A coding theory construction of new systematic authentication codes

Cunsheng Ding*, Xuesong Wang

Department of Computer Science, Hong Kong University of Science and Technology, Clearwater Bay, Kowloon, Hong Kong, China

Abstract

There are several approaches to the construction of authentication codes without secrecy using error correcting codes. In this paper, we describe one approach and construct several classes of authentication codes using several types of error correcting codes. Some of the authentication codes constructed here are asymptotically optimal, and some are optimal.

© 2004 Elsevier B.V. All rights reserved.

Keywords: Authentication codes; Cryptography; Error correcting codes

1. Introduction

Authentication codes are divided into two classes: those with secrecy and those without secrecy. Authentication codes without secrecy are designed to authenticate transmitted messages and the sender. A subclass of authentication codes without secrecy is the systematic authentication. A systematic authentication codes is a four-tuple

\((S, T, K, \{E_k : k \in K\})\),

where \(S\) is the source state, \(T\) is the tag space, \(K\) is the key space and \(E_k : S \rightarrow T\) is called an encoding rule. A transmitter and a receiver share a secret key \(k \in K\). To send a piece of information (called source state) \(s \in S\) to the receiver, the transmitter computes \(t = E_k(s) \in T\) and puts the message \(m = (s, t)\) into a public channel. After receiving

* Corresponding author.

E-mail addresses: cding@cs.ust.hk (C. Ding), cswxs@cs.ust.hk (X. Wang).

0304-3975/ - see front matter © 2004 Elsevier B.V. All rights reserved.
\( m' = (s', t') \), the receiver will compute \( E_k(s') \) and checks whether \( t' = E_k(s') \). If yes, the receiver will accept it as authentic. Otherwise, the receiver will reject it.

Because the communication channel is public, there is the risk that an opponent could deliberately observe or even disturb the ordinary communication. In the authentication model introduced by Simmons [12], an opponent is involved in addition to the transmitter and receiver. We assume that the opponent can insert his message into the channel or substitute an observed message \( m \) with another message \( m' \). Therefore, we consider two kinds of attacks, the \textit{impersonation} and \textit{substitution} attacks. In the impersonation attack, the opponent deliberately chooses a message and inserts it into the channel, hoping that the receiver will accept it as authentic. We use \( P_I \) to denote the maximum success probability of this attack. In the substitution attack, the opponent observed a message \( m \), and replaces it with a new message \( m' \neq m \), hoping that the receiver will accept the latter one. \( P_S \) is used to denote the maximum success probability of this attack.

It is obvious that the opponent will choose certain messages to enhance the probability of successful cheating. So the authentication codes must be designed to deal with the worst case, which means \( P_I \) and \( P_S \) must be as small as possible. However, we have the following two lower bounds on \( P_I \) and \( P_S \) [10,11]:

\[
P_I \geq \frac{|S|}{|M|} \quad \text{and} \quad P_S \geq \frac{|S| - 1}{|M| - 1},
\]

where \( S \) and \( M = S \times T \) are the source state space and message space, respectively. For authentication codes without secrecy, it is well known that \( P_S \geq P_I \). So the bounds for systematic authentication codes can be strengthened into

\[
P_I \geq \frac{1}{|T|} \quad \text{and} \quad P_S \geq \frac{1}{|T|}.
\]

There are several approaches to the construction of authentication codes without secrecy using error correcting codes: the \( q \)-twisted construction [8], the construction using rank distance codes [15], the construction using geometric codes [2,3], and a generic approach [5]. Some algebraic constructions [7,16,4] can also be viewed as constructions based on error correcting codes (see [5] for details).

In this paper, we describe one approach and construct several classes of authentication codes using several types of error correcting codes. Some authentication codes constructed in this paper are asymptotically optimal, and some are optimal. The underlying error correcting codes used within the framework of this paper were employed to construct several classes of authentication codes in [5]. Here we use these error correcting codes to construct authentication codes with a different approach.

\section{A projective construction using linear codes}

Let \( \mathcal{C} \) be an \([n, k]\) linear code over \( \text{GF}(q) \). We classify all the nonzero codewords of \( \mathcal{C} \) into \((q^k - 1)/(q - 1)\) equivalent classes, where two codewords are in the same equivalence class if and only if they are multiples of each other. In each equivalence class, we choose a
codeword and use \( c_0, c_1, \ldots, c_{(q^k - 1)/(q - 1) - 1} \) to denote these nonequivalent codewords of \( C \). Then the authentication code based on \( C \) under this construction is

\[
(S, T, K, E) = (Z_{(q^k - 1)/(q - 1)}, \mathbb{GF}(q), Z_n, \{E_k|k \in K\}),
\]

where for any \( k \in K \) and \( s \in S \) the encoding rule is defined by

\[
E_k(s) = c_{s,k},
\]

where \( c_{s,k} \) is the \((k+1)\)-th component of the codeword \( c_s \). Here all the source states are used equally likely, and all the keys are used with equally probability. This construction depends on the choice of the set \( \{c_0, \ldots, c_{(q^k - 1)/(q - 1) - 1}\} \) of representatives of the equivalence classes because the authenticators depend on the specific selection of these codewords. However, it will be shown below that the two probabilities \( P_I \) and \( P_S \) are independent of the selection of these representatives \( c_i \). So the selection of these representatives is of no importance, and we shall not mention the selection of these \( c_i \) in specific constructions in the sequel.

Given the construction of authentication codes above, one natural question is how to compute the two probabilities \( P_I \) and \( P_S \). This question is answered by the following theorem, where \( N(c, u) \) denotes the number of times \( u \) occurs as coordinates of the codeword \( c \).

**Theorem 1.** For the authentication code of (2), we have

\[
P_I = \max_{0 \neq c \in C} \max_{u \in \mathbb{GF}(q)} \frac{N(c, u)}{n},
\]

\[
P_S = \max_{s \in S, t \in T} \max_{s' \neq s, t'} \frac{|\{k \in K : t = c_{s,k}, t' = c_{s',k}\}|}{N(c_s, t)}.
\]

Furthermore

\[
|S| = \frac{q^k - 1}{q - 1}, \quad |T| = q, \quad |K| = n.
\]

**Proof.** In the impersonation attack, the opponent wants to generate a message \( m = (s, t) \) so that \( t = c_{s,k} \) has the highest probability. However, the keys and the source states are equally likely, and the opponent has not observed any message from the transmitter to the receiver, and thus has no information about the secret key shared by the transmitter and receiver. Hence

\[
P_I = \max_{s \in S, t \in T} \frac{|\{k \in K : t = c_{s,k}\}|}{|\{k \in K\}|} = \max_{0 \neq c \in C} \max_{u \in \mathbb{GF}(q)} \frac{N(c, u)}{n}.
\]

In the substitution attack, the opponent observed a message \( m = (s, t) \) and replaces it with another message \( m' = (s', t') \), where \( s \neq s' \). The maximum probability of success with respect to the substitution attack is

\[
P_S = \max_{s \in S, t \in T} \max_{s' \neq s, t'} \frac{|\{k \in K : t = c_{s,k}, t' = c_{s',k}\}|}{|\{k \in K : t = c_{s,k}\}|} = \max_{s \in S, t \in T} \max_{s' \neq s, t'} \frac{|\{k \in K : t = c_{s,k}, t' = c_{s',k}\}|}{N(c_s, t)}.
\]

This completes the proof.  \( \square \)
It is hard to compute \( P_I \) and \( P_S \) in general, but this can be done in certain cases, as demonstrated later.

