RESULTS ON SOME AUTHENTICATION CODES

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

BY

ELİF KURTARAN ÖZBUDAK

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

FEBRUARY 2009

Approval of the thesis:

RESULTS ON SOME AUTHENTICATION CODES

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

Prof. Dr. Ersan Akyıldız _____
Director, Graduate School of **Applied Mathematics**

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

Prof. Dr. Ferruh Özbudak _____
Supervisor, **Department of Mathematics, METU**

Examining Committee Members:

Assoc. Prof. Dr. Ali Doğanaksoy _____
Department of Mathematics, METU

Prof. Dr. Ferruh Özbudak _____
Institute of Applied Mathematics, METU

Assoc. Prof. Dr. Emrah Çakçak _____
Department of Mathematics, METU

Dr. Zülfükar Saygı _____
Department of Mathematics, TOBB ETU

Dr. Burcu Gülmez Temur _____
Department of Mathematics, Atılım University

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: ELİF KURTARAN ÖZBUDAK

Signature :

ABSTRACT

RESULTS ON SOME AUTHENTICATION CODES

Kurtaran Özbudak, Elif
Ph.D., Department of Cryptography
Supervisor : Prof. Dr. Ferruh Özbudak

February 2009, 80 pages

In this thesis we study a class of authentication codes with secrecy. We obtain the maximum success probability of the impersonation attack and the maximum success probability of the substitution attack on these authentication codes with secrecy. Moreover we determine the level of secrecy provided by these authentication codes. Our methods are based on the theory of algebraic function fields over finite fields. We study a certain class of algebraic function fields over finite fields related to this class of authentication codes. We also determine the number of rational places of this class of algebraic function fields.

Keywords: Authentication codes with secrecy, algebraic function fields over finite fields

ÖZ

BAZI DOĞRULAMA KODLARI ÜZERİNE SONUÇLAR

Kurtaran Özbudak, Elif
Doktora, Kriptografi Bölümü
Tez Yöneticisi : Prof. Dr. Ferruh Özbudak

Şubat 2009, 80 sayfa

Bu tezde bir sınıf sırlı doğrulama kodlarını çalıştık. Bu sırlı doğrulama kodları üzerindeki yerine geçme atağının en yüksek başarı olasılığını ve yerine koyma atağının en yüksek başarı olasılığını bulduk. Ayrıca bu doğrulama kodları tarafından sunulan sır derecesini elde ettik. Metodlarımız sonlu cisimler üzerindeki foksiyon cisimleri teorisine dayanmaktadır. Bu doğrulama kodlarıyla ilişkili bır sınıf sonlu cisimler üzerindeki foksiyon cisimlerini çalıştık. Bu fonksiyon cisimleri üzerindeki rasyonel nokta sayısını da elde ettik.

Anahtar Kelimeler: Sırlı doğrulama kodları, sonlu cisimler üzerindeki cebirsel fonksiyon cisimleri

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my supervisor and to the members of the Institute of Applied Mathematics for their encouragement, motivation and guidance throughout my graduate studies and in completing this thesis.

Moreover I would like to thank to my colleagues at TÜBİTAK-UEKAE G222 Unit and to my managers Önder Yetiş, Alparslan Babaoğlu and Kıvanç Dinçer for the support they provided me.

Finally very special thanks go to my family for their unfailing support.

PREFACE

In this thesis we study a class of authentication codes with secrecy. This class is related to a class of authentication codes considered in [4]. We obtain the maximum success probability of the impersonation attack and the maximum success probability of the substitution attack on these authentication codes with secrecy. Moreover we determine the level of secrecy provided by these authentication codes. These results give new contributions to some open problems mentioned in [4].

Our methods are based on the theory of algebraic function fields. We study a certain class of algebraic function fields over finite fields related to this class of authentication codes. We determine the number of rational places of this class of algebraic function fields. These results extend some of the corresponding results of [1].

This thesis is organized as follows. In Chapter 1 we give a general background on authentication codes and algebraic function fields over finite fields. Our results on the class of algebraic function fields over finite fields mentioned above are presented in Chapter 2. We give our results on the class of authentication codes with secrecy that we study in Chapter 3. The results of Chapter 2 are essentially used in Chapter 3.

TABLE OF CONTENTS

ABSTRACT iv

ÖZ v

ACKNOWLEDGMENTS vi

PREFACE vii

TABLE OF CONTENTS viii

CHAPTERS

1 BACKGROUND ON AUTHENTICATION CODES AND ALGEBRAIC FUNCTION FIELDS 1

1.1 AN INTRODUCTION TO AUTHENTICATION CODES 1

1.2 AN INTRODUCTION TO ALGEBRAIC FUNCTION FIELDS OVER FINITE FIELDS 4

2 A CLASS OF ALGEBRAIC FUNCTION FIELDS OVER FINITE FIELDS . 6

2.1 INTRODUCTION 6

2.2 SOME RESULTS USING QUADRATIC FORMS 8

2.3 NUMBER OF RATIONAL PLACES 15

3 A CLASS OF AUTHENTICATION CODES WITH SECRECY 19

3.1 PRELIMINARIES 20

3.2 THE MAXIMUM SUCCESS PROBABILITY OF THE IMPERSONATION ATTACK 26

3.3 THE MAXIMUM SUCCESS PROBABILITY OF THE SUBSTITUTION ATTACK: CASE $\frac{m}{\gcd(2h,m)}$ IS EVEN 34

3.4 THE MAXIMUM SUCCESS PROBABILITY OF THE SUBSTITUTION ATTACK: CASE $\frac{m}{\gcd(2h,m)}$ IS ODD AND m IS EVEN . . . 37

3.5 THE MAXIMUM SUCCESS PROBABILITY OF THE SUBSTITUTION ATTACK: CASE $\frac{m}{\gcd(2h,m)}$ IS ODD AND m IS ODD 67

3.6 THE LEVEL OF SECRECY 72

REFERENCES 78

VITA 79

CHAPTER 1

BACKGROUND ON AUTHENTICATION CODES AND ALGEBRAIC FUNCTION FIELDS

In this chapter, a general background on authentication codes and algebraic function fields over finite fields is presented.

In Section 1.1 we give some basic definitions on authentication codes. Our main concern in the class of authentication codes in this thesis is the subclass of authentication codes with secrecy and we give more emphasis on authentication codes with secrecy.

There are various approaches to the study of authentication codes. Some of these approaches use methods from areas including computer science, information theory, combinatoric, graph theory and design theory. Our approach is based on algebraic methods, and in particular based on algebraic function fields over finite fields.

A part of our contributions and most of our methods in this thesis are related to the theory of algebraic function fields over finite fields. In Section 1.2 we give a very short introduction to some basic notions of algebraic function fields over finite fields. We refer the reader to [14] for a very nice and detailed account of algebraic function fields over finite fields.

1.1 AN INTRODUCTION TO AUTHENTICATION CODES

In 1974, Gilbert, MacWilliams and Sloane introduced the idea of authentication codes [6]. In their model, there are two trusting parties: a transmitter and a receiver. The transmitter wants to send a piece of information securely using her secret key over a public channel.

In 1984, Simmons proposed a new model [13]. In his model, there is also an opponent involved together with the two trusting parties. In this model, the opponent could observe and disturb the ordinary communication.

The class of authentication codes are divided into two subclasses:

i) authentication codes without secrecy,

ii) authentication codes with secrecy.

In an authentication code without secrecy, the transmitter and the receiver share a secret key. In the transmitter end, a message is obtained by encoding a source state to the corresponding tag. The shared key is used for the generation of the tag. Then the transmitter sends the message to the receiver over the public channel. Here there is no encryption of the message. Therefore, without knowledge of the shared secret key, an opponent can recover the source state from the encoded message.

In the authentication code with secrecy, there is an encryption of the source state. Again the transmitter and the receiver share a secret key. A part of the shared key is used for the encryption of the source state. The remaining part of the key is used for the generation of the tag. Then the message is obtained from the source state using the encrypted version of the source state and the generated tag. Therefore, without knowledge of the shared secret key, an opponent cannot recover the source state from the encoded message.

Authentication codes with secrecy are considered, using a variety of approaches in, for example, [2], [4], [5], [6], [9], [11], [12], [13], [15], [16], [17].

A formal definition of authentication codes is given as follows.

Definition 1.1.1 *An authentication code is a quadruple* $(\mathcal{S}, \mathcal{K}, \mathcal{M}, \mathcal{E})$*, where*

1. $\mathcal{S}$ *is the set of possible source states (plain texts),*

2. $\mathcal{K}$ *is the set of available keys,*

3. $\mathcal{M}$ *is the set of messages, and*

4. *$\mathcal{E}$ is the set of authentication maps (encoding rules) from $\mathcal{S} \times \mathcal{K}$ to $\mathcal{M}$. For authentication codes with secrecy, the encryption is considered as a part of the authentication map in this definition.*

There is a generalization of the model above. In this generalized model, an authentication map can send a source state to more than one message. This is called splitting. In this thesis we consider authentication codes without splitting.

For authentication codes with secrecy, the general protocol can be described in detail as follows:

(1) Let $s \in \mathcal{S}$ be a source state to be transmitted. Let $k \in \mathcal{K}$ be a secret key, which is known by the transmitter and the receiver. Let E_k be the corresponding authentication map. We consider E_k as

$$E_k = (f_k, g_k) \in \mathcal{E},$$

where f_k is the part of the authentication map used for the encryption of the source state, and g_k is the part of the authentication map used for the generation of the corresponding tag. The message is considered as consisting of two parts. The first part is the image of the map of the source state under the map f_k, which is the encrypted part. The second part of the message is the image of the map g_k of the source state to the corresponding tag. Note that the second part is used only for authentication and hence the length of the second part is shorter than the first part.

Let the transmitted message be

$$m_k = (f_k(s), g_k(s)).$$

(2) The receiver gets the message $m' = (m_1, m_2)$. Using the shared key k and the decryption map f_k^{-1}, the receiver computes $s' = f_k^{-1}(m_1)$.

(3) The receiver computes $m_2' = g_k(s')$. Then the receiver compares m_2 with m_2'.

   (a) If $m_2 = m_2'$, then the receiver assumes that m' is a valid message.

   (b) If $m_2 \neq m_2'$, then the receiver rejects the message m'.

We assume that everything about the authentication model is publicly known due to the *Kerckhoff's principle*. Hence the opponent knows the whole parameters of the authentication code, except the secret key shared by the transmitter and the receiver.

Now we explain two attacks by the opponent that we will study.

Assume that the opponent generates a random message m' from the message set $\mathcal{M}$ and inserts it to the public channel. This is called the *impersonation attack*.

Assume that the opponent observes a message m to be transmitted, and then the opponent changes it with a different message m' randomly. This is called the *substitution attack*.

Usually the maximum success probabilities of the impersonation and the substitution attacks are denoted by $\mathcal{P}_I$ and $\mathcal{P}_S$, respectively.

Finally we recall the definition of the level of secrecy of authentication codes with secrecy. The level of secrecy provided by an authentication code with secrecy is the uncertainty of the source state when the corresponding message is observed.

1.2 AN INTRODUCTION TO ALGEBRAIC FUNCTION FIELDS OVER FINITE FIELDS

In this section we recall some basic definitions and we explain some notation that we use in this thesis on algebraic function fields over finite fields.

Let q be a power of a prime. Let $\mathbb{F}_q$ denote a finite field with q elements.

An *algebraic function field* F over $\mathbb{F}_q$ is an extension field of $\mathbb{F}_q$ such that there exists an element $z \in F$ that is transcendental over $\mathbb{F}_q$ and for which F is a finite extension of the rational function field $\mathbb{F}_q(z)$. Moreover, we call $\mathbb{F}_q$ the *full constant field* of F if $\mathbb{F}_q$ is algebraically closed in F. A *place* of F is the maximal ideal of some valuation ring of F. Let $\mathbb{Z}$ denote the set of integers. A *normalized discrete valuation* of F is a surjective map $v : F \to \mathbb{Z} \cup \{\infty\}$ satisfying the following:

(i) $v(x) = \infty \iff x = 0$;

(ii) $v(xy) = v(x) + v(y)$ for all $x, y \in F$;

(iii) $\nu(x+y) \geq \min(\nu(x), \nu(y))$ for all $x, y \in F$;

(iv) $\nu(a) = 0$ for all $a \in \mathbb{F}_q \setminus \{0\}$.

There is a bijective correspondence between the places of F and the normalized discrete valuations of F. Let v_P be the normalized discrete valuation of F corresponding to the place P of F. The valuation ring of P is

$$O_P = \{x \in F : v_P(x) \geq 0\}$$

and the maximal ideal of O_P is

$$M_P = \{x \in O_P : v_P(x) > 0\}.$$

If $\mathbb{F}_q$ is the full constant field of F, then the residue class field O_P/M_P can be identified with a finite extension of $\mathbb{F}_q$. The degree of this extension is called the *degree* of the place P. A place of degree 1 is called *rational*. We usually denote the number of rational places of F by $N(F)$.

The research area on algebraic function fields over finite fields is a very active research area and it has many applications. For further information on algebraic function fields and their applications we refer, for example, to the excellent books of Stichtenoth [14] and Niderreiter and Xing [10].

CHAPTER 2

A CLASS OF ALGEBRAIC FUNCTION FIELDS OVER FINITE FIELDS

In this chapter we study a class of algebraic function fields defined in Section 2.1 below (see the definition in (2.1)). We determine the number of rational places of these algebraic function fields. In particular our results extend some of the corresponding results of [1].

We refer to Chapter 1 for a basic background on algebraic function fields over finite fields. We also refer to Chapter 1 for the notation and basic definitions.

This chapter is organized as follows: In Section 2.1 we introduce the class of algebraic function fields that we will study. We also introduce some basic definitions and some notation. In Section 2.2, using some results from [8], we obtain useful results that we will use in Section 2.3. We conclude our chapter in Section 2.3. The main result of this chapter is Theorem 2.3.1.

The results of this chapter will be used in Chapter 3 essentially.

2.1 INTRODUCTION

In this section we introduce a class of algebraic function fields that we will study. Moreover we recall some basic definitions and we fix some notation.

Let q be a power of an odd prime. Let $m \geq 2$ be a positive integer. By a curve we mean a smooth, geometrically irreducible, projective curve defined over a finite field. The theory of algebraic curves is essentially equivalent to the theory of algebraic function fields. Therefore we use the terms function field and curve interchangeably.

Let

$$S(X) = s_0X + s_1X^q + \cdots + s_hX^{q^h} \in \mathbb{F}_{q^m}[X]$$

be an $\mathbb{F}_q$-linearized polynomial with $h \geq 0$ and $s_h \neq 0$. Let

$$L(X) = \mu_0X + \mu_1X^q + \cdots + \mu_nX^{q^n} \in \mathbb{F}_{q^m}[X]$$

be an arbitrary $\mathbb{F}_q$-linearized polynomial. Let $\beta \in \mathbb{F}_{q^m}$ be an arbitrary element. Let F be the algebraic function field

$$F := \mathbb{F}_{q^m}(X, Y) \quad \text{with} \quad Y^q - Y = XS(X) + L(X) + \beta. \tag{2.1}$$

In this chapter we determine the number $N(F)$ of rational places of F. Our results in this chapter extend the corresponding results of [1].

Let Tr denote the trace map from $\mathbb{F}_{q^m}$ onto $\mathbb{F}_q$, i.e., $\mathrm{Tr}(x) = x + x^q + \cdots + x^{q^{m-1}}$. Let B_S be the symmetric bilinear form on the $\mathbb{F}_q$-linear vector space $\mathbb{F}_{q^m}$ defined as

$$\begin{aligned} B_S : \mathbb{F}_{q^m} \times \mathbb{F}_{q^m} &\to \mathbb{F}_q \\ (x, y) &\mapsto \mathrm{Tr}\left(xS(y) + yS(x)\right). \end{aligned}$$

Let Q_S be the map

$$\begin{aligned} Q_S : \mathbb{F}_{q^m} &\to \mathbb{F}_q \\ x &\mapsto \mathrm{Tr}\left(xS(x)\right). \end{aligned}$$

Let W_S be the radical of B_S, which is defined as

$$W_S = \{x \in \mathbb{F}_{q^m} : B_S(x, y) = 0 \quad \text{for each } y \in \mathbb{F}_{q^m}\}. \tag{2.2}$$

For $x \in \mathbb{F}_{q^m}$, we observe that $x \in W_S$ if and only if $\mathrm{Tr}\left(xS(y) + yS(x)\right) = 0$ for all $y \in \mathbb{F}_{q^m}$, which means

$$\mathrm{Tr}\left(x\left(s_oy + s_1y^q + \cdots + s_hy^{q^h}\right) + y\left(s_0x + s_1x^q + \cdots + s_hx^{q^h}\right)\right) = 0$$

for all $y \in \mathbb{F}_{q^m}$. Note that

$$\begin{aligned} \mathrm{Tr}\left(xs_1y^q\right) &= \mathrm{Tr}\left((xs_1)^{q^{-1}}y\right), \\ \mathrm{Tr}\left(xs_2y^{q^2}\right) &= \mathrm{Tr}\left((xs_2)^{q^{-2}}y\right), \\ &\vdots \\ \mathrm{Tr}\left(xs_hy^{q^h}\right) &= \mathrm{Tr}\left((xs_h)^{q^{-h}}y\right) \end{aligned}$$

Hence for $x \in \mathbb{F}_{q^m}$, we have that $x \in W_S$ if and only if

$$\mathrm{Tr}\left(y \left(\sum_{i=1}^{h} (xs_i)^{q^{-i}} + (xs_0) + (s_0 x) + \sum_{i=1}^{h} \left(s_i x^{q^i} \right) \right) \right) = 0,$$

for each $y \in \mathbb{F}_{q^m}$. Let $u \in \mathbb{F}_{q^m}$ be the term, depending on $x \in \mathbb{F}_{q^m}$ and $S(X) \in \mathbb{F}_{q^m}[X]$, defined as

$$u = \left(\sum_{i=1}^{h} (xs_i)^{q^{-i}} + xs_0 \right) + \left(s_0 x + \sum_{i=1}^{h} \left(s_i x^{q^i} \right) \right).$$

Note that

$$\mathrm{Tr}(yu) = 0 \quad \text{for each } y \in \mathbb{F}_{q^m}$$

if and only if $u = 0$. Taking q^h-th power of u we obtain that, for $x \in \mathbb{F}_{q^m}$, $x \in W_s$ if and only if x is a root of the $\mathbb{F}_q$-linearized polynomial

$$\sum_{i=0}^{h-1} s_{h-i}^{q^i} T^{q^i} + 2s_0^{q^h} T^{q^h} + \sum_{i=1}^{h} s_i^{q^h} T^{q^{h+i}} \in \mathbb{F}_{q^m}[T]. \tag{2.3}$$

Let k be the $\mathbb{F}_q$-dimension

$$k := \dim_{\mathbb{F}_q} W_S$$

of W_S. Note that the degree of the $\mathbb{F}_q$-linearized polynomial in (2.3) is q^{2h}. Hence we have that

$$k \leq \min\{2h, m\}.$$

We choose an $\mathbb{F}_q$-linear subspace $\overline{W}_S$ of $\mathbb{F}_{q^m}$ such that

$$W_S \oplus \overline{W}_S = \mathbb{F}_{q^m}.$$

In particular $\dim_{\mathbb{F}_q} \overline{W}_S = m - k$. It is clear that the restriction of B_S onto $\mathbb{F}_q$-linear space $\overline{W}_S$ gives a nondegenerate symmetric bilinear form on $\overline{W}_S$.

2.2 SOME RESULTS USING QUADRATIC FORMS

In this section we obtain some results using quadratic forms. In particular we use some results from [8]. These will be useful in the next section.

We start with the following lemma.

Lemma 2.2.1 *There exists a basis* $\{e_1, e_2, \ldots, e_{m-k}\}$ *of* $\overline{W}_S$ *over* $\mathbb{F}_q$ *and* $d \in \mathbb{F}_q \setminus \{0\}$ *such that*

$$\begin{aligned} &B_S\left(x_1e_1 + x_2e_2 + \cdots + x_{m-k}e_{m-k}, y_1e_1 + y_2e_2 + \cdots + y_{m-k}e_{m-k}\right) \\ &= x_1y_1 + x_2y_2 + \cdots + x_{m-k-1}y_{m-k-1} + dx_{m-k}y_{m-k} \end{aligned}$$

for all $x_1, y_1, \ldots, x_{m-k}, y_{m-k} \in \mathbb{F}_q$.

Proof. Note that B_S is a nondegenerate symmetric bilinear from on $\overline{W}_S$. Moreover the characteristic of $\mathbb{F}_q$ is odd. Therefore by [7, Theorem 4.9] there exists a basis $\{e_1, e_2, \ldots, e_{m-k}\}$ of $\overline{W}_S$ over $\mathbb{F}_q$ such that the representing matrix of B_S corresponding to the basis $\{e_1, e_2, \ldots, e_{m-k}\}$ is the $(m-k) \times (m-k)$ diagonal matrix

$$\begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ & & & & d \end{bmatrix},$$

where $d \in \mathbb{F}_q \setminus \{0\}$. This completes the proof. ■

We choose a basis $\{e_1, e_2, \ldots, e_{m-k}\}$ of $\overline{W}_S$ as in Lemma 2.2.1. Moreover let $d \in \mathbb{F}_q \setminus \{0\}$ be the corresponding nonzero element given in Lemma 2.2.1.

We further choose a basis $\{f_1, f_2, \ldots, f_k\}$ of W_S over $\mathbb{F}_q$ in an arbitrary manner. Note that $\{e_1, e_2, \ldots, e_{m-k}, f_1, f_2, \ldots, f_k\}$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

Lemma 2.2.2 *Under the notation and assumptions as above, for* $x_1, x_2, \ldots, x_{m-k}, y_1, y_2, y_k \in \mathbb{F}_q$, *we have the identity that*

$$\begin{aligned} &Q_S\left(x_1e_1 + x_2e_2 + \cdots + x_{m-k}e_{m-k} + y_1f_1 + y_2f_2 + \cdots + y_kf_k\right) \\ &= \frac{1}{2}\left(x_1^2 + x_2^2 + \cdots + x_{m-k-1}^2 + dx_{m-k}^2\right). \end{aligned}$$

In particular the term above is independent from $y_1, y_2, \ldots, y_k$.

Proof. Note that for $x, y \in \mathbb{F}_{q^m}$ we have

$$B_S(x, y) = \mathrm{Tr}(xS(y) + yS(x)),$$

and

$$Q_S(x) = \mathrm{Tr}(xS(x)).$$

Hence

$$\begin{aligned} B_S(x,x) &= \mathrm{Tr}(xS(x)+xS(x)) \\ &= 2\mathrm{Tr}(xS(x)) \\ &= 2Q_S(x). \end{aligned}$$

Note that $2 \neq 0$ as q is odd. Putting

$$x = x_1e_1 + x_2e_2 + \cdots + x_{m-k}e_{m-k} + y_1f_1 + y_2f_2 + \cdots + y_kf_k,$$

and

$$u = x_1e_1 + x_2e_2 + \cdots + x_{m-k}e_{m-k}, \quad v = y_1f_1 + y_2f_2 + \cdots + y_kf_k,$$

we obtain that

$$B_S(x,x) = B_S(u+v,u+v) = B_S(u,u) + 2B_S(u,v) + B_S(v,v).$$

As $v \in W_S$, we have that $B_S(u,v) = B_S(v,v) = 0$ and hence

$$\begin{aligned} B_S(x,x) &= B_S(x_1e_1 + x_2e_2 + \cdots + x_{m-k}e_{m-k}) \\ &= x_1^2 + x_2^2 + \cdots + x_{m-k-1}^2 + dx_{m-k}^2, \end{aligned}$$

where we use Lemma 2.2.1 in the last step. This completes the proof. ■

Let $H(x_1,\ldots,x_{m-k}) \in \mathbb{F}_q[x_1,\ldots,x_{m-k}]$ be the polynomial over $\mathbb{F}_q$ in $m-k$ indeterminates $x_1, x_2, \ldots, x_{m-k}$ given by

$$H(x_1,\ldots,x_{m-k}) := \frac{1}{2}\left(x_1^2 + x_2^2 + \cdots + dx_{m-k}^2\right).$$

Recall that the function field F is defined as

$$F = \mathbb{F}_{q^m}(X,Y) \quad \text{with} \quad Y^q - Y = XS(X) + L(X) + \beta,$$

where

$$L(X) = \mu_0X + \mu_1X^q + \cdots + \mu_nX^{q^n} \in \mathbb{F}_{q^m}[X]$$

is an arbitrary $\mathbb{F}_q$-linearized polynomial and $\beta \in \mathbb{F}_{q^m}$ is an arbitrary element.

