CONSTRUCTIONS OF AUTHENTICATION CODES

ZÜLFÜKAR SAYGI

JULY 2007

CONSTRUCTIONS OF AUTHENTICATION CODES

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

BY

ZÜLFÜKAR SAYGI

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

JULY 2007

Approval of the Graduate School of Applied Mathematics

Prof. Dr. Ersan AKYILDIZ
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Doctor of Philosophy.

Prof. Dr. Ersan AKYILDIZ
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Doctor of Philosophy.

Prof. Dr. Ferruh ÖZBUDAK
Supervisor

Examining Committee Members

Prof. Dr. İsmail Ş. GÜLOĞLU

Prof. Dr. Ferruh ÖZBUDAK

Prof. Dr. Ersan AKYILDIZ

Assoc. Prof. Dr. Ali DOĞANAKSOY

Assist. Prof. Dr. Ali Aydın SELÇUK

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 :

Signature :

Abstract

Constructions of Authentication Codes

Saygı, Zülfükar
Ph.D., Department of Cryptography
Supervisor: Prof. Dr. Ferruh Özbudak

July 2007, 61 pages

Authentication codes are used in many cryptographic applications. They are divided into two main classes: authentication codes with secrecy and the ones without secrecy. In this thesis, authentication codes are constructed using three different methods. In the first method, by using some codes over Galois rings and generalized Gray map, authentication codes without secrecy over finite fields are obtained. In the second and third methods, by using additive polynomials related to some curves over finite fields, authentication codes with secrecy and without secrecy are constructed. It is observed that the parameters of these codes are better than the existing ones in some cases.

Keywords: Additive Polynomials, Authentication Codes, Cryptography, Galois rings, Secrecy Codes.

Öz

Doğrulama Kodlarının Üretilmesi

Saygı, Zülfükar
Doktora, Kriptografi Bölümü
Tez Yöneticisi: Prof. Dr. Ferruh Özbudak

Temmuz 2007, 61 sayfa

Doğrulama kodları kriptografik birçok uygulamanın içerisinde kullanılmaktadır. Bu kodlar sırlı ve sırsız doğrulama kodları olmak üzere iki ana sınıfa ayrılır. Bu tezde, üç farklı yöntem kullanılarak doğrulama kodları üretildi. İlk yöntemde Galois halkaları üzerindeki bazı kodlar ve genelleştirilmiş Gray dönüşümü kullanılarak sonlu cisimler üzerinde sırsız doğrulama kodları elde edildi. İkinci ve üçüncü yöntemlerde sonlu cisimler üzerindeki bazı eğrilerle ilişkili toplamsal polinomlar kullanılarak sırsız ve sırlı doğrulama kodları üretildi. Bu kodların parametrelerinin bilinen kodların parametrelerinden bazı durumlarda daha iyi oldukları görüldü.

Anahtar Kelimeler: Toplamsal Polinomlar, Doğrulama Kodları, Kriptografi, Galois halkaları, Sır Saklama Kodları.

To my big family,
Especially Elif and Emir Ali

Acknowledgments

I would like to express my sincere gratitude to my supervisor Prof. Dr. Ferruh Özbudak. His ideas and tremendous support had a major influence on this thesis.

I would like to thank Prof. Dr. Ersan Akyıldız, who encourage me to study more mathematical subject.

A very special thanks goes to Prof. Dr. Ali Doğanaksoy. Everyday he encourage us and gives great motivation for our studies.

I would also like to thank my family (Elif, Emir Ali, Şevket, Elife, Aslan, Tuncer, Nazik, Hanım) for the support they provided me through my entire life.

I deeply thank the members of the Institute of Applied Mathematics and my friends for their supports during the period of writing this thesis.

Preface

One of the important topic in the field of communication is the security of the messages. In cryptography many applications are developed to guarantee the secrecy of the messages. Moreover, the assurance about the origin and content of the messages are provided by using authentication codes.

The idea of authentication was first introduced in 1974 by Gilbert, MacWilliams and Sloane [27]. In 1984, Simmons proposed a new model [53], in which an opponent is involved in addition to two trusting parties, a transmitter and a receiver. In this model, the idea of unconditional authentication, an analogous of the idea of the unconditional secrecy proposed by Shannon [52], is developed.

In general authentication codes are divided into two main classes: authentication codes with secrecy and the ones without secrecy. In an authentication code without secrecy, a message is obtained by encoding a source state and the corresponding tag. Transmitter sends this message to the receiver. In this case, there is no encryption of the source state, that is, without knowledge of the shared secret key one can recover the source state from the encoded message. In authentication codes with secrecy, there is an encryption of the source state. Transmitter obtains a message by encoding the encrypted version of a source state and the corresponding tag. In this case, without knowledge of the shared secret key one cannot recover this source state from the message. In these codes, a part of the secret key is used for encryption and another part of the secret key is used for authentication.

In this thesis, authentication codes are constructed using three different methods. In the first method, by using some codes over Galois rings and generalized Gray map, authentication codes without secrecy over finite fields are obtained. In the second and third methods, by using additive polynomials related to some curves over finite fields, authentication codes with secrecy and without secrecy are constructed. It is observed that the parameters of these codes are better than the existing ones in some cases.

This thesis is organized as follows.

In Chapter 1, a general introduction to authentication codes is presented. It includes an

authentication model, some known bounds on the parameters of the authentication codes, some characterizations and some well-known constructions.

In Chapter 2, some constructions of systematic authentication codes over finite field $\mathbb{F}_q$ using Galois rings are presented.

In Chapter 3, two families of systematic authentication codes using additive polynomials related to some curves over finite fields are constructed. It is observed that the parameters of the codes are better than the existing ones in some cases.

In Chapter 4, three different constructions of authentication codes with secrecy using additive polynomials related to some curves over finite fields are given.

In Chapter 5, conclusions and some future work topics are given.

The main parts of this thesis come from the following papers:

F. Özbudak and Z. Saygı, Some constructions of systematic authentication codes using Galois rings, *Designs, Codes and Cryptography*, vol 41, no. 3, pp. 343-357, 2006.

F. Özbudak and Z. Saygı, Constructions of systematic authentication codes using additive polynomials, *Proceedings of International Workshop on Coding ad Cryptography 2007*, Versailles, France, pp. 405-414, 2007.

F. Özbudak and Z. Saygı, Systematic authentication codes using additive polynomials, *Designs, Codes and Cryptography*, submitted.

F. Özbudak and Z. Saygı, Authentication codes with secrecy using additive polynomials, in preparation.

Table of Contents

Chapter 1

Introduction to Authentication Codes

In this chapter, a general introduction to authentication codes is presented. First, the authentication problem with a solution model is explained, then some known bounds on the parameters of the authentication codes are given together with some characterizations and some well-known constructions.

1.1 An Authentication Model

Starting from the ancient times, one of the main problems in the field of communication is the security of the messages. In a general manner, cryptography deals with the alternative solutions to this problem. It has been extensively being used in many diplomatic and military applications in recent years. The topic of cryptography has been widely introduced into various areas of everyday life as a result of the currently popular technology and internet evolvement. The impact of cryptography can be easily detected and discussed in many aspects starting from ATM cards, computer passwords, through internet banking and emails, file transfers and electronic commerce. The crucial issue of the above stated areas is the monitoring of any interference made by a potential opponent to the entire or partial data, which consequently makes it crucial to validate the source and integrity of the original one. As a result, authentication codes are being developed to produce solutions to that problems.

The idea of authentication was first introduced in 1974 by Gilbert, MacWilliams and Sloane [27]. There are two trusting parties in the proposed authentication model, a transmitter and a receiver who share a secret key. The transmitter wants to securely send a piece of information using his/her secret key to the receiver over a public insecure channel. In 1984, Simmons proposed a new model [53], in which an opponent is involved in addition to these two trusting

parties. In such a situation, an opponent could observe or disturb the ordinary communication. The possible transmission errors in the communication due to the noise in public channel are not considered in this model. Those type of errors can be removed using error correcting codes. Such applications are out of the scope of this thesis. Therefore we assume that the channel is public and noiseless. In this thesis we deal with the authentication model proposed by Simmons.

Authentication codes are divided into two main classes: authentication codes with secrecy and the ones without secrecy. In Section 1.1.1 and Section 1.1.2 these two classes are described extensively. We note that using the secret key, a single message can be mapped onto more than one message and this is called splitting. They are considered in [16, 25, 34, 36, 50, 54, 55, 56]. In this thesis, we consider only the authentication codes without splitting and throughout the thesis authentication codes refer to those codes without splitting.

A formal definition for an authentication code is presented as follows:

Definition 1.1.1. An authentication code is a quadruple $(\mathcal{S}, \mathcal{K}, \mathcal{M}, \mathcal{E})$ where $\mathcal{S}$ is the set of source states (plaintexts), $\mathcal{K}$ is the set of keys, $\mathcal{M}$ is the set of messages and $\mathcal{E}$ is the set of authentication maps (encoding rules) from $\mathcal{S} \times \mathcal{K}$ to $\mathcal{M}$.

Note that, for any fixed $k \in \mathcal{K}$ and $E \in \mathcal{E}$ the projection of the authentication map E, say E_k, from $\mathcal{S}$ to $\mathcal{M}$ is one to one. Here it is assumed that the sets $\mathcal{S}$, $\mathcal{K}$ and $\mathcal{M}$ are finite and nonempty. Using the notations as in Definition 1.1.1 the general protocol can be described as follows:

1. The transmitter sends the information $s \in \mathcal{S}$ as $m = E_k(s) \in \mathcal{M}$ where k is the shared secret key.
2. The receiver receives the message $m' = E_{k'}(s')$.
3. Checks the authenticity by checking whether $m' = E_k(s')$ or not.
   (a) If $m' = E_k(s')$, the receiver assumes m' as a valid message.
   (b) If $m' \neq E_k(s')$, the receiver will reject the message.

It is assumed that everything about the authentication model is publicly known due to the *Kerckhoff's principle*. That is, the opponent knows the whole parameters of the authentication code except the secret key shared by the transmitter and the receiver. In this situation, we consider two kinds of attacks. When the opponent generates a message m' and inserts m' into the channel, this is called *impersonation*. When the opponent sees a message m and changes it to a different message m', this is called *substitution*. Let the success probabilities of these attacks be $\mathcal{P}_{\mathcal{I}}$ and $\mathcal{P}_{\mathcal{S}}$ respectively. We assume that the keys and the source states are distributed

equally likely. Then we get the following probabilities

$$\mathcal{P}_{\mathcal{I}} = max_{m\in\mathcal{M}}\ p(m \text{ is a valid message}), \tag{1.1.1}$$

$$\mathcal{P}_{\mathcal{S}} = max_{m,m'\in\mathcal{M},m'\neq m}\ p(m' \text{ is a valid message}|m \text{ is an observed message}). \tag{1.1.2}$$

Note that, $p(\cdot)$ denotes the probability and $p(m'|m)$ denotes the conditional probability that m' is a valid message, after observing m as a valid message.

At this point, it is seen that authentication codes have at least five parameters

$$|\mathcal{S}|, |\mathcal{K}|, |\mathcal{M}|, \mathcal{P}_{\mathcal{I}} \text{ and } \mathcal{P}_{\mathcal{S}}.$$

For any good authentication code the cardinality of the set of source states should be large enough and the other parameters $|\mathcal{K}|, |\mathcal{M}|, \mathcal{P}_{\mathcal{I}}$ and $\mathcal{P}_{\mathcal{S}}$ should be as small as possible. There are two main constrains for the constructions:

1. Given fixed $|\mathcal{S}|, |\mathcal{K}|, |\mathcal{M}|$ find authentication codes having $\mathcal{P}_{\mathcal{I}}$ and $\mathcal{P}_{\mathcal{S}}$ as small as possible,
2. Given fixed $\mathcal{P}_{\mathcal{I}}$ and $\mathcal{P}_{\mathcal{S}}$ find authentication codes having $|\mathcal{S}|$ as large as possible and $|\mathcal{K}|$ and $|\mathcal{M}|$ as small as possible,

It is known that to compare two authentication codes, at least three of the five parameters of the codes should be fixed to be the same respectively.

1.1.1 Authentication Codes without Secrecy

In an authentication code without secrecy, a message is obtained by encoding a source state and the corresponding tag. Transmitter sends this message to the receiver. In this case, there is no encryption of the source state, that is, without knowledge of the shared secret key one can recover the source state from the encoded message. They are considered in [3, 4, 5, 7, 10, 17, 18, 21, 22, 23, 27, 31, 42, 43, 44, 53, 57, 71, 73]. In this thesis, we deal with some constructions of a subclass of authentication codes without secrecy called *systematic authentication codes* (or sometimes called cartesian authentication codes).

Definition 1.1.2. A systematic authentication code is a quadruple $(\mathcal{S}, \mathcal{K}, \mathcal{T}, \mathcal{E})$ where $\mathcal{S}$ is the set of source states (plaintexts), $\mathcal{K}$ is the set of keys, $\mathcal{T}$ is the set of authenticators (tags) and $\mathcal{E}$ is the authentication map from $\mathcal{S} \times \mathcal{K}$ to $\mathcal{T}$.

Here it is assumed that $\mathcal{M} = \mathcal{S} \times \mathcal{T}$. Similar to the general protocol, the authentication protocol for systematic authentication codes is defined as follows:

1. The transmitter sends the information $s \in \mathcal{S}$ as $m = (s, t) \in \mathcal{M}$ by computing $t = \mathcal{E}(s, k) \in \mathcal{T}$ where $k \in \mathcal{K}$ is the shared secret key.

2. The receiver receives the message $m' = (s', t')$.

3. Checks the authenticity by checking whether $t' = \mathcal{E}(s', k)$ or not.

   (a) If $t' = \mathcal{E}(s', k)$, the receiver assumes m' as a valid message.

   (b) If $t' \neq \mathcal{E}(s', k)$, the receiver will reject the message.

For the impersonation attack the opponent generates a message $m_1 = (s_1, t_1)$ and inserts m_1 into the channel and for the substitution attack the opponent sees a message $m = (s, t)$ and changes it to a different message $m_1 = (s_1, t_1)$ with $s \neq s_1$. Therefore the attack probabilities (1.1.1) and (1.1.2) become

$$\mathcal{P}_{\mathcal{I}} = max_{(s,t)\in\mathcal{M}} \frac{|\{k \in \mathcal{K} : t = \mathcal{E}(s,k)\}|}{|\{k \in \mathcal{K}\}|}, \tag{1.1.3}$$

$$\mathcal{P}_{\mathcal{S}} = max_{(s,t)\in\mathcal{M}} max_{(s',t')\in\mathcal{M}, s'\neq s} \frac{|\{k \in \mathcal{K} : t = \mathcal{E}(s,k), t' = \mathcal{E}(s',k)\}|}{|\{k \in \mathcal{K} : t = \mathcal{E}(s,k)\}|}. \tag{1.1.4}$$

1.1.2 Authentication Codes with Secrecy

In authentication codes with secrecy, there is an encryption of the source state. Transmitter obtains a message by encoding the encrypted version of a source state and the corresponding tag. In this case, without knowledge of the shared secret key one cannot recover this source state from the message. In these codes, a part of the secret key is used for encryption and another part of the secret key is used for authentication. They are considered in [9, 15, 19, 20, 27, 41, 49, 45, 53, 63, 64, 65]. Since we have an encryption in authentication codes with secrecy, the uncertainty of a source state becomes an important parameter. The idea of unconditional secrecy is defined by Shannon in 1949 [52]. Using this definition, if for any given message m we have $p(s|m) = p(s)$ then we say that the authentication code with secrecy provides *perfect secrecy*.

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

1. The transmitter sends the information $s \in \mathcal{S}$ as $m = (f_k(s), g_k(s)) \in \mathcal{M}$ by computing $f_k(s)$ and $g_k(s)$ where $k \in \mathcal{K}$ is the shared secret key and the authentication map $E_k = (f_k, g_k) \in \mathcal{E}$. Here f_k is used for the encryption of the source state and g_k is used to compute the tag.

2. The receiver receives the message $m' = (m_1, m_2)$ and computes $s' = f_k^{-1}(m_1)$.

3. Using s' he/she checks the authenticity by checking whether $m_2 = g_k(s')$ or not.

   (a) If $m_2 = g_k(s')$, the receiver assumes m' as a valid message.

(b) If $m_2 \neq g_k(s')$, the receiver will reject the message.

For the impersonation attack the opponent picks an element $m = (m_1, m_2)$ in some way and sends it to the receiver and for substitution attack the opponent has observed one message $m = (m_1, m_2)$, and he/she wants to replace m with another message $m' = (m'_1, m'_2)$, where $m'_1 \neq m_1$.

1.2 Known bounds on the Parameters of the Authentication Codes

In this section some known bounds are presented. In the literature there are many combinatorial and information theoretic bounds on the parameters of the authentication codes. They can be found in [6, 9, 33, 40, 48, 58, 62, 49, 67, 46, 53, 51, 40, 47, 65]. Here only four of them are given. First two theorems are obtained by combinatorial methods, and the last two theorems are proved by using information theoretic techniques.

Theorem 1.2.1 ([40, 48]). *In any authentication code* $(\mathcal{S}, \mathcal{K}, \mathcal{M}, \mathcal{E})$,

$$\mathcal{P}_{\mathcal{I}} \geq \frac{|\mathcal{S}|}{|\mathcal{M}|} \text{ and } \mathcal{P}_{\mathcal{S}} \geq \frac{|\mathcal{S}| - 1}{|\mathcal{M}| - 1}.$$

If both equalities are achieved, then $|\mathcal{K}| \geq |\mathcal{M}|$.

For the systematic authentication code this theorem becomes

Theorem 1.2.2 ([58]). *For any systematic authentication code* $(\mathcal{S}, \mathcal{K}, \mathcal{T}, \mathcal{E})$ *we have*

$$\mathcal{P}_{\mathcal{I}} \geq \frac{1}{|\mathcal{T}|} \text{ and } \mathcal{P}_{\mathcal{S}} \geq \frac{1}{|\mathcal{T}|}.$$

Here some basic information theoretic definitions are given. Details for information theory can be found in [47, 58]. Suppose X is a random variable whose possible values are $x_1, x_2, \ldots, x_n$ with probability distribution $\{p(x_i)\}_{x_i \in X} > 0$. The entropy of X, denoted by $H(X)$, is defined by

$$H(X) = -\sum_{x_i \in X} p(x_i) \log_2 p(x_i).$$

For any random variables X and Y the conditional entropy $H(X|Y)$ is then defined by

$$H(X|Y) = -\sum_{x \in X} \sum_{y \in Y} p(y) p(x|y) \log_2 p(x|y).$$

The generalization of following information theoretic bounds are first given by Rosenbaum [49], and were first proved for the systematic authentication codes in [67]. The $\mathcal{P}_{\mathcal{I}}$ part of the theorem were first proved by Simmons, Sgarro and Massey in [53, 51, 40].

Theorem 1.2.3. *For any authentication code* $(\mathcal{S}, \mathcal{K}, \mathcal{M}, \mathcal{E})$ *we have*

$$\mathcal{P}_{\mathcal{I}} \geq 2^{H(\mathcal{K}|\mathcal{M})-H(\mathcal{K})} \text{ and } \mathcal{P}_{\mathcal{S}} \geq 2^{H(\mathcal{K}|\mathcal{M}^2)-H(\mathcal{K}|\mathcal{M})}$$

Note that $H(\mathcal{K}|\mathcal{M}^2)$ corresponds to the conditional entropy of $\mathcal{K}$ given that the first 2 messages have been observed.

Also the following bound on $\mathcal{P}_{\mathcal{S}}$ was proved by Brickell in [6].

Theorem 1.2.4. *For any authentication code* $(\mathcal{S}, \mathcal{K}, \mathcal{M}, \mathcal{E})$ *we have*

$$\mathcal{P}_{\mathcal{S}} \geq 2^{H(\mathcal{M})-H(\mathcal{K})-H(\mathcal{S})}$$

1.3 Some Characterizations of Authentication Codes

In this section three important characterizations of authentication codes are presented. First an equivalence of authentication codes with a subclass of universal hash functions is described, then an equivalence with balanced incomplete block designs is given and at the end of this section an equivalence with orthogonal arrays is presented.

Wegman and Carter introduced the concept of universal hashing in 1979 [8]. One of the interesting part of the universal hashing is strongly universal hash functions that are closely related to the systematic authentication codes. A hash family H is a set of $|H|$ functions such that for any $h \in H$ we have a map from the set A to the set B. Consider a hash family $H = \{h|h : A \longrightarrow B\}$.

Definition 1.3.1. A hash family H is called *ϵ-almost strongly universal($\epsilon - ASU$)* if

1. for any $a \in A$ and any $b \in B$, there are exactly $|H|/|B|$ functions $h \in H$ such that $h(a) = b$.
2. for any two distinct elements $a_1, a_2 \in A$, for any two elements $b_1, b_2 \in B$ there are at most $\epsilon|H|/|B|$ functions $h \in H$ such that $h(a_1) = b_1$ and $h(a_1) = b_2$.

The following lemma gives an equivalence between universal hash functions and systematic authentication codes:

Lemma 1.3.2 ([4, 57]). *If there exists a systematic authentication code* $(\mathcal{S}, \mathcal{K}, \mathcal{T}, \mathcal{E})$ *with parameters* $|\mathcal{S}|$, $|\mathcal{K}|$, $\mathcal{P}_{\mathcal{I}} = 1/|\mathcal{T}|$, *and* $\mathcal{P}_{\mathcal{S}}$, *then there exists an* ϵ*-almost strongly universal family of hash functions where* $\epsilon = \mathcal{P}_{\mathcal{S}}$, $|H| = |\mathcal{K}|$, $|A| = |\mathcal{S}|$, *and* $|B| = |\mathcal{T}|$. *Conversely, if there exists an* ϵ*-almost strongly universal family of hash functions, then there exists a systematic authentication code with parameters as above.*

In literature, many authors used this lemma to construct universal hash functions and systematic authentication codes [1, 3, 4, 31, 33, 57, 61, 72, 73].

Now an equivalence of authentication codes and balanced incomplete block designs (BIBD) is presented. First the definition of a BIBD is given. Details for BIBDs can be found in [11].

Definition 1.3.3. A (m, s, λ) balanced incomplete block design, (m, s, λ)-BIBD is a pair (X, A), where X is a set of points with $|X| = m$ and A is a family of k-subsets of X (called blocks) such that every pair of points occurs in exactly λ blocks.

Since each encoding rule is a one-to-one function from $\mathcal{S}$ to $\mathcal{M}$, the authentication code can be represented by a $|\mathcal{K}| \times |\mathcal{S}|$ *encoding matrix*, whose (k, s)-th entry is $E_k(s)$, where the rows are indexed by encoding rules and the columns are indexed by source states. The following equivalence between a BIDB and an authentication code is proved in [62].

Lemma 1.3.4. *Suppose we have an authentication code $(\mathcal{S}, \mathcal{K}, \mathcal{M}, \mathcal{E})$ in which $\mathcal{P}_{\mathcal{I}} = |\mathcal{S}|/|\mathcal{M}|$ and $\mathcal{P}_{\mathcal{S}} = (|\mathcal{S}| - 1)/(|\mathcal{M}| - 1)$. Then $|\mathcal{K}| \geq (|\mathcal{M}|^2 - |\mathcal{M}|)/(|\mathcal{S}|^2 - |\mathcal{S}|)$, and equality occurs if and only if the rows of the encoding matrix (taken as unordered sets) form a $(|\mathcal{M}|, |\mathcal{S}|, 1)$-BIBD, and both the source states and encoding rules are equiprobable.*

Here an equivalence of systematic authentication codes and orthogonal arrays is presented. First the definition of an orthogonal array is given. Details for orthogonal arrays can be found in [30].

Definition 1.3.5. An orthogonal array $OA(t, s, \lambda)$ is a $\lambda t^2 \times s$ array of t symbols, such that in any two columns of the array every one of the possible t^2 pairs of symbol occurs in exactly λ rows.

The following equivalence between orthogonal arrays and systematic authentication codes is proved in [62, 60].

Lemma 1.3.6. *Suppose there exists a systematic authentication code $(\mathcal{S}, \mathcal{K}, \mathcal{T}, \mathcal{E})$ with parameters $|\mathcal{S}|$, $|\mathcal{K}|$, $|\mathcal{T}|$ and $\mathcal{P}_{\mathcal{I}} = \mathcal{P}_{\mathcal{S}} = 1/|\mathcal{T}|$. Then $|\mathcal{K}| \geq |\mathcal{S}|(|\mathcal{T}| - 1) + 1$ and equality holds if and only if there exists an orthogonal array $OA(|\mathcal{T}|, |\mathcal{S}|, \lambda)$, where $\lambda = (|\mathcal{S}|(|\mathcal{T}| - 1) + 1)/|\mathcal{T}|^2$*

1.4 Known Construction Methods of Authentication Codes

In this section some well-known construction methods in the literature are provided. There are several approaches to construct authentication codes with or without secrecy. Main construction methods can be classified as algebraic, combinatoric, geometric and coding theoretic constructions.

The authentication codes developed by Gilbert, MacWilliams and Sloane [27] may be given as the first example of geometric construction methods. In this method, some specific subsets of the points and the lines in projective spaces are used to represent encoding rules and messages. Some other geometric constructions can be found in [2, 23, 24, 69, 70, 74]. In [69, 70] several constructions of systematic authentication codes based on symplectic spaces and unitary geometry over finite fields are presented.

There are many combinatorial constructions of authentication codes, e.g. [25, 26, 41, 47, 48, 59, 60, 61, 62, 63, 64]. In [26] perpendicular arrays are used to construct authentication codes. As explained in Section 1.3 Stinson present characterizations of authentication codes in terms of balanced incomplete block designs in [59, 60, 62]. Also Stinson give a characterization of systematic authentication codes in terms of orthogonal arrays in [62]. Note that these two characterizations give optimal authentication codes, that is, $\mathcal{P}_{\mathcal{I}}$ and $\mathcal{P}_{\mathcal{S}}$ attains its minimum values.

As it is noted in Section 1.3 many algebraic and coding theoretic constructions of universal hash functions and authentication codes are presented in the literature using Lemma 1.3.2. In [4] the concatenation of codes is used to construct authentication codes. Mainly the Reed-Solomon codes and algebraic geometric codes are used in the constructions. Helleseth and Johansson construct authentication codes using exponential sums over finite fields and Galois rings in [31]. In recent years, highly nonlinear functions have been used to construct good and optimal authentication codes in [7, 10, 18, 19]. Also some good authentication codes is constructed using some coding theoretic techniques in [17, 21, 42].

