ACADEMIC
PRESS

Available at
www.ComputerScienceWeb.com
POWERED BY SCIENCE @ DIRECT®

Information and Computation 184 (2003) 93–108

Information
and
Computation

www.elsevier.com/locate/ic

Logarithm Cartesian authentication codes

T.W. Sze,[a] S. Chanson,[a] C. Ding,[a] T. Helleseth,[b] and M.G. Parker [b,*]

[a]Department of Computer Science, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, China
[b]Department of Informatics, University of Bergen, 5020 Bergen, Norway

Received 13 December 2001; revised 4 March 2002

Abstract

Chanson, Ding and Salomaa have recently constructed several classes of authentication codes using certain classes of functions. In this paper, we further extend that work by constructing two classes of Cartesian authentication codes using the logarithm functions. The codes constructed here involve the theory of cyclotomy and are better than a subclass of Helleseth–Johansson's codes and Bierbrauer's codes in terms of the maximum success probability with respect to the substitution attack.

Keywords: Authentication codes; Cryptography; Cyclotomy

1. Introduction

Authentication codes were considered in 1974 by Gilbert and Sloane [5]. In the model of authentication theory described by Simmons [11], there are three participants: a transmitter, a receiver, and an opponent. The transmitter wants to send information to the receiver through a public channel which is subject to active attacks, while the opponent wants to deceive the receiver. Without observing any message from the transmitter to the receiver, the opponent impersonates the transmitter by sending his message to the receiver, causing the receiver to accept a fraudulent message as authentic. This is called the *impersonation attack*, and we use P_{d_0} to denote the opponent's maximum success probability with respect to this attack. Having observed one message from the transmitter to the receiver, the opponent

[*] Corresponding author. Fax: +47-55-58-4199.

E-mail addresses: szetszwo@cs.ust.hk (T.W. Sze), chanson@cs.ust.hk (S. Chanson), cding@cs.ust.hk (C. Ding), torh@ii.uib.no (T. Helleseth), Matthew.Parker@ii.uib.no (M.G. Parker).

0890-5401/03/$ - see front matter © 2003 Elsevier Science (USA). All rights reserved.
doi:10.1016/S0890-5401(03)00053-1

replaces the original message with his own message. This is called the *substitution attack*, and we use P_{d_1} to denote the opponent's maximum success probability with respect to this attack.

To protect against these attacks, the transmitter and the receiver share a secret key, which is used in an authentication code. In this model there is only one receiver, and it is the model considered in this paper. For multireceiver authentication codes, the reader is referred to [4,7,9,10].

A *systematic Cartesian authentication code* is a code in which the source state (i.e., the plaintext) is concatenated with an authenticator (also called a tag) to form a message which is sent via a channel. Such a code is a 5-tuple (S, E, M, T, f), where S is the set of source states, E is the set of keys, and T is the set of authenticators, M is the set of all possible messages, and $f : S \times E \to T$ is the authentication mapping. Each function $f(\cdot, e)$ is called an encoding rule. When the transmitter wants to send the information $s \in S$ using a key $e \in E$, which is secretly shared with the receiver, he transmits the message $m = (s, t)$, where $t = f(s, e) \in T$ is the tag (authenticator). When the receiver receives the message $m = (s, t)$, he checks its authenticity by verifying whether $t = f(s, e)$ or not using the secret key $e \in E$. If the equality holds, the message is regarded as authentic and is accepted. Otherwise the message is rejected.

Combinatorial designs have been successfully used to construct certain optimal authentication codes [8,12]. Certain algebraic curves give also very good authentication codes [1,13]. Chanson, Ding and Salomaa [2] have recently presented two constructions of authentication codes using certain classes of functions. Some of their codes are optimal. In this paper, using the framework of [2] we construct authentication codes with logarithm functions. The authentication codes constructed in this paper are better than a subclass of Helleseth–Johansson's codes and Bierbrauer's codes in terms of the success probability P_{d_1} with respect to the substitution attack.

2. The first class of Cartesian authentication codes based on logarithm functions

Let F be a mapping from A to B, where $(A, +)$ and $(B, +)$ are finite abelian groups. The first construction of [2] gives authentication codes

$$(S, E, T, f), \tag{1}$$

where the set of source states is $(S, +) = (A, +)$, the set of keys $(E, +) = (A, +)$, the tag space is $(T, +) = (B, +)$, and the authentication mapping f from $S \times E$ to T is defined by

$$f(s, e) = F(s + e), \quad e \in A.$$

It is assumed that there is a probability distribution on both the source state space and the key space. In this construction, the keys and the source states are equally likely. The message space $M = S \times T$, which depends totally on S and T.

As for the code of (1), the two deception probabilities are given in the following theorem [2], whose proof is included here for completeness.

Theorem 1. *Let $(S, +)$ and $(T, +)$ be finite abelian groups, and let F be a mapping from S to T. Then for the authentication code (S, E, T, f) of (1) defined above, we have*

$$P_{d_0} = \max_{t' \in T} \frac{\left|F^{-1}(t')\right|}{|S|}.$$

$$P_{d_1} = \max_{s\in S, t\in F(S)} \max_{s'\neq s, t'} \frac{\left|\left(F^{-1}(t)-s\right)\cap\left(F^{-1}(t')-s'\right)\right|}{\left|F^{-1}(t)\right|},$$

where $F(S)$ is the image of S under the mapping F.