For $1 \leq i \leq m-k$, let

$$a_i := \mathrm{Tr}(L(e_i)) \in \mathbb{F}_q.$$

For $1 \leq i \leq k$, let

$$b_i := \mathrm{Tr}(L(f_i)) \in \mathbb{F}_q.$$

Finally let

$$b := \mathrm{Tr}(\beta) \in \mathbb{F}_q.$$

Lemma 2.2.3 *Under the notation and assumptions above, for* $x_1, x_2, \ldots, x_{m-k}, y_1, \ldots, y_k \in \mathbb{F}_q$, *let*

$$X = x_1 e_1 + x_2 e_2 + \cdots x_{m-k} e_{m-k} + y_1 f_1 + y_2 f_2 + \cdots + y_k f_k \in \mathbb{F}_{q^m},$$

and let

$$\begin{aligned} \overline{x}_1 &= x_1 + a_1, \\ \overline{x}_2 &= x_2 + a_2, \\ &\vdots \\ \overline{x}_{m-k-1} &= x_{m-k-1} = a_{m-k-1}, \\ \overline{x}_{m-k} &= x_{m-k} + \tfrac{a_{m-k}}{d}. \end{aligned}$$

Moreover let $A \in \mathbb{F}_q$ *be the evaluation*

$$A = H\left(a_1, a_2, \ldots, a_{m-k-1}, \frac{a_{m-k}}{d}\right)$$

of the polynomial $H(x_1, x_2, \ldots, x_{m-k}) \in \mathbb{F}_q[x_1, x_2, \ldots, x_{m-k}]$ *at the point* $(a_1, a_2, \ldots, a_{m-k-1}, \frac{a_{m-k}}{d}) \in \mathbb{F}_q^{m-k}$. *Then we have the identity*

$$\mathrm{Tr}\left(XS(X) + L(X) + \beta\right) = H(\overline{x}_1, \overline{x}_2 \ldots, \overline{x}_{m-k}) + b_1 y_1 + b_2 y_2 + \cdots + b_k y_k - A + b.$$

Proof. We first consider the left hand side

$$\mathrm{Tr}(XS(X) + L(X) + \beta).$$

Using Lemma 2.2.2 we have

$$Q_S(X) = \mathrm{Tr}(XS(X)) = \frac{1}{2}\left(x_1^2 + x_2^2 + \cdots + x_{m-k-1}^2 + d x_{m-k}^2\right).$$

It is easy to observe that

$$\mathrm{Tr}(L(X)) = a_1 x_1 + a_2 x_2 + \cdots + a_{m-k} x_{m-k} + b_1 y_1 + b_2 y_2 + \cdots + b_k y_k,$$

and

$$\mathrm{Tr}(\beta) = b.$$

Hence the left hand side is

$$\frac{1}{2}\left(x_1^2 + x_2^2 + \cdots + x_{m-k-1}^2 + dx_{m-k}^2\right) + \sum_{i=1}^{m-k} a_i x_i + \sum_{i=1}^{k} b_i y_i + b. \tag{2.4}$$

Next we consider the right hand side

$$H(\overline{x}_1, \overline{x}_2 \ldots, \overline{x}_{m-k}) + b_1 y_1 + b_2 y_2 + \cdots + b_k y_k - A + b.$$

Note that

$$\begin{aligned}
\tfrac{1}{2}\overline{x}_1^2 - \tfrac{1}{2}a_1^2 &= \tfrac{1}{2}(x_1 + a_1)^2 - \tfrac{1}{2}a_1^2 = \tfrac{1}{2}x_1^2 + a_1 x_1, \\
\tfrac{1}{2}\overline{x}_2^2 - \tfrac{1}{2}a_2^2 &= \tfrac{1}{2}(x_2 + a_2)^2 - \tfrac{1}{2}a_2^2 = \tfrac{1}{2}x_2^2 + a_2 x_2, \\
&\vdots \\
\tfrac{1}{2}\overline{x}_{m-k-1}^2 - \tfrac{1}{2}a_{m-k-1}^2 &= \tfrac{1}{2}(x_{m-k-1} + a_{m-k-1})^2 - \tfrac{1}{2}a_{m-k-1}^2 = \tfrac{1}{2}x_{m-k-1}^2 + a_{m-k-1}x_{m-k-1},
\end{aligned}$$

and

$$\frac{d}{2}\overline{x}_{m-k}^2 - \frac{d}{2}\left(\frac{a_{m-k}}{d}\right)^2 = \frac{d}{2}\left(x_{m-k} + \frac{a_{m-k}}{d}\right)^2 - \frac{1}{2}\frac{a_{m-k}^2}{d} = \frac{d}{2}x_{m-k}^2 + x_{m-k}a_{m-k}.$$

Hence the right hand side is equal to (2.4). This completes the proof. ■

The following lemma holds for q even as well.

Lemma 2.2.4 *Let q be a power of an arbitrary prime number, i.e., including the case of even characteristic as well. Let $n \geq 2$ be an integer and $g(x_1, x_2, \ldots, x_{n-1}) \in \mathbb{F}_q[x_1, x_2, \ldots, x_{n-1}]$ be a polynomial in $n-1$ indeterminates $x_1, x_2, \ldots, x_{n-1}$. Let $a \in \mathbb{F}_q \setminus \{0\}$ be a nonzero element. The number of the solutions of the equation*

$$g(x_1, x_2, \ldots, x_{n-1}) + ax_n = 0,$$

with $x_1, x_2, \ldots, x_{n-1}, x_n \in \mathbb{F}_q$ is q^{n-1}.

Proof. We show that for any $u_1, u_2, \ldots, u_{n-1} \in \mathbb{F}_q$, there exists a uniquely determined $u_n \in \mathbb{F}_q$ such that $(x_1, x_2, \ldots, x_{n-1}, x_n) = (u_1, u_2, \ldots, u_{n-1}, u_n)$ is a solution. Let

$$u_n = -\frac{g(u_1 u_2, \ldots, u_{n-1})}{a}. \tag{2.5}$$

As $g(x_1, x_2, \ldots, x_{n-1})$ is a polynomial in $\mathbb{F}_q[x_1, x_2, \ldots, x_{n-1}]$ and $a \in \mathbb{F}_q \backslash \{0\}$, for any $u_1, u_2, \ldots, u_{n-1} \in \mathbb{F}_q$ the evaluation $g(u_1, u_2, \ldots, u_{n-1})$ and hence $u_n \in \mathbb{F}_q$ is uniquely determined by (2.5). Running through all $u_1, u_2, \ldots, u_{n-1}$ we obtain all q^{n-1} solutions. This completes the proof.

■

Let $\psi : \mathbb{F}_{q^m} \to \mathbb{F}_q$ be the $\mathbb{F}_q$-linear map

$$\psi(x) = \mathrm{Tr}(L(x)). \tag{2.6}$$

Recall that $\{f_1, f_2, \ldots, f_k\}$ is a basis of $W_S \subseteq \mathbb{F}_{q^m}$ and $b_i = \mathrm{Tr}(L(f_i))$ for $1 \leq i \leq k$. Hence

$$W_S \subseteq \mathrm{Ker}\psi \Longleftrightarrow b_1 = b_2 = \cdots = b_k = 0. \tag{2.7}$$

In the following proposition we would like to determine $N(F)$ in a relatively easier particular case. Its proof will be included in the proof of Theorem 2.3.1 below.

Proposition 2.2.5 *Let q be a power of an odd prime and $m \geq 2$ be a positive integer. Let $S(X) = s_0X + s_1X^q + \cdots + s_hX^{q^h} \in \mathbb{F}_{q^m}[X]$ be an $\mathbb{F}_q$-linearized polynomial with $s_h \neq 0$ and $h \geq 0$. Let*

$$L(X) = \mu_0X + \mu_1X^q + \cdots + \mu_nX^{q^n} \in \mathbb{F}_{q^m}[X]$$

be an arbitrary $\mathbb{F}_q$-linear polynomial. Let $\beta \in \mathbb{F}_{q^m}$ be an arbitrary element. Let F be the algebraic function field

$$F = \mathbb{F}_{q^m}(X, Y) \quad with \quad Y^q - Y = XS(X) + L(X) + \beta.$$

Let W_S be the radical defined in (2.2). Let ψ be the $\mathbb{F}_q$-linear map defined in (2.6). If $W_s \nsubseteq$ Kerψ, then for the number $N(F)$ of rational places of F we have

$$N(F) = 1 + q^m.$$

In this chapter, from now on we assume that $W_S \subseteq \mathrm{Ker}\psi$, or equivalently, $b_1 = b_2 = \cdots = b_k = 0$. Therefore the identity in Lemma 2.2.3 becomes

$$\mathrm{Tr}\,(XS(X) + L(X) + \beta) = H(\overline{x}_1, \overline{x}_2 \ldots, \overline{x}_{m-k}) - A + b.$$

We will use the following lemmas.

Lemma 2.2.6 *Let q be a power of an odd prime, $u \in \mathbb{F}_q$ and $d \in \mathbb{F}_q \setminus \{0\}$. Let $n \geq 2$ be an even integer. We consider the number N of solutions of the equation*

$$x_1^2 + x_2^2 + \cdots + x_{n-1}^2 + dx_n^2 = u$$

with $x_1, x_2, \ldots, x_n \in \mathbb{F}_q$. Assume first that $u \neq 0$. Then we have

$$N = \begin{cases} q^{n-1} - q^{n/2-1} & \text{if } (-1)^{n/2}d \text{ is a square in } \mathbb{F}_q, \\ q^{n-1} + q^{n/2-1} & \text{if } (-1)^{n/2}d \text{ is not a square in } \mathbb{F}_q. \end{cases} \tag{2.8}$$

Assume next that $u = 0$. Then we have

$$N = \begin{cases} q^{n-1} + (q-1)q^{n/2-1} & \text{if } (-1)^{n/2}d \text{ is a square in } \mathbb{F}_q, \\ q^{n-1} - (q-1)q^{n/2-1} & \text{if } (-1)^{n/2}d \text{ is not a square in } \mathbb{F}_q. \end{cases} \tag{2.9}$$

Proof. We use the notation of [8, Theorem 6.26] in this proof. Under this notation we have $f(x_1, x_2, \ldots, x_n) = x_1^2 + x_2^2 + \cdots + x_{n-1}^2 + dx_n^2 \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$. For the determinant of the polynomial f we have $\det(f) = d$ (see [8, page 280] for a definition of the determinant $\det(f)$).

For the integer valued-function $\upsilon(\cdot)$ on $\mathbb{F}_q$ (see [8, Definition 6.22]) we have

$$\upsilon(u) = \begin{cases} -1 & \text{if } u \neq 0, \\ q-1 & \text{if } u = 0. \end{cases} \tag{2.10}$$

Note that if η is the quadratic character of $\mathbb{F}_q$ and $x \in \mathbb{F}_q \setminus \{0\}$, then

$$\eta(x) = \begin{cases} 1 & \text{if } x \text{ is a square in } \mathbb{F}_q, \\ -1 & \text{if } x \text{ is not a square in } \mathbb{F}_q. \end{cases} \tag{2.11}$$

Assume first that $u \neq 0$. Then $\upsilon(u) = -1$ by (2.10). Moreover

$$\eta(d) = \begin{cases} 1 & \text{if } d \text{ is a square in } \mathbb{F}_q, \\ -1 & \text{if } d \text{ is not a square in } \mathbb{F}_q \end{cases} \tag{2.12}$$

by (2.11). Hence using [8, Theorem 6.26] we obtain (2.8).

Assume next that $u = 0$. Then $\upsilon(u) = q - 1$ by (2.10). Hence using (2.12) and [8, Theorem 6.26] we obtain (2.9). This completes the proof. ■

Lemma 2.2.7 *Let q be a power of an odd prime, $u \in \mathbb{F}_q$ and $d \in \mathbb{F}_q \setminus \{0\}$. Let $n \geq 3$ be an odd integer. We consider the number N of solutions of the equation*

$$x_1^2 + x_2^2 + \cdots + x_{n-1}^2 + dx_n^2 = u$$

with $x_1, x_2, \ldots, x_n \in \mathbb{F}_q$. *Then we have*

$$N = \begin{cases} q^{n-1} + q^{(n-1)/2} & \text{if } (-1)^{(n-1)/2} du \text{ is a square in } \mathbb{F}_q, \\ q^{n-1} - q^{(n-1)/2} & \text{if } (-1)^{(n-1)/2} du \text{ is not a square in } \mathbb{F}_q. \end{cases} \tag{2.13}$$

Proof. We use the notation of [8, Theorem 6.27] in this proof. Under this notation we have the polynomial $f(x_1, x_2, \ldots, x_m)$ and the (extended) quadratic character η of $\mathbb{F}_q$ as in the proof of Lemma 2.2.6. Here N does not depend on $v(u)$, but it depends only on $\eta\left((-1)^{(n-1)/2} du\right)$. Hence we have two cases in (2.13) instead of four cases of Lemma 2.2.6. Using [8, Theorem 6.27] we complete the proof. ■

2.3 NUMBER OF RATIONAL PLACES

Thanks to the results of Section 2.2, now we are ready to determine the number $N(F)$ of the rational places of F in all cases. In this section we determine the number of rational places of the algebraic function field given in (2.1).

Theorem 2.3.1 *Let q be a power of an odd prime. Let $m \geq 2$ be an integer. Let $S(X) = s_0 X + s_1 X^q + \cdots + s_h X^{q^h} \in \mathbb{F}_{q^m}[X]$ be an $\mathbb{F}_q$-linearized polynomial with $s_h \neq 0$ and $h \geq 0$. Let*

$$L(X) = \mu_0 X + \mu_1 X^q + \cdots + \mu_n X^{q^n} \in \mathbb{F}_{q^m}[X]$$

be an arbitrary $\mathbb{F}_q$-linear polynomial. Let $\beta \in \mathbb{F}_{q^m}$ be an arbitrary element. Let F be the algebraic function field

$$F = \mathbb{F}_{q^m}(X, Y) \quad \text{with} \quad Y^q - Y = XS(X) + L(X) + \beta.$$

Let W_S be the radical defined in (2.2). Let $k = \dim_{\mathbb{F}_q} W_S$ be the $\mathbb{F}_q$-dimension of W_S. We choose an $\mathbb{F}_q$-linear subspace $\overline{W}_S$ of $\mathbb{F}_{q^m}$ such that $W_S \oplus \overline{W}_S = \mathbb{F}_{q^m}$. Let $\{e_1, e_2, \ldots, e_{m-k}\}$ be an $\mathbb{F}_q$-basis of $\overline{W}_S$ and $d \in \mathbb{F}_q \setminus \{0\}$ be a nonzero element given by Lemma 2.2.1. Let $H(x_1, x_2, \ldots, x_{m-k}) \in \mathbb{F}_q[x_1, x_2, \ldots, x_{m-k}]$ be the polynomial over $\mathbb{F}_q$ in $m-k$ indeterminates $x_1, x_2, \ldots, x_{m-k}$ given by

$$H(x_1, \ldots, x_{m-k}) = \frac{1}{2}\left(x_1^2 + x_2^2 + \cdots + d x_{m-k}^2\right).$$

For $1 \leq i \leq m-k$, let

$$a_i = \mathrm{Tr}(L(e_i)) \in \mathbb{F}_q.$$

Let

$$A = H\left(a_1, a_2, \ldots, a_{m-k-1}, \frac{a_{m-k}}{d}\right) \in \mathbb{F}_q$$

and

$$b = \mathrm{Tr}(\beta) \in \mathbb{F}_q.$$

Let $\psi : \mathbb{F}_{q^m} \to \mathbb{F}_q$ *be the* $\mathbb{F}_q$*-linear map*

$$\psi(x) = \mathrm{Tr}(L(x)).$$

If $W_S \nsubseteq \mathrm{Ker}\psi$*, then for the number* $N(F)$ *of rational places of* F *we have*

$$N(F) = 1 + q^m. \tag{2.14}$$

If $W_S \subseteq \mathrm{Ker}\psi$*,* $m - k$ *is even and* $A \neq b$*, then for the number* $N(F)$ *of rational places of* F *we have*

$$N(F) = \begin{cases} 1 + q^m - q^{(m+k)/2} & \text{if } (-1)^{(m-k)/2}d \text{ is a square in } \mathbb{F}_q, \\ 1 + q^m + q^{(m+k)/2} & \text{if } (-1)^{(m-k)/2}d \text{ is not a square in } \mathbb{F}_q. \end{cases} \tag{2.15}$$

If $W_S \subseteq \mathrm{Ker}\psi$*,* $m - k$ *is even and* $A = b$*, then for the number* $N(F)$ *of rational places of* F *we have*

$$N(F) = \begin{cases} 1 + q^m + (q-1)q^{(m+k)/2} & \text{if } u \text{ is a square in } \mathbb{F}_q, \\ 1 + q^m - (q-1)q^{(m+k)/2} & \text{if } u \text{ is not a square in } \mathbb{F}_q, \end{cases} \tag{2.16}$$

where $u = (-1)^{(m-k)/2}d \in \mathbb{F}_q$*.*

If $W_S \subseteq \mathrm{Ker}\psi$ *and* $m - k$ *is odd, then for the number* $N(F)$ *of rational places of* F *we have*

$$N(F) = \begin{cases} 1 + q^m + q^{(m+k+1)/2} & \text{if } u \text{ is a square in } \mathbb{F}_q, \\ 1 + q^m - q^{(m+k+1)/2} & \text{if } u \text{ is not a square in } \mathbb{F}_q, \end{cases} \tag{2.17}$$

where $u = (-1)^{(m-k-1)/2}2d(A - b) \in \mathbb{F}_q$*.*

Proof. For $\gamma \in \mathbb{F}_{q^m}$, consider the equation

$$x^q - x = \gamma. \tag{2.18}$$

This has a solution if and only if

$$\mathrm{Tr}(\gamma) = 0.$$

Moreover if $\mathrm{Tr}(\gamma) = 0$, then the number of solutions of (2.18) with $x \in \mathbb{F}_{q^m}$ is q. Also these statements hold independent from the characteristic of $\mathbb{F}_q$, i.e., they hold for any finite field $\mathbb{F}_q$ and any extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ with $m \geq 2$. This useful result is well known and it is called as Hilbert's Theorem 90.

Let P_∞ be the place of the rational function field $\mathbb{F}_q(X)$ corresponding to the pole of X. It is also well known that the place P_∞ is totally ramified in the extension $F/\mathbb{F}_q(X)$ and there is a unique rational place of F over P_∞.

Let N be the number of solutions of the equation

$$H(x_1, x_2, \ldots, x_{m-k}) + b_1y_1 + b_2y_2 + \cdots + b_ky_k - A + b = 0$$

with $x_1, x_2, \ldots, x_{m-k}, y_1, y_2, \ldots, y_k \in \mathbb{F}_q$. Then using the arguments above, Hilbert's Theorem 90 and Lemma 2.2.3 we obtain that

$$N(F) = 1 + qN. \tag{2.19}$$

First we assume that $W_s \nsubseteq \mathrm{Ker}\psi$ (cf. Proposition 2.2.5). Using (2.7) we conclude that there exists a nonzero element of the set $\{b_1, b_2, \ldots, b_k\}$. Hence using Lemma 2.2.4 we obtain that

$$N = q^{m-1}. \tag{2.20}$$

Combining (2.19) and (2.20) we obtain (2.14), which also proves Proposition 2.2.5.

In this proof from now on we assume that $W_S \subseteq \mathrm{Ker}\psi$, or equivalently $b_1 = b_2 = \cdots = b_k = 0$. Let N_1 be the number of the solutions of

$$H(x_1, x_2, \ldots, x_{m-k}) - A + b = 0$$

with $x_1, x_2, \ldots, x_{m-k} \in \mathbb{F}_q$. Then we immediately obtain that

$$N = q^k N_1. \tag{2.21}$$

We consider the case that $m-k$ is even and $A \neq b$. Then using (2.8) in Lemma 2.2.6 we obtain that

$$N_1 = \begin{cases} q^{m-k-1} - q^{(m-k)/2-1} & \text{if } (-1)^{(m-k)/2}d \text{ is a square in } \mathbb{F}_q, \\ q^{m-k-1} + q^{(m-k)/2-1} & \text{if } (-1)^{(m-k)/2}d \text{ is not a square in } \mathbb{F}_q. \end{cases} \tag{2.22}$$

Note that

$$q \cdot q^k \cdot q^{m-k-1} = q^m, \quad q \cdot q^k \cdot q^{(m-k)/2-1} = q^{(m+k)/2}. \tag{2.23}$$

Hence combining (2.19), (2.21), (2.22) and (2.23) we prove (2.15).

Next we consider the case that $m-k$ is even and $A = b$. Using (2.9) in Lemma 2.2.6 we obtain that

$$N_1 = \begin{cases} q^{m-k-1} + (q-1)q^{(m-k)/2-1} & \text{if } u \text{ is a square in } \mathbb{F}_q, \\ q^{m-k-1} - (q-1)q^{(m-k)/2-1} & \text{if } u \text{ is not a square in } \mathbb{F}_q, \end{cases} \tag{2.24}$$

where $u = (-1)^{(m-k)/2}d \in \mathbb{F}_q$. Combining (2.19), (2.21), (2.23) and (2.24) we prove (2.16).

Finally we consider the remaining case that $m-k$ is odd. Using Lemma 2.2.7 we obtain that

$$N_1 = \begin{cases} q^{m-k-1} + q^{(m-k-1)/2} & \text{if } u \text{ is a square in } \mathbb{F}_q, \\ q^{m-k-1} - q^{(m-k-1)/2} & \text{if } u \text{ is not a square in } \mathbb{F}_q, \end{cases} \tag{2.25}$$

where $u = (-1)^{(m-k-1)/2}2d(A-b) \in \mathbb{F}_q$. Note that

$$q \cdot q^k \cdot q^{(m-k-1)/2} = q^{(m+k+1)/2}. \tag{2.26}$$

Combining (2.19), (2.21), (2.23), (2.25) and (2.26) we prove (2.17). This completes the proof.

■

CHAPTER 3

A CLASS OF AUTHENTICATION CODES WITH SECRECY

In this chapter we study the class of authentication codes with secrecy defined in Section 3.1 below (see the definition in (3.1)). In particular we obtain some contributions to some open problems mentioned in [4].

We refer to Chapter 1 for a background on authentications codes with secrecy. We also refer to Chapter 1 for the notions and definitions of impersonation attack, substitution attack and level of secrecy protection.

This chapter is organized as follows: We introduce a class of authentication codes with secrecy, fix some notation and give some preliminary results in Section 3.1. We study the maximum success probability $\mathcal{P}_I$ of the impersonation attack on these codes in Section 3.2. The determination of the maximum success probability $\mathcal{P}_S$ of the substitution attack on these codes is more involved. We begin our study on $\mathcal{P}_S$ and we determine $\mathcal{P}_S$ when $\frac{m}{\gcd(2h,m)}$ is even in Section 3.3. It will be clear below why it is necessary to consider the cases $\frac{m}{\gcd(2h,m)}$ is even and $\frac{m}{\gcd(2h,m)}$ is odd separately when we study $\mathcal{P}_S$. The study of $\mathcal{P}_S$ is more interesting when $\frac{m}{\gcd(2h,m)}$ is odd. In Section 3.4 we obtain some preliminary results on $\mathcal{P}_S$ and study $\mathcal{P}_S$ when $\frac{m}{\gcd(2h,m)}$ is odd and m is even. Similarly, using the preliminary results of Section 3.4, we obtain $\mathcal{P}_S$ when $\frac{m}{\gcd(2h,m)}$ is odd and m is odd in Section 3.5. Finally we study the level of secrecy provided by these authentication codes in Section 3.6.