Chapter 2

Some Constructions of Systematic Authentication Codes Using Galois Rings

In this chapter, a coding theory oriented approach is used to construct systematic authentication codes over finite field $\mathbb{F}_q$. Corrections of the construction of [5] are given. Corresponding systematic authentication codes of [31] are generalized in various ways.

2.1 Introduction

Let p be a prime, m, n, l be positive integers and $q = p^m$. Throughout this chapter R denotes the Galois ring $GR(p^l, m)$ of characteristic p^l and cardinality q^l and S denotes $GR(p^l, mn)$ of the same characteristic but cardinality q^{ln}. Our constructions use elements from a suitable space of polynomials or rational functions over S as source states. We form codewords over $R \subseteq S$ by traces of evaluations of these functions on a "regular" subset of Teichmüller set of S. Our constructions differ into two types at this point. In type I, we extend this set of codewords by component wise addition of them with some constant codewords over R (cf. (2.3.1)). In type II, we do not have such an addition. For both types, tags of our systematic authentication codes over finite field $\mathbb{F}_q$ are obtained after generalized Gray map (cf. (2.3.2)).

Our constructions A and B of Section 2.3 are of type I. They corresponds to constructions C and D, respectively, of type II given in Section 2.4. The difference of type I and type II codes appears in estimating the probabilities $\mathcal{P}_{\mathcal{I}}$ and $\mathcal{P}_{\mathcal{S}}$. In general the estimation of $\mathcal{P}_{\mathcal{S}}$ is more difficult than the estimation of $\mathcal{P}_{\mathcal{I}}$. For a type I code, component wise addition with some constant codewords guarantees that $\mathcal{P}_{\mathcal{I}} = 1/q$. For a type II code, the probability $\mathcal{P}_{\mathcal{I}}$ of it is exactly the probability $\mathcal{P}_{\mathcal{S}}$ of the corresponding type I code. Estimation of the probability $\mathcal{P}_{\mathcal{S}}$

of a type II codes is much more difficult.

In [5], Bini gave a construction of type II codes (cf. (2.4.4)). However the estimates of the probabilities $\mathcal{P}_{\mathcal{I}}$ and $\mathcal{P}_{\mathcal{S}}$ are incorrect in [5]. In particular, estimation of $\mathcal{P}_{\mathcal{S}}$ for such codes need more involved machinery.

In this chapter, we give constructions A and B as type I codes in Section 2.3. Construction A is a generalization of [31, Theorem 17] from p-ary to q-ary codes. This generalization would be useful for example to have systematic authentication codes with large $|\mathcal{S}|$ in characteristic 2. Construction B is a generalization of Construction A, which would be considered as a generalization from p-ary to q-ary case of a correction of [5]. We give their type II counterparts as constructions C and D respectively in Section 2.4. The probabilities $\mathcal{P}_{\mathcal{I}}$ and $\mathcal{P}_{\mathcal{S}}$ of Construction D correspond to the correct values of the estimates in [5]. Estimating the probability $\mathcal{P}_{\mathcal{S}}$ of constructions C and D is much more involved and we use some tools from [39] and assume that $q = p$ for simplicity. We also give some generalizations to Galois ring of arbitrary characteristic and a nonexistence result in Section 2.5.

2.2 Algebraic Background

In this section, we recall some definitions and basic results. For $t \geq 1$, let $GR(p^l, t)$ the Galois ring of characteristic p^l and cardinality p^{lt}, which is a local ring having unique maximal ideal $pGR(p^l, t)$. The group of units of the Galois ring $GR(p^l, t)$ contains a unique cyclic group of order $p^t - 1$. If ξ is a generator of this group, the set

$$\tau(GR(p^l, t)) = \{0, 1, \xi, \cdots, \xi^{p^t-2}\}$$

is called the Teichmüller set of $GR(p^l, t)$.

For any Galois ring $GR(p^l, t)$ the trace map can be defined as follows

$$\begin{array}{rcl} \mathrm{Tr}_t : GR(p^l, t) & \longrightarrow & \mathbb{Z}_{p^l} \\ \sum_{i=0}^{l-1} p^i r_i & \longmapsto & \sum_{i=0}^{l-1} (r_i + r_i^p + \cdots + r_i^{p^{t-1}}) p^i. \end{array}$$

Recall that R and S correspond to $GR(p^l, m)$ and $GR(p^l, mn)$ respectively. First we define the generalized Gray map from R into $(\mathbb{F}_q)^{q^{l-1}}$ and relate it to some exponential sums ([28]). We begin with some simple but useful lemmas.

Lemma 2.2.1. *For any $u \in R$ we have*

$$\sum_{x \in R} e^{2\pi i \frac{\mathrm{Tr}_m(ux)}{p^l}} = \begin{cases} q^l, & \text{if } u = 0 \\ 0, & \text{otherwise.} \end{cases}$$

Proof. The case $u = 0$ is trivial. For $u \neq 0$, as the trace map is surjective ([68, Theorem 14.37]), there exists $y \in R$ s.t. $\mathrm{Tr}_m(uy) \neq 0$. Then we have

$$\sum_{x\in R} e^{2\pi i \frac{\mathrm{Tr}_m(ux)}{p^l}} = \sum_{x+y\in R} e^{2\pi i \frac{\mathrm{Tr}_m(u(x+y))}{p^l}} = e^{2\pi i \frac{\mathrm{Tr}_m(uy)}{p^l}} \sum_{x\in R} e^{2\pi i \frac{\mathrm{Tr}_m(ux)}{p^l}}.$$

As $1 - e^{2\pi i \frac{\mathrm{Tr}_m(uy)}{p^l}} \neq 0$, we get $\sum_{x\in R} e^{2\pi i \frac{\mathrm{Tr}_m(ux)}{p^l}} = 0$. □

Lemma 2.2.2. *For any $u \in R$ we have*

$$\sum_{x\in pR} e^{2\pi i \frac{\mathrm{Tr}_m(ux)}{p^l}} = \begin{cases} q^{l-1}, & \text{if } u \in p^{l-1}R \\ 0, & \text{if } u \in R\backslash p^{l-1}R. \end{cases}$$

Proof. Again the case $u \in p^{l-1}R$ is trivial. For $u \in R\backslash p^{l-1}R$, the surjectivity of the trace map also implies the existence of $y \in p^{l-1}R$ s.t. $\mathrm{Tr}_m(uy) \neq 0$. We complete the proof similarly as in the proof of Lemma 2.2.1. □

Combining Lemma 2.2.1 and Lemma 2.2.2 we get the following result.

Lemma 2.2.3. *For any $u \in R$ we have*

$$\sum_{x\in R\backslash pR} e^{2\pi i \frac{\mathrm{Tr}_m(ux)}{p^l}} = \begin{cases} q^l - q^{l-1}, & \text{if } u = 0 \\ -q^{l-1}, & \text{if } u \in p^{l-1}R\backslash\{0\} \\ 0, & \text{if } u \in R\backslash p^{l-1}R. \end{cases}$$

We are ready to define the homogeneous weight on R, which extends [12].

Definition 2.2.4. For $u \in R$, let

$$s(u) := \sum_{x\in R\backslash pR} e^{2\pi i \frac{\mathrm{Tr}_m(ux)}{p^l}} \text{ and } w(u) := -\frac{1}{q}s(u) + (q^{l-1} - q^{l-2}).$$

For any $u \in R$, using the above definition and Lemma 2.2.3, we have

$$w(u) = \begin{cases} 0, & \text{if } u = 0 \\ q^{l-1}, & \text{if } u \in p^{l-1}R\backslash\{0\} \\ q^{l-1} - q^{l-2}, & \text{if } u \in R\backslash p^{l-1}R. \end{cases}$$

Let μ be the projection map onto the residue field of $GR(p^2, m)$ defined as

$$\begin{aligned} \mu : GR(p^2, m) &\longrightarrow GR(p^2, m)/pGR(p^2, m) \cong \mathbb{F}_q \\ u &\longmapsto \overline{u} := u + pGR(p^2, m). \end{aligned}$$

Note that μ is a ring homomorphism. The following lemma is clear from the definition of the projection map.

Lemma 2.2.5. *For any $r, s \in \tau(GR(p^2, m))$, if $\mu(r) = \mu(s)$ then $r = s$.*

Using the projection map μ we can define the generalized Gray map.

Definition 2.2.6 (Generalized Gray Map).

$$\begin{aligned} \phi : GR(p^2, m) &\longrightarrow (\mathbb{F}_q)^q \\ (r_0 + pr_1) &\longmapsto (\overline{r_1}, \overline{r_1 + \eta r_0}, \overline{r_1 + \eta^2 r_0}, \cdots, \overline{r_1 + \eta^{q-1} r_0}), \end{aligned}$$

where $< \eta >= \tau(GR(p^2, m)) \backslash \{0\}$.

Lemma 2.2.7. *The generalized Gray map ϕ is an injection.*

Proof. For any $r, s \in GR(p^2, m)$ with $r = r_0 + pr_1$ and $s = s_0 + ps_1$, if $\phi(r_0 + pr_1) = \phi(s_0 + ps_1)$ then in particular $\overline{r_1} = \overline{s_1}$. As μ is a ring homomorphism, using $\overline{r_1 + \eta r_0} = \overline{s_1 + \eta s_0}$ we get $\overline{\eta r_0} = \overline{\eta s_0}$ and hence $\overline{r_0} = \overline{s_0}$. We complete the proof using the fact that μ is one to one on $\tau(GR(p^2, m))$. □

Note in general that the Definition 2.2.6 is generalized in [28] for Galois rings of arbitrary characteristics. From now on ϕ will denote the Gray map on $GR(p^l, m)$, which reduces to Definition 2.2.6 when the characteristic is p^2. For any $r_1, r_2 \in GR(p^l, m)$ we have $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$.

To calculate the probability $\mathcal{P}_{\mathcal{S}}$ of our systematic authentication codes of type I we need the distance between a codeword and any constant vector. For any $k \geq 1$ and $\underline{c}, \underline{r} \in {\mathbb{F}_q}^k$, let $d_H(\underline{c}, \underline{r})$ denote the number of different coordinates between $\underline{c}$ and $\underline{r}$. Also it is clear from the definition of ϕ that for any $\underline{r} = (t, t, \ldots, t) \in (\mathbb{F}_q)^{q^{l-1}}$ we have a unique $r \in p^{l-1}R$ such that $\phi(r) = \underline{r}$. Using Lemma 2.2.7 we obtain the following result.

Lemma 2.2.8. *Let $\underline{r} = (t, t, \ldots, t) \in (\mathbb{F}_q)^{q^{l-1}}$ s.t. $\phi(r) = \underline{r}$ and $u \in R$. Then the following holds:*

$$d_H(\phi(u), \underline{r}) = \begin{cases} 0, & \text{if } u - r = 0 \\ q^{l-1}, & \text{if } u - r \in p^{l-1}R \backslash \{0\} \\ q^{l-1} - q^{l-2}, & \text{if } u - r \in R \backslash p^{l-1}R. \end{cases}$$

Corollary 2.2.9. *For any $u \in R$ and $r \in p^{l-1}R$, we have $w(u - r) = d_H(\phi(u), \phi(r))$.*

The *relative trace map* $\mathrm{Tr}_{S/R} : S \to R$ sends $(a_0 + pa_1 + \cdots + p^{l-1}a_{l-1}) \in S$ to $\sum_{i=0}^{l-1} p^i (a_i^q + a_i^{q^2} + \cdots + a_i^{q^{n-1}}) \in R$.

We note that for any $(a_0 + pa_1 + \cdots + p^{l-1}a_{l-1}) \in S$,

$$\mathrm{Tr}_{nm}(a_0 + pa_1 + \cdots + p^{l-1}a_{l-1}) = \mathrm{Tr}_m(\mathrm{Tr}_{S/R}(a_0 + pa_1 + \cdots + p^{l-1}a_{l-1})). \tag{2.2.1}$$

The *Frobenious automorphism* $\sigma : S \to S$ sending $(a_0 + pa_1 + \cdots + p^{l-1}a_{l-1})$ to $(a_0{}^p + pa_1{}^p + \cdots + p^{l-1}a_{l-1}{}^p))$ is a ring automorphism of S fixing $\mathbb{Z}_{p^l}$. We will say that $f(x) \in S[x]$ is nondegenerate when it is not expressible of the form $f(x) = \sigma(g(x)) - g(x) + \beta \ (mod\ p^l)$, for any $g(x) \in S[x]$, $\beta \in S$. Here $\sigma(g(x)) = \sigma(\sum_i g_i x^i) = \sum_i \sigma(g_i)x^{pi}$. Also the weighted degree of the function $f(x) \in S[x]$ is defined as $D = max\{d_0 p^{l-1}, d_1 p^{l-2}, \ldots, d_{l-1}\}$ where $f(x) = f_0(x) + pf_1(x) + \cdots + p^{l-1}f_{l-1}(x)$, $f_0, \ldots, f_{l-1} \in \tau(S)[x]$ and $\deg(f_i) = d_i$, $i = 0, \ldots, l-1$ [35]. Define $\mathcal{F}_\mathcal{D}$ to be the subset of nondegenerate polynomials of weighted degree $D \leq \sqrt{q^n}$ as

$$\mathcal{F}_D = \{f(x) : f(x) = f_0(x) + pf_1(x) + \cdots + p^{l-1}f_{l-1}(x) \in S[x],\ f_i = 0 \ whenever\ p|i\}.$$

We know that $|\mathcal{F}_\mathcal{D}| = q^{n(D-\lfloor D/p^l \rfloor)}$. The following important results are very useful.

Proposition 2.2.10 ([35]). *Let $f(x) \in S[x]$ be non-degenerate, then we have*

$$\left| \sum_{\alpha \in \tau(S)} e^{2\pi i \frac{\mathrm{Tr}_{mn}(f(\alpha))}{p^l}} \right| \leq (D-1)\sqrt{q^n}$$

where D is the weighted degree of f.

Proposition 2.2.11 ([32]). *Let $f \in S(x)\backslash\{0\}$ have expansion $f = ax + \sum_{i=1}^{N} \frac{b_i}{x-p_i}$, where $a, b_i \in S$ and $P = \{p_1, \ldots, p_N\} \subset \tau(S)$, then we have*

$$\left| \sum_{\alpha \in \tau(S)\backslash P} e^{2\pi i \frac{\mathrm{Tr}_{mn}(f(\alpha))}{p^l}} \right| \leq (p^{l-1}(N+1) + N - 1)\sqrt{q^n}.$$

Define $\mathcal{G}_\mathcal{N}$ as the following set of rational functions in $S(x)$

$$\{f \in S(x) : f = ax + \sum_{i=1}^{N} \frac{b_i}{x-p_i},\ where\ a, b_i \in S\ and\ P = \{p_1, \ldots, p_N\} \subset \tau(S)\}.$$

Also define $\tau(S)\backslash P = \{\alpha_1, \ldots, \alpha_{q^n - N}\}$.

Remark 2.2.12. Assume that $q^n - N > (p^{l-1}(N+1) + N - 1)\sqrt{q^n}$. Then $|\mathcal{G}_\mathcal{N}| = q^{ln(N+1)}$.

Proof. The proof is very similar to the proof in [5]. Define a linear map

$$\begin{aligned} \Psi : S^{(N+1)} &\to \mathbb{Z}_{p^l}^{(q^n-N)} \\ (a, b_1, \ldots, b_N) &\mapsto \left(\mathrm{Tr}_{mn}(ax + \sum_{i=1}^{N} \frac{b_i}{x-p_i})_{x \in \tau(S)\backslash P} \right). \end{aligned}$$

If $\Psi(a, b_1, \ldots, b_N) = 0$ and $f = ax + \sum_{i=1}^{N} \frac{b_i}{x-p_i} \neq 0$, then

$$q^n - N = \left| \sum_{\alpha \in \tau(S)\backslash P} e^{2\pi i \frac{\mathrm{Tr}_{mn}(f(\alpha))}{p^l}} \right| \leq (p^{l-1}(N+1) + N - 1)\sqrt{q^n}$$

which contradicts the assumption. Therefore Ψ is one to one, which completes the proof. □

2.3 Constructions of Type I

In this section, we give constructions A and B. Construction A is a generalization of [31, Theorem 17] from p-ary to q-ary codes. Construction B is a correct generalization of construction A to rational functions. Also we assume that $l = 2$ and hence R and S are of characteristic p^2.

2.3.1 Construction A

For any $f(x) \in S[x]$ and $\{\beta_1, \ldots, \beta_q\} = pR$, a corresponding codeword $c_f \in R^{(q^{n+1})}$ is

$$c_f = \left[c_{f,\beta_1}, c_{f,\beta_2}, \cdots, c_{f,\beta_q}\right] \tag{2.3.1}$$

where $c_{f,\beta_i} = \left[\beta_i + \mathrm{Tr}_{S/R}(f(0)), \beta_i + \mathrm{Tr}_{S/R}(f(\xi)), \cdots, \beta_i + \mathrm{Tr}_{S/R}(f(\xi^{q^n-1}))\right]$ for $i = 1, \ldots, q$ and $< \xi >= \tau(S)\backslash\{0\}$.

Applying the generalized Gray map to the above codeword c_f, we obtain the following codeword in ${\mathbb{F}_q}^{(q \cdot q^{n+1})} = {\mathbb{F}_q}^{(q^{n+2})}$

$$\underline{u_f} = \left[u_{f,\beta_1}, u_{f,\beta_2}, \cdots, u_{f,\beta_q}\right] \tag{2.3.2}$$

where $u_{f,\beta_i} = \left[\phi(\beta_i) + \phi(\mathrm{Tr}_{S/R}(f(0))), \cdots, \phi(\beta_i) + \phi(\mathrm{Tr}_{S/R}(f(\xi^{q^n-1})))\right]$ for $i = 1, \ldots, q$.

Let pr_i be the projection map from ${\mathbb{F}_q}^{(q^{n+2})}$ to $\mathbb{F}_q$ sending $\underline{u_f}$ to its i-th coordinate. Using the codewords in (2.3.2) the systematic authentication code is defined by

$$\begin{cases} \mathcal{S} = & \mathcal{F}_{\mathcal{D}} \\ \mathcal{T} = & \mathbb{F}_q \\ \mathcal{K} = & \mathbb{Z}_{q^{n+2}} \\ \mathcal{E} = & \{E_k : E_k(f) = pr_k(\underline{u_f})\} \end{cases} \tag{2.3.3}$$

where $k \in \mathcal{K}$ and $f \in \mathcal{S}$.

The following lemma is useful to obtain an upper bound on the probability $\mathcal{P}_{\mathcal{S}}$.

Lemma 2.3.1. *Let $f \in \mathcal{F}_{\mathcal{D}}$ and $\underline{r} = (\phi(r), \ldots, \phi(r)) \in {\mathbb{F}_q}^{(q^{n+1})}$ such that $r \in pR$, then for any $\beta \in pR$, we have*

$$d_H(u_{f,\beta}, \underline{r}) \geq q^n(q-1) - (q-1)(D-1)\sqrt{q^n},$$

$$d_H(u_{f,\beta}, \underline{r}) \leq q^n(q-1) + (q-1)(D-1)\sqrt{q^n}.$$

Proof. Using Corollary 2.2.9, we get

$$\begin{aligned}
d_H(u_{f,\beta},\underline{r}) &= \sum_{\alpha\in\tau(S)} w(\beta+\mathrm{Tr}_{S/R}(f(\alpha))-r)\\
&= \sum_{\alpha\in\tau(S)} \{-\frac{1}{q}s(\mathrm{Tr}_{S/R}(f(\alpha))-r)+(q-1)\}\\
&= q^n(q-1)-\frac{1}{q}\sum_{\alpha\in\tau(S)}\{s(\mathrm{Tr}_{S/R}(f(\alpha))-r)\}\\
&= q^n(q-1)-\frac{1}{q}\sum_{\alpha\in\tau(S)}\sum_{r'\in R\setminus pR} e^{2\pi i\frac{\mathrm{Tr}_m((\mathrm{Tr}_{S/R}(f(\alpha))-r)r')}{p^2}}\\
&= q^n(q-1)-\frac{1}{q}\sum_{\alpha\in\tau(S)}\sum_{r'\in R\setminus pR} e^{2\pi i\frac{\mathrm{Tr}_m(r'\mathrm{Tr}_{S/R}(f(\alpha)))-\mathrm{Tr}_m(r'r)}{p^2}}\\
&= q^n(q-1)-\frac{1}{q}\sum_{\alpha\in\tau(S)}\sum_{r'\in R\setminus pR} e^{2\pi i\frac{\mathrm{Tr}_m(r'\mathrm{Tr}_{S/R}(f(\alpha)))-\mathrm{Tr}_m(r'r)}{p^2}}\\
&= q^n(q-1)-\frac{1}{q}\sum_{r'\in R\setminus pR} e^{2\pi i\frac{-\mathrm{Tr}_m(r'r)}{p^2}}\sum_{\alpha\in\tau(S)} e^{2\pi i\frac{\mathrm{Tr}_{mn}(r'f(\alpha))}{p^2}},\ \text{by using (2.2.1).}
\end{aligned}$$

Then using Proposition 2.2.10 we get

$$|q^n(q-1)-d_H(u_{f,\beta},\underline{r})|\le\frac{1}{q}(q^2-q)(D-1)\sqrt{q^n}.$$

The conclusion of the lemma then follows. □

Proposition 2.3.2. *The systematic authentication code in (2.3.3) has the following parameters:*

$$|\mathcal{S}|=q^{n(D-\lfloor D/p^2\rfloor)},\ |\mathcal{K}|=q^{n+2},\ |\mathcal{T}|=q,\ \mathcal{P}_{\mathcal{I}}=\frac{1}{q},\ \textit{and}$$

$$\mathcal{P}_{\mathcal{S}}\le\frac{1}{q}+\frac{(q-1)}{q}\cdot\frac{(D-1)}{\sqrt{q^n}}.$$

Proof. For any message $f\in\mathcal{S}=\mathcal{F}_{\mathcal{D}}$ and key $k\in\mathbb{Z}_{q^{n+2}}$ by (1.1.3) we have

$$\mathcal{P}_{\mathcal{I}} = max_{f,t}\frac{|\{k\in\mathcal{K}:t=pr_k(\underline{u_f})\}|}{|\{k\in\mathcal{K}\}|}=\frac{1}{q},$$

since for each $\alpha\in\tau(S)$, the k-th coordinate of $\phi(\beta_i)+\phi(\mathrm{Tr}_{S/R}(f(\alpha)))$ and the k-th coordinate of $\phi(\beta_j)+\phi(\mathrm{Tr}_{S/R}(f(\alpha)))$ are different for $\beta_i\neq\beta_j$.

For any $\beta\in pR$ and $\underline{t}=(t,t,\ldots,t)\in\mathbb{F}_q{}^{(q^{n+1})}$, using Lemma 2.3.1 we know that $d_H(u_{f,\beta},\underline{t})\ge q^n(q-1)-(q-1)(D-1)\sqrt{q^n}$. Then using By (1.1.4) we get

$$\begin{aligned}
\mathcal{P}_{\mathcal{S}} &= max_{f,t} max_{f' \neq f,t'} \frac{|\{k \in \mathcal{K} : t = pr_k(\underline{u_f}), t' = pr_k(\underline{u_{f'}})\}|}{|\{k \in \mathcal{K} : t = pr_k(\underline{u_f})\}|} \\
&= max_{f,t} max_{f' \neq f,t'} \frac{|\{k \in \mathcal{K} : t = pr_k(\underline{u_f}), t - t' = pr_k(\underline{u_f} - \underline{u_{f'}})\}|}{q^{n+1}} \\
&= max_{f \neq 0,t} \frac{|\{\alpha \in \tau(S) : t = pr_k(u_{f,\beta})\}|}{q^{n+1}} \\
&= max_{f \neq 0,t} \frac{q^{n+1} - d_H(u_{f,\beta}, \underline{t})}{q^{n+1}} \\
&\leq \frac{1}{q} + \frac{(q-1)}{q} \cdot \frac{(D-1)}{\sqrt{q^n}}.
\end{aligned}$$

The remaining conclusions of this theorem are clear. □

Remark 2.3.3. Proposition 2.3.2 is a generalization of [31, Theorem 17] from p-ary to q-ary case. In the estimate of $\mathcal{P}_{\mathcal{S}}$, $\frac{(D-1)}{\sqrt{q^n}}$ is multiplied by $\frac{(q-1)}{q}$. This does not appear in [31, Theorem 17], however this multiplication exists in the proof of [31, Lemma 15]. Moreover, our estimate of $\mathcal{P}_{\mathcal{S}}$, which uses Lemma 2.3.1, is better than that of [31, Theorem 17], since we do not have the extra term $min(\frac{1}{p^2}, \frac{(D-1)}{\sqrt{p^n}})$ that [31, Theorem 17] has.

2.3.2 Construction B

In this section, we use the same technique as in the previous construction, but instead of nondegenerate polynomials we use rational functions in $S(x)$.

For any $f \in \mathcal{G}_{\mathcal{N}}$ and $\{\beta_1, \ldots, \beta_q\} = pR$, we have a corresponding codeword in $R^{q(q^n-N)}$

$$c_f = \left[c_{f,\beta_1}, c_{f,\beta_2}, \cdots, c_{f,\beta_q}\right]$$

where $c_{f,\beta_i} = \left[\beta_i + \mathrm{Tr}_{S/R}(f(\alpha_1)), \beta_i + \mathrm{Tr}_{S/R}(f(\alpha_2)), \cdots, \beta_i + \mathrm{Tr}_{S/R}(f(\alpha_{q^n-N}))\right]$ for $i = 1, \ldots, q$.

Applying the generalized Gray map to the above codeword c_f, we obtain the following codeword in $\mathbb{F}_q{}^{(q^2(q^n-N))}$

$$\underline{u_f} = \left[u_{f,\beta_1}, u_{f,\beta_2}, \cdots, u_{f,\beta_q}\right] \tag{2.3.4}$$

where $u_{f,\beta_i} = \left[\phi(\beta_i) + \phi(\mathrm{Tr}_{S/R}(f(\alpha_1))), \cdots, \phi(\beta_i) + \phi(\mathrm{Tr}_{S/R}(f(\alpha_{q^n-N})))\right]$ for $i = 1, \ldots, q$.

