NEW CONSTRUCTIONS OF SYSTEMATIC AUTHENTICATION CODES FROM THREE CLASSES OF CYCLIC CODES

YUNWEN LIU*

College of Liberal Arts and Sciences
National University of Defense Technology
Changsha, Hunan, China

and

imec-COSIC KU Leuven, Leuven, Belgium

LONGJIANG QU

College of Liberal Arts and Sciences
National University of Defense Technology
Changsha, Hunan, China

CHAO LI

College of Liberal Arts and Sciences and College of Computer
National University of Defense Technology
Changsha, Hunan, China

(Communicated by Gary McGuire)

Abstract. Recently, several classes of cyclic codes with three nonzero weights were constructed. With the generic construction presented by C. Ding, T. Helleseth, T. Kløve and X. Wang, we present new systematic authentication codes based on these cyclic codes. In this paper, we study three special classes of cyclic codes and their authentication codes. With the help of exponential sums, we calculate the maximum success probabilities of the impersonation and substitution attacks on the authentication codes. Our results show that these new authentication codes are better than some of the authentication codes in the literature. As a byproduct, the number of times that each element occurs as the coordinates in the codewords of the cyclic codes is settled, which is a difficult problem in general.

1. Introduction

There are two types of authentication codes, those with secrecy and those without secrecy. In this paper, we will focus on the authentication codes without secrecy which are called systematic authentication codes. A systematic authentication code is defined as 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 the encoding rule. To send information $s \in S$ to a receiver, the transmitter computes the tag $t = E_k(s) \in T$ and sends the concatenated message $m = (s, t) \in \mathcal{M}$ into a public channel. When the receiver gets the message $m' = (s', t')$ through

2010 Mathematics Subject Classification: Primary: 94A60; Secondary: 94A62.

Key words and phrases: Systematic authentication code, cyclic codes, exponential sums.

* Corresponding author: Yunwen Liu.
the channel, he/she will check whether \( t' \) equals \( E_k(s') \). If so, the receiver will accept \( m' \) as authentic, otherwise reject it.

Since the communication channel is public, an adversary could involve in the procedure to attack. In the authentication model by Simmons [17], there are two kinds of attacks, namely the impersonation attack and the substitution attack. In the impersonation attack, the adversary chooses a message and puts it into the channel, disguised to be a message from the transmitter. We denote by \( P_I \) the maximum probability that the receiver takes the disguised message as authentic. In the substitution attack, the adversary notices a message \( m \) in the channel and replaces it with a new message \( m' \neq m \), hoping the receiver will accept \( m' \) as authentic. We use \( P_S \) to denote the maximum success probability of the substitution attack. For systematic authentication codes, it is a well-known fact that \( P_S \geq P_I \geq \frac{1}{|T|} \) [16].

The security of the systematic authentication codes is not generally based on the complexity of the exhaustion provided by long keys, which is different from that of ciphers. Furthermore, systematic authentication codes are widely used in authenticating large data files, so taking the efficiency and storage cost into account, we need to obtain better ratio between the key length and the message length. Therefore, a variety of new approaches were proposed, such as constructions based on projective geometry [1], error-correcting codes [7, 9] and functions over Galois rings [15].

Among these constructions, methods which construct systematic authentication codes by error-correcting codes, such as \( q \)-twisted construction [11] and construction using rank distance codes [18], error-correcting codes [7], are of special interests. A main problem is to find “good” error-correcting codes to construct systematic authentication codes with nice properties. Thus, in this paper, we will use the generic construction presented in [7] to construct new authentication codes from several classes of cyclic codes with three nonzero weights. The major contribution of this paper is that we found examples of “good” error-correcting codes and successfully calculated the exact values of \( P_S \).

The rest of the paper is organized as follows. In Section 2, we give notations, the definition of the generic construction and lemmas which will be used in the sequel. In Section 3, we study three classes of authentication codes generated from three classes of cyclic codes with three nonzero weights. We compare our authentication codes with other authentication codes in the literature in Section 4. Finally, we conclude this paper in Section 5.

2. Preliminaries

2.1. Notations.

- \( p \) is an odd prime, \( m \) is an integer, \( q = p^m \), \( n = q - 1 \).
- \( k \) is an integer, \( d = (m, k) \), \( s = m/d \), \( q_0 = p^d \).
- \( GF(q) \) is the finite field with \( q \) elements. \( GF(q)^* \) is the set of all the nonzero elements of \( GF(q) \).
- \( \omega = e^{2\pi i/p} \) is a primitive \( p \)-th root of unity, \( i = \sqrt{-1} \).
- \( \text{Tr}_{l/j}(x) = \sum_{t=0}^{l/j-1} x^{p^{jt}} \) is the trace function from \( GF(p^l) \) to \( GF(p^j) \), where \( l, j \) are positive integers such that \( j|l \). Especially, when \( l = m \) and \( j = 1 \), \( \text{Tr}_{m/1}(\cdot) \), or simply denoted by \( \text{Tr}(\cdot) \), is the trace function from \( GF(q) \) to \( GF(p) \).
Assume that \( \chi(x) = \omega^\text{Tr}(x) \) is the canonical additive character of \( \text{GF}(q) \), and \( \chi_b(c) = \chi(bc) \), for \( b, c \in \text{GF}(q) \). Similarly, \( \tilde{\chi}(x) = \omega^x \) is the canonical additive character of \( \text{GF}(p) \), and \( \tilde{\chi}_b(c) = \tilde{\chi}(bc) \), for \( b, c \in \text{GF}(p) \).

\( \eta_0 \) is the quadratic character of \( \text{GF}(p) \), and \( \eta \) is the quadratic character of \( \text{GF}(q) \).

- \( c \in \{1, -1\} \).
- Let \( C \) be an error-correcting code over \( \text{GF}(p) \) (resp. \( \text{GF}(q) \)), \( c \) be a codeword of \( C \). Then, we denote by \( N(c, u) \) the number of times that an element \( u \in \text{GF}(p) \) (resp. \( \text{GF}(q) \)) occurs as a coordinate in the codeword \( c \).

### 2.2. A Generic Construction of Authentication Codes

In [7], a generic construction of authentication codes using the error-correcting codes was presented.

Let \( C \) be an \( (n, M) \) code over an alphabet \( B \) where \((B, +)\) is an Abelian group with \( q \) elements. In the generic construction, we define a Cartesian authentication code by

\[
(S, T, K, \{E_k : k \in K\}) = (\mathbb{Z}_M, B, \mathbb{Z}_n \times B, \{E_k : k \in K\}),
\]

where for any \( k = (k_1, k_2) \in K \) and \( s \in S \), the encoding rule is defined by \( E_k(s) = c_{s,k_1} + k_2 \), and \( c_{s,k_1} \) is the \((k_1+1)\)-th component of the codeword \( c_s \).