Our results in this chapter refine and improve some of the results of [12] extensively. Throughout this chapter, we use some results from Chapter 2.

3.1 PRELIMINARIES

In this section we introduce a class of authentication codes with secrecy, give some results that we use later and we fix some notation.

Let q be a power of a prime. For a positive integer m, $\mathbb{F}_{q^m}$ denotes a finite field with q^m elements. For $m \geq 2$, let $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ denote the trace map from $\mathbb{F}_{q^m}$ onto $\mathbb{F}_q$ given by

$$\begin{aligned} \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q} : \mathbb{F}_{q^m} &\to \mathbb{F}_q \\ x &\mapsto x + x^q + \cdots + x^{q^{m-1}}. \end{aligned}$$

When it is clear from context, we also denote $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ as Tr in short.

Now we introduce a class of authentication codes.

Let q be a power of an odd prime, $m \geq 2$ and $h \geq 1$ be integers. Let Tr denote the trace map from $\mathbb{F}_{q^m}$ onto $\mathbb{F}_q$.

Let Π be the map defined as

$$\begin{aligned} \Pi : \mathbb{F}_{q^m} &\to \mathbb{F}_q \\ x &\mapsto \mathrm{Tr}\left(x^{q^h+1}\right). \end{aligned}$$

The authentication code with secrecy we consider is $(\mathcal{S}, \mathcal{K}, \mathcal{M}, \mathcal{E})$ with

$$\begin{cases} \mathcal{S} = \mathbb{F}_{q^m}, \\ \mathcal{K} = \mathbb{F}_{q^m}, \\ \mathcal{M} = \mathbb{F}_{q^m} \times \mathbb{F}_q, \\ \mathcal{E} = \{E_k : k \in \mathcal{K}\}, \end{cases} \tag{3.1}$$

where for $k \in \mathcal{K}$, the authentication map E_k is defined as

$$\begin{aligned} E_k : \mathcal{S} &\to \mathcal{M} \\ s &\mapsto (s + k, \Pi(s) + \Pi(k)). \end{aligned}$$

It follows from the definition that the maximum success probability $\mathcal{P}_I$ of the impersonation attack on the authentication code with secrecy in (3.1) is

$$\mathcal{P}_I = \max_{m=(m_1,m_2)} \frac{|\{k \in \mathcal{K} : \Pi(m_1 - k) + \Pi(k) = m_2\}|}{|\mathcal{K}|}$$

where the maximum is over $\mathcal{M}$, that is the maximum is defined as m_1 runs through $\mathbb{F}_{q^m}$ and m_2 runs through $\mathbb{F}_q$.

Again it follows from the definition that the maximum success probability $\mathcal{P}_{\mathcal{S}}$ of the substitution attack on the authentication code with secrecy in (3.1) is

$$\mathcal{P}_{\mathcal{S}} = \max_{\boldsymbol{m},\boldsymbol{d}} \frac{|\{s \in \mathcal{S} : \Pi(s) + \Pi(m_1 - s) = m_2, \quad \Pi(s + d_1) - \Pi(s) = d_2\}|}{|\{s \in \mathcal{S} : \Pi(s) + \Pi(m_1 - s) = m_2\}|},$$

where the maximum is over $\boldsymbol{m} = (m_1, m_2) \in \mathcal{M} = \mathbb{F}_{q^m} \times \mathbb{F}_q$ and $\boldsymbol{d} = (d_1, d_2) \in \mathcal{M}$ with $d_1 \neq 0$.

In the rest of this section we give some preliminary results that we will use later. We start with a simple lemma.

Lemma 3.1.1 *Let q be a power of a prime. Let a, b be positive integers. Then we have*

$$\gcd\left(q^a - 1, q^b - 1\right) = q^{\gcd(a,b)} - 1.$$

Proof. We begin with an observation. Let c be a positive integer dividing a. We have

$$q^a - 1 = q^{c\left(\frac{a}{c}\right)} - 1 = (q^c - 1)\left(1 + q^c + q^{2c} + \cdots + q^{\left(\frac{a}{c}-1\right)c}\right).$$

This implies that

$$\left(q^{\gcd(a,b)} - 1\right) \mid (q^a - 1),$$

and

$$\left(q^{\gcd(a,b)} - 1\right) \mid \left(q^b - 1\right).$$

Therefore we have

$$\left(q^{\gcd(a,b)} - 1\right) \mid \gcd\left(q^a - 1, q^b - 1\right). \tag{3.2}$$

Let $r = \gcd(q^a - 1, q^b - 1)$. Then $r \mid (q^a - 1)$, $r \mid (q^b - 1)$, and in particular

$$\begin{aligned} q^a &\equiv 1 \mod r, \\ q^b &\equiv 1 \mod r. \end{aligned}$$

For any integers $\ell_1, \ell_2 \in \mathbb{Z}$ we have that

$$q^{\ell_1 a + \ell_2 b} \equiv (q^a)^{\ell_1} \left(q^b\right)^{\ell_2} \equiv 1 \cdot 1 \equiv 1 \mod r. \tag{3.3}$$

There exist integers $\ell_1, \ell_2 \in \mathbb{Z}$ such that

$$\gcd(a, b) = \ell_1 a + \ell_2 b. \tag{3.4}$$

Then using (3.3) and (3.4) we obtain that

$$q^{\gcd(a,b)} \equiv 1 \mod r,$$

and hence

$$\gcd\left(q^a - 1, q^b - 1\right) \mid \left(q^{\gcd(a,b)} - 1\right). \tag{3.5}$$

Combining (3.2) and (3.5) we complete the proof. ■

The following lemma is crucial for our results.

Lemma 3.1.2 *Let q be a power of an odd prime. Let a, m be positive integers. Let W be the set of the zeroes of the $\mathbb{F}_q$-linearized polynomial*

$$T + T^{q^a} \in \mathbb{F}_q[T]$$

in $\mathbb{F}_{q^m}$. Let

$$\overline{a} = \gcd(a, m).$$

If $\frac{m}{\overline{a}}$ is odd, then

$$W = \{0\},$$

and in particular $|W| = 1$.

If $\frac{m}{\overline{a}}$ is even, then the $\mathbb{F}_q$-linearized polynomial

$$T + T^{q^{\overline{a}}} \in \mathbb{F}_q[T] \tag{3.6}$$

splits in the subfield $\mathbb{F}_{q^{2\overline{a}}}$ of $\mathbb{F}_{q^m}$. Moreover, in this case, W is equal to the set of zeroes of the polynomial in (3.6), in particular $|W| = q^{\overline{a}}$.

Proof. Note that $0 \in W$. Let $x \in \mathbb{F}_{q^m} \setminus \{0\}$ and assume that $x \in W$. Then

$$x^{q^a} = -x,$$

and hence

$$x^{2(q^a-1)} = 1. \tag{3.7}$$

As $x \in \mathbb{F}_{q^m} \setminus \{0\}$, we also have

$$x^{q^m-1} = 1. \tag{3.8}$$

Combining (3.7) and (3.8) we obtain that

$$x^{\gcd(2(q^a-1),q^m-1)} = 1. \tag{3.9}$$

By Lemma 3.1.1 we have

$$q^{\overline{a}} - 1 = \gcd\left(q^a - 1, q^m - 1\right). \tag{3.10}$$

Note that

$$q^m - 1 = q^{\overline{a}\cdot\frac{m}{\overline{a}}} - 1 = \left(q^{\overline{a}} - 1\right)\left(1 + q^{\overline{a}} + q^{2\overline{a}} + \cdots + q^{\left(\frac{m}{\overline{a}}-1\right)\overline{a}}\right). \tag{3.11}$$

The number of terms in the sum

$$1 + q^{\overline{a}} + q^{2\overline{a}} + \cdots + q^{\left(\frac{m}{\overline{a}}-1\right)\overline{a}}$$

is $\dfrac{m}{\overline{a}}$. Moreover

$$q^{i\overline{a}} \equiv 1 \mod 2$$

for $1 \le i \le \frac{m}{\overline{a}} - 1$, as q is odd. Hence

$$1 + q^{\overline{a}} + q^{2\overline{a}} + \cdots + q^{\left(\frac{m}{\overline{a}}-1\right)\overline{a}} \equiv \begin{cases} 1 \mod 2 & \text{if } \frac{m}{\overline{a}} \text{ is odd,} \\ 0 \mod 2 & \text{if } \frac{m}{\overline{a}} \text{ is even.} \end{cases} \tag{3.12}$$

Using (3.10), (3.11) and (3.12) we obtain that

$$\gcd\left(2\frac{q^a-1}{q^{\overline{a}}-1}, \frac{q^m-1}{q^{\overline{a}}-1}\right) = \begin{cases} 1 & \text{if } \frac{m}{\overline{a}} \text{ is odd,} \\ 2 & \text{if } \frac{m}{\overline{a}} \text{ is even.} \end{cases} \tag{3.13}$$

In (3.13) we use the fact that

$$\gcd\left(\frac{q^a-1}{q^{\overline{a}}-1}, \frac{q^m-1}{q^{\overline{a}}-1}\right) = 1,$$

which follows from (3.10). Then using (3.13) we obtain that

$$\gcd\left(2(q^a-1), q^m-1\right) = \begin{cases} q^{\overline{a}} - 1 & \text{if } \frac{m}{\overline{a}} \text{ is odd,} \\ 2\left(q^{\overline{a}} - 1\right) & \text{if } \frac{m}{\overline{a}} \text{ is even.} \end{cases} \tag{3.14}$$

First we consider the case that $\frac{m}{\overline{a}}$ is odd. By (3.9) and (3.14) we have

$$x^{q^{\overline{a}}-1} = 1$$

and hence

$$x^{q^{\overline{a}}} = x.$$

Then

$$x^{q^{2\overline{a}}} = \left(x^{q^{\overline{a}}}\right)^{q^{\overline{a}}} = (x)^{q^{\overline{a}}} = x.$$

Similarly for any integer $\ell \geq 1$ we have

$$x^{q^{\ell\overline{a}}} = x.$$

In particular for $\ell = \frac{a}{\overline{a}}$ we obtain that

$$x^{q^a} = x. \tag{3.15}$$

As $x \in W$, we also have

$$x^{q^a} = -x. \tag{3.16}$$

Recall that $x \in \mathbb{F}_{q^m} \setminus \{0\}$. Combining (3.15), (3.16) and using the fact that q is odd we arrive to the contradiction that $x = 0$. Hence $W = \{0\}$ in the case that $\frac{m}{\overline{a}}$ is odd.

Next we consider the case that $\frac{m}{\overline{a}}$ is even. By (3.9) and (3.14) we have

$$\left(x^{q^{\overline{a}}-1}\right)^2 = 1.$$

Hence

$$x^{q^{\overline{a}}-1} = 1 \quad \text{or} \quad x^{q^{\overline{a}}-1} = -1.$$

If $x^{q^{\overline{a}}-1} = 1$, then as in the case that $\frac{m}{\overline{a}}$ is odd, we arrive to the conclusion that $x^{q^a} = x$. As $x^{q^a} = -x$, $x \neq 0$, and q is odd, we obtain a contradiction. Therefore $x^{q^{\overline{a}}-1} = -1$ and

$$x + x^{q^{\overline{a}}} = 0. \tag{3.17}$$

Note that $\mathbb{F}_{q^{2\overline{a}}} \subseteq \mathbb{F}_{q^m}$ as $\frac{m}{\overline{a}}$ is even. Moreover for $y \in \mathbb{F}_{q^{2\overline{a}}}$, its trace $\mathrm{Tr}_{\mathbb{F}_{q^{2\overline{a}}}/\mathbb{F}_{q^{\overline{a}}}}(y)$ relative to $\mathbb{F}_{q^{\overline{a}}}$ is given by

$$\mathrm{Tr}_{\mathbb{F}_{q^{2\overline{a}}}/\mathbb{F}_{q^{\overline{a}}}}(y) = y + y^{q^{\overline{a}}}.$$

It is well known that the equation $\mathrm{Tr}_{\mathbb{F}_{q^{2\overline{a}}}/\mathbb{F}_{q^{\overline{a}}}}(y) = 0$ has exactly $q^{\overline{a}}$ solutions with $y \in \mathbb{F}_{q^{2\overline{a}}}$. Hence the number of solutions of (3.17) with $x \in \mathbb{F}_{q^m}$ is $q^{\overline{a}}$. This completes the proof. ■

The following lemma will be used later.

Lemma 3.1.3 *Let q be a power of a prime. Let h, m be positive integers. Let $W \subseteq \mathbb{F}_{q^m}$ be the subset defined as*

$$W = \{x \in \mathbb{F}_{q^m} : x + x^{q^{2h}} = 0\}.$$

Let Tr *denote the trace map from $\mathbb{F}_{q^m}$ onto $\mathbb{F}_q$. Let $\alpha \in \mathbb{F}_{q^m}$ and ψ be the $\mathbb{F}_q$-linear map defined as*

$$\begin{aligned} \psi : \mathbb{F}_{q^m} &\to \mathbb{F}_q \\ x &\mapsto \mathrm{Tr}\left(\left(\alpha^{q^{-h}} + \alpha^{q^h}\right) x\right). \end{aligned}$$

Then

$$W \subseteq \mathrm{Ker}\psi.$$

Proof. Let $x \in W$. We have

$$\begin{aligned} \psi(x) &= \mathrm{Tr}\left(\left(\alpha^{q^{-h}} + \alpha^{q^h}\right) x\right) \\ &= \mathrm{Tr}\left(\alpha^{q^{-h}} x\right) + \mathrm{Tr}\left(\alpha^{q^h} x\right) \qquad (3.18) \\ &= \mathrm{Tr}\left(\alpha^{q^h}\left(x + x^{q^{2h}}\right)\right). \end{aligned}$$

As $x \in W$, we have

$$x + x^{q^{2h}} = 0. \qquad (3.19)$$

Using (3.18) and (3.19) we obtain that

$$\psi(x) = 0.$$

This completes the proof. ■

3.2 THE MAXIMUM SUCCESS PROBABILITY OF THE IMPERSONATION ATTACK

In this section we consider the maximum success probability $\mathcal{P}_I$ of the impersonation attack on the authentication code with secrecy defined in (3.1).

We recall that $\mathcal{P}_I$ is given by

$$\begin{aligned} \mathcal{P}_I &= \max_{m=(m_1,m_2)} \frac{|\{k \in \mathcal{K} : \Pi(m_1 - k) + \Pi(k) = m_2\}|}{|\mathcal{K}|} \\ &= \max_{m=(m_1,m_2)} \frac{|\{k \in \mathcal{K} : \Pi(m_1 - k) + \Pi(k) = m_2\}|}{q^m}, \end{aligned} \tag{3.20}$$

where the maximum is over $\mathcal{M}$, that is the maximum is defined as m_1 runs through $\mathbb{F}_{q^m}$ and m_2 runs through $\mathbb{F}_q$.

Let $x \in \mathbb{F}_{q^m}$, $\alpha \in \mathbb{F}_{q^m}$ and $b \in \mathbb{F}_q$. Note that

$$\Pi(\alpha - x) + \Pi(x) = b \tag{3.21}$$

means that

$$\mathrm{Tr}\left((\alpha - x)^{q^h+1}\right) + \mathrm{Tr}\left(x^{q^h+1}\right) = b. \tag{3.22}$$

We have

$$\begin{aligned} (\alpha - x)^{q^h+1} &= (\alpha - x)^{q^h}(\alpha - x) \\ &= (\alpha^{q^h} - x^{q^h})(\alpha - x) \\ &= \alpha^{q^h+1} - \alpha^{q^h}x - \alpha x^{q^h} + x^{q^h+1}. \end{aligned} \tag{3.23}$$

We choose $\beta \in \mathbb{F}_{q^m}$ such that

$$\mathrm{Tr}(\beta) = b. \tag{3.24}$$

Note that

$$\mathrm{Tr}\left(\alpha x^{q^h}\right) = \mathrm{Tr}\left(\alpha^{q^{-h}} x\right). \tag{3.25}$$

Combining (3.22), (3.23), (3.24) and (3.25) we obtain that (3.22) holds if and only if

$$\mathrm{Tr}\left(2x^{q^h+1} - \left(\alpha^{q^{-h}} + \alpha^{q^h}\right)x + \alpha^{q^h+1} - \beta\right) = 0. \tag{3.26}$$

For $\gamma \in \mathbb{F}_{q^m}$, let $F_{\alpha,\gamma}$ be the algebraic function field

$$F_{\alpha,\gamma} = \mathbb{F}_{q^m}(x,y) \quad \text{with} \quad y^q - y = 2x^{q^h+1} - \left(\alpha^{q^{-h}} + \alpha^{q^h}\right)x + \gamma. \tag{3.27}$$

Note that the polynomial

$$T^q - T - \left(2x^{q^h+1} - \left(\alpha^{q^{-h}} + \alpha^{q^h}\right)x + \gamma\right) \in \mathbb{F}_{q^m}(x)[T]$$

is irreducible over the field $\mathbb{F}_{q^m}(x)$. Hence $[F_{\alpha,\gamma} : \mathbb{F}_{q^m}(x)] = q$.

Let $N(\alpha,\beta)$ denote the number of solutions of the equation (3.26) with $x \in \mathbb{F}_{q^m}$.

Let $N(F_{\alpha,\gamma})$ denote the number of rational places of $F_{\alpha,\gamma}$.

Using (3.26) and (3.27) we obtain that if

$$\gamma = \alpha^{q^h+1} - \beta, \tag{3.28}$$

then

$$N(F_{\alpha,\gamma}) = 1 + qN(\alpha,\beta). \tag{3.29}$$

It is also clear that α and β runs through $\mathbb{F}_{q^m}$ if and only if α and $\alpha^{q^h+1} - \beta$ runs through $\mathbb{F}_{q^m}$. Hence, by (3.28) and (3.29), we have that

$$\max_{\alpha,\gamma} N\left(F_{\alpha,\gamma}\right) = 1 + q \max_{\alpha,\beta} N(\alpha,\beta). \tag{3.30}$$

Here $\max_{\alpha,\gamma} N\left(F_{\alpha,\gamma}\right)$ is the maximum of $N\left(F_{\alpha,\gamma}\right)$ as α and γ runs through $\mathbb{F}_{q^m}$. Similarly $\max_{\alpha,\beta} N(\alpha,\beta)$ is the maximum of $N(\alpha,\beta)$ as α and β runs through $\mathbb{F}_{q^m}$.

Therefore the determination of $\mathcal{P}_I$ reduces to the determination of

$$\max_{\alpha,\gamma} N\left(F_{\alpha,\gamma}\right), \tag{3.31}$$

where the maximum is over $\alpha, \gamma \in \mathbb{F}_{q^m}$. We will determine (3.31) using the results of Chapter 2.

Let $S(T) = 2T^{q^h} \in \mathbb{F}_{q^m}[T]$ be the $\mathbb{F}_q$-linearized polynomial. Under the notation of Chapter 2, for the mapping Q_S we have

$$\begin{aligned} Q_S : \mathbb{F}_{q^m} : &\to \mathbb{F}_q \\ x &\mapsto \mathrm{Tr}(xS(x)) = \mathrm{Tr}\left(2x^{q^h+1}\right). \end{aligned}$$

The corresponding bilinear form B_s is given by

$$\begin{aligned} B_S : \mathbb{F}_{q^m} \times \mathbb{F}_{q^m} &\to \mathbb{F}_q \\ (x, y) &\mapsto \mathrm{Tr}(xS(y) + yS(x)). \end{aligned}$$

Using (2.3) in Chapter 2, for the radical W_S of the bilinear form B_S we have

$$\begin{aligned} W_S &= \{x \in \mathbb{F}_{q^m} : 2x + 2x^{q^{2h}} = 0\} \\ &= \{x \in \mathbb{F}_{q^m} : x + x^{q^{2h}} = 0\}. \end{aligned}$$

Let $\overline{h} = \gcd(2h, m)$ and $k = \dim_{\mathbb{F}_q} W_S$ be the $\mathbb{F}_q$-dimension of W_S.

If $\frac{m}{\overline{h}}$ is odd, then using Lemma 3.1.2 we have

$$W_S = \{0\} \quad \text{and} \quad k = 0. \tag{3.32}$$

If $\frac{m}{\overline{h}}$ is even, then using Lemma 3.1.2 we have

$$W_S = \{x \in \mathbb{F}_{q^m} : x + x^{q^{\overline{h}}} = 0\} \quad \text{and} \quad k = \overline{h}. \tag{3.33}$$

Let ψ be the $\mathbb{F}_q$-linear map

$$\begin{aligned} \psi : \mathbb{F}_{q^m} &\to \mathbb{F}_q \\ x &\mapsto \mathrm{Tr}\left(\left(\alpha^{q^{-h}} + \alpha^{q^h}\right) x\right). \end{aligned}$$

By Lemma 3.1.3 we have that

$$W_S \subseteq \mathrm{Ker}\psi. \tag{3.34}$$

The following simple lemma will be useful.

Lemma 3.2.1 *Let a, b be positive integers. Let $\overline{a} = \gcd(2a, b)$. If $\frac{b}{\overline{a}}$ is even, then $\overline{a}$ is even.*

Proof. Assume that $\frac{b}{\overline{a}}$ is even. Then b is even, $2 \mid b$ and $2 \mid (2a)$. This implies that $2 \mid \gcd(2a, b)$. Therefore $\overline{a} = \gcd(2a, b)$ is even. ■

Now we are ready to determine $\mathcal{P}_I$.

Theorem 3.2.2 *Let q be a power of an odd prime. Let $m \geq 2$ and $h \geq 1$ be integers. Let Π be the map*

$$\begin{aligned} \Pi : \mathbb{F}_{q^m} &\to \mathbb{F}_q \\ x &\mapsto \mathrm{Tr}\left(x^{q^h+1}\right). \end{aligned}$$

Let $(\mathcal{S}, \mathcal{K}, \mathcal{M}, \mathcal{E})$ be the authentication code with secrecy defined as

$$\begin{cases} \mathcal{S} = \mathbb{F}_{q^m}, \\ \mathcal{K} = \mathbb{F}_{q^m}, \\ \mathcal{M} = \mathbb{F}_{q^m} \times \mathbb{F}_q, \\ \mathcal{E} = \{E_k : k \in \mathcal{K}\}, \end{cases}$$

where for $k \in \mathcal{K}$, the authentication map E_k is defined as

$$\begin{aligned} E_k : \mathcal{S} &\to \mathcal{M} \\ s &\mapsto (s + k, \Pi(s) + \Pi(k)). \end{aligned}$$

Let $\mathcal{P}_I$ denote the maximum success probability of the impersonation attack on the authentication code with secrecy defined above. Let

$$\overline{h} = \gcd(2h, m).$$

If $\frac{m}{\overline{h}}$ is odd and m is odd, then

$$\mathcal{P}_I = \frac{1}{q} + \frac{1}{q^{\frac{m+1}{2}}}. \tag{3.35}$$

If $\frac{m}{\overline{h}}$ is odd and m is even, then

$$\mathcal{P}_I = \frac{1}{q} + \frac{1}{q^{\frac{m}{2}+1}} \quad or \quad \mathcal{P}_I = \frac{1}{q} + \frac{q-1}{q^{\frac{m}{2}+1}}. \tag{3.36}$$

If $\frac{m}{\overline{h}}$ is even, $\overline{h}$ is even, and m is even, then

$$\mathcal{P}_I = \frac{1}{q} + \frac{1}{q^{\frac{m-\bar{h}}{2}+1}} \quad or \quad \mathcal{P}_I = \frac{1}{q} + \frac{q-1}{q^{\frac{m-\bar{h}}{2}+1}}. \tag{3.37}$$

Proof. We use the notation introduced before Lemma 3.2.1 above. In particular we note that

$$W_S \subseteq \mathrm{Ker}\psi \tag{3.38}$$

in all cases.

First we consider the case that $\frac{m}{h}$ is odd and m is odd. For the dimension k of W_S we have

$$k = 0,$$

by (3.32). Then $m - k$ is odd. Using Theorem 2.3.1 of Chapter 2 we obtain that

$$N\left(F_{\alpha,\gamma}\right) = 1 + q^m + q^{\frac{m+1}{2}} \quad \text{or} \quad N\left(F_{\alpha,\gamma}\right) = 1 + q^m - q^{\frac{m+1}{2}}, \tag{3.39}$$

where $\alpha, \gamma \in \mathbb{F}_{q^m}$.