Let pr_i be the projection map from $\mathbb{F}_q{}^{(q^2(q^n-N))}$ to $\mathbb{F}_q$ sending $\underline{u_f}$ to its i-th coordinate. Using the codewords in (2.3.4) and assuming $q^n - N > (p(N+1) + N - 1)\sqrt{q^n}$ the systematic authentication code is defined by

$$\begin{cases}
\mathcal{S} = & \mathcal{G}_{\mathcal{N}} \\
\mathcal{T} = & \mathbb{F}_q \\
\mathcal{K} = & \mathbb{Z}_{q^2(q^n-N)} \\
\mathcal{E} = & \{E_k : E_k(f) = pr_k(\underline{u_f})\}
\end{cases} \tag{2.3.5}$$

where $k \in \mathcal{K}$ and $f \in \mathcal{S}$.

The following lemma is useful to obtain an upper bound on the probability $\mathcal{P}_{\mathcal{S}}$.

Lemma 2.3.4. *Let $f \in \mathcal{G}_{\mathcal{N}}$ and $\underline{r} = (\phi(r), \ldots, \phi(r)) \in \mathbb{F}_q{}^{(q(q^n-N))}$ such that $r \in pR$, then for any $\beta \in pR$, we have*

$$d_H(u_{f,\beta}, \underline{r}) \geq (q^n - N)(q-1) - (q-1)(p(N+1)+N-1)\sqrt{q^n},$$

$$d_H(u_{f,\beta}, \underline{r}) \leq (q^n - N)(q-1) + (q-1)(p(N+1)+N-1)\sqrt{q^n}.$$

Proof. Again using Corollary 2.2.9 and similar to the proof of Lemma 2.3.1 we get

$$\begin{aligned} d_H(u_{f,\beta}, \underline{r}) &= \sum_{\alpha \in \tau(S)\setminus P} w(\beta + \mathrm{Tr}_{S/R}(f(\alpha)) - r) \\ &= (q^n - N)(q-1) - \frac{1}{q} \sum_{r' \in R \setminus pR} e^{2\pi i \frac{-\mathrm{Tr}_m(r'r)}{p^2}} \sum_{\alpha \in \tau(S)\setminus P} e^{2\pi i \frac{\mathrm{Tr}_{mn}(r'f(\alpha))}{p^2}}. \end{aligned}$$

Then using Proposition 2.2.11 we get

$$|(q^n - N)(q-1) - d_H(u_{f,\beta}, \underline{r})| \leq \frac{1}{q}(q^2 - q)(p(N+1)+N-1)\sqrt{q^n}.$$

The conclusion of the lemma then follows. □

Proposition 2.3.5. *The systematic authentication code in (2.3.5) has the following parameters:*

$$|\mathcal{S}| = q^{2n(N+1)},\ |\mathcal{K}| = q^2(q^n - N),\ |\mathcal{T}| = q,\ \mathcal{P}_{\mathcal{I}} = \frac{1}{q},\ \textit{and}$$

$$\mathcal{P}_{\mathcal{S}} \leq \frac{1}{q} + \frac{(q-1)}{q} \cdot \frac{(p(N+1)+N-1)\sqrt{q^n}}{q^n - N}.$$

Proof. Similarly as in the proof of Proposition 2.3.2, it can be shown that $\mathcal{P}_{\mathcal{I}} = \frac{1}{q}$. Using Lemma 2.3.4 with $\underline{t} = (t, t, \ldots, t) \in \mathbb{F}_q{}^{(q(q^n-N))}$ and (1.1.4) one obtains

$$\begin{aligned} \mathcal{P}_{\mathcal{S}} &= max_{f \neq 0, t} \frac{q(q^n - N) - d_H(u_{f,\beta}, \underline{t})}{q(q^n - N)} \\ &\leq \frac{1}{q} + \frac{(q-1)}{q} \cdot \frac{(p(N+1)+N-1)\sqrt{q^n}}{q^n - N}. \end{aligned}$$

The remaining conclusions of this theorem are clear. □

2.4 Constructions of Type II

In this section, we give counterparts of the constructions A and B as constructions C and D respectively. Again we assume that the characteristics of the Galois rings R and S are p^2.

2.4.1 Construction C

In this section we analyze the properties of the following code for the case $q = p$ a prime. For any $f(x) \in S[x]$, a corresponding codeword $c_f \in R^{p^n}$ is

$$c_f = \left[\mathrm{Tr}_{S/R}(f(0)), \mathrm{Tr}_{S/R}(f(\xi)), \cdots, \mathrm{Tr}_{S/R}(f(\xi^{p^n-1}))\right]$$

where $< \xi >= \tau(S)\backslash\{0\}$.

Applying the generalized Gray map to the above codeword c_f, we obtain the following codeword in $\mathbb{F}_p{}^{(p\cdot p^n)} = \mathbb{F}_p{}^{(p^{n+1})}$

$$\underline{u_f} = \left[\phi(\mathrm{Tr}_{S/R}(f(0))), \phi(\mathrm{Tr}_{S/R}(f(\xi))), \cdots, \phi(\mathrm{Tr}_{S/R}(f(\xi^{p^n-1})))\right]. \tag{2.4.1}$$

Here we classify the functions in $\mathcal{F}_\mathcal{D}$ into $|\mathcal{F}_\mathcal{D}|/(p-1)$ equivalent classes, where two functions are in the same class if and only if they are constant multiple of each other (i.e. $f_1 = \lambda f_2$, for some $\lambda \in F_p^*$). By taking only one function from each classes we define the set $\mathcal{F}'_\mathcal{D}$. Let pr_i be the projection map from $\mathbb{F}_p{}^{(p^{n+1})}$ to $\mathbb{F}_p$ sending $\underline{u_f}$ to its i-th coordinate. Using the codewords in (2.4.1) the systematic authentication code is defined by

$$\begin{cases} \mathcal{S} = & \mathcal{F}'_\mathcal{D} \\ \mathcal{T} = & \mathbb{F}_p \\ \mathcal{K} = & \mathbb{Z}_{p^{n+1}} \\ \mathcal{E} = & \{E_k : E_k(f) = pr_k(\underline{u_f})\} \end{cases} \tag{2.4.2}$$

where $k \in \mathcal{K}$ and $f \in \mathcal{S}$.

We need the following definition and lemmas to calculate an upper bound on the probability $\mathcal{P}_\mathcal{S}$ of the code.

Definition 2.4.1 ([39]). For $\omega = e^{\frac{2\pi i}{p^2}}$, $\theta = 1/\omega$ and $0 \le l \le p-1$, let a_{1+lp} be the complex number given by

$$a_{1+lp} = \frac{1}{p}\{1 + \theta^{1+lp} + \theta^{2(1+lp)} + \cdots + \theta^{(p-1)(1+lp)}\}.$$

Lemma 2.4.2 ([39]). *For $x \in \mathbb{Z}_{p^2}$ we have*

$$e^{\frac{2\pi i}{p}\rho_1(x)} = \sum_{l=0}^{p-1} a_{1+lp}\, e^{\frac{2\pi i}{p^2}(1+lp)x},$$

where $\rho_1 : \mathbb{Z}_{p^2} \to \mathbb{F}_p$ is the map sending $r_0 + pr_1$ with $0 \le r_0, r_1 \le p-1$ to r_1.

Lemma 2.4.3. *Let f_1 and f_2 be two distinct elements of $\mathcal{F}'_\mathcal{D}$ and let $t_1, t_2 \in \mathbb{F}_p$, $i = 1, \ldots, p$. Define $N(f_1, f_2, t_1, t_2, i) = |\{\alpha \in \tau(S) : pr_i(\phi(\mathrm{Tr}_{S/R}(f_1(\alpha)))) = t_1,\ pr_i(\phi(\mathrm{Tr}_{S/R}(f_2(\alpha)))) = t_2\}|$. Then*

$$N(f_1, f_2, t_1, t_2, i) \le \frac{1}{p^2}[p^n + (p^2-1)(D-1)\sqrt{p^n}]\left|\sum_{l=0}^{p-1} a_{1+lp}\right|.$$

Proof. Using the definition of the Gray map and the map ρ_1, we have seen that

$$N(f_1, f_2, t_1, t_2, 1) = |\{\alpha \in \tau(S) : \rho_1(\mathrm{Tr}_{S/R}(f_1(\alpha))) = t_1,\ \rho_1(\mathrm{Tr}_{S/R}(f_2(\alpha))) = t_2, \}|$$

and for $1 < i \leq p$,

$$N(f_1, f_2, t_1, t_2, i) = |\{\alpha \in \tau(S) : \rho_1(\mathrm{Tr}_{S/R}(f_1(\alpha))(1+p\alpha^i)) = t_1,\ \rho_1(\mathrm{Tr}_{S/R}(f_2(\alpha))(1+p\alpha^i)) = t_2\}|.$$

Here we prove for the case $i > 1$ only and it is easy to prove the case $i = 1$ similarly.

We know that $p^2 N(f_1, f_2, t_1, t_2, i)$

$$\begin{aligned}
&= \sum_{\alpha\in\tau(S)} \sum_{y_1\in\mathbb{F}_p} \sum_{y_2\in\mathbb{F}_p} e^{\frac{2\pi i}{p}[y_1(\rho_1(\mathrm{Tr}_{S/R}(f_1(\alpha))(1+p\alpha^i))-t_1)+y_2(\rho_1(\mathrm{Tr}_{S/R}(f_2(\alpha))(1+p\alpha^i))-t_2)]} \\
&= \sum_{\alpha\in\tau(S)} \sum_{y_1\in\mathbb{F}_p} \sum_{y_2\in\mathbb{F}_p} e^{\frac{2\pi i}{p}[\rho_1\{(1+p\alpha^i)(y_1\mathrm{Tr}_{S/R}(f_1(\alpha))+y_2\mathrm{Tr}_{S/R}(f_2(\alpha)))-p(y_1t_1+y_2t_2)\}]} \\
&= \sum_{\alpha\in\tau(S)} \sum_{y_1\in\mathbb{F}_p} \sum_{y_2\in\mathbb{F}_p} \\
&\quad \sum_{l=0}^{p-1} a_{1+lp}\ e^{\frac{2\pi i}{p^2}[(1+lp)\{(1+p\alpha^i)(y_1\mathrm{Tr}_{S/R}(f_1(\alpha))+y_2\mathrm{Tr}_{S/R}(f_2(\alpha)))-p(y_1t_1+y_2t_2)\}]} \\
&= \sum_{y_1\in\mathbb{F}_p} \sum_{y_2\in\mathbb{F}_p} \sum_{l=0}^{p-1} a_{1+lp} \\
&\quad \sum_{\alpha\in\tau(S)} e^{\frac{2\pi i}{p^2}[(1+lp)\{(1+p\alpha^i)(y_1\mathrm{Tr}_{S/R}(f_1(\alpha))+y_2\mathrm{Tr}_{S/R}(f_2(\alpha)))-p(y_1t_1+y_2t_2)\}]} \\
&\leq [p^n + (p^2-1)(D-1)\sqrt{p^n}] \left|\sum_{l=0}^{p-1} a_{1+lp}\right|.
\end{aligned}$$

The conclusion of the lemma then follows. □

Remark 2.4.4. Let p be a prime. Then we have $\left|\sum_{l=0}^{p-1} a_{1+lp}\right| = 1$.

Proposition 2.4.5. *The systematic authentication code in (2.4.2) has the following parameters for a prime p,*

$$|\mathcal{S}| = \frac{p^{n(D-\lfloor D/p^2 \rfloor)}}{p-1},\ |\mathcal{K}| = p^{n+1},\ |\mathcal{T}| = p,$$

$$\mathcal{P}_{\mathcal{I}} \leq \frac{1}{p} + \frac{(p-1)}{p} \cdot \frac{(D-1)}{\sqrt{p^n}},\ \textit{and}\ \mathcal{P}_{\mathcal{S}} \leq \frac{1}{p} + \frac{(p^2+p-2)(D-1)}{p(\sqrt{p^n} - (p-1)(D-1))}.$$

Proof. For any message $f \in \mathcal{S} = \mathcal{F}'_{\mathcal{D}}$ and key $k \in \mathbb{Z}_{p^{n+1}}$ by using (1.1.3) and Lemma 2.3.1 we get

$$\mathcal{P}_{\mathcal{I}} \quad = \quad max_{f,t} \frac{|\{k \in \mathcal{K} : t = pr_k(\underline{u_f})\}|}{|\{k \in \mathcal{K}\}|} \leq \frac{1}{p} + \frac{(p-1)}{p} \cdot \frac{(D-1)}{\sqrt{p^n}}.$$

By using (1.1.4), Lemma 2.3.1 and Lemma 2.4.3 we have

$$\begin{aligned}\mathcal{P}_{\mathcal{S}} &= max_{f,t} max_{f' \neq f,t'} \frac{|\{k \in \mathcal{K} : t = pr_k(\underline{u_f}), t' = pr_k(\underline{u_{f'}})\}|}{|\{k \in \mathcal{K} : t = pr_k(\underline{u_f})\}|} \\ &\leq \frac{1}{p} + \frac{(p^2+p-2)(D-1)}{p(\sqrt{p^n} - (p-1)(D-1))}.\end{aligned}$$

The remaining conclusions of this theorem are clear. □

2.4.2 Construction D

In this section, we give the generalization of the authentication codes in [5] from p-ary to q-ary codes and we calculate the correct parameters of the codes and also by restricting the source space as in the previous construction we improve the parameters of the codes for $q = p$ a prime. Recall that $\tau(S) \backslash P = \{\alpha_1, \ldots, \alpha_{q^n - N}\}$.

For any $f \in \mathcal{G}_{\mathcal{N}}$ we have a corresponding codeword in $R^{(q^n - N)}$

$$c_f = \left[\mathrm{Tr}_{S/R}(f(\alpha_1)), \mathrm{Tr}_{S/R}(f(\alpha_2)), \cdots, \mathrm{Tr}_{S/R}(f(\alpha_{q^n-N}))\right].$$

Applying the generalized Gray map to the above codeword c_f, we obtain the following codeword in $\mathbb{F}_q{}^{(q(q^n-N))}$

$$\underline{u_f} = \left[\phi(\mathrm{Tr}_{S/R}(f(\alpha_1))), \cdots, \phi(\mathrm{Tr}_{S/R}(f(\alpha_{q^n-N})))\right]. \tag{2.4.3}$$

Let pr_i be the projection map from $\mathbb{F}_q{}^{(q(q^n-N))}$ to $\mathbb{F}_q$ sending $\underline{u_f}$ to its i-th coordinate. Using the codewords in (2.4.3) and assuming $q^n - N > (p(N+1) + N - 1)\sqrt{q^n}$ the systematic authentication code is defined by

$$\begin{cases} \mathcal{S} = & \mathcal{G}_{\mathcal{N}} \\ \mathcal{T} = & \mathbb{F}_q \\ \mathcal{K} = & \mathbb{Z}_{q(q^n-N)} \\ \mathcal{E} = & \{E_k : E_k(f) = pr_k(\underline{u_f})\} \end{cases} \tag{2.4.4}$$

where $k \in \mathcal{K}$ and $f \in \mathcal{S}$.

Proposition 2.4.6. *The systematic authentication code in (2.4.4) has the following parameters:*

$$|\mathcal{S}| = q^{2n(N+1)},\ |\mathcal{K}| = q(q^n - N),\ |\mathcal{T}| = q,$$

$$\mathcal{P}_{\mathcal{I}} \leq \frac{1}{q} + \frac{(q-1)}{q} \cdot \frac{(p(N+1)+N-1)\sqrt{q^n}}{q^n - N},\ \textit{and}$$

$\mathcal{P}_{\mathcal{S}} \leq 1$ *and the equality holds if* q *is power of an odd prime.*

Proof. For any message $f \in \mathcal{S} = \mathcal{G}_{\mathcal{N}}$ and key $k \in \mathbb{Z}_{q(q^n-N)}$ by using (1.1.3) and Lemma 2.3.4 we get

$$\mathcal{P}_{\mathcal{I}} = max_{f,t}\frac{|\{k \in \mathcal{K} : t = pr_k(\underline{u_f})\}|}{|\{k \in \mathcal{K}\}|} \leq \frac{1}{q} + \frac{(q-1)}{q} \cdot \frac{(p(N+1)+N-1)\sqrt{q^n}}{q^n - N}.$$

By (1.1.4) we have

$$\mathcal{P}_{\mathcal{S}} = max_{f,t}max_{f' \neq f,t'}\frac{|\{k \in \mathcal{K} : t = pr_k(\underline{u_f}), t' = pr_k(\underline{u_{f'}})\}|}{|\{k \in \mathcal{K} : t = pr_k(\underline{u_f})\}|}$$

If we choose $f = x$ and $f' = \lambda x$, $\lambda \in \mathbb{F}_p$ and $\lambda \neq 1$, then since the code is R-linear we have $\underline{u_f} = \lambda \underline{u_{f'}}$. Therefore $\mathcal{P}_{\mathcal{S}} = 1$. The remaining conclusions are clear. □

Here we remark that the probability $\mathcal{P}_{\mathcal{S}}$ of the authentication code in [5] is very bad. By restricting the source space we get better probability $\mathcal{P}_{\mathcal{S}}$.

Assume that $q = p$ is a prime. Classify the functions in $\mathcal{G}_{\mathcal{N}}$ into $|\mathcal{G}_{\mathcal{N}}|/(p-1)$ equivalent classes, where two functions are in the same class if and only if they are constant multiple of each other (i.e. $f_1 = \lambda f_2$, for some $\lambda \in F_p^*$). By taking only one function from each classes we define the set $\mathcal{G}'_{\mathcal{N}}$. Then using the codewords in (2.4.4) and assuming $p^n - N > (p(N+1)+N-1)\sqrt{p^n}$ we can define the following systematic authentication code

$$\begin{cases} \mathcal{S} = & \mathcal{G}'_{\mathcal{N}} \\ \mathcal{T} = & \mathbb{F}_p \\ \mathcal{K} = & \mathbb{Z}_{p(p^n-N)} \\ \mathcal{E} = & \{E_k : E_k(f) = pr_k(\underline{u_f})\} \end{cases} \tag{2.4.5}$$

where $k \in \mathcal{K}$ and $f \in \mathcal{S}$.

We will calculate the probability $\mathcal{P}_{\mathcal{S}}$ using the following fact, which can be easily proved similar to Lemma 2.4.3.

Lemma 2.4.7. *Let f_1 and f_2 be two distinct elements of $\mathcal{G}'_{\mathcal{N}}$ and let $t_1, t_2 \in \mathbb{F}_p$, $i = 1, \ldots, p$. Define $N(f_1, f_2, t_1, t_2, i) = |\{\alpha \in \tau(S) \backslash P : pr_i(\phi(\mathrm{Tr}_{S/R}(f_1(\alpha)))) = t_1,\ pr_i(\phi(\mathrm{Tr}_{S/R}(f_2(\alpha)))) = t_2\}|$. Then*

$$N(f_1, f_2, t_1, t_2, i) \leq \frac{1}{p^2}[(p^n - N) + (p^2 - 1)(p(N+1)+N-1)\sqrt{p^n}].$$

Using Lemma 2.3.4 and Lemma 2.4.7 we have the following result,

Proposition 2.4.8. *The systematic authentication code in (2.4.5) has the following parameters:*

$$|\mathcal{S}| = \frac{p^{2n(N+1)}}{p-1},\ |\mathcal{K}| = p(p^n - N),\ |\mathcal{T}| = p,$$

$$\mathcal{P}_{\mathcal{I}} \leq \frac{1}{p} + \frac{(p-1)}{p} \cdot \frac{(p(N+1)+N-1)\sqrt{p^n}}{p^n - N},\ \textit{and}$$

$$\mathcal{P}_{\mathcal{S}} \leq \frac{1}{p} + \frac{(p^2+p-2)(p(N+1)+N-1)\sqrt{p^n} - pN}{p(p^n + (p-1)N - (p-1)(p(N+1)+N-1)\sqrt{p^n})}.$$

2.5 Generalization to Arbitrary Characteristic

In this section, we extend the constructions given in Section 2.3 using Galois rings having characteristic p^l. We omit the proofs which are very similar to the proofs in Section 2.3.

For any $f(x) \in \mathcal{F}_D$ and $\{\beta_1, \ldots, \beta_q\} = p^{l-1}R$, a corresponding codeword in $\mathbb{F}_q{}^{(q^{l-1} \cdot q^{n+1})} = \mathbb{F}_q{}^{(q^{n+l})}$

$$\underline{u_f} = \left[u_{f,\beta_1}, u_{f,\beta_2}, \cdots, u_{f,\beta_q}\right] \tag{2.5.1}$$

where $u_{f,\beta_i} = \left[\phi(\beta_i) + \phi(\mathrm{Tr}_{S/R}(f(0))), \cdots, \phi(\beta_i) + \phi(\mathrm{Tr}_{S/R}(f(\xi^{q^n-1})))\right]$ for $i = 1, \ldots, q$.

Let pr_i be the projection map from $\mathbb{F}_q{}^{(q^{n+l})}$ to $\mathbb{F}_q$ sending $\underline{u_f}$ to its i-th coordinate. Using the codewords in (2.5.1) the systematic authentication code is defined by

$$\begin{cases} \mathcal{S} = & \mathcal{F}_D \\ \mathcal{T} = & \mathbb{F}_q \\ \mathcal{K} = & \mathbb{Z}_{q^{n+l}} \\ \mathcal{E} = & \{E_k : E_k(f) = pr_k(\underline{u_f})\} \end{cases} \tag{2.5.2}$$

where $k \in \mathcal{K}$ and $f \in \mathcal{S}$.

Theorem 2.5.1. *The systematic authentication code in (2.5.2) has the following parameters:*

$$|\mathcal{S}| = q^{n(D-\lfloor D/p^l \rfloor)},\ |\mathcal{K}| = q^{n+l},\ |\mathcal{T}| = q,\ \mathcal{P}_{\mathcal{I}} = \frac{1}{q} \text{ and}$$

$$\mathcal{P}_{\mathcal{S}} \leq \frac{1}{q} + \frac{(q-1)}{q} \cdot \frac{(D-1)}{\sqrt{q^n}}.$$

For any $f \in \mathcal{G}_N$ and $\{\beta_1, \ldots, \beta_q\} = p^{l-1}R$, we have a corresponding codeword in $\mathbb{F}_q{}^{(q^l(q^n-N))}$

$$\underline{u_f} = \left[u_{f,\beta_1}, u_{f,\beta_2}, \cdots, u_{f,\beta_q}\right] \tag{2.5.3}$$

where $u_{f,\beta_i} = \left[\phi(\beta_i) + \phi(\mathrm{Tr}_{S/R}(f(\alpha_1))), \cdots, \phi(\beta_i) + \phi(\mathrm{Tr}_{S/R}(f(\alpha_{q^n-N})))\right]$ for $i = 1, \ldots, q$.

Let pr_i be the projection map from $\mathbb{F}_q{}^{(q^l(q^n-N))}$ to $\mathbb{F}_q$ sending $\underline{u_f}$ to its i-th coordinate. Using the codewords in (2.5.3) and assuming $q^n - N > (p^{l-1}(N+1) + N - 1)\sqrt{q^n}$ the systematic authentication code is defined by

$$\begin{cases} \mathcal{S} = & \mathcal{G}_N \\ \mathcal{T} = & \mathbb{F}_q \\ \mathcal{K} = & \mathbb{Z}_{q^l(q^n-N)} \\ \mathcal{E} = & \{E_k : E_k(f) = pr_k(\underline{u_f})\} \end{cases} \tag{2.5.4}$$

where $k \in \mathcal{K}$ and $f \in \mathcal{S}$.

Theorem 2.5.2. *The systematic authentication code in (2.5.4) has the following parameters:*

$$|\mathcal{S}| = q^{ln(N+1)},\ |\mathcal{K}| = q^l(q^n - N),\ |\mathcal{T}| = q,\ \mathcal{P}_{\mathcal{I}} = \frac{1}{q} \text{ and}$$

$$\mathcal{P}_{\mathcal{S}} \leq \frac{1}{q} + \frac{(q-1)}{q} \cdot \frac{(p^{l-1}(N+1) + N - 1)\sqrt{q^n}}{q^n - N}.$$

For each $1 \leq t \leq l-1$ and $u \in R$, let

$$s_t(u) := \sum_{x \in R \setminus p^t R} e^{2\pi i \frac{\mathrm{Tr}_m(ux)}{p^l}} \text{ and } w_t(u) := -\frac{1}{q} s_t(u) + (q^{l-1} - q^{l-t-1}).$$

We note that

$$w_t(u) = \begin{cases} 0, & \text{if } u = 0 \\ q^{l-1}, & \text{if } u \in p^{l-t}R \setminus \{0\} \\ q^{l-1} - q^{l-t-1}, & \text{if } u \notin p^{l-t}R. \end{cases}$$

is a generalization of the weight $w(\cdot)$ in Definition 2.2.4 and is related to exponential sum in analogous way [38].

Recall that the generalized Gray map gives an injection of R into $(\mathbb{F}_q)^{q^{l-1}}$ preserving the corresponding weights. Using the fact that $\mathcal{P}_{\mathcal{S}} \geq 1/|\mathcal{T}|$, we prove the following nonexistence result.

Proposition 2.5.3. *For $1 \leq t \leq l-1$, there is an injection of R into $(\mathbb{F}_q)^{q^{l-1}}$ preserving the corresponding weights given w_t and the Hamming weight respectively if and only if $t = 1$. In this case the generalized Gray map is such an injection.*

Proof. Assume $t > 1$, that is, $l \geq 3$. Using the connection $w_t(u)$ to the exponential sum given by $s_t(u)$ and similar methods of Subsection 2.3.1 and Section 2.5 with $D = 1$ and $|\mathcal{T}| = q$ we obtain that $\mathcal{P}_{\mathcal{S}} \leq 1/q^t$, which contradicts with the fact $\mathcal{P}_{\mathcal{S}} \geq 1/|\mathcal{T}|$. □

Chapter 3

Systematic Authentication Codes Using Additive Polynomials

In this chapter two families of systematic authentication codes using additive polynomials related to some curves over finite fields are constructed. Tight bounds for the number of rational points of these curves are used in estimating the probabilities of the systematic authentication codes. Their parameters are compared with some existing codes in the literature. It is observed that the parameters are better than the existing ones in some cases.