Proof. In an impersonation attack, the opponent wants to generate a new message $m' = (s', t')$ by choosing a source state s' and an $e' \in E$ and computing $t' = F(s' + e')$. The new message m' is then inserted into the channel. This attack is successful if and only if $F(s' + e) = t'$. We now need to compute the probability $\Pr(F(s' + e) = t')$. Note that the keys and source states are equiprobable. We have

$$\begin{aligned} P_{d_0} &= \max_{s',t'} \frac{|\{e\in E : t' = f(s',e)\}|}{|\{e\in E\}|} \\ &= \max_{s',t'} \frac{\left|F^{-1}(t')-s'\right|}{|E|} \\ &= \max_{t'\in T} \frac{\left|F^{-1}(t')\right|}{v}. \end{aligned}$$

In a substitution attack, the opponent observed a message $m = (s, t)$ and replaces it with another message $m' = (s', t')$, where $s \neq s'$. Since the keys and source states are equiprobable, the probability of success of the substitution attack is

$$\begin{aligned} P_{d_1} &= \max_{s\in S, t\in F(S)} \max_{s'\neq s, t'} \frac{|\{e\in E : t = f(s,e), t' = f(s',e)\}|}{|\{e\in E : t = f(s,e)\}|} \\ &= \max_{s\in S, t\in F(S)} \max_{s'\neq s, t'} \frac{\left|\left(F^{-1}(t)-s\right)\cap\left(F^{-1}(t')-s'\right)\right|}{\left|F^{-1}(t)\right|}. \quad \square \end{aligned}$$

With the framework above, several classes of authentication codes were constructed by Chanson, Ding and Salomaa [2]. Their codes were based on several classes of functions. In this paper, we use some types of logarithm functions to construct a new class of authentication codes. Throughout this paper we define $Z_d = \{0, 1, \ldots, d-1\}$. It is known that $P_{d_0} \leqslant P_{d_1}$ for all systematic Cartesian authentication codes [12].

To describe authentication codes based on the logarithm functions, we make use of the theory of cyclotomy. Let $\mathrm{GF}(q)$ be a finite field, and let $q - 1 = dl$. For a primitive element α of $\mathrm{GF}(q)$, define $D_0^{(d,q)} = (\alpha^d)$, the multiplicative group generated by α^d, and

$$D_i^{(d,q)} = \alpha^i D_0^{(d,q)} \quad \text{for } i = 1, 2, \ldots, d-1.$$

The $D_i^{(d,q)}$ are called *cyclotomic classes* of order d. The *cyclotomic numbers* of order d with respect to $\mathrm{GF}(q)$ are defined as

$$(i, j)_d = \left|\left(D_i^{(d,q)} + 1\right) \cap D_j^{(d,q)}\right|.$$

Clearly, there are at most d^2 different cyclotomic numbers of order d [3].

To prove properties of the authentication codes dealt with in the following sections, for each $j \in Z_d$ we define

$$C_j^{(d,q)}=\begin{cases} D_j^{(d,q)} & \text{if } 1 \leqslant j \leqslant d-1, \\ D_0^{(d,q)} \cup \{0\} & \text{if } j=0. \end{cases} \tag{2}$$

Theorem 2. *Let $q-1=dl$, where $d \geqslant 2$ and l are positive integers. Set $S=GF(q)$ and $T=Z_d$. Define $F(x)=(\log_\alpha x) \bmod d$, where $\log_\alpha 0=0$. Then for the authentication code (S, E, T, f) of* (1), *we have*

$$|S|=q, \quad |E|=q, \quad |T|=d$$

and

$$P_{d_0}=\frac{1}{d}+\frac{d-1}{dq},$$

$$\frac{d(\max(i,\, j)_d)}{q-1+d} \leqslant P_{d_1} \leqslant \begin{cases} d\,\frac{\max(i,j)_d+1}{q-1}, & \textit{if } \frac{q-1}{d} \textit{ odd}, \\ d\max\left(\frac{(0,0)_d+2}{q+d-1}, \frac{\max(i,j)_d+1}{q-1}\right), & \textit{if } \frac{q-1}{d} \textit{ even}. \end{cases}$$

Proof. By the definition of $F(x)$, we have $F^{-1}(0)=D_0^{(d,q)} \cup \{0\}$ and $F^{-1}(i)=D_i^{(d,q)}$ for each $i \in Z_d \setminus \{0\}$. It then follows from Theorem 1 that

$$P_{d_0}=\max_{t' \in T}\frac{\left|F^{-1}(t')\right|}{|S|}=\frac{1+(q-1)/d}{q}=\frac{1}{d}+\frac{d-1}{dq}.$$

To prove the inequalities for P_{d_1}, we need to determine $\frac{\left|F^{-1}(t) \cap \left(F^{-1}(t')+a\right)\right|}{F^{-1}(t)}$, where $0 \neq a \in \mathrm{GF}(q)$. Let $a^{-1} \in D_i^{(d,q)}$, $t \not\equiv 0 \pmod d$ and $t' \not\equiv 0 \pmod d$. By Lemma 5 in Appendix A, we have

$$\begin{aligned} \frac{\left|F^{-1}(0) \cap \left(F^{-1}(0)+a\right)\right|}{F^{-1}(0)} &= \frac{\left|C_0^{(d,q)} \cap \left(C_0^{(d,q)}+a\right)\right|}{\frac{q-1}{d}+1} \\ &= \frac{d\left((i,i)_d+\left|D_0^{(d,q)} \cap \{a,-a\}\right|\right)}{q+d-1}, \\ \frac{\left|F^{-1}(t) \cap \left(F^{-1}(0)+a\right)\right|}{F^{-1}(t)} &= \frac{\left|C_t^{(d,q)} \cap \left(C_0^{(d,q)}+a\right)\right|}{\frac{q-1}{d}} \\ &= \frac{d\left((i,t+i)_d+\left|D_t^{(d,q)} \cap \{a\}\right|\right)}{q-1}, \\ \frac{\left|F^{-1}(0) \cap \left(F^{-1}(t)+a\right)\right|}{F^{-1}(0)} &= \frac{\left|C_0^{(d,q)} \cap \left(C_t^{(d,q)}+a\right)\right|}{\frac{q-1}{d}+1} \\ &= \frac{d\left((t+i,i)_d+\left|D_t^{(d,q)} \cap \{-a\}\right|\right)}{q+d-1}, \end{aligned}$$