**Proposition 1 ([7]).** Let \( C \) be an \([n, \kappa, d]\) linear code over \( \text{GF}(q) \). Let \((B, +) = (\text{GF}(q), +)\). Then \( M = q^\kappa \). The authentication code constructed as Equation (1) becomes

\[
(S, T, K, \{E_k : k \in K\}) = (\mathbb{Z}_{q^\kappa}, \text{GF}(q), \mathbb{Z}_n \times \text{GF}(q), \{E_k : k \in K\}),
\]

and we have

\[
P_T = \frac{1}{q},
\]

\[
P_S = \max_{\emptyset \neq E \subseteq T} \max_{u \in \text{GF}(q)} \frac{N(c, u)}{n}.
\]

Furthermore,

\[
|S| = q^n, |T| = q, |K| = nq.
\]

According to Proposition 1, the difficult part of this generic construction is the selection of the underlying error-correcting code and the computation of the success probability of the substitution attack. While obtaining the weight distribution of a linear code is a well-known hard problem, computing the success probability \( P_S \) of the authentication code is more difficult.

### 2.3. Lemmas

In this subsection, we recall several definitions and results about quadratic forms and exponential sums.

**Lemma 2.1 ([14]).** Let \( m \geq 2 \) and \( k \) be integers, \( d = \gcd(m, k) \) and let \( s = m/d \).

Assume that \( q = p^m \) and \( q_0 = p^d \), where \( p \) is an odd prime, i.e., \( q = q_0^s \). Let \( Q(a, b) = \text{Tr}_{m/d}(ax^{p^k+1} + bx^2) \). Then, the following two statements hold:

1. for \((a, b) \in (\text{GF}(q) \times \text{GF}(q)) \setminus \{(0, 0)\}\), the quadratic form \( Q(a, b) \) has rank no less than \( s - 2 \);

2. for any \( a \in \text{GF}(q)^* \) and \( b \in \text{GF}(q) \), at least one of \( Q(a, b) \) and \( Q(-a, b) \) has rank \( s \).
Furthermore, for $j = 0, 1, 2$, assume that the rank of $Q(a, b)$ is $s - j$. Thus, the possible values of $\sum_{x \in \text{GF}(q)} \omega^{xQ(a,b)}$ are

$$
\sum_{x \in \text{GF}(q)} \omega^{xQ(a,b)} := v_j = \begin{cases} 
\varepsilon p^{(m+jd)/2}, & \text{if } m+jd \text{ is even;} \\
\varepsilon \sqrt{p^{v-1}p^{(m+jd-1)/2}}, & \text{if } m+jd \text{ is odd.}
\end{cases}
$$

In addition, for any $y \in \text{GF}(p)^*$,

$$
\sum_{x \in \text{GF}(q)} \omega^{yQ(a,b)} = \eta_0(y^r) \sum_{x \in \text{GF}(q)} \omega^{xQ(a,b)},
$$

where $r$ is the rank of the quadratic form $Q(a,b)$.

Particularly, when $d = \gcd(m, k) = 1$, the following result holds.

**Lemma 2.2** ([12]). Let $R(a, b) = \sum_{x \in \text{GF}(q)} \omega^{xQ(a,b)}$ and let $v_j, j = 0, 1, 2$, be defined as Equation (2). Define

$$
N_{e,j}^+ = \{(a, b) \in \text{GF}(q)^2 | R(a, b) = \varepsilon v_j \},
$$

$$
N_{e,j}^- = \{(a, b) \in \text{GF}(q)^2 | R(-a, b) = \varepsilon v_j \}.
$$

Assume that $\lambda$ is a non-square of $\text{GF}(p)^*$. For $j = 0, 1, 2$, we have

1. $(a, b) \in N_{\pm,j}^+$ if and only if $(-a, b) \in N_{\mp,j}$;
2. $\lambda N_{e,0}^+ = N_{\pm,0}^+, \lambda N_{e,0}^- = N_{\pm,0}$;
3. $\lambda N_{e,1}^+ = N_{\mp,1}^+, \lambda N_{e,1}^- = N_{\pm,1}$;
4. $\lambda N_{e,2}^+ = N_{\pm,2}^+, \lambda N_{e,2}^- = N_{\pm,2}$.

Furthermore, for odd $m \geq 3$ and positive integer $k$ with $\gcd(m, k) = 1$, the values of the multi-sets

$$\{(R(a, b), R(-a, b)) | a, b \in \text{GF}(q)\}
$$

are $(\pm v_0, \pm v_0), (\pm v_1, \pm v_1), (\pm v_2, v_0), (\pm v_2, v_0), (p^m, p^m)$.

**Definition 2.3** ([13]). 1. Let $\phi$ be a multiplicative character and $\chi_b$ an additive character of $\text{GF}(q)$. Then, the Gaussian sum $G(\phi, \chi_b)$ is defined by

$$
G(\phi, \chi_b) = \sum_{c \in \text{GF}(q)^*} \phi(c)\chi_b(c).
$$

2. Let $\lambda_1, \ldots, \lambda_k$ be $k$ multiplicative characters of $\text{GF}(q)$. Then, the Jacobi sum in $\text{GF}(q)$ is defined by

$$
J(\lambda_1, \ldots, \lambda_k) = \sum_{c_1 + c_2 + \ldots + c_k = 1} \lambda_1(c_1)\ldots\lambda_k(c_k),
$$

with the summation extended over all $k$-tuples $(c_1, \ldots, c_k) \in \text{GF}(q)^k$ satisfying $c_1 + c_2 + \ldots + c_k = 1$.

The following lemma indicates the calculation of some Gaussian sums with quadratic multiplication characters.

**Lemma 2.4** ([13, Exercise 5.19]). Let $p$ be an odd prime and $q = p^m$. Let $\eta$ be the quadratic character of $\text{GF}(q)$ and $\chi_b$ be an additive character, where $b \in \text{GF}(q)$. Then, we have

$$
G(\eta, \chi_b) = \eta(b)(-1)^{(q+1)/2}q^{(p^2+2p+5)/4}q^{1/2}.
$$
3. Authentication codes based on cyclic codes with two zeroes

Let $p$ be a prime, $m$ be a positive integer, $q = p^m$ and $\pi$ be a primitive element in $\text{GF}(q)$. Let $\Gamma_j$ be the $p$-cyclotomic coset modulo $q - 1$ containing $j$. Assume that $t \geq 1$, $i_1, \ldots, i_t$ are elements of $\mathbb{Z}_{q-1}$ such that the cyclotomic cosets $\Gamma_{i_1}, \ldots, \Gamma_{i_t}$ are pairwise disjoint with size $m$. Define the code $C_{(i_1, \ldots, i_t)}$ by the cyclic code with parity-check polynomial $h(x) = m_{i_1}(x) \cdots m_{i_t}(x)$, where $m_i(x)$ is the minimal polynomial of $\pi^{-i}$ over $\text{GF}(p)$. It is obvious that $C_{(i_1, \ldots, i_t)}$ is a $[q - 1, tm]$ cyclic code.