3.1 Introduction

Let q be a power of a prime p and m be a positive integer. Throughout this chapter $\mathbb{F}_{q^m}$ denotes the finite field of cardinality q^m. In our constructions, using the source space, we obtain some additive polynomials over $\mathbb{F}_{q^m}$. Our tag space is always $\mathbb{F}_q$. For the authentication map, we first apply a suitable operation to the additive polynomials obtained from the source space. Then we evaluate the resulting polynomials in $\mathbb{F}_{q^m}$ and take traces to $\mathbb{F}_q$, which is the tag space.

We have two types of authentication maps. In type I, we further use a part of the key for an addition in $\mathbb{F}_q$. This final operation guarantees that the probability $\mathcal{P}_{\mathcal{I}}$ is $1/q$. In type II, we use smaller key space but we may have slightly larger values for the probabilities $\mathcal{P}_{\mathcal{I}}$ and $\mathcal{P}_{\mathcal{S}}$. Our Construction (3.4.1) is of type I and the Construction (3.4.2) is of type II given in Section 3.4. The difference of type I and type II codes appears in estimating the probabilities $\mathcal{P}_{\mathcal{I}}$ and $\mathcal{P}_{\mathcal{S}}$.

For estimating the probabilities in some constructions of systematic authentication codes, it is useful to have nontrivial bounds on certain exponential sums. In this chapter we use some tight bounds on certain exponential sums for a large class of polynomials over finite fields, which are related to additive polynomials. These bounds on exponential sums follow from the bounds

on the number of rational points of a class of curves determined in [13] and [14]. Also we prove the analogous results in Theorems 3.2.1 and 3.2.2. The results in Theorems 3.2.1 and 3.2.2 were not considered in [13] or [14] and they are useful for the constructions in this chapter.

This chapter is organized as follows. We give some preliminaries in Section 3.2. In this section, using results from [13] and their analogues, we obtain tight bounds for the number of elements of $\mathbb{F}_{q^m}$ satisfying certain equations. In Section 3.3 we use these bounds to obtain some useful results for estimating the probabilities of our constructions and we give our constructions in Section 3.4. We present some examples in Section 3.5. We compare our codes with some existing ones in the literature in Section 3.6. We show by examples that the parameters of our codes are better than the existing ones in some cases.

3.2 Preliminaries

In this section we give some preliminaries which will be used in this chapter. Let $m > 1$ be an integer and let Tr denote the trace map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$, i.e. $\mathrm{Tr}(a) = a + a^q + \cdots + a^{q^{m-1}}$ and $\mathrm{Tr}_{q/p}$ (resp. $\mathrm{Tr}_{q^m/p}$) denote the trace map from $\mathbb{F}_q$ (resp. $\mathbb{F}_{q^m}$) to $\mathbb{F}_p$. Let $h \geq 0$ and $L(x) = u_0x + u_1x^q + \cdots + u_hx^{q^h} \in \mathbb{F}_{q^m}[x]$ be an $\mathbb{F}_q$ additive polynomial. If q is even, we further assume that $h \geq 1$ throughout the chapter. Let B_L be the symmetric bilinear form on $\mathbb{F}_{q^m}$ defined as

$$\begin{aligned} B_L : \mathbb{F}_{q^m} \times \mathbb{F}_{q^m} &\rightarrow \mathbb{F}_q \\ (x, y) &\rightarrow \mathrm{Tr}(xL(y) + yL(x)). \end{aligned}$$

We remind that the radical W_L of B_L is

$$\begin{aligned} W_L &= \{a \in \mathbb{F}_{q^m} : B_L(a, b) = 0 \text{ for each } b \in \mathbb{F}_{q^m}\} \\ &= \{x \in \mathbb{F}_{q^m} : 0 = \sum_{i=0}^{h-1} u_{h-i}^{q^i} x^{q^i} + 2u_0^{q^h} x^{q^h} + \sum_{i=1}^{h} u_i^{q^h} x^{q^{h+i}}\}. \end{aligned}$$

Let d_L be the $\mathbb{F}_q$-dimension of W_L. If $L \neq 0$, then it follows from the definition of W_L that $d_L \leq 2h$.

For any $L(x) = u_0x + u_1x^q + \cdots + u_hx^{q^h}$, $M(x) = v_0x + v_1x^q + \cdots + v_{h'}x^{q^{h'}}$ in $\mathbb{F}_{q^m}[x]$, let $V_L = \{x \in \mathbb{F}_{q^m} : \mathrm{Tr}(xL(x)) = 0\}$ and ψ_M be the $\mathbb{F}_q$-linear map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ sending x to $\mathrm{Tr}(M(x))$. Let $N(\mathrm{Tr}(xL(x) + M(x)) = 0)$ denote the number of solutions of the equation $\mathrm{Tr}(xL(x) + M(x)) = 0$ with $x \in \mathbb{F}_{q^m}$. If $m \geq 2$ is an even integer, then we will use results of [13, Theorem 3.1] and [13, Theorem 4.1] in our estimates of some constructions. If $m \geq 3$ is an odd integer, then using similar methods as in [13], we prove the following theorems. These analogous results, corresponding to an odd integer $m \geq 3$, were not considered in [13] or [14].

The following theorems will also be used later in this chapter for estimating the probabilities of further constructions when $m \geq 3$ is odd.

Theorem 3.2.1. *Assume that q is even and m is odd. Under the notation as above, we have*

1.) If $W_L \subseteq V_L$ then

$$N\left(\mathrm{Tr}(xL(x)+M(x))=0\right)=\begin{cases} q^{m-1} \text{ or} \\ q^{m-1}\mp(q-1)q^{(m+d_L-2)/2} \text{ or} \\ q^{m-1}\mp q^{(m+d_L-2)/2}. \end{cases}$$

2.) If $W_L \not\subseteq V_L$ then

$$N\left(\mathrm{Tr}(xL(x)+M(x))=0\right)=\begin{cases} q^{m-1} \text{ or} \\ q^{m-1}\mp q^{(m+d_L-2)/2}. \end{cases}$$

Proof. Let Q_L be the map sending $x \in \mathbb{F}_{q^m}$ to $\mathrm{Tr}(xL(x)) \in \mathbb{F}_q$. Let $\{f_1,\ldots,f_{d_L}\}$ be a basis of W_L over $\mathbb{F}_q$. Let $\overline{W}_L$ be an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}$ such that $\dim_{\mathbb{F}_q}\overline{W}_L = m-d_L$ and $W_L \oplus \overline{W}_L = \mathbb{F}_{q^m}$. As q is even and m is odd, we have d_L is odd (cf. [29, Corollary 2.11]). Moreover there exists a basis $\{e_1,\ldots,e_{m-d_L}\}$ of $\overline{W}_L$ such that for $x_1,\ldots,x_{m-d_L} \in \mathbb{F}_q$ we have that $Q_L\left(x_1e_1+\cdots+x_{m-d_L}e_{m-d_L}\right)$ is equal to either

$$\begin{aligned} H_1\left(x_1,\ldots,x_{m-d_L}\right) &= x_1x_2+x_3x_4+\cdots+x_{m-d_L-1}x_{m-d_L}, \text{ or} && (3.2.1)\\ H_2\left(x_1,\ldots,x_{m-d_L}\right) &= x_1x_2+x_3x_4+\cdots+x_{m-d_L-1}x_{m-d_L} && (3.2.2)\\ &\quad +x_{m-d_L-1}^2+\alpha x_{m-d_L}^2, \end{aligned}$$

where $\alpha \in \mathbb{F}_q$ and $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\alpha)=\alpha+\alpha^2+\cdots+\alpha^{q/2}=1$ (cf. [13] and [37, Theorem 6.30]).

Let ψ_M be the $\mathbb{F}_q$-linear map sending $x \in \mathbb{F}_{q^m}$ to $\mathrm{Tr}(M(x)) \in \mathbb{F}_q$. Let $a_i=\psi_M(e_i)$ for $1 \leq i \leq d_L$ and $b_i=\psi_M(f_i)$ for $1 \leq i \leq d_L$. Finally, let Ψ be the map sending $x \in \mathbb{F}_{q^m}$ to $Q_L(x)+\psi_M(x) \in \mathbb{F}_q$.

We first prove item 1.) in the statement of the theorem. As $W_L \subseteq V_L$ we have $Q_L(f_1)=\cdots=Q_L(f_{d_L})=0$ and for $x_1,\ldots,x_{m-d_L},y_1,\ldots,y_{d_L} \in \mathbb{F}_q$ we obtain

$$\begin{aligned} &\Psi\left(x_1e_1+\cdots+x_{m-d_L}e_{m-d_L}+y_1f_1+\cdots+y_{d_L}f_{d_L}\right)\\ &=H(x_1,\ldots,x_{m-d_L})+a_1x_1+\cdots+a_{m-d_L}x_{m-d_L}+b_1y_1+\cdots+b_{d_L}y_{d_L}, \end{aligned}$$

where H is either H_1 or H_2 given in (3.2.1) and (3.2.2).

If $W_L \not\subseteq \mathrm{Ker}\psi_M$, then there exists $1 \leq i_0 \leq d_L$ such that $b_{i_0} \neq 0$. Hence using [13, Lemma 2.1] we obtain that $N\left(\mathrm{Tr}(xL(x)+M(x))=0\right)=q^{m-1}$. If $W_L \subseteq \mathrm{Ker}\psi_M$, then using [37, Theorem 6.32] we obtain that $N\left(\mathrm{Tr}(xL(x)+M(x))=0\right)$ is either

$$q^{m-1}\mp(q-1)q^{(m+d_L-2)/2} \text{ or } q^{m-1}\mp q^{(m+d_L-2)/2}.$$

Now we prove item 2.) in the statement of the theorem. For $1 \leq i \leq d_L$, let $c_i = Q_L(f_i) \in \mathbb{F}_q$. For $x_1, \ldots, x_{m-d_L}, y_1, \ldots, y_{d_L} \in \mathbb{F}_q$ we obtain

$$\begin{aligned}
&\Psi\left(x_1e_1 + \cdots + x_{m-d_L}e_{m-d_L} + y_1f_1 + \cdots + y_{d_L}f_{d_L}\right)\\
&= H(x_1, \ldots, x_{m-d_L}) + a_1x_1 + \cdots + a_{m-d_L}x_{m-d_L} + b_1y_1 + \cdots + b_{d_L}y_{d_L}\\
&\quad + c_1y_1^2 + \cdots + c_{d_L}y_{d_L}^2,
\end{aligned}$$

where H is either H_1 or H_2 given in (3.2.1) and (3.2.2). If $\mathrm{Ker}\psi_M \cap W_L \not\subseteq V_L \cap W_L$, then we can choose the basis $\{f_1, \ldots, f_{d_L}\}$ of W_L such that $b_{d_L} = 0$ and $c_{d_L} \neq 0$. Hence, again using [13, Lemma 2.1], we obtain that $N\left(\mathrm{Tr}(xL(x) + M(x)) = 0\right) = q^{m-1}$.

Finally, we assume that $W_L \not\subseteq V_L$ and $\mathrm{Ker}\psi_M \cap W_L = V_L \cap W_L$. In this case we have $\dim_{\mathbb{F}_q} \mathrm{Ker}\psi_M = m-1$, $\dim_{\mathbb{F}_q}\left(\mathrm{Ker}\psi_M \cap W_L\right) = d_L - 1$ and we can choose the basis $\{f_1, \ldots, f_{d_L}\}$ of W_L such that $b_2 = \cdots = b_{d_L} = c_2 = \cdots = c_{d_L} = 0$. Hence for $x_1, \ldots, x_{m-d_L}, y_1, \cdots, y_{d_L} \in \mathbb{F}_q$ we obtain

$$\begin{aligned}
&\Psi\left(x_1e_1 + \cdots + x_{m-d_L}e_{m-d_L} + y_1f_1 + \cdots + y_{d_L}f_{d_L}\right)\\
&= H(x_1, \ldots, x_{m-d_L}) + a_1x_1 + \cdots + a_{m-d_L}x_{m-d_L} + b_1y_1 + c_1y_1^2,
\end{aligned}$$

where H is either H_1 or H_2 given in (3.2.1) and (3.2.2). Using similar methods as in the proof of [13, Theorem 3.1] we complete the proof. □

Theorem 3.2.2. *Assume that q is odd and m is odd. Under the notation as above, we have*

1.) If $W_L \not\subseteq \mathrm{Ker}\psi_M$ then $N\left(\mathrm{Tr}(xL(x) + M(x)) = 0\right) = q^{m-1}$.

2.) If $W_L \subseteq \mathrm{Ker}\psi_M$ and d_L is even then

$$N\left(\mathrm{Tr}(xL(x) + M(x)) = 0\right) = \begin{cases} q^{m-1} \text{ or} \\ q^{m-1} \mp q^{(m+d_L-1)/2}. \end{cases}$$

3.) If $W_L \subseteq \mathrm{Ker}\psi_M$ and d_L is odd then

$$N\left(\mathrm{Tr}(xL(x) + M(x)) = 0\right) = \begin{cases} q^{m-1} \mp (q-1)q^{(m+d_L-2)/2} \text{ or} \\ q^{m-1} \mp q^{(m+d_L-2)/2}. \end{cases}$$

Proof. Let ψ_M be the $\mathbb{F}_q$-linear map sending $x \in \mathbb{F}_{q^m}$ to $\mathrm{Tr}(M(x)) \in \mathbb{F}_q$. Let Ψ be the map sending $x \in \mathbb{F}_{q^m}$ to $\mathrm{Tr}\left(xL(x) + M(x)\right) \in \mathbb{F}_q$. Let $\{f_1, \ldots, f_{d_L}\}$ be a basis of W_L over $\mathbb{F}_q$. We note that, as q is odd, we always have $W_L \subseteq V_L$ and moreover d_L can be either even or odd. As in the proof of [13, Theorem 4.1], we obtain $\{e_1, \ldots, e_{m-d_L}\} \in \mathbb{F}_{q^m} \setminus W_L$ such that $\{e_1, \ldots, e_{m-d_L}, f_1, \ldots, f_{d_L}\}$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, and for $x_1, \ldots, x_{m-d_L}, y_1, \ldots, y_{d_L} \in \mathbb{F}_q$ we have

$$\begin{aligned}
&\Psi\left(x_1e_1 + \cdots + x_{m-d_L}e_{m-d_L} + y_1f_1 + \cdots + y_{d_L}f_{d_L}\right) \qquad (3.2.3)\\
&= H(x_1, \ldots, x_{m-d_L}) + a_1x_1 + \cdots + a_{m-d_L}x_{m-d_L} + b_1y_1 + \cdots + b_{d_L}y_{d_L},
\end{aligned}$$

where $a_i = \psi_M(e_i)$ for $1 \leq i \leq m - d_L$, $b_i = \psi_M(f_i)$ for $1 \leq i \leq d_L$ and

$$H(x_1, \ldots, x_{m-d_L}) = \frac{1}{2}\left(x_1^2 + x_2^2 + \cdots + x_{m-d_L-1}^2 + \alpha x_{m-d_L}^2\right), \tag{3.2.4}$$

with $\alpha \in \mathbb{F}_q \setminus \{0\}$.

If $W_L \not\subseteq \mathrm{Ker}\psi_M$, then there exists $1 \leq i_0 \leq d_L$ such that $b_{i_0} \neq 0$ in (3.2.3). Hence [13, Lemma 2.1] implies that $N\left(\mathrm{Tr}(xL(x) + M(x)) = 0\right) = q^{m-1}$.

Let $A = H\left(a_1, a_2, \ldots, a_{m-d_L-1}, \frac{a_{m-d_L}}{\alpha}\right)$, where $H(x_1, \ldots, x_{m-d_L})$ and the parameters are as given in (3.2.3) and (3.2.4). If $W_L \subseteq \mathrm{Ker}\psi_M$, then $b_1 = \cdots = b_{d_L} = 0$ in (3.2.3) and for $x_1, \ldots, x_{m-d_L}, y_1, \ldots, y_{d_L} \in \mathbb{F}_q$ we obtain

$$\begin{aligned}
&\Psi\left(x_1e_1 + \cdots + x_{m-d_L}e_{m-d_L} + y_1f_1 + \cdots + y_{d_L}f_{d_L}\right) \\
&= H\left(x_1 + a_1, x_2 + a_2, \ldots, x_{m-d_L-1} + a_{m-d_L-1} + x_{m-d_L} + \frac{a_{m-d_L}}{\alpha}\right) - A.
\end{aligned}$$

Hence we complete the proof using [37, Theorem 6.26] and [37, Theorem 6.27]. □

Remark 3.2.3. As in [13, Theorem 3.1] and [13, Theorem 4.1], when $m \geq 3$ is an odd integer we obtain the cases corresponding to the each number of solutions in where the number of solutions in the statements of Theorems 3.2.1 and 3.2.2 hold. For example, assume that q is even and $m \geq 3$ is odd. Let Q_L be the map defined in the proof of Theorem 3.2.1. Let $\overline{W}_L$ be an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}$ as given in the proof of Theorem 3.2.1. Let $\{e_1, \ldots, e_{m-d_L}\}$ be a basis of $\overline{W}_L$ such that for $x_1, \ldots, x_{m-d_L} \in \mathbb{F}_q$ we have that $Q_L\left(x_1e_1 + \cdots + x_{m-d_L}e_{m-d_L}\right)$ is equal to either $H_1\left(x_1, \ldots, x_{m-d_L}\right)$ or $H_2\left(x_1, \ldots, x_{m-d_L}\right)$ defined in (3.2.1) and (3.2.2). Let $a_1, \ldots, a_{m-d_L} \in \mathbb{F}_q$ be defined as in the proof of Theorem 3.2.1 and put

$$C_1 = H_1(a_2, a_1, a_4, a_3, \ldots, a_{m-d_L}, a_{m-d_L-1}).$$

We recall that, as q is even and m is odd, we have d_L is odd and $m - d_L$ is even. In Theorem 3.2.1, we have that $N\left(\mathrm{Tr}(xL(x) + M(x))\right) = q^{m-1} + (q-1)q^{(m+d_L-2)/2}$ if and only if for $x_1, \ldots, x_{m-d_L} \in \mathbb{F}_q$ we have that $Q_L\left(x_1e_1 + \cdots + x_{m-d_L}e_{m-d_L}\right)$ is equal to $H_1\left(x_1, \ldots, x_{m-d_L}\right)$, and $C_1 = 0$.

The following lemma will be useful in this chapter and it is directly obtained from [13, Theorem 3.1], [13, Theorem 4.1], Theorem 3.2.1 and Theorem 3.2.2.

Lemma 3.2.4. *For any* $\mathbf{u} = (u_0, u_1, \ldots, u_h) \in \mathbb{F}_{q^m}^{h+1}$, $v \in \mathbb{F}_{q^m}$ *with* $(\mathbf{u}, v) \neq (\mathbf{0}, 0)$, $L(x) = u_0x + u_1x^q + \cdots + u_hx^{q^h}$, $M(x) = vx$ *and for any nonzero* $y \in \mathbb{F}_q$, *define*

$$\sigma(y) = \sum_{x \in \mathbb{F}_{q^m}} e^{\frac{2\pi i}{p}\mathrm{Tr}_{q^m/p}(xyL(x) + yM(x))}.$$

Then we have

$$|\sigma(y)| \leq \begin{cases} q^{\frac{m+d_L}{2}} & \text{if } q \text{ is even, or } q \text{ is odd and } d_L \equiv m \bmod 2 \\ \frac{1}{q-1} \cdot q^{\frac{m+d_L+1}{2}} & \text{if } q \text{ is odd and } d_L \equiv m+1 \bmod 2. \end{cases}$$

Proof. For any fixed $x \in \mathbb{F}_{q^m}$ and $t \in \mathbb{F}_q$ we have

$$\sum_{y\in\mathbb{F}_q} e^{\frac{2\pi i}{p}\mathrm{Tr}_{q/p}[y(\mathrm{Tr}(xL(x)+M(x))-t)]} = \begin{cases} q & \text{if } \mathrm{Tr}(xL(x)+M(x))-t=0 \\ 0 & \text{if } \mathrm{Tr}(xL(x)+M(x))-t\neq 0. \end{cases}$$

Hence,

$$\begin{aligned} N(\mathrm{Tr}(xL(x)+M(x))=0) &= \frac{1}{q}\sum_{x\in\mathbb{F}_{q^m}}\sum_{y\in\mathbb{F}_q} e^{\frac{2\pi i}{p}\mathrm{Tr}_{q/p}[y(\mathrm{Tr}(xL(x)+M(x)))]} \\ &= \frac{1}{q}\left(q^m + \sum_{y\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_{q^m}} e^{\frac{2\pi i}{p}\mathrm{Tr}_{q^m/p}(xyL(x)+yM(x))}\right). \end{aligned}$$

Therefore we obtain that

$$|\sigma(y)| = \frac{1}{q-1}\cdot|qN(\mathrm{Tr}(xL(x)+M(x))=0) - q^m|.$$

Then the result follows from [13, Theorem 3.1], [13, Theorem 4.1], Theorem 3.2.1 and Theorem 3.2.2. □

Remark 3.2.5. For some special choices of $L(x) = u_0x + u_1x^q + \cdots + u_hx^{q^h} \in \mathbb{F}_{q^m}[x]$, it is possible to improve the bounds given in Lemma 3.2.4. Indeed, if the additive polynomials L are chosen carefully, then using [13, Theorem 3.1], [13, Theorem 4.1], Theorem 3.2.1 and Theorem 3.2.2 (see also Remark 3.2.3), the corresponding inequalities in Lemma 3.2.4 become

$$|\sigma(y)| \leq \begin{cases} \frac{1}{q-1}\cdot q^{\frac{m+d_L}{2}} & \text{if } q \text{ is even, or } q \text{ is odd and } d_L \equiv m \bmod 2 \\ \frac{1}{q-1}\cdot q^{\frac{m+d_L+1}{2}} & \text{if } q \text{ is odd and } d_L \equiv m+1 \bmod 2. \end{cases}$$

This improvement will be useful in some examples in Section 3.5.

3.3 Auxiliary Results

In this section we obtain some auxiliary results for estimating upper bounds for the probabilities $\mathcal{P}_{\mathcal{I}}$ and $\mathcal{P}_{\mathcal{S}}$ in our constructions presented later in this chapter.

Lemma 3.3.1. *For any* $\mathbf{u} = (u_0, u_1, \ldots, u_h) \in \mathbb{F}_{q^m}^{h+1}$, $v \in \mathbb{F}_{q^m}$ *with* $(\mathbf{u}, v) \neq (\mathbf{0}, 0)$, $L(x) = u_0x + u_1x^q + \cdots + u_hx^{q^h}$, $M(x) = vx$ *and for* $t \in \mathbb{F}_q$ *put*

$$N(\mathbf{u}, v; t) = |\{x \in \mathbb{F}_{q^m} : \mathrm{Tr}(xL(x)+M(x)) = t\}|.$$

Then

$$N(\mathbf{u}, v; t) \leq \begin{cases} q^{m-1} + \frac{q-1}{q}\cdot q^{\frac{m+d_L}{2}} & \text{if } q \text{ is even, or } q \text{ is odd and } d_L \equiv m \bmod 2 \\ q^{m-1} + q^{\frac{m+d_L-1}{2}} & \text{if } q \text{ is odd and } d_L \equiv m+1 \bmod 2 \end{cases}$$

and

$$N(\mathbf{u},v;t) \geq \begin{cases} q^{m-1} - \frac{q-1}{q} \cdot q^{\frac{m+d_L}{2}} & \text{if } q \text{ is even, or } q \text{ is odd and } d_L \equiv m \bmod 2 \\ q^{m-1} - q^{\frac{m+d_L-1}{2}} & \text{if } q \text{ is odd and } d_L \equiv m+1 \bmod 2. \end{cases}$$

Proof. If $\mathbf{u} = \mathbf{0}$ and $v \neq 0$, we have

$$\begin{aligned} N(\mathbf{0},v;t) &= |\{x \in \mathbb{F}_{q^m} : \mathrm{Tr}(M(x)) - t = 0\}| \\ &= |\{x \in \mathbb{F}_{q^m} : \mathrm{Tr}(vx) - t = 0\}| \\ &= q^{m-1}, \end{aligned}$$

since $\mathrm{Tr}(vx)$ is linear and surjective. Thus, the inequalities hold.