In order to get good authentication codes within the framework of this construction, the underlying linear code should satisfy two conditions. First of all, all the elements of \( \text{GF}(q) \) should appear approximately the same number of times as coordinates in each nonzero codeword of \( C \). Second, for each pair of distinct nonzero codewords \( c_i \) and \( c_j \) all the pairs \( (a, b) \in \text{GF}(q)^2 \) appear approximately the same number of times as column vectors of the matrix

\[
\begin{bmatrix}
c_{i,0} & c_{i,1} & \cdots & c_{i,n-1} \\
c_{j,0} & c_{j,1} & \cdots & c_{j,n-1}
\end{bmatrix}.
\]

This follows from Theorem 1. In the following sections, we shall use special classes of such linear codes to construct systematic authentication codes.

**Comment:** The projective construction of authentication codes presented in this section is obviously different from the \( q \)-twisted construction in [8], and the constructions of [2,3,5,15,16], although these constructions all are based or may be viewed as constructions based on error correcting codes.

### 3. Authentication codes from irreducible cyclic codes

Let \( p \) be an odd prime, and let \( q = p^m \). Let \( N \) be a positive integer \( N \) dividing \( q - 1 \). Define \( n = (q - 1)/N \). Let \( \alpha \) be a primitive element of \( \text{GF}(q) \), and let \( \theta = \alpha^N \). The set

\[
C = \{ c(\beta) = (\text{Tr}_{q/p}(\beta), \text{Tr}_{q/p}(\beta\theta), \ldots, \text{Tr}_{q/p}(\beta\theta^{n-1})) | \beta \in \text{GF}(q) \}
\]

is called an irreducible cyclic \([n, m_0]\) code over \( \text{GF}(p) \), where \( \text{Tr}_{q/p} \) is the trace function of \( \text{GF}(q)/\text{GF}(p) \) and \( m_0 = \text{ord}_n(p) \), i.e., the multiplicative order of \( p \) modulo \( n \). If \( m_0 \neq m \), the code is degenerate. We only consider the case \( m_0 = m \) in this paper. This is guaranteed by enforcing certain conditions on the parameters \( p, m, \) and \( N \).

In order to use an \([n, m]\) irreducible code to construct authentication codes within the framework of the construction described in the previous section, we need to choose a set of nonequivalent codewords \( c_0, c_1, \ldots, c_{(p^m - 1)(p-1) - 1} \). Note that each nonzero element \( \beta \in \text{GF}(q) \) can be expressed as

\[
\beta = \alpha^{p^m - 1} x^{i+j}
\]

for a pair \((i, j)\) where \( 0 \leq i \leq p - 2 \) and \( 0 \leq j \leq (p^m - 1)/(p-1) - 1 \). The codewords

\[
c_j = c(\alpha^j), \quad j = 0, 1, \ldots, \frac{p^m - 1}{p - 1}
\]

are pairwise nonequivalent. In this section, we construct systematic authentication codes using the irreducible cyclic codes and this selection of the representative codewords. For these authentication codes we could compute \( P_I \), and can give a fairly tight bound on \( P_S \).
To give bounds on $P_S$, we need exponential sums and Weil’s bound. Exponential sums are of the form

$$S(X, f) = \sum_{x \in X} e(f(x)),$$

where $e(z) = \exp(2\pi iz)$, $X$ is an arbitrary set, and $f$ is a real-valued function on $X$.

For each $c \in \text{GF}(q)$

$$\chi_b(c) = e^{2\pi i Tr_{q/p}(bc)/p}$$

defines an additive character of $\text{GF}(q)$ [9].

**Lemma 2** (Weil’s bound [9]). Let $f \in \text{GF}(q)[x]$ be of degree $n \geq 1$ with $\gcd(n, q) = 1$, and let $\chi$ be a nontrivial additive character of $\text{GF}(q)$. Then

$$\left| \sum_{c \in \text{GF}(q)} \chi(f(c)) \right| \leq (n - 1)q^{1/2}.$$

3.1. The semiprimitive case

**Lemma 3** (Baumert and McEliece [1]). Let $C$ be an $[n, m]$ irreducible cyclic code over $\text{GF}(p)$ with $Nn = p^m - 1 = q - 1$, $N > 2$. If there exists a divisor $j$ of $m/2$ for which $p^j \equiv -1 \pmod{N}$, then there are only two distributions of elements from $\text{GF}(p)$ which occur in the nonzero codewords of $C$:

**Class s:** (containing $n$ codewords)

$$N_0 = \frac{q - 1}{Np} + \frac{1 - p + u(1 - p)(N - 1)\sqrt{q}}{Np},$$

$$N_i = \frac{q - 1}{Np} + \frac{1 + u(N - 1)\sqrt{q}}{Np}, \quad i = 1, \ldots, p - 1.$$

**Class *:** (containing $n(N - 1)$ codewords)

$$N_0 = \frac{q - 1}{Np} + \frac{1 - p - u(1 - p)\sqrt{q}}{Np},$$

$$N_i = \frac{q - 1}{Np} + \frac{1 - u\sqrt{q}}{Np}, \quad i = 1, \ldots, p - 1.$$

Here $N_i$ is the number of times $i$ occurs in the codeword, and $u = \pm 1$. For any particular code this sign is determined uniquely by the requirement that all the $N_i$ must be nonnegative integers.

For our application, we are not interested in the case $m = 2$. Because in this case $N = p + 1$, and the irreducible code is degenerate (i.e., the dimension of the code is less than $m$). So we always assume that $m \geq 4$ in the sequel.