From Delsarte’s Theorem [5], the trace representation of $C_{(i_1, \ldots, i_t)}$ is

$$C_{(i_1, \ldots, i_t)} = \left\{ \left( \sum_{s=1}^t \text{Tr}(a_s \pi^{j_s}) \right)^{q-2} \mid a_1, \ldots, a_t \in \text{GF}(q) \right\}$$

with $j_s = (1, \ldots, 1, 0, \ldots, 0)$, for $s = 1, \ldots, t$.

Herein and after, we will consider the cyclic codes in Equation (4) with two zeroes, namely, $C_{(1,e)}$, where we choose proper values for $e$ to get special cyclic codes. A general study into this kind of codes was presented in [12]. The original idea of constructing the cyclic code was from [2, 19], where the monomial $x^e$ is a PN polynomial. Moreover, the code here is so general that it contains several classes of three-weight codes in the literature as special cases, for example, [4, 6, 14, 20, 21].

In the next three subsections, we will use three classes of cyclic codes from [20], [4] and [21], respectively, to construct the authentication codes.

The most difficult part is the computation of the probability $P_S$ of the authentication codes, which is harder than the determination of the weight distribution of the linear codes. This is also the major contribution of this paper.

3.1. Authentication code based on the first class of cyclic codes.

Lemma 3.1 ([20]). Let $m \geq 3$ be odd, $p = 3$ and $e = 3^{(m+1)/2} - 1$. Then, $C_{(1,e)}$ is a $[p^m - 1, 2m]$ cyclic code over $\text{GF}(p)$ with three nonzero weights $(p-1)p^{m-1} \pm \frac{p-1}{2}p^{(m-1)/2}, (p-1)p^{m-1}$.

With the generic construction of authentication codes, we can get the first class of authentication codes as follows.

Theorem 3.2. The authentication code constructed from code $C_{(1, 3^{(m+1)/2} - 1)}$ is

$$(S, T, \mathcal{K}, \{ E_k : k \in \mathcal{K} \}) = (\mathbb{Z}_{3^2m}, \text{GF}(3), \mathbb{Z}_{3^{m-1}} \times \text{GF}(3), \{ E_k : k \in \mathcal{K} \}),$$

with

$$P_T = \frac{1}{3},$$

and

$$P_S = \frac{3^{m-1} + \frac{1}{2}(3^{(m-1)/2} + 3^{(m+1)/2})}{3^m - 1}.$$
Proof. Let \( n = p^m - 1 \) and \( h = (m + 1)/2 \). To obtain the success probability of the substitution attack, we need to know the number of times that each element in \( \text{GF}(p) \) occurs as the coordinates in the codewords of the cyclic code. We have

\[
N(c(a), u) = \frac{1}{p} \left[ \sum_{x \in \text{GF}(q)^*} \sum_{y \in \text{GF}(p)} \omega^y(\text{Tr}(ax + bx^{h-1}) - u) \right]
\]

\[
= \frac{1}{p} \left[ \sum_{x \in \text{GF}(q)} \sum_{y \in \text{GF}(p)} \omega^y(\text{Tr}(ax + bx^{h-1}) - u) - \sum_{y \in \text{GF}(p)} \omega^{-yu} \right].
\]

When \( u = 0 \), we get

\[
\max N(c(a), 0) = \max(n - wt(c(a), b)) = n - d = p^{m-1} + \frac{p - 1}{2}p^{(m-1)/2} - 1.
\]

So the rest is to consider the cases for \( u \neq 0 \), and we have

\[
N(c(a), u) = \frac{1}{p} \left[ \sum_{x \in \text{GF}(q)^*} \sum_{y \in \text{GF}(p)} \omega^y(\text{Tr}(ax + bx^{h-1}) - u) \right]
\]

\[
= \frac{1}{p} \left[ q \sum_{x \in \text{GF}(q)} \sum_{y \in \text{GF}(p)^*} \omega^y(\text{Tr}(ax + bx^{h-1}) - u) \right]
\]

\[
= p^{m-1} + \frac{1}{p} \sum_{y \in \text{GF}(p)^*} \sum_{x \in \text{GF}(q)} \omega^{-yu} \omega^y\text{Tr}(ax + bx^{h-1}).
\]

Let

\[
\sigma := \sum_{y \in \text{GF}(p)^*} \omega^{-yu} \sum_{x \in \text{GF}(q)} \omega^y\text{Tr}(ax + bx^{h-1}),
\]

and

\[
R(a, b) = \sum_{x \in \text{GF}(3^m)} \omega^x\text{Tr}(ax + bx^{h-2}).
\]

Noting that \(-1\) is a non-square of \( \text{GF}(3^m) \), the following equality (Theorem 6.2 of [20]) can be easily verified:

\[
T(a, b) := \sum_{x \in \text{GF}(3^m)} \omega^x\text{Tr}(ax + bx^{h-1}) = \frac{1}{2}(R(a, b) + R(-a, b)).
\]

Hence if \( u = 1 \), then we have

\[
\sigma = \sum_{y \in \text{GF}(3^m)^*} \omega^{-yu} \sum_{x \in \text{GF}(3^m)} \omega^y\text{Tr}(ax + bx^{h-1})
\]

\[
= \sum_{y \in \text{GF}(3^m)^*} \omega^{-yu} T(ya, yb)
\]

\[
= -\frac{1}{2} - \frac{\sqrt{3}}{2}i T(a, b) + \omega T(-a, -b)
\]

\[
= -\frac{1}{2} \left( R(a, b) + R(-a, b) + R(-a, -b) + R(a, -b) \right)
\]

\[
= -\frac{1}{2} \left( R(a, b) + R(-a, b) - R(-a, -b) - R(a, -b) \right).
\]

