definition 4.1. Let

$$f(x) = \sum_{i=1}^{k} A_i x^{p^{s_i}+1} \qquad \in \mathbb{F}_{p^n}[x]$$

where $s_i = \alpha_i n/2k$ with $\alpha_i = (2i-1)$ for $1 \leq i \leq k$. For simplification of proof we assume that $A_i \neq 0$ for $1 \leq i \leq k$ and $\delta := gcd(s_1, \ldots, s_k) = n/2k$. Emulation conditions are trivially satisfied with $n/\delta = 2k$ even and $s_i/\delta = \alpha_i$ odd for $1 \leq i \leq k$.

To evaluate equation (4.17), let the trace map be defined as $Tr : \mathbb{F}_{p^n} \to \mathbb{F}_{p^\delta}$. We need to prove the following:

$$Tr(f(x)) \ = Tr(\sum_{i=1}^{k} A_i x^{p^{s_i}+1}) = 0 \text{ for all } x \in \mathbb{F}_{p^n}. \tag{4.21}$$

We show in two steps that the equation (4.21) holds. First we will show that $Tr(A_i x^{p^{\alpha_i n/2k}+1}) = 0$ for an odd integer k and $i = (k+1)/2$. In the second step, we will show that $Tr(A_i x^{p^{\alpha_i n/2k}+1}) = -Tr(A'_i x^{p^{\alpha'_i n/2k}+1})$ for $i' = k+1-i$ and $i = 1, 2, \ldots, k$. We start with the first step. Let k be an odd integer and $i = (k+1)/2$. Then, the trace of the monomial $A_i x^{p^{\alpha_i n/2k}+1}$ with $\alpha_i = k$ and $A_i + A_i^{p^{n/2}} = 0$ is

$$\begin{aligned}
Tr(A_i x^{p^{\alpha_i n/2k}+1}) &= Tr(A_i x^{p^{kn/2k}+1}) \\
&= A_i x^{p^{kn/2k}+1} + A_i^{p^{n/2k}} x^{p^{(k+1)n/2k}+p^{n/2k}} + \ldots \\
&+ A_i^{p^{(k-1)n/2k}} x^{p^{(2k-1)n/2k}+p^{(k-1)n/2k}} + A_i^{p^{kn/2k}} x^{p^{(2k)n/2k}+p^{kn/2k}} \\
&+ \ldots + A_i^{p^{(2k-1)n/2k}} x^{p^{(k-1)n/2k}+p^{(2k-1)n/2k}} \\
&= A_i x^{p^{n/2}+1} + A_i^{p^{n/2k}} x^{p^{(k+1)n/2k}+p^{n/2k}} + \ldots \\
&+ A_i^{p^{(k-1)n/2k}} x^{p^{(2k-1)n/2k}+p^{(k-1)n/2k}} + A_i^{p^{n/2}} x^{1+p^{n/2}} \\
&+ \ldots + A_i^{p^{(2k-1)n/2k}} x^{p^{(k-1)n/2k}+p^{(2k-1)n/2k}} \\
&= A_i x^{p^{n/2}+1} + A_i^{p^{n/2k}} x^{p^{(k+1)n/2k}+p^{n/2k}} + \ldots \\
&+ A_i^{p^{(k-1)n/2k}} x^{p^{(2k-1)n/2k}+p^{(k-1)n/2k}} \\
&- A_i x^{1+p^{n/2}} - A_i^{p^{n/2k}} x^{p^{n/2k}+p^{(k+1)n/2k}} \\
&- \ldots - A_i^{p^{(k-1)n/2k}} x^{p^{(k-1)n/2k}+p^{(2k-1)n/2k}}.
\end{aligned}$$

Hence we have $Tr(A_i x^{p^{\alpha_i n/2k}+1}) = 0$ for $i = \frac{k+1}{2}$. In the second step, let $i' = k+1-i$, we evaluate the $\alpha_{i'}$-th conjugate of the monomials of the form $A_i x^{p^{\alpha_i n/2k}+1}$ for $1 \leq i \leq k$ and $i \neq \frac{k+1}{2}$.

$$\begin{aligned}
(A_i x^{p^{\alpha_i n/2k}+1})^{p^{\alpha_{i'} n/2k}} &= A_i^{p^{\alpha_{i'} n/2k}} x^{p^{(\alpha_i+\alpha_{i'})n/2k}+p^{\alpha_{i'} n/2k}} \\
&= A_i^{p^{\alpha_{i'} n/2k}} x^{1+p^{\alpha_{i'} n/2k}} \\
&= -A_{i'} x^{1+p^{\alpha_{i'} n/2k}}.
\end{aligned}$$

Hence $Tr(A_i x^{p^{\alpha_i n/2k}+1}) = -Tr(A'_i x^{p^{\alpha'_i n/2k}+1})$ for $i' = k+1-i$ and $i = 1, 2, \ldots, k$. Therefore, equation (4.21) holds. Now, we consider the following Artin - Schrier

type curve

$$F \;=\; \mathbb{F}_{p^n}(x,y) \quad \text{with } y^q - y = xS(x) \qquad \text{where } q = p^{n/2k} \tag{4.22}$$

with

$$S(x) = \sum_{i=1}^{k} A_i x^{q^{\alpha_i}} \;\in \mathbb{F}_{p^n}[x].$$

The number N(F) of $\mathbb{F}_{p^n}$ rational points on the Artin-Schrier type curve in (4.22) can be evaluated using (4.14). It is observed that N(F) is greater than bound for weak DO polynomials in (4.8) for $k, n \in \mathbb{Z}^+$ such that $2k|n$. Similar to Theorem 2.5, for a particular choice of k we get infinite classes of weak DO polynomials i.e. over various extension $\mathbb{F}_{p^n}$ of $\mathbb{F}_p$ such that $2k|n$.

In the cases where $A_i = 0$ for some $1 \leq i < k$ we perform the similar steps in the proof. Let $A_{i_1}, A_{i_2}, \ldots, A_{i_t}$ be non-zero elements. Then, we have $\delta = gcd(s_{i_1}, \ldots, s_{i_t}) = dn/2k$ for $gcd(\alpha_{i_1}, \ldots, \alpha_{i_t}) = d > 1$. The corresponding DO polynomial $f(x)$ will satisfy the emulation conditions in Definition 4.1 with $n/\delta = 2k'$ even with $k = k'd$ and $s_{i_j}/\delta = \alpha_{i_j}/d$ odd for $1 \leq j \leq t$. The remaining steps of the proof holds for $\delta = n/2k'$. □

Remark 4.8. : It is clear that Theorem 4.6 is a subclass of Theorem 4.8. With suitable choice of parameters, we can get subclass of Theorem 4.6 from bigger class of Theorem 4.8. However, we present them as separate classes to prove the existence of conjectured class[34] of weak DO polynomials. Theorem 4.8 partially addresses the second open problem in [34] of enumerating weak DO polynomials.

Similar to Table 4.1, classes of polynomials for weak DO polynomial classes satisfying Theorem 4.8 can be constructed for different values of $k, n \in \mathbb{Z}^+$ such that $2k|n$.

Using conditions in Theorem 4.8 on $A_i \in \mathbb{F}_{p^n}$ for $1 \leq i \leq k$ such that $A_i + A_{k+1-i}^{p^{s_i}} = 0$, we state few example weak DO class polynomials over $\mathbb{F}_{p^n}$ in Table 4.3.

Table 4.3: Example classes of Weak DO polynomials over $\mathbb{F}_{p^n}$

k	Class Polynomial
2	$A_1 x^{p^{n/4}+1} + A_2 x^{p^{3n/4}+1}$
3	$A_1 x^{p^{n/6}+1} + A_2 x^{p^{3n/6}+1} + A_3 x^{p^{5n/6}+1}$
4	$A_1 x^{p^{n/8}+1} + A_2 x^{p^{3n/8}+1} + A_3 x^{p^{5n/8}+1} + A_4 x^{p^{7n/8}+1}$
5	$A_1 x^{p^{n/10}+1} + A_2 x^{p^{3n/10}+1} + A_3 x^{p^{5n/10}+1} + A_4 x^{p^{7n/10}+1} + A_5 x^{p^{9n/10}+1}$
6	$A_1 x^{p^{n/12}+1} + A_2 x^{p^{3n/12}+1} + A_3 x^{p^{5n/12}+1} + A_4 x^{p^{7n/12}+1} + A_5 x^{p^{9n/10}+1} + A_6 x^{p^{11n/12}+1}$
⋮	⋮

CHAPTER 5

Hidden Field Equations

HFE based MQ cryptosystems were proposed by Patarin [48] after he successfully attacked the MIA scheme [51]. HFE is a generalisation of the MIA scheme with the central trapdoor using a univariate quadratic polynomial over finite field $\mathbb{E}$ i.e. n degree extension of $\mathbb{F}$, instead of a monomial x^{q^h+1} used as a permutation map in MIA. In HFE cryptosystem the central quadratic polynomial P is kept secret and it's security is not based on the hardness of IP problem where private key P is known along with public key $\mathcal{P}$. However, Patarin [48] claimed that even if the private key central quadratic polynomial P is made public the extraction of remaining affine maps S, T is not feasible. Hence similar to MIA, HFE can be considered as a public key cryptosystem relying on the hardness of computing a functional decomposition (or IP problem): given a composition $f_1 \circ f_2$, can one identify the two components. In HFE, this translates to recovering the two affine polynomial maps(S, T) given a composition $(T \circ P \circ S)$ of these maps with the central quadratic polynomial map P. There have been various practical attacks on this scheme, however some standard variations that we will discuss in this chapter render those attacks in-efficient. Hence, we can consider HFE still a viable candidate with suitable parameter and variation choice. In this chapter, we shall look at the developments in terms of cryptanalytic attacks on these HFE schemes and their relation to other mathematical problems.

5.1 HFE and Multi-HFE

Patarin in [48] defined the basic HFE as follows.

Definition 5.1. Let $\mathbb{F}$ be a finite field and $\mathbb{E}$ its n degree extension such that $|\mathbb{F}| := q$, then

$$P(X) = \sum_{0 \leq i,j \leq D} A_{i,j} X^{q^i + q^j} + \sum_{0 \leq k \leq D} B_k q^k + C \qquad \forall \quad X \in \mathbb{E} \tag{5.1}$$

such that $q^i + q^j, q^k \leq D$ and co-efficients $A_{i,j}, B_i, C \in \mathbb{E}$ define the central quadratic polynomial map P for the HFE scheme. We may write this univariate quadratic polynomial in the form of system of multivarite quadratic equations over $\mathbb{F}$ as $P' := \phi \circ P \circ \phi^{-1}(x)$ for $x = (x_1, \ldots, x_n) \in \mathbb{F}^n$.