$$\begin{aligned}\frac{\left|F^{-1}(t)\cap\left(F^{-1}(t')+a\right)\right|}{F^{-1}(t)} &= \frac{\left|C_t^{(d,q)}\cap\left(C_{t'}^{(d,q)}+a\right)\right|}{\frac{q-1}{d}}\\ &= \frac{d(t'+i,t+i)_d}{q-1}.\end{aligned}$$

By Theorem 1 and Lemma 5 in Appendix A,

$$\begin{aligned}P_{d_1} &= \max_{s\in S,t\in F(S)}\ \max_{s'\neq s,t'} \frac{\left|(F^{-1}(t)-s)\cap\left(F^{-1}(t')-s'\right)\right|}{|F^{-1}(t)|}\\ &= \max_{a\neq 0,t\neq 0 \pmod d,t'\neq 0 \pmod d} \begin{pmatrix} \frac{d\left((i,i)_d+\left|D_0^{(d,q)}\cap\{a,-a\}\right|\right)}{q+d-1}, \\ \frac{d\left((i,t+i)_d+\left|D_t^{(d,q)}\cap\{a\}\right|\right)}{q-1}, \\ \frac{d\left((t+i,i)_d+\left|D_t^{(d,q)}\cap\{-a\}\right|\right)}{q+d-1}, \\ \frac{d(t'+i,t+i)_d}{q-1} \end{pmatrix}\\ &\leqslant \max\left\{d\frac{(0,0)_d+2}{q+d-1}, d\frac{\max(i,j)_d+1}{q-1}\right\}.\end{aligned}$$

If $(q-1)/d$ is odd, we prove that

$$\left|D_0^{(d,q)}\cap\{a,-a\}\right|\leqslant 1. \tag{3}$$

If $l=(q-1)/d$ is even, then $-1=\alpha^{d(l/2)}$, where α is the primitive element used to define the cyclotomic classes. Hence $-1\in D_0^{(d,q)}$. On the other hand, if $-1\in D_0^{(d,q)}$, then there is a positive integer $k<l$ such that $-1=\alpha^{dk}$. Hence $1=\alpha^{2dk}$ and thus $2k\equiv 0 \pmod l$. It follows that l is even. Thus $-1\in D_0^{(d,q)}$ if and only if l is even.

Hence if $(q-1)/d$ is odd, we have

$$\begin{aligned}P_{d_1} &\leqslant \max\left\{d\frac{\max(i,j)_d+1}{q+d-1}, d\frac{\max(i,j)_d+1}{q-1}\right\}\\ &= d\frac{\max(i,j)_d+1}{q-1}.\end{aligned}$$

It is obvious that

$$\frac{d(\max(i,j)_d)}{q-1+d}\leqslant P_{d_1}.$$

This completes the proof. □

For the authentication codes of Theorem 2, the success probability of impersonation P_{d_0} is essentially $1/d$ when d is small compared to q. The probability of successful substitution P_{d_1} is bounded below and above by the maximum cyclotomic number of order d. In general it is hard to determine the maximum cyclotomic number of order d for large d.

The codes described in Theorem 2 do contain very good codes, as given in the following theorem.

Theorem 3. *Let $q = p^{2s}$ and $d = p^s - 1$. Then the code of Theorem 2 has parameters*

$$|S| = p^{2s}, \quad |E| = p^{2s}, \quad |T| = p^s - 1$$

and

$$P_{d_0} = \frac{1}{p^s - 1} + \frac{p^s - 2}{p^{2s}(p^s - 1)},$$

$$P_{d_1} \leqslant \begin{cases} \frac{3}{p^s+1}, & \text{if } p = 2 \\ \frac{3}{p^s+1}, & \text{if } p \text{ odd, and } p^s + 1 \neq 0 \pmod 3, \\ \frac{4}{p^s+2}, & \text{if } p \text{ odd, and } p^s + 1 = 0 \pmod 3. \end{cases}$$

Proof. To prove this theorem, we first show that $(i, j)_d \leqslant 2$ for any pair (i, j). To this end, we consider the number of solutions (u, v) to the equation

$$\alpha^j \alpha^{du} = 1 + \alpha^i \alpha^{dv}, \tag{4}$$

where $0 \leqslant i, j \leqslant d - 1$ and $0 \leqslant u, v \leqslant p^s$. Define

$$l = p^s + 1, \quad a = \alpha^i, \quad b = \alpha^j.$$

Then it follows from (4) that

$$\left(1 + a\alpha^{dv}\right)^{p^s+1} = b^{p^s+1},$$

which gives

$$a\left(\alpha^{dv}\right)^2 + \left(1 + a^{p^s+1} - b^{p^s+1}\right)\alpha^{dv} + a^{p^s} = 0.$$

Note that the equation

$$ax^2 + \left(1 + a^{p^s+1} - b^{p^s+1}\right)x + a^{p^s} = 0 \tag{5}$$

has at most two solutions. Hence $(i, j)_d \leqslant 2$.