By Lemma 2.2, we know the relationship between \( R(a, b) \) and \( R(-a, -b) \) and all the possible values of the multi-sets \( (R(a, b), R(-a, b)) \).
When \((R(a, b), R(-a, b)) = (v_0, v_0)\), since \(-1\) is a non-square element in GF\((p)\), we have
\[-N_{e,0}^+ = N_{-e,0}^+, \quad -N_{e,0}^- = N_{-e,0}^-,\]
which means \(R(a, b) = -R(-a, -b)\) and \(R(-a, b) = -R(a, -b)\). And it follows that
\[
\sigma = -\frac{1}{2} \left[ (R(a, b) + R(-a, b) + R(-a, -b) + R(a, -b)) \right] - \frac{\sqrt{3}}{2} |\frac{1}{2} (R(a, b) + R(-a, b) - R(-a, -b) - R(a, -b))| = -\frac{\sqrt{3}}{2} i (R(a, b) + R(-a, b) - 2v_0) = 3^{(m+1)/2}.
\]

With a similar method, for all possible values of \(R(a, b)\) and \(R(-a, b)\), we have
\[
\sigma = \begin{cases} 
\pm 3^{(m+1)/2}, & \text{if } R(a, b) = R(-a, b) = \pm v_0; \\
0, & \text{if } R(a, b) = -R(-a, b) = \pm v_0; \\
0, & \text{if } (R(a, b), R(-a, b)) = (v_0, v_1) \text{ or } (v_1, v_0); \\
-3^{(m+1)/2}, & \text{if } (R(a, b), R(-a, b)) = (-v_0, v_1) \text{ or } (v_1, -v_0); \\
3^{(m+1)/2}, & \text{if } (R(a, b), R(-a, b)) = (v_0, -v_1) \text{ or } (-v_1, v_0); \\
0, & \text{if } (R(a, b), R(-a, b)) = (-v_0, -v_1) \text{ or } (-v_1, -v_0); \\
\pm 3^{(m+1)/2} + 3^{(m-1)/2}, & \text{if } (R(a, b), R(-a, b)) = (v_0, v_2) \text{ or } (v_2, v_0); \\
-3^m, & \text{if } R(a, b) = R(-a, b) = 3^m.
\end{cases}
\]

It is easy to verify that the values of \(\sigma\) for \(u = -1\) are the same as those in Equation (5).

Hence, we have
\[
N(c(a, b), \pm 1) = \begin{cases} 
3^{m-1}, & \text{if } c(a, b) = \pm 1; \\
3^{m-1} + 3^{(m-1)/2}, & \text{if } c(a, b) = 3^{(m-1)/2} + 3^{(m+1)/2}; \\
3^{m-1} + 3^{(m+1)/2}, & \text{if } c(a, b) = 3^{m-1} + \frac{1}{2} (3^{(m-1)/2} + 3^{(m+1)/2}).
\end{cases}
\]

Therefore, the maximum can be obtained by
\[
\max N(c(a, b), u) = 3^{m-1} + \frac{1}{2} (3^{(m-1)/2} + 3^{(m+1)/2}).
\]

It then follows from Proposition 1 that
\[
P_3 = \frac{3^{m-1} + \frac{1}{2} (3^{(m-1)/2} + 3^{(m+1)/2})}{3^{m-1}}.
\]
Lemma 3.4 ([4]). Let $S(a, b) = \sum_{x \in \mathbb{GF}(p^m)} \omega^{Tr_m/(ax + bx^e)}$. Then, one has

$$S(a, b) = \begin{cases} p^m, & \text{if } a = b = 0; \\ 0, & \text{if } a \neq 0 \text{ and } b = 0; \\ \pm ip^{m/2}, & \text{if } a = 0 \text{ and } b \neq 0; \\ \frac{1}{2}(S_1(a, b) + S_1(-a, b)), & \text{if } a, b \in \mathbb{GF}(q)^* , \end{cases}$$

where

$$S_1(a, b) = \sum_{x \in \mathbb{GF}(p^m)} \omega^{Tr_m/(ax^e + bx^2)}.$$ 

Theorem 3.5. The authentication code constructed from the code $C_{(1,(p^m+1)/(p^e+1)+(p^m+1)/2)}$ is

$$(S, T, K, \{E_k : k \in K\}) = (\mathbb{Z}_{p^2m}, \mathbb{GF}(p), \mathbb{Z}_{p^m-1} \times \mathbb{GF}(p), \{E_k : k \in K\}),$$

with

$$P_I = \frac{1}{p}$$

and

$$P_S = \begin{cases} \frac{1}{2}p^{m-1} + \frac{1}{2}p^{(m-1)/2}, & \text{if } m = k; \\ \frac{1}{2}p^{m-1} + \frac{1}{2}p^{(m-1)/2} + \frac{1}{2}p^{(m+2k-1)/2}, & \text{if } m > k. \end{cases}$$

Furthermore, we have

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

Proof. To calculate the probability of the substitution attack, we need to know the number of times that each element in $\mathbb{GF}(p)$ occurs as the coordinates in the codewords. Similar to the proof of Theorem 3.2, we consider the cases for $u \neq 0$, and have

$$N(c(a, b), u) = \frac{1}{p} \left[ \sum_{x \in \mathbb{GF}(q)} \sum_{y \in \mathbb{GF}(p)} \omega^{g(Tr_m/(ax + bx^e) - u)} \right]$$

$$= \frac{1}{p} \left[ g + \sum_{x \in \mathbb{GF}(q)} \sum_{y \in \mathbb{GF}(p)^*} \omega^{g(Tr_m/(ax + bx^e) - u)} \right]$$

$$= p^{m-1} + \frac{1}{p} \sum_{y \in \mathbb{GF}(p)^*} \omega^{-yu} \sum_{x \in \mathbb{GF}(q)} \omega^{g(Tr_m/(ax + bx^e))}$$

$$= p^{m-1} + \frac{1}{p} \sum_{y \in \mathbb{GF}(p)^*} \omega^{-yu} S(ya, yb).$$

For $a, b \in \mathbb{GF}(q)^*$, one has

$$S(ya, yb) = \sum_{x \in \mathbb{GF}(p^m)} \omega^{g(Tr_m/(ax + bx^e))}$$

$$= \frac{1}{2}(S_1(ya, yb) + S_1(-ya, yb))$$

$$= \frac{1}{2} \left( \sum_{x \in \mathbb{GF}(p^m)} \omega^{g(Tr_m/(ax + bx^e))} \right)$$

$$= \frac{1}{2} \left( \sum_{x \in \mathbb{GF}(p^m)} \omega^{Tr_m/(ax + bx^e)} + \sum_{x \in \mathbb{GF}(p^m)} \omega^{Tr_m/(a(-x) + b(-x^e))} \right)$$

$$= \frac{1}{2} \left( \eta_0(y^{\text{tr}}) \sum_{x \in \mathbb{GF}(p^m)} \omega^{Tr_m/(ax + bx^e)} + \eta_0(y^{\text{tr}}) \sum_{x \in \mathbb{GF}(p^m)} \omega^{Tr_m/(a(-x) + b(-x^e))} \right),$$
where \( r_1, r_2 \) are the ranks of \( Q(a, b), Q(-a, b) \), respectively. The last identity follows from Equation (3). According to Lemma 2.1, we know that \( r_1, r_2 \in \{ s, s - 1, s - 2 \} \) and at least one of \( r_1 \) and \( r_2 \) is equal to \( s \). Hence the rest of the calculation of \( S(ya, yb) \) splits into the following cases. Recall that \( d = \gcd(m, k) = k \) and \( s = m/d = m/k \). It is clear that \( s = m/k \) is odd since \( m \) is odd.