In order to decide which value in (3.39) occurs depending on α and γ, we need to consider whether the element

$$(-1)^{\frac{m-1}{2}} 2d(A - b) \in \mathbb{F}_q \tag{3.40}$$

is square or not in $\mathbb{F}_q$. Here d is a nonzero constant in $\mathbb{F}_q \setminus \{0\}$ depending on q, m and h. Moreover in (3.40) $A \in \mathbb{F}_q$ is a constant depending on q, m, h, and α. Finally in (3.40), the constant $b \in \mathbb{F}_q$ is defined as

$$b = \mathrm{Tr}(\gamma). \tag{3.41}$$

Using (3.41) we obtain that the value in (3.40) takes both square and nonsquare values in $\mathbb{F}_q$ as α and γ run through $\mathbb{F}_{q^m}$. Therefore both of the values in (3.39) occur as α and γ run through $\mathbb{F}_{q^m}$. Therefore

$$\max_{\alpha,\gamma} N\left(F_{\alpha,\gamma}\right) = 1 + q^m + q^{\frac{m+1}{2}}, \tag{3.42}$$

where the maximum is over $\alpha, \gamma \in \mathbb{F}_{q^m}$. Recall that for $\alpha, \beta \in \mathbb{F}_{q^m}$, $N(\alpha, \beta)$ denotes the number of solutions of the equation in (3.26) with $x \in \mathbb{F}_{q^m}$. Using (3.30) and (3.42) we obtain that

$$\begin{aligned} \max_{\alpha,\beta} N(\alpha,\beta) &= \frac{\max_{\alpha,\gamma} N\left(F_{\alpha,\gamma}\right) - 1}{q} \\ &= q^{m-1} + q^{\frac{m-1}{2}}. \end{aligned} \tag{3.43}$$

For $\max_{\alpha,\beta} N(\alpha, \beta)$ in (3.43), the maximum is over $\alpha, \beta \in \mathbb{F}_{q^m}$.

Using (3.20) and (3.43) we obtain that

$$\begin{aligned} \mathcal{P}_I &= \frac{q^{m-1} + q^{\frac{m-1}{2}}}{q^m} \\ &= \frac{1}{q} + \frac{1}{q^{\frac{m+1}{2}}}, \end{aligned}$$

which completes the proof of (3.35).

Next we consider the case that $\frac{m}{h}$ is odd and m is even. Again

$$k = \dim W_S = 0$$

by (3.32). Then $m - k$ is even. Using Theorem 2.3.1 of Chapter 2, we obtain that

$$N\left(F_{\alpha,\gamma}\right) = 1 + q^m - q^{\frac{m}{2}} \quad \text{or} \quad N\left(F_{\alpha,\gamma}\right) = 1 + q^m + q^{\frac{m}{2}} \tag{3.44}$$

if $A \neq b$, and

$$N\left(F_{\alpha,\gamma}\right) = 1 + q^m + (q-1)q^{\frac{m}{2}} \quad \text{or} \quad N\left(F_{\alpha,\gamma}\right) = 1 + q^m - (q-1)q^{\frac{m}{2}} \tag{3.45}$$

if $A = b$. Here, as in the case that $\frac{m}{h}$ is odd and m is odd above, $A \in \mathbb{F}_q$ is a constant depending on q, m, h, and α. Moreover $b = \mathrm{Tr}(\gamma)$. Hence both of the cases

$$A = b \quad \text{and} \quad A \neq b$$

occur as α and γ run through $\mathbb{F}_{q^m}$. Also the values in (3.44) and (3.45) depend on whether

$$(-1)^{\frac{m}{2}} d \quad \text{is a square in } \mathbb{F}_q \text{ or not,} \tag{3.46}$$

where $d \in \mathbb{F}_q \setminus \{0\}$ is a nonzero constant depending on q, m and h.

If the value in (3.46) is a square in $\mathbb{F}_q$, then using (3.44) and (3.45) we obtain that

$$\begin{aligned} \max_{\alpha,\gamma} N\left(F_{\alpha,\gamma}\right) &= \max\left\{1 + q^m - q^{\frac{m}{2}}, 1 + q^m + (q-1)q^{\frac{m}{2}}\right\} \\ &= 1 + q^m + (q-1)q^{\frac{m}{2}}. \end{aligned} \tag{3.47}$$

If the value in (3.46) is not a square in $\mathbb{F}_q$, then using (3.44) and (3.45) we obtain that

$$\begin{aligned} \max_{\alpha,\gamma} N\left(F_{\alpha,\gamma}\right) &= \max\left\{1 + q^m + q^{\frac{m}{2}}, 1 + q^m - (q-1)q^{\frac{m}{2}}\right\} \\ &= 1 + q^m + q^{\frac{m}{2}}. \end{aligned} \tag{3.48}$$

Combining (3.47), (3.48) and using (3.30) we obtain that

$$\max_{\alpha,\beta} N(\alpha,\beta) = \frac{\max_{\alpha,\gamma} N\left(F_{\alpha,\gamma}\right) - 1}{q}$$

and hence

$$\max_{\alpha,\beta} N(\alpha,\beta) = q^{m-1} + (q-1)q^{\frac{m}{2}-1} \tag{3.49}$$

or

$$\max_{\alpha,\beta} N(\alpha,\beta) = q^{m-1} + q^{\frac{m}{2}-1}. \tag{3.50}$$

Using (3.20), (3.49) and (3.50) we get that

$$\begin{aligned} \mathcal{P}_{\mathcal{I}} &= \frac{q^{m-1} + (q-1)q^{\frac{m}{2}-1}}{q^m} \\ &= \frac{1}{q} + \frac{q-1}{q^{\frac{m}{2}+1}} \end{aligned}$$

or

$$\begin{aligned} \mathcal{P}_{\mathcal{I}} &= \frac{q^{m-1} + q^{\frac{m}{2}-1}}{q^m} \\ &= \frac{1}{q} + \frac{1}{q^{\frac{m}{2}+1}}, \end{aligned}$$

which completes the proof of (3.36).

Finally we consider the case that $\frac{m}{\overline{h}}$ is even, $\overline{h}$ is even and m is even. For the dimension k of W_S we have

$$k = \overline{h}$$

by (3.33). Then $m-k$ is even. Using Theorem 2.3.1 of Chapter 2 we obtain that

$$N\left(F_{\alpha,\gamma}\right) = 1 + q^m - q^{\frac{m+\bar{h}}{2}} \quad \text{or} \quad N\left(F_{\alpha,\gamma}\right) = 1 + q^m + q^{\frac{m+\bar{h}}{2}} \tag{3.51}$$

if $A \neq b$ and

$$N\left(F_{\alpha,\gamma}\right) = 1 + q^m + (q-1)q^{\frac{m+\bar{h}}{2}} \quad \text{or} \quad N\left(F_{\alpha,\gamma}\right) = 1 + q^m - (q-1)q^{\frac{m+\bar{h}}{2}} \tag{3.52}$$

if $A = b$. Here, as in the case of $\frac{m}{\overline{h}}$ is odd and m is even above, the occurrence of values in (3.51) and (3.52) depend on the constants A, b and d. Again $A \in \mathbb{F}_q$ is a constant depending on q, m, h and α. Moreover $b = \mathrm{Tr}(\gamma)$, and $d \in \mathbb{F}_q \setminus \{0\}$ is a nonzero constant depending on q, m, and h.

If $(-1)^{\frac{m-\bar{h}}{2}} d$ is a square in $\mathbb{F}_q$, then both of the values

$$N\left(F_{\alpha,\gamma}\right) = 1 + q^m - q^{\frac{m+\bar{h}}{2}} \quad \text{and} \quad N\left(F_{\alpha,\gamma}\right) = 1 + q^m + (q-1)q^{\frac{m+\bar{h}}{2}} \tag{3.53}$$

occur as α and γ run through $\mathbb{F}_{q^m}$.

If $(-1)^{\frac{m-\overline{h}}{2}}d$ is not a square in $\mathbb{F}_q$, then both of the values

$$N\left(F_{\alpha,\gamma}\right) = 1 + q^m + q^{\frac{m+\overline{h}}{2}} \quad \text{and} \quad N\left(F_{\alpha,\gamma}\right) = 1 + q^m - (q-1)q^{\frac{m+\overline{h}}{2}} \tag{3.54}$$

occur as α and γ run through $\mathbb{F}_{q^m}$.

Therefore, by (3.53) and (3.54), we have

$$\begin{aligned} \max_{\alpha,\gamma} N\left(F_{\alpha,\gamma}\right) &= \max\left\{1 + q^m - q^{\frac{m+\overline{h}}{2}}, 1 + q^m + (q-1)q^{\frac{m+\overline{h}}{2}}\right\} \\ &= 1 + q^m + (q-1)q^{\frac{m+\overline{h}}{2}} \end{aligned} \tag{3.55}$$

or

$$\begin{aligned} \max_{\alpha,\gamma} N\left(F_{\alpha,\gamma}\right) &= \max\left\{1 + q^m + q^{\frac{m+\overline{h}}{2}}, 1 + q^m - (q-1)q^{\frac{m+\overline{h}}{2}}\right\} \\ &= 1 + q^m + q^{\frac{m+\overline{h}}{2}}. \end{aligned} \tag{3.56}$$

Using (3.30), (3.55) and (3.56) we get that

$$\max_{\alpha,\beta} N(\alpha,\beta) = q^{m-1} + (q-1)q^{\frac{m+\overline{h}}{2}-1} \tag{3.57}$$

or

$$\max_{\alpha,\beta} N(\alpha,\beta) = q^{m-1} + q^{\frac{m+\overline{h}}{2}-1}. \tag{3.58}$$

Hence from (3.20), (3.57) and (3.58) we obtain that

$$\begin{aligned} \mathcal{P}_I &= \frac{q^{m-1} + (q-1)q^{\frac{m+\overline{h}}{2}-1}}{q^m} \\ &= \frac{1}{q} + \frac{q-1}{q^{\frac{m-\overline{h}}{2}+1}} \end{aligned}$$

or

$$\begin{aligned} \mathcal{P}_I &= \frac{q^{m-1} + q^{\frac{m+\overline{h}}{2}-1}}{q^m} \\ &= \frac{1}{q} + \frac{1}{q^{\frac{m-\overline{h}}{2}+1}}, \end{aligned}$$

which completes the proof of (3.37). ■

Remark 3.2.3 *Using Lemma 3.2.1 we obtain that there is no case in Theorem 3.2.2 with $\frac{m}{\overline{h}}$ is even and $\overline{h}$ is odd. Moreover if $\frac{m}{\overline{h}}$ is even, then m is even and there is no case that $\frac{m}{\overline{h}}$ is even, $\overline{h}$ is even and m is odd. Therefore Theorem 3.2.2 considers $\mathcal{P}_I$ in all possible cases. Also all three cases considered in Theorem 3.2.2 occur. For example:*

i) If $m = 9$ *and* $h = 3$*, then* $\overline{h} = \gcd(2h, m) = 3$ *and we have*

$$\tfrac{m}{\overline{h}} = 3 \text{ is odd}, \quad \text{and} \quad m = 9 \text{ is odd}.$$

ii) If $m = 6$ *and* $h = 2$*, then* $\overline{h} = \gcd(2h, m) = 2$ *and we have*

$$\tfrac{m}{\overline{h}} = 3 \text{ is odd}, \quad \text{and} \quad m = 6 \text{ is even}.$$

iii) If $m = 8$ *and* $h = 2$*, then* $\overline{h} = \gcd(2h, m) = 4$ *and we have*

$$\tfrac{m}{\overline{h}} = 2 \text{ is even}, \quad \overline{h} = 4 \text{ is even} \quad \text{and} \quad m = 8 \text{ is even}.$$

3.3 THE MAXIMUM SUCCESS PROBABILITY OF THE SUBSTITUTION ATTACK: CASE $\frac{m}{\gcd(2h,m)}$ IS EVEN

In this section we begin to consider the maximum success probability $\mathcal{P}_{\mathcal{S}}$ of the substitution attack on the authentication code with secrecy defined in (3.1) and we determine it when $\frac{m}{\gcd(2h,m)}$ is even.

We recall that $\mathcal{P}_{\mathcal{S}}$ is given by

$$P_s = \max_{\boldsymbol{m},\boldsymbol{d}} \frac{|\{s \in S : \Pi(s) + \Pi(m_1 - s) = m_2, \quad \Pi(s + d_1) - \Pi(s) = d_2\}|}{|\{s \in S : \Pi(s) + \Pi(m_1 - s) = m_2\}|}, \tag{3.59}$$

where the maximum is over $\boldsymbol{m} = (m_1, m_2) \in \mathcal{M} = \mathbb{F}_{q^m} \times \mathbb{F}_q$ and $\boldsymbol{d} = (d_1, d_2) \in \mathcal{M}$ with $d_1 \neq 0$.

Let $\alpha_1 \in \mathbb{F}_{q^m}$, $b_1 \in \mathbb{F}_q$, $\alpha_2 \in \mathbb{F}_{q^m} \setminus \{0\}$ and $b_2 \in \mathbb{F}_q$.

For the denominator of the right hand side of the equation in (3.59) we consider the cardinality of the set

$$\{x \in \mathbb{F}_{q^m} : \Pi(x) + \Pi(\alpha_1 - x) = b_1\}. \tag{3.60}$$

For the numerator of the right hand side of the equation in (3.59) we consider the cardinality of the set

$$\{x \in \mathbb{F}_{q^m} : \Pi(x) + \Pi(\alpha_1 - x) = b_1, \quad \Pi(x + \alpha_2) - \Pi(x) = b_2\}. \tag{3.61}$$

We choose $\beta_1 \in \mathbb{F}_{q^m}$ such that $\mathrm{Tr}(\beta_1) = b_1$. Let $N_1(\alpha_1, \beta_1)$ denote the number of solutions of the equation

$$\mathrm{Tr}\left(2x^{q^h+1} - \left(\alpha_1^{q^{-h}} + \alpha_1^{q^h}\right)x + \alpha_1^{q^h+1} - \beta_1\right) = 0 \tag{3.62}$$

with $x \in \mathbb{F}_{q^m}$. Using (3.21), (3.22), (3.23) , (3.24), and (3.25), as in determination of the maximum success probability $\mathcal{P}_I$ of the impersonation attack, we obtain that $N_1(\alpha_1, \beta_1)$ is equal to the cardinality of the set in (3.60).

For $x \in \mathbb{F}_{q^m}$, note that

$$\begin{aligned}
(x+\alpha_2)^{q^h+1} - x^{q^h+1} &= \left(x^{q^h} + \alpha_2^{q^h}\right)(x+\alpha_2) - x^{q^h+1} \\
&= \left(x^{q^h+1} + x^{q^h}\alpha_2 + x\alpha_2^{q^h} + \alpha_2^{q^h+1}\right) - x^{q^h+1} \\
&= x^{q^h}\alpha_2 + x\alpha_2^{q^h} + \alpha_2^{q^h+1}.
\end{aligned}$$

Then we have

$$\begin{aligned}
\Pi(x+\alpha_2) - \Pi(x) &= \mathrm{Tr}\left((x+\alpha_2)^{q^h+1}\right) - \mathrm{Tr}\left(x^{q^h+1}\right) \\
&= \mathrm{Tr}\left(x^{q^h}\alpha_2 + x\alpha_2^{q^h} + \alpha_2^{q^h+1}\right) \\
&= \mathrm{Tr}\left(\left(\alpha_2^{q^{-h}} + \alpha_2^{q^h}\right)x + \alpha_2^{q^h+1}\right).
\end{aligned} \tag{3.63}$$

We choose $\beta_2 \in \mathbb{F}_{q^m}$ such that $\mathrm{Tr}(\beta_2) = b_2$. Using (3.63) we observe that the number of solutions of the system of equations

$$\begin{cases}
\Pi(x) + \Pi(\alpha_1 - x) &= b_1, \\
\Pi(x+\alpha_2) - \Pi(x) &= b_2,
\end{cases}$$

with $x \in \mathbb{F}_{q^m}$ is the same as the number of solutions of the system of equations

$$\begin{cases}
\mathrm{Tr}\left(2x^{q^h+1} - \left(\alpha_1^{q^{-h}} + \alpha_1^{q^h}\right)x + \alpha_1^{q^h+1} - \beta_1\right) &= 0, \\
\mathrm{Tr}\left(\left(\alpha_2^{q^{-h}} + \alpha_2^{q^h}\right)x + \alpha_2^{q^h+1} - \beta_2\right) &= 0,
\end{cases} \tag{3.64}$$

with $x \in \mathbb{F}_{q^m}$. Let $N_2(\alpha_1, \beta_1; \alpha_2, \beta_2)$ denote the number of solutions of the system (3.64) with $x \in \mathbb{F}_{q^m}$. Using (3.59) we observe that

$$\mathcal{P}_S = \max_{\alpha_1, \beta_1, \alpha_2, \beta_2} \frac{N_2(\alpha_1, \beta_1; \alpha_2, \beta_2)}{N_1(\alpha_1, \beta_1)}, \tag{3.65}$$

where the maximum is over $\alpha_1, \beta_1, \alpha_2, \beta_2 \in \mathbb{F}_{q^m}$ with $\alpha_2 \neq 0$.

We consider whether there exists $\alpha_2 \in \mathbb{F}_{q^m} \setminus \{0\}$ such that

$$\alpha_2^{q^{-h}} + \alpha_2^{q^h} = 0, \tag{3.66}$$

which is equivalent to

$$\alpha_2 + \alpha_2^{q^{2h}} = 0.$$

Now we use Lemma 3.1.2. Let $\overline{h} = \gcd(2h, m)$. If $\frac{m}{\overline{h}}$ is odd, then there is no $\alpha_2 \in \mathbb{F}_{q^m} \setminus \{0\}$ such that (3.66) holds. If $\frac{m}{\overline{h}}$ is even, then the number of $\alpha_2 \in \mathbb{F}_{q^m} \setminus \{0\}$ such that (3.66) holds is $q^{\overline{h}} - 1$.

First we deal with the case that $\frac{m}{\overline{h}}$ is even and we choose $\alpha_2 \in \mathbb{F}_{q^m} \setminus \{0\}$ such that

$$\alpha_2^{q^{-h}} + \alpha_2^{q^h} = 0.$$

Moreover we choose $\beta_2 \in \mathbb{F}_{q^m}$ such that

$$\mathrm{Tr}\left(\alpha_2^{q^h+1} - \beta_2\right) = 0.$$

The number of such β_2 is exactly q^{m-1}. Then the system (3.64) of equations becomes the system of equations given by

$$\begin{cases} \mathrm{Tr}\left(2x^{q^h+1} - \left(\alpha_1^{q^{-h}} + \alpha_1^{q^h}\right)x + \alpha_1^{q^h+1} - \beta_1\right) &= 0, \\ \\ \mathrm{Tr}\,(0 \cdot x) &= 0. \end{cases} \tag{3.67}$$

As the second equation in system (3.67) is trivially satisfied, the system in (3.67) is equivalent to the equation in (3.62) for these choices of $\alpha_2 \in \mathbb{F}_{q^m} \setminus \{0\}$ and $\beta_2 \in \mathbb{F}_{q^m}$. Therefore for any $\alpha_1, \beta_1 \in \mathbb{F}_{q^m}$ and for those choices of $\alpha_2 \in \mathbb{F}_{q^m} \setminus \{0\}$ and $\beta_2 \in \mathbb{F}_{q^m}$ we have

$$N_1(\alpha_1, \beta_1) = N_2(\alpha_1, \beta_1; \alpha_2, \beta_2). \tag{3.68}$$

Moreover we observe that the system in (3.64) includes the equation in (3.62) as its first equation. Therefore for any choice of $\alpha_1, \beta_1 \in \mathbb{F}_{q^m}$ and for any choice of $\alpha_2 \in \mathbb{F}_{q^m} \setminus \{0\}$ and $\beta_2 \in \mathbb{F}_{q^m}$ we have

$$N_1(\alpha_1, \beta_1) \geq N_2(\alpha_1, \beta_1; \alpha_2, \beta_2). \tag{3.69}$$

Therefore using (3.65), (3.68) and (3.69) we obtain that

$$\mathcal{P}_{\mathcal{S}} = 1,$$

whenever $\frac{m}{\overline{h}}$ is even.

We have proved the following proposition.

Proposition 3.3.1 *Let q be a power of an odd prime. Let $m \geq 2$ and $h \geq 1$ be integers. Let Π be the map*

$$\begin{aligned} \Pi : \mathbb{F}_{q^m} &\rightarrow \mathbb{F}_q \\ x &\mapsto \mathrm{Tr}\left(x^{q^h+1}\right). \end{aligned}$$

Let $(\mathcal{S}, \mathcal{K}, \mathcal{M}, \mathcal{E})$ be the authentication code with secrecy defined as

$$\begin{cases} \mathcal{S} = \mathbb{F}_{q^m}, \\ \mathcal{K} = \mathbb{F}_{q^m}, \\ \mathcal{M} = \mathbb{F}_{q^m} \times \mathbb{F}_q, \\ \mathcal{E} = \{E_k : k \in \mathcal{K}\}, \end{cases}$$

where for $k \in \mathcal{K}$, the authentication map E_k is defined as

$$\begin{aligned} E_k : \mathcal{S} &\rightarrow \mathcal{M} \\ s &\mapsto (s + k, \Pi(s) + \Pi(k)). \end{aligned}$$

Let $\mathcal{P}_{\mathcal{S}}$ denote the maximum success probability of the substitution attack on the authentication code with secrecy defined above. Let

$$\overline{h} = \gcd(2h, m).$$

If $\frac{m}{\overline{h}}$ is even, then

$$\mathcal{P}_{\mathcal{S}} = 1.$$

3.4 THE MAXIMUM SUCCESS PROBABILITY OF THE SUBSTITUTION ATTACK: CASE $\frac{m}{\gcd(2h,m)}$ IS ODD AND m IS EVEN

The study of the maximum success probability $\mathcal{P}_{\mathcal{S}}$ of the impersonation attack on the authentication code with secrecy defined in (3.1) is more interesting when $\frac{m}{\gcd(2h,m)}$ is odd.

In this section we begin to study $\mathcal{P}_{\mathcal{S}}$ when $\frac{m}{\gcd(2h,m)}$ is odd. We obtain some useful results and we consider the subcase that $\frac{m}{\gcd(2h,m)}$ is odd and m is even. The remaining subcase that $\frac{m}{\gcd(2h,m)}$ is odd and m is odd will be considered in the next section.

Let φ be the map

$$\begin{array}{rcl} \varphi : \mathbb{F}_{q^m} & \to & \mathbb{F}_{q^m} \\ \alpha_2 & \mapsto & \alpha_2^{q^{-h}} + \alpha_2^{q^h}. \end{array} \tag{3.70}$$

Using Lemma 3.1.2 we obtain that there is no $\alpha_2 \in \mathbb{F}_{q^m} \setminus \{0\}$ with

$$\alpha_2^{q^{-h}} + \alpha_2^{q^h} = 0,$$

and hence the $\mathbb{F}_q$-linear map φ in (3.70) gives an $\mathbb{F}_q$-linear isomorphism on $\mathbb{F}_{q^m}$, under our assumption that $\frac{m}{h}$ is odd.

For $\alpha_1, \beta_1 \in \mathbb{F}_{q^m}$, $\alpha_3 \in \mathbb{F}_{q^m} \setminus \{0\}$ and $\beta_3 \in \mathbb{F}_{q^m}$, let $N_3(\alpha_1, \beta_1; \alpha_3, \beta_3)$ denote the number of solutions of the system

$$\begin{cases} \operatorname{Tr}\left(2x^{q^h+1} - \left(\alpha_1^{q^{-h}} + \alpha_1^{q^h}\right)x + \alpha_1^{q^h+1} - \beta_1\right) = 0, \\ \\ \operatorname{Tr}\left(\alpha_3 x + \beta_3\right) = 0, \end{cases} \tag{3.71}$$

with $x \in \mathbb{F}_{q^m}$.