If $p = 2$, then $l = p^s + 1$ must be odd. It then follows from Theorem 2 that $P_{d_1} \leqslant \frac{3}{p^s+1}$.

If $p^s + 1 \neq 0 \pmod 3$, we claim that $(0, 0)_d \leqslant 1$. In this case we have $(i, j) = (0, 0)$. So (5) becomes $x^2 + x + 1 = 0$. If $x = \alpha^{dv} \neq 1$ is a solution of $x^2 + x + 1 = 0$, then $v \neq 0$ and $x^3 - 1 = (x - 1)(x^2 + x + 1) = 0$. Hence $x^3 = \alpha^{3dv} = 1$ and 3 divides $l = p^s + 1$. This is contrary to the assumption that $p^s + 1 \neq 0 \pmod 3$. Hence in the case $p^s + 1 \neq 0 \pmod 3$, $x^2 + x + 1$ has at most one solution $x = 1$. It then follows again from Theorem 2 that $P_{d_1} \leqslant \frac{3}{p^s+1}$.

If $p^s + 1 = 0 \pmod 3$, it follows from the fact $(i, j)_d \leqslant 2$ and Theorem 2 that $P_{d_1} \leqslant \frac{4}{p^s+2}$. This completes the proof. □

The class of codes of Theorem 3 are the best among all the codes described in Theorem 2, because at least one cyclotomic number of order d must be 2. This is justified by one of the following two formulas [3]:

(A) $\sum_{m=0}^{d-1}(h,m)_d = l - n_h$, where

$$n_h = \begin{cases} 1, & h \equiv 0 \pmod{d},\ l \text{ even} \\ 1, & l \equiv d/2 \pmod{d},\ l \text{ odd} \\ 0, & \text{otherwise.} \end{cases}$$

(B) $\sum_{h=0}^{d-1}(h,m)_d = l - k_m$, where

$$k_m = \begin{cases} 1, & \text{if } m \equiv 0 \pmod{d}; \\ 0, & \text{otherwise.} \end{cases}$$

2.1. Comparison with Helleseth–Johansson's codes

We now compare the codes of Theorem 3 with a subclass of codes constructed by Helleseth and Johansson [6]. They constructed a class of codes with parameters

$$|S| = r^{m(D-\lfloor D/p\rfloor)}, \quad |E| = r^{m+n}, \quad |T| = r^n \tag{6}$$

and

$$\begin{aligned} P_{d_0} &= \frac{1}{r^n}, \\ P_{d_1} &= \frac{1}{r^n} + \frac{D-1}{\sqrt{r^m}}, \end{aligned} \tag{7}$$

where r is a power of a prime p, and $D \geqslant 1$ is an integer.

For the two codes to be comparable, we need to set $m = n = s$, $r = p > 2$, and $D = 2$. Then the subclass of codes constructed by Helleseth and Johansson have parameters

$$|S'| = p^{2s}, \quad |E'| = p^{2s}, \quad |T'| = p^s \tag{8}$$

and

$$\begin{aligned} P'_{d_0} &= \frac{1}{p^s}, \\ P'_{d_1} &= \frac{1}{p^s} + \frac{1}{\sqrt{p^s}}. \end{aligned} \tag{9}$$

Note that the tag space of the subclass of codes constructed by Helleseth and Johansson has one more element than the codes in Theorem 3. So $\max\{P_{d_0}, P_{d_1}\} = P_{d_1}$ for the former should be smaller than that for the latter. However, if $p^s \geqslant 4$, we have

$$\frac{1+\sqrt{p^s}}{p^s} - \frac{4}{2+p^s} = \frac{2-3p^s+\sqrt{p^s}(p^s+2)}{p^s(p^s+2)} > 0.$$

Hence from Table 1 the codes of Theorem 3 are better than the subclass of codes constructed by Helleseth and Johansson. Note that while the parameters of Helleseth–Johansson's codes are more flexible, the two code construction schemes are comparable only when the above mentioned conditions are satisfied.

Table 1
Comparison of a subclass of Helleseth–Johansson's codes with those in Theorem 3

Parameters	S	E	T	$\max\{P_{d_0}, P_{d_1}\} = P_{d_1}$
Subclass of HJ's codes	p^{2s}	p^{2s}	p^s	$\frac{1+\sqrt{p^s}}{p^s}$
Codes in Theorem 3	p^{2s}	p^{2s}	$p^s - 1$	$\frac{4}{2+p^s}$

3. The second class of authentication codes based on the logarithm function

Let F be a mapping from A to B, where $(A, +)$ and $(B, +)$ are finite abelian groups. The second construction of [2] gives authentication codes

$$(S, E, T, f), \tag{10}$$

where the set of source states is $(S, +) = (A, +)$, the set of keys $(E, +) = (A \times B, +)$, the tag space is $(T, +) = (B, +)$, and the authentication mapping f from $S \times E$ to T is defined by

$$f(s, (e_a, e_b)) = F(s + e_a) + e_b, \quad (e_a, e_b) \in A \times B.$$

In this construction, all keys and all state sources are equally likely. Hence, the number of keys (encoding rules) is equal to the number of messages, while in the first construction given in Section 2 the number of keys (encoding rules) is much smaller.

This construction of systematic authentication codes is quite general. The key task is to search for functions that give good authentication codes within the framework of this construction. In this section, we use some logarithm functions to construct another class of authentication codes.