The degree of the polynomial P is upper bounded by D to allow efficient inversion of the equation $P(X) = Y$ for given $Y \in \mathbb{E}$. There are deterministic algorithms [48] for this inversion in time polynomial in D and the dimension n of extension field $\mathbb{E}$ over $\mathbb{F}$. HFE cryptosystems are susceptible to Grobner bases attacks [27]. A thorough investigation of the Grobner bases attack was given by Granboulan in [33] for HFE based MQ systems over finite fields of characteristic 2 and later by J.Ding and J.Hodges in [22] for those over finite fields of characteristic any prime p. The attack exploits the fact that the univariate equation in the extension field has a total degree that is much lower than the one for a randomly chosen equation. In order to improve upon this degree of the univariate polynomial representation over extension field $\mathbb{E}$, Patarin [2, 48] proposed a generalization of HFE that uses instead of a single univariate quadratic polynomial over extension field $\mathbb{E}$, a system of N quadratic polynomials in N variables over an extension field of degree d over $\mathbb{F}$. The basic HFE in Definition 5.1 is an instance of Multi-HFE with $N = 1$, $d = n$.

Definition 5.2. Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}_{q^d}$ its d degree extension. Let N be the number of variables and the number of secret quadratic polynomials in the polynomial ring $\mathbb{F}_{q^d}[X_1, \ldots, X_N]$ and D be their degree. Then the polynomial map $\mathcal{F} : (\mathbb{F}_{q^d})^N$ to $(\mathbb{F}_{q^d})^N$ given by

$$\mathcal{F} : (X_1, \ldots, X_N) \rightarrow (F_1(X_1, \ldots, X_N), \ldots, F_N(X_1, \ldots, X_N)$$

where

$$F_k = \sum_{1 \leq i,j \leq N} \sum_{0 \leq u,v < d} A_{k,i,j,u,v} X_i^{q^u} X_j^{q^v} + \sum_{1 \leq i \leq N} \sum_{0 \leq l < d} B_{k,i,l} X_i^{q^l} + C_k \tag{5.2}$$

such that $A_{k,i,j,u,v}, B_{k,i,u}, C_k \in \mathbb{F}_{q^d}$ for all $1 \leq i, j \leq N$, $0 \leq u, v, l < d$ and $q^l, q^u + q^v \leq D$ with $n = Nd$, defines the central quadratic polynomial map P for multi-HFE scheme.

5.2 HFE Variations

HFE has been a focus of research on MQ cryptosystems in the past and we can find recent attacks or analysis of existing attacks with new developed theoretical tools. Several major methods have been developed to attack the HFE based MQ cryptosystems. Structural attacks target the specific structure of the trapdoor involved to recover the private key. General attacks use various methods of solving set of multivariate polynomial equations e.g Gröbner basis method and its improvements and are meant to recover the plaintext for known ciphertext. Thus, we see that there are some important variations of these HFE systems developed to alter the public or private key quadratic polynomial map that increases the complexity of proposed attacks in general. We shall be discussing only few important HFE variations focused in recent cryptanalytic attacks.

5.2.1 HFE-

This variation seems simple but proves very powerful in terms of recent algebraic attacks using Gröbner bases. It basically employs the reduction map R that we discussed in Theorem 3.1. This variation has been introduced by Adi Shamir in [61]. The reduction map R is defined as $R : \mathbb{F}^m \rightarrow \mathbb{F}^{m-r}$ where m is the degree of extension as well as number of public quadratic polynomial equations. The details of this map can be reviewed from Theorem 3.1. The resultant structure of the HFE scheme can be defined as

$$\begin{aligned}\mathcal{P}' &= R \circ T \circ P \circ S \\ &= (\mathbb{F}^m, \mathbb{F}^{m-r}) \circ (\text{Aff}^{-1}(\mathbb{F}^m)) \ \circ \ \text{MQ}(\mathbb{F}^n, \mathbb{F}^m) \ \circ \ (\text{Aff}^{-1}(\mathbb{F}^n))\end{aligned}$$

Thus, a given public key $\mathcal{P}$ from $\mathbb{F}^n$ to $\mathbb{F}^m$ is transferred to public key $\mathcal{P}'$ from $\mathbb{F}^n$ to $\mathbb{F}^{m-r}$ by discarding the last r multivariate public key quadratic polynomial equations. In encryption, this slows the process of decryption for the actual recipient by a factor of $O(q^r)$ as the decryption has to be tried against q^r different possible plaintexts. Same workload is added to the signature generation, however this is already desired to add redundancy for obtaining a valid signature for the given message. In terms of algebraic attacks where the adversary is looking for obtaining relations among bits of cleartext and ciphertext, each missing bit of information (corresponding to each missing polynomial) adds a complexity of q^ω if q is the cardinality of finite field used and ω is the number of (cleartext,ciphertext) pairs to be examined for each relation.

5.2.2 HFE+

Similar to HFE-, this variation is simple to perform. Instead of hiding the public polynomial equations, this variation requires adding few redundant public quadratic polynomials to the system. Thus the resultant public key is a mapping from $\mathcal{P}$ from $\mathbb{F}^n$ to $\mathbb{F}^{m+r}$ instead of $\mathbb{F}^m$. This modification was introduced by J.Patarin in [48]. C.Wolf [56] explains different options to incorporate these additional quadratic polynomials through affine transformation in the scheme. This variation was introduced to improve the security of the HFE scheme, however it adds a workload of q^r to the resultant signature scheme as in terms of signature scheme only q^{-r} valid signatures will satisfy these additional equations and in terms of encryption it makes the resultant system over defined and hence more susceptible to algebraic attacks.

5.2.3 HFEv

This modification alters the structure of the private key central polynomial P instead of the public key polynomial map $\mathcal{P}$ as in HFE- and HFE+. Instead of allowing one central polynomial map, it introduces q^v different polynomials indirectly. The concept was introduced by Kipnis, Patarin and Goubin in [37]. We

termed the introduction of new central quadratic polynomials indirect following C.Wolf observation in [56] that would can be understood easily from Definition 5.3. HFEv differs from basic HFE in Definition 5.1 in the context of co-efficients B_i and C. In HFEv, these co-efficients are linearly and quadratically dependent on v new variables, termed as *vinegar variables*. C.Wolf in [56] gave general mathematical representation of this variation as follows:

Definition 5.3. Let $\mathbb{F}$ be a finite field and $\mathbb{E}$ its n' degree extension where $n' = n + v$ such that $|\mathbb{F}| := q$. Let $v \in \mathbb{N}$ be the number of vinegar variables then

$$P(X) = \sum_{0 \leq i,j \leq D} A_{i,j} X^{q^i + q^j} + \sum_{0 \leq k \leq D} B_k(z_1, \ldots, z_v) q^k + C(z_1, \ldots, z_v) \qquad \forall \quad X \in \mathbb{E} \tag{5.3}$$

such that $q^i + q^j, q^k \leq D$ and co-efficients $A_{i,j}, B_i, C \in \mathbb{E}$. Here $A_{i,j} X^{q^i + q^j}$, $B_k(z_1, \ldots, z_v) q^k, C$ are the quadratic, linear and constant terms respectively with $B_k(z_1, \ldots, z_v) q^k, C$ as the affine and quadratic maps in $(z_1, \ldots, z_v)$ vinegar variables.

With q^v possible choices for the v vinegar variables the central polynomial P is transformed into a polynomial map $P' := P_{z_1, \ldots, z_v}$ consisting of q^v quadratic polynomials. Inverting this polynomial map requires q^v polynomial inversions. For a signature scheme, inverting any one of the possible equation yields a valid signature for the resultant system. However, additional workload of q^v is too high for an encryption scheme to be practical. In general, for a signature scheme a random choice is made for vinegar variables $(z_1, \ldots, z_v)$ and then the resultant system consists of a single central quadratic polynomial P. This variation is susceptible to Gröbner Bases attack by Faugere [27] with another successful attack by Ding and Schmidt in [23].

5.3 Cryptanalytic Attacks against HFE

In this section we shall be reviewing briefly algebraic attacks against the HFE scheme. The interested reader can find similar overview in [56], however we present an updated version by including few recent attacks and their relation to other mathematical problems.

5.3.1 Linear Attack

The linear attack is proposed by Patarin in [48]. The attacker assumes to have two cipher-texts y, y' of related plaintexts $x, x + \lambda$. The main principle of the attack is that attacker knowing the difference λ among the unknown plaintexts evaluates the difference among the ciphertexts and in the process obtain system of linear equations in the components of plaintexts which can be solved using any equation solving method like Gaussian elimination to obtain the corresponding plaintexts.

Using Definition 3.2, we can write mathematically the difference among the i-th component of the ciphertexts as follows:

$$\begin{aligned} y'_i - y_i &= P_i(x_1 + \lambda, \ldots, x_n + \lambda) - P_i(x_1, \ldots, x_n) \\ &= \sum_{1 \le j,k \le n} \alpha_{i,j,k}(x_j + \lambda)(x_k + \lambda) + \sum_{1 \le j \le n} \beta_{i,j}(x_j + \lambda) \\ &- \sum_{1 \le j,k \le n} \alpha_{i,j,k} x_j x_k + \sum_{1 \le j \le n} \beta_{i,j} x_j \\ &= \sum_{1 \le j,k \le n} \alpha_{i,j,k}(x_j\lambda + x_k\lambda + \lambda^2) + \sum_{1 \le j \le n} \beta_{i,j}\lambda. \end{aligned}$$

Since the attacker only needs few ciphertext component equations, therefore hiding few public key equations may not effect the linear attack as in HFE- variation. However, introduction of linear attack resistant function to the plaintext may render the attack void. And in practice, an HFE encryption scheme is used to transfer the session keys that are generated using non-linear pseudo-random number generators and HFE signature scheme uses hash of the message instead which again is a non-linear function. Hence in practice the linear attack is no threat to HFE schemes.