Computing $P_I$ seems very hard, not to mention $P_S$. So we develop bounds on both $P_I$ and $P_S$ for the authentication code based on the irreducible cyclic code in the semiprimitive case.
By Theorem 1,

$$P_S = \max_{s \in \mathcal{S}} \max_{t \in T} \frac{\left| \{ k \in \mathcal{K} : t = c_{s,k}, t' = c_{s',k} \} \right|}{N(c_s, t)}$$

$$= \max_{s \in \mathcal{S}} \max_{t \in T} \frac{\left| \{ k \in \mathcal{K} : \text{Tr}_{q/p}(x^k) = t, \text{Tr}_{q/p}(x^k) = t' \} \right|}{N(c_s, t)}$$

$$= \max_{a \in \text{GF}(q)^*} \max_{u \in \text{GF}(p) , 0 \neq a, v \in \text{GF}(p)} \frac{1}{N} \left| \left\{ x \in \text{GF}(q) : \text{Tr}_{q/p}(ax^u) = u, \text{Tr}_{q/p}(bx^v) = v \right\} \right|.$$

For any $(a, b) \in \text{GF}(q)^2$ such that $ab \neq 0$ and $(u, v) \in \text{GF}(p)^2$, define

$$N(a, u; b, v) = \left| \{ x \in \text{GF}(q) : \text{Tr}_{q/p}(ax^u) = u, \text{Tr}_{q/p}(bx^v) = v \} \right|.$$

Then

$$P_S = \max_{a \in \text{GF}(q)^*} \max_{u \in \text{GF}(p) , 0 \neq a, v \in \text{GF}(p)} \frac{1}{N} \frac{N(a, u; b, v)}{N(c(a), u)}.$$  \hspace{1cm} (4)

Similarly

$$p^2 N(a, u; b, v) = \sum_{x \in \text{GF}(q)} \sum_{y_1, y_2 \in \text{GF}(p)} \chi_1'(y_1(\text{Tr}_{q/p}(ax^u) - u) + y_2(\text{Tr}_{q/p}(bx^v) - v))$$

$$= \sum_{x \in \text{GF}(q)} \sum_{y_1, y_2 \in \text{GF}(p)} [\chi_1'(-y_1u - y_2v)][\chi_1'(\text{Tr}_{q/p}(ay_1x^u + by_2x^v))]$$

$$= \sum_{x \in \text{GF}(q)} \sum_{y_1, y_2 \in \text{GF}(p)} \chi_1'(-y_1u - y_2v) \chi_1(ay_1x^u + by_2x^v)$$

$$= q + \sum_{(y_1, y_2) \neq (0,0)} \chi_1'(1 - y_1u - y_2v) \sum_{x \in \text{GF}(q)} \chi_1[(ay_1 + by_2)x^u].$$

By Lemma 2, $|p^2 N(a, u; b, v) - q| \leq (p^2 - 1)(N - 1)q^{1/2}$. Hence

$$\frac{p^m - p^{m/2}(p^2 - 1)(N - 1)}{p^2} \leq N(a, u; b, v) \leq \frac{p^m + p^{m/2}(p^2 - 1)(N - 1)}{p^2}. \hspace{1cm} (5)$$

From Lemma 3 it follows that

$$\min_{0 \neq a \in \text{GF}(q)} \min_{u \in \text{GF}(p)} N(c(a), u) = \frac{q - p + (1 - p)(N - 1)\sqrt{q}}{Np},$$

$$\max_{0 \neq a \in \text{GF}(q)} \max_{u \in \text{GF}(p)} N(c(a), u) = \begin{cases} \frac{q + (N - 1)\sqrt{q}}{Np} & N > p, \\ \frac{q - p - (1 - p)\sqrt{q}}{Np} & N < p. \end{cases} \hspace{1cm} (6)$$
when \( u = 1 \); and that

\[
\begin{align*}
\min_{0 \neq a \in \mathbb{F}(q)} \min_{u \in \mathbb{F}(p)} N(c(a), u) &= \begin{cases} 
q - p - (p - 1)\sqrt{q} & \text{if } N < p, \\
q - (N - 1)\sqrt{q} & \text{if } N > p,
\end{cases} \\
\max_{0 \neq a \in \mathbb{F}(q)} \max_{u \in \mathbb{F}(p)} N(c(a), u) &= \frac{q - p + (p - 1)(N - 1)\sqrt{q}}{Np},
\end{align*}
\]

when \( u = -1 \).

Therefore, by Theorem 1, (4)–(7), we obtain the following.

**Theorem 4.** Let \( C \) be the irreducible cyclic code of the semiprimitive case. Then for the authentication code of (2), we have

\[
P_I = \begin{cases} 
\frac{1}{p} \left( \frac{p^m + (N - 1)p^{m/2}}{p^m - 1} \right) & \text{if } N > p, \\
\frac{1}{p} \left( \frac{p^m + (p - 1)p^{m/2} - p}{p^m - 1} \right) & \text{if } N < p
\end{cases}
\]

and

\[
\frac{1}{p} \left( p^m + p^{m/2}(p^2 - 1)(N - 1) / p^m - p - (p - 1)(N - 1)p^{m/2} \right) \geq P_S \geq \begin{cases} 
\frac{1}{p} \left( \frac{p^m + (N - 1)p^{m/2}}{p^m - 1} \right) & \text{if } N > p, \\
\frac{1}{p} \left( \frac{p^m + (p - 1)p^{m/2} - p}{p^m - 1} \right) & \text{if } N < p
\end{cases}
\]

when \( u = 1 \); and

\[
P_I = \frac{1}{p} \left( \frac{p^m - p - (1 - p)(N - 1)p^{m/2}}{p^m - 1} \right)
\]

and

\[
\frac{1}{p} \left( \frac{p^m - p - (1 - p)(N - 1)p^{m/2}}{p^m - 1} \right) \leq P_S \leq \begin{cases} 
\frac{1}{p} \left( \frac{p^m - p^{m/2}(p^2 - 1)(N - 1)}{p^m - p - (p - 1)p^{m/2}} \right) & \text{if } N < p, \\
\frac{1}{p} \left( \frac{p^m - p^{m/2}(p^2 - 1)(N - 1)}{p^m - (N - 1)p^{m/2}} \right) & \text{if } N > p
\end{cases}
\]

when \( u = -1 \).

### 3.2. \( N = 2 \) case

**Lemma 5** (Baumert and McEliece [11]). Let \( C \) be the irreducible cyclic code with \( N = 2 \). The distribution of elements from \( \mathbb{F}(p) \) in each nonzero codeword \( c(\beta) \) is given as follows. For \( m \) even

\[
N_0 = \frac{q - 1}{2p} + \frac{(1 - p)(1 + \sqrt{q})}{2p}.
\]
\[ N_i = \frac{q - 1}{2p} + \frac{1 + \sqrt{q}}{2p}, \quad i = 1, \ldots, p - 1 \]

and
\[ N_0 = \frac{q - 1}{2p} + \frac{(1 - p)(1 - \sqrt{q})}{2p}, \]
\[ N_i = \frac{q - 1}{2p} + \frac{1 - \sqrt{q}}{2p}, \quad i = 1, \ldots, p - 1, \]

where \( N_i \) is the number of times \( i \) appears in the codeword.