Assume that $\mathbf{u} \neq \mathbf{0}$.

$$\begin{aligned} N(\mathbf{u},v;t) &= |\{x \in \mathbb{F}_{q^m} : \mathrm{Tr}(xL(x) + M(x)) - t = 0\}| \\ &= \frac{1}{q} \sum_{x \in \mathbb{F}_{q^m}} \sum_{y \in \mathbb{F}_q} e^{\frac{2\pi i}{p} \mathrm{Tr}_{q/p}[y(\mathrm{Tr}(xL(x)+M(x))-t)]} \\ &= \frac{1}{q} \left(q^m + \sum_{y \in \mathbb{F}_q^*} e^{\frac{2\pi i}{p} \mathrm{Tr}_{q/p}(-yt)} \sum_{x \in \mathbb{F}_{q^m}} e^{\frac{2\pi i}{p} \mathrm{Tr}_{q^m/p}(xyL(x)+yM(x))} \right). \end{aligned}$$

Then using Lemma 3.2.4 we have $|qN(\mathbf{u},v;t) - q^m| \leq (q-1)|\sigma(y)|$. Then the result follows. □

Lemma 3.3.2. *Let* $\mathbf{u}_1 = (u_{1,0}, u_{1,1}, \ldots, u_{1,h})$, $\mathbf{u}_2 = (u_{2,0}, u_{2,1}, \ldots, u_{2,h}) \in \mathbb{F}_{q^m}^{h+1}$, $v_1, v_2 \in \mathbb{F}_{q^m}$ *such that* $(\mathbf{u}_1, v_1) \neq c(\mathbf{u}_2, v_2)$, *for all* $c \in \mathbb{F}_q^*$, *with* $L_i(x) = u_{i,0}x + u_{i,1}x^q + \cdots + u_{i,h}x^{q^h}$ *and* $M_i(x) = v_i x$, $(i = 1, 2)$, *and* $t_1, t_2 \in \mathbb{F}_q$. *Define* $d = max\{\dim_{\mathbb{F}_q} W_L : L = y_1L_1 + y_2L_2,\ (0,0) \neq (y_1, y_2) \in {\mathbb{F}_q}^2\}$ *and*

$$N(\mathbf{u}_1, \mathbf{u}_2, v_1, v_2; t_1, t_2) = |\{x \in \mathbb{F}_{q^m} : \mathrm{Tr}(xL_i(x) + M_i(x)) = t_i,\ i = 1, 2\}|.$$

Then

$$N(\mathbf{u}_1, \mathbf{u}_2, v_1, v_2; t_1, t_2) \leq \begin{cases} q^{m-2} + \frac{q^2-1}{q^2} \cdot q^{\frac{m+d}{2}} & \text{if } q \text{ is even, or} \\ & q \text{ is odd and } d \equiv m \bmod 2 \\ q^{m-2} + \frac{q+1}{q} \cdot q^{\frac{m+d-1}{2}} & \text{if } q \text{ is odd and } d \equiv m+1 \bmod 2 \end{cases}$$

and

$$N(\mathbf{u}_1, \mathbf{u}_2, v_1, v_2; t_1, t_2) \geq \begin{cases} q^{m-2} - \frac{q^2-1}{q^2} \cdot q^{\frac{m+d}{2}} & \text{if } q \text{ is even, or} \\ & q \text{ is odd and } d \equiv m \bmod 2 \\ q^{m-2} - \frac{q+1}{q} \cdot q^{\frac{m+d-1}{2}} & \text{if } q \text{ is odd and } d \equiv m+1 \bmod 2. \end{cases}$$

Proof.

$$\begin{aligned}
& N(\mathbf{u}_1, \mathbf{u}_2, v_1, v_2; t_1, t_2) \\
= \; & |\{x \in \mathbb{F}_{q^m} : \mathrm{Tr}(xL_i(x) + M_i(x)) - t_i = 0,\ i = 1, 2\}| \\
= \; & \frac{1}{q^2} \sum_{x \in \mathbb{F}_{q^m}} \sum_{y_1, y_2 \in \mathbb{F}_q} e^{\frac{2\pi i}{p} \mathrm{Tr}_{q/p}[\sum_{i=1}^{2} y_i (\mathrm{Tr}(xL_i(x) + M_i(x)) - t_i)]} \\
= \; & \frac{1}{q^2} \left(q^m + \sum_{(0,0) \neq (y_1, y_2) \in \mathbb{F}_q^2} e^{\frac{2\pi i}{p} \mathrm{Tr}_{q/p}(-y_1 t_1 - y_2 t_2)} \sum_{x \in \mathbb{F}_{q^m}} e^{\frac{2\pi i}{p} \mathrm{Tr}_{q^m/p}(\sum_{i=1}^{2} y_i (xL_i(x) + M_i(x)))} \right).
\end{aligned}$$

Since $(\mathbf{u}_1, v_1) \neq c(\mathbf{u}_2, v_2)$, for all $c \in \mathbb{F}_q^*$, $(\mathbf{u}_1, v_1)$ and $(\mathbf{u}_2, v_2)$ are linearly independent over $\mathbb{F}_q$. If $(y_1, y_2) \neq (0, 0)$, then $y_1\mathbf{u}_1 + y_2\mathbf{u}_2$ and $y_1 v_1 + y_2 v_2$ cannot be both zero at the same time, that is, $y_1 L_1 + y_2 L_2$ and $y_1 M_1 + y_2 M_2$ cannot both be the zero polynomial at the same time. Then using Lemma 3.2.4, we have $|q^2 N(\mathbf{u}_1, \mathbf{u}_2, v_1, v_2; t_1, t_2) - q^m| \leq (q^2 - 1)|\sigma(y)|$. The conclusion of the lemma then follows. □

As a special case, if we have $L_i(x) = u_i x^{q^h}$ for some $h \geq 0$, $i = 1, 2$, then the bounds in Lemma 3.3.2 can be improved.

Corollary 3.3.3. *Let $u_1, u_2, v_1, v_2 \in \mathbb{F}_{q^m}$ such that $(u_1, v_1) \neq c(u_2, v_2)$, for all $c \in \mathbb{F}_q^*$, with $L_i(x) = u_i x^{q^h}$ for some $h \geq 0$ and $M_i(x) = v_i x$, $(i = 1, 2)$, and $t_1, t_2 \in \mathbb{F}_q$. Define $d = max\{\dim_{\mathbb{F}_q} W_L : L = y_1 L_1 + y_2 L_2,\ (0, 0) \neq (y_1, y_2) \in {\mathbb{F}_q}^2\}$ and*

$$N(u_1, u_2, v_1, v_2; t_1, t_2) = |\{x \in \mathbb{F}_{q^m} : \mathrm{Tr}(xL_i(x) + M_i(x)) = t_i,\ i = 1, 2\}|.$$

Then

$$N(u_1, u_2, v_1, v_2; t_1, t_2) \leq \begin{cases} q^{m-2} + \frac{q-1}{q} \cdot q^{\frac{m+d}{2}} & \text{if } q \text{ is even, or} \\ & q \text{ is odd and } d \equiv m \bmod 2 \\ q^{m-2} + q^{\frac{m+d-1}{2}} & \text{if } q \text{ is odd and } d \equiv m + 1 \bmod 2 \end{cases}$$

and

$$N(u_1, u_2, v_1, v_2; t_1, t_2) \geq \begin{cases} q^{m-2} - \frac{q-1}{q} \cdot q^{\frac{m+d}{2}} & \text{if } q \text{ is even, or} \\ & q \text{ is odd and } d \equiv m \bmod 2 \\ q^{m-2} - q^{\frac{m+d-1}{2}} & \text{if } q \text{ is odd and } d \equiv m + 1 \bmod 2. \end{cases}$$

Proof. Similar to the proof of Lemma 3.3.2, we have

$$\begin{aligned}
& N(u_1, u_2, v_1, v_2; t_1, t_2) \\
= \; & \frac{1}{q^2} \left(q^m + \sum_{(0,0) \neq (y_1, y_2) \in \mathbb{F}_q^2} e^{\frac{2\pi i}{p} \mathrm{Tr}_{q/p}(-y_1 t_1 - y_2 t_2)} \sum_{x \in \mathbb{F}_{q^m}} e^{\frac{2\pi i}{p} \mathrm{Tr}_{q^m/p}(\sum_{i=1}^{2} y_i (xL_i(x) + M_i(x)))} \right) \\
= \; & \frac{1}{q^2} \left(q^m + \sum_{y_1 u_1 + y_2 u_2 \neq 0} e^{\frac{2\pi i}{p} \mathrm{Tr}_{q/p}(-y_1 t_1 - y_2 t_2)} \sum_{x \in \mathbb{F}_{q^m}} e^{\frac{2\pi i}{p} \mathrm{Tr}_{q^m/p}(\sum_{i=1}^{2} y_i (xL_i(x) + M_i(x)))} \right).
\end{aligned}$$

The conclusion then follows. □

3.4 Constructions

In this section, we present our general constructions of type I and type II codes using additive polynomials. Our source spaces $\mathcal{S}$ are specific subsets of $\mathbb{F}_{q^m}^{h+1} \times \mathbb{F}_{q^m}$. For any $(\mathbf{u}, v) = (u_0, u_1, \ldots, u_h, v) \in \mathbb{F}_{q^m}^{h+1} \times \mathbb{F}_{q^m}$ we have corresponding additive polynomials $L(x) = u_0 x + u_1 x^q + \cdots + u_h x^{q^h}$ and $M(x) = vx$. In our constructions the probabilities $\mathcal{P}_\mathcal{I}$ and $\mathcal{P}_\mathcal{S}$ depend on the dimension of the radical W_L. By the definition of W_L, as $L \neq 0$, we know that $\dim_{\mathbb{F}_q} W_L \leq 2h$. But in many cases it is possible to have $\dim_{\mathbb{F}_q} W_L < 2h$. If $\dim_{\mathbb{F}_q} W_L < 2h$, then our bounds in Lemma 3.3.1 and Lemma 3.3.2 are better than the bounds of [31, Lemma 6 and Lemma 9] in some cases. Remark 3.2.5 and Corollary 3.3.3 give further improvements for some choices of $L(x)$.

3.4.1 Construction of Type I

In this construction we choose our source spaces $\mathcal{S} \subseteq \mathbb{F}_{q^m}^{h+1} \times \mathbb{F}_{q^m}$ such that for any two different elements $(\mathbf{u}_1, v_1) = (u_{1,0}, u_{1,1}, \ldots, u_{1,h}, v_1)$, $(\mathbf{u}_2, v_2) = (u_{2,0}, u_{2,1}, \ldots, u_{2,h}, v_2)$ in the source space $\mathcal{S}$ with corresponding additive polynomials $L_i(x) = u_{i,0}x + u_{i,1}x^q + \cdots + u_{i,h}x^{q^h}$ and $M_i(x) = v_i x$, $(i = 1, 2)$, we have $\dim_{\mathbb{F}_q} W_{L_1 - L_2}$ is small enough when $L_1 \neq L_2$. The systematic authentication code is defined by

$$\begin{cases} \mathcal{S} \subseteq & \mathbb{F}_{q^m}^{h+1} \times \mathbb{F}_{q^m} \\ \mathcal{T} = & \mathbb{F}_q \\ \mathcal{K} = & \mathbb{F}_{q^m} \times \mathbb{F}_q \\ \mathcal{E} = & \{E_k : E_k(\mathbf{u}, v) = \mathrm{Tr}(k_1 L(k_1) + M(k_1)) + k_2\} \end{cases} \tag{3.4.1}$$

where $k = (k_1, k_2) \in \mathcal{K}$, $(\mathbf{u}, v) \in \mathcal{S}$ such that $\mathbf{u} = (u_0, u_1, \ldots, u_h) \in \mathbb{F}_{q^m}^{h+1}$, $v \in \mathbb{F}_{q^m}$ with $L(x) = u_0 x + u_1 x^q + \cdots + u_h x^{q^h}$ and $M(x) = vx$.

Theorem 3.4.1. *Let d be the maximum of $\dim_{\mathbb{F}_q} W_{\bar{L}}$ over the set of additive polynomials $\bar{L} = L_1 - L_2$, where $L_1 \neq L_2$, and L_1 and L_2 are defined by the coefficients of $(h+1)$-tuples $\mathbf{u}_1 = (u_{1,0}, u_{1,1}, \ldots, u_{1,h})$ and $\mathbf{u}_2 = (u_{2,0}, u_{2,1}, \ldots, u_{2,h})$ running through the first $(h+1)$-tuples of $\mathcal{S}$. Then the systematic authentication code defined in (3.4.1) has the following parameters:*

$$|\mathcal{S}| \leq q^{m(h+2)}, \quad |\mathcal{T}| = q, \quad |\mathcal{K}| = q^{m+1}, \quad \mathcal{P}_\mathcal{I} = \frac{1}{q},$$

$$\mathcal{P}_\mathcal{S} \leq \begin{cases} \frac{1}{q} + \frac{q-1}{q} \cdot \frac{q^{\frac{d}{2}}}{q^{\frac{m}{2}}} & \text{if } q \text{ is even, or } q \text{ is odd and } d \equiv m \bmod 2 \\ \frac{1}{q} + \frac{q^{\frac{d-1}{2}}}{q^{\frac{m}{2}}} & \text{if } q \text{ is odd and } d \equiv m+1 \bmod 2. \end{cases}$$

Proof. Assume we have any message $(\mathbf{u}, v) \in \mathcal{S}$ with the corresponding polynomials $L(x)$ and

$M(x)$ respectively and $k = (k_1, k_2) \in \mathcal{K}$. By (1.1.3) we have

$$\mathcal{P}_{\mathcal{I}} = max_{(\mathbf{u},v)\in\mathcal{S},t\in\mathcal{T}} \frac{|\{k \in \mathcal{K} : t = \mathrm{Tr}(k_1 L(k_1) + M(k_1)) + k_2\}|}{|\{k \in \mathcal{K}\}|} = \frac{1}{q}.$$

We now estimate an upper bound for $\mathcal{P}_{\mathcal{S}}$. Let $(\bar{\mathbf{u}}, \bar{v}) \neq (\mathbf{u}, v) \in \mathcal{S}$ with the corresponding polynomials $\bar{L}(x)$ and $\bar{M}(x)$ respectively, then by (1.1.4) we have

$$\begin{aligned}
\mathcal{P}_{\mathcal{S}} &= max_{(\mathbf{u},v)\in\mathcal{S},t\in\mathcal{T}} max_{(\bar{\mathbf{u}},\bar{\mathbf{v}})\in\mathcal{S},(\bar{\mathbf{u}},\bar{\mathbf{v}})\neq(\mathbf{u},v),\bar{t}\in\mathcal{T}} \\
&\quad \frac{|\{k \in \mathcal{K} : t = \mathrm{Tr}(k_1 L(k_1) + M(k_1)) + k_2, \bar{t} = \mathrm{Tr}(k_1 \bar{L}(k_1) + \bar{M}(k_1)) + k_2\}|}{|\{k \in \mathcal{K} : t = \mathrm{Tr}(k_1 L(k_1) + M(k_1)) + k_2\}|} \\
&= max_{(\mathbf{u},v)\in\mathcal{S},t\in\mathcal{T}} max_{(\bar{\mathbf{u}},\bar{\mathbf{v}})\in\mathcal{S},(\bar{\mathbf{u}},\bar{\mathbf{v}})\neq(\mathbf{u},v),\bar{t}\in\mathcal{T}} \\
&\quad \frac{|\{k_1 \in \mathbb{F}_{q^m} : t - \bar{t} = \mathrm{Tr}(k_1(L(k_1) - \bar{L}(k_1)) + (M(k_1) - \bar{M}(k_1))\}|}{q^m} \\
&\leq \frac{1}{q^m} \cdot \begin{cases} q^{m-1} + \frac{q-1}{q} \cdot q^{\frac{m+d_L}{2}} & \text{if } q \text{ is even, or } q \text{ is odd and } d_L \equiv m \bmod 2 \\ q^{m-1} + q^{\frac{m+d_L-1}{2}} & \text{if } q \text{ is odd and } d_L \equiv m+1 \bmod 2, \end{cases} \\
&\quad \text{by Lemma 3.3.1.}
\end{aligned}$$

The remaining conclusions of this theorem are clear. □

3.4.2 Construction of Type II

Here we classify the elements in $\mathbb{F}_{q^m}^{h+1} \times \mathbb{F}_{q^m} \setminus \{(\mathbf{0}, 0)\}$ into $(q^{m(h+2)} - 1)/(q - 1)$ equivalent classes, where two elements are in the same class if and only if they are constant multiple of each other (i.e. $\mathbf{u}_1 = c \cdot \mathbf{u}_2$, for some $c \in \mathbb{F}_q^*$). By taking only one element from each classes we define the set $\mathcal{S}'$. Similar to the previous construction we can construct type II code as follows:

$$\begin{cases} \mathcal{S} \subseteq & \mathcal{S}' \subseteq (\mathbb{F}_{q^m}^{h+1} \times \mathbb{F}_{q^m}) \setminus \{(\mathbf{0}, 0)\} \\ \mathcal{T} = & \mathbb{F}_q \\ \mathcal{K} = & \mathbb{F}_{q^m} \\ \mathcal{E} = & \{E_k : E_k(\mathbf{u}, v) = \mathrm{Tr}(kL(k) + M(k))\} \end{cases} \tag{3.4.2}$$

where $k \in \mathcal{K}$, $(\mathbf{u}, v) \in \mathcal{S}$ such that $\mathbf{u} = (u_0, u_1, \ldots, u_h) \in \mathbb{F}_{q^m}^{h+1}$, $v \in \mathbb{F}_{q^m}$ with $L(x) = u_0 x + u_1 x^q + \cdots + u_h x^{q^h}$ and $M(x) = vx$.

Theorem 3.4.2. *Let d be the maximum of $\dim_{\mathbb{F}_q} W_{\bar{L}}$ over the set of additive polynomials $\bar{L} = y_1 L_1 + y_2 L_2$, $(0,0) \neq (y_1, y_2) \in {\mathbb{F}_q}^2$ where L_1 and L_2 are defined by the coefficients of $(h+1)$-tuples $\mathbf{u}_1 = (u_{1,0}, u_{1,1}, \ldots, u_{1,h})$ and $\mathbf{u}_2 = (u_{2,0}, u_{2,1}, \ldots, u_{2,h})$ running through the first $(h+1)$-tuples of $\mathcal{S}$. Then the systematic authentication code defined in (3.4.2) has the following parameters:*

$$|\mathcal{S}| \leq \frac{q^{m(h+2)} - 1}{q - 1}, \quad |\mathcal{T}| = q, \quad |\mathcal{K}| = q^m,$$

$$\mathcal{P}_{\mathcal{I}} \leq \begin{cases} \frac{1}{q} + \frac{q-1}{q} \cdot \frac{q^{\frac{d}{2}}}{q^{\frac{m}{2}}} & \textit{if } q \textit{ is even, or } q \textit{ is odd and } d \equiv m \textit{ mod } 2 \\ \frac{1}{q} + \frac{q^{\frac{d-1}{2}}}{q^{\frac{m}{2}}} & \textit{if } q \textit{ is odd and } d \equiv m+1 \textit{ mod } 2. \end{cases}$$

$$\mathcal{P}_{\mathcal{S}} \leq \begin{cases} \frac{1}{q} + \frac{(q^2+q-2)q^{\frac{d}{2}}}{q\left(q^{\frac{m}{2}} - (q-1)q^{\frac{d}{2}}\right)} & \textit{if } q \textit{ is even, or } q \textit{ is odd and } d \equiv m \textit{ mod } 2 \\ \frac{1}{q} + \frac{(q+2)q^{\frac{d-1}{2}}}{q^{\frac{m}{2}} - q^{\frac{d+1}{2}}} & \textit{if } q \textit{ is odd and } d \equiv m+1 \textit{ mod } 2. \end{cases}$$

Proof. We first estimate an upper bound for $\mathcal{P}_{\mathcal{I}}$. Assume we have any message $(\mathbf{u}, v) \in \mathcal{S}$ with corresponding polynomials L and M respectively and $k \in \mathcal{K}$. By (1.1.3) we have

$$\begin{aligned} \mathcal{P}_{\mathcal{I}} &= max_{(\mathbf{u},v)\in\mathcal{S},t\in\mathcal{T}} \frac{|\{k \in \mathcal{K} : t = \mathrm{Tr}(kL(k) + M(k))\}|}{|\{k \in \mathcal{K}\}|} \\ &\leq \frac{1}{q^m} \cdot \begin{cases} q^{m-1} + \frac{q-1}{q} \cdot q^{\frac{m+d}{2}} & \text{if } q \text{ is even, or } q \text{ is odd and } d \equiv m \bmod 2 \\ q^{m-1} + q^{\frac{m+d-1}{2}} & \text{if } q \text{ is odd and } d \equiv m+1 \bmod 2, \end{cases} \\ &\quad \text{by Lemma 3.3.1.} \end{aligned}$$

We now prove the upper bound on $\mathcal{P}_{\mathcal{S}}$. Let $(\bar{\mathbf{u}}, \bar{v}) \neq (\mathbf{u}, v) \in \mathcal{S}$ with the corresponding polynomials $\bar{L}(x)$ and $\bar{M}(x)$ respectively, then by (1.1.4) we have

$$\begin{aligned} \mathcal{P}_{\mathcal{S}} &= max_{(\mathbf{u},v)\in\mathcal{S},t\in\mathcal{T}} max_{(\bar{\mathbf{u}},\bar{v})\in\mathcal{S},(\bar{\mathbf{u}},\bar{v})\neq(\mathbf{u},v),\bar{t}\in\mathcal{T}} \\ &\quad \frac{|\{k \in \mathcal{K} : t = \mathrm{Tr}(kL(k) + M(k)), \bar{t} = \mathrm{Tr}(k\bar{L}(k) + \bar{M}(k))\}|}{|\{k \in \mathcal{K} : t = \mathrm{Tr}(kL(k) + M(k))\}|} \\ &= \frac{max_{(\mathbf{u},v),(\bar{\mathbf{u}},\bar{v})\in\mathcal{S},(\bar{\mathbf{u}},\bar{v})\neq(\mathbf{u},v),t,\bar{t}\in\mathcal{T}} N(\mathbf{u}, \bar{\mathbf{u}}, v, \bar{v}; t, \bar{t})}{min_{(\mathbf{u},v)\in\mathcal{S},t\in\mathcal{T}} N(\mathbf{u}, v; t)} \\ &\leq \begin{cases} \frac{1}{q} + \frac{(q^2+q-2)q^{\frac{d}{2}}}{q\left(q^{\frac{m}{2}} - (q-1)q^{\frac{d}{2}}\right)} & \text{if } q \text{ is even, or } q \text{ is odd and } d \equiv m \bmod 2 \\ \frac{1}{q} + \frac{(q+2)q^{\frac{d-1}{2}}}{q^{\frac{m}{2}} - q^{\frac{d+1}{2}}} & \text{if } q \text{ is odd and } d \equiv m+1 \bmod 2 \end{cases} \\ &\quad \text{by using Lemma 3.3.1 and Lemma 3.3.2.} \end{aligned}$$

The remaining conclusions of the theorem are clear. □

3.5 Examples

In this section we present examples of systematic authentication codes having good parameters. In order to compare our examples with a larger class of existing codes, we have restricted ourselves to the source spaces such that the parameter d of Theorem 3.4.1 and Theorem 3.4.2 are bounded as $d \leq 1$ or $d \leq 2$. We note that further codes with good parameters can be obtained by increasing the upper bound on d slightly.

Example 3.5.1. Let q be a power of an odd prime and $h \geq 0$. Let $\mathcal{S}$ be the subset of $\mathbb{F}_{q^m}^{h+1} \times \mathbb{F}_{q^m}$ such that the corresponding 2-tuples $(L(x), M(x))$ of additive polynomials form the set $\{(ax^{q^h}, bx) : a, b \in \mathbb{F}_{q^m}\}$. Assume that $m/gcd(h, m/2)$ is odd for $h > 0$, then for any nonzero $L(x) = ax^{q^h}$ below we prove that $\dim_{\mathbb{F}_q} W_L = 0$. Then by Theorem 3.4.1 the parameters of the type I code in (3.4.1) become

$$|\mathcal{S}| = q^{2m}, \quad |\mathcal{T}| = q, \quad |\mathcal{K}| = q^{m+1}, \quad \mathcal{P}_{\mathcal{I}} = \frac{1}{q}, \quad \mathcal{P}_{\mathcal{S}} \leq \begin{cases} \frac{1}{q} + \frac{q-1}{q} \cdot \frac{1}{q^{m/2}} & \text{if } m \text{ is even} \\ \frac{1}{q} + \frac{1}{q^{(m+1)/2}} & \text{if } m \text{ is odd.} \end{cases}$$

Similarly, using Corollary 3.3.3 and Theorem 3.4.2 the parameters of the type II code in (3.4.2) become

$$|\mathcal{S}| = \frac{q^{2m}-1}{q-1}, \quad |\mathcal{T}| = q, \quad |\mathcal{K}| = q^m,$$

$$\mathcal{P}_{\mathcal{I}} \leq \begin{cases} \frac{1}{q} + \frac{q-1}{q} \cdot \frac{1}{q^{m/2}} & \text{if } m \text{ is even} \\ \frac{1}{q} + \frac{1}{q^{(m+1)/2}} & \text{if } m \text{ is odd,} \end{cases} \quad \mathcal{P}_{\mathcal{S}} \leq \begin{cases} \frac{1}{q} + \frac{q^2-1}{q(q^{m/2}-q+1)} & \text{if } m \text{ is even} \\ \frac{1}{q} + \frac{q+1}{q^{(m+1)/2}-q} & \text{if } m \text{ is odd.} \end{cases}$$

Now we prove that for any nonzero $L(x) = ax^{q^h}$ $\dim_{\mathbb{F}_q} W_L = 0$. By definition we have $W_L = \{z \in \mathbb{F}_{q^m} : az + a^{q^h} z^{q^{2h}} = 0\}$. Let w be a generator of the multiplicative group $\mathbb{F}_{q^m} \setminus \{0\}$ and $a = w^s$ for some integer s. Assume that $w^l \in W_S$ for an integer $l \geq 0$. Then

$$\begin{aligned} w^s w^l + w^{sq^h} w^{lq^{2h}} = 0 \quad &\Rightarrow \quad 1 + w^{s(q^h-1)+l(q^{2h}-1)} = 0 \\ &\Rightarrow \quad w^{s(q^h-1)+l(q^{2h}-1)} = w^{\frac{q^m-1}{2}}, \text{ as } q \text{ is odd.} \end{aligned}$$

Hence we obtain that

$$l(q^{2h}-1) + s(q^h-1) \equiv \frac{q^m-1}{2} \bmod (q^m-1). \tag{3.5.1}$$

Let $k = gcd(m, 2h)$. Note that $gcd(q^m-1, q^{2h}-1) = q^k-1$. There exists a solution l of (3.5.1) if and only if

$$s(q^h-1) \equiv \frac{q^m-1}{2} \bmod q^k-1. \tag{3.5.2}$$

As $m/gcd(h, m/2)$ is odd, we have that q^k-1 divides q^h-1. So (3.5.2) holds if and only if q^k-1 divides $\frac{q^m-1}{2}$ which is not the case because

$$\frac{q^m-1}{2} = (q^k-1)\frac{1+q^k+q^{2k}+\cdots+q^{(\frac{m}{k}-1)k}}{2}$$

where m/k is odd and so $1+q^k+q^{2k}+\cdots+q^{(\frac{m}{k}-1)k}$ is odd. Therefore $\dim_{\mathbb{F}_q} W_L = 0$.

In the following examples using Trachtenberg Lemma 4 [66] we obtain upper bounds on $\dim_{\mathbb{F}_q} W_L$.