5.3.2 Affine Multiple Attack

The attack was first proposed by Patarin against MIA scheme in [50]. The principle of the attack is to find relations among plaintext and ciphertext bits (components) that are affine (of degree one) in plaintext bits. Later any equations solving algorithm like Gaussian elimination is used to solve the system for any given plaintext. In MIA scheme these relations can be trivially extracted using the general equation for any (ciphertext(y), plaintext(x)) pair over $\mathbb{F}_{2^n}$.

$$y = x^{2^h+1}.$$

Raising both sides by $2^h - 1$ gives the relation

$$y^{2^h-1} = x^{2^{2h}-1}.$$

Multiplying both sides by xy we get

$$xy^{2^h} = yx^{2^{2h}}. \tag{5.4}$$

One side of the equation is affine in $y := (y_1, \ldots, y_n)$ and the other is affine in $x := (x_1, \ldots, x_n)$. Hence equation (5.4) can be equivalently expressed in multivariate form as a system of n equations as follows

$$L_i : \sum_{1 \le j,k \le n} \alpha_{i,j,k} x_j y_k + \sum_{1 \le j \le n} \beta_{i,j} x_i + \sum_{1 \le j \le n} \gamma_{i,j} y_i + \delta_i \qquad 1 \le i \le n. \tag{5.5}$$

These equations are quadratic in $x_j y_k$ and linear in x_i and thus can be solved for the bases for L_i using Gaussian elimination if enough of the $(x, y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ pairs

are evaluated. However, since all these equations L_i are not linearly independent in practice therefore for a given y we may not get a unique x. Assuming λ to be the number of linearly independent equations, Patarin in [50] showed that $\lambda \geq \frac{2n}{3}$ in practice and for most of the cases $\lambda \geq n - 1$.

For, HFE which is a natural generalization of MIA we can also find such an affine multiple for the public key and a constructive proof of this fact along with general algorithm to obtain an affine multiple for any polynomial, is given in [42]. Similar to MIA, this affine multiple of the HFE public key P can also be expressed in multivariate form as a system of n equations L_i as in (5.5). However, in an affine multiple of HFE, generally the y terms are not linear and hence in L_i we get exponentially many terms in variables y_i. Patarin in [48] observed that these terms in y have degree bounded by Hamming weight k. In practice, Gaussian reduction in γ terms requires a complexity of γ^ω where $\omega < 2.376$. Hence for y terms bounded by Hamming weight k, we have $O(n^{1+k})$ terms and requires a Gaussian reduction of complexity $O(n^{(1+k)\omega})$. So in general this attack is feasible for smaller values of k. Permutation polynomials generally exhibit smaller values of k in affine multiples. Patarin in [48] successfully performed this affine multiple attack against HFE systems employing Dobbertin and Dickson permutation polynomials as central quadratic polynomials P and showed the vulnerability of such permutation polynomials to affine multiple attacks.

5.3.3 Quadratic Attack

Quadratic Attack is also proposed by Patarin in [48] and is a generalization of affine multiple attack. Unlike affine multiple attack where the adversary looks for relations L_i that are affine in x (i.e. of degree one), in quadratic attack even quadratic terms in x are allowed of the form $x_i x_j$ for $1 \leq i, j \leq n$. Later these quadratic terms are linearized by introducing new variable of the form $X_{ij} := x_i x_j$ and the system is solved for the existing and $n + \frac{n(n-1)}{2}$ new variables. When the HFE cryptosystem is largely overdefined than such attack becomes feasible. In [48], Patarin showed that for many choices of P in HFE, several additional such quadratic polynomials can be obtained than those present in the public key $\mathbb{P}$. After evaluating many such (x,y) plaintext-ciphertext pairs and finding additional linear equations with redefined new variables, the attack works similar to affine multiple attack by using Gaussian reduction or any other equation solving method to evaluate the co-efficients.

Courtois [15] showed that it is possible to work with reduced system by fixing many x_i to 0. If carefully chosen the resultant system of equations is still useful to attack the basic HFE. After suggesting many variations of quadratic attack in [15], the author concluded that the basic HFE with degree of central polynomial $d > 128$ for $n > 80$, the basic HFE and its variations are still secure under quadratic attack. However, it is obvious that for such an attack the main complexity is of the memory required to store the co-efficients for additional equations.

5.3.4 Relinearization Attack

The attack was proposed by Kipnis and Shamir in [36] as the first key recover attack on the HFE systems. To review the attack we consider the private key central quadratic polynomial for homogeneous HFE cryptosystems. (cf. Definition 5.1). In the univariate representation over E i.e. n degree extension of finite field $\mathbb{F}$, the private key P is given as

$$P(X) = \sum_{0 \le i \le r-1} \sum_{0 \le j \le r-1} p_{i,j} X^{q^i + q^j} \tag{5.6}$$

such that $q^i + q^j, q^k \le D$ and co-efficients $p_{i,j} \in \mathbb{E}$. The restriction on the degree of $P(X)$ is to facilitate the efficient inversion in decryption. The resultant private key polynomial map is expressed as

$$G(X) = \phi^{-1} \circ T \circ \phi \circ P \circ \phi^{-1} \circ S \circ \phi(X)$$

where T, S are randomly chosen invertible linear transformations over $\mathbb{F}^n$ i.e. a vector space of dimension n over $\mathbb{F}$ and ϕ is a homomorphism from $\mathbb{E}$ to $\mathbb{F}^n$ with its inverse as ϕ^{-1}. Corresponding public key is expressed as:

$$\mathcal{P} = \phi \circ G \circ \phi^{-1}.$$

Kipnis and Shamir in [36] observed that every linear transformation S, T over $\mathbb{F}^n$ can be equivalently expressed over $\mathbb{E}$ as

$$S(X) = \sum_{i=0}^{n-1} s_i X^{q^i} \quad , T^{-1}(X) = \sum_{i=0}^{n-1} t_i X^{q^i} \tag{5.7}$$

where $X = \sum_{i=0}^{n-1} X_i \omega_i$ for $X_i \in \mathbb{F}$. Hence, the public key polynomial can be expressed as: $G(X) = T(P(S(X)))$ and this can be written in the matrix form over $\mathbb{E}$ as follows

$$G(X) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} g_{ij} X^{q^i + q^j} = \underline{X} G \underline{X^t} \tag{5.8}$$

where $G = [g_{ij}]$ is a matrix over $\mathbb{E}$ and $\underline{X} = (X^{q^0}, X^{q^1}, \ldots, X^{q^{n-1}})$ is the vector over $\mathbb{E}$ with $\underline{X^t}$ as its transpose. Thus, we can write

$$T^{-1}(G(X)) = \sum_{k=0}^{n-1} t_k \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} (g_{i-k,j-k})^{q^k} X^{q^i + q^j} \tag{5.9}$$

and

$$P(S(X)) = \underline{X} W P W^t \underline{X^t} \tag{5.10}$$

where $P = [p_{ij}]$ and $W = [W_{ij}] = s_{j-i}^{q^i}$ are the matrices over $\mathbb{E}$. Let G^k denote the matrix over $\mathbb{E}$ obtained from G by raising all the entries of G to q^k-th power and

cyclically rotating all rows and columns of G forward k times. Then $T^{-1}(G(X)) = \underline{X}G'\underline{X^t}$ where

$$G' = \sum_{k=0}^{n-1} t_k G^k = WPW^t \tag{5.11}$$

The $n \times n$ matrix P can only have its top left $r \times r$ block as non-zero where $r << n$. Similarly the matrix $G' = WPW^t$ has each entry as the linear combination of the t_k variables. Thus, the rank of both P and G' cannot exceed r. The main principle of the attack is to express this rank condition of $r \cong log(D)$ as a large number of equations in small number of variables. Kipnis and Shamir observed that every correct choice for n variables $t_0, t_1, \ldots, t_{n-1}$ results in the rank of G' not more than r and any other random choice results in rank close to n.

Now, the matrix G can be easily obtained from the public key of the HFE cryptosystem and G^k is derived from G as explained earlier. Taking $t_0, t_1, \ldots, t_{n-1}$ as n variables and under the condition that its rank does not exceed r establishes the fact that its left kernel $\widetilde{X} : \widetilde{X}G' = 0$ is at least an $(n-r)$ dimensional vector subspace. Thus, there exist at least $n-r$ linearly independent n-dimensional vectors $\widetilde{X_1}, \ldots, \widetilde{X_{n-r}}$ over $\mathbb{E}$ such that one can assign random values to their first $n-r$ entries still keeping them linearly independent. Assuming the remaining r entries as new variables overall we have $r(n-r)$ new variables added to the system. Each $\widetilde{X_i}G' = 0$ gives n scalar equations and in total, we have $n(n-r)$ equations in $n + r(n-r)$ variables. This gives an overdefined system of about n^2 equations in about rn variables where $r << n$. But these equations are quadratic and general technique to solve this system of equations by linearization is to replace any product of two variables $X_i X_j$ for $i \leq j$ by a new variable X_{ij} which are in total $n(n+1)/2$. In general, the resultant system is no more overdefined and by normal linearization we are not expected to obtain a unique solution.

To filter the correct solutions from many parasitic solutions obtained by Gaussian elimination of linear system of equations obtained after linearization, Kipnis and Shamir performed the technique of relinearization. In relinearization technique, they add additional constraints to relate the new variable X_{ij} with each other and obtain additional equations. For example, in degree 4 relinearization any 4-tuple of indices $1 \leq i, j, k, l \leq m$, where m is the number of total variables, can be parenthesized as follows

$$(X_i X_j)(X_k X_l) = (X_i X_k)(X_j X_l) = (X_i X_l)(X_j X_k) \Rightarrow X_{ij}X_{kl} = X_{ik}X_{jl} = X_{il}X_{jk}.$$

Hence, there are about $m^4/4!$ ways to choose 4-tuple of indices with each choice resulting in 2 quadratic equations in new variables introduced by linearization. In relinearization, these quadratic equations are further linearized by introducing new variables Y_{ij}. In general, for a system with ϵn^2 quadratic equations in n variables, the relinearization method is expected to run in polynomial time for $0 < \epsilon \leq 1/2$. Further optimization of the basic technique was also suggested by choosing degree 6 relinearization of indices and obtaining further set of equations. However in [6], it was pointed out by Curtois that degree 6 and higher relinearizations result in far less linearly independent equations and require far

more computational power becoming less useful than degree 4 relinearization. After determining t_k variables i.e. T linear transformation, known algorithms exist for solving overdefined system of equations over $\mathbb{F}$ for S, however, we only discussed the main complex part of attack in this section. The overall complexity of this attack was estimated by Curtois in [15] as $n^{log^2 d}$ where d is the degree of the central quadratic polynomial P over $\mathbb{E}$ of extension degree n.