For \( m \) odd, one distribution is
\[ N_0 = \frac{q - 1}{2p} + \frac{1 - p}{2p}, \]
\[ N_a = \frac{q - 1}{2p} + \frac{1 + \sqrt{pq}}{2p}, \quad a \text{ a nonzero square of } \mathbb{GF}(p), \]
\[ N_b = \frac{q - 1}{2p} + \frac{1 - \sqrt{pq}}{2p}, \quad b \text{ a nonzero nonsquare of } \mathbb{GF}(p) \]

and in the other distribution the values for \( N_a \) and \( N_b \) are interchanged.

Let \( C \) be the irreducible cyclic code with \( N = 2 \). We now compute \( P_1 \) and \( P_S \) for the authentication code of (2) based on \( C \).

We first compute \( P_1 \). By Lemma 5 and Theorem 1, we have
\[
P_1 = \max_{0 \neq c \in C} \max_{u \in \mathbb{GF}(q)} \frac{N(c, u)}{n} = \begin{cases} 
1 + \frac{(p - 1)(\sqrt{q} - 1)}{p(q - 1)} & \text{m even}, \\
1 + \frac{\sqrt{pq} + 1}{p(q - 1)} & \text{m odd}.
\end{cases}
\]

Computing \( P_S \) is very hard. So we shall develop tight upper bounds on \( P_S \) instead. By Theorem 1
\[
P_S = \max_{s \in S} \max_{t \in T \neq s, t'} \frac{|\{k \in \mathbb{K} : t = c_{s,k}, t' = c'_{s,k}\}|}{N(c_s, t)}
= \max_{s \in S} \max_{t \in T \neq s, t'} \frac{|\{k \in \mathbb{K} : \text{Tr}_{q/p}(x^2(a^k) = t, \text{Tr}_{q/p}(x^2(a'^k) = t')\}|}{N(c_s, t)}
= \max_{a \in \mathbb{GF}(q)^* \neq 0} \max_{u \in \mathbb{GF}(p)} \frac{1}{2} \max_{v \in \mathbb{GF}(p)} \frac{|\{x \in \mathbb{GF}(q) : \text{Tr}_{q/p}(ax^2) = u, \text{Tr}_{q/p}(bx^2) = v\}|}{N(c(a), u)}.
\]

For any \((a, b) \in \mathbb{GF}(q)^2\) such that \(ab \neq 0\) and \((u, v) \in \mathbb{GF}(p)^2\), define
\[ N(a, u; b, v) = |\{x \in \mathbb{GF}(q) : \text{Tr}_{q/p}(ax^2) = u, \text{Tr}_{q/p}(bx^2) = v\}|. \]

Then
\[
P_S = \max_{a \in \mathbb{GF}(q)^* \neq 0} \max_{u \in \mathbb{GF}(p)} \frac{1}{2} N(a, u; b, v) \frac{N(c(a), u)}{N(c(a), u)}.
\]
To establish bounds on $P_S$, we should calculate the minimum and maximum value of $N(c, u)$. From Lemma 5, it is obvious that

$$\min_{a \in \text{GF}(q)^*} \min_{u \in \text{GF}(p)} N(c(a), u) = \begin{cases} \frac{q-1}{2p} + \frac{(1-p)(1+\sqrt{q})}{2p} & \text{m even,} \\ \frac{q-1}{2p} + 1 - \frac{\sqrt{pq}}{2p} & \text{m odd,} \end{cases}$$

$$\max_{a \in \text{GF}(q)^*} \max_{u \in \text{GF}(p)} N(c(a), u) = \begin{cases} \frac{q-1}{2p} + \frac{(1-p)(1-\sqrt{q})}{2p} & \text{m even,} \\ \frac{q-1}{2p} + \frac{\sqrt{pq}}{2p} & \text{m odd.} \end{cases}$$

Combining (8), (5) for $N=2$, (9), and the fact that $P_S \geq P_I$, we obtain the following result.

Theorem 6. Let $C$ be the irreducible cyclic code with $N=2$. Then for the authentication code of (2), we have

$$P_I = \frac{1}{p} + \frac{p-1}{p(p^{m/2}+1)},$$

$$\frac{1}{p} + \frac{p-1}{p(p^{m/2}+1)} \leq P_S \leq \frac{p^m + p^{m/2+2} - p^{m/2}}{p^{m+1} + p^{m/2+1} - p^2 - p^{m/2+2}}$$

if $m$ is even; and

$$P_I = \frac{1}{p} + \frac{1}{p^{m/2} - 1},$$

$$\frac{1}{p} + \frac{1}{p^{m/2} - 1} \leq P_S \leq \frac{p^m + p^{m/2+2} - p^{m/2}}{p^{m+1} - p^{(m+3)/2}}$$

if $m$ is odd. Furthermore, we have

$$|S| = \frac{p^m - 1}{p - 1}, \quad |T| = p, \quad |K| = (p^m - 1)/2.$$

Remark. In both cases $\lim_{m \to \infty} P_I = \lim_{m \to \infty} P_S = \frac{1}{p}$. Thus the codes are asymptotically optimal with respect to the bounds of (1). Also the upper and lower bounds for $P_S$ given in Theorem 6 are very close to each other.

4. Authentication codes from the second class of linear codes

4.1. The first type of linear codes and their authentication codes

Let $p$ be an odd prime. We define a $[p^m, 2m]$ linear code $C$ over GF$(p)$ as

$$C = \left\{ c_{a,b} = \left( f_{a,b}(0), f_{a,b}(1), f_{a,b}(\alpha), \ldots, f_{a,b}(\alpha^{p^m-2}) \right) \mid a, b \in \text{GF}(p^m) \right\},$$

(10)

where $\alpha$ is a generating element of GF$(p^m)$, and $f_{a,b}(x) = \text{Tr}_{p^m/p}(ax + bx^N)$. 