We note that

$$N_2(\alpha_1, \beta_1; \alpha_2, \beta_2) = N_3(\alpha_1, \beta_1; \alpha_3, \beta_3) \tag{3.72}$$

if

$$\alpha_3 = \alpha_2^{q^{-h}} + \alpha_2^{q^h} \quad \text{and} \quad \beta_3 = \alpha_2^{q^h+1} - \beta_2. \tag{3.73}$$

For $\alpha_1, \gamma_1, \alpha_3, \gamma_3 \in \mathbb{F}_{q^m}$ with $\alpha_3 \neq 0$, let $F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}$ denote the algebraic function field

$$F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3} = \mathbb{F}_{q^m}(x, y_1, y_2) \quad \text{with}$$

$$\begin{cases} y_1^q - y_1 = 2x^{q^h+1} - \left(\alpha_1^{q^{-h}} + \alpha_1^{q^h}\right)x + \gamma_1, \\ \\ y_2^q - y_2 = \alpha_3 x + \gamma_3. \end{cases} \tag{3.74}$$

Note that the polynomial

$$T^q - T - \left(2x^{q^h+1} - \left(\alpha_1^{q^{-h}} + \alpha_1^{q^h}\right) + \gamma_1\right)x \in \mathbb{F}_{q^m}(x)[T]$$

is irreducible over the field $\mathbb{F}_{q^m}(x)$. Similarly the polynomial

$$T^q - T - (\alpha_3 x + \gamma_3) \in \mathbb{F}_{q^m}(x, y_1)$$

is irreducible over the field $\mathbb{F}_{q^m}(x, y_1)$. Then we have that

$$\left[\mathbb{F}_{q^m}(x, y_1) : \mathbb{F}_{q^m}(x)\right] = q, \quad \left[\mathbb{F}_{q^m}(x, y_1, y_2) : \mathbb{F}_{q^m}(x, y_1)\right] = q,$$

and hence

$$\left[F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3} : \mathbb{F}_{q^m}(x)\right] = q^2.$$

Let $N\left(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}\right)$ denote the number of rational places of the algebraic function field $F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}$.

Using (3.72), (3.73) and (3.74) we observe that

$$N\left(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}\right) = 1 + q^2 N_2(\alpha_1, \beta_1; \alpha_2, \beta_2) \tag{3.75}$$

provided that we have

$$\gamma_1 = \alpha_1^{q^h+1} - \beta_1, \quad \alpha_3 = \alpha_2^{q^{-h}} + \alpha_2^{q^h}, \quad \text{and} \quad \gamma_3 = \alpha_2^{q^h+1} - \beta_2. \tag{3.76}$$

For a choice of $\alpha_1, \gamma_1, \alpha_3, \gamma_3 \in \mathbb{F}_{q^m}$ with $\alpha_3 \neq 0$ for defining $F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}$, using the same α_1 and γ_1, let E_{α_1,γ_1} be the algebraic function field

$$E_{\alpha_1,\gamma_1} = \mathbb{F}_{q^m}(x, y) \quad \text{with} \quad y^q - y = 2x^{q^h+1} - \left(\alpha_1^{q^{-h}} + \alpha_1^{q^h}\right)x + \gamma_1.$$

Note that

$$\left[E_{\alpha_1,\gamma_1} : \mathbb{F}_{q^m}(x)\right] = q.$$

Recall that for $\alpha_1, \beta_1 \in \mathbb{F}_{q^m}$, $N_1(\alpha_1, \beta_1)$ denotes the number of solutions of the equation

$$\mathrm{Tr}\left(2x^{q^h+1} - \left(\alpha_1^{q^{-h}} + \alpha_1^{q^h}\right)x + \alpha_1^{q^h+1} - \beta_1\right) = 0$$

with $x \in \mathbb{F}_{q^m}$. Let $N\left(E_{\alpha_1,\gamma_1}\right)$ denote the number of rational places of the algebraic function field E_{α_1,γ_1}. Therefore we have

$$N\left(E_{\alpha_1,\gamma_1}\right) = 1 + qN_1(\alpha_1, \beta_1). \tag{3.77}$$

provided that we have

$$\gamma_1 = \alpha_1^{q^h+1} - \beta_1. \tag{3.78}$$

Using (3.65), (3.75), (3.76), (3.77) and (3.78), for the maximum success probability $\mathcal{P}_{\mathcal{S}}$ of the substitution attack on the codes defined in (3.1) we obtain that

$$\mathcal{P}_{\mathcal{S}} = \max_{\alpha_1,\gamma_1,\alpha_3,\gamma_3} \frac{\left(\frac{N\left(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}\right)-1}{q^2}\right)}{\left(\frac{N\left(E_{\alpha_1,\gamma_1}\right)-1}{q}\right)}, \tag{3.79}$$

where the maximum is over $\alpha_1, \gamma_1, \alpha_3, \gamma_3 \in \mathbb{F}_{q^m}$ with $\alpha_3 \neq 0$.

Our arguments above related to the maximum success probability $\mathcal{P}_{\mathcal{I}}$ of the impersonation attack give sufficient information for determining $N(E_{\alpha_1,\gamma_1})$ in (3.79). However we need further information for determining $N(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3})$ in (3.79). We develop such results below.

Let $\alpha_1, \gamma_1, \alpha_3, \gamma_3 \in \mathbb{F}_{q^m}$ with $\alpha_3 \neq 0$. We derive an equivalent definition of the algebraic function field $F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}$ instead of the one in (3.74). Using (3.74), we have

$$x = \frac{y_2^q}{\alpha_3} - \frac{y_2}{\alpha_3} - \frac{\gamma_3}{\alpha_3}, \tag{3.80}$$

and

$$y_1^q - y_1 = 2\left(\frac{y_2^q}{\alpha_3} - \frac{y_2}{\alpha_3} - \frac{\gamma_3}{\alpha_3}\right)^{q^h+1} - \left(\alpha_1^{q^{-h}} + \alpha_1^{q^h}\right)x + \gamma_1. \tag{3.81}$$

Note that

$$\begin{aligned}
\left(\frac{y_2^q}{\alpha_3} - \frac{y_2}{\alpha_3} - \frac{\gamma_3}{\alpha_3}\right)^{q^h+1} &= \left(\frac{y_2^q}{\alpha_3} - \frac{y_2}{\alpha_3} - \frac{\gamma_3}{\alpha_3}\right)^{q^h}\left(\frac{y_2^q}{\alpha_3} - \frac{y_2}{\alpha_3} - \frac{\gamma_3}{\alpha_3}\right) \\
&= \left(\left(\frac{y_2^q}{\alpha_3} - \frac{y_2}{\alpha_3}\right)^{q^h} - \left(\frac{\gamma_3}{\alpha_3}\right)^{q^h}\right)\left(\left(\frac{y_2^q}{\alpha_3} - \frac{y_2}{\alpha_3}\right) - \frac{\gamma_3}{\alpha_3}\right) \\
&= \left(\frac{y_2^q}{\alpha_3} - \frac{y_2}{\alpha_3}\right)^{q^h}\left(\frac{y_2^q}{\alpha_3} - \frac{y_2}{\alpha_3}\right) \\
&\quad - \frac{\gamma_3}{\alpha_3}\left(\frac{y_2^q}{\alpha_3} - \frac{y_2}{\alpha_3}\right)^{q^h} - \left(\frac{\gamma_3}{\alpha_3}\right)^{q^h}\left(\frac{y_2^q}{\alpha_3} - \frac{y_2}{\alpha_3}\right) \\
&\quad + \left(\frac{\gamma_3}{\alpha_3}\right)^{q^h+1}.
\end{aligned} \tag{3.82}$$

Let L_1 be the $\mathbb{F}_q$-linear map defined as

$$\begin{aligned} L_1 : \mathbb{F}_{q^m} &\rightarrow \mathbb{F}_{q^m} \\ y &\mapsto -\left(\alpha_1^{q^{-h}} + \alpha_1^{q^h}\right) y. \end{aligned} \tag{3.83}$$

Let L_2 be the $\mathbb{F}_q$-linear map defined as

$$\begin{aligned} L_2 : \mathbb{F}_{q^m} &\rightarrow \mathbb{F}_{q^m} \\ y &\mapsto -2\left(\left(\tfrac{\gamma_3}{\alpha_3}\right)^{q^{-h}} + \left(\tfrac{\gamma_3}{\alpha_3}\right)^{q^h}\right) y. \end{aligned} \tag{3.84}$$

Using (3.83) and (3.84) we define the $\mathbb{F}_q$-linear map L as

$$\begin{aligned} L : \mathbb{F}_{q^m} &\rightarrow \mathbb{F}_{q^m} \\ y &\mapsto L_1(y) + L_2(y) \end{aligned} \tag{3.85}$$

Let $\alpha_1, \gamma_1, \alpha_3, \gamma_3 \in \mathbb{F}_{q^m}$ with $\alpha_3 \neq 0$. Using (3.81), (3.82), and (3.85) we obtain the following equivalent representation of the algebraic function field $F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}$ consisting of one affine equation instead of the two affine equations in (3.74):

$$\begin{aligned} &F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3} = \mathbb{F}_{q^m}(y_2, y_1) \quad \text{with} \\ &y_1^q - y_1 = 2\left(\frac{y_2^q}{\alpha_3} - \frac{y_2}{\alpha_3}\right)^{q^h+1} + L\left(\frac{y_2^q}{\alpha_3} - \frac{y_2}{\alpha_3}\right) + \left(\gamma_1 + 2\left(\frac{\gamma_3}{\alpha_3}\right)^{q^h+1}\right). \end{aligned} \tag{3.86}$$

Note that the polynomial

$$T^q - T - \left(2\left(\frac{y_2^q}{\alpha_3} - \frac{y_2}{\alpha_3}\right)^{q^h+1} + L\left(\frac{y_2^q}{\alpha_3} - \frac{y_2}{\alpha_3}\right) + \left(\gamma_1 + 2\left(\frac{\gamma_3}{\alpha_3}\right)^{q^h+1}\right)\right) \in \mathbb{F}_{q^m}(y_2)[T]$$

is irreducible over the field $\mathbb{F}_{q^m}(y_2)$ and hence

$$\left[F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3} : \mathbb{F}_{q^m}(y_2)\right] = q.$$

It is clear from (3.80) that $x \in \mathbb{F}_{q^m}(y_2) \subseteq F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}$.

We will use the representation of $F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}$ in (3.86) and the results of Chapter 2 in order to consider $N\left(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}\right)$ and the maximum success probability $\mathcal{P}_{\mathcal{S}}$ of the substitution attack on the authentication code with secrecy defined above.

Using the notation of Chapter 2, let $S(X) \in \mathbb{F}_{q^m}[X]$ be the $\mathbb{F}_q$-linearized polynomial

$$S(X) = 2X^{q^h} \in \mathbb{F}_{q^m}[X]$$

Let B_S be the symmetric bilinear form

$$\begin{aligned} B_S : \mathbb{F}_{q^m} \times \mathbb{F}_{q^m} &\to \mathbb{F}_q \\ (x, y) &\mapsto \mathrm{Tr}\left(xS(y) + yS(x)\right) \end{aligned}$$

on the $\mathbb{F}_q$-linear space $\mathbb{F}_{q^m}$.

Let Q_S be the map

$$\begin{aligned} Q_S : \mathbb{F}_{q^m} &\to \mathbb{F}_q \\ x &\mapsto \frac{1}{2} B_S(x, x). \end{aligned}$$

Recall that, conversely, the symmetric bilinear form B_S is obtained from the map Q_S via

$$B_S(x, y) = Q_S(x + y) - Q_S(x) - Q_S(y). \tag{3.87}$$

We also observe that

$$Q_S(x) = \mathrm{Tr}\left(2x^{q^h+1}\right)$$

for all $x \in \mathbb{F}_{q^m}$.

Let Q_R be the map

$$\begin{aligned} Q_R : \mathbb{F}_{q^m} &\to \mathbb{F}_q \\ x &\mapsto Q_S\left(\frac{x^q}{\alpha_3} - \frac{x}{\alpha_3}\right). \end{aligned} \tag{3.88}$$

As in (3.87) we define the symmetric bilinear form B_R on the $\mathbb{F}_q$-linear space $\mathbb{F}_{q^m}$ using the map Q_R defined in (3.88) as

$$\begin{aligned} B_R : \mathbb{F}_{q^m} \times \mathbb{F}_{q^m} &\to \mathbb{F}_q \\ (x, y) &\mapsto Q_R(x + y) - Q_R(x) - Q_R(y). \end{aligned} \tag{3.89}$$

The following lemma will be useful.

Lemma 3.4.1 *Under the notation as above we have*

$$B_R(x,y) = B_S\left(\frac{x^q}{\alpha_3} - \frac{x}{\alpha_3}, \frac{y^q}{\alpha_3} - \frac{y}{\alpha_3}\right)$$

for all $x, y \in \mathbb{F}_{q^m}$.

Proof. Let $x, y \in \mathbb{F}_{q^m}$. Using (3.89) we have

$$B_R(x,y) = Q_R(x,y) - Q_R(x) - Q_R(y).$$

Then by (3.88) we get

$$\begin{aligned} &B_R(x,y) \\ &= Q_S\left(\frac{(x+y)^q}{\alpha_3} - \frac{x+y}{\alpha_3}\right) - Q_S\left(\frac{x^q}{\alpha_3} - \frac{x}{\alpha_3}\right) - Q_S\left(\frac{y^q}{\alpha_3} - \frac{y}{\alpha_3}\right). \end{aligned} \tag{3.90}$$

Note that

$$Q_S\left(\frac{(x+y)^q}{\alpha_3} - \frac{x+y}{\alpha_3}\right) = Q_S\left(\frac{x^q - x}{\alpha_3} + \frac{y^q - y}{\alpha_3}\right) \tag{3.91}$$

Then by (3.87) and (3.91) we have

$$\begin{aligned} &B_S\left(\frac{x^q - x}{\alpha_3}, \frac{y^q - y}{\alpha_3}\right) \\ &= Q_S\left(\frac{x^q - x}{\alpha_3} + \frac{y^q - y}{\alpha_3}\right) - Q_S\left(\frac{x^q - x}{\alpha_3}\right) - Q_S\left(\frac{y^q - y}{\alpha_3}\right) \\ &= Q_S\left(\frac{(x+y)^q}{\alpha_3} - \frac{x+y}{\alpha_3}\right) - Q_S\left(\frac{x^q - x}{\alpha_3}\right) - Q_S\left(\frac{y^q - y}{\alpha_3}\right). \end{aligned} \tag{3.92}$$

Combining (3.90) and (3.92) we obtain that

$$B_R(x,y) = B_S\left(\frac{x^q - x}{\alpha_3}, \frac{y^q - y}{\alpha_3}\right),$$

which completes the proof. ■

Let W_S be the radical of B_S and let W_R be the radical of B_R. We have

$$W_S = \{x \in \mathbb{F}_{q^m} : B_S(x,y) = 0 \quad \text{for all} \quad y \in \mathbb{F}_{q^m}\}.$$

Using Lemma 3.4.1 we obtain that

$$W_R = \left\{x \in \mathbb{F}_{q^m} : B_S\left(\frac{x^q}{\alpha_3} - \frac{x}{\alpha_3}, \frac{y^q}{\alpha_3} - \frac{y}{\alpha_3}\right) = 0 \quad \text{for all} \quad y \in \mathbb{F}_{q^m}\right\}.$$

Let W be the $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}$ defined as

$$W = \left\{ x \in \mathbb{F}_{q^m} : B_S\left(x, \frac{y^q}{\alpha_3} - \frac{y}{\alpha_3}\right) = 0 \quad \text{for all} \quad y \in \mathbb{F}_{q^m} \right\}.$$

The fact that W is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}$ follows from the bilinearity of B_S.

Let η be the $\mathbb{F}_q$-linear map

$$\begin{aligned} \eta : \mathbb{F}_{q^m} &\to \mathbb{F}_{q^m} \\ x &\mapsto \tfrac{x^q}{\alpha_3} - \tfrac{x}{\alpha_3}. \end{aligned}$$

Let $H = \mathrm{Im}(\eta)$ be the image of η, or equivalently the image $\eta\left(\mathbb{F}_{q^m}\right)$ of $\mathbb{F}_{q^m}$ under the map η.

Lemma 3.4.2 *Under the notation as above, for the image $\eta(W_R)$ of W_R under the map η, we have*

$$\eta(W_R) = W \cap H.$$

Proof. We first show that $\eta(W_R) \subseteq W \cap H$. It is clear that $\eta(W_R) \subseteq H$ and its is enough to show that $\eta(W_R) \subseteq W$. Let $x \in W_R$. By definition of W_R we have

$$B_S\left(\frac{x^q}{\alpha_3} - \frac{x}{\alpha_3}, \frac{y^q}{\alpha_3} - \frac{y}{\alpha_3}\right) = 0$$

for all $y \in \mathbb{F}_{q^m}$. Hence

$$B_S\left(\eta(x), \frac{y^q}{\alpha_3} - \frac{y}{\alpha_3}\right) = 0$$

for all $y \in \mathbb{F}_{q^m}$. Using the definition of W we obtain that $\eta(x) \in W$.

Conversely let $x \in W \cap H$. Then, as $x \in H$, there exists $x_1 \in \mathbb{F}_{q^m}$ such that

$$x = \frac{x_1^q}{\alpha_3} - \frac{x_1}{\alpha_3}. \tag{3.93}$$

Using the definition of W and (3.93) we get that

$$B_S\left(\frac{x_1^q}{\alpha_3} - \frac{x_1}{\alpha_3}, \frac{y^q}{\alpha_3} - \frac{y}{\alpha_3}\right) = 0$$

for all $y \in \mathbb{F}_{q^m}$. Hence $x_1 \in W_R$ and

$$x = \eta(x_1) \in \eta(W_R)).$$

This completes the proof. ■

As a consequence of Lemma 3.4.2, we obtain the following useful lemma.

Lemma 3.4.3 *We keep the notation as above.*

If $W \subseteq H$, then

$$\dim W_R = \dim W + 1. \tag{3.94}$$

If $W \nsubseteq H$, then

$$\dim W_R = \dim W. \tag{3.95}$$

Proof. We note that

$$\mathrm{Ker}\eta = \mathbb{F}_q$$

and hence

$$\dim W_R = \dim \eta(W_R) + 1. \tag{3.96}$$

Assume first that $W \subseteq H$. Then using Lemma 3.4.2 we obtain that

$$\dim \eta(W_R) = \dim (W \cap H) = \dim W. \tag{3.97}$$

using (3.96) and (3.97) we prove (3.94).

Next we assume that $W \nsubseteq H$. We have, by linear algebra,

$$\dim(W \cap H) + \dim \left(\mathrm{Span}\{W \cup H\}\right) = \dim W + \dim H. \tag{3.98}$$

Note that

$$\dim H = m - 1$$

as $\mathrm{Ker}\eta = \mathbb{F}_q$. Moreover

$$dim W \geq 1.$$

Indeed, otherwise $\dim W = 0$ and $W \subseteq H$ trivially, which is a contradiction to our assumption that $W \nsubseteq H$. Therefore

$$\dim \left(\mathrm{Span}\{W \cup H\}\right) > \dim H = m - 1,$$

which implies that

$$\dim\left(\mathrm{Span}\{W \cup H\}\right) = m. \tag{3.99}$$

Combining (3.98) and (3.99) we obtain that

$$\begin{aligned} \dim(W \cap H) &= \dim W + (m-1) - m \\ &= \dim W - 1. \end{aligned} \tag{3.100}$$

Moreover we have

$$\dim(W \cap H) = \dim \eta(W_R) \tag{3.101}$$

by Lemma 3.4.2.

The proof of (3.95) follows from (3.96), (3.100) and (3.101). ■

Now we consider W in detail. Note that the map

$$\begin{aligned} \widetilde{\varphi} : \mathbb{F}_{q^m} &\to \mathbb{F}_{q^m} \\ x &\mapsto x + x^{q^{2h}} \end{aligned}$$

is injective as $\frac{m}{h}$ is odd. Let $\xi_3 \in \mathbb{F}_{q^m} \setminus \{0\}$ be the uniquely determined nonzero element such that

$$\widetilde{\varphi}(\xi_3) = \alpha_3^{q^h}.$$

Lemma 3.4.4 *Under the notation as above, we have that*

$$W = \{c\xi_3 : c \in \mathbb{F}_q\}.$$

Proof. Let $x \in \mathbb{F}_{q^m}$. By definition of W we have that $x \in W$ if and only if

$$B_S\left(x, \frac{y^q}{\alpha_3} - \frac{y}{\alpha_3}\right) = 0$$

for all $y \in \mathbb{F}_{q^m}$.

For $y \in \mathbb{F}_{q^m}$, we have that $B_S\left(x, \frac{y^q}{\alpha_3} - \frac{y}{\alpha_3}\right) = 0$ if and only if

$$\mathrm{Tr}\left(x\left(\frac{y^q}{\alpha_3} - \frac{y}{\alpha_3}\right)^{q^h} + x^{q^h}\left(\frac{y^q}{\alpha_3} - \frac{y}{\alpha_3}\right)\right) = 0.$$

Note that

$$\mathrm{Tr}\left(x\left(\frac{y^q}{\alpha_3}-\frac{y}{\alpha_3}\right)^{q^h}\right)=\mathrm{Tr}\left(x^{q^{-h}}\left(\frac{y^q}{\alpha_3}-\frac{y}{\alpha_3}\right)\right).$$

Moreover

$$\mathrm{Tr}\left(\left(\frac{x^{q^h}+x^{q^{-h}}}{\alpha_3}\right)y^q\right)=\mathrm{Tr}\left(\left(\frac{x^{q^{h-1}}+x^{q^{-h-1}}}{\alpha_3^{q^{-1}}}\right)y\right).$$

Then for $x, y \in \mathbb{F}_{q^m}$ we have that $B_S\left(x, \frac{y^q}{\alpha_3}-\frac{y}{\alpha_3}\right)=0$ if and only if

$$\mathrm{Tr}\left(\left(\frac{x^{q^{h-1}}+x^{q^{-h-1}}}{\alpha_3^{q^{-1}}}-\frac{x^{q^h}+x^{q^{-h}}}{\alpha_3}\right)y\right)=0.$$

This implies, for $x \in \mathbb{F}_{q^m}$, that $B_S\left(x, \frac{y^q}{\alpha_3}-\frac{y}{\alpha_3}\right)=0$ for all $y \in \mathbb{F}_{q^m}$ if and only if

$$\left(\frac{x^{q^{h-1}}+x^{q^{-h-1}}}{\alpha_3^{q^{-1}}}-\frac{x^{q^h}+x^{q^{-h}}}{\alpha_3}\right)=0. \tag{3.102}$$

Taking q^{h+1}-th power of both sides of the equation in (3.102) we obtain

$$\frac{x^{q^{2h}}+x}{\alpha_3^{q^h}}-\frac{x^{q^{2h+1}}+x^q}{\alpha_3^{q^{h+1}}}=0.$$

Hence for $x \in \mathbb{F}_{q^m}$, we have that $x \in W$ if and only if

$$\frac{\widetilde{\varphi}(x)}{\alpha_3^{q^h}}=\left(\frac{\widetilde{\varphi}(x)}{\alpha_3^{q^h}}\right)^q$$

or equivalently

$$\frac{\widetilde{\varphi}(x)}{\alpha_3^{q^h}} \in \mathbb{F}_q.$$

We conclude that

$$W=\left\{x \in \mathbb{F}_{q^m} : \widetilde{\varphi}(x)=c\alpha_3^{q^h} \quad \text{for some} \quad c \in \mathbb{F}_q\right\}.$$

As $\widetilde{\varphi}$ is an $\mathbb{F}_q$-linear (vector space) isomorphism on $\mathbb{F}_{q^m}$ and $\widetilde{\varphi}(\xi_3)=\alpha_3^{q^h}$, for $x \in \mathbb{F}_{q^m}$ we have

$$\widetilde{\varphi}(x)=c\alpha_3^{q^h} \iff x=c\xi_3,$$

where $c \in \mathbb{F}_q$. This completes the proof. ■

Combining Lemma 3.4.3 and Lemma 3.4.4 we obtain the following.