5.3.5 Reconciliation/Distillation Attack

In [15], Curtois proposed a variant of affine multiple attack by Patarin [48] using ideas similar to Kipnis and Shamir relinearization attack [36]. Based on their simulation results for suggested parameter values of HFE in [48], they observed the existence of bi-affine equations in the input(plaintext) and output(ciphertext) components x_i, y_i of the form

$$L_i : \sum_{1 \leq j,k \leq n} \alpha_{i,j,k} x_j y_k + \sum_{1 \leq j \leq n} \beta_{i,j} x_i + \sum_{1 \leq j \leq n} \gamma_{i,j} y_i + \delta_i \qquad 1 \leq i \leq n. \tag{5.12}$$

Similar to these they also observed existence of other algebraic relations that they term as invariant or biased equations based on the criteria of invariance under any bijective affine maps like S, T in HFE and the equations that after substitution of $y = 0$ reduce to affine relation in x_i. Based on these equations they introduce reconciliation step where only certain variables are evaluated rather than all involved in the system of equations and in the subsequent distillation step they remove the unnecessary equations, reducing the overall memory requirement. As a result of their improved attack they were able to reduce the complexity in comparison to Kipnis and Shamir attack in [36] of $n^{log^2 d}$ to $n^{3 \log d + O(1)}$ where d is the degree of central quadratic polynomial P over $\mathbb{E}$ of extension degree n.

5.3.6 eXtended Linearization (XL) Attack/ Fixing and XL (FXL) Attack

The classical algorithm for solving system of equations is Gröbner bases. To construct Gröbner bases the algorithm order the monomials (lexicographical in general) and works to eliminate the highest degree monomial by combining two equations with polynomial coefficients. The process continues until a particular univariate equation remains which is then solved to solve for other variables in earlier eliminated multivariate equations. However, during the elimination process the degree of the monomials grow rapidly resulting in exponential time complexity of overall process for even modest number of variables. Curtois in [6] introduced eXtended Linearization technique which is a combination of bounded degree Gröbner bases and Linearization. The main principle of the attack is to generate higher degree variants from each polynomial by multiplying it with all possible monomials of some bounded degree and then linearize the resultant system. After linearization is the elimination step which is similar to the one in

Gröbner bases algorithm where we try to keep the univariate equations at the end and solve in reverse order for other variables.

For given m quadratic equations with n variables if the bounded degree of the monomials multiplied is $D-2$ to achieve the resultant system of equations with maximum degree D. Let l be the system of polynomial equations and $x^{D-2}l$ be the system of generated equations after monomials multiplication. Let α be the number of generated equations which is about $\frac{n^{D-2}}{(D-2)!}m$. Let β be the number of variables after linearization which is about $\frac{n^D}{D!}$, the XL algorithm is expected to succeed when $D \geq n/\sqrt{m}$ (approximately). However, their simulation results showed that

1. For $m = n : D = 2^n$.
2. For $m = n + 1 : D = n$.
3. For $m = n + C : D = \sqrt{n} \quad C \geq 2$.
4. For $m = \epsilon n^2 : D \approx 1/\sqrt{\epsilon}$; $\epsilon > 0$.

Based on their simulation results they observed that as the gap between the number of equations m and the number of variables n widens the working degree D drops significantly. Hence they developed an extension of XL algorithm as FXL algorithm (that stands for fixing and XL). It is a very simple extension with guessing step added to XL algorithm. Hence FXL algorithm works as follows

1. Fix δ variables.
2. Solve the resultant system of m equations in $n - \delta$ variables with XL algorithm.

In practice δ is kept very small since there will be q^δ choices for δ variables and the overall complexity of FXL algorithm is $q^\delta e^{c\sqrt{n}\ln n}$ for XL algorithm with complexity $e^{c\sqrt{n}\ln n}$ when $D \approx \sqrt{n}$.

5.3.7 Gröbner Bases Attack

One of the most efficient algorithm for solving system of equations is Gröbner bases and is implemented in all Computer Algebra Systems. A detailed treatment of the subject can be found in [7]. To solve a system of m polynomial equations in n variables over finite field $\mathbb{F}_q$ such that

$$P_i(x_1, \ldots, x_n) = y_i \qquad \text{for } i = 1, \ldots, m$$

where $x_j, y_i \in \mathbb{F}$ for $1 \leq j \leq n$ and $1 \leq i \leq m$, the idea is to consider the ideal I generated by the polynomials $(\widetilde{P}_i = P_i - y_i)$ for $1 \leq i \leq m$ and compute the set

of all the common zeros over the algebraic closure i.e the algebraic variety for the system. However, since we are interested in solutions over $\mathbb{F}_q$ and not algebraic closure, so the ideal considered is of the following system of $m+n$ polynomials instead i.e $I(\widetilde{P_1}, \ldots, \widetilde{P_m}, x_1^q - x, \ldots, x_n^q - x)$. In this entire process, polynomial divisions are involved and in order to get unique division results Gröbner bases are used which are defined based on specific monomial ordering.

The first successful attack on HFE system using Gröbner bases was done by Faugere in [27] where ideal is computed for the system of public polynomials for HFE system. In order to improve the complexity of the attack Faugere defined a variant of classical Buchberger algorithm [7] using a special degree reverse lexicographic order (DRL) on monomials. This enabled Faugere to determine all the algebraic relations among $m+n$ polynomial equations and propose an improved Gröbner bases computation algorithm F_5 (termed $F_5/2$ for $q=2$). The results of the experimental computations in [27] were based on the crucial point that algebraic system of polynomial equations coming from HFE can be distinguished from a random algebraic system. Hence for all practical values of d(less than 512) where d is the degree of the secret central quadratic polynomial P of the HFE system, the complexity of the $F_5/2$ attack was observed to be polynomial i.e. at most $O(n^{10})$.

Another variant of Gröbner bases attack by Faugere in [27] was proposed by Curtois in [14] for the variants of HFE such as HFE-, HFEv and HFEv-. Their attack was based on the observation that out of q^{n-m} solutions for the HFE system of m quadratic equations in n variables, we require only one candidate solution when employed as a signature scheme. Hence, certain number of variables say l may be fixed reducing the average number of solutions to q^{n-m-l}. The HFEv- variant of HFE has in general $m = h-r$ equations in $n = h+v$ variables based on the reduction map of degree r and introduction of v new vinegar variables. Hence, fixing $l = r+v$ variables, reduces the number of unknowns to $h-r$ with average number of solutions to 1. After fixing, they employ the normal Gröbner bases attack. They also proved that such perturbations of adding v new variables and reducing the public polynomial equations by factor of r lead to added security of q^{v+r} for the HFE system.

5.4 Cryptanalytic Attacks against HFE by Reduction to Other Mathematical Problems

In connection with multivariate cryptography in general, there are two very closely related problems namely isomorphism of polynomials(IP) and the MinRank(MR) as mentioned earlier in Section 3.5. In this section we shall be discussing attacks on HFE based multivariate cryptosystem based on reduction to an instance of these problem.

5.4.1 MinRank Attacks

First cryptanalytic attack on HFE based multivariate cryptosystems by reducing the problem to an instance of MinRank problem (defined in 3.5.2) was proposed by Kipnis and Shamir [36]. To improve clarity, we would like to restate the MinRank problem over finite field $\mathbb{F}$.

Definition 5.4. Let $n, r, k \in \mathbb{N}$ and given matrices $M_0, M_1, \ldots, M_k \in \mathcal{M}_{n\times n}(\mathbb{F})$ where $\mathcal{M}_{n\times n}(\mathbb{F})$ denote the $n \times n$ matrices with co-efficients in $\mathbb{F}$. The (square) MinRank Problem relates to finding any k-tuple $(\lambda_1, \ldots, \lambda_k) \in \mathbb{F}^k$ such that linear combination of the matrices M_i for $0 \leq i \leq k$ given as

$$\sum_{i=1}^{k} \lambda_i M_i - M_0$$

has rank $\leq r$.

5.4.1.1 Kipnis and Shamir Attack: Using Relinearization

Kipnis and Shamir in their relinearization attack on HFE based multivariate quadratic system over $\mathbb{F}_q$(*cf.* Section 5.3.4) proposed to consider the problem of key recovery as an instance of MinRank Problem. They formulated the key recovery attack by considering the matrix representation of public(G) and private (T, P, S) keys over $\mathbb{E}$ (i.e. an n-dimensional extension of $\mathbb{F}$).

$$\begin{aligned}
P(X) &= \sum_{0\leq i\leq r-1} \sum_{0\leq j\leq r-1} p_{i,j} X^{q^i+q^j} \\
G(X) &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} g_{ij} X^{q^i+q^j} \\
S(X) &= \sum_{i=0}^{n-1} s_i X^{q^i} \quad , \quad T(X) = \sum_{i=0}^{n-1} t_i X^{q^i}
\end{aligned}$$

such that matrices $G = [g_{ij}]$ and $P = [p_{ij}]$. Later, they obtain the following equivalence: (equation 5.11)

$$G' = \sum_{k=0}^{n-1} t_k G^k = WPW^t \tag{5.13}$$

where $W = [W_{ij}] = s_{j-i}^{q^i}$ and G^k is matrix obtained from G by raising all the entries to q^k-th power and cyclically rotating all rows and columns forward k times. From the entries of G' we get the linear combination of the t_k variables. Moreover, they observed that the rank of both P and G' cannot exceed r and suggested to express this rank condition of $r \approxeq log(D)$ (where D is the degree of $P(X)$) as a large number of equations in small number of variables. Rank

condition establishes the fact that the left kernel $\widehat{X} : \widehat{X}G' = 0$ of G' is at least an $(n-r)$ dimensional vector subspace. Thus, there exist at least $n-r$ linearly independent n-dimensional vectors $\widehat{X_1}, \ldots, \widehat{X_{n-r}}$ over $\mathbb{E}$ such that one can assign random values to their first $n-r$ entries still keeping them linearly independent. Assuming the remaining r entries as new variables overall we have $r(n-r)$ new variables added to the system. Each $\widehat{X_i}G' = 0$ gives n scalar equations and in total, we have $n(n-r)$ equations in $n+r(n-r)$ variables which can be expressed as

$$\begin{pmatrix} 1 & & & X_{1,1} & \ldots & X_{1,r} \\ & \ddots & & \vdots & \ldots & \vdots \\ & & 1 & X_{n-r,1} & \ldots & X_{n-r,r} \end{pmatrix} \big(\sum_{i=1}^{n} \lambda_i G^i - G^0 \big) = 0_n \tag{5.14}$$

which is an expression of MinRank problem as a set of multivariate quadratic equations. Kipnis and Shamir proposed to solve this system of multivariate quadratic equations by relinearization, the details of which is mentioned earlier in Section 5.3.4.