Example 3.5.2. Assume that q is even, m is odd, $h \geq 1$ and $gcd(m,h) = 1$. Let $\mathcal{S}$ be the subset of $\mathbb{F}_{q^m}^{h+1} \times \mathbb{F}_{q^m}$ such that the corresponding 2-tuples $(L(x), M(x))$ of additive polynomials form the set $\{(ax^{q^h}, bx) : a, b \in \mathbb{F}_{q^m}\}$. In this example for any nonzero additive polynomial L below we prove that $\dim_{\mathbb{F}_q} W_L \leq 1$ and if $\dim_{\mathbb{F}_q} W_L = 1$ then $W_L \not\subseteq V_L$. Therefore using Theorem 3.2.1, Remark 3.2.5 and Theorem 3.4.1 the parameters of the type I code in (3.4.1) become

$$|\mathcal{S}| = q^{2m}, \quad |\mathcal{T}| = q, \quad |\mathcal{K}| = q^{m+1}, \quad \mathcal{P}_{\mathcal{I}} = \frac{1}{q}, \quad \mathcal{P}_{\mathcal{S}} \leq \frac{1}{q} + \frac{1}{q^{(m+1)/2}}.$$

Similarly, using Theorem 3.2.1, Remark 3.2.5, Corollary 3.3.3 and Theorem 3.4.2 the parameters of the type II code in (3.4.2) become

$$|\mathcal{S}| = \frac{q^{2m}-1}{q-1}, \quad |\mathcal{T}| = q, \quad |\mathcal{K}| = q^m,$$

$$\mathcal{P}_{\mathcal{I}} \leq \frac{1}{q} + \frac{1}{q^{(m+1)/2}}, \quad \mathcal{P}_{\mathcal{S}} \leq \frac{1}{q} + \frac{q+2}{q^{(m+1)/2}-q}.$$

Now we prove our assertions that $\dim_{\mathbb{F}_q} W_L \leq 1$ and $W_L \not\subseteq V_L$. By definition we have $W_L = \{z \in \mathbb{F}_{q^m} : az + a^{q^h} z^{q^{2h}} = 0\}$. For $a \neq 0$ the equation $az + a^{q^h} z^{q^{2h}} = 0$ has at most q^{2h} solution in the algebraic closure of $\mathbb{F}_q$ and therefore, W_L has dimension at most 1 over $\mathbb{F}_{q^{2h}}$. Since $gcd(m, 2h) = 1$, using [66, Lemma 4] we have W_L has dimension at most 1 over $\mathbb{F}_{q^m}$. Recall that $V_L = \{x \in \mathbb{F}_{q^m} : \mathrm{Tr}(xL(x)) = \mathrm{Tr}(ax^{q^h+1}) = 0\}$. But if $z \in W_L \setminus \{0\}$ we have $az + a^{q^h} z^{q^{2h}} = 0$, that is, $(az^{q^h+1})^{q^h-1} = 1$. Since $az^{q^h+1} \in \mathbb{F}_{q^m} \setminus \{0\}$ and $gcd(q^h - 1, q^m - 1) = q - 1$, we have $az^{q^h+1} \in \mathbb{F}_q$. Therefore, $\mathrm{Tr}(az^{q^h+1}) = maz^{q^h+1} \neq 0$ as m is odd and q is even.

In the following example we obtain larger source spaces than the previous examples.

Example 3.5.3. Let q be a power of a prime, $m \geq 1$. Let $\{i_1, i_2, \ldots, i_t\}$ be the set of integers between 1 and $\lfloor m/2 \rfloor$ that are relatively prime to m such that $i_{j_1} < i_{j_2}$ if $j_1 < j_2$. Define $L(x) = u_{i_1} x^{q^{i_1}} + u_{i_2} x^{q^{i_2}} + \cdots + u_{i_t} x^{q^{i_t}}$ and $M(x) = vx$ where $(u_{i_1}, u_{i_2}, \ldots, u_{i_t}) \in \mathbb{F}_{q^m}^t$ and $v \in \mathbb{F}_{q^m}$. In this example for any $L \neq 0$, using [66, Lemma 4] we get

$$\dim_{\mathbb{F}_q} W_L \leq \begin{cases} 2 & \text{if } m \text{ is even} \\ 1 & \text{if } m \text{ is odd.} \end{cases}$$

Below we prove this assertion similar to the proof in Example 3.5.2. Then using Theorem 3.4.1 the parameters of the type I code in (3.4.1) become

$$|\mathcal{S}| = q^{m(t+1)}, \quad |\mathcal{T}| = q, \quad |\mathcal{K}| = q^{m+1}, \quad \mathcal{P}_{\mathcal{I}} = \frac{1}{q}, \quad \mathcal{P}_{\mathcal{S}} \leq \begin{cases} \frac{1}{q} + \frac{q-1}{q^{m/2}} & \text{if } m \text{ is even} \\ \frac{1}{q} + \frac{q-1}{q^{(m+1)/2}} & \text{if } m \text{ is odd.} \end{cases}$$

Similarly, using Theorem 3.4.2 the parameters of the type II code in (3.4.2) become

$$|\mathcal{S}| = \frac{q^{m(t+1)}-1}{q-1}, \quad |\mathcal{T}| = q, \quad |\mathcal{K}| = q^m,$$

$$\mathcal{P}_{\mathcal{I}} \leq \begin{cases} \frac{1}{q} + \frac{q-1}{q^{m/2}} & \text{if } m \text{ is even} \\ \frac{1}{q} + \frac{q-1}{q^{(m+1)/2}} & \text{if } m \text{ is odd,} \end{cases} \quad \mathcal{P}_{\mathcal{S}} \leq \begin{cases} \frac{1}{q} + \frac{q^2+q-2}{q^{m/2}-q^2+q} & \text{if } m \text{ is even} \\ \frac{1}{q} + \frac{q^2+q-2}{q^{(m+1)/2}-q^2+q} & \text{if } m \text{ is odd.} \end{cases}$$

Now we prove our assertion that $\dim_{\mathbb{F}_q} W_L \leq \begin{cases} 2 & \text{if } m \text{ is even} \\ 1 & \text{if } m \text{ is odd.} \end{cases}$ By definition we know that the elements of W_L are the roots of some specific linearized polynomial, say $g_L(z)$. We have $deg(g_L(z)) = q^{2i_t}$ over $\mathbb{F}_{q^m}$. Then for any $L \neq 0$ the polynomial $g_L(z)$ has at most q^{2i_t} roots in the algebraic closure of $\mathbb{F}_q$ and therefore, W_L has dimension at most 1 over $\mathbb{F}_{q^{2i_t}}$ and at most 2 over $\mathbb{F}_{q^{i_t}}$. We know that $gcd(m, i_t) = 1$ and so $gcd(m, 2i_t) = 1$ if m is odd. Therefore, using [66, Lemma 4] we obtain the desired result.

3.6 Comparisons With Some Known Authentication Codes

In this section we will compare our results with some known codes [18, 31, 7] and the codes given in Proposition 2.3.2. It is known that the systematic authentication codes have at least five parameters $|\mathcal{S}|$, $|\mathcal{T}|$, $|\mathcal{K}|$, $\mathcal{P}_{\mathcal{I}}$, and $\mathcal{P}_{\mathcal{S}}$. To compare two systematic authentication codes we need to fix at least three of the five parameters to be the same respectively.

3.6.1 Comparisons With the Authentication Codes of [18]

In [18] authentication codes with parameters

$$|\mathcal{S}| = q^{2n}, \;\; |\mathcal{T}| = q, \;\; |\mathcal{K}| = q^{n+1}, \;\; \mathcal{P}_{\mathcal{I}} = \frac{1}{q}, \;\; \mathcal{P}_{\mathcal{S}} \leq \frac{1}{q} + \frac{(q-1)}{q} \cdot \frac{1}{q^{n/2}}$$

are constructed using highly nonlinear functions where q is a power of an odd prime [18, Theorem 2].

If we set $n = m$ is odd, our type I codes in Example 3.5.1 have exactly the same parameters with this subclass of codes in [18, Theorem 2] except $\mathcal{P}_{\mathcal{S}}$, which is smaller than that of the codes in [18, Theorem 2].

Also in [18] authentication codes with parameters

$$|\mathcal{S}| = q^n + 1, \; |\mathcal{T}| = q, \; |\mathcal{K}| = q^n, \; \mathcal{P}_{\mathcal{I}} = \frac{1}{q} + \frac{(q-1)}{q} \cdot \frac{1}{q^{n/2}}, \; \mathcal{P}_{\mathcal{S}} \leq \frac{1}{q} + \frac{(q^2-1)}{q(q^{n/2}-q+1)}$$

are constructed using highly nonlinear functions where q is a power of an odd prime [18, Theorem 4].

If we set $n = m$ is even, our type II codes in Example 3.5.1 have exactly the same parameters with this subclass of codes in [18, Theorem 4] except $|\mathcal{S}|$. It is clear that our type II codes in Example 3.5.1 have larger source space. Furthermore, if we set $n = m$ is odd, $\mathcal{P}_{\mathcal{I}}$ and $\mathcal{P}_{\mathcal{S}}$ of

our type II codes in Example 3.5.1 are smaller and $|\mathcal{S}|$ of our type II codes in Example 3.5.1 is larger than that of the codes in [18, Theorem 2]. For this case the other parameters $|\mathcal{T}|$ and $|\mathcal{K}|$ are the same respectively.

3.6.2 Comparisons With the Authentication Codes of [31]

In [31] authentication codes with parameters

$$|\mathcal{S}| = q^{n(D-\lfloor D/p \rfloor)},\ |\mathcal{T}| = q,\ |\mathcal{K}| = q^{n+1},\ \ \mathcal{P}_{\mathcal{I}} = \frac{1}{q},\ \ \mathcal{P}_{\mathcal{S}} \leq \frac{1}{q} + \frac{D-1}{q^{n/2}}$$

are constructed using exponential sums over finite fields, where D is an integer $1 \leq D \leq q^{n/2}$ and p is the characteristic of the finite field $\mathbb{F}_q$ [31, Corollary 8].

In the case q is odd (that is $p > 2$) these codes are comparable with our type I codes in Example 3.5.1 for $D = 2$. If we set $n = m$, the parameters of the subclass of codes in [31, Corollary 8] become

$$|\mathcal{S}| = q^{2m},\ |\mathcal{T}| = q,\ |\mathcal{K}| = q^{m+1},\ \ \mathcal{P}_{\mathcal{I}} = \frac{1}{q},\ \ \mathcal{P}_{\mathcal{S}} \leq \frac{1}{q} + \frac{1}{q^{m/2}}.$$

It can be easily seen that our type I codes in Example 3.5.1 have exactly the same parameters with this subclass of codes in [31, Corollary 8], except the probability $\mathcal{P}_{\mathcal{S}}$, which is smaller than that of the codes in [31, Corollary 8].

In the case q is even (that is $p = 2$) and m is odd these codes are comparable with our type I codes in Example 3.5.2 for $D = 3$. If we set $n = m$, the parameters of the subclass of codes in [31, Corollary 8] become

$$|\mathcal{S}| = q^{2m},\ |\mathcal{T}| = q,\ |\mathcal{K}| = q^{m+1},\ \ \mathcal{P}_{\mathcal{I}} = \frac{1}{q},\ \ \mathcal{P}_{\mathcal{S}} \leq \frac{1}{q} + \frac{2}{q^{m/2}}.$$

For this case our type I codes in Example 3.5.2 have exactly the same parameters with this subclass of codes in [31, Corollary 8], except the probability $\mathcal{P}_{\mathcal{S}}$, which is smaller than that of the codes in [31, Corollary 8].

3.6.3 Comparisons With the Authentication Codes in Section 2.3

In Proposition 2.3.2 systematic authentication codes with parameters

$$|\mathcal{S}| = q^{n(D-\lfloor D/p^2 \rfloor)},\ |\mathcal{T}| = q,\ |\mathcal{K}| = q^{n+2},\ \ \mathcal{P}_{\mathcal{I}} = \frac{1}{q},\ \ \mathcal{P}_{\mathcal{S}} \leq \frac{1}{q} + \frac{(q-1)}{q} \cdot \frac{D-1}{q^{n/2}}$$

are constructed using exponential sums over Galois rings and generalized Gray map, where D is an integer $1 \leq D \leq q^{n/2}$ and p^2 is the characteristic of the Galois ring $GR(p^2, m)$.

In order to compare the codes in Proposition 2.3.2 with our codes in Example 3.5.1 and in Example 3.5.2 we set $D = 2$ and $n = m$. Then the parameters of the subclass of codes in Proposition 2.3.2 become

$$|\mathcal{S}| = q^{2m},\ |\mathcal{T}| = q,\ |\mathcal{K}| = q^{m+2},\ \ \mathcal{P}_{\mathcal{I}} = \frac{1}{q},\ \ \mathcal{P}_{\mathcal{S}} \leq \frac{1}{q} + \frac{(q-1)}{q} \cdot \frac{1}{q^{m/2}}.$$

If q is odd and m is even, it can be easily seen that our type I codes in Example 3.5.1 has exactly the same parameters with this subclass of codes in Proposition 2.3.2, except the size of the key space $|\mathcal{K}|$, which is smaller than that of the codes in Proposition 2.3.2. Furthermore, if m is odd for any q, the size of the key space $|\mathcal{K}|$ and $\mathcal{P}_{\mathcal{S}}$ of our type I codes in Example 3.5.1 and Example 3.5.2 are smaller than those of the codes in Proposition 2.3.2 respectively. For this case the other parameters are the same respectively.

3.6.4 Comparisons With the Authentication Codes of [7]

In [7] authentication codes with parameters

$$|\mathcal{S}| = 2^{2n},\ \ |\mathcal{T}| = 2^r,\ \ |\mathcal{K}| = 2^{n+r},\ \ \mathcal{P}_{\mathcal{I}} = \frac{1}{2^r},\ \ \mathcal{P}_{\mathcal{S}} \leq \frac{1}{2^r} + \frac{(1-2^{-r})}{2^{(n-1)/2}}$$

are constructed using almost bent functions f from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ [7, Example 1].

In order to compare the codes in [7, Example 1] with our type I codes in Example 3.5.2 we set m, n are odd, $n = rm$ and $2^r = q$. Then the parameters of the codes in [7, Example 1] become

$$|\mathcal{S}| = q^{2m},\ \ |\mathcal{T}| = q,\ \ |\mathcal{K}| = q^{m+1},\ \ \mathcal{P}_{\mathcal{I}} = \frac{1}{q},\ \ \mathcal{P}_{\mathcal{S}} \leq \frac{1}{q} + \frac{q-1}{q} \cdot \frac{\sqrt{2}}{q^{m/2}}.$$

So the $\mathcal{P}_{\mathcal{S}}$ of our type I codes in Example 3.5.2 is smaller than that of [7, Example 1].

Also in [7] authentication codes with parameters

$$|\mathcal{S}| = 2^n + 1,\ \ |\mathcal{T}| = 2^r,\ \ |\mathcal{K}| = 2^n,$$
$$\mathcal{P}_{\mathcal{I}} \leq \frac{1}{2^r} + \frac{(1-2^{-r})}{2^{(n-1)/2}},\ \ \mathcal{P}_{\mathcal{S}} \leq \frac{1}{2^r} + \frac{(2^r - 2^{-r})}{2^{(n-1)/2} - 2^r + 1}$$

are constructed using almost bent functions f from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ [7, Example 2].

In order to compare the codes in [7, Example 2] with our type II codes in Example 3.5.2 we set m, n are odd, $n = rm$ and $2^r = q$. Then the parameters of the codes in [7, Example 1] become

$$|\mathcal{S}| = q^m + 1,\ \ |\mathcal{T}| = q,\ \ |\mathcal{K}| = q^m,$$
$$\mathcal{P}_{\mathcal{I}} \leq \frac{1}{q} + \frac{q-1}{q} \cdot \frac{\sqrt{2}}{q^{m/2}},\ \ \mathcal{P}_{\mathcal{S}} \leq \frac{1}{q} + \frac{\sqrt{2}(q^2-1)}{q^{m/2} - \sqrt{2}(q-1)}.$$

It can be easily seen that $\mathcal{P}_{\mathcal{I}}$ and $\mathcal{P}_{\mathcal{S}}$ of our type II codes in Example 3.5.2 are smaller and $|\mathcal{S}|$ of our type II codes in Example 3.5.2 is larger than that of the codes in [7, Example 2]. For this case the other parameters $|\mathcal{T}|$ and $|\mathcal{K}|$ are the same respectively.

Chapter 4

Authentication Codes With Secrecy Using Additive Polynomials

In this chapter three different constructions of authentication codes with secrecy using additive polynomials related to some curves over finite fields are given. Tight bounds for the number of rational points of these curves are used in estimating the probabilities of the codes. First two constructions are generalizations of the corresponding constructions in [20] and [19] using additive polynomials. The last specific construction answers the open problem given in [19, Section 6.3.1] for some cases.

4.1 Introduction

Let q be a power of a prime p and $m > 1$ be an integer. Throughout this chapter $\mathbb{F}_{q^m}$ denotes the finite field of cardinality q^m and we use the same notations given in Section 3.2.

In our constructions, the first part of the message (encrypted part) is obtained by addition of the source state and a part of the key. This addition guarantees that the encryption is done in a secure way. We propose three different methods to get the second part of the message (tag part). In Construction (4.2.1) and Construction (4.2.2), first we evaluate the source state by an additive polynomial, and we multiply the result by a part of the key in $\mathbb{F}_{q^m}$. Then we take traces to $\mathbb{F}_q$, which is the tag space. In Construction (4.2.1) we further use a part of the key for an addition in $\mathbb{F}_q$. In Construction (4.3.1) first we evaluate the key and the source state by a specific function Π, and the results are added in $\mathbb{F}_q$. This general method proposed in [19]. But the parameters of the authentication codes are estimated only for two specific functions, and it is stated that the construction gives good authentication codes for different choices of the

specific function Π. In Section 4.3.2, we take $\Pi = \mathrm{Tr}(x^{q^h+1})$ and we estimate the parameters of the codes obtained by this general method, which answers the open problem given in [19, Section 6.3.1] for some cases.

This chapter is organized as follows. In Section 4.2 we present two types of authentication codes and estimate their parameters. In Section 4.3 we give the general construction proposed in [19]. We estimate the parameters of the authentication codes obtained by this general construction using a specific additive polynomial.

4.2 Construction I

In this section, we present two types of authentication codes with secrecy. In type I codes the number of keys and the number of messages are the same. In type II codes, the cardinality of the key spaces is smaller than the cardinality of the message spaces.

4.2.1 Construction of Type I

Let q be a power of a prime and $m > 1$ be an integer. Let $L(x) = u_0x + u_1x^q + \cdots + u_hx^{q^h} \in \mathbb{F}_{q^m}[x]$ be a nonzero additive polynomial and Tr denotes the trace map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$. Then the authentication code is defined by

$$\begin{cases} \mathcal{S} = & \mathbb{F}_{q^m} \\ \mathcal{K} = & \mathbb{F}_{q^m} \times \mathbb{F}_q \\ \mathcal{M} = & \mathbb{F}_{q^m} \times \mathbb{F}_q \\ \mathcal{E} = & \{E_k : E_k(s) = (s + k_1, \mathrm{Tr}(k_1L(s)) + k_2)\} \end{cases} \tag{4.2.1}$$

where $k = (k_1, k_2) \in \mathcal{K}$, $s \in \mathcal{S}$.

Theorem 4.2.1. *The authentication codes defined in (4.2.1) have the following parameters.*

$$|\mathcal{S}| = q^m, \quad |\mathcal{K}| = q^{m+1}, \quad |\mathcal{M}| = q^{m+1}, \quad \mathcal{P}_{\mathcal{I}} = \frac{1}{q}, \quad \mathcal{P}_{\mathcal{S}} = \frac{1}{q}.$$

Proof. For the impersonation attack the opponent picks an element $m = (m_1, m_2)$ and sends it to the receiver. The receiver will compute $s = m_1 - k_1$ and $\mathrm{Tr}(k_1L(s)) + k_2$. Then he will check whether $\mathrm{Tr}(k_1L(m_1 - k_1)) + k_2 = m_2$ or not. Hence

$$\begin{aligned} \mathcal{P}_{\mathcal{I}} &= max_{m_1,m_2}\, Pr[\mathrm{Tr}(k_1L(m_1 - k_1)) + k_2 = m_2] \\ &= max_{m_1,m_2} \frac{|\{k \in \mathcal{K} : \mathrm{Tr}(k_1L(m_1 - k_1)) + k_2 = m_2\}|}{|\{k \in \mathcal{K}\}|} \\ &= \frac{1}{q}, \end{aligned}$$

since for each $k_1 \in \mathbb{F}_{q^m}$, there is exactly one $k_2 \in \mathbb{F}_q$ satisfying $\mathrm{Tr}(k_1 L(m_1 - k_1)) + k_2 = m_2$.

We now prove the upper bound on $\mathcal{P}_{\mathcal{S}}$. For the substitution attack the opponent has observed one message $m = (m_1, m_2)$ s.t $m_1 = s + k_1$ and $m_2 = \mathrm{Tr}(k_1 L(s)) + k_2$, and he wants to replace m with another message $m' = (m_1', m_2')$, where $m_1' \neq m_1$. Set $d_1 = m_1' - m_1$ and $d_2 = m_2' - m_2$. Hence substituting m with m' is equivalent to adding $d_1 \neq 0$ to m_1 and d_2 to m_2. This is successful if and only if $\mathrm{Tr}(k_1 L(s)) + k_2 + d_2 = \mathrm{Tr}(k_1 L(s + d_1)) + k_2$, which is equivalent to $\mathrm{Tr}(k_1 L(d_1)) = d_2$. Let $d = (d_1, d_2)$ with $d_1 \neq 0$. Therefore,

$$\begin{aligned}
\mathcal{P}_{\mathcal{S}} &= max_{m,d}\, Pr[\mathrm{Tr}(k_1 L(d_1)) = d_2 \mid m_2 = \mathrm{Tr}(k_1 L(m_1 - k_1)) + k_2] \\
&= max_{m,d} \frac{|\{k \in \mathcal{K} : \mathrm{Tr}(k_1 L(m_1 - k_1)) + k_2 = m_2, \mathrm{Tr}(k_1 L(d_1)) = d_2\}|}{|\{k \in \mathcal{K} : m_2 = \mathrm{Tr}(k_1 L(m_1 - k_1)) + k_2\}} \\
&= \frac{q^{m-1}}{q^m} = \frac{1}{q},
\end{aligned}$$

since $\mathrm{Tr}(k_1 L(d_1))$ is a linear mapping, it has exactly q^{m-1} solutions and for each solution $k_1 \in \mathbb{F}_{q^m}$, there is exactly one $k_2 \in \mathbb{F}_q$ satisfying $\mathrm{Tr}(k_1 L(m_1 - k_1)) + k_2 = m_2$. The remaining conclusions of the theorem are clear. □

Theorem 4.2.2. *The authentication codes defined in (4.2.1) provides perfect secrecy.*

Proof. Given a message $m = (m_1, m_2) = (s + k_1, \mathrm{Tr}(k_1 L(s)) + k_2)$, we have that the uncertainty of the source state is $|\{s \in \mathcal{S} : \mathrm{Tr}((m_1 - s)L(s)) + k_2 = m_2\}|$. In this case, for each $s \in \mathcal{S}$, there is exactly one k_2 satisfying $\mathrm{Tr}((m_1 - s)L(s)) + k_2 = m_2$. Therefore, we have no information about s. □

Remark 4.2.3. The authentication codes in (4.2.1) are generalizations of the codes in [20, Section 4]. If we take $L(x) = x$, then we obtain exactly the same codes with the codes in [20, Section 4].

4.2.2 Construction of Type II

Let q be a power of a prime and $m > 1$ be an integer. Let $L(x) = u_0 x + u_1 x^q + \cdots + u_h x^{q^h} \in \mathbb{F}_{q^m}[x]$ be a nonzero additive polynomial, d be the dimension of the radical W_L and Tr denotes the trace map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$. Then the authentication code is defined by

$$\begin{cases}
\mathcal{S} = & \mathbb{F}_{q^m} \\
\mathcal{K} = & \mathbb{F}_{q^m} \\
\mathcal{M} = & \mathbb{F}_{q^m} \times \mathbb{F}_q \\
\mathcal{E} = & \{E_k : E_k(s) = (s + k, \mathrm{Tr}(kL(s)))\}
\end{cases} \tag{4.2.2}$$

where $k \in \mathcal{K}$, $s \in \mathcal{S}$.