Lemma 3.4.5 *Under the notation as above, for the dimension* $\dim W_R$ *of the* $\mathbb{F}_q$*-linear space* W_R *we have*

$$\dim W_R = \begin{cases} 2 & \text{if } W \subseteq H, \\ 1 & \text{if } W \nsubseteq H. \end{cases}$$

Proof. Assume first that $W \subseteq H$, then by Lemma 3.4.3 we have

$$\begin{aligned} \dim W_R &= \dim W + 1 \\ &= 2, \end{aligned},$$

where in the last equality we use the fact that $\dim W = 1$, which follows from Lemma 3.4.4.

Assume next that $W \nsubseteq H$, then by Lemma 3.4.3 we have

$$\begin{aligned} \dim W_R &= \dim W \\ &= 1, \end{aligned},$$

where in the last equality we again use Lemma 3.4.4 and the fact that $\dim W = 1$. ■

Next we consider H in detail.

Lemma 3.4.6 *Under the notation as above, we have that*

$$H = \left\{ x \in \mathbb{F}_{q^m} : \mathrm{Tr}(\alpha_3 x) = 0 \right\}.$$

Proof. If $x \in H$, then there exists $x_1 \in \mathbb{F}_{q^m}$ with $\eta(x_1) = x$, or equivalently

$$\frac{x_1^q}{\alpha_3} - \frac{x_1}{\alpha_3} = x,$$

that is

$$x_1^q - x_1 = \alpha_3 x.$$

Therefore using Hilbert's Theorem 90 we obtain that if $x \in H$, then

$$\mathrm{Tr}(\alpha_3 x) = 0.$$

Conversely, let $x \in \mathbb{F}_{q^m}$ with $\mathrm{Tr}(\alpha_3 x) = 0$. Then, again by Hilbert's Theorem 90, there exists $x_1 \in \mathbb{F}_{q^m}$ such that

$$x_1^q - x_1 = \alpha_3 x.$$

This means that

$$\eta(x_1) = \frac{x_1^q}{\alpha_3} - \frac{x_1}{\alpha_3} = x,$$

which completes the proof. ■

Recall that $\xi_3 \in \mathbb{F}_{q^m} \setminus \{0\}$ is the nonzero element with

$$\xi_3 + \xi_3^{q^{2h}} = \alpha_3^{q^h}. \tag{3.103}$$

Lemma 3.4.7 *Under the notation as above, we have*

$$W \subseteq H \Longleftrightarrow \mathrm{Tr}\left(\left(\xi_3 + \xi_3^{q^{2h}}\right)\xi_3^{q^h}\right) = 0.$$

Proof. By Lemma 3.4.4 we have

$$W = \left\{c\xi_3 : c \in \mathbb{F}_q\right\}. \tag{3.104}$$

Moreover by Lemma 3.4.6 we have

$$H = \left\{x \in \mathbb{F}_{q^m} : \mathrm{Tr}(\alpha_3 x) = 0\right\}. \tag{3.105}$$

Note that as W and H are $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_{q^m}$ and $\dim W = 1$,

$$W \subseteq H \Longleftrightarrow \xi_3 \in H. \tag{3.106}$$

Indeed if $\xi_3 \in H$, then $c\xi_3 \in H$ for all $c \in \mathbb{F}_q$, and hence using (3.104) we get that $W \subseteq H$. Conversely if $W \subseteq H$, then as $\xi_3 = 1 \cdot \xi_3 \in W$ we have $\xi_3 \in H$ trivially.

Using (3.105) and (3.106) we obtain that

$$W \subseteq H \Longleftrightarrow \mathrm{Tr}\,(\alpha_3\xi_3) = 0. \tag{3.107}$$

From (3.103) we get

$$\begin{aligned} \mathrm{Tr}(\alpha_3\xi_3) &= \mathrm{Tr}\left((\alpha_3\xi_3)^{q^h}\right) \\ &= \mathrm{Tr}\left(\alpha_3^{q^h}\xi_3^{q^h}\right) \\ &= \mathrm{Tr}\left(\left(\xi_3 + \xi_3^{q^{2h}}\right)\xi_3^{q^h}\right). \end{aligned} \tag{3.108}$$

The proof follows from (3.107) and (3.108). ■

Combining Lemma 3.4.5 and Lemma 3.4.7 we obtain the following.

Lemma 3.4.8 *Under the notation as above, for the dimension* $\dim W_R$ *of the* $\mathbb{F}_q$*-linear subspace* W_R *of* $\mathbb{F}_{q^m}$ *we have*

$$\dim W_R = \begin{cases} 2 & \text{if} \quad \mathrm{Tr}\left(\left(\xi_3 + \xi_3^{q^{2h}}\right)\xi_3^{q^h}\right) = 0, \\ \\ 1 & \text{if} \quad \mathrm{Tr}\left(\left(\xi_3 + \xi_3^{q^{2h}}\right)\xi_3^{q^h}\right) \neq 0. \end{cases}$$

Proof. The proof follows directly from Lemma 3.4.5 and Lemma 3.4.7. ■

The following proposition is useful.

Proposition 3.4.9 *Let* q *be a power of an odd prime. Let* $m \geq 2$ *and* $h \geq 1$ *be integers. Let* Tr *denote the trace map from* $\mathbb{F}_{q^m}$ *onto* $\mathbb{F}_q$*.*

There exists $\xi \in \mathbb{F}_{q^m} \setminus \{0\}$ *such that*

$$\mathrm{Tr}\left(\left(\xi + \xi^{q^{2h}}\right)\xi^{q^h}\right) = 0. \tag{3.109}$$

There exists $\xi \in \mathbb{F}_{q^m} \setminus \{0\}$ *such that*

$$\mathrm{Tr}\left(\left(\xi + \xi^{q^{2h}}\right)\xi^{q^h}\right) \neq 0. \tag{3.110}$$

Proof. Let $0 \leq h_1 < m$ and $0 \leq h_2 < m$ be the integers with

$$h \equiv h_1 \mod m,$$

and

$$2h \equiv h_2 \mod m.$$

Hence for $\xi \in \mathbb{F}_{q^m}$ we have

$$\mathrm{Tr}\left(\left(\xi + \xi^{q^{2h}}\right)\xi^{q^h}\right) = \mathrm{Tr}\left(\left(\xi + \xi^{q^{h_2}}\right)\xi^{q^{h_1}}\right). \tag{3.111}$$

Let $m_1 = m - h_1$. Then, for $\xi \in \mathbb{F}_{q^m}$, taking q^{m_1}-th power we obtain that

$$\mathrm{Tr}\left(\left(\xi + \xi^{q^{h_2}}\right)\xi^{q^{h_1}}\right) = \mathrm{Tr}\left(\left(\xi^{q^{m_1}} + \xi^{q^{h_2+m_1}}\right)\xi\right). \tag{3.112}$$

Let $S_1(X)$ be the $\mathbb{F}_q$-linearized polynomial

$$S_1(X) = X^{q^{m_1}} + X^{q^{h_2+m_1}} \in \mathbb{F}_{q^m}[X].$$

Let F_1 be the algebraic function field with

$$F_1 = \mathbb{F}_{q^m}(x, y) \quad \text{with} \quad y^q - y = S_1(x)x.$$

Let B_{S_1} be the symmetric bilinear form on the $\mathbb{F}_q$-linear space $\mathbb{F}_{q^m}$ defined as

$$\begin{aligned} B_{S_1} : \mathbb{F}_{q^m} \times \mathbb{F}_{q^m} &\to \mathbb{F}_q \\ (x, y) &\mapsto \mathrm{Tr}\left(xS_1(y) + yS_1(x)\right). \end{aligned}$$

Let W_1 be the radical of B_{S_1}, which is given by

$$W_1 = \left\{x \in \mathbb{F}_{q^m} : B_{S_1}(x, y) = 0 \quad \text{for all} \quad y \in \mathbb{F}_{q^m}\right\}.$$

Let $k_1 = \dim W_1$ be the $\mathbb{F}_q$-dimension of W_1.

As $W_1 \subseteq \mathbb{F}_{q^m}$, it is clear that

$$0 \le k_1 \le m. \tag{3.113}$$

Let $N(F_1)$ denote the number of rational places of F_1.

Using Theorem 2.3.1 of Chapter 2, we obtain that $N(F_1)$ is in the set

$$\begin{aligned} T_1 \quad = \quad & \Big\{1 + q^m - q^{\frac{m+k_1}{2}}, 1 + q^m + q^{\frac{m+k_1}{2}}, \\ & 1 + q^m + (q-1)q^{\frac{m+k_1}{2}}, 1 + q^m - (q-1)q^{\frac{m+k_1}{2}} \\ & 1 + q^m + q^{\frac{m+k_1+1}{2}}, 1 + q^m - q^{\frac{m+k_1+1}{2}}\Big\}. \end{aligned}$$

Using (3.113), we get

$$1 + q < \min T_1 \quad \text{and} \quad \max T_1 < 1 + q^{m+1}. \tag{3.114}$$

Let N_1 denote the number of solutions of

$$\mathrm{Tr}\left(xS_1(x)\right) = 0$$

with $x \in \mathbb{F}_{q^m}$. Using Hilbert's Theorem 90 we obtain that

$$N(F_1) = 1 + qN_1. \tag{3.115}$$

First we consider the case (3.109) of the proposition and we assume that there is no $\xi \in \mathbb{F}_{q^m} \setminus \{0\}$ such that

$$\mathrm{Tr}\left(\left(\xi + \xi^{q^{2h}}\right)\xi^{q^h}\right) = 0.$$

Note that for $\xi = 0$, we have that $\mathrm{Tr}\left(\left(\xi + \xi^{q^{2h}}\right)\xi^{q^h}\right) = 0$ holds trivially. Therefore $N_1 = 1$ and using (3.115) we obtain that

$$N(F_1) = 1 + q. \tag{3.116}$$

As $N(F_1) \notin T_1$, using (3.114) and (3.116) we obtain a contradiction. This proves that there exists $\xi \in \mathbb{F}_{q^m} \setminus \{0\}$ such that (3.109) holds.

Next we consider the case (3.110) of the proposition and we assume that there is no $\xi \in \mathbb{F}_{q^m} \setminus \{0\}$ such that

$$\mathrm{Tr}\left(\left(\xi + \xi^{q^{2h}}\right)\xi^{q^h}\right) \neq 0.$$

Hence we obtain that $N_1 = q^m$ and from (3.115) we get that

$$N(F_1) = 1 + q^{m+1}. \tag{3.117}$$

Again, as $N(F_1) \notin T_1$, using (3.114) and (3.116) we obtain a contradiction. This completes the proof. ■

Recall that (see 3.85) L is an $\mathbb{F}_q$-linear map on $\mathbb{F}_{q^m}$ given by

$$\begin{aligned} L : \mathbb{F}_{q^m} &\to \mathbb{F}_{q^m} \\ x &\mapsto -\left(\left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^{-h}} + \left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^h}\right)x. \end{aligned}$$

Let ψ_1 be the $\mathbb{F}_q$-linear map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ defined by

$$\begin{aligned} \psi_1 : \mathbb{F}_{q^m} &\to \mathbb{F}_q \\ x &\mapsto \mathrm{Tr}\left(L(x)\right). \end{aligned}$$

Recall that η is the $\mathbb{F}_q$-linear map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_{q^m}$ given by

$$\begin{aligned} \eta : \mathbb{F}_{q^m} &\rightarrow \mathbb{F}_{q^m} \\ x &\mapsto \frac{x^q}{\alpha_3} - \frac{x}{\alpha_3}. \end{aligned}$$

Let ψ be the $\mathbb{F}_q$-linear map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ defined by

$$\begin{aligned} \psi : \mathbb{F}_{q^m} &\rightarrow \mathbb{F}_q \\ x &\mapsto \psi_1\left(\frac{x^q}{\alpha_3} - \frac{x}{\alpha_3}\right). \end{aligned}$$

Lemma 3.4.10 *Under notation as above, we have that*

$$W_R \subseteq \mathrm{Ker}\psi$$

if and only if

$$\eta\left(W_R\right) \subseteq \mathrm{Ker}\psi_1.$$

Proof. If $x \in W_R$ and $\psi(x) = 0$, then

$$\psi_1\left(\frac{x^q}{\alpha_3} - \frac{x}{\alpha_3}\right) = \psi_1\left(\eta(x)\right) = 0,$$

which implies that $\eta\left(W_R\right) \subseteq \mathrm{Ker}\psi_1$.

Conversely assume that $\eta\left(W_R\right) \subseteq \mathrm{Ker}\psi_1$ and there exists $x \in W_R \setminus \mathrm{Ker}\psi$. Then $\eta(x) \in \mathrm{Ker}\psi_1$,

$$\psi_1\left(\frac{x^q}{\alpha_3} - \frac{x}{\alpha_3}\right) = 0,$$

and hence $\psi(x) = 0$, which is a contradiction.

This completes the proof. ■

In the following lemma, we use Lemma 3.4.2, Lemma 3.4.4, Lemma 3.4.8 and Lemma 3.4.10.

Lemma 3.4.11 *We keep the notation as above.*

If $W \nsubseteq H$, *then*

$$W_R \subseteq \mathrm{Ker}\psi$$

always.

If $W \subseteq H$, then

$$W_R \subseteq \mathrm{Ker}\psi \Longleftrightarrow \mathrm{Tr}\left(\left(\left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^{-h}} + \left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^h}\right)\xi_3\right) = 0,$$

where $\xi_3 \in \mathbb{F}_{q^m} \setminus \{0\}$ is the uniquely determined element by α_3 such that

$$\xi_3 + \xi_3^{q^{2h}} = \alpha_3^{q^h}.$$

Proof. Recall that

$$W_R = \left\{x \in \mathbb{F}_{q^m} : B_S\left(\frac{x^q - x}{\alpha_3}, \frac{y^q - y}{\alpha_3}\right) = 0 \quad \text{for all} \quad y \in \mathbb{F}_{q^m}\right\}.$$

If $x \in \mathbb{F}_q$, then $x^q - x = 0$ and hence

$$B_S\left(\frac{x^q - x}{\alpha_3}, \frac{y^q - y}{\alpha_3}\right) = B_S\left(0, \frac{y^q - y}{\alpha_3}\right) = 0$$

for all $y \in \mathbb{F}_{q^m}$. This shows that

$$\mathbb{F}_q \subseteq W_R.$$

Recall that

$$\mathrm{Ker}\eta = \mathbb{F}_q.$$

Therefore we obtain that

$$\dim W_R = \dim \eta(W_R) + 1. \tag{3.118}$$

Assume first that $W \nsubseteq H$. Then by Lemma 3.4.5 we have that

$$\dim W_R = 1. \tag{3.119}$$

Using (3.118) and (3.119) we conclude that

$$\dim \eta(W_R) = 0.$$

Therefore

$$\eta(W_R) \subseteq \mathrm{Ker}\psi_1$$

holds trivially, and using Lemma 3.4.10 we obtain that

$$W_R \subseteq \mathrm{Ker}\psi.$$

Assume next that $W \subseteq H$. Then by Lemma 3.4.2

$$\eta(W_R) = W \cap H = W. \tag{3.120}$$

Using (3.120) and Lemma 3.4.4

$$\eta(W_R) = \{c\xi_3 : c \in \mathbb{F}_q\}. \tag{3.121}$$

Note that $\dim \eta(W_R) = 1$. Using (3.121) and Lemma 3.4.10 we obtain that $W_R \subseteq \mathrm{Ker}\psi$ if and only if

$$\psi_1(\xi_3) = 0,$$

which is equivalent to

$$-\mathrm{Tr}\left(\left(\left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^{-h}} + \left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^h}\right)\xi_3\right) = 0.$$

This completes the proof. ■

Lemma 3.4.12 *Let $\xi_3 \in \mathbb{F}_{q^m} \setminus \{0\}$. Let $\alpha_3 \in \mathbb{F}_{q^m} \setminus \{0\}$ be the uniquely determined element by ξ_3 such that*

$$\xi_3 + \xi_3^{q^{2h}} = \alpha_3^{q^h}.$$

Let $\gamma_3 \in \mathbb{F}_{q^m}$.

The number of $\alpha_1 \in \mathbb{F}_{q^m}$ such that

$$\mathrm{Tr}\left(\left(\left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^{-h}} + \left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^h}\right)\xi_3\right) = 0 \tag{3.122}$$

is q^{m-1}.

The number of $\alpha_1 \in \mathbb{F}_{q^m}$ such that

$$\mathrm{Tr}\left(\left(\left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^{-h}} + \left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^h}\right)\xi_3\right) \neq 0 \tag{3.123}$$

is $q^m - q^{m-1}$.

Proof. Let

$$\overline{\alpha}_1 = \alpha_1 + \frac{2\gamma_3}{\alpha_3}.$$

Note that the number of $\alpha_1 \in \mathbb{F}_{q^m}$ satisfying (3.122) is equal to the number of $\overline{\alpha}_1 \in \mathbb{F}_{q^m}$ satisfying

$$\mathrm{Tr}\left(\left((\overline{\alpha}_1)^{q^{-h}} + (\overline{\alpha}_1)^{q^h}\right)\xi_3\right) = 0. \tag{3.124}$$

Similarly the number of $\alpha_1 \in \mathbb{F}_{q^m}$ satisfying (3.123) is equal to the number of $\overline{\alpha}_1 \in \mathbb{F}_{q^m}$ satisfying

$$\mathrm{Tr}\left(\left((\overline{\alpha}_1)^{q^{-h}} + (\overline{\alpha}_1)^{q^h}\right)\xi_3\right) \neq 0. \tag{3.125}$$

For $\overline{\alpha}_1 \in \mathbb{F}_{q^m}$, we have

$$\mathrm{Tr}\left((\overline{\alpha}_1)^{q^{-h}}\,\xi_3\right) = \mathrm{Tr}\left(\overline{\alpha}_1 \xi_3^{q^h}\right),$$

and

$$\mathrm{Tr}\left((\overline{\alpha}_1)^{q^h}\,\xi_3\right) = \mathrm{Tr}\left(\overline{\alpha}_1 \xi_3^{q^{-h}}\right).$$

Hence for $\overline{\alpha}_1 \in \mathbb{F}_{q^m}$, (3.124) holds if and only if

$$\mathrm{Tr}\left(\overline{\alpha}_1\left(\xi_3^{q^h} + \xi_3^{q^{-h}}\right)\right) = 0. \tag{3.126}$$

As

$$\alpha_3^{q^h} = \xi_3 + \xi_3^{q^{2h}},$$

and $\alpha_3 \neq 0$, we have

$$\xi_3^{q^h} + \xi_3^{q^{-h}} = \alpha_3 \in \mathbb{F}_{q^m} \setminus \{0\}.$$

Therefore the number of $\overline{\alpha}_1 \in \mathbb{F}_{q^m}$ satisfying (3.124) is equal to the number of $\overline{\alpha}_1 \in \mathbb{F}_{q^m}$ satisfying

$$\mathrm{Tr}\,(\overline{\alpha}_1\alpha_3) = 0.$$

As $\alpha_3 \neq 0$, this number is well known to be q^{m-1}.

For the number of $\overline{\alpha}_1 \in \mathbb{F}_{q^m}$ satisfying (3.125), or equivalently for the number of $\alpha_1 \in \mathbb{F}_{q^m}$ satisfying (3.123), we subtract q^{m-1} from $q^m = |\mathbb{F}_{q^m}|$, which gives $q^m - q^{m-1}$. This completes the proof. ■

We combine Proposition 3.4.9 and Lemma 3.4.12 in the next proposition.

Proposition 3.4.13 *We keep the notation and assumptions as above. The statements in each of the following four cases hold:*

Case i) *There exist* $\xi_3 \in \mathbb{F}_{q^m} \setminus \{0\}$, $\gamma_3 \in \mathbb{F}_{q^m}$, *and* $\alpha_1 \in \mathbb{F}_{q^m}$ *such that*

$$\mathrm{Tr}\left(\left(\xi_3 + \xi_3^{q^{2h}}\right)\xi_3^{q^h}\right) = 0,$$

and

$$\mathrm{Tr}\left(\left(\left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^{-h}} + \left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^h}\right)\xi_3\right) = 0,$$

where $\alpha_3 \in \mathbb{F}_{q^m} \setminus \{0\}$ *is the uniquely determined element by* ξ_3 *such that* $\xi_3 + \xi_3^{q^{2h}} = \alpha_3^{q^h}$.

Case ii) *There exist* $\xi_3 \in \mathbb{F}_{q^m} \setminus \{0\}$, $\gamma_3 \in \mathbb{F}_{q^m}$, *and* $\alpha_1 \in \mathbb{F}_{q^m}$ *such that*

$$\mathrm{Tr}\left(\left(\xi_3 + \xi_3^{q^{2h}}\right)\xi_3^{q^h}\right) = 0,$$

and

$$\mathrm{Tr}\left(\left(\left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^{-h}} + \left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^h}\right)\xi_3\right) \neq 0,$$

where $\alpha_3 \in \mathbb{F}_{q^m} \setminus \{0\}$ *is the uniquely determined element by* ξ_3 *such that* $\xi_3 + \xi_3^{q^{2h}} = \alpha_3^{q^h}$.

Case iii) *There exist* $\xi_3 \in \mathbb{F}_{q^m} \setminus \{0\}$, $\gamma_3 \in \mathbb{F}_{q^m}$, *and* $\alpha_1 \in \mathbb{F}_{q^m}$ *such that*

$$\mathrm{Tr}\left(\left(\xi_3 + \xi_3^{q^{2h}}\right)\xi_3^{q^h}\right) \neq 0,$$

and

$$\mathrm{Tr}\left(\left(\left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^{-h}} + \left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^h}\right)\xi_3\right) = 0,$$

where $\alpha_3 \in \mathbb{F}_{q^m} \setminus \{0\}$ *is the uniquely determined element by* ξ_3 *such that* $\xi_3 + \xi_3^{q^{2h}} = \alpha_3^{q^h}$.

Case iv) There exist $\xi_3 \in \mathbb{F}_{q^m} \setminus \{0\}$, $\gamma_3 \in \mathbb{F}_{q^m}$, *and* $\alpha_1 \in \mathbb{F}_{q^m}$ *such that*

$$\mathrm{Tr}\left(\left(\xi_3 + \xi_3^{q^{2h}}\right)\xi_3^{q^h}\right) \neq 0,$$

and

$$\mathrm{Tr}\left(\left(\left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^{-h}} + \left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^h}\right)\xi_3\right) \neq 0,$$

where $\alpha_3 \in \mathbb{F}_{q^m} \setminus \{0\}$ *is the uniquely determined element by* ξ_3 *such that* $\xi_3 + \xi_3^{q^{2h}} = \alpha_3^{q^h}$.

Proof. Using Proposition 3.4.9 we choose $\xi_3 \in \mathbb{F}_{q^m} \setminus \{0\}$ such that

$$\mathrm{Tr}\left(\left(\xi_3 + \xi_3^{q^{2h}}\right)\xi_3^{q^h}\right) = 0.$$

Let $\alpha_3 \in \mathbb{F}_{q^m} \setminus \{0\}$ be the uniquely determined nonzero element such that

$$\xi_3 + \xi_3^{q^{2h}} = \alpha_3^{q^h}.$$

We choose $\gamma_3 \in \mathbb{F}_{q^m}$ arbitrarily.

Using Lemma 3.4.12 we know that there exists $\alpha_1 \in \mathbb{F}_{q^m}$ such that

$$\mathrm{Tr}\left(\left(\left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^{-h}} + \left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^h}\right)\xi_3\right) = 0. \tag{3.127}$$

Moreover we also know that there exists $\alpha_1 \in \mathbb{F}_{q^m}$ such that

$$\mathrm{Tr}\left(\left(\left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^{-h}} + \left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^h}\right)\xi_3\right) \neq 0. \tag{3.128}$$

These prove the statements in Case i) and Case ii).

For Case iii) and Case iv), using Proposition 3.4.9, we choose $\xi_3 \in \mathbb{F}_{q^m} \setminus \{0\}$ such that

$$\mathrm{Tr}\left(\left(\xi_3 + \xi_3^{q^{2h}}\right)\xi_3^{q^h}\right) \neq 0.$$

Again we choose $\gamma_3 \in \mathbb{F}_{q^m}$ arbitrarily. By Lemma 3.4.12, as above, we know existence of $\alpha_1 \in \mathbb{F}_{q^m}$ satisfying (3.127). Also we know existence of $\alpha_1 \in \mathbb{F}_{q^m}$ satisfying (3.128). Hence we prove the statements in Case iii) and Case iv).