Theorem 7. Let \( C \) be the code of (10). Then for the authentication code of (2) based on \( C \), we have
\[
\frac{1}{p} \leq P_1 \leq \frac{1}{p} + \frac{(p-1)(N-1)}{p^{m/2+1}}, \quad \frac{1}{p} \leq P_S \leq \frac{1}{p} \frac{p^m + (p^2-1)(N-1)p^{m/2}}{p^m - (p-1)(N-1)p^{m/2}}.
\]
Furthermore,
\[
|S| = \frac{p^{2m} - 1}{p-1}, \quad |T| = p, \quad |K| = p^m.
\]

Proof. By Theorem 1,
\[
P_S = \max_{s \in \mathcal{S}} \max_{t \in \mathcal{T}, t' \neq s, t'} \frac{[k \in \mathcal{K} : t = c_{s,k}, t' = c_{s',k}]}{N(c_s, t)} = \max_{(0,0) \neq (a_1, b_1) \in \text{GF}(p^m)^2, u \in \text{GF}(p)} \max_{(a_2, b_2) \neq h(a_1, b_1), v, h \in \text{GF}(p)} \max_{(a_3, b_3) \neq (0,0)} \frac{[x \in \text{GF}(q) : \text{Tr}_{q/p}(a_1 x + b_1 x^N) = u, \text{Tr}_{q/p}(a_2 x + b_2 x^N) = v]}{N(c_{a_1, b_1}, u)}.
\]

Let
\[
N((a_1, b_1), u; (a_2, b_2), v) = \left\{ x \in \text{GF}(q) : \left[ \begin{array}{c} \text{Tr}_{q/p}(a_1 x + b_1 x^N) = u, \\ \text{Tr}_{q/p}(a_2 x + b_2 x^N) = v \end{array} \right] \right\}.
\]

Then
\[
P_S = \max_{(a_1, b_1) \in \text{GF}(p^m)^2, u \in \text{GF}(p)} \max_{h(a_1, b_1), v, h \in \text{GF}(p)} \max_{(a_2, b_2) \neq (0,0)} \frac{N((a_1, b_1), u; (a_2, b_2), v)}{N(c_{a_1, b_1}, u)},
\]
\[
P_1 = \max_{(a, b) \in \text{GF}(p^m)^2, u \in \text{GF}(p)} \frac{N(c_{a, b}, u)}{n}.
\]

We now develop bounds on \( N((a_1, b_1), u; (a_2, b_2), v) \), where \((a_1, b_1)\) and \((a_2, b_2)\) are linearly independent over \(\text{GF}(p)\). Similarly
\[
p^2 N((a_1, b_1), u; (a_2, b_2), v)
\]
\[
= \sum_{x \in \text{GF}(q)} \left\{ \chi_1(y_1(\text{Tr}_{q/p}(a_1 x + b_1 x^N) - u) \\ + y_2(\text{Tr}_{q/p}(a_2 x + b_2 x^N) - v)) \right\}
\]
\[
= \sum_{x \in \text{GF}(q)} \left\{ \chi_1(-y_1 u - y_2 v)\chi_1(\text{Tr}_{q/p}([a_1 y_1 + a_2 y_2]x) \\ + [b_1 y_1 + b_2 y_2]x^N) \right\}
\]
\[
= \sum_{x \in \text{GF}(q)} \left\{ \chi_1(-y_1 u - y_2 v)\chi_1([b_1 y_1 + b_2 y_2]x^N + (a_1 y_1 + a_2 y_2)x) \right\}
\]
\[
= \sum_{x \in \text{GF}(q)} 1 + \sum_{x \in \text{GF}(q)} \sum_{(y_1, y_2) \neq (0,0)} \left\{ \chi_1(-y_1 u - y_2 v)\chi_1([b_1 y_1 + b_2 y_2]x^N \\ + (a_1 y_1 + a_2 y_2)x) \right\}
\]
\[
= q + \sum_{(y_1, y_2) \neq (0,0)} \left\{ \chi_1(-y_1 u - y_2 v) \sum_{x \in \text{GF}(q)} \chi_1([b_1 y_1 + b_2 y_2]x^N \\ + (a_1 y_1 + a_2 y_2)x) \right\}
\]
Note that \((a_1, b_1) \neq h(a_2, b_2)\) for any \(h \in \text{GF}(p)\) and \((a_i, b_i) \neq (0, 0)\) for each \(i\). \(b_1y_1 + b_2y_2 = a_1y_1 + a_2y_2 = 0\) if and only if \(y_1 = y_2 = 0\). Hence by Lemma 2,
\[
|p^2N((a_1, b_1), u; (a_2, b_2), v) - q| \leq (p^2 - 1)(N - 1)q^{1/2}.
\]
It follows that
\[
N((a_1, b_1), u; (a_2, b_2), v) \geq \frac{p^m - (p^2 - 1)(N - 1)p^{m/2}}{p^2},
\]
\[
N((a_1, b_1), u; (a_2, b_2), v) \leq \frac{p^m + (p^2 - 1)(N - 1)p^{m/2}}{p^2}.
\] (12)
On the other hand, \(N(c_{a,b}, u) = |\{x \in \text{GF}(q) : \text{Tr}_{q/p}(ax + bx^N) = u\}|\). Similarly, we can get
\[
pN(c_{a,b}, u) = \sum_{x \in \text{GF}(q)} \sum_{z \in \text{GF}(p)} \chi_1([\text{Tr}_{q/p}(ax + bx^N) - u]z) = \sum_{x \in \text{GF}(q)} \sum_{z \in \text{GF}(p)} [\chi_1(-u)z] \chi_1(azx + bxz^N) = \sum_{x \in \text{GF}(q)} 1 + \sum_{z \neq 0} [\chi_1(-u)z] \chi_1(azx + bxz^N) = q + \sum_{z \neq 0} [\chi_1(-u)z] \sum_{x \in \text{GF}(q)} \chi_1(bxz^N + azx).
\]
When \((a, b) \neq (0, 0)\), by Lemma 2, \(|pN(c_{a,b}, u) - q| \leq (p - 1)(N - 1)q^{1/2}\). Hence
\[
\frac{p^m - (p - 1)(N - 1)p^{m/2}}{p} \leq N(c_{a,b}, u) \leq \frac{p^m + (p - 1)(N - 1)p^{m/2}}{p}.
\] (13)
Then the upper bounds on \(P_1\) and \(P_5\) follow from (11)–(13). The lower bound on both \(P_1\) and \(P_5\) is from (1). \(\square\)

4.2. The second type of linear codes and their authentication codes

Let \(p\) be an odd prime. The following linear code \(C\) over \(\text{GF}(p)\)
\[
C = \{c_{a,b} = (f_{a,b}(0), f_{a,b}(1), f_{a,b}(x), \ldots, f_{a,b}(x^{p^m-2})|a, b \in \text{GF}(p^m)\},
\] (14)
has parameters \([p^m, 2m]\), where \(x\) is a primitive element of \(\text{GF}(p^m)\), and \(f_{a,b}(x) = \text{Tr}_{p^m/p}(ax + bx^2)\). This class of codes was defined and used to construct authentication codes in [5]. Here we employ these linear codes to construct new authentication codes within the framework of the projective construction of this paper.

The following lemma comes from [5].