Theorem 4.2.4. *Let $L(x) = u_0x + u_1x^q + \cdots + u_hx^{q^h} \in \mathbb{F}_{q^m}$ be a nonzero additive polynomial and $d = \dim W_L$. Then the authentication codes defined in (4.2.2) have the following parameters.*

$$|\mathcal{S}| = q^m, \quad |\mathcal{K}| = q^m, \quad |\mathcal{M}| = q^{m+1},$$

$$\mathcal{P}_{\mathcal{I}} \leq \begin{cases} \frac{1}{q} + \frac{q-1}{q} \cdot \frac{q^{\frac{d}{2}}}{q^{\frac{m}{2}}} & \text{if } q \text{ is even, or } q \text{ is odd and } d \equiv m \bmod 2 \\ \frac{1}{q} + \frac{q^{\frac{d-1}{2}}}{q^{\frac{m}{2}}} & \text{if } q \text{ is odd and } d \equiv m+1 \bmod 2. \end{cases}$$

$$\mathcal{P}_{\mathcal{S}} \leq \begin{cases} \frac{1}{q} + \frac{(q^2+q-2)q^{\frac{d}{2}}}{q\left(q^{\frac{m}{2}} - (q-1)q^{\frac{d}{2}}\right)} & \text{if } q \text{ is even, or } q \text{ is odd and } d \equiv m \bmod 2 \\ \frac{1}{q} + \frac{(q+2)q^{\frac{d-1}{2}}}{q^{\frac{m}{2}} - q^{\frac{d+1}{2}}} & \text{if } q \text{ is odd and } d \equiv m+1 \bmod 2. \end{cases}$$

Proof. For the impersonation attack the opponent picks an element $m = (m_1, m_2)$ and sends it to the receiver. The receiver will compute $s = m_1 - k$ and $\mathrm{Tr}(kL(s))$. Then he will check whether $\mathrm{Tr}(kL(m_1 - k)) = m_2$ or not. Hence

$$\begin{aligned} \mathcal{P}_{\mathcal{I}} &= max_{m_1,m_2}\, Pr[\mathrm{Tr}(kL(m_1-k)) = m_2] \\ &= max_{m_1,m_2} \frac{|\{k \in \mathcal{K} : \mathrm{Tr}(kL(m_1-k)) = m_2\}|}{|\{k \in \mathcal{K}\}|} \\ &= max_{m_1,m_2} \frac{|\{k \in \mathcal{K} : \mathrm{Tr}(-kL(k) + L(m_1)k)) = m_2\}|}{q^m} \\ &\leq \frac{1}{q^m} \cdot \begin{cases} q^{m-1} + \frac{q-1}{q} \cdot q^{\frac{m+d}{2}} & \text{if } q \text{ is even, or } q \text{ is odd and } d \equiv m \bmod 2 \\ q^{m-1} + q^{\frac{m+d-1}{2}} & \text{if } q \text{ is odd and } d \equiv m+1 \bmod 2, \end{cases} \\ &\quad \text{by Lemma 3.3.1.} \end{aligned}$$

We now prove the upper bound on $\mathcal{P}_{\mathcal{S}}$. For the substitution attack the opponent has observed one message $m = (m_1, m_2)$ s.t $m_1 = s + k$ and $m_2 = \mathrm{Tr}(kL(s))$, and he wants to replace m with another message $m' = (m_1', m_2')$, where $m_1' \neq m_1$. Set $d_1 = m_1' - m_1$ and $d_2 = m_2' - m_2$. Hence substituting m with m' is equivalent to adding $d_1 \neq 0$ to m_1 and d_2 to m_2. This is successful if and only if $\mathrm{Tr}(kL(s)) + d_2 = \mathrm{Tr}(kL(s + d_1))$, which is equivalent to $\mathrm{Tr}(kL(d_1)) = d_2$. Let $d = (d_1, d_2)$ with $d_1 \neq 0$. Therefore,

$$\begin{aligned} \mathcal{P}_{\mathcal{S}} &= max_{m,d}\, Pr[\mathrm{Tr}(kL(d_1)) = d_2 \mid m_2 = \mathrm{Tr}(kL(m_1-k))] \\ &= max_{m,d} \frac{|\{k \in \mathcal{K} : \mathrm{Tr}(kL(m_1-k)) = m_2, \mathrm{Tr}(kL(d_1)) = d_2\}|}{|\{k \in \mathcal{K} : m_2 = \mathrm{Tr}(kL(m_1-k))\}} \\ &\leq \begin{cases} \frac{1}{q} + \frac{(q^2+q-2)q^{\frac{d}{2}}}{q\left(q^{\frac{m}{2}} - (q-1)q^{\frac{d}{2}}\right)} & \text{if } q \text{ is even, or } q \text{ is odd and } d \equiv m \bmod 2 \\ \frac{1}{q} + \frac{(q+2)q^{\frac{d-1}{2}}}{q^{\frac{m}{2}} - q^{\frac{d+1}{2}}} & \text{if } q \text{ is odd and } d \equiv m+1 \bmod 2 \end{cases} \\ &\quad \text{by using Lemma 3.3.1 and Lemma 3.3.2.} \end{aligned}$$

The remaining conclusions of the theorem are clear. □

To estimate the secrecy level of the authentication codes defined in (4.2.2) we need the following lemma.

Lemma 4.2.5. *Let* $L(x) = u_0x + u_1x^q + \cdots + u_hx^{q^h} \in \mathbb{F}_{q^m}$ *be a nonzero additive polynomial and* $d = \dim W_L$. *For* $v \in \mathbb{F}_{q^m}$ *and for* $t \in \mathbb{F}_q$ *put*

$$N(L, v; t) = |\{x \in \mathbb{F}_{q^m} : \mathrm{Tr}(xL(x) + vL(x)) = t\}|.$$

Then

$$N(L, v; t) \leq \begin{cases} q^{m-1} + \frac{q-1}{q} \cdot q^{\frac{m+d}{2}} & \text{if } q \text{ is even, or } q \text{ is odd and } d \equiv m \bmod 2 \\ q^{m-1} + q^{\frac{m+d-1}{2}} & \text{if } q \text{ is odd and } d \equiv m+1 \bmod 2 \end{cases}$$

and

$$N(L, v; t) \geq \begin{cases} q^{m-1} - \frac{q-1}{q} \cdot q^{\frac{m+d}{2}} & \text{if } q \text{ is even, or } q \text{ is odd and } d \equiv m \bmod 2 \\ q^{m-1} - q^{\frac{m+d-1}{2}} & \text{if } q \text{ is odd and } d \equiv m+1 \bmod 2. \end{cases}$$

Proof. The proof is similar to the proof of Lemma 3.3.1. □

Theorem 4.2.6. *The authentication codes defined in (4.2.2) provides at least* $log_2\left(q^{m-1} - \frac{q-1}{q} \cdot q^{\frac{m+d}{2}}\right)$ *bits of secrecy protection if* q *is even, or* q *is odd and* $d \equiv m \bmod 2$, *and* $log_2\left(q^{m-1} - q^{\frac{m+d-1}{2}}\right)$ *bits of secrecy protection if* q *is odd and* $d \equiv m+1 \bmod 2$.

Proof. Given a message $m = (m_1, m_2) = (s + k, \mathrm{Tr}(kL(s)))$, we have that the uncertainty of the source state is $|\{s \in \mathcal{S} : \mathrm{Tr}((m_1 - s)L(s)) = m_2\}| = |\{s \in \mathcal{S} : \mathrm{Tr}(-sL(s) + m_1L(s)) = m_2\}|$. Then the results follow from Lemma 4.2.5. □

Remark 4.2.7. The authentication codes in (4.2.2) are generalizations of the codes in [19, Section 4]. If we take $L(x) = x$, then we obtain exactly the same codes with the codes in [19, Section 4]. Our codes are defined for any prime power q, but the codes in [19, Section 4] are defined only if q is a power of an odd prime.

4.3 Construction II

In this section first we give the construction given in [19, Section 6]. It is shown that the parameters of the codes totaly depend on the properties of a specific map Π and it is noted that the estimation of the parameters $\mathcal{P}_\mathcal{I}$ and $\mathcal{P}_\mathcal{S}$ is not easy for different choices of Π. Now we define the map $\Pi(x) = \mathrm{Tr}(x^{q^h+1})$ and compute the parameters of the codes. It answers the open problem given in [19, Section 6.3.1] for some cases.

4.3.1 The General Construction [19]

Let $(A,+)$ and $(B,+)$ be two finite abelian groups and let Π be a mapping from A to B. Then the authentication code with secrecy is defined as

$$(\mathcal{S},\mathcal{K},\mathcal{M},\mathcal{E}) = (A, A, A\times B, \{E_k : k\in\mathcal{K}\}) \tag{4.3.1}$$

where for any $k\in\mathcal{K}$ and $s\in\mathcal{S}$, $E_k(s) = (s+k, \Pi(s)+\Pi(k))$.

Impersonation Attack

The opponent picks an element $m = (m_1, m_2) \in \mathcal{M}$ in some way and sends it to the receiver. The receiver will compute $s = m_1 - k$ and $\Pi(s)+\Pi(k)$. Then he will check whether $\Pi(m_1-k)+\Pi(k) = m_2$. Hence

$$\begin{aligned} \mathcal{P}_{\mathcal{I}} &= max_{m_1,m_2}\, Pr[\Pi(m_1-k)+\Pi(k) = m_2] \\ &= \frac{|\{k\in\mathcal{K} : \Pi(m_1-k)+\Pi(k) = m_2\}|}{|\{k\in\mathcal{K}\}|}. \end{aligned} \tag{4.3.2}$$

Substitution Attack

The opponent has observed one message $m = (m_1, m_2)$ s.t $m_1 = s+k$ and $m_2 = \Pi(s)+\Pi(k)$, and he wants to replace m with another message $m' = (m_1', m_2')$, where $m_1' \neq m_1$. Set $d_1 = m_1' - m_1$ and $d_2 = m_2' - m_2$. Hence substituting m with m' is equivalent to adding $d_1 \neq 0$ to m_1 and d_2 to m_2. This is successful if and only if $\Pi(s)+\Pi(k)+d_2 = \Pi(s+d_1)+\Pi(k)$, which is equivalent to $\Pi(s+d_1)-\Pi(s) = d_2$. Let $d = (d_1, d_2)$ with $d_1 \neq 0$. Therefore,

$$\begin{aligned} \mathcal{P}_{\mathcal{S}} &= max_{m,d}\, Pr[\Pi(s+d_1)-\Pi(s) = d_2 \mid m_2 = \Pi(s)+\Pi(m_1-s)] \\ &= max_{m,d}\frac{|\{s\in\mathcal{S} : \Pi(s)+\Pi(m_1-s) = m_2, \Pi(s+d_1)-\Pi(s) = d_2\}|}{|\{s\in\mathcal{S} : m_2 = \Pi(s)+\Pi(m_1-s)\}|}. \end{aligned} \tag{4.3.3}$$

4.3.2 Specific Construction of Type II

Let q be a power of a prime, $m > 1$ be an integer and Tr denotes the trace map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$.

Theorem 4.3.1. *Let $(A,+) = (\mathbb{F}_{q^m},+)$, $(B,+) = (\mathbb{F}_q,+)$ and $\Pi(x) = \mathrm{Tr}(x^{q^h+1})$ for some nonnegative integer h. Define $\overline{h} := gcd(2h, m)$. Then the authentication code defined in (4.3.1) has parameters*

$$|\mathcal{S}| = q^m, \quad |\mathcal{K}| = q^m, \quad |\mathcal{M}| = q^{m+1},$$

$$\mathcal{P}_{\mathcal{I}} \leq \begin{cases} \frac{1}{q} + \frac{q-1}{q}\cdot\frac{1}{q^{m/2}} & \text{if } m \text{ is even and } m/\overline{h} \text{ is odd} \\ \frac{1}{q} + \frac{1}{q^{(m+1)/2}} & \text{if } m \text{ is odd.} \end{cases}$$

$$\mathcal{P}_{\mathcal{S}} \leq \begin{cases} \frac{1}{q} + \frac{q^2-1}{q(q^{m/2}-(q-1))} & \text{if } m \text{ is even and } m/\overline{h} \text{ is odd} \\ \frac{1}{q} + \frac{q+1}{q^{(m+1)/2}-q} & \text{if } m \text{ is odd.} \end{cases}$$

To prove the above theorem we need the following lemmas.

Lemma 4.3.2. *Assume that q is odd, $A(x) = 2x^{q^h} \in \mathbb{F}_{q^m}[x]$, $h \geq 1$ and $m > 1$ are integers. Define $\overline{h} := gcd(2h, m)$. If $m/\overline{h}$ is odd then $W_A = \{0\}$. If $m/\overline{h}$ is even then $\mathbb{W}_A = \{x \in \mathbb{F}_{q^m} : x + x^{q^{\overline{h}}} = 0\}$.*

Proof. As $h \geq 1$ and for any $x \in \mathbb{F}_{q^m}$ we have $x^{q^m} = x$, we can assume that $h < m$. We know that

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

Let w be a generator of the multiplicative group $\mathbb{F}_{q^m} \setminus \{0\}$. Assume that $x = w^l \in W_A$ for an integer $l \geq 0$. Then

$$\begin{aligned} w^l + w^{lq^{2h}} = 0 &\Rightarrow 1 + w^{l(q^{2h}-1)} = 0 \\ &\Rightarrow w^{l(q^{2h}-1)} = w^{\frac{q^m-1}{2}}, \text{ as q is odd} \\ &\Rightarrow w^{l(q^{2h}-1)-\frac{q^m-1}{2}} = 1. \end{aligned}$$

Hence we obtain that

$$l(q^{2h}-1) - \frac{q^m-1}{2} \equiv 0 \bmod (q^m-1). \tag{4.3.4}$$

Note that $gcd(q^m-1, q^{2h}-1) = q^{\overline{h}}-1$ where $\overline{h} = gcd(2h, m)$. There exists a solution l of (4.3.4) if and only if

$$\frac{q^m-1}{2} \equiv 0 \bmod q^{\overline{h}} - 1. \tag{4.3.5}$$

So (4.3.5) holds if and only if $q^{\overline{h}} - 1$ divides $\frac{q^m-1}{2}$. We know that

$$\frac{q^m-1}{2} = (q^{\overline{h}}-1)\frac{1 + q^{\overline{h}} + q^{2\overline{h}} + \cdots + q^{(\frac{m}{\overline{h}}-1)\overline{h}}}{2}.$$

If $m/\overline{h}$ is odd then $1 + q^{\overline{h}} + q^{2\overline{h}} + \cdots + q^{(\frac{m}{\overline{h}}-1)\overline{h}}$ is odd, that is, $(q^{\overline{h}}-1) \nmid (\frac{q^m-1}{2})$. Therefore $W_A = \{0\}$.

Next we assume that $m/\overline{h}$ is even. It can be easily seen that $(q^m-1) \nmid (q^{2h}-1)$. Then

$$l\frac{(q^{2h}-1)}{q^{\overline{h}}-1} - \frac{q^m-1}{2(q^{\overline{h}}-1)} \equiv 0 \bmod \frac{q^m-1}{q^{\overline{h}}-1}. \tag{4.3.6}$$

As $gcd\left(\frac{q^{2h}-1}{q^{\overline{h}}-1}, \frac{q^m-1}{q^{\overline{h}}-1}\right) = 1$, there exists a uniquely determined solution, modulo $\frac{(q^m-1)}{q^{\overline{h}}-1}$, of (4.3.6). Let l be such a solution. All other solutions of (4.3.4) are

$$l + c\frac{q^m-1}{q^{\overline{h}}-1},\ 0 \leq c < q^{\overline{h}} - 1.$$

Note that $\left[w^{c\frac{q^m-1}{q^{\overline{h}}-1}}\right]^{q^{\overline{h}}-1} = 1$. Now we show that all the solutions of (4.3.4) satisfies the equation

$$x + x^{q^{\overline{h}}} = 0.$$

Let b be the uniquely determined integer with $0 \leq b < \frac{(q^m-1)}{q^{\overline{h}}-1}$ such that

$$b\frac{q^{2h}-1}{q^{\overline{h}}-1} \equiv 1 \bmod \frac{q^m-1}{q^{\overline{h}}-1}. \tag{4.3.7}$$

We can assume, without loss of generality, that

$$l = b \cdot \frac{q^m-1}{2(q^{\overline{h}}-1)}.$$

Then

$$\left[w^l\right]^{(q^{\overline{h}}-1)} = w^{b\frac{q^m-1}{2}} = (-1)^b = -1,$$

since b is the uniquely determined integer satisfying the equation (4.3.7), that is, b is odd. This completes the proof. □

We have the $\mathbb{F}_q$-linear map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ defined by

$$\begin{aligned} \Psi_b : \mathbb{F}_{q^m} &\to \mathbb{F}_q \\ x &\mapsto \mathrm{Tr}(L_b(x)) = \mathrm{Tr}(bx^{q^h} + b^{q^h}x). \end{aligned}$$

Lemma 4.3.3. *Assume that q is odd, $h \geq 1$, $m > 1$ are integers and $\overline{h} = gcd(2h, m)$. Then for any $b \in \mathbb{F}_{q^m}$ the $\mathbb{F}_q$-linear map $\Psi_b = \mathrm{Tr}(bx^{q^h} + b^{q^h}x)$ from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ is either the zero map or an onto map. Furthermore, if $m/\overline{h}$ is odd then Ψ_b is an onto map.*

Proof. We know that for all $x \in \mathbb{F}_{q^m}$, we have $\mathrm{Tr}(x) = \mathrm{Tr}(x^{q^h})$. Then

$$\begin{aligned} \mathrm{Tr}(bx^{q^h} + b^{q^h}x) &= \mathrm{Tr}(bx^{q^h} + b^{q^{2h}}x^{q^h}) \\ &= \mathrm{Tr}((b + b^{q^{2h}})x^{q^h}). \end{aligned}$$

Therefore, Ψ_b is the zero map if $b + b^{q^{2h}} = 0$. Otherwise, Ψ_b is an onto map since $x \mapsto x^{q^h}$ is an automorphism. □

Lemma 4.3.4. *Assume that q is odd, $A(x) = 2x^{q^h} \in \mathbb{F}_{q^m}[x]$, $m > 1$, $h \geq 1$ are integers and $\overline{h} = gcd(2h, m)$. Let $\Psi_b(x) = \mathrm{Tr}(bx^{q^h} + b^{q^h}x)$ for any $b \in \mathbb{F}_{q^m}$. Then we have $W_A \subseteq Ker\Psi_b$.*

Proof. If $m/\overline{h}$ is odd, then $W_A = \{0\} \subseteq Ker\Psi_b$ trivially.

Assume that $m/\overline{h}$ is even. If $\overline{h}|h$ then $m = 2s\overline{h}$ and $h = r\overline{h}$ for some integers r and s. But it gives a contradiction, since $\overline{h} = gcd(2h, m) = gcd(2r\overline{h}, 2s\overline{h}) > \overline{h}$. So we have

$$\overline{h} = 2h_1,\ h_1 = gcd(h, m),\ m = 4sh_1 \text{ and } h = rh_1,$$

for some integer s and odd integer r.

Note that for all $y \in \mathbb{F}_{q^m}$, we have $\mathrm{Tr}(y^{q^h}) = \mathrm{Tr}(y^{q^{h_1}})$. Recall that $W_A = \{x \in \mathbb{F}_{q^m} : x + x^{q^{\overline{h}}} = 0\} = \{x \in \mathbb{F}_{q^m} : x^{q^{2h_1}} = -x\}$ in this case. Hence for all $x \in W_A$ we have

$$\begin{aligned}
\mathrm{Tr}(b^{q^h}x) &= \mathrm{Tr}((bx^{q^{-h}})^{q^h}) \\
&= \mathrm{Tr}((bx^{q^{-h}})^{q^{h_1}}) \\
&= \mathrm{Tr}((bx^{q^{m-2h+h}})^{q^{h_1}}) \\
&= \mathrm{Tr}((bx^{q^{(2s-r)2h_1+h}})^{q^{h_1}}) \\
&= \mathrm{Tr}\left\{\left[b\left(\left(\left(\left(x^{q^{2h_1}}\right)^{q^{2h_1}}\right)^{\overbrace{\cdots}^{\substack{2s-r\\times}}}\right)^{q^{2h_1}}\right)^{q^h}\right]^{q^{h_1}}\right\} \\
&= \mathrm{Tr}\left[\left(b\left((-1)^{2s-r}x\right)^{q^h}\right)^{q^{h_1}}\right] \\
&= \mathrm{Tr}(-(bx^{q^h})^{q^{h_1}}), \text{ as } (2s-r) \text{ is odd.}
\end{aligned}$$

Therefore, for all $x \in W_A$ we have

$$\begin{aligned}
\mathrm{Tr}(bx^{q^h} + b^{q^h}x) &= \mathrm{Tr}(bx^{q^h} - (bx^{q^h})^{q^{h_1}}) \\
&= \mathrm{Tr}_{\mathbb{F}_{q^{h_1}}/\mathbb{F}_q}\left(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_{q^{h_1}}}\left[bx^{q^h} - (bx^{q^h})^{q^{h_1}}\right]\right) \\
&= 0, \text{ using [37, Theorem 2.25],}
\end{aligned}$$

which completes the proof. □

Lemma 4.3.5. *Assume that q is odd, $m > 1$ and $h \geq 1$ are integers such that $m/gcd(2h, m)$ is odd and $L(x) = bx^{q^h} + b^{q^h}x$ for some nonzero $b \in \mathbb{F}_{q^m}$. For any nonzero $y \in \mathbb{F}_q$, we have*

$$\sum_{x \in \mathbb{F}_{q^m}} e^{\frac{2\pi i}{p}\mathrm{Tr}_{q^m/p}(yL(x))} = 0.$$

Proof. We know that $\mathrm{Tr}(L(x))$ is an onto map by Lemma 4.3.3. So there exists $x_0 \in \mathbb{F}_{q^m}$ such that $\mathrm{Tr}_{q^m/p}(yL(x_0)) \neq 0$. Then

$$\begin{aligned}
\sum_{x \in \mathbb{F}_{q^m}} e^{\frac{2\pi i}{p}\mathrm{Tr}_{q^m/p}(yL(x))} &= \sum_{x \in \mathbb{F}_{q^m}} e^{\frac{2\pi i}{p}\mathrm{Tr}_{q^m/p}(yL(x+x_0))} \text{ using } \mathbb{F}_{q^m} = \{x + x_0 : x \in \mathbb{F}_{q^m}\}, \\
&= \sum_{x \in \mathbb{F}_{q^m}} e^{\frac{2\pi i}{p}\mathrm{Tr}_{q^m/p}(yL(x)+yL(x_0))} \\
&\quad \text{since } L \text{ is linear, i.e. } L(x + x_0) = L(x) + L(x_0).
\end{aligned}$$

After a simple algebraic operation, we get

$$(1 - e^{\frac{2\pi i}{p}\mathrm{Tr}_{q^m/p}(yL(x_0))}) \sum_{x \in \mathbb{F}_{q^m}} e^{\frac{2\pi i}{p}\mathrm{Tr}_{q^m/p}(yL(x))} = 0.$$

As $e^{\frac{2\pi i}{p}\mathrm{Tr}(yL(x_0))} \neq 1$, since we have $x_0 \in \mathbb{F}_{q^m}$ such that $\mathrm{Tr}(yL(x_0)) \neq 0$, we obtain that

$$\sum_{x\in\mathbb{F}_{q^m}} e^{\frac{2\pi i}{p}\mathrm{Tr}_{q^m/p}(yL(x))} = 0.$$

□

Lemma 4.3.6. *Assume that q is odd, $A(x) = 2x^{q^h} \in \mathbb{F}_{q^m}[x]$, $m > 1$ and $h \geq 1$ are integers, $\overline{h} = gcd(2h, m)$ and $L(x) = bx^{q^h} + b^{q^h}x$ for some $b \in \mathbb{F}_{q^m}$. For any nonzero $y \in \mathbb{F}_q$, define*

$$\sigma(y) = \sum_{x\in\mathbb{F}_{q^m}} e^{\frac{2\pi i}{p}\mathrm{Tr}_{q^m/p}(xyA(x)+yL(x))}.$$

Then we have

$$|\sigma(y)| \leq \begin{cases} q^{\frac{m+\overline{h}}{2}} & \text{if } m/\overline{h} \text{ is even} \\ q^{\frac{m}{2}} & \text{if } m \text{ is even and } m/\overline{h} \text{ is odd} \\ \frac{1}{q-1}\cdot q^{\frac{m+1}{2}} & \text{if } m \text{ is odd.} \end{cases}$$

Proof. For any fixed $x \in \mathbb{F}_{q^m}$ and $t \in \mathbb{F}_q$ we have

$$\sum_{y\in\mathbb{F}_q} e^{\frac{2\pi i}{p}\mathrm{Tr}_{q/p}[y(\mathrm{Tr}(xA(x)+L(x))-t)]} = \begin{cases} q & \text{if } \mathrm{Tr}(xA(x)+L(x))-t = 0 \\ 0 & \text{if } \mathrm{Tr}(xA(x)+L(x))-t \neq 0. \end{cases}$$

Hence,

$$\begin{aligned} N(\mathrm{Tr}(xA(x)+L(x))=0) &= \frac{1}{q}\sum_{x\in\mathbb{F}_{q^m}}\sum_{y\in\mathbb{F}_q} e^{\frac{2\pi i}{p}\mathrm{Tr}_{q/p}[y(\mathrm{Tr}(xA(x)+L(x)))]} \\ &= \frac{1}{q}\left(q^m + \sum_{y\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_{q^m}} e^{\frac{2\pi i}{p}\mathrm{Tr}_{q^m/p}(xyA(x)+yL(x))}\right). \end{aligned}$$

Therefore we obtain that

$$|\sigma(y)| = \frac{1}{q-1}\cdot|qN(\mathrm{Tr}(xA(x)+L(x))=0) - q^m|.$$

Then the result follows from [13, Theorem 4.1], Theorem 3.2.2, Lemma 4.3.2 and Lemma 4.3.4.