This completes the proof. ■

In the following corollary we use Lemma 3.4.7, Lemma 3.4.8 and Lemma 3.4.11 together with Proposition 3.4.13.

Corollary 3.4.14 *We keep the notation and assumptions as above. For $\alpha_1, \alpha_3, \gamma_3 \in \mathbb{F}_{q^m}$ with $\alpha_3 \neq 0$, we are in one of the four cases of Proposition 3.4.13, and, conversely, each case of Proposition 3.4.13 occurs as α_1, α_3 and γ_3 run through $\mathbb{F}_{q^m}$ with $\alpha_3 \neq 0$.*

If we are in Case i) of Proposition 3.4.13, then

$$\dim W_R = 2 \quad \textit{and} \quad W_R \subseteq \mathrm{Ker}\psi. \tag{3.129}$$

If we are in Case ii) of Proposition 3.4.13, then

$$\dim W_R = 2 \quad \textit{and} \quad W_R \nsubseteq \mathrm{Ker}\psi. \tag{3.130}$$

If we are in Case iii) or Case iv) of Proposition 3.4.13, then

$$\dim W_R = 1 \quad \textit{and} \quad W_R \subseteq \mathrm{Ker}\psi. \tag{3.131}$$

Proof. Let $\alpha_1, \alpha_3, \gamma_3 \in \mathbb{F}_{q^m}$ with $\alpha_3 \neq 0$. Then it is clear that these elements define exactly one of the four cases of Proposition 3.4.13 depending on whether the corresponding equations give zero or nonzero values. Also by Proposition 3.4.13, each of these four cases occur as $\alpha_1, \alpha_3, \gamma_3$ run through $\mathbb{F}_{q^m}$ with $\alpha_3 \neq 0$.

Assume first that we are in Case i) of Proposition 3.4.13. Then by Lemma 3.4.8

$$\dim W_R = 2,$$

and

$$W \subseteq H$$

by Lemma 3.4.7. Then using Lemma 3.4.11 we obtain that

$$W_R \subseteq \mathrm{Ker}\psi,$$

which proves (3.129).

Assume now that we are in Case ii) of Proposition 3.4.13. Then, still by Lemma 3.4.7 and Lemma 3.4.8, we have

$$\dim W_R = 2,$$

and

$$W \subseteq H.$$

However by Lemma 3.4.11, now we have

$$W_R \nsubseteq \mathrm{Ker}\psi,$$

which proves (3.130).

Assume finally that we are in Case iii) or Case iv) of Proposition 3.4.13. By Lemma 3.4.7 and Lemma 3.4.8,

$$\dim W_R = 1,$$

and

$$W \nsubseteq H.$$

Then by Lemma 3.4.11, both in Case iii) and Case iv) we have

$$W_R \subseteq \mathrm{Ker}\psi,$$

which proves (3.131).

This completes the proof. ■

We are ready to determine the number of rational places of the algebraic function fields $F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}$ and E_{α_1,γ_1} in each case.

We first consider the situation that $\frac{m}{\overline{h}}$ is odd and m is even.

Theorem 3.4.15 *Let q be a power of an odd prime. Let $m \geq 2$ and $h \geq 1$ be integers. Let $\overline{h} = \gcd(2h, m)$.*

Assume that $\frac{m}{\overline{h}}$ is odd and m is even.

Let $\alpha_1, \alpha_3, \gamma_3 \in \mathbb{F}_{q^m}$ with $\alpha_3 \neq 0$.

Let $\xi_3 \in \mathbb{F}_{q^m} \setminus \{0\}$ be the unique element determined by α_3 such that

$$\xi_3 + \xi_3^{q^{2h}} = \alpha_3^{q^h}.$$

For $\gamma_1 \in \mathbb{F}_{q^m}$, let $F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}$ and E_{α_1,γ_1} be the algebraic function fields defined as

$$F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3} = \mathbb{F}_{q^m}(y_2, y_1) \quad \textit{with}$$

$$y_1^q - y_1 = 2\left(\frac{y_2^q}{\alpha_3} - \frac{y_2}{\alpha_3}\right)^{q^h+1} + L\left(\frac{y_2^q}{\alpha_3} - \frac{y_2}{\alpha_3}\right) + \left(\gamma_1 + 2\left(\frac{\gamma_3}{\alpha_3}\right)^{q^h+1}\right),$$

and

$$E_{\alpha_1,\gamma_1} = \mathbb{F}_{q^m}(x, y) \quad \textit{with} \quad y^q - y = 2x^{q^h+1} - \left(\alpha_1^{q^{-h}} + \alpha_1^{q^h}\right)x + \gamma_1.$$

Here L is an $\mathbb{F}_q$-linear map on $\mathbb{F}_{q^m}$ given by

$$\begin{aligned} L : \mathbb{F}_{q^m} &\to \mathbb{F}_{q^m} \\ x &\mapsto -\left(\left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^{-h}} + \left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^h}\right)x. \end{aligned}$$

As γ_1 runs through $\mathbb{F}_{q^m}$, the number $N\left(E_{\alpha_1,\gamma_1}\right)$ of E_{α_1,γ_1} takes both of the values in the set

$$\left\{1 + q^m - q^{\frac{m}{2}}, 1 + q^m + (q-1)q^{\frac{m}{2}}\right\}, \tag{3.132}$$

or takes both values of in the set

$$\left\{1 + q^m + q^{\frac{m}{2}}, 1 + q^m - (q-1)q^{\frac{m}{2}}\right\} \tag{3.133}$$

Assume that $\alpha_1, \alpha_3, \gamma_3 \in \mathbb{F}_{q^m}$ with $\alpha_3 \neq 0$ is chosen such that we are in Case i) of Proposition 3.4.13. Then as γ_1 runs through $\mathbb{F}_{q^m}$, the number $N\left(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}\right)$ of $F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}$ takes both of the values in the set

$$\left\{1 + q^m - q^{\frac{m}{2}+1}, 1 + q^m + (q-1)q^{\frac{m}{2}+1}\right\},$$

or takes both values of in the set

$$\left\{1 + q^m + q^{\frac{m}{2}+1}, 1 + q^m - (q-1)q^{\frac{m}{2}+1}\right\}.$$

Assume that $\alpha_1, \alpha_3, \gamma_3 \in \mathbb{F}_{q^m}$ with $\alpha_3 \neq 0$ is chosen such that we are in Case ii) of Proposition 3.4.13. Then as γ_1 runs through $\mathbb{F}_{q^m}$, the number $N\left(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}\right)$ of $F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}$ is always given by

$$N\left(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}\right) = 1 + q^m.$$

Assume that $\alpha_1, \alpha_3, \gamma_3 \in \mathbb{F}_{q^m}$ with $\alpha_3 \neq 0$ is chosen such that we are in Case iii) or Case iv) of Proposition 3.4.13. Then as γ_1 runs through $\mathbb{F}_{q^m}$, the number $N\left(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}\right)$ of $F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}$ takes both of the values in the set

$$\left\{1 + q^m + q^{\frac{m}{2}+1}, 1 + q^m - q^{\frac{m}{2}+1}\right\}.$$

Proof. We complete the proof using Theorem 2.3.1 of Chapter 2.

First we consider $N(E_{\alpha_1,\gamma_1})$. We use similar arguments as in the proof of Theorem 3.2.2. By Lemma 3.1.2, as $\frac{m}{h}$ is odd, for the dimension k_E of the radical of the corresponding symmetric bilinear form of E_{α_1,γ_1}, which is independent from α_1 and γ_1, we have

$$k_E = 0.$$

Moreover there exists a nonzero element $d_E \in \mathbb{F}_q \setminus \{0\}$, which depends only on q, h and m, used for the determination of the number $N(E_{\alpha_1,\gamma_1})$ of rational places of E_{α_1,γ_1}.

Recall that m is even by our assumption.

If

$$(-1)^{\frac{m}{2}} d_E \quad \text{is a square in} \quad \mathbb{F}_q,$$

then $N(E_{\alpha_1,\gamma_1})$ takes both of the values in the set

$$\left\{1 + q^m - q^{\frac{m}{2}}, 1 + q^m + (q-1)q^{\frac{m}{2}}\right\}$$

as α_1 and γ_1 run through $\mathbb{F}_{q^m}$, Here we use Lemma 3.1.3 and Theorem 2.3.1 of Chapter 2.

If

$$(-1)^{\frac{m}{2}} d_E \quad \text{is a not square in} \quad \mathbb{F}_q,$$

then $N(E_{\alpha_1,\gamma_1})$ takes both of the values in the set

$$\left\{1 + q^m + q^{\frac{m}{2}}, 1 + q^m - (q-1)q^{\frac{m}{2}}\right\}$$

as α_1 and γ_1 run through $\mathbb{F}_{q^m}$. Here we again use Lemma 3.1.3 and Theorem 2.3.1 of Chapter 2. These complete the proof of the statements in the theorem related to the number $N(E_{\alpha_1,\gamma_1})$ of rational places of E_{α_1,γ_1}.

Next we consider $N(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3})$ case by case.

Assume that $\alpha_1, \alpha_3, \gamma_3 \in \mathbb{F}_{q^m}$ with $\alpha_3 \neq 0$ is chosen such that we are in Case i) of Proposition 3.4.13. Then by Corollary 3.4.14 we have

$$k_R := \dim W_R = 2 \quad \text{and} \quad W_R \subseteq \mathrm{Ker}\psi.$$

There exists a nonzero element $d_L \in \mathbb{F}_q \setminus \{0\}$, which depends on the map L together with q, h and m. Here d_L is used for the determination of the number $N(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3})$ of rational places of $F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}$.

As m is even, if

$$(-1)^{\frac{m-2}{2}} d_L \quad \text{is a square in} \quad \mathbb{F}_q,$$

then $N(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3})$ takes both of the values

$$\left\{1 + q^m - q^{\frac{m}{2}+1}, 1 + q^m + (q-1)q^{\frac{m}{2}+1}\right\}$$

as γ_1 runs through $\mathbb{F}_{q^m}$.

If

$$(-1)^{\frac{m-2}{2}} d_L \quad \text{is not a square in} \quad \mathbb{F}_q,$$

then $N(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3})$ takes both of the values

$$\left\{1 + q^m + q^{\frac{m}{2}+1}, 1 + q^m - (q-1)q^{\frac{m}{2}+1}\right\}$$

as γ_1 runs through $\mathbb{F}_{q^m}$.

These complete the proof of the statements in the theorem related to the number $N(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3})$ of rational places of $F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}$ for Case i) of Proposition 3.4.13.

Assume next that $\alpha_1, \alpha_3, \gamma_3 \in \mathbb{F}_{q^m}$ with $\alpha_3 \neq 0$ is chosen such that we are in Case ii) of Proposition 3.4.13. Then by Corollary 3.4.14 we have

$$k_R = \dim W_R = 2 \quad \text{and} \quad W_R \nsubseteq \mathrm{Ker}\psi.$$

Then, as $W_R \nsubseteq \mathrm{Ker}\psi$, we have

$$N(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}) = 1 + q^m$$

for each value of $\gamma_1 \in \mathbb{F}_{q^m}$.

This completes the proof of the statements in the theorem related to the number $N(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3})$ of rational places of $F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}$ for Case ii) of Proposition 3.4.13.

Finally we assume that $\alpha_1, \alpha_3, \gamma_3 \in \mathbb{F}_{q^m}$ with $\alpha_3 \neq 0$ is chosen such that we are in Case iii) or Case iv) of Proposition 3.4.13. Then by Corollary 3.4.14 we have

$$k_R = \dim W_R = 1 \quad \text{and} \quad W_R \subseteq \mathrm{Ker}\psi.$$

As $m - k_R$ is odd, $N(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3})$ takes both of the values

$$\left\{1 + q^m - q^{\frac{m}{2}+1}, 1 + q^m + q^{\frac{m}{2}+1}\right\}$$

as γ_1 runs through $\mathbb{F}_{q^m}$.

This completes the proof of the statements in the theorem related to the number $N(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3})$ of rational places of $F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}$ for Case iii) and Case iv) of Proposition 3.4.13. ■

We determine $\mathcal{P}_S$ in the next corollary when $\frac{m}{\overline{h}}$ is odd and m is even.

Corollary 3.4.16 *Let q be a power of an odd prime. Let $m \geq 2$ and $h \geq 1$ be integers. Let $\overline{h} = \gcd(2h, m)$.*

Assume that $\frac{m}{\overline{h}}$ is odd and m is even.

Let Π be the map

$$\begin{aligned} \Pi : \mathbb{F}_{q^m} &\to \mathbb{F}_q \\ x &\mapsto \mathrm{Tr}\left(x^{q^h+1}\right). \end{aligned}$$

Let $(\mathcal{S}, \mathcal{K}, \mathcal{M}, \mathcal{E})$ be the authentication code with secrecy defined as

$$\begin{cases} \mathcal{S} = \mathbb{F}_{q^m}, \\ \mathcal{K} = \mathbb{F}_{q^m}, \\ \mathcal{M} = \mathbb{F}_{q^m} \times \mathbb{F}_q, \\ \mathcal{E} = \{E_k : k \in \mathcal{K}\}, \end{cases}$$

where for $k \in \mathcal{K}$, the authentication map E_k is defined as

$$\begin{aligned} E_k : \mathcal{S} &\to \mathcal{M} \\ s &\mapsto (s + k, \Pi(s) + \Pi(k)). \end{aligned}$$

Let $\mathcal{P}_S$ denote the maximum success probability of the substitution attack on the authentication code with secrecy defined above. Then $\mathcal{P}_S$ takes one of the values in the set

$$\left\{\frac{q^{m-2}+(q-1)q^{\frac{m}{2}-1}}{q^{m-1}-q^{\frac{m}{2}-1}}, \frac{q^{m-2}+q^{\frac{m}{2}-1}}{q^{m-1}-q^{\frac{m}{2}-1}}\right\},$$

or takes one of the values in the set

$$\left\{\frac{q^{m-2}+(q-1)q^{\frac{m}{2}-1}}{q^{m-1}-(q-1)q^{\frac{m}{2}-1}}, \frac{q^{m-2}+q^{\frac{m}{2}-1}}{q^{m-1}-(q-1)q^{\frac{m}{2}-1}}\right\}.$$

Proof. We will complete the proof using (3.79) and Theorem 3.4.15.

For the number $N(E_{\alpha_1,\gamma_1})$ there are two cases we should consider, which correspond to the sets in (3.132) and (3.133) of Theorem 3.4.15.

Assume first that $N(E_{\alpha_1,\gamma_1})$ takes one of the values in the set in (3.132). Taking (3.79) into account we need to consider

$$N_1 := \min\left\{1+q^m-q^{\frac{m}{2}}, 1+q^m+(q-1)q^{\frac{m}{2}}\right\} = 1+q^m-q^{\frac{m}{2}}.$$

Then, again by (3.79), we compute

$$\frac{N_1-1}{q} = q^{m-1}-q^{\frac{m}{2}-1}. \tag{3.134}$$

For the number $N(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3})$ of $F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}$, we need to consider all of four cases of proposition 3.4.13 one by one, as all of them occur. From Case i) of Proposition 3.4.13 we get

$$\begin{aligned} N_{2,1} &:= \max\left\{1+q^m-q^{\frac{m}{2}+1}, 1+q^m+(q-1)q^{\frac{m}{2}+1}\right\} \\ &= 1+q^m+(q-1)q^{\frac{m}{2}+1} \end{aligned} \tag{3.135}$$

or

$$\begin{aligned} N_{2,1} &:= \max\left\{1+q^m+q^{\frac{m}{2}+1}, 1+q^m-(q-1)q^{\frac{m}{2}+1}\right\} \\ &= 1+q^m+q^{\frac{m}{2}+1} \end{aligned} \tag{3.136}$$

From Case ii) of Proposition 3.4.13 we get

$$N_{2,2} := 1+q^m.$$

From Case iii) and Case iv) of proposition 3.4.13 we get

$$\begin{aligned} N_{2,3} &:= \max\left\{1+q^m+q^{\frac{m}{2}+1}, 1+q^m-q^{\frac{m}{2}+1}\right\} \\ &= 1+q^m+q^{\frac{m}{2}+1} \end{aligned} \tag{3.137}$$

Let

$$N_2 := \max\{N_{2,1}, N_{2,2}, N_{2,3}\}.$$

If (3.135) holds, then we have

$$N_2 = 1+q^m+(q-1)q^{\frac{m}{2}+1}. \tag{3.138}$$

If (3.136) holds, then we have

$$N_2 = 1+q^m+q^{\frac{m}{2}+1}. \tag{3.139}$$

Using (3.79), (3.138) and (3.139) we compute and conclude that

$$\frac{N_2-1}{q^2} \in \left\{q^{m-2}+(q-1)q^{\frac{m}{2}-1}, q^{m-2}+q^{\frac{m}{2}-1}\right\}. \tag{3.140}$$

Hence by (3.134) and (3.140), using (3.79) we get that

$$\mathcal{P}_{\mathcal{S}} \in \left\{\frac{q^{m-2}+(q-1)q^{\frac{m}{2}-1}}{q^{m-1}-q^{\frac{m}{2}-1}}, \frac{q^{m-2}+q^{\frac{m}{2}-1}}{q^{m-1}-q^{\frac{m}{2}-1}}\right\},$$

provided that $N(E_{\alpha_1,\gamma_1})$ takes one of the values in the set in (3.132).

Assume next that $N(E_{\alpha_1,\gamma_1})$ takes one of the values in the set in (3.133). Taking (3.79) into account we need to consider

$$N_1 := \min\left\{1+q^m+q^{\frac{m}{2}}, 1+q^m-(q-1)q^{\frac{m}{2}}\right\} = 1+q^m-(q-1)q^{\frac{m}{2}}.$$

Then by (3.79), we compute

$$\frac{N_1-1}{q} = q^{m-1}-(q-1)q^{\frac{m}{2}-1}. \tag{3.141}$$

By the same reasoning corresponding to the case that $N(E_{\alpha_1,\gamma_1})$ takes one of the values in the set in (3.133) above, for the numerator of the right hand side of (3.79) we consider and obtain

$$\frac{N_2-1}{q^2} \in \left\{q^{m-2}+(q-1)q^{\frac{m}{2}-1}, q^{m-2}+q^{\frac{m}{2}-1}\right\}. \tag{3.142}$$

From (3.79), (3.141) and (3.142) we get that

$$\mathcal{P}_{\mathcal{S}} = \frac{\left(\frac{N_2-1}{q^2}\right)}{\left(\frac{N_1-1}{q}\right)} \in \left\{ \frac{q^{m-2}+(q-1)q^{\frac{m}{2}-1}}{q^{m-1}-(q-1)q^{\frac{m}{2}-1}}, \frac{q^{m-2}+q^{\frac{m}{2}-1}}{q^{m-1}-(q-1)q^{\frac{m}{2}-1}} \right\},$$

provided that $N(E_{\alpha_1,\gamma_1})$ takes one of the values in the set in (3.133).

This completes the proof. ■

3.5 THE MAXIMUM SUCCESS PROBABILITY OF THE SUBSTITUTION ATTACK: CASE $\frac{m}{\gcd(2h,m)}$ IS ODD AND m IS ODD

We continue our study on the maximum success probability $\mathcal{P}_{\mathcal{S}}$ of the impersonation attack on the authentication code with secrecy defined in (3.1) when $\frac{m}{\gcd(2h,m)}$ is odd.

Using similar methods as in Section 3.4, we determine $\mathcal{P}_{\mathcal{S}}$ when $\frac{m}{\gcd(2h,m)}$ is odd and m is odd.

This section will conclude our study of $\mathcal{P}_{\mathcal{S}}$ in all cases.

Theorem 3.5.1 *Let q be a power of an odd prime. Let $m \geq 2$ and $h \geq 1$ be integers. Let $\overline{h} = \gcd(2h, m)$.*

Assume that $\frac{m}{\overline{h}}$ is odd and m is odd.

Let $\alpha_1, \alpha_3, \gamma_3 \in \mathbb{F}_{q^m}$ with $\alpha_3 \neq 0$.

Let $\xi_3 \in \mathbb{F}_{q^m} \setminus \{0\}$ be the unique element determined by α_3 such that

$$\xi_3 + \xi_3^{q^{2h}} = \alpha_3^{q^h}.$$

For $\gamma_1 \in \mathbb{F}_{q^m}$, let $F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}$ and E_{α_1,γ_1} be the algebraic function fields defined as

$$F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3} = \mathbb{F}_{q^m}(y_2, y_1) \quad \textit{with}$$

$$y_1^q - y_1 = 2\left(\frac{y_2^q}{\alpha_3} - \frac{y_2}{\alpha_3}\right)^{q^h+1} + L\left(\frac{y_2^q}{\alpha_3} - \frac{y_2}{\alpha_3}\right) + \left(\gamma_1 + 2\left(\frac{\gamma_3}{\alpha_3}\right)^{q^h+1}\right),$$

and

$$E_{\alpha_1,\gamma_1} = \mathbb{F}_{q^m}(x, y) \quad \textit{with} \quad y^q - y = 2x^{q^h+1} - \left(\alpha_1^{q^{-h}} + \alpha_1^{q^h}\right)x + \gamma_1.$$

Here L is an $\mathbb{F}_q$-linear map on $\mathbb{F}_{q^m}$ given by

$$\begin{aligned} L : \mathbb{F}_{q^m} &\to \mathbb{F}_{q^m} \\ x &\mapsto -\left(\left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^{-h}} + \left(\alpha_1 + \frac{2\gamma_3}{\alpha_3}\right)^{q^h}\right)x. \end{aligned}$$

As γ_1 runs through $\mathbb{F}_{q^m}$, the number $N\left(E_{\alpha_1,\gamma_1}\right)$ of E_{α_1,γ_1} takes both of the values in the set

$$\left\{1 + q^m + q^{\frac{m+1}{2}}, 1 + q^m - q^{\frac{m+1}{2}}\right\},$$

Assume that $\alpha_1, \alpha_3, \gamma_3 \in \mathbb{F}_{q^m}$ with $\alpha_3 \neq 0$ is chosen such that we are in Case i) of Proposition 3.4.13. Then as γ_1 runs through $\mathbb{F}_{q^m}$, the number $N\left(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}\right)$ of $F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}$ takes both of the values in the set

$$\left\{1 + q^m + q^{\frac{m+1}{2}+1}, 1 + q^m - q^{\frac{m+1}{2}+1}\right\}.$$

Assume that $\alpha_1, \alpha_3, \gamma_3 \in \mathbb{F}_{q^m}$ with $\alpha_3 \neq 0$ is chosen such that we are in Case ii) of Proposition 3.4.13. Then as γ_1 runs through $\mathbb{F}_{q^m}$, the number $N\left(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}\right)$ of $F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}$ is always given by

$$N\left(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}\right) = 1 + q^m.$$

Assume that $\alpha_1, \alpha_3, \gamma_3 \in \mathbb{F}_{q^m}$ with $\alpha_3 \neq 0$ is chosen such that we are in Case iii) or Case iv) of Proposition 3.4.13. Then as γ_1 runs through $\mathbb{F}_{q^m}$, the number $N\left(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}\right)$ of $F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}$ takes both of the values in the set

$$\left\{1 + q^m - q^{\frac{m+1}{2}}, 1 + q^m + (q-1)q^{\frac{m+1}{2}}\right\},$$

or takes both values in the set

$$\left\{1 + q^m + q^{\frac{m+1}{2}}, 1 + q^m - (q-1)q^{\frac{m+1}{2}}\right\}.$$

Proof. The proof is similar to the proof of Theorem 3.4.15.

Again we first consider $N(E_{\alpha_1,\gamma_1})$. Under the notation of the proof of Theorem 3.4.15 we still have

$$k_E = 0,$$

and there exists a nonzero element $d_E \in \mathbb{F}_q \setminus \{0\}$, which depends only on q, h and m.