Theorem 4. *Let $q - 1 = dl$, where d and l are positive integers and q is a power of an odd prime. Set $S = GF(q)$ and $T = Z_d$. Define $F(x) = (\log_\alpha x) \bmod d$, where $\log_\alpha 0 = 0$. Then for the code (S, E, T, f) of (10), we have*

$$|S| = q, \quad |E| = qd, \quad |T| = d$$

and

$$P_{d_0} = \frac{1}{d},$$

$$P_{d_1} = \begin{cases} \frac{1}{d} + \frac{2d-1}{qd} & l \text{ even and } d \text{ even} \\ & \text{or } l \text{ odd and } d \equiv 0 \pmod 4, \\ \frac{1}{d} + \frac{d-1}{qd} & \text{otherwise.} \end{cases}$$

Proof. By Theorem 1,

$$P_{d_0} = \max_{s \in S, t \in f(S,E)} \frac{|\{e \in E \mid t = f(s, e)\}|}{|\{e \in E\}|}$$
$$= \max_{s \in S, t \in f(S,E)} \frac{|\{(e_a, e_b) \mid t = F(s + e_a) + e_b\}|}{|A||B|}$$

$$
\begin{aligned}
&= \frac{|A|}{|A||B|}\\
&= \frac{1}{d}.
\end{aligned}
$$

$$
\begin{aligned}
P_{d_1} &= \max_{s\in S, t\in f(S,E)} \max_{s'\neq s, t'\in f(S,E)} \frac{|\{e\in E \mid t = f(s,e), t' = f(s',e)\}|}{|\{e \in E \mid t = f(s,e)\}|}\\
&= \max_{s\in S, t\in f(S,E)} \max_{s'\neq s, t'\in f(S,E)} \frac{|\{(e_a, e_b) \mid t = F(s+e_a)+e_b, t' = F(s'+e_a)+e_b\}|}{|A|}\\
&= \frac{\max_{s\in S, t\in f(S,E)} \max_{s'\neq s, t'\in f(S,E)} \left[\sum_{e_b\in Z_d} \left|\left(C_{t-e_b}^{(d,q)} - s\right) \cap \left(C_{t'-e_b}^{(d,q)} - s'\right)\right|\right]}{q}\\
&= \max_{a\neq 0, b}\left[\sum_{b'\in Z_d} \left|\left(C_{b'}^{(d,q)} + a\right) \cap C_{b+b'}^{(d,q)}\right|\right] / q,
\end{aligned}
$$

where $a = s' - s \neq 0$, $a^{-1} \in D_i^{(2,q)}$, $b' = t - e_b$ and $b = t' - t$.

Case 1: $b \bmod d = 0$, by Lemmas 5 and 7,

$$
\begin{aligned}
P_{d_1} &= \max_{a\neq 0}\left[\left|\left(C_0^{(d,q)} + a\right) \cap C_0^{(d,q)}\right| + \sum_{b'\in Z_d\setminus\{0\}} \left|\left(C_{b'}^{(d,q)} + a\right) \cap C_{b'}^{(d,q)}\right|\right] / q\\
&= \max_{a\neq 0}\left[(i,i)_d + \left|D_0^{(d,q)} \cap \{a, -a\}\right| + \sum_{b'\in Z_d\setminus\{0\}} (i+b', i+b')_d\right] / q\\
&= \max_{a\neq 0}\left[\left|D_0^{(d,q)} \cap \{a, -a\}\right| + \sum_{b'\in Z_d} (i+b', i+b')_d\right] / q\\
&= \max_{a\neq 0}\left[\left|D_0^{(d,q)} \cap \{a, -a\}\right| + \sum_{b'\in Z_d} (b', b')_d\right] / q\\
&= \max_{a\neq 0}\left[\left|D_0^{(d,q)} \cap \{a, -a\}\right| + l - 1\right] / q\\
&= \begin{cases} \frac{l+1}{q} & \text{for } \frac{dl}{2} \pmod d = 0,\\ \frac{l}{q} & \text{otherwise.} \end{cases}
\end{aligned}
$$

Case 2: $b \bmod d \neq 0$, by Lemmas 5 and 7 in the Appendix A,

$$
\begin{aligned}
P_{d_1} = \max_{a\neq 0, b}\Big[&\left|\left(C_0^{(d,q)} + a\right) \cap C_b^{(d,q)}\right| + \left|\left(C_{-b}^{(d,q)} + a\right) \cap C_0^{(d,q)}\right|\\
&+ \sum_{b'\in Z_d\setminus\{0,-b\}} \left|\left(C_{b'}^{(d,q)} + a\right) \cap C_{b+b'}^{(d,q)}\right|\Big] / q
\end{aligned}
$$

$$\begin{aligned}&= \max_{a\neq 0,b}\Big[(i,i+b)_d+\Big|D_b^{(d,q)}\cap\{a\}\Big|+(i-b,i)_d+\Big|D_{-b}^{(d,q)}\cap\{-a\}\Big|\\ &\quad+\sum_{b'\in Z_d\backslash\{0,-b\}}(i+b',i+b+b')_d\Big]/q\\ &= \max_{a\neq 0,b}\left[\Big|D_b^{(d,q)}\cap\{a\}\Big|+\Big|D_{-b}^{(d,q)}\cap\{-a\}\Big|+\sum_{b'\in Z_d}(i+b',i+b+b')_d\right]/q\\ &= \max_{a\neq 0,b}\left[\Big|D_b^{(d,q)}\cap\{a\}\Big|+\Big|D_{-b}^{(d,q)}\cap\{-a\}\Big|+\sum_{b'\in Z_d}(b',b+b')_d\right]/q\\ &= \max_{a\neq 0,b}\Big[\Big|D_b^{(d,q)}\cap\{a\}\Big|+\Big|D_{-b}^{(d,q)}\cap\{-a\}\Big|+l\Big]/q.\end{aligned}$$

To maximize $|D_b^{(d,q)}\cap\{a\}|+|D_{-b}^{(d,q)}\cap\{-a\}|$, without loss of generality, assume $a\in D_b^{(d,q)}$. $-1\in D_{\frac{q-1}{2}}^{(d,q)}$ and so $-a\in D_{b+\frac{q-1}{2}}^{(d,q)}$. For $-a\in D_{-b}^{(d,q)}$, we consider the equation

$$-b\equiv b+\frac{q-1}{2}\pmod d$$

which is equivalent to

$$2b\equiv\frac{dl}{2}\pmod d.$$

We now check whether this equation has a solution.