**Lemma 8.** Let \(C\) to be the code of (14). Then
\[
\max_{(0,0)\neq(a,b)\in\text{GF}(p^m)^2} \min_{u\in\text{GF}(p)} N(c_{a,b}, u) = \begin{cases} p^{m-1} + (p - 1)p^{m/2 - 1} & \text{if } m \text{ even,} \\ p^{m-1} + p^{(m-1)/2} & \text{if } m \text{ odd.} \end{cases}
\]
\[
\min_{(0,0)\neq(a,b)\in\text{GF}(p^m)^2} \max_{u\in\text{GF}(p)} N(c_{a,b}, u) = \begin{cases} p^{m-1} - (p - 1)p^{m/2 - 1} & \text{if } m \text{ even,} \\ p^{m-1} - p^{(m-1)/2} & \text{if } m \text{ odd.} \end{cases}
\]
Theorem 9. Let \( C \) be the code of (14). Then for the authentication code of (2) based on \( C \), we have

\[
P_I = \frac{1}{p} + \frac{p - 1}{p^{m/2+1}},
\]

if \( m \) is even; and

\[
P_I = \frac{1}{p} + \frac{1}{p^{(m+1)/2}}
\]

if \( m \) is odd. Furthermore, we have

\[
|S| = \frac{p^m - 1}{p - 1}, \quad |T| = p, \quad |K| = p^m.
\]

Proof. The values of \( P_I \) in the two cases follow from Theorem 1 and Lemma 8. Then the lower bounds on \( P_S \) are obtained from the values of \( P_I \) and the fact that \( P_S \geq P_I \). We now develop the upper bounds on \( P_S \). By Theorem 1

\[
P_S = \max_{s \in S} \max_{t \neq t'} \left[ \frac{|\{ k \in K : t = c_{s,k}, t' = c_{s',k} \}|}{N(e_1, t)} \right]
\]

\[
\times \max_{(0,0) \neq (a_1, b_1) \in GF(p^m), u \in GF(p)} \max_{(0,0) \neq (a_2, b_2) \neq (a_1, b_1), v \in GF(p)} \left[ \frac{|\{ k \in K : \text{Tr}_{q/p}(a_1 x^k + b_1 x^{2k}) = u, \text{Tr}_{q/p}(a_2 x^k + b_2 x^{2k}) = v \}|}{N(e_{a_1, b_1}, u)} \right].
\]

Let

\[
N((a_1, b_1), u; (a_2, b_2), v) = \left| \left\{ x \in GF(q) : \left[ \begin{array}{l} \text{Tr}_{q/p}(a_1 x + b_1 x^2) = u, \\ \text{Tr}_{q/p}(a_2 x + b_2 x^2) = v \end{array} \right] \right\} \right|.
\]

Then

\[
P_S = \max_{(0,0) \neq (a_1, b_1) \in GF(p^m), u \in GF(p)} \max_{(0,0) \neq (a_2, b_2) \neq (a_1, b_1), v, h \in GF(p)} \left[ \frac{N((a_1, b_1), u; (a_2, b_2), v)}{N(e_{a_1, b_1}, u)} \right].
\]

Setting \( N = 2 \) in (12) yields

\[
\frac{p^m - p^{m/2+2} + p^{m/2}}{p^2} \leq N((a_1, b_1), u; (a_2, b_2), v) \leq \frac{p^m + p^{m/2+2} - p^{m/2}}{p^2}. \tag{16}
\]

Combining Lemma 8, (15) and (16) yields the upper bound on \( P_S \). \( \Box \)
5. Authentication codes from the third class of linear codes

Let \( \chi \) be a nontrivial additive character of GF\((q^m)\) and let \( a \in (\text{GF}(q^m))^r, b \in \text{GF}(q^m) \). Then the sum

\[
K(\chi; a, b) = \sum_{(x_1, \ldots, x_r) \in (\text{GF}(q^m))^r} \chi(a_1 x_1 + \cdots + a_r x_r + b x_{1}^{-1} \cdots x_{r}^{-1})
\]

is called the multiple Kloosterman sum, where \( a = (a_1, \ldots, a_r) \).

Lemma 10 (Lidl and Niederreiter [9]). If \( \chi \) is a nontrivial additive character of GF\((q^m)\), \( a \in (\text{GF}(q^m))^r \) and \( b \in \text{GF}(q^m) \) with \( (a, b) \neq (0, 0) \), then

\[
K(\chi; a, b) \leq (r + 1)q^{mr/2}.
\]

The following linear code \( C \) over GF\((q)\)

\[
C = \{c_{a,b} = (f_{a,b}(\gamma_0), f_{a,b}(\gamma_1), \ldots, f_{a,b}(\gamma_{(q^m-1)^r-1})) | (a, b)\},
\]

has parameters \([(q^m - 1)^r, (r + 1)m]\), where \( \gamma_0, \gamma_1, \ldots, \gamma_{(q^m-1)^r-1} \) are all the elements of \((\text{GF}(q^m)^*)^r\), \( x = (x_1, \ldots, x_r) \), and \( f_{a,b}(x) = \text{Tr}_{q^m/q}(a_1 x_1 + \cdots + a_r x_r + b x_{1}^{-1} \cdots x_{r}^{-1}) \).

This class of codes was defined and used to construct authentication codes in [5]. Here we employ them to construct authentication codes within the framework of the projective construction of this paper.

Theorem 11. Let \( C \) be the code of (17). Then for the authentication code of (2) based on \( C \), we have

\[
1 \leq P_1 \leq \frac{1}{q} + \frac{(r + 1)(q - 1)q^{mr/2}}{q(q^m - 1)^r},
\]

\[
1 \leq P_S \leq \frac{(q^m - 1)^r + (r + 1)(q^2 - 1)q^{mr/2}}{q(q^m - 1)^r - (r + 1)(q - 1)q^{mr/2} + 1}.
\]

Furthermore,

\[
|S| = \frac{q^{(r+1)m} - 1}{q - 1}, \quad |T| = q, \quad |K| = (q^m - 1)^r.
\]

Proof. In this case, by Theorem 1

\[
P_S = \max_{s \in S, t \in T, t' \neq s, t'} \frac{|\{k \in K : t = c_{s,k}, t' = c_{s',k}\}|}{N(c_s, t)}
\]

\[
= \max_{(0,0) \neq (a, b) \in (\text{GF}(q^m))^r \times \text{GF}(q), u \in \text{GF}(q)} \max \frac{\max_{(0,0) \neq (a', b') \neq (a, b), v, h \in \text{GF}(q)} \left\{ |x \in (\text{GF}(q^m)^*)^r : f_{a,b}(x) = u, f_{a',b'}(x) = v \right\} \right]}{N(c_{a,b}, u)}
\]

\[
= \max_{(0,0) \neq (a, b) \in (\text{GF}(q^m))^r \times \text{GF}(q), u \in \text{GF}(q)} \max \frac{\max_{(0,0) \neq (a', b') \neq (a, b), v, h \in \text{GF}(q)} \left\{ |(a, b, u; (a', b'), v) \right\} \right]}{N((a, b), u)}.
\]
where
\[ N((\mathbf{a}, b), u; (\mathbf{a}', b'), v) = |\{ x \in (\text{GF}(q^m))^r : f_{\mathbf{a}, b}(x) = u, f_{\mathbf{a}', b'}(x) = v \}|, \]
\[ N((\mathbf{a}, b), u) = |\{ x \in (\text{GF}(q^m))^r : f_{\mathbf{a}, b}(x) = u \}|. \]