5.4.1.2 Faugere Attack: Using Gröbner Bases

Faugere in their work on cryptanalysis of MinRank problem [25] proposed to consider these $n-r$ linearly independent n dimensional vectors of the form $x^{(i)} = (a_1, \ldots, a_{n-r}, x_1^{(i)}, \ldots, x_r^{(i)})$ in the left kernel $\mathcal{K}_l$ of G' in (5.13) and define the equalities:

$$\big(\sum_{i=1}^{k} \lambda_i M_i - M_0 \big) x^{(i)} = 0_n \qquad \text{for all} \quad i: \quad 1 \leq i \leq n-r \tag{5.15}$$

to yield a quadratic system of $(n-r)n$ equations in $r.(n-r)+k$ variables. They termed these quadratic equations as f_{ij} for $1 \leq i \leq n-r$ and $1 \leq j \leq n$ corresponding to the j-th component of $\big(\sum_{i=1}^{k} \lambda_i M_i - M_0 \big) x^{(i)} = 0_n$ to define the ideal of Kipnis Shamir equations $\mathcal{I}_{KS} := \langle f_1, \ldots, f_{n(n-r)} \rangle$. To show equivalence of MinRank problem solving to this Kipnis Shamir polynomial system solving they proved that using either Minors method [13] or the Schnorr's method [16] to solve the MinRank problem results in the set of equations that belong to $\mathcal{I}_{KS}$. Hence, any solution to MinRank problem resides in the variety $\mathcal{V}_{KS}$ of Kipnis-Shamir quadratic equations. Moreover, they also observed that Kipnis-Shamir system of quadratic equations is of bilinear form i.e linear with respect to two variables.

The usual fast gröbner bases algorithm F_5 [26] works by removing all the *reductions to zero* which are useless equations not required in the Gröbner bases computations for the system. For bilinear systems these *reductions to zero* cannot be removed by usual F_5 criterion. Hence they proposed an extension of fast Gröbner bases algorithm F_5 in [28] by introducing an additional subroutine to remove all these *reductions to zero* ocurring in Gröbner bases computation for bilinear systems of equations. This also allowed them to give a complexity estimate

for such Gröbner bases computation as

$$O\left(\binom{n_x + n_y + min(n_x + 1, n_y + 1)}{min(n_x + 1, n_y + 1)}^{\omega}\right)$$

where n_x, n_y is the number of components in the two variables x, y of bilinear system of equations.

5.4.1.3 Faugere Attack: Using Matrix/Vector Operations

In [26], Faugere et al. suggested to solve the Kipnis-Shamir system of quadratic equations by computing Gröbner bases for the variety $\mathcal{V}_{KS}$. In order to further improve the complexity of the attack in section 5.4.1.2 Faugere, Betttale and Perret [1] proposed to reduce this problem of computing Gröbner bases of a polynomial system to one with computations over smaller field $\mathbb{F}_q$ instead of $\mathbb{F}_{q^n}$. In order to achieve this they introduce the change of basis matrix $M_n \in \mathcal{M}_{n\times n}(\mathbb{F}_{q^n})$ where $\mathcal{M}_{n\times n}(\mathbb{F}_{q^n})$ is the set of $n \times n$ matrices with co-efficients in $\mathbb{F}_{q^n}$ such that

$$M_n = \begin{pmatrix} \theta_1 & \theta_1^q & \dots & \theta_1^{q^{n-1}} \\ \theta_2 & \theta_2^q & \dots & \theta_2^{q^{n-1}} \\ \vdots & & \ddots & \vdots \\ \theta_n & \theta_n^q & \dots & \theta_n^{q^{n-1}} \end{pmatrix} \tag{5.16}$$

and $(\theta_1, \dots, \theta_n) \in (\mathbb{F}_{q^n})^n$ is the vector basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Using M_n, one gets the following morphism $\phi_1 : \mathbb{F}_{q^n} \to \mathbb{F}_q^n$

$$X \rightarrowtail (X, X^q, \dots, X^{q^{n-1}})M_n^{-1}$$

and its inverse $\phi_1^{-1} : \mathbb{F}_q^n \to \mathbb{F}_{q^n}$

$$(x_1, \dots, x_n) \rightarrowtail ((x_1, \dots, x_n)M_n)[1]$$

where $((x_1, \dots, x_n)M_n)[1]$ denotes the first component of the resultant vector $(x_1, \dots, x_n)M_n$. Using the morphism ϕ_1 and its inverse, the secret central polynomials in the small field can be obtained from big field univariate representation. And through this change of basis matrix M_n, they obtained the following useful result.

Lemma 5.1. *Let $M_n \in \mathcal{M}_{n\times n}(\mathbb{F}_{q^n})$. Let the symmetric matrices $(B_1, \dots, B_n) \in (\mathcal{M}_{n\times n}(\mathbb{F}_q))^n$ be associated to the multivariate secret central quadratic polynomials in the small field $(b_1, \dots, b_n) \in (\mathbb{F}_q[x_1, \dots, x_n])^n$ i.e. $b_i = \underline{x}B_i\underline{x}^t$ for $1 \leq i \leq n$. Then*

$$(B_1, \dots, B_n) = (M_n P^{*0} M_n^t, \dots, M_n P^{*n-1} M_n^t)M_n^{-1} \tag{5.17}$$

where $P = [p_{ij}] \in \mathcal{M}_{n\times n}(\mathbb{F}_{q^n})$ is the matrix associated to the univariate secret central quadratic polynomial in the big field

$$P(X) = \sum_{0\leq i\leq r-1} \sum_{0\leq j\leq r-1} p_{i,j} X^{q^i+q^j} \in \mathbb{F}_{q^n}[X]$$

and

$$P^{*k} = p^{q^k}_{(i-k) mod\, n,(j-k) mod\, n} \in \mathcal{M}_{n\times n}(\mathbb{F}_{q^n})\ \forall k \in \mathbb{N}.$$

In order to relate the small field matrix representation of public key polynomial map in HFE to the big field matrix representation of private key, Lemma 5.1 can be used. Let $G(\underline{x}), T(\underline{x}), S(\underline{x})$ and $P(\underline{x})$ be the small field representations of the public and big field representations of private keys such that $\underline{x} = (x^{q^0}, x^{q^1}, \ldots, x^{q^{n-1}})$, then we have

$$\begin{aligned}
G(\underline{x}) &= T(P(S(\underline{x}))) \\
(g_1(\underline{x}), \ldots, g_n(\underline{x}) &= (b_1(\underline{x}S), \ldots, b_n(\underline{x}S))T \\
(\underline{x}G_1\underline{x}^t, \ldots, \underline{x}G_n\underline{x}^t) &= (\underline{x}SB_1S^t\underline{x}^t, \ldots, \underline{x}SB_nS^t\underline{x}^t)T \\
(G_1, \ldots, G_n) &= (SB_1S^t, \ldots, SB_nS^t)T \\
(G_1, \ldots, G_n) &= (SM_nP^{*0}M_n^tS^t, \ldots, SM_nP^{*n-1}M_n^tS^t)M_n^{-1}T \\
(G_1, \ldots, G_n)T^{-1}M_n &= (SM_nP^{*0}M_n^tS^t, \ldots, SM_nP^{*n-1}M_n^tS^t) \\
(G_1, \ldots, G_n)U &= (WP^{*0}W^t, \ldots, WP^{*n-1}W^t) \qquad ; T^{-1}M_n = U\ ,\ SM_n = W
\end{aligned}$$

where the matrices $U = [u_{ij}], W = [w_{ij}] \in \mathcal{M}_{n\times n}(\mathbb{F}_{q^n})$. Let $(u_{0,0}, \ldots, u_{n-1,0}) \in (\mathbb{F}_{q^n})^n$ represent the first column of matrix U, then this can be expressed as:

$$\sum_{i=0}^{n-1} u_{i,0}G_{i+1} = WP^{*0}W^t = WPW^t. \tag{5.18}$$

As observed by Kipnis and Shamir, the rank of the matrices on right hand side of equations is $\log(D)$ where D is the degree bound of the secret central quadratic polynomial P. This equation is very similar to Kipnis and Shamir equation in (5.11). However, the co-efficients of the quadratic equations originating from 5.18 are in small field $\mathbb{F}_q$ unlike (5.11) where the co-efficients are in the big field $\mathbb{F}_{q^n}$. Hence, they obtained the following result.

Theorem 5.2. *[1, Theorem 2] In HFE cryptosystems, the problem of key recovery reduces to solution of MinRank problem with $k = n$ and $r = \lceil \log_q(D) \rceil$ on the public matrices $(G_1, \ldots, G_n) \in \mathcal{M}_{n\times n}(\mathbb{F}_q)^n$. The solutions of this MinRank are in $(\mathbb{F}_{q^n})^n$.*

From here on, the attack proceeds similar to Faugere attack in Section 5.4.1.2 by computing the gröbner bases of the system of quadratic equations and then its variety. However, the cost of operations is reduced by an expected factor equivalent to the cost of multiplication of two univariate polynomials of degree n over big field.

In multi-HFE cryptosystems (cf. Definition 5.2) a multivariate quadratic system of polynomials is used as the secret central private key P rather than a single univariate polynomial as in HFE. For $n = Nd$, the general form of this polynomial map $\mathcal{P} : (\mathbb{F}_{q^d})^N$ to $(\mathbb{F}_{q^d})^N$ for homogeneous system is as follows

$$\mathcal{P} : (X_1, \ldots, X_N) \to (P_1(X_1, \ldots, X_N), \ldots, P_N(X_1, \ldots, X_N)$$

where

$$P_k = \sum_{1 \le i,j \le N} \sum_{0 \le u,v < d} A_{k,i,j,u,v} X_i^{q^u} X_j^{q^v} \tag{5.19}$$

such that $A_{k,i,j,u,v} \in \mathbb{F}_{q^d}$ for all $1 \le i, j \le N$, $0 \le u, v, l < d$ and $q^u + q^v \le D$. In order to extend the attack to multi-HFE case the change of basis matrix is generalised to the following form

$$M_{N,d} = \begin{pmatrix} \theta_1 & \theta_1^q & \dots & \theta_1^{q^{d-1}} & & & & \\ \theta_2 & \theta_2^q & \dots & \theta_2^{q^{d-1}} & & & & \\ \vdots & & \ddots & \vdots & & & & \\ \theta_d & \theta_d^q & \dots & \theta_d^{q^{d-1}} & & 0 & & \\ & & & & & & & \\ & & & \ddots & & & & \\ & & & & & & & \\ & & & & \theta_1 & \theta_1^q & \dots & \theta_1^{q^{d-1}} \\ & & & & \theta_2 & \theta_2^q & \dots & \theta_2^{q^{d-1}} \\ & & 0 & & \vdots & & \ddots & \vdots \\ & & & & \theta_d & \theta_d^q & \dots & \theta_d^{q^{d-1}} \end{pmatrix} \tag{5.20}$$

Using $M_{N,d}$, one gets the following morphism $\phi_N : (\mathbb{F}_{q^d})^N \to \mathbb{F}_{q^n}$ as

$$(X_1, \dots, X_N) \rightarrowtail (V_1, V_1^q, \dots, V_N^{q^{d-1}}, \dots, V_N, V_N^q, \dots, V_N^{q^{d-1}}) M_{N,d}^{-1}$$

and its inverse $\phi_N^{-1} : \mathbb{F}_{q^n} \to (\mathbb{F}_{q^d})^N$ as

$$(x_1, \dots, x_n) \rightarrowtail (X_1, X_{d+1}, \dots, X_{d(N-1)+1}) = (x_1, \dots, x_n) M_{N,d}$$

and following from these morphisms the generalisation of Lemma 5.1 is as follows.