Firstly, we assume that \( m > k \), i.e., \( s > 2 \).

**CASE A.1** \( r_1 \geq r_2 \)

**CASE A.1** \( r_1 = r_2 = s \)

With the knowledge of

\[
S(ya, yb) = \frac{1}{2}(\eta_0(y^{r_1}) + \eta_0(y^{r_2})) = \frac{1}{2}(\eta_0(y^s) + \eta_0(y^s)) = \pm \eta(y^s)ip^{m/2},
\]

one has

\[
\sum_{y \in \text{GF}(p)^*} \omega^{-yu} S(ya, yb) = \pm ip^{m/2} \sum_{y \in \text{GF}(p)^*} \omega^{-yu} \eta_0(y) = \pm ip^{m/2} \sum_{y \in \text{GF}(p)^*} \eta_0(y) = \pm ip^{m/2} G(\eta_0, \hat{\chi} - u)
\]

where Lemma 2.4 is used in the last but one equality.

Thus, we have

\[
\max N(c(a, b), u) = p^{m-1} + p^{(m-1)/2}.
\]

**CASE A.2** \( r_1 = s, r_2 = s - 1 \)

Similarly, the following equation holds

\[
S(ya, yb) = \frac{1}{2}(\eta_0(y^{r_1}) + \eta_0(y^{r_2})) = \frac{1}{2}(\eta_0(y^s) + \eta_0(y^{s-1})) = \pm \eta(y^s)ip^{m/2} \pm p(m+k)/2.
\]

As a result, we have

\[
\sum_{y \in \text{GF}(p)^*} \omega^{-yu} S(ya, yb) = \pm \frac{1}{2} \sum_{y \in \text{GF}(p)^*} \omega^{-yu} (\eta_0(y) \pm \eta_0(y^{s-1})p^{(m+k)/2}) = \pm \frac{1}{2} (p^{(m+1)/2} \eta(1) - p^{(m+1)/2} \pm p(m+k)/2),
\]

and

\[
\max N(c(a, b), u) = p^{m-1} + \frac{1}{2}(p^{(m-1)/2} + p^{(m+k-2)/2}).
\]
CASE A.3 \( r_1 = s, r_2 = s - 2 \)

\[
S(ya, yb) = \frac{1}{2}(\eta_0(y^{r_1}) \sum_{x \in \text{GF}(p^m)} \omega^{|x|/2}Q(a, b) + \eta_0(y^{r_2}) \sum_{x \in \text{GF}(p^m)} \omega^{|x|/2}Q(-a, b))
\]

\[
= \frac{1}{2}(\eta_0(y^s)\sqrt{p^{p-1}}p^{(m-1)/2} + \eta_0(y^{s-2})(\sqrt{p^{p-1}}p^{(m+2k-1)/2}))
\]

\[
= \frac{1}{2}(\eta_0(y^s)\sqrt{p^{p-1}}p^{(m-1)/2} + \eta_0(y^{s-2})(\sqrt{p^{p-1}}p^{(m+2k-1)/2}))
\]

Hence, we have

\[
\sum_{y \in \text{GF}(p^m)} \omega^{-yu}S(ya, yb) = \pm \frac{1}{2}(p^{(m+1)/2}(\eta(-u)(-1)(p+1)/2(p^2+2p+5)/4) \pm p^{(m+2k+1)/2}(\eta(-u)(-1)(p+1)/2(p^2+2p+5)/4),
\]

and

\[
\max N(c(a, b), u) = p^{m-1} + \frac{1}{2}p^{(m-1)/2} + p^{(m+2k-1)/2}.
\]

CASE B \( r_1 \leq r_2 \)

For these three symmetric cases (CASE B.1, B.2, B.3) when \( r_1 \) and \( r_2 \) switch their values, we can easily check that the conclusions remain.

Therefore, we have

\[
\max N(c(a, b), u) = \begin{cases} 
  p^{m-1} + \frac{1}{2}p^{(m-1)/2} + \frac{1}{2}p^{(m+2k-1)/2}, & \text{if } u \neq 0 \text{ and } m > k; \\
  p^{m-1} + \frac{1}{2}p^{(m+k)/2} - \frac{1}{2}p^{(m+k)/2-1}, & \text{if } u = 0 \text{ and } m > k.
\end{cases}
\]

that is, when \( m > k \), we have

\[
\max N(c(a, b), u) = p^{m-1} + \frac{1}{2}p^{(m-1)/2} + \frac{1}{2}p^{(m+2k-1)/2}.
\]

Special situation \( s = 1 \)

When \( s = 1 \), CASE A.3(CASE B.3) is impossible. Hence, there are only two cases.

The first case is \( r_1 = r_2 = 1 \).

\[
\max N(c(a, b), u) = p^{m-1} + p^{(m-1)/2}.
\]

The second is that one of \( r_1, r_2 \) is 1 and the other is 0. In this case,

\[
\max N(c(a, b), u) = p^{m-1} + \frac{1}{2}(p^{(m-1)/2} + p^{(m+k-2)/2}) = \frac{3}{2}p^{m-1} + \frac{1}{2}p^{(m-1)/2}.
\]

Therefore, we have

\[
\max N(c(a, b), u) = \begin{cases} 
  \frac{3}{2}p^{m-1} + \frac{1}{2}p^{(m-1)/2}, & \text{if } m = k; \\
  \frac{p^{m-1} + \frac{1}{2}p^{(m-1)/2} + \frac{1}{2}p^{(m+2k-1)/2}}{p^{m-1}}, & \text{if } m > k.
\end{cases}
\]

\[ \square \]
3.3. Authentication code based on the third class of cyclic codes.