Let \( q = p^h \) for some \( h \), where \( p \) is a prime. Let \( \chi \) to be a nontrivial additive character of \( \text{GF}(q^m) \), then
\[
q N(\mathbf{a}, b; u) = \sum_{x \in (\text{GF}(q^m))^r} \sum_{y \in \text{GF}(q)} \chi_1[y(f_{\mathbf{a}, b}(x) - u)]
= \sum_{y \in \text{GF}(q)} \sum_{x \in (\text{GF}(q^m))^r} \chi_1[y(f_{\mathbf{a}, b}(x) - u)]
= (q^m - 1)^r + \sum_{y \in (\text{GF}(q))^*} \sum_{x \in (\text{GF}(q^m))^r} \chi_1[y(f_{\mathbf{a}, b}(x) - u)]
= (q^m - 1)^r + \sum_{y \in (\text{GF}(q))^*} \chi_1(-yu) \sum_{x \in (\text{GF}(q^m))^r} \chi_1[y(f_{\mathbf{a}, b}(x))] .
\]

By Lemma 10,
\[
|q N(\mathbf{a}, b; u) - (q^m - 1)^r| \leq \sum_{y \in (\text{GF}(q))^*} \left| \sum_{x \in (\text{GF}(q^m))^r} \chi_1[y(f_{\mathbf{a}, b}(x))] \right| \leq (r + 1)(q - 1)q^{mr/2}.
\]

Hence
\[
N(\mathbf{a}, b; u) \geq \frac{(q^m - 1)^r - (r + 1)(q - 1)q^{mr/2}}{q},
\]
\[
N(\mathbf{a}, b; u) \leq \frac{(q^m - 1)^r + (r + 1)(q - 1)q^{mr/2}}{q} . \tag{18}
\]

The upper bound on \( P_1 \) follows from (18) and Theorem 1.

We now derive the upper bound on \( P_5 \). Let \( \chi' \) to be a nontrivial additive character of \( \text{GF}(q^m) \), and let \( \chi' \) to be a nontrivial additive character of \( \text{GF}(q) \). Then
\[
q^2 N((\mathbf{a}, b), u; (\mathbf{a}', b'), v)
= \sum_{x \in (\text{GF}(q^m))^r} \sum_{y_1, y_2 \in \text{GF}(q)} \chi'_1(y_1[f_{\mathbf{a}, b}(x) - u] + y_2[f_{\mathbf{a}', b'}(x) - v])
= \sum_{y_1, y_2 \in (\text{GF}(q))^*} \sum_{x \in (\text{GF}(q^m))^r} \chi'_1(-yu - y_2v) \chi'_1(y_1 f_{\mathbf{a}, b}(x) + y_2 f_{\mathbf{a}', b'}(x))
= \frac{(q^m - 1)^r}{q^m}
+ \sum_{(y_1, y_2) \neq (0, 0)} \chi'_1(-yu - y_2v) \sum_{x \in (\text{GF}(q^m))^r} \chi'_1[y_1 f_{\mathbf{a}, b}(x) + y_2 f_{\mathbf{a}', b'}(x)].
\]

Note that \( (\mathbf{a}, b) \) and \( (\mathbf{a}', b') \) are linearly independent over \( \text{GF}(q) \) and that \( (\mathbf{a}, b) \neq (0, 0) \) and \( (\mathbf{a}', b') \neq (0, 0) \). Then
\[
(a_1y_1 + a'_1y_2, a_2y_1 + a'_2y_2, \ldots, a_ry_1 + a'_ry_2) \neq (0, 0, \ldots, 0)
\]
if \( (y_1, y_2) \neq (0, 0) \). Hence
\[
\sum_{x \in (\text{GF}(q^m))^r} \chi'_1[y_1 f_{\mathbf{a}, b}(x) + y_2 f_{\mathbf{a}', b'}(x)].
\]
\[
= \sum_{x \in (\mathbb{F}_{q^m})^r} \chi_1 \left[ (by_1 + b'y_2)x_1^{-1} \cdots x_r^{-1} + \sum_{j=1}^r (a_jy_1 + a'_jy_2)x \right]
\]
is still a Kloosterman sum with at least one nonzero coefficient. Thus by Lemma 10

\[|q^2N((a, b), u; (a', b'), v) - (q^m - 1)^r| \leq (q^2 - 1)(r + 1)q^{mr/2}.\]

Hence,

\[N((a, b), u; (a', b'), v) \geq \frac{(q^m - 1)^r - (r + 1)(q^2 - 1)q^{mr/2}}{q^2},\]

\[N((a, b), u; (a', b'), v) \leq \frac{(q^m - 1)^r + (r + 1)(q^2 - 1)q^{mr/2}}{q^2}.\]

(19)

The upper bound on \(P_S\) then follows from (18) and (19). \(\square\)

6. Authentication codes obtained from a subcode of the generalized first-order Reed–Muller codes

For any \(a \in \mathbb{F}_q(k\), define a function \(f_a\) from \(\mathbb{F}_q(k\) to \(\mathbb{F}_q\) by

\[f_a(x) = a_1x_1 + a_2x_2 + \cdots + a_kx_k,\]

where \(a = (a_1, a_2, \ldots, a_k)\) and \(x = (x_1, x_2, \ldots, x_k)\).

Define

\[C = \{f_a(\beta_0), f_a(\beta_1), \ldots, f_a(\beta_{q^k-1}) : a \in \mathbb{F}_q(k)\},\]

(20)

where \(\beta_0, \beta_1, \ldots, \beta_{q^k-1}\) denote all the elements of \(\mathbb{F}_q(k)\). Then \(C\) is a \([q^k, k, (q - 1)q^{k-1}]\) code, a subcode of the generalized first-order Reed–Muller code.