Lemma 5.3. *Let $M_{N,d} \in \mathcal{M}_{n\times n}(\mathbb{F}_{q^d})$. Let the symmetric matrices $(\mathbf{P_1}, \dots, \mathbf{P_N}) \in (\mathcal{M}_{n\times n}(\mathbb{F}_{q^d}))^n$ be associated to the multivariate secret central quadratic polynomials $(P_1, \dots, P_N) \in (\mathbb{F}_{q^d}[x_1, \dots, x_n])^N$ such that $P_i = \underline{X}\mathbf{P_i}\underline{X^t}$ where $\underline{X} = (X_1, X_1^q, \dots, X_1^{q^{d-1}}, \dots, X_N, X_N^q, \dots, X_N^{q^{d-1}})$. Let ${\mathbf{P_i}}^{*d,k} \in \mathcal{M}_{n\times n}(\mathbb{F}_{q^d})$ be the matrix obtained from $\mathbf{P_i}$ by rotating the rows and columns of each $d \times d$ blocks by k positions and raising each entry in the matrix to the power q^k. Also, let the symmetric matrices $(B_1, \dots, B_n) \in (\mathcal{M}_{n\times n}(\mathbb{F}_q))^n$ be associated to the multivariate secret central quadratic polynomials in the small field $(b_1, \dots, b_n) \in (\mathbb{F}_q[x_1, \dots, x_n])^n$ i.e. $b_i = \underline{x}B_i\underline{x^t}$ for $1 \le i \le n$. Then*

$$\begin{aligned}(B_1, \dots, B_n) = (&M_{N,d}{\mathbf{P_1}}^{*d,0} M_{N,d}^t, \dots, M_{N,d}{\mathbf{P_1}}^{*d,d-1} M_{N,d}^t, \dots\dots \\ &, M_{N,d}{\mathbf{P_N}}^{*d,0} M_{N,d}^t, \dots, M_{N,d}{\mathbf{P_N}}^{*d,d-1} M_{N,d}^t) M_{N,d}^{-1}.\end{aligned}$$

Thus, the relation among the public matrices $(G_1, \dots, G_n) \in (\mathcal{M}_{n\times n}(\mathbb{F}_q))^n$ and the private matrices in big field $(\mathbf{P_1}, \dots, \mathbf{P_N}) \in (\mathcal{M}_{n\times n}(\mathbb{F}_{q^d}))^N$ can be expressed

using Lemma 5.3 for multiHFE systems using change of basis matrix $M_{N,d}$ as follows

$$\begin{aligned}(G_1,\ldots,G_n)T^{-1}M_{N,d} = (&SM_{N,d}{\mathbf{P_1}}^{*d,0}S^tM_{N,d}^t,\ldots,SM_{N,d}{\mathbf{P_1}}^{*d,d-1}S^tM_{N,d}^t,\ldots\\ &,SM_{N,d}{\mathbf{P_N}}^{*d,0}S^tM_{N,d}^t,\ldots,SM_{N,d}{\mathbf{P_N}}^{*d,d-1}S^tM_{N,d}^t)\\ (G_1,\ldots,G_n)U = (&W{\mathbf{P_1}}^{*d,0}W^t,\ldots,W{\mathbf{P_1}}^{*d,d-1}W^t,\ldots,W{\mathbf{P_N}}^{*d,0}W^t,\\ &\ldots,W{\mathbf{P_N}}^{*d,d-1}W^t)\end{aligned}$$

where $U = T^{-1}M_{N,d}$ and $W = SM_{N,d}$. As a generalisation of MinRank problem in the HFE case this can be written as

$$\sum_{k=0}^{n-1} u_{k,0}G_{k+1} = W{\mathbf{P_1}}^{*d,0}W^t,\ldots,\sum_{k=0}^{n-1} u_{k,0}G_{k+1} = W{\mathbf{P_N}}^{*d,0}W^t \tag{5.21}$$

And they obtained the following result for multi-HFE as a generalisation of Theorem 5.2 in HFE case.

Theorem 5.4. *[1, Theorem 2] In multi-HFE cryptosystems, the problem of key recovery reduces to solution of MinRank problem N times with $k = n$ and $r = N\lceil\log_q(D)\rceil$ on the public matrices $(G_1,\ldots,G_n) \in \mathcal{M}_{n\times n}(\mathbb{F}_q)^n$. The solutions of this MinRank are in $(\mathbb{F}_{q^d})$.*

5.4.2 IP Attacks

In general, to unrelate the IP problem from the secret key recovery in HFE, the central quadratic polynomial is kept secret in the design of HFE systems. However, Bouillaguet, Charles, et al in [3] proposed the framework under which equivalent secret central polynomial P' can be used to reduce the problem of private key recovery to an instance of IP problem. The concept of equivalent keys for multivariate public key cryptosystems has already been introduced earlier in Section 3.4.

In [3], authors considered the usefulness of commutation of secret central polynomial with Frobenius map $F : X \to X^q$ over a finite field $\mathbb{F}$. They also observed that such property holds for certain instances of secret central polynomial $P(X) \in \mathbb{E}[X]$ where $\mathbb{E}$ is the n-dimensional extension of $\mathbb{F}$.

$$P(X) = \sum_{0\le i,j\le D} Ai,jX^{q^i+q^j} + \sum_{0\le k\le D} B_kq^k + C \qquad \forall \quad X \in \mathbb{E} \tag{5.22}$$

where $A_{i,j}, B_k, C \in \mathbb{F}$. Equivalently if the secret central polynomial P can be written as the product of some element $\omega \in \mathbb{E}$, then by employing the concept of equivalent keys, by considering equivalent affine transformations S', T' composed of original transformations S, T and the multiplication factor ω, the secret central polynomial can be considered as having co-efficients in $\mathbb{F}$. Such secret central polynomials P are observed to commute with Frobenius map F i.e.

$$P \circ F(X) = F \circ P(X).$$

Based on such commutation property, certain automorphisms among the public key $\mathcal{P} = T \circ P \circ S$ can be observed. Precisely, the authors defined $\psi(F), \ldots, \psi(F^{n-1})$ as the only solutions of such automorphism where

$$\psi : F \rightarrowtail (T.F^{-1}.T^{-1}, S^{-1}.F.S)$$

such that

$$\mathcal{P} = (T \circ F^{-1} \circ T^{-1})^{-1} \circ \mathcal{P} \circ (S^{-1} \circ F \circ S). \tag{5.23}$$

We assume to have found such an automorphism $(V, W) = \psi(F^u)$ of the public key P for some $u \in [1, n-1]$. They also observed [3, Preposition 3] that if $gcd(u, n) = 1$ (which holds if R and F are similar) then there exist equivalent linear transformations $\overline{S}, \overline{T} \in GL_n(\mathbb{F})$ such that $F = \overline{S} \circ W^k \circ \overline{S}^{-1}$ and $F = \overline{T}^{-1} \circ V^k \circ \overline{T}$ for $k := u^{-1} \bmod n$ and $\overline{S}.S^{-1}$ and $\overline{T}.T^{-1}$ commute with F. Hence, in practice $\overline{S}, \overline{T}$ can be found efficiently using knowledge of u.

The relationship among $\overline{S}, \overline{T}$ and S, T can be used to neutralize the action of S, T on the public key $\mathcal{P}$. Considering the matrix representation of Frobenius map F it can be trivially observed that other matrices commuting with F over $\mathcal{M}_{n \times n}\mathbb{F}$ (set of $n \times n$ matrices over $\mathbb{F}$) form a vector space of dimension n generated by $(F^0, F, \ldots, F^{n-1})$. From this it follows that $F_1 = \overline{S}.S^{-1}$ and $F_2 = \overline{T}.T^{-1}$ are linear combinations of powers of F over $\mathbb{F}$. Composing the public key $\mathcal{P}$ as

$$\mathcal{P} = T \circ P \circ S$$
$$\overline{T}^{-1} \circ \mathcal{P} \circ \overline{S}^{-1} = F_2^{-1} \circ P \circ F_1^{-1}$$

results in the equivalent private key

$$P' = F_2^{-1} \circ P \circ F_1^{-1}. \tag{5.24}$$

Hence we get the following equations:

$$F_1(X) = \sum_{k=0}^{n-1} a_k X^{q^k} \qquad F_1^{-1} = \sum_{k=0}^{n-1} b_k X^{q^k}$$
$$F_2(X) = \sum_{k=0}^{n-1} c_k X^{q^k} \qquad F_2^{-1} = \sum_{k=0}^{n-1} d_k X^{q^k}$$
$$P'(X) = \sum_{0 \le i,j \le D} A_{ij} X^{q^i + q^j} + \sum_{0 \le i \le D} B_i X^{q^i} + C$$
$$P(X) = \sum_{0 \le i,j \le D} e_{ij} X^{q^i + q^j} + \sum_{0 \le i \le D} f_i X^{q^i} + g$$

with unknowns $a_k, b_k, c_k, d_k, e_{ij}, f_i, g$. Composing both sides of equation (5.24) with F_1, we can write

$$F_1 \circ P' = F_2^{-1} \circ P.$$

This can be expressed as follows for left hand side

$$F_1 \circ P' = \sum_{0 \le i,j \le D} A_{ij} (\sum_{k=0}^{n-1} a_k X^{q^k})^{q^i+q^j} + \sum_{0 \le i \le D} B_i (\sum_{k=0}^{n-1} a_k X^{q^k})^{q^i} + C$$
$$= \sum_{i,j,k,l} A_{ij}.a_k.a_l.X^{q^{i+k}+q^{j+l}} + \sum_{i,k} B_i.a_k.X^{q^{i+k}} + C$$

and for right hand side

$$F_2^{-1} \circ P = \sum_{k=0}^{n-1} d_k (\sum_{0 \le i,j \le D} e_{ij} X^{q^i+q^j} + \sum_{0 \le i \le D} f_i X^{q^i} + g)^{q^k}$$
$$= \sum_{i,j,k} d_k.e_{ij}.X^{q^{i+k}+q^{j+k}} + \sum_{i,k} d_k.f_i.X^{q^{i+k}} + g.\sum_k d_k.$$

Finally, we have a system of $O(n^2)$ equations in $O(n + D^2)$ unknowns which is highly overdetermined system of equations and can be solved efficiently using fast Gröbner bases algorithms [26]. Based on their simulation results, authors in [3] also conjecture about the upper bound of complexity for their attack while using fast gröbner bases algorithm F_5 as $O(n^{21})$.