Case 1: l even and d even. In this case $b=d/2$ is a solution.
Case 2: l even and d odd. In this case there is no solution.
Case 3: l odd and $d\equiv 0$ mod 4 . In this case $b=d/4$ is a solution.
Case 4: l odd and $d\equiv 2$ mod 4 . In this case there is no solution.

Note that $q-1=dl$, and the two cases d odd and l odd cannot happen at the same time. Thus

$$P_{d_1}=\begin{cases}\frac{l+2}{q} & l \text{ even and } d \text{ even}\\ & \text{or } l \text{ odd and } d\equiv 0\pmod 4,\\ \frac{l+1}{q} & \text{otherwise.}\end{cases}$$

All the values of P_{d_1} in Case 2 are greater than or equal to the values of P_{d_1} in Case 1. By substituting $q=dl+1$, the theorem is proved. □

3.1. *Comparison with another class of codes described in* [6]

There are authentication codes with parameters [6]

$$|S|=r^m,\quad |E|=r^{m+n}=|S||T|,\quad T=r^n \tag{11}$$

and

$$P_{d_0} = P_{d_1} = \frac{1}{r^n}.$$

These codes are usually constructed by using linear functions in a natural way. For these codes we have $\gcd(|S|, |T|) = r^{\min(m,n)} \neq 1$. However, for the codes of Theorem 4 we have

$$\gcd(|S|, |T|) = 1, \tag{12}$$

and the corresponding P_{d_1} is slightly bigger than $\frac{1}{|T|}$. Under the condition of (12), it may be proved that no code with $P_{d_0} = P_{d_1} = \frac{1}{r^n}$ exists, because orthogonal arrays with corresponding parameters may not exist. Hence the parameters of (11) are of different types compared with those in Theorem 4. On the other hand, the code construction in Theorem 4 uses the logarithm function.

3.2. Comparison with Bierbrauer's codes

We now compare the codes of Theorem 4 with Bierbrauer's codes [1]. Bierbrauer employed the composition method to geometry codes and obtained an authentication code with the following parameters:

$$|S| = r^{s(1+r^{s-t})}, \quad |E| = r^{2s+t}, \quad |T| = r^t \tag{13}$$

and

$$P_{d_0} = \frac{1}{r^t}, \quad P_{d_1} = \frac{2}{r^t}, \tag{14}$$

where r is a power of a prime p, and $s \geqslant t$ are natural numbers.

In order for the codes to be comparable to the codes of Theorem 4 we set $s = t$. Then (13) and (14) become

$$|S| = q^{2t}, \quad |E| = q^{3t}, \quad |T| = q^t \tag{15}$$

and

$$\begin{aligned} P_{d_0} &= \frac{1}{q^t} = \frac{1}{|T|}, \\ P_{d_1} &= \frac{2}{q^t} = \frac{1}{|T|} + \frac{1}{\sqrt{|S|}}. \end{aligned} \tag{16}$$

In this case we have $|E| = |S||T|$.

For the code of Theorem 4, we have also $|E| = |S||T|$ and $P_{d_0} = \frac{1}{|T|}$. But the success probability of the substitution attack on the code of Theorem 4 is

$$P_{d_1} \leqslant \frac{l+2}{q} < \frac{1}{d} + \frac{2}{q} = \frac{1}{|T|} + \frac{1}{|S|/2}.$$

Thus in the case that $|S| > 2|T|$, the code of Theorem 4 is better than the subclass of codes of [1] in the special case $s = t$. Note that the codes of Theorem 4 are comparable with only this subclass of Bierbrauer's codes due to restrictions on the code parameters.

4. Conclusions

In this paper within the framework of Chanson, Ding and Salomaa [2], we presented two classes of systematic authentication codes using the theory of cyclotomy and the logarithm function. In all the cases that the codes are comparable, our codes are better than Helleseth–Johansson's codes and also Bierbrauer's codes. With the known relations between universal hash families and authentication codes [13,14], the authentication codes described in this paper may be used to construct universal hash families.

The parameters of the authentication codes described in Theorem 2 are flexible in that d could be any proper divisor of $q-1$. However, d must be chosen carefully in order to get good authentication codes. For example, if $q = p^{2s}$ and $d = p^s + 1$, the code is bad in the sense that P_{d_1} is quite large. Thus the codes of Theorem 2 contain both good and bad codes.

A class of very good authentication codes based on algebraic curves were constructed by Xing, Wang and Lam [13]. Unfortunately the codes described in this paper cannot be compared with the Xing–Wang–Lam codes because their parameters are not comparable.

Acknowledgments

The authors thank both referees for their constructive comments and suggestions that greatly improved this paper.

Appendix A. Several auxiliary results

Recall that $q-1 = dl$ and that $D_i^{(d,q)}$ are the cyclotomic classes of order d. Also recall the definition of $C_i^{(d,q)}$ in (2). The following lemma is useful in the proof of Theorem 2.