□

Lemma 4.3.7. *Assume that q is odd, $A(x) = 2x^{q^h} \in \mathbb{F}_{q^m}[x]$, $m > 1$ and $h \geq 1$ are integers, $\overline{h} = gcd(2h, m)$. Let $L(x) = bx^{q^h} + b^{q^h}x$ for some $b \in \mathbb{F}_{q^m}$ and for any $v \in \mathbb{F}_q$ put*

$$N(2, b; v) = |\{x \in F_{q^m} : \mathrm{Tr}(xA(x)+L(x)) = v\}|.$$

Then

$$N(2,b;v) \leq \begin{cases} q^{m-1} + (q-1)q^{\frac{m-2}{2}} & \text{if } m \text{ is even and } m/\overline{h} \text{ is odd} \\ q^{m-1} + q^{\frac{m-1}{2}} & \text{if } m \text{ is odd.} \end{cases}$$

and

$$N(2,b;v) \geq \begin{cases} q^{m-1} - (q-1)q^{\frac{m-2}{2}} & \text{if } m \text{ is even and } m/\overline{h} \text{ is odd} \\ q^{m-1} - q^{\frac{m-1}{2}} & \text{if } m \text{ is odd.} \end{cases}$$

Proof. Let $Tr_{q/p}$ (resp. $Tr_{q^m/p}$) denote the trace map from F_q (resp. F_{q^m}) to F_p.

$$\begin{aligned} N(2,b;v) &= |\{x \in F_{q^m} : Tr(xA(x)+L(x))-v=0\}| \\ &= \frac{1}{q}\sum_{x\in F_{q^m}}\sum_{y\in F_q} e^{\frac{2\pi i}{p}Tr_{q/p}[y(Tr(xA(x)+L(x))-v)]} \\ &= \frac{1}{q}\left(q^m + \sum_{y\in F_q^*} e^{\frac{2\pi i}{p}Tr_{q/p}(-yv)}\sum_{x\in F_{q^m}} e^{\frac{2\pi i}{p}Tr_{q^m/p}(xyA(x)+yL(x))}\right). \end{aligned}$$

Then using Lemma 4.3.6 we have $|qN(2,b;v)-q^m| \le (q-1)|\sigma(y)|$. Then the result follows. □

Lemma 4.3.8. *Assume that q is odd, $A(x) = 2x^{q^h} \in \mathbb{F}_{q^m}[x]$, $m > 1$ and $h \ge 1$ are integers, $\overline{h} = gcd(2h, m)$. Let $L_1(x) = bx^{q^h} + b^{q^h}x$ and $L_2(x) = cx^{q^h} + c^{q^h}x$ for some $b, c \in \mathbb{F}_{q^m}$. For any $v_1, v_2 \in \mathbb{F}_q$ define*

$$N(2,b,c;v_1,v_2) = |\{x \in F_{q^m} : Tr(xA(x)+L_1(x)) = v_1, Tr(L_2(x)) = v_2\}|.$$

Then

$$N(2,b;v) \le \begin{cases} q^{m-2} + (q-1)q^{\frac{m-2}{2}} & \text{if } m \text{ is even and } m/\overline{h} \text{ is odd} \\ q^{m-2} + q^{\frac{m-1}{2}} & \text{if } m \text{ is odd.} \end{cases}$$

and

$$N(2,b;v) \ge \begin{cases} q^{m-2} - (q-1)q^{\frac{m-2}{2}} & \text{if } m \text{ is even and } m/\overline{h} \text{ is odd} \\ q^{m-2} - q^{\frac{m-1}{2}} & \text{if } m \text{ is odd.} \end{cases}$$

Proof. Let $Tr_{q/p}$ (resp. $Tr_{q^m/p}$) denote the trace map from F_q (resp. F_{q^m}) to F_p.

$$\begin{aligned} & N(2,b,c;v_1,v_2) \\ = \;& |\{x \in F_{q^m} : Tr(xA(x)+L_1(x))-v_1=0, Tr(L_2(x))-v_2=0\}| \\ = \;& \frac{1}{q^2}\sum_{x\in F_{q^m}}\sum_{y_1,y_2\in F_q} e^{\frac{2\pi i}{p}Tr_{q/p}[y_1(Tr(xA(x)+L_1(x))-v_1)+y_2(Tr(L_2(x))-v_2)]} \\ = \;& \frac{1}{q^2}\left(q^m + \sum_{(0,0)\neq(y_1,y_2)\in F_q^2} e^{\frac{2\pi i}{p}Tr_{q/p}(-y_1v_1-y_2v_2)}\sum_{x\in F_{q^m}} e^{\frac{2\pi i}{p}Tr_{q^m/p}(y_1(xA(x)+L_1(x))+y_2(L_2(x)))}\right) \\ = \;& \frac{1}{q^2}\left(q^m + \sum_{y_1\in F_q^*,y_2\in F_q} e^{\frac{2\pi i}{p}Tr_{q/p}(-y_1v_1-y_2v_2)}\sum_{x\in F_{q^m}} e^{\frac{2\pi i}{p}Tr_{q^m/p}(y_1(xA(x)+L_1(x))+y_2(L_2(x)))}\right) \end{aligned}$$

by Lemma 4.3.5.

Then using Lemma 4.3.6 we get $|q^2N(2,b,c;v_1,v_2)-q^m| \le (q^2-q)|\sigma(y)|$. The conclusion of the lemma then follows. □

Now using the Lemma 4.3.7 and Lemma 4.3.8 we are ready to prove Theorem 4.3.1.

Proof of Theorem 4.3.1. We first compute $\mathcal{P}_{\mathcal{I}}$. By (4.3.2) we know that

$$\begin{aligned}
\mathcal{P}_{\mathcal{I}} &= max_{m_1,m_2}\, Pr[\Pi(m_1-k)+\Pi(k)=m_2] \\
&= max_{m_1,m_2}\frac{|\{k\in\mathcal{K}:\Pi(m_1-k)+\Pi(k)=m_2\}|}{|\{k\in\mathcal{K}\}|} \\
&= max_{m_1,m_2}\frac{|\{k\in\mathcal{K}:\Pi(m_1-k)+\Pi(k)=m_2\}|}{q^m} \\
&= max_{m_1,m_2}\frac{|\{k\in\mathcal{K}:\mathrm{Tr}(2k^{q^h+1}-m_1k^{q^h}-{m_1}^{q^h}k+{m_1}^{q^h+1})=m_2\}|}{q^m} \\
&\leq \begin{cases} \frac{1}{q}+\frac{q-1}{q}\cdot\frac{1}{q^{m/2}} & \text{if } m \text{ is even and } m/\overline{h} \text{ is odd} \\ \frac{1}{q}+\frac{1}{q^{(m+1)/2}} & \text{if } m \text{ is odd.} \end{cases} \\
&\quad \text{by Lemma 4.3.7.}
\end{aligned}$$

We now estimate the upper bound on $\mathcal{P}_{\mathcal{S}}$. By (4.3.3),

$$\begin{aligned}
\mathcal{P}_{\mathcal{S}} &= max_{m,d_2,d_1\neq 0}\frac{|\{s\in\mathcal{S}:\Pi(s)+\Pi(m_1-s)=m_2,\Pi(s+d_1)-\Pi(s)=d_2\}|}{|\{s\in\mathcal{S}:\Pi(s)+\Pi(m_1-s)=m_2\}} \\
&= \frac{max_{m,d_2,d_1\neq 0}\left|\left\{s\in\mathcal{S}:\begin{array}{rcl}\mathrm{Tr}(d_1s^{q^h}+{d_1}^{q^h}s+{d_1}^{q^h+1}) &=& d_2\\ \mathrm{Tr}(2s^{q^h+1}-m_1s^{q^h}-{m_1}^{q^h}s+{m_1}^{q^h+1}) &=& m_2\end{array}\right\}\right|}{max_{m_1,m_2}|\{s\in\mathcal{S}:\mathrm{Tr}(2s^{q^h+1}-m_1s^{q^h}-{m_1}^{q^h}s+{m_1}^{q^h+1})=m_2\}} \\
&\leq \begin{cases} \frac{1}{q}+\frac{q^2-1}{q(q^{m/2}-(q-1))} & \text{if } m \text{ is even and } m/\overline{h} \text{ is odd} \\ \frac{1}{q}+\frac{q+1}{q^{(m+1)/2}-q} & \text{if } m \text{ is odd.} \end{cases} \\
&\quad \text{by Lemma 4.3.7 and Lemma 4.3.8.}
\end{aligned}$$

The remaining conclusions of the theorem are clear. □

Theorem 4.3.9. *Let $(A,+)=(\mathbb{F}_{q^m},+)$, $(B,+)=(\mathbb{F}_q,+)$, $\Pi(x)=\mathrm{Tr}(x^{q^h+1})$ for some nonnegative integer h and $\overline{h}=gcd(2h,m)$. Then the authentication code defined in (4.3.1) provides at least $log_2\left(q^{m-1}-(q-1)q^{\frac{m-2}{2}}\right)$ bits of secrecy protection if m is even and $m/\overline{h}$ is odd, and $log_2\left(q^{m-1}-q^{\frac{m-1}{2}}\right)$ bits of secrecy protection if m is odd.*

Proof. Given a message $m=(m_1,m_2)=(s+k,\mathrm{Tr}(kL(s)))$, we have that the uncertainty of the source state is

$$|\{s\in\mathcal{S}:\Pi(s)+\Pi(m_1-s)=m_2\}|=|\{s\in\mathcal{S}:\mathrm{Tr}(2s^{q^h+1}-m_1s^{q^h}-{m_1}^{q^h}s+{m_1}^{q^h+1})=m_2\}|.$$

Then we complete the proof using Lemma 4.3.7. □

Chapter 5

Conclusions and Future Works

In this thesis different constructions of authentication codes with and without secrecy are presented. Their parameters are better than the existing ones in some cases.

There are two types of authentication maps in our constructions. In type I maps, further a part of the key is used as an addition. This final operation guarantees that $\mathcal{P}_{\mathcal{I}} = \frac{|\mathcal{S}|}{|\mathcal{M}|} = \frac{1}{|\mathcal{T}|}$. In type II maps, there is no extra addition. Furthermore, the difference of type I and type II codes appears in estimating the probabilities $\mathcal{P}_{\mathcal{I}}$ and $\mathcal{P}_{\mathcal{S}}$. It is seen that, the estimation of the probability $\mathcal{P}_{\mathcal{S}}$ of type II codes is much more difficult.

Some future works can be summarized as follows:

- The constructions given in Section 2.4 are defined over $\mathbb{F}_p$, where p is a prime. This constructions can be extended to the codes over $\mathbb{F}_{p^n}$ for some integer $n \geq 2$. But the estimation of the probability $\mathcal{P}_{\mathcal{S}}$ seems to be much more difficult.

- For the constructions given in Section 3.4 can be used to obtain good systematic authentication codes having some fixed parameters. It can be done by putting some conditions on dimension of the radical of polynomials obtained by the elements of the source states. Here the following two different strategies can be observed.

  1. Fixing the parameters $|\mathcal{K}|, |\mathcal{T}|, \mathcal{P}_{\mathcal{I}}$ and $\mathcal{P}_{\mathcal{S}}$ one can search for larger special set of source states $\mathcal{S}$.
  2. Fixing the parameters $|\mathcal{K}|, |\mathcal{T}|$ one can search for larger special set of source states $\mathcal{S}$ to obtain better codes having $\mathcal{P}_{\mathcal{I}}$ and $\mathcal{P}_{\mathcal{S}}$ as small as possible.

- Using additive polynomials as in Chapter 3 and Chapter 4 many different authentication codes with/without secrecy having good parameters can be obtained.

- Using specific maps Π, the general construction proposed in [19] may give different authentication codes having good parameters. We estimate the parameters by taking $\Pi(x) =$

$\mathrm{Tr}(x^{q^h+1})$. One can construct authentication codes taking $\Pi(x) = \mathrm{Tr}(xL(x))$ for some specific additive polynomial $L(x)$.

References

[1] M. Atici and D. R. Stinson, Universal Hashing and Multiple Authentication, *Advances in Cryptology, CRYPTO'96*, Lecture Notes in Computer Science, vol. 1109, pp. 16-30, 1996.

[2] A. Beutelspacher, G. Tallini and C. Zanella, Examples of essentially s-fold secure geometric authentication systems with large s, *Rend. Mat. Appl.*, vol. 10, pp. 321-326, 1990.

[3] J. Bierbrauer, Universal hashing and geometric codes, *Designs, Codes and Cryptography*, vol. 11, no. 3, pp. 207-221, 1997.

[4] J. Bierbrauer, T. Johansson, G. Kabatianskii, and B. Smeets, On families of hash functions via geometric codes and concatenation, *Advances in Cryptology, CRYPTO'93*, Lecture Notes in Computer Science, vol. 773, pp. 331-342, Springer-Verlag, 1994.

[5] G. Bini, A-codes from rational functions over Galois rings, *Designs, Codes and Cryptography*, vol. 39, Issue 2, pp. 207-214, 2006.

[6] E. F. Brickell, A few results in message authentication, *Congressus Numerantium*, vol. 43, pp. 141-154, 1984.

[7] C. Carlet, C. Ding and H. Niederreiter, Authentication schemes from highly nonlinear functions, *Designs, Codes and Cryptography*, vol. 40, no. 1, pp. 71-79, 2006.

[8] J. L. Carter and M. N. Wegman, Universal Classes of Hash Functions, *Journal Computer and System Sciences*, vol. 18, pp. 143-154, 1979.

[9] L. R. A. Casse, K. M. Martin, P. R. Wild, Bounds and characterizations of authentication/secrecy schemes, *Designs, Codes and Cryptography*, vol. 13, pp. 107-129, 1998.

[10] S. Chanson, C. Ding and A. Salomaa, Cartesian authentication codes from functions with optimal nonlinearity, *Theoretical Computer Science*, vol. 290, no. 3, pp. 1737-1752, 2003.

[11] C. J. Colbourn, J. H. Dinitz, *Handbook of Combinatorial Designs*, 2nd ed., Boca Raton, FL : Chapman & Hall/Taylor & Francis, 2007.

[12] I. Constantinescu and T. Heise, A metric for codes over residue class rings of integers, *Problemy Peredachi Informatsii*, vol. 33, no. 3, pp. 22-28, 1997.

[13] E. Çakçak and F. Özbudak, Curves Related to Coulter's Maximal Curves, Finite Fields Appl., (in press). Available online at doi:10.1016/j.ffa.2006.10.003.

[14] E. Çakçak and F. Özbudak, Some Artin-Schreier type function fields over finite fields with prescribed genus and number of rational places, *Journal of Pure and Applied Algebra*, vol. 210, Issue 1, pp. 113-135, 2007.

[15] M. De Soete, Some constructions for authentication-secrecy codes, *Advances in Cryptology Eurocrypt88*, Lecture Notes in Computer Science, vol. 330, pp. 5776, 1988.

[16] M. De Soete, New bounds and constructions for authentication/secrecy codes with splitting, *Journal of Cryptology*, vol. 3, pp. 173186, 1991.

[17] C. Ding, T. Helleseth, T. Klve and X. Wang: A Generic Construction of Cartesian Authentication Codes, *IEEE Transactions on Information Theory* vol. 53, no. 6, pp. 2229-2235, 2007.

[18] C. Ding and H. Niederreiter, Systematic authentication codes from highly nonlinear functions, *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2421-2428, 2004.

[19] C. Ding, A. Salomaa, P. Sole and X. Tian, Three constructions of authentication secrecy codes, *Journal Pure and Applied Algebra*, vol. 196, pp. 149-168, 2005.

[20] C. Ding and X. Tian, Three constructions of authentication codes with perfect secrecy, *Designs, Codes and Cryptography*, vol. 33, no. 3, pp. 227-239, 2004.

[21] C. Ding and X. Wang, A coding theory construction of new systematic authentication codes. *Theoretical Computer Science*, vol. 330, no. 1, pp. 81-99, 2005.

[22] C. Ding, X. Tian and X. Wang, Simple and efficient systematic A-codes from error correcting code, *Progress on cryptography*, pp. 33-43, Kluwer Internat. Ser. Engrg. Comput. Sci., vol. 769, Kluwer Academic Publications, Boston, MA, 2004.

[23] R. Feng and Z. Wan, A construction of Cartesian authentication codes from vector space and dual authentication codes, *Northeastern Mathematical Journal*, vol. 13, pp. 63-72, 1997.

[24] Y. Gao and Z. Zou, Two new constructions of Cartesian authentication codes from symplectic geometry, *Appl. Math. Journal Chinese Univ. Ser.*, vol. B 10 , pp. 345-356, 1995.

[25] G. Ge, Y. Miao and L. Wang, Combinatorial Constructions for Optimal Splitting Authentication Codes, *SIAM Journal on Discrete Mathematics*, vol. 18, no.4, pp. 663-678, 2005.

[26] G. Ge and L. Zhu, Authentication perpendicular arrays $APA_1(2, 5, v)$, *Journal Combinatorial Designs*, vol. 4,pp. 365-375, 1996.

[27] E. N. Gilbert, F. J. MacWilliams and N. J. A. Sloane, Codes which detect deception, *Bell Syst. Tech. J.*, vol. 53, pp. 405424, 1974.

[28] M. Greferath, S. E. Schmidt, Gray isometries for finite chain rings, *IEEE Transactions on Information Theory*, vol. 45, pp. 2522-2524, 1999.

[29] L. C. Grove, *Classical groups and geometric algebra*, American Mathematical Society, Providence, 2002.

[30] A. S. Hedayat, N. J. A. Sloane and J. Stufken, *Orthogonal Arrays: Theory and Applications*, Springer Verlag, New York, 1999.

[31] T. Helleseth and T. Johansson, Universal hash functions from exponential sums over finite fields and Galois rings, *Advances in Cryptology*, CRYPTO'96, LNCS 1107, pp. 31-44, Springer-Verlag, 1996.

[32] T. Helleseth, K. V. Kumar and A. G. Shanbhag, Exponential sums over Galois rings and their applications, *Finite fields and applications* (Glasgow, 1995), London Math. Soc. Lecture Note Ser., vol. 233, pp. 109-128, Cambridge Univ. Press, Cambridge, 1996.

[33] T. Johansson, *Contributions to unconditionally secure authentication*, Ph.D. dissertation, Lund University, Lund, Sweden, 1994.

[34] T. Johansson, Lower bounds on the probability of deception in authentication with arbitration, *Proceedings of 1993 IEEE International Symposium on Information Theory*, San Antonio, pp. 231, 1993.

[35] P. V. Kumar, T. Helleseth and A. R. Calderbank, An upper bound for Weil exponential sums over Galois rings and applications, *IEEE Transactions on Information Theory*, vol. 41, pp. 456-468, 1995.

[36] K. Kurosawa and S. Obana, Combinatorial Bounds on Authentication Codes with Arbitration, *Designs, Codes and Cryptography*, vol. 22, no. 3, pp. 265-281, 2001.

[37] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1997.

[38] S. Ling and F. Özbudak, Improved bounds on Weil sums over Galois rings and homogeneous weights, In: Ythervs O (ed) *Proceedings of International Workshop on Coding ad Cryptography 2005*, LNCS 3969, Springer-Verlag, Berlin, pp. 412-426, 2005.

[39] S. Ling and F. Özbudak, Aperiodic and odd correlations of some p-ary sequences, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science*, vol. E89-A, no. 9, pp. 2258-2263, 2006.

[40] J. L. Massey, *Cryptographya selective survey*, in: E. Biglieri, G. Pratti (Eds.), Digital Communications, Elsevier Science, North-Holland, pp. 325, 1986.

[41] C. Mitchell, M. Walker and P. Wild, The combinatorics of perfect authentication schemes, *SIAM Journal of Discrete Mathematics*, vol. 7, pp. 102-107, 1994.

[42] F. Özbudak and Z. Saygı, Some constructions of systematic authentication codes using Galois rings, *Designs, Codes and Cryptography*, vol. 41, no. 3, pp. 343-357, 2006.

[43] F. Özbudak and Z. Saygı, Constructions of systematic authentication codes using additive polynomials, *Proceedings of International Workshop on Coding ad Cryptography 2007*, Versailles, France, pp. 405-414, 2007.

[44] F. Özbudak and Z. Saygı, Systematic authentication codes using additive polynomials, *Designs, Codes and Cryptography*, submitted.

[45] F. Özbudak and Z. Saygı, Authentication codes with secrecy using additive polynomials, in preparation.

[46] D. Pei, Information-theoretic bounds for authentication codes and block designs, *Journal of Cryptology*, vol. 8, pp. 177188, 1995.

[47] D. Pei, *Authentication Codes and Combinatorial Designs*, Chapman and Hall/CRC, Taylor and Francis Group, Boca Raton, 2006.

[48] R. S. Rees, D. R. Stinson, Combinatorial characterizations of authentication codes, *Designs, Codes and Cryptography*, vol. 7, pp. 239259, 1996.

[49] U. Rosenbaum, A lower bound on authentication after having observed a sequence of messages, *Journal of Cryptology*, vol. 6, pp. 135156, 1993.

[50] A. Sgarro, Lower bounds for authentication codes with splitting, *Advances in Cryptology, EUROCRYPT'90*, I. B. Damgard, ed., Lecture Notes in Computer Science, vol. 473, pp. 283-293, 1991.

[51] A. Sgarro, Information-theoretic bounds for authentication frauds, *Journal of Computer Security*, vol. 2, pp. 5363, 1993.

[52] C. E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal*, vol. 28, pp. 656-715, 1949.

[53] 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.

[54] G. J. Simmons, Message authentication with arbitration of transmitter/receiver disputes, *Proceedings of EUROCRYPT'87*, Lecture Notes in Computer Science, vol. 304, pp. 150-166, 1987.

[55] G. J. Simmons, A Cartesian product construction for unconditionally secure authentication codes that permit arbitration, *Journal of Cryptology*, vol. 2, no. 2, pp. 77-104, 1990.

[56] M. De Soete, Bounds and constructions for authentication - secrecy codes with splitting, *Advances in Cryptology, CRYPTO '88*, S. Goldwasser, ed., Lecture Notes in Computer Science 403, pp. 311-317, 1989.

[57] D. R. Stinson, Universal hashing and authentication codes, *Designs, Codes and Cryptography*, vol. 4, pp. 337-346, 1994.

[58] D. R. Stinson, *Cryptography: Theory and Practice*, Boca Raton, FL: CRC, 1995.

[59] D. R. Stinson. Some constructions and bounds for authentication codes, *Journal of Cryptology*, vol. 1, pp. 37-51, 1988.

[60] D. R. Stinson, The combinatorics of authentication and secrecy codes, *Journal of Cryptology*, vol. 2, pp. 23-49, 1990.

[61] D. R. Stinson, Combinatorial techniques for universal hashing, *Journal of Computer and Systems Science*, vol. 48, pp. 337-346, 1994.

[62] D. R. Stinson, Combinatorial characterizations of authentication codes, *Designs, Codes and Cryptography*, vol. 2, pp. 175-187, 1992. [Preliminary version appeared in *Advances in Cryptology, CRYPTO'91*, J. Feigenbaum, ed., Lecture Notes in Computer Science, vol. 576, pp. 62-73, 1992.]

[63] D. R. Stinson, A construction for authentication/secrecy codes from certain combinatorial designs, *Journal of Cryptology*, vol. 1, pp. 119127, 1988.

[64] D. R. Stinson and L. Teirlinck, A construction for authentication/secrecy codes from 3-homogeneous permutation groups, *European Journal of Combinatorics*, vol. 11, pp. 7379, 1990.

[65] X. Tian, *Several constructions of authentication codes with secrecy*, Ph.D. dissertation, University of Hong Kong, Hong Kong, 2004.

[66] H. M. Trachtenberg, *On the cross-correlation function of maximal linear sequences*, Ph.D. dissertation, University of Southern California, Los Angeles, 1970.

[67] M. Walker, Information-theoretic bounds for authentication schemes, *Journal of Cryptology*, vol. 2, pp. 131143, 1990.

[68] Z. -X. Wan, *Lectures on Finite Fields and Galois Rings*, World Scientific, Singapore, 2003.

[69] Z. -X. Wan, Construction of Cartesian authentication codes from unitary geometry, *Designs, Codes and Cryptography* vol. 2, pp. 333-356, 1992.

[70] Z. -X. Wan, B. Smeets and P. Vanroose, On the construction of Cartesian authentication codes over symplectic spaces, *IEEE Transactions on Information Theory* vol. 40, 920-929, 1994.

[71] X. Wang, *Cartesian authentication codes from error correcting codes*, Ph.D. dissertation, University of Hong Kong, Hong Kong, 2004.

[72] M. N. Wegman and J. L. Carter, New hash functions and their use in authentication and set equality, *Journal Computer and System Science*, vol. 22, pp. 265279, 1981.

[73] C. Xing, H. Wang and K. Y. Lam, Construction of authentication codes from algebraic curves over finite fields, *IEEE Transactions on Information Theory*, vol. 46, pp. 886-892, 2000.

[74] C. Zanella, Linear sections of the finite Veronese varieties and authentication systems defined using geometry, *Designs, Codes and Crytography*, vol. 13, pp. 199-212, 1998.

VITA

PERSONAL INFORMATION

Surname, Name:	Saygı, Zülfükar
Nationality:	Turkish (TC)
Date and Place of Birth:	February 10, 1978, Yerköy
Marital Status:	Married to Elif Saygı, have son Emir Ali Saygı
Phone:	+90 312 210 56 09
Fax:	+90 312 210 29 85
email:	saygi@metu.edu.tr

ACADEMIC DEGREES

Ph.D. Department of Cryptography, 2007 July
Institute of Applied Mathematics
Middle East Technical University-Ankara
Advisor: Prof. Dr. Ferruh Özbudak
Thesis Title: Constructions of Authentication Codes

M.Sc. Department of Mathematics, 2003 January
Middle East Technical University-Ankara
Supervisor: Prof. Dr. Ersan Akyıldız
Thesis Title: A Method of Constructing Secure S-boxes

B.S. Department of Mathematics, June 2000
Middle East Technical University-Ankara

EMPLOYMENT

2002- Research Assistant,
Department of Cryptography, Institute of Applied Mathematics,
Middle East Technical University-Ankara

2000-2002 Researcher,
Cryptographic Test and Design Group,
TÜBİTAK-UEKAE, Gebze-Kocaeli

PUBLICATIONS

• F. Özbudak, Z. Saygı, Some constructions of systematic authentication codes using galois rings, Designs, Codes and Cryptography, vol 41, No. 3, pp. 343-357 (2006).

• A. Doğanaksoy, E. Saygı, Z. Saygı, Quadratic Feedback Shift Registers Generating Maximum Length Sequences, BFCA 2007, Third International Workshop on Boolean Functions : Cryptography and Applications, May 2-3, 2007, Paris, France.

• F. Özbudak, Z. Saygı, Constructions of Systematic Authentication Codes Using Additive Polynomials, WCC 2007, International Workshop on Coding and Cryptography, April 16-20, 2007, Versailles, France.

• B. G. Dündar, F. Göloğlu, A. Doğanaksoy, Z. Saygı, A method of constructing highly nonlinear balanced Boolean functions, BFCA'06, Boolean Functions: Cryptography and Applications, Editors: J-F. Michon, P. Valarcher, J-B. Yuns, pp. 1-11, 13-15 Mart 2006, Rouen, France.

• A. Doğanaksoy, S. Sağdıçoğlu, Z. Saygı, M. Uğuz, A note on linearity and homomorphicity, BFCA'06, Boolean Functions: Cryptography and Applications, Editors: J-F. Michon, P. Valarcher, J-B. Yuns, pp. 99-106, 13-15 Mart 2006, Rouen, France.

• E. Saygı, Z. Saygı, M. S. Turan, A. Doğanaksoy, Statistical approach on the number of SAC satisfying functions, BFCA'05, Boolean Functions: Cryptography and Applications, Editors: J-F. Michon, P. Valarcher, J-B. Yuns, pp. 39-48, 7-9 Mart 2005, Rouen, France.

• A. Doğanaksoy, B. G. Dündar, F. Göloğlu, Z. Saygı, F. Sulak, M. Uğuz, A Survey on Bent Functions and Normality, National Cryptology Symposium II, Editor: Ali Doğanaksoy pp. 19-26 , 15-17 December 2006, Ankara, Türkiye.

• Z. Saygı, S. Yeşil, Açık Anahtar Altyapısı Konusunda Araştırma, Geliştirme ve Uygulamalar, National Digital Signature Symposium I, pp.28-34, 7-8 December 2006, Ankara, Türkiye.

• F. Özbudak, Z. Saygı, Construction of Systematic Authentication Codes, National Cryptology Symposium I, Editor: Ersan Akyıldız, pp. 142-148 , 18-20 November 2005, Ankara, Türkiye.