In this attack using knowledge of public key $\mathcal{P}$ and determining an equivalent central private polynomial P' but of high degree, the adversary proceeds to evaluate the private key $(T, P, S) = (\overline{T}.F_2^{-1}, P, F_1^{-1}.\overline{S})$. Initial assumption that coefficients of the actual central private polynomial P are in ground field $\mathbb{F}$ rather than extension field $\mathbb{E}$ is meaningful assumption by considering the concept of equivalent keys and sustaining transformation (*cf.* Section 3.4).

5.5 Ore's p-polynomials and security of HFE

Coulter, Havas and Henderson [10] gave an interesting insight into the security of HFE cryptosystems employing Dembowski Ostrom(DO) polynomials as the private key central polynomial. Their observation is based on the alternative definition of DO polynomials stated in [11] that establishes an important connection between p-polynomials and DO polynomials. Using this realtion they propose a partial attack on HFE cryptosystems that tries to recover one of the secret linear map T in the private key tuple (S, P, T). Hence the corresponding pubic key $\mathcal{P} = T \circ P \circ S$ gets partially factored and the resultant (expected) low degree factors can be evaluated for their inverses using efficient root finding algortihm [52, 53]

HFE cryptosystem are designed by choosing a relatively low degree central polynomial P of the form

$$P(X) = \sum_{0 \le i,j \le D} A_{ij} X^{q^i+q^j} \qquad \forall \quad X \in \mathbb{F}_q$$

where $A_{ij} \in \mathbb{F}_q$ i.e. n-degree extension of $\mathbb{F}_p$. Then this polynomial is mixed using right and left composition with two linear transformations S, T such that the resultant public key $\mathcal{P}$ is again a DO polynomial of reasonably high degree making it infeasible to compute the inverse. This was independently observed by Kipnis and Shamir [36] earlier and they also proved that any linear map can be expressed as a p-polynomial of the form

$$\sum_{i=0}^{n-1} a_i X^{p^i}.$$

It is not difficult to observe that DO polynomials are closed w.r.t left and right composition with p-polynomials. Hence the resultant public key $\mathcal{P}$ was proved [36] to have an equivalent univariate representation in the form of DO polynomial but it may have an exponential number of co-efficients and even if sparse it may have an exponentially high degree which makes inversion infeasible. However, just being a DO polynomial it is bounded to have $O(n^2)$ terms.

Coulter et al.[10] observed that there could be a possible way to reduce the degree of this resultant public key $\mathcal{P}$. Their observation is based on the following result in [11].

Theorem 5.5. *[10, Theorem 1][11, Theorem 3.2] For $f \in \mathbb{F}_q[X]$ with degree less than q the following statements are equivalent*

1. *$f = DO + L_p$ where DO is a Dembowski Ostrom polynomial and L_p is p-polynomial.*
2. *The difference polynomial $\triangle_{f,a} = L_{p_a}$ for each $a \in \mathbb{F}_q^*$ where $\triangle_{f,a} := f(X + a) - f(X) - f(a)$ is the difference polynomial of f w.r.t a and L_{p_a} is the p-polynomial depending on a.*

Considering the structure of public key $\mathcal{P} = T \circ P \circ S$, it can be considered as a left composition of $f = P \circ S$ (which is a DO polynomial itself) with T. The difference polynomial $\triangle_{\mathcal{P},a}$ can be evaluated as follows

$$\begin{aligned}
\triangle_{\mathcal{P},a} &= \mathcal{P}(X + a) - \mathcal{P}(X) - \mathcal{P}(a) \\
&= T(f(X + a)) - T(f(X)) - T(f(a)) \\
&= T(f(X + a) - f(X) - f(a)) \\
&= T \circ \triangle_{f,a}
\end{aligned}$$

$\triangle_{f,a}$ is a p-polynomial that follows from Theorem 5.5 and $\triangle_{\mathcal{P},a}$ is a p-polynomial as p-polynomials are closed w.r.t polynomial composition [44]. Ore in [44] extending his work in [45] on non-commutative polynomial rings described the algorithm to compute left and right decompositional factors of p-polynomials. In [10] authors suggested to use Ore's ideas to develop a variant of famous Euclidean algorithm [39] and evaluate Greatest Common Left Decompositional Factor (GCLDF) of the p-polynomial composition. Their proposed attack on HFE cryptosystems works as follows

1. Randomly choose distinct $a_1, a_2 \in \mathbb{F}_q^*$.
2. Calculate $L(X) = GCLDF(\triangle_{\mathcal{P},a_1}, \triangle_{\mathcal{P},a_2})$.
3. Check whether L is the left decompositional factor of $\mathcal{P}$ i.e $L(X) = T(X)$. If this holds then we are done. In [10] authors suggested $O(\log_p(deg(\mathcal{P})))$ as it's complexity where $deg(\mathcal{P})$ is the degree of public key DO polynomial.
4. If L is not the left decompositional factor of $\mathcal{P}$ then choose a different $a \in \mathbb{F}_q^*$ and calculate $L(X) = GCLDF(L(X), \triangle_{\mathcal{P},a})$. Re-evaluate 3.

In [10], they also observed that since Ore's arguments are restricted to non-commutative rings and p-polynomials and not applicable directly on the DO polynomials, hence it is not possible to use them and compute $GCLDF(L(X), \mathcal{P}(X))$ to obtain T. They also commented that a recent approach by Giesbrecht in [32] cannot be used to obtain the left decompositional factor of public key polynomial $\mathcal{P}$ since though it does claim to provide a probabilistic polynomial time algorithm to determine complete decomposition of p-polynomial but based on Ritt's theorem [60] many such decompositions exist that have equivalent factors permuted and the resultant factors from Giesbrecht's algorithm may not all fall on the left. Finally the evaluation in step 3 may not be successful as DO polynomial may or may not have a non-trivial left decompositional factor and the resultant factors may still have reasonably high degree making inversion infeasible.

Though the attack seems impractical or at least probabilistic in nature but it would be interesting to perform some simulations on practical HFE parameters and evaluate success probability of the stated attack for such parameters.

CHAPTER 6

Conclusion

In this thesis, we reviewed the MQ cryptosystems as a candidate scheme in asymmetric cryptography model. We studied the multivariate cryptosystems in a systematic way. We discussed the concept of existential forgery in regard to such schemes. Harayama and Friesen in [35] proposed the LBA on MQ cryptosystems which is an existential forgery attack. We reviewed the LBA attack originally proposed for MQ cryptosystems over $\mathbb{F}_2$ and extended it to MQ cryptosystems over $\mathbb{F}_p$ for any prime p using results from Mills [43]

Harayama and Friesen in [34] identified weak public keys that render the MQ cryptosystem susceptible to LBA in complexity asymptotically better than normal birthday attack. These weak public keys belong to DO polynomials and thus termed as *weak Dembowski Ostrom (DO) polynomials* in [34]. They also conjecture about the existence of a class of weak DO polynomials based on their simulation results. We generalised the conjectured problem to proving existence of weak DO polynomials over $\mathbb{F}_{p^n}$ for any prime p. We observed that this problem is equivalent to proving existence of certain classes of Artin-Schrier type algebraic curves over $\mathbb{F}_p[x, y]$ with many rational points without caring much about their genus. In fact, the desired rational points are at least greater than bound for weak DO polynomials. This motivated us to approach the problem from the theory of algebraic functions fields where we already had few results that assisted us in solving this problem. We proved the existence of conjectured class of weak DO polynomials given in [34] and also gave a general answer to the second open problem of enumerating such weak DO polynomials by presenting a general infinite class over finite fields $\mathbb{F}_{p^n}$ for any prime p.

HFE based MQ cryptosystems represent an important class of MQ cryptosystems and till date are considered as the most promising candidate out of this league. There are quite a few significant recent cryptanalytic attacks on HFE based MQ cryptosystems especially after introduction of odd characteristic variants for these cryptosystems. We present a comprehensive survey of these recent results for HFE cryptosystems. Coulter [10] discussed a possible connection between cryptanalysing an HFE cryptosystems and decomposition of p-polynomials [44]. They presented a partial key recovery and subsequent inversion attack on HFE cryptosystems based on this concept. We concluded our thesis with the discussion of this significant result.

REFERENCES

[1] Bettale, Luk, Faugére, Jean-Charles, and Ludovic Perret. *Cryptanalysis of HFE, multi-HFE and Variants for Odd and Even Characteristic.* Designs, Codes and Cryptography (2012): 1-52.

[2] Billet, Olivier, J. Patain, and Yannick Seurin. *Analysis of intermediate field systems.* Proceedings of the First International Conference on Symbolic Computation and Cryptography, Beijing, China. 2008.

[3] Bouillaguet, Charles, et al. *A family of weak keys in hfe (and the corresponding practical key-recovery).* Journal of Mathematical Cryptology (2009).

[4] Cannon, John, and Catherine Playoust. *MAGMA: a new computer algebra system.* Euromath Bull 2.1 (1996): 113-144.

[5] Chen, Chia-Hsin Owen, et al. *Odd - char multivariate hidden field equations.* Cryptology ePrint Archive, Report 2008/543, 2008.

[6] Courtois, Nicolas, et al. *Efficient algorithms for solving overdefined systems of multivariate polynomial equations.* Advances in Cryptology - EUROCRYPT 2000. Springer Berlin Heidelberg, 2000.

[7] Cox, David A., John Little, and Donal O'Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra.* Vol. 10. Springer Verlag, 2007.

[8] Coulter, Robert S, *Explicit evaluations of some Weil sums*, Acta Arith. 83 (1998), 241 - 251.

[9] Coulter, Robert S, *Further evaluations of Weil sums*, Acta Arith. 86 (1998), 217 - 226.

[10] Coulter, Robert S., George Havas, and Marie Henderson. *Giesbrecht's algorithm, the HFE cryptosystem, and Ore's ps-polynomials.* Lecture Notes Series of Computing 9 (2001): 36-45.