Lemma 5. *Let $a \neq 0$, where $a^{-1} \in D_i^{(d,q)}$, $t \not\equiv 0 \pmod{d}$ and $t' \not\equiv 0 \pmod{d}$. Then*

$$\begin{aligned}
\left|\left(C_0^{(d,q)}+a\right)\cap C_0^{(d,q)}\right| &= (i,i)_d + \left|D_0^{(d,q)}\cap\{a,-a\}\right|,\\
\left|\left(C_0^{(d,q)}+a\right)\cap C_t^{(d,q)}\right| &= (i,i+t)_d + \left|D_t^{(d,q)}\cap\{a\}\right|,\\
\left|\left(C_t^{(d,q)}+a\right)\cap C_0^{(d,q)}\right| &= (i+t,i)_d + \left|D_t^{(d,q)}\cap\{-a\}\right|,\\
\left|\left(C_t^{(d,q)}+a\right)\cap C_{t'}^{(d,q)}\right| &= (i+t,i+t')_d.
\end{aligned}$$

Proof.

$$\begin{aligned}
\left|\left(C_0^{(d,q)}+a\right)\cap C_0^{(d,q)}\right| &= \left|\left(D_0^{(d,q)}\cup\{0\}+a\right)\cap\left(D_0^{(d,q)}\cup\{0\}\right)\right|\\
&= \left|\left(D_0^{(d,q)}+a\right)\cap D_0^{(d,q)}\right| + \left|D_0^{(d,q)}\cap\{a,-a\}\right|\\
&= \left|\left(a^{-1}D_0^{(d,q)}+1\right)\cap a^{-1}D_0^{(d,q)}\right| + \left|D_0^{(d,q)}\cap\{a,-a\}\right|\\
&= (i,i)_d + \left|D_0^{(d,q)}\cap\{a,-a\}\right|.
\end{aligned}$$

The remaining parts are proved similarly. □

The *Gaussian periods* η_i of order d, $i = 0, 1, \ldots, d-1$, are defined as follows:

$$\eta_i = \sum_{c \in D_i^{(d,q)}} \xi^c,$$

where ξ is a complex qth root of unity.

The following results are well known, but we include a proof for the sake of completeness. To simplify the notations, we use (i, j) to denote $(i, j)_d$, which is the cyclotomic number of order d.

Lemma 6. *For cyclotomic numbers and Gaussian periods of order* d, *we have the following*:

(A) $\sum_{i=0}^{d-1} \eta_i = -1$.

(B) $\eta_i \eta_{i+k} = \sum_{h=0}^{d-1}(k, h)\eta_{i+h} + l\theta_k$, *where*

$$\theta_k = \begin{cases} 1 & \textit{if } l \textit{ is even and } k = 0, \textit{ or } l \textit{ is odd and } k = d/2, \\ 0 & \textit{otherwise.} \end{cases}$$

(C) $\sum_{h=0}^{d-1}(k, h) = l - \theta_k$.

(D) $q(k, h) = \begin{cases} l^2 + \sum_{i=0}^{d-1} \eta_i \eta_{i+k} \eta_{i+h} & \textit{if } l \textit{ is even}, \\ l^2 + \sum_{i=0}^{d-1} \eta_i \eta_{i+k} \eta_{i+h+d/2} & \textit{if } l \textit{ is odd}. \end{cases}$

Proof. (A) By definition,

$$\sum_{i=0}^{d-1} \eta_i = \sum_{i=0}^{d-1} \sum_{c \in D_i^{(d,q)}} \xi^c = \sum_{c \in Z_q^*} \xi^c = -1$$

(B) By definition,

$$\begin{aligned} \eta_i \eta_{i+k} &= \sum_{c \in D_i^{(d,q)}} \sum_{u \in D_{i+k}^{(d,q)}} \omega^{c+u} \\ &= \sum_{c \in D_i^{(d,q)}} \sum_{u \in D_{i+k}^{(d,q)}} \omega^{c[1+uc^{-1}]} \\ &= \sum_{h=0}^{d-1} (k, h)\eta_{i+h} + l\theta_k, \end{aligned}$$

where θ_k is 1 if $-1 \in D_k^{(d,q)}$ and 0 otherwise, implying the condition on θ_k as defined above.

(C) The expression $\sum_{h=0}^{d-1}(k, h)$ equals the number of times an element in $D_k^{(d,q)}$ is followed by an element in some $D_h^{(d,q)}$. Since $D_k^{(d,q)}$ contains l elements and the only element not in any $D_h^{(d,q)}$ is 0, it follows that the sum equals l except when -1 is in $D_k^{(d,q)}$, in which case the sum equals $l - 1$.

(D) Let $h^* = h$ if l is even and $h^* = h + d/2$ if l is odd. Then, from (A), (B) and (C), we obtain

$$\begin{aligned}
\sum_{i=0}^{d-1} \eta_i \eta_{i+k} \eta_{i+h^*} &= \sum_{i=0}^{d-1} \left(\sum_{a=0}^{d-1} (k,a)\eta_{i+a} + l\theta_k \right) \eta_{i+h^*} \\
&= \sum_{a=0}^{d-1} (k,a) \sum_{i=0}^{d-1} \eta_{i+a}\eta_{i+h^*} - l\theta_k \\
&= \sum_{a=0}^{d-1} (k,a) \sum_{u=0}^{d-1} \eta_u \eta_{u+h^*-a} - l\theta_k \\
&= \sum_{a=0}^{d-1} (k,a) \sum_{u=0}^{d-1} \left(\sum_{b=0}^{d-1} (h^*-a,b)\eta_{u+b} + l\theta_{h^*-a} \right) - l\theta_k \\
&= \sum_{a=0}^{d-1} (k,a) \left(\sum_{b=0}^{d-1} (h^*-a,b)(-1) + dl\theta_{h^*-a} \right) - l\theta_k \\
&= \sum_{a=0}^{d-1} (k,a) \left((l-\theta_{h^*-a})(-1) + dl\theta_{h^*-a} \right) - l\theta_k \\
&= \sum_{a=0}^{d-1} (k,a)((dl+1)\theta_{h^*-a} - l) - l\theta_k \\
&= q \sum_{a=0}^{d-1} (k,a)\theta_{h^*-a} - (l-\theta_k)l - l\theta_k \\
&= -l^2 + q \sum_{a=0}^{d-1} (k,a)\theta_{h^*-a} \\
&= -l^2 + q(k,h)
\end{aligned}$$