Recall that m is odd by our assumption. Then using Lemma 3.1.3 and Theorem 2.3.1 of Chapter 2, $N(E_{\alpha_1,\gamma_1})$ takes both of the values in the set

$$\left\{1 + q^m + q^{\frac{m+1}{2}}, 1 + q^m - q^{\frac{m+1}{2}}\right\} \tag{3.143}$$

as α_1 and γ_1 run through $\mathbb{F}_{q^m}$. There is only one set given in (3.143), which is independent from d_E. This completes the proof of the statement in the theorem related to the number $N(E_{\alpha_1,\gamma_1})$ of rational places of E_{α_1,γ_1}.

Next, similarly, we consider $N(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3})$ case by case.

Assume that $\alpha_1, \alpha_3, \gamma_3 \in \mathbb{F}_{q^m}$ with $\alpha_3 \neq 0$ is chosen such that we are in Case i) of Proposition 3.4.13. Then by Corollary 3.4.14 we have

$$k_R = \dim W_R = 2 \quad \text{and} \quad W_R \subseteq \text{Ker}\psi.$$

There exists a nonzero element $d_L \in \mathbb{F}_q \setminus \{0\}$, which depends on the map L together with q, h and m.

As m is odd, $m - k_R$ is odd and hence $N(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3})$ takes both of the values

$$\left\{1 + q^m - q^{\frac{m+1}{2}+1}, 1 + q^m + q^{\frac{m+1}{2}+1}\right\}$$

as γ_1 runs through $\mathbb{F}_{q^m}$. Note again that there is only one set given in (3.143), which is independent from d_L.

Assume next that $\alpha_1, \alpha_3, \gamma_3 \in \mathbb{F}_{q^m}$ with $\alpha_3 \neq 0$ is chosen such that we are in Case ii) of Proposition 3.4.13. As in the case of Theorem 3.4.15, by Corollary 3.4.14 we have

$$k_R = \dim W_R = 2 \quad \text{and} \quad W_R \nsubseteq \text{Ker}\psi.$$

Then, as $W_R \nsubseteq \text{Ker}\psi$, we have

$$N(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}) = 1 + q^m$$

for each value of $\gamma_1 \in \mathbb{F}_{q^m}$.

Finally we assume that $\alpha_1, \alpha_3, \gamma_3 \in \mathbb{F}_{q^m}$ with $\alpha_3 \neq 0$ is chosen such that we are in Case iii) or Case iv) of Proposition 3.4.13. Then by Corollary 3.4.14 we have

$$k_R = \dim W_R = 1 \quad \text{and} \quad W_R \subseteq \text{Ker}\psi.$$

Again there exists a nonzero element $d_{\alpha_3} \in \mathbb{F}_q \setminus \{0\}$, which depends on α_3 together with q, h and m.

As $m - k_R$ is even, we need to take d_{α_3} into account.

If

$$(-1)^{\frac{m-1}{2}} d_{\alpha_3} \quad \text{is a square in} \quad \mathbb{F}_q,$$

then $N(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3})$ takes both of the values

$$\left\{1 + q^m - q^{\frac{m+1}{2}}, 1 + q^m + (q-1)q^{\frac{m+1}{2}}\right\}$$

as γ_1 runs through $\mathbb{F}_{q^m}$.

If

$$(-1)^{\frac{m-1}{2}} d_{\alpha_3} \quad \text{is not a square in} \quad \mathbb{F}_q,$$

then $N(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3})$ takes both of the values

$$\left\{1 + q^m + q^{\frac{m+1}{2}}, 1 + q^m - (q-1)q^{\frac{m+1}{2}}\right\}$$

as γ_1 runs through $\mathbb{F}_{q^m}$.

These complete the proof of the statements in the theorem related to the number $N(F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3})$ of rational places of $F_{\alpha_1,\gamma_1,\alpha_3,\gamma_3}$ for Case iii) and Case iv) of Proposition 3.4.13. ■

Corollary 3.5.2 *Let q be a power of an odd prime. Let $m \geq 2$ and $h \geq 1$ be integers. Let $\overline{h} = \gcd(2h, m)$.*

Assume that $\frac{m}{\overline{h}}$ is odd and m is odd.

Let Π be the map

$$\begin{aligned} \Pi : \mathbb{F}_{q^m} &\to \mathbb{F}_q \\ x &\mapsto \mathrm{Tr}\left(x^{q^h+1}\right). \end{aligned}$$

Let $(\mathcal{S}, \mathcal{K}, \mathcal{M}, \mathcal{E})$ be the authentication code with secrecy defined as

$$\begin{cases} \mathcal{S} = \mathbb{F}_{q^m}, \\ \mathcal{K} = \mathbb{F}_{q^m}, \\ \mathcal{M} = \mathbb{F}_{q^m} \times \mathbb{F}_q, \\ \mathcal{E} = \{E_k : k \in \mathcal{K}\}, \end{cases}$$

where for $k \in \mathcal{K}$, the authentication map E_k is defined as

$$\begin{aligned} E_k : \mathcal{S} &\to \mathcal{M} \\ s &\mapsto (s + k, \Pi(s) + \Pi(k)) . \end{aligned}$$

Let $\mathcal{P}_S$ denote the maximum success probability of the substitution attack on the authentication code with secrecy defined above. Then $\mathcal{P}_S$ is given exactly by

$$\mathcal{P}_S = \frac{q^{m-2} + q^{\frac{m-1}{2}}}{q^{m-1} - q^{\frac{m-1}{2}}}.$$

Proof. The proof is similar to the proof of Corollary 3.4.16.

For the number $N(E_{\alpha_1,\gamma_1})$, using Theorem 3.5.1 and (3.79) we define

$$N_1 := \min\left\{1 + q^m + q^{\frac{m+1}{2}}, 1 + q^m - q^{\frac{m+1}{2}}\right\} = 1 + q^m - q^{\frac{m+1}{2}}.$$

Then we have

$$\frac{N_1 - 1}{q} = q^{m-1} - q^{\frac{m-1}{2}}. \tag{3.144}$$

For the number $N(F_{\alpha_1,\gamma_2,\alpha_3,\gamma_3})$ we consider all four cases of Proposition 3.4.13.

When we are in Case i) of Proposition 3.4.13 we define

$$N_{2,1} := \max\left\{1 + q^m + q^{\frac{m+1}{2}+1}, 1 + q^m - q^{\frac{m+1}{2}+1}\right\} = 1 + q^m + q^{\frac{m+1}{2}+1}.$$

When we are in Case ii) of Proposition 3.4.13 we define

$$N_{2,2} := 1 + q^m.$$

When we are in Case iii) or Case iv) of Proposition 3.4.13 we define $N_{2,3}$ as

$$\begin{aligned} N_{2,3} &:= \max\left\{1 + q^m - q^{\frac{m+1}{2}}, 1 + q^m + (q-1)q^{\frac{m+1}{2}}\right\} \\ &= 1 + q^m + (q-1)q^{\frac{m+1}{2}}, \end{aligned} \tag{3.145}$$

or

$$\begin{aligned} N_{2,3} &:= \max\left\{1 + q^m - (q-1)q^{\frac{m+1}{2}}, 1 + q^m + q^{\frac{m+1}{2}}\right\} \\ &= 1 + q^m + q^{\frac{m+1}{2}}. \end{aligned} \tag{3.146}$$

Let

$$N_2 := \max\{N_{2,1}, N_{2,2}, N_{2,3}\}.$$

Note that

$$1 + q^m + q^{\frac{m+1}{2}+1} > 1 + q^m + (q-1)q^{\frac{m+1}{2}}.$$

Therefore, independent from whether we define $N_{2,3}$ as in (3.145) or as in (3.146), we have

$$N_2 = 1 + q^m + q^{\frac{m+1}{2}+1}.$$

Hence we get

$$\frac{N_2 - 1}{q^2} = q^{m-2} + q^{\frac{m-1}{2}}. \tag{3.147}$$

Using (3.79), (3.144), and (3.147) we obtain that

$$\mathcal{P}_{\mathcal{S}} = \frac{\left(\frac{N_2 - 1}{q^2}\right)}{\left(\frac{N_1 - 1}{q}\right)} = \frac{q^{m-2} + q^{\frac{m-1}{2}}}{q^{m-1} - q^{\frac{m-1}{2}}}.$$

This completes the proof. ■

3.6 THE LEVEL OF SECRECY

In this section we study the level of secrecy provided by the authentication codes defined in (3.1).

We use similar methods as in Section 3.2 above.

First we recall some notation and some results that we will use in this section.

Let Π denote the map introduced in the definition of the authentication codes with secrecy given in (3.1) above. For the minimum level of secrecy provided by these authentication codes with secrecy, we need to consider the minimum value

$$\min_{m_1, m_2} |\{s \in \mathcal{S} : \Pi(s) + \Pi(m_1 - s) = m_2\}|, \tag{3.148}$$

where the minimum is over $(m_1, m_2) \in \mathcal{M}$, or equivalently over $m_1 \in \mathbb{F}_{q^m}$ and $m_2 \in \mathbb{F}_q$.

Let $\alpha \in \mathbb{F}_{q^m}$ and $b \in \mathbb{F}_q$. For $x \in \mathbb{F}_{q^m}$ we have

$$\Pi(x) + \Pi(\alpha - x) = \mathrm{Tr}\left(2x^{q^h+1} - \left(\alpha^{q^{-h}} + \alpha^{q^h}\right)x + \alpha^{q^h+1}\right).$$

Let $\beta \in \mathbb{F}_{q^m}$ with $\mathrm{Tr}(\beta) = b$. Hence, for $x \in \mathbb{F}_{q^m}$, we have that

$$\Pi(x) + \Pi(\alpha - x) = b$$

if and only if

$$\mathrm{Tr}\left(2x^{q^h+1} - \left(\alpha^{q^{-h}} + \alpha^{q^h}\right)x + \alpha^{q^h+1} - \beta\right) = 0.$$

For $\alpha \in \mathbb{F}_{q^m}$ and $\gamma \in \mathbb{F}_{q^m}$, let $N(\alpha, \gamma)$ denote the number of solutions of the equation

$$\mathrm{Tr}\left(2x^{q^h+1} - \left(\alpha^{q^{-h}} + \alpha^{q^h}\right)x + \gamma\right) = 0$$

with $x \in \mathbb{F}_{q^m}$.

For $\alpha \in \mathbb{F}_{q^m}$ and $\gamma \in \mathbb{F}_{q^m}$, let $F_{\alpha,\gamma}$ be the algebraic function field

$$F_{\alpha,\gamma} = \mathbb{F}_{q^m}(x, y) \quad \text{with} \quad y^q - y = 2x^{q^h+1} - \left(\alpha^{q^{-h}} + \alpha^{q^h}\right)x + \gamma. \tag{3.149}$$

Let $N(F_{\alpha,\gamma})$ denote the number of rational places of $F_{\alpha,\gamma}$. Using Hilbert's Theorem 90 we have that

$$N\left(F_{\alpha,\gamma}\right) = 1 + qN(\alpha, \gamma).$$

Therefore the minimum value in (3.148) is equal to the minimum value

$$\min_{\alpha,\gamma} \frac{N(F_{\alpha,\gamma}) - 1}{q}, \tag{3.150}$$

where the minimum is over $\alpha, \gamma \in \mathbb{F}_{q^m}$.

Let ψ be the $\mathbb{F}_q$-linear map

$$\begin{aligned} \psi : \mathbb{F}_{q^m} &\to \mathbb{F}_q \\ x &\mapsto \mathrm{Tr}\left(-\left(\alpha^{q^{-h}} + \alpha^{q^h}\right)x\right). \end{aligned}$$

Let $S(T) = 2T^{q^h} \in \mathbb{F}_{q^m}[T]$ be the $\mathbb{F}_q$-linearized polynomial.

Let B_S be the bilinear form

$$\begin{aligned} B_S : \mathbb{F}_{q^m} \times \mathbb{F}_{q^m} &\rightarrow \mathbb{F}_q \\ (x, y) &\mapsto \mathrm{Tr}\left(xS(y) + yS(x)\right). \end{aligned}$$

Let W_S denote the radical of B_S. We have

$$W_S = \left\{x \in \mathbb{F}_{q^m} : x + x^{q^{2h}} = 0\right\}.$$

Using Lemma 3.1.3 we obtain that

$$W_S \subseteq \mathrm{Ker}\psi, \tag{3.151}$$

for any positive integer h.

Let $\overline{h} = \gcd(2h, m)$.

By Lemma 3.1.2 we have

$$\dim W_S = 0 \quad \text{if} \quad \frac{m}{\overline{h}} \quad \text{is odd},$$

and

$$\dim W_S = \overline{h} \quad \text{if} \quad \frac{m}{\overline{h}} \quad \text{is even},$$

Now we are ready to determine the level of secrecy.

Theorem 3.6.1 *Let q be a power of an odd prime. Let $m \geq 2$ and $h \geq 1$ be integers. Let Π be the map*

$$\begin{aligned} \Pi : \mathbb{F}_{q^m} &\rightarrow \mathbb{F}_q \\ x &\mapsto \mathrm{Tr}\left(x^{q^h+1}\right). \end{aligned}$$

Let $(\mathcal{S}, \mathcal{K}, \mathcal{M}, \mathcal{E})$ be the authentication code with secrecy defined as

$$\begin{cases} \mathcal{S} = \mathbb{F}_{q^m}, \\ \mathcal{K} = \mathbb{F}_{q^m}, \\ \mathcal{M} = \mathbb{F}_{q^m} \times \mathbb{F}_q, \\ \mathcal{E} = \{E_k : k \in \mathcal{K}\}, \end{cases}$$

where for $k \in \mathcal{K}$, the authentication map E_k is defined as

$$\begin{aligned} E_k : \mathcal{S} &\to \mathcal{M} \\ s &\mapsto (s + k, \Pi(s) + \Pi(k)) . \end{aligned}$$

Moreover let $\overline{h}$ be the positive integer given by

$$\overline{h} = \gcd(2h, m).$$

If $\frac{m}{\overline{h}}$ is odd and m is odd, then the authentication codes with secrecy defined above provides at least

$$\log_2 \left(q^{m-1} - q^{\frac{m-1}{2}} \right) \tag{3.152}$$

bits of secrecy.

If $\frac{m}{\overline{h}}$ is odd and m is even, then the authentication codes with secrecy defined above provides at least

$$\log_2 \left(q^{m-1} - q^{\frac{m}{2}-1} \right) \quad or \quad \log_2 \left(q^{m-1} - (q-1) q^{\frac{m}{2}-1} \right) \tag{3.153}$$

bits of secrecy.

If $\frac{m}{\overline{h}}$ is even, then the authentication codes with secrecy defined above provides at least

$$\log_2 \left(q^{m-1} - q^{\frac{m+\overline{h}}{2}-1} \right) \quad or \quad \log_2 \left(q^{m-1} - (q-1) q^{\frac{m+\overline{h}}{2}-1} \right) \tag{3.154}$$

bits of secrecy.

Proof. Let

$$k = \dim W_S .$$

First we consider the case that $\frac{m}{\overline{h}}$ is odd and m is odd. Then

$$k = 0 \quad \text{and} \quad m - k \quad \text{is odd.} \tag{3.155}$$

Let $\alpha, \gamma \in \mathbb{F}_{q^m}$. Using (3.151), (3.155) and Theorem 2.3.1 of Chapter 2, for the number $N(F_{\alpha,\gamma})$ of the algebraic function field defined in (3.149), we have that $N(F_{\alpha,\gamma})$ is in the set

$$\left\{ 1 + q^m - q^{\frac{m+1}{2}}, 1 + q^m + q^{\frac{m+1}{2}} \right\}. \tag{3.156}$$

Moreover both of the values in the set (3.156) are attained as α and γ run through $\mathbb{F}_{q^m}$. Therefore we get

$$\min_{\alpha,\gamma} N(F_{\alpha,\gamma}) = 1 + q^m - q^{\frac{m+1}{2}}$$

and

$$\min_{\alpha,\gamma} \frac{N(F_{\alpha,\gamma}) - 1}{q} = q^{m-1} - q^{\frac{m-1}{2}}$$

Here the minimum values are defined as α and γ run through $\mathbb{F}_{q^m}$.

Therefore using (3.148), (3.150) and taking the logarithm we prove (3.152).

Next we consider the case that $\frac{m}{\overline{h}}$ is odd and m is even. Then

$$k = 0 \quad \text{and} \quad m - k \quad \text{is even.} \tag{3.157}$$

Let $\alpha, \gamma \in \mathbb{F}_{q^m}$. Using (3.151), (3.157) and Theorem 2.3.1 of Chapter 2, for the number $N(F_{\alpha,\gamma})$ of the algebraic function field defined in (3.149), we have that $N(F_{\alpha,\gamma})$ is in the set

$$\left\{1 + q^m - q^{\frac{m}{2}}, 1 + q^m + (q-1)q^{\frac{m}{2}}\right\} \tag{3.158}$$

or $N(F_{\alpha,\gamma})$ is in the set

$$\left\{1 + q^m + q^{\frac{m}{2}}, 1 + q^m - (q-1)q^{\frac{m}{2}}\right\} \tag{3.159}$$

Moreover if $N(F_{\alpha,\gamma})$ is in the set (3.158), then both of the values in the set (3.158) are attained as α and γ run through $\mathbb{F}_{q^m}$. Similarly if $N(F_{\alpha,\gamma})$ is in the set (3.159), then both of the values in the set (3.159) are attained as α and γ run through $\mathbb{F}_{q^m}$.

Therefore we get

$$\min_{\alpha,\gamma} \frac{N(F_{\alpha,\gamma}) - 1}{q} \in \left\{q^{m-1} - q^{\frac{m}{2}-1}, q^{m-1} - (q-1)q^{\frac{m}{2}-1}\right\},$$

where the minimum value is over $\alpha, \gamma \in \mathbb{F}_{q^m}$. Using (3.148), (3.150) and taking the logarithm we complete the proof of (3.153).

Finally we consider the case that $\frac{m}{\overline{h}}$ is even. It is not difficult to observe that m is even and $\overline{h}$ is even in this case (see Remark 3.2.3 above). Then we have

$$k = \overline{h} \quad \text{and} \quad m - k \quad \text{is even.} \tag{3.160}$$

Let $\alpha, \gamma \in \mathbb{F}_{q^m}$. Using (3.151), (3.160) and Theorem 2.3.1 of Chapter 2, for the number $N(F_{\alpha,\gamma})$ of the algebraic function field defined in (3.149), we have that $N(F_{\alpha,\gamma})$ is in the set

$$\left\{1 + q^m - q^{\frac{m+\bar{h}}{2}}, 1 + q^m + (q-1)q^{\frac{m+\bar{h}}{2}}\right\} \tag{3.161}$$

or $N(F_{\alpha,\gamma})$ is in the set

$$\left\{1 + q^m + q^{\frac{m+\bar{h}}{2}}, 1 + q^m - (q-1)q^{\frac{m+\bar{h}}{2}}\right\} \tag{3.162}$$

Moreover, as in the case above, if $N(F_{\alpha,\gamma})$ is in the set (3.161), then both of the values in the set (3.161) are attained as α and γ run through $\mathbb{F}_{q^m}$. Similarly if $N(F_{\alpha,\gamma})$ is in the set (3.162), then both of the values in the set (3.162) are attained as α and γ run through $\mathbb{F}_{q^m}$.

Therefore we get

$$\min_{\alpha,\gamma} \frac{N(F_{\alpha,\gamma}) - 1}{q} \in \left\{q^{m-1} - q^{\frac{m+\bar{h}}{2}-1}, q^{m-1} - (q-1)q^{\frac{m+\bar{h}}{2}-1}\right\},$$

where the minimum value is over $\alpha, \gamma \in \mathbb{F}_{q^m}$. Using (3.148), (3.150) and taking the logarithm we complete the proof of (3.154).

This completes the proof. ■

REFERENCES

[1] E. Çakçak and F. Özbudak, Curves related to Coulter's maximal curves, Finite Fields Appl., 14 (2008) 209–220.

[2] L. R. A. Casse, K. M. Martin, P. R. Wild, Bounds and characterizations of authentication/secrecy schemes, Des. Codes and Cryptogr., 13 (1998) 107–129.

[3] M. De Soete, Some constructions for authentication-secrecy codes, *Advances in Cryptology, Eurocrypt'88*, Lecture Notes in Computer Science, vol. 330, pp. 57-76, 1988.

[4] C. Ding, A. Salomaa, P. Solé, T. Xiaojian, Three constructions of auhentication/secrecy codes, J. Pure App. Algebra, 196 (2005) 149–168.

[5] C. Ding and X. Tian, Three constructions of authentication codes with perfect secrecy, Des. Codes and Cryptogr., 33 (2004) 227–239.

[6] E. N. Gilbert, F. J. MacWilliams and N. J. A. Sloane, Codes which detect deception, Bell Syst. Tech. J., 53 (1974) 405–424.

[7] L. C. Grove, *Classical groups and Geometric Algebra*, American Mathematical Society, Providence, 2002.

[8] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1997.

[9] C. Mitchell, M. Walker and P. Wild, The combinatorics of perfect authentication schemes, SIAM J. Discrete Math., 7 (1994) 102–107.

[10] H. Niederreiter and C. Xing, *Rational Points on Curves over Finite Fields*, Cambridge University Press, 2001.

[11] U. Rosenbaum, A lower bound on authentication after having observed a sequence of messages, J. Cryptology, 6 (1993) 135–156.

[12] Z. Saygı, *Constructions of Authentication Codes*, Ph.D. Thesis, Middle East Technical University, Ankara, Turkey, 2007.

[13] G. J. Simmons, Authentication theory/coding theory, *Advances in Cryptology, CRYPTO'84*, Lecture Notes in Computer Science, vol. 196, pp. 411-431, Springer-Verlag, 1984.

[14] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.

[15] D. R. Stinson, A construction for authentication/secrecy codes from certain combinatorial designs, J. Cryptology, 1 (1988) 119–127.

[16] D. R. Stinson and L. Teirlinck, A construction for authentication/secrecy codes from 3-homogeneous permutation groups, European J. Combin., 11 (1990) 73–79.

[17] X. Tian, *Several constructions of authentication codes with secrecy*, Ph.D. Dissertation, University of Hong Kong, Hong Kong, 2004.

VITA

Elif Kurtaran Özbudak graduated from Galatasaray High School in 1989 and she received her B.Sc. degree in Mathematics from Middle East Technical University in 1994. She was placed at the first rank among 1994 year's Mathematics graduates at Middle East Technical University. She got her M.Sc. degree in Mathematics at Bilkent University in 1996 and she got her M.Sc degree in Computer Engineering from Marmara University in 1999, in Turkey. She has been working at Scientific and Technical Research Council of Turkey - National Electronics and Cryptography Research Institute since 1997, and she is currently a Chief Researcher. Her research interests include authentication codes, cryptography, finite fields, group characters, computer information systems, software project management.

She is married and she has two daughters.

She is Project Management Professional (PMP) certified in August 2006, given by the international Project Management Institute (www.pmi.org).

Publications

1. E. Kurtaran Özbudak, F. Özbudak, Z. Saygı, "A class of authentication codes with secrecy ", submitted.

2. E. Kurtaran Özbudak, F. Özbudak, "Number of points of certain curves over finite fields", to be submitted.

3. E. Kurtaran, A. Klyachko, "Some Identities and Asymptotics for Characters of the Symmetric Group", Journal of Algebra 206, pp. 413-437, 1998.

4. Ö. Yürekten, K. Dinçer, B. Akar, M. Sungur and E. Kurtaran Özbudak, "Migrating a Hierarchical Legacy Database Application onto an XML-Based Service-Oriented Web Platform", in the Proc.of ISCIS'06 (The 21st International Symposium on Computer and Information Systems), November 2006, İstanbul, TURKEY, Lecture Notes in Computer Science (LNCS) vol. 4263, pp. 645-654, Springer-Verlag 2006.

5. A. Tumay, K. Dinçer, O. Avci, M. Demirsoy, A. Erdem, Ö. Yürekten, M. Sungur, A. Erdem, and E. K. Özbudak, “Information System Infrastructure for a National Crisis Management Center”, in Proc. of TIEMS 2002 Conference (9th Int. Conference of International Emergency Management Society), Waterloo, Ontario, Canada, May 14-17, 2002.