[11] Coulter, Robert S., and Rex W. Matthews. *Planar functions and planes of Lenz-Barlotti class II.* Designs, Codes and Cryptography 10.2 (1997): 167-184.

[12] Courtois, Nicolas T. *Short signatures, provable security, generic attacks, and computational security of multivariate polynomial schemes such as hfe, quartz and sflash." Polynomial Schemes such as HFE, Quartz and Sflash.* IACR E-print. 2004.

[13] Courtois, Nicolas T. *Efficient zero-knowledge authentication based on a linear algebra problem MinRank*. Advances in Cryptology - ASIACRYPT 2001. Springer Berlin Heidelberg, 2001. 402-421.

[14] Courtois, Nicolas T., Magnus Daum, and Patrick Felke. *On the security of HFE, HFEv-and Quartz*. Public Key Cryptography - PKC 2003. Springer Berlin Heidelberg, 2002. 337 - 350.

[15] Courtois, Nicolas T. *The security of hidden field equations (HFE)*. Topics in Cryptology - CT - RSA 2001. Springer Berlin Heidelberg, 2001. 266 - 281.

[16] Courtois, Nicolas T. *Decoding Linear and Rank-Distance Codes, MinRank problem and Multivariate Cryptanalysis*. (2006).

[17] Çakçak, Emrah, and Ferruh Özbudak, *Some Artin - Schreier type function fields over finite fields with prescribed genus and number of rational places*, Journal of Pure and Applied Algebra Volume 210, Issue 1, July 2007, Pages 113 - 135.

[18] Dembowski, Peter, and Thedore G. Ostrom. *Planes of order n with collineation groups of order n^2*. Mathematische Zeitschrift 103.3 (1968): 239-258.

[19] Ding, Jintai, Dieter Schmidt, and Fabian Werner. *Algebraic attack on HFE revisited*. Information Security. Springer Berlin Heidelberg, 2008. 215-227.

[20] Ding, Jintai, and Dieter Schmidt. *Rainbow, a new multivariable polynomial signature scheme*. Applied Cryptography and Network Security. Springer Berlin Heidelberg, 2005.

[21] Ding, Jintai, and Bo-Yin Yang. *Multivariate public key cryptography*. Post-Quantum Cryptography. Springer Berlin Heidelberg, 2009. 193-241.

[22] Ding, Jintai, and Timothy J. Hodges. *Inverting HFE systems is quasi-polynomial for all fields*. Advances in Cryptology - CRYPTO 2011. Springer Berlin Heidelberg, 2011. 724-742.

[23] Ding, Jintai, and Dieter Schmidt. *Cryptanalysis of HFEv and internal perturbation of HFE*. Public Key Cryptography-PKC 2005. Springer Berlin Heidelberg, 2005. 288-301.

[24] Diffie, Whitfield, and Martin E. Hellman. *Multiuser cryptographic techniques*. Proceedings of the June 7-10, 1976, national computer conference and exposition. ACM, 1976.

[25] Faugére, Jean-Charles, Françoise Levy-Dit-Vehel, and Ludovic Perret. *Cryptanalysis of minrank*. Advances in Cryptology - CRYPTO 2008. Springer Berlin Heidelberg, 2008. 280-296.

[26] Faugére, Jean-Charles. *A new efficient algorithm for computing Gröbner bases without reduction to zero F5*. Proceedings of the 2002 international symposium on Symbolic and algebraic computation. ACM, 2002.

[27] Faugére, Jean-Charles, and Antoine Joux. *Algebraic cryptanalysis of Hidden Field Equation (HFE) cryptosystems using Gröbner bases*. Advances in Cryptology - CRYPTO 2003, Lecture Notes in Computer Science, vol. 2729, pp. 44 - 60. Springer, Berlin (2003).

[28] Faugére, Jean-Charles, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. *Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1, 1): Algorithms and complexity.* Journal of Symbolic Computation 46.4 (2011): 406-437.

[29] Ferguson, Niels, Bruce Schneier, and Tadayoshi Kohno. *Cryptography engineering: design principles and practical applications*. Wiley, 2012.

[30] Fischlin, Marc, et al. *Random oracles with (out) programmability*. Advances in Cryptology-ASIACRYPT 2010. Springer Berlin Heidelberg, 2010. 303-320.

[31] Geiselmann, Willi, Willi Meier, and Rainer Steinwandt. *An attack on the isomorphisms of polynomials problem with one secret*. International Journal of Information Security 2.1 (2003): 59-64.

[32] Giesbrecht, Mark. *Factoring in skew-polynomial rings over finite fields*. Journal of Symbolic Computation 26.4 (1998): 463-486.

[33] Granboulan, Louis, Antoine Joux, and Jacques Stern. *Inverting HFE is quasipolynomial*. Advances in Cryptology - CRYPTO 2006. Springer Berlin Heidelberg, 2006. 345-356.

[34] Harayama, Tomohiro, and Donald K. Friesen. *Weil sum for birthday attack in multivariate quadratic cryptosystem*. Mathematical Cryptology JMC 1.1 (2007): 79-104.

[35] Harayama, Tomohiro. *On the weil sum evaluation of central polynomial in multivariate quadratic cryptosystem*. Cryptology ePrint Archive, Report 2006/075, 2006. Available at http://eprint. iacr. org/2006/075, 2006.

[36] Kipnis, Aviad, and Adi Shamir. *Cryptanalysis of the HFE public key cryptosystem by relinearization*. Advances in cryptology - CRYPTO 99. Springer Berlin Heidelberg, 1999.

[37] Kipnis, Aviad, Jacques Patarin, and Louis Goubin. *Unbalanced oil and vinegar signature schemes*. Advances in Cryptology - EUROCRYPT 99. Springer Berlin Heidelberg, 1999.

[38] Koblitz, Neal. *Algebraic aspects of cryptography*. Vol. 3. Springer, 2004.

[39] Lidl, Rudolf, Harald Niederreiter, and P. M. Cohn, *Finite Fields, second edition, Encyclopedia Math. Applications* Vol 20. Cambridge University Press. Cambridge 1997.

[40] Matsumoto, Tsutomu, and Hideki Imai. *Public quadratic polynomial-tuples for efficient signature-verification and message-encryption*. Advances in Cryptology - EUROCRYPT 88. Springer Berlin Heidelberg, 1988.

[41] Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. CRC press, 2010.

[42] Menezes, Alfred J., et al. *Applications of finite fields*. Vol. 199. Springer, 1992.

[43] Mills, Donald, *On the evaluation of Weil sums of Dembowski - Ostrom polynomials*. Journal of Number Theory 92 (2002), Pages 87 - 98.

[44] Ore, Oystein. *On a special class of polynomials*. Transactions of the American Mathematical Society 35.3 (1933): 559-584.

[45] Ore, Oystein. *Theory of non-commutative polynomials*. The Annals of Mathematics 34.3 (1933): 480-508.

[46] Patarin, Jacques. *Asymmetric cryptography with a hidden monomial*. Advances in Cryptology - CRYPTO 96. Springer Berlin Heidelberg, 1996.

[47] Patarin, Jacques, and Louis Goubin. *Trapdoor one-way permutations and multivariate polynomials*. Information and Communications Security (1997): 356-368.

[48] Patarin, Jacques. *Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms*. In Advances in Cryptology - EUROCRYPT 1996, volume 1070 of Lecture Notes in Computer Science, pages 33 - 48. Ueli Maurer, editor, Springer, 1996.

[49] Patarin, Jacques, and Louis Goubin. *Trapdoor one-way permutations and multivariate polynomials*. Information and Communications Security (1997): 356-368.

[50] Patarin, Jacques. *Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'98*. Designs, codes and cryptography 20.2 (2000): 175 - 209.

[51] Patarin, Jacques. *The oil and vinegar signature scheme* Dagstuhl Workshop on Cryptography, September 1997.

[52] Van Oorschot, Paul C., and Scott A. Vanstone. *A geometric approach to root finding in* $GF(q^m)$. Information Theory, IEEE Transactions on 35.2 (1989): 444-453.

[53] Von Zur Gathen, Joachim, and Victor Shoup. *Computing Frobenius maps and factoring polynomials*. Computational complexity 2.3 (1992): 187-224.

[54] Wan, Zhe-Xian. *Lectures on finite fields and Galois rings*. World Scientific Publishing Company, 2003.

[55] Wolf, Christopher, and Bart Preneel. *Taxonomy of public key schemes based on the problem of multivariate quadratic equations*. manuscript, E-Print Archive 77 (2005).

[56] Wolf, Christopher. *Multivariate quadratic polynomials in public key cryptography*. PhD thesis, Department Electrical Engineering, Katholieke Universiteit Leuven, 2005.

[57] Wolf, Christopher. *Efficient public key generation for HFE and variations*. Cryptographic Algorithms and their Uses-2004 (2004): 78-93.

[58] Wolf, Christopher, An Braeken, and Bart Preneel. *Efficient cryptanalysis of rse (2) pkc and rsse (2) pkc*. Security in Communication Networks. Springer Berlin Heidelberg, 2005. 294-309.

[59] Wolf, Christopher, and Bart Preneel. *Equivalent keys in Multivariate quadratic public key systems*. Journal of Mathematical Cryptology 4.4 (2011): 375-415.

[60] Ritt, Joseph Fels. *Prime and composite polynomials*. Transactions of the American Mathematical Society 23.1 (1922): 51-66.

[61] Shamir, Adi. *Efficient signature schemes based on birational permutations*. Advances in Cryptology CRYPTO 93. Springer Berlin Heidelberg, 1994.

[62] Stichtenoth, Henning. *Algebraic function fields and codes*. Vol. 254. Springer, 2008.

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: Alam, Bilal
Nationality: Pakistani
Date and Place of Birth: 15 Dec 1981, Pakistan
Marital Status: Married
Email: alam54b@gmail.com

EDUCATION

Degree	Institution	Year of Graduation
M.S.	IAM, METU Ankara, Turkey	2009
B.Sc(Avionics).	College of Aeronautical Engineering Pakistan	2001
High School	PAF Intermediate College Chaklala, Pakistan	1997

PROFESSIONAL EXPERIENCE

Year	Place	Enrollment
2001-till date	Pakistan Air Force	Engineer

PUBLICATIONS

Bilal Alam, Oğuz Yayla, Ferruh Özbudak. ***Classes of Weak Dembowski-Ostrom Polynomials for Multivariate Quadratic Cryptosystems***, Submitted.

Bilal Alam, Oğuz Yayla ***Recent attacks against HFE/Multi-HFE MQ cryptosystems and Connection with Ore's p-polynomial decomposition***. Submitted.