Lemma 3.6 ([21]). Let \( m \) and \( k \) be positive integers such that \( s = m/d \) is odd and \( s \geq 3 \), where \( d = \text{gcd}(m, k) \). Let \( p \) be an odd prime, \( q = p^m \) and \( q_0 = p^d \). Then, the cyclic code \( C \) with parity check polynomial \( h_1(x)h_2(x) \), where \( h_1(x), h_2(x) \) are the minimal polynomials of \((-\pi)^{-1} \) and \( \pi^{-(p^k+1)/2} \), has the following trace representation:

\[
C = \{c(a, b) | a, b \in \text{GF}(q)\},
\]

where

\[
c(a, b) = \left( \text{Tr}(a(-\pi)^t + b\pi^{(p^k+1)t/2}) \right)_{t=0}^{q-2}.
\]

The parameter of the code is \([p^m - 1, 2m, p^m - p^{m-1} - \frac{p-1}{2}p^{(m+d-2)/2}]\).

Theorem 3.7. The authentication code constructed from the code in Lemma 3.6 is

\[\{(S, T, K, \{E_k : k \in K\}) = (Z_{p^2m}, \text{GF}(p), Z_{p^m-1} \times \text{GF}(p), \{E_k : k \in K\})\},\]

with

\[P_I = \frac{1}{p},\]

and

\[P_S = \begin{cases} 
p^{m-1} + \frac{1}{p}p^{(m-2)/2} + \frac{1}{p}p^{(m-2d-1)/2}, & \text{if } k/d \text{ is even}; \\
p^{m-1} + \frac{1}{p}p^{(m-2d-1)/2}, & \text{if } k/d \text{ is odd}.
\end{cases}\]

Furthermore,

\[|S| = p^{2m}, |T| = p, |K| = (p^m - 1)p.\]

Proof. When \( u = 0 \), we have

\[\max N(c(a, b), 0) = p^{m-1} + \frac{p-1}{2}p^{(m+d-2)/2} - 1.\]

When \( u \neq 0 \), as in the previous subsections, the key to calculate \( P_S \) is to compute the following exponential sum:

\[N(c(a, b), u) = \frac{1}{p} \sum_{t=0}^{q-2} \sum_{y \in \text{GF}(p)} \omega^y [\text{Tr}_{m/1}(a(-\pi)^t + b\pi^{(p^k+1)t/2}) - u]\]

\[= \frac{1}{p} \sum_{x \in \text{GF}(q)} \sum_{y \in \text{GF}(p)} \omega^y [\text{Tr}_{m/1}(a\eta x + bx^{(p^k+1)/2}) - u]\]

\[= \frac{1}{p} \sum_{x \in \text{GF}(q)} \sum_{y \in \text{GF}(p)^*} \omega^y [\text{Tr}_{m/1}(a\eta x + bx^{(p^k+1)/2}) - u]\]

\[= p^{m-1} + \frac{1}{p} \sum_{y \in \text{GF}(p)^*} \omega^{-yu} \sum_{x \in \text{GF}(q)} \omega^{y [\text{Tr}_{m/1}(a\eta x + bx^{(p^k+1)/2})]}\]

Let \( \lambda \) be a fixed non-square of \( \text{GF}(q_0) \). One can easily verify the following result (Proposition 3.1 of [21]):

\[\lambda^{(1+p^k)/2} = \begin{cases} 
\lambda, & \text{if } k/d \text{ is even}, \\
-\lambda, & \text{if } k/d \text{ is odd}.
\end{cases}\]

Let

\[\rho(ya, yb) = \sum_{x \in \text{GF}(q)} \omega^{y [\text{Tr}_{m/1}(a\eta x + bx^{(p^k+1)/2})]}\]
Then we have
\[
\rho(ya, yb) = \frac{1}{2} \sum_{x \in \mathbb{GF}(q)} \left( \omega^{\text{Tr}_{m/1}(ya^2 + yb^2)} + \omega^{\text{Tr}_{m/1}(-ya \lambda^2 + yb \lambda)} \right)
\]
\[
= \begin{cases} 
\frac{1}{2} \sum_{x \in \mathbb{GF}(q)} \left( \omega^{\text{Tr}_{m/1}(ya^2 + yb^2)} + \omega^{\text{Tr}_{m/1}(-ya \lambda^2 + yb \lambda)} \right), & \text{if } k/d \text{ is even;} \\
\frac{1}{2} \sum_{x \in \mathbb{GF}(q)} \left( \omega^{\text{Tr}_{m/1}(ya^2 + yb^2)} + \omega^{\text{Tr}_{m/1}(-ya \lambda^2 - yb \lambda)} \right), & \text{if } k/d \text{ is odd;}
\end{cases}
\]
\[
= \begin{cases} 
\frac{1}{2} \sum_{x \in \mathbb{GF}(q)} \left( \omega^{\text{Tr}_{d/1}(y(a, b)) + \text{Tr}_{d/1}(y(-a, -b))} \right), & \text{if } k/d \text{ is even;}
\end{cases}
\]
where \(Q(a, b) = \text{Tr}_{m/d}(ax^2 + by^2 + 1)\).

When \(k/d\) is even, similarly as the calculation of \(S(ya, yb)\) in Theorem 3.5, we have
\[
\rho(ya, yb) = \frac{1}{2} \left( \eta_0(y) \varepsilon i^m/2 + \eta_0(y) (\varepsilon i)^{(m+2d)/2} \right).
\]
Thus, one has
\[
\max N(c(a, b), u) = \max(p^{m-1} + \frac{1}{p} \sum_{y \in \mathbb{GF}(p)^*} \omega^{-yu} \rho(ya, yb))
\]
\[
= p^{m-1} + \frac{1}{2}p^{(m-1)/2} + \frac{1}{2}p^{(m+2d-1)/2}
\]
and
\[
P_S = \frac{p^{m-1} + \frac{1}{2}p^{(m-1)/2} + \frac{1}{2}p^{(m+2d-1)/2}}{p^m - 1}.
\]