which completes the proof. □

The next lemma gives a very nice and perhaps surprising formula for the summations $\sum_{u=0}^{d-1}(u, u+k)$, which turn out to be independent of the individual cyclotomic numbers. It plays an important role in proving Theorem 4.

Lemma 7. *Let $q - 1 = dl$ and let q be an odd prime. Then*

$$\sum_{u=0}^{d-1} (u, u+k) = \begin{cases} l-1 & \text{if } k = 0, \\ l & \text{if } k \neq 0. \end{cases}$$

Proof. Let $k^* = k$ if l is even and $k^* = k + d/2$ if l is odd. By definition, and the previous lemmas, it follows that:

$$\begin{aligned}
q\sum_{u=0}^{d-1}(u, u+k) &= l^2 d + \sum_{u=0}^{d-1}\sum_{i=0}^{d-1}\eta_i\eta_{i+u}\eta_{i+u+k^*}\\
&= (q-1)l + \sum_{i=0}^{d-1}\eta_i\sum_{u=0}^{d-1}\eta_{i+u}\eta_{i+u+k^*}\\
&= (q-1)l + \sum_{i=0}^{d-1}\eta_i\sum_{t=0}^{d-1}\eta_t\eta_{t+k^*}\\
&= (q-1)l + \sum_{i=0}^{d-1}\eta_i\sum_{t=0}^{d-1}\left(\sum_{h=0}^{d-1}(k^*, h)\eta_{t+h} + l\theta_{k^*}\right)\\
&= (q-1)l + \sum_{i=0}^{d-1}\eta_i\sum_{h=0}^{d-1}(k^*, h)\sum_{t=0}^{d-1}\eta_{t+h} - dl\theta_{k^*}\\
&= (q-1)l + (-1)\sum_{h=0}^{d-1}(k^*, h)(-1) - (q-1)\theta_{k^*}\\
&= (q-1)l + (l-\theta_{k^*}) - (q-1)\theta_{k^*}\\
&= q(l-\theta_{k^*}).
\end{aligned}$$

Dividing both sides by q and using the definition of θ_{k^*} prove this lemma. □

References

[1] J. Bierbrauer, Universal hashing and geometric codes, Designs, Codes, and Cryptography 11 (1997) 207–221.

[2] S. Chanson, C. Ding, A. Salomaa, Cartesian authentication codes from functions with optimal nonlinearity, Theoretical Computer Science 290 (2003) 1737–1752.

[3] T.W. Cusick, C. Ding, A. Renvall, in: Stream Ciphers and Number Theory, North-Holland Mathematical Library, vol. 55, North-Holland/Elsevier, Amsterdam, 1998.

[4] Y. Desmedt, Y. Frankel, M. Yung, Multi-sender network security: efficient authenticated multicast/feedback, in: Proceedings of IEEE Infocom ’92, 1992, pp. 1045–2054.

[5] E.N. Gilbert, F.J. MacWilliams, N.J.A. Sloane, Codes which detect deception, Bell System Techn. Journal 53 (1974) 405–424.

[6] T. Helleseth, T. Johansson, Universal hash functions from exponential sums over finite fields and Galois rings, in: Advances in Cryptology – Crypto’ 96, Lecture Notes in Computer Science, vol. 1109, Springer, New York, 1997.

[7] K. Kurosawa, S. Obana, Characterization of (k, n) multi-receiver authentication, in: Information Security and Privacy: Proceedings of ACISP’ 97, Lecture Notes in Computer Science, vol. 1270, Springer, New York, 1997, pp. 204–215.

[8] R.S. Rees, D.R. Stinson, Combinatorial characterizations of authentication codes II, Design, Codes, and Cryptography 7 (1996) 239–259.

[9] R. Safavi-Naini, H. Wang, New results on multi-receiver authentication codes, in: Advances in Cryptology: Proceedings of Eurocrypt’ 98, Lecture Notes in Computer Science, vol. 1403, Springer, New York, 1998, pp. 527–541.

[10] R. Safavi-Naini, H. Wang, Multi-receiver authentication codes: models, bounds, constructions, and extensions, Information and Computation 151 (1999) 148–172.

[11] G.J. Simmons, Authentication theory/coding theor, in: Advances in Cryptology: Proceedings of Crypto' 84, Lecture Notes in Computer Science, vol. 196, Springer, New York, 1985, pp. 411–432.

[12] D.R. Stinson, Combinatorial characterizations of authentication codes, Designs, Codes, and Cryptography 2 (1992) 175–187.

[13] C. Xing, H. Wang, K.Y. Lam, Construction of authentication codes from algebraic curves over finite fields, IEEE Transactions on Information Theory 46 (2000) 886–892.

[14] M.N. Wegman, J.L. Carter, New hash functions and their use in authentication and set equality, Journal of Computer and System Sciences 22 (1981) 265–279.