Theorem 12. Let \(C\) be the code of (20). Then for the authentication code of (2) based on \(C\), we have

\[|S| = \frac{q^k - 1}{q - 1}, \quad |T| = q, \quad |K| = q^k, \quad P_I = P_S = \frac{1}{q}.\]

Proof. For each nonzero \(a \in \mathbb{F}_q(k)\), \(f_a(x)\) takes on each element of \(\mathbb{F}_q\) exactly \(q^k-1\) times when \(x\) ranges over \(\mathbb{F}_q(k)\). Hence

\[P_I = \max_{0 \neq a \in \mathbb{F}_q(k)} \max_u \left\{ \frac{|\{x \in \mathbb{F}_q(k) : f_a(x) = u\}|}{q^k} \right\} = \frac{1}{q}.\]

We now compute \(P_S\). For any pair of nonzero \(a\) and \(b\) that are linearly independent over \(\mathbb{F}_q\), we have

\[\left\{ x \in \mathbb{F}_q(k) : f_a(x) = u, f_b(x) = v \right\} = q^{k-2}\]
for any \((u, v) \in \mathbb{GF}(q)^k \times \mathbb{GF}(q)^k\). Hence
\[
P_S = \max_{a, b \neq h, h \in \mathbb{GF}(q)} \max_{a, b, h \in \mathbb{GF}(q)} \frac{|\{x \in \mathbb{GF}(q)^k : f_a(x) = u, f_b(x) = v\}|}{|\{x \in \mathbb{GF}(q)^k : f_a(x) = u\}|}
\]
\[
= \max_{a, b \neq h, h \in \mathbb{GF}(q)} \max_{a, b, h \in \mathbb{GF}(q)} \frac{q^{k-2}}{q^{k-1}} = \frac{1}{q}.
\]
This completes the proof. □

When \(k = 2\) the authentication codes described above coincide with the projective plane codes by Gilbert et al. [6]. The authentication codes described in this section are optimal with respect to the following bound.

**Lemma 13** (Stinson [13]). In any authentication code without secrecy in which
\[
P_I = P_S = \frac{|S|}{|M|} = \frac{1}{|T|},
\]
(1) \(|\mathbb{K}| \geq |T|\) if \(|S| \leq |T| + 1\), with equality occurring if and only if the authentication matrix is an orthogonal array \(OA(|T|, |S|, 1)\) and the authentication rules (keys) are used equally likely.
(2) \(|\mathbb{K}| \geq |S|(|T| - 1) + 1\) if \(|S| \geq |T| + 1\), with equality occurring if and only if the authentication matrix is an orthogonal array \(OA(|T|, |S|, \lambda)\), where
\[
\lambda = \frac{|S|(|T| - 1) + 1}{|T|^2}
\]
and the authentication rules are used with equally probability.

The authentication codes described in this section are based on linear functions. We shall demonstrate below they are better than other codes based on linear functions. We shall also show that they are better than certain subclasses of authentication codes constructed using perfect nonlinear functions and other approaches.

### 6.1. Comparison with codes from polynomials

In [7] authentication codes with parameters
\[
|S| = q^{m(D-[(D/p)])}, \ |\mathbb{K}| = q^{m+1}, \ |T| = q, \ P_I = \frac{1}{q}, \ P_S = \frac{1}{q} + \frac{D - 1}{\sqrt{q^m}}
\]
are constructed using polynomials of degree \(D\), where \(D\) is an integer with \(1 \leq D \leq \sqrt{q^m}\) and \(p\) is the characteristic of the field \(\mathbb{GF}(q^m)\). When \(D = 1\), it gives a subclass of authentication codes with parameters
\[
|S| = q^m, \ |\mathbb{K}| = q^{m+1}, \ |T| = q, \ P_I = \frac{1}{q}, \ P_S = \frac{1}{q}.
\]
Since \(D = 1\), this subclass of authentication codes is actually constructed using affine functions. We now compare this subclass of codes with the codes described in this section.
To this end, we set $k = m + 1$ in Theorem 12. Then the authentication codes of Theorem 12 have parameters

$$|S| = q^m + q^{m-1} + \cdots + q + 1, \quad |K| = q^{m+1}, \quad |T| = q, \quad P_1 = \frac{1}{q}, \quad P_S = \frac{1}{q}.$$ 

Thus the codes of Theorem 12 are better.

### 6.2. Comparison with codes obtained from $q$-twisted construction

In [8] authentication codes with parameters

$$|S| = q^t, \quad |K| = q^2, \quad |T| = q, \quad P_1 = \frac{1}{q}, \quad P_S = \frac{t}{q}$$

are constructed by applying the “$q$-twisted construction” to the Reed–Solomon codes. It is also proved in [8] that they are weakly optimal. When $t = 1$, it gives a subclass of authentication codes with parameters

$$|S| = q, \quad |K| = q^2, \quad |T| = q, \quad P_1 = \frac{1}{q}, \quad P_S = \frac{1}{q}.$$

We now compare this subclass of codes with a subclass of codes of Theorem 12. Set $k = 2$, then the authentication codes of Theorem 12 have parameters

$$|S| = q + 1, \quad |K| = q^2, \quad |T| = q, \quad P_1 = \frac{1}{q}, \quad P_S = \frac{1}{q}.$$

Thus this subclass of codes of Theorem 12 are better.

### 6.3. Comparison with codes from perfect nonlinear functions

In [4] authentication codes with parameters

$$|S| = q^m, \quad |K| = q^{m+1}, \quad |T| = q, \quad P_1 = \frac{1}{q}, \quad P_S = \frac{1}{q}$$

are constructed using perfect nonlinear functions. The authentication codes of Theorem 12 have parameters

$$|S| = q^m + q^{m-1} + \cdots + q + 1, \quad |K| = q^{m+1}, \quad |T| = q, \quad P_1 = \frac{1}{q}, \quad P_S = \frac{1}{q}$$

and are thus better.

### 7. Conclusion

In this paper, we present a projective construction of authentication codes using error correcting codes. In order to get good authentication codes with the framework of this construction, the underlying error correcting codes should satisfy certain conditions, as
specified at the end of Section 2. However, if the codewords \((a, a, \ldots, a)\) appear in a code, one can throw away this equivalence class, and construct authentication codes similarly.

We have not been able to find existing authentication codes that could be compared with the authentication codes constructed in Sections 3–5. This is because our codes in Sections 3–5 have \(P_I \neq 1/|T|\), while most existing authentication codes have \(P_I = 1/|T|\). However, we can conclude that we have not seen any authentication code that is better than those of Sections 3–5.

Section 6 presents a class of optimal authentication codes which are better than several classes of well-known codes constructed using affine functions and perfect nonlinear functions. It demonstrates that the projective construction of authentication codes using error correcting codes described in this paper does give good and optimal authentication codes. In fact, we believe that this construction makes use of the most properties of error correcting codes and is promising. However, the main problem with this approach is that computing \(P_I\) and \(P_S\) is extremely hard.

Finally, we mention that the constructions in [5] and in this paper give different authentication codes, although they all employ the linear codes of Sections 3–5 within their frameworks. This is because the two constructions are different. The construction of [5] uses much more secret keys, compared with the construction of this paper.

Acknowledgements

This work is supported by the Research Grants Council of the Hong Kong Special Administration Region, China (Project No. HKUST6173/03E).

References