When \(k/d\) is odd, we get
\[
\rho(ya, yb) = \frac{1}{2} \left( \sum_{x \in \mathbb{GF}(q)} \omega^{\text{Tr}_{d/1}Q(ya, yb)} + \sum_{x \in \mathbb{GF}(q)} \omega^{\text{Tr}_{d/1}Q(-ya, -yb)} \right).
\]
It follows from Lemma 2.1 that \(Q(a, b)\) and \(Q(-a, -b)\) have the same rank. In addition, with Equation (3), we have
\[
\left\{ \begin{array}{c}
\sum_{x \in \mathbb{GF}(q)} \omega^{\text{Tr}_{d/1}Q(a, b)} = - \sum_{x \in \mathbb{GF}(q)} \omega^{\text{Tr}_{d/1}Q(-a, -b)}, & \text{when the rank of } Q(a, b) \text{ is } s, s - 2; \\
\sum_{x \in \mathbb{GF}(q)} \omega^{\text{Tr}_{d/1}Q(a, b)} = - \sum_{x \in \mathbb{GF}(q)} \omega^{\text{Tr}_{d/1}Q(-a, -b)}, & \text{when the rank of } Q(a, b) \text{ is } s - 1.
\end{array} \right.
\]
As a result, the following equation holds
\[
\rho(ya, yb) = \frac{1}{2} \left( \sum_{x \in \mathbb{GF}(q)} \omega^{\text{Tr}_{d/1}Q(ya, yb)} + \sum_{x \in \mathbb{GF}(q)} \omega^{\text{Tr}_{d/1}Q(-ya, -yb)} \right)
\]
\[
= \frac{1}{2} \left( \eta_0(y^s) \sum_{x \in \mathbb{GF}(q)} \omega^{\text{Tr}_{d/1}Q(a, b)} + \eta_0(y^s) \sum_{x \in \mathbb{GF}(q)} \omega^{\text{Tr}_{d/1}Q(-a, -b)} \right)
\]
\[
= \frac{1}{2} \eta_0(y^s) \left( \sum_{x \in \mathbb{GF}(q)} \omega^{\text{Tr}_{d/1}Q(a, b)} + \sum_{x \in \mathbb{GF}(q)} \omega^{\text{Tr}_{d/1}Q(-a, -b)} \right)
\]
\[
= \eta_0(y^{s-1}) \sum_{x \in \mathbb{GF}(q)} \omega^{\text{Tr}_{d/1}Q(a, b)}.
\]
Therefore, we have
\[
\max N(c(a, b), u) = \max (p^{m-1} + \frac{1}{p} \sum_{y \in GF(p)^*} \omega^{-yu} p(ya, yb))
\]
\[
= p^{m-1} + p^{(m+2d-1)/2}
\]
and
\[
\frac{\sum_{y \in GF(p)^*} \omega^{-yu} \rho(ya, yb)}{p^{m-1} + p^{(m+2d-1)/2}}
\]

4. Comparison

There are five parameters, namely \(|S|, |T|, |K|, P_I\) and \(P_S\), in a systematic authentication code. Hence, for any two authentication codes, they are comparable when they have at least three parameters in common. However, it does not mean that we cannot compare authentication codes with less than three parameters in common, since there are examples that all the parameters of one code are better than those of another code.

In this section, we call the authentication codes constructed in Theorems 1, 2 and 3 as Code C1, C2 and C3 respectively.

(1) It is clear that the source state, tag space, key space and maximum success probability of the impersonation attack are the same for C1 and C2 when \(p = 3\), while

\[
P_S(C1) = \frac{3^{m-1} + \frac{1}{3} \left( 3^{(m-1)/2} + 3^{(m+1)/2} \right)}{3^m - 1},
\]

\[
P_S(C2) = \left\{ \begin{array}{ll}
\frac{3^{m-1} + \frac{1}{3} \left( 3^{(m-1)/2} + 3^{(m+2d-1)/2} \right)}{3^m - 1}, & \text{if } k/d \text{ is even;}
\frac{3^{m-1} + \frac{1}{3} \left( 3^{(m+2d-1)/2} \right)}{3^m - 1}, & \text{if } k/d \text{ is odd.}
\end{array} \right.
\]

As a consequence, when \(k = 1 < m\), the two authentication codes have the same parameters. However, when \(m > k \geq 2\) or \(m = k > 3\), C1 is better than C2 since \(P_S(C1) < P_S(C2)\), which means the success probability of the substitution attack of C1 is smaller than that of C2. Similarly, C1 is better than C3 when \(p = 3\).

(2) The source space and key space of C2 and C3 are of the same size, when \(d = k\) in C3, the two codes are comparable with \(P_S(C2) \leq P_S(C3)\). Thus, under a special condition, C2 is better than C3.

(3) Compared with the authentication codes constructed in the literature, our new authentication codes also have some advantages. In Theorem 8 of [7], the authors constructed a class of authentication codes (denoted by C4) with the following parameter:

\[
P_I = \frac{1}{p}, P_S = \left\{ \begin{array}{ll}
\frac{1}{p} + \frac{p-1}{p^{m+1}}, & \text{when } m \text{ is even;}
\frac{1}{p} + \frac{1}{p^{m+1}}, & \text{when } m \text{ is odd,}
\end{array} \right.
\]

and \(|S| = p^{2m}, |T| = p, |K| = p^{m+1}\). Compared with C2, it has the same parameters \(|S|, |T|\) and \(P_I\). However, the key space of C2 is smaller, which indicates less cost on the key storage and better ratio between the key length and the message length, while \(P_S\) of C2 is certainly larger than that of C4. However, it is necessary to point out that the differences between \(P_S\) of C2 and \(P_S\) of C4 is negligible. For example, when \(p = 3, m = 3, k = 1\), the difference is 0.039, and when \(p = 11, m = 9, k = 3\), the difference is 0.004. The differences narrow down with the increases of \(p, m\) and \(k\). Therefore, it is worthy for us to make the tradeoff between the key length and \(P_S\), compared with the authentication code in C4.
When \( q = p \geq 3 \), the systematic authentication codes (denoted by C5) constructed from some highly nonlinear functions have the following parameters [8]:

\[
|S| = p^{2m}, \quad |T| = p, \quad |K| = p^{m+1},
\]

\[
P_I = \frac{1}{p}, \quad P_S = \frac{1}{p} + \frac{p-1}{q^{(m+2)/2}}.
\]

Similar with the previous comparison, C2 and C5 have the same \( |S|, |T|, P_I \), and \( |K(C5)| > |K(C2)| \). Although we have \( P_S(C2) > P_S(C5) \), the difference decreases with the growing of \( p, m \), which means that C2 is better than C5 when authenticating large files.

(5) Recall the construction by Helleseth and Johansson [10], and denote it by C6. When \( q = p \geq 3 \), we have:

\[
|S| = p^{m(D-\lfloor D/p \rfloor)}, \quad |T| = p, \quad |K| = p^{m+1},
\]

\[
P_I = \frac{1}{p}, \quad P_S = \frac{1}{p} + \frac{D-1}{\sqrt{p}}.
\]

Particularly, if \( D = 2 \), then we have

\[
|S| = p^{2m}, \quad |T| = p, \quad |K| = p^{m+1},
\]

\[
P_I = \frac{1}{p}, \quad P_S = \frac{1}{p} + \frac{1}{\sqrt{p}}.
\]

It is clear that \( |K(C6)| = |K(C4)| > |K(C2)| \). Besides, since \( P_S(C6) > P_S(C4) \), C2 is better than C4, therefore better than C5.

As for those authentication codes with three or more different parameters, we define a new parameter as \( \rho \) value. To obtain a better ratio between the key length and the message length, the \( \rho \) value is expected to be relatively small with a decent key length.

**Definition 4.1.** Let a systematic authentication code be \((S, T, K, P_I, P_S)\). We define the ratio between key space and source space as its \( \rho \) value, i.e.,

\[
\rho = \frac{|K|}{|S|}.
\]

(6) There is a construction by optimal nonlinear functions (Theorem 11 of [3]), when \( q = p \geq 3 \), the code (denoted by C7) has the following parameters

\[
|S| = p^m, \quad |T| = p, \quad |K| = p^m.
\]

Besides, it has \( P_S > P_I > 1/p \).

\( |T| \) of C7 is the only parameter which is the same as that of C2. Meanwhile, we have \( \rho(C7) = 1 \). When dealing with large files, i.e., \( p \) and \( m \) are large enough, \( \rho(C2) = \frac{p^m-1}{p^{m-1}} < \rho(C7) \), therefore, C2 is better than C7.

5. Conclusion

In this paper, we employed three classes of cyclic codes to construct new systematic authentication codes. The exact values of \( P_I, P_S \) were deduced by calculating the number of times that each element occurs as the coordinates in the codewords. Compared with some authentication codes generated in the literature, our authentication codes are better with a lower probability of successful substitution attack or a smaller key space.
The results in this paper imply that one could obtain good authentication codes from good cyclic codes, especially those cyclic codes with relatively fewer weights. Recently, many constructions of three-weight [20] and five-weight cyclic codes [22] were presented and most of them were constructed with the same rule as the cyclic codes used in our paper. So we believe it is worthwhile to study the authentication codes based on these cyclic codes. The readers are cordially invited to join this adventure.

ACKNOWLEDGMENTS

We would like to thank the reviewers for their valuable suggestions and comments. This work was supported by the NSFC of China under Grant 61722213, Grant 11531002, and Grant 61572026, the National Basic Research Program of China under Grant 2013CB338002, the Basic Research Fund of National University of Defense Technology under Grant CJ 13-02-01, and the Program for New Century Excellent Talents in University.

REFERENCES

[1] J. Bierbrauer, Universal hashing and geometric codes, Des. Codes Crypt., 11 (1997), 207–221.
[2] C. Carlet, C. Ding and J. Yuan, Linear codes from perfect nonlinear mappings and their secret sharing schemes, IEEE Trans. Inf. Theory, 51 (2005), 2089–2102.
[3] S. Chanson, C. Ding and A. Salomaas, Cartesian authentication codes from functions with optimal nonlinearity, Theor. Comp. Sci., 290 (2003), 1737–1752.
[4] S.-T. Choi, J.-Y. Kim, J.-S. No and H. Chung, Weight distribution of some cyclic codes, in 2012 IEEE Int. Symp. Inf. Theory Proc. (ISIT), 2012, 2901–2903.
[5] P. Delsarte, On subfield subcodes of modified Reed-Solomon codes (corresp.), IEEE Trans. Inf. Theory, 21 (1975), 575–576.
[6] C. Ding, Y. Gao and Z. Zhou, Five families of three-weight ternary cyclic codes and their duals, IEEE Trans. Inf. Theory, 59 (2013), 7940–7946.
[7] C. Ding, T. Helleseth, T. Klove and X. Wang, A generic construction of Cartesian authentication codes, IEEE Trans. Inf. Theory, 53 (2007), 2229–2235.
[8] C. Ding and H. Niederreiter, Systematic authentication codes from highly nonlinear functions, IEEE Trans. Inf. Theory, 50 (2004), 2421–2428.
[9] C. Ding and X. Wang, A coding theory construction of new systematic authentication codes, Theor. Comp. Sci., 330 (2005), 81–99.
[10] T. Helleseth and T. Johansson, Universal hash functions from exponential sums over finite fields and Galois rings, in Adv. Crypt. - CRYPTO’96, Springer, 1996, 31–44.
[11] G. A. Kabatianskii, B. Smeets and T. Johansson, On the cardinality of systematic authentication codes via error-correcting codes, IEEE Trans. Inf. Theory, 42 (1996), 566–578.
[12] C. Li, N. Li, T. Helleseth and C. Ding, The weight distributions of several classes of cyclic codes from APN monomials, IEEE Trans. Inf. Theory, 60 (2014), 4710–4721.
[13] R. Lidl and H. Niederreiter, Finite Fields, Cambridge Univ. Press, 1997.
[14] J. Luo and K. Feng, On the weight distributions of two classes of cyclic codes, IEEE Trans. Inf. Theory, 54 (2008), 5332–5344.
[15] F. Özbudak and Z. Saygi, Some constructions of systematic authentication codes using Galois rings, Des. Codes Crypt., 41 (2006), 343–357.
[16] R. S. Rees and D. R. Stinson, Combinatorial characterizations of authentication codes II, Des. Codes Crypt., 7 (1996), 239–259.
[17] G. J. Simmons, Authentication theory/coding theory, in Adv. Crypt. - CRYPTO’84, Springer, 1984, 411–431.
[18] H. Wang, C. Xing and R. Safavi-Naini, Linear authentication codes: bounds and constructions, IEEE Trans. Inf. Theory, 49 (2003), 866–872.
[19] J. Yuan, C. Carlet and C. Ding, The weight distribution of a class of linear codes from perfect nonlinear functions, IEEE Trans. Inf. Theory, 52 (2006), 712–717.
[20] Z. Zhou and C. Ding, Seven classes of three-weight cyclic codes, IEEE Trans. Commun., 61 (2013), 4120–4126.
[21] Z. Zhou and C. Ding, A class of three-weight cyclic codes, *Finite Fields Appl.*, **25** (2014), 79–93.

[22] Z. Zhou, C. Ding, J. Luo and A. Zhang, A family of five-weight cyclic codes and their weight enumerators, *IEEE Trans. Inf. Theory*, **59** (2013), 6674–6682.

Received July 2015; revised July 2017.

*E-mail address: univerlyw@hotmail.com*

*E-mail address: ljqu_happy@hotmail.com*

*E-mail address: lichao_nudt@sina.com*