A Generic Construction of Cartesian Authentication Codes

Cunsheng Ding, *Senior Member, IEEE*, Tor Helleseth, *Fellow, IEEE*, Torleiv Kløve, *Fellow, IEEE*, and Xuesong Wang

***Abstract*—In this paper, a coding-theory construction of Cartesian authentication codes is presented. The construction is a generalization of some known constructions. Within the framework of this generic construction, several classes of authentication codes using certain classes of error-correcting codes are described. The authentication codes presented in this paper are better than known ones with comparable parameters. It is demonstrated that the construction is related to certain combinatorial designs, such as difference matrices and generalized Hadamard matrices.**

***Index Terms*—Authentication codes, coding theory, cryptography.**

I. Introduction

A CARTESIAN authentication code or systematic authentication code is a four-tuple $(\mathcal{S}, \mathcal{T}, \mathcal{K}, \{E_k : k \in \mathcal{K}\})$, where $\mathcal{S}$ is the source state space associated with a probability distribution, $\mathcal{T}$ is the *tag space*, $\mathcal{K}$ is the *key space* associated with a probability distribution, and $E_k : \mathcal{S} \to \mathcal{T}$ is called an *encoding rule*. A transmitter and a receiver share a key k for authentication purpose. If the transmitter wants to send a source state s to the receiver, he computes $t = E_k(s)$ and sends the message $m = (s, t)$ to the receiver through a public communication channel. When receiving $m' = (s', t')$, the receiver will compute $E_k(s')$ and checks whether $t' = E_k(s')$. If it does, the receiver will accept it as authentic. Otherwise, the receiver will reject it.

In the authentication model introduced by Simmons [14], in addition to a transmitter and a receiver, an opponent is also involved. Within this authentication model, we assume that the opponent can insert his message into the channel, and can substitute an observed message m with another message m'. We consider two kinds of attacks, the *impersonation* and *substitution* attacks. In the impersonation attack, an opponent inserts his message into the channel and wishes to make the receiver accept it as authentic. In a substitution attack, the opponent observed a message sent by the transmitter and replaces it with his message $m' \neq m$, hoping that the receiver accepts it as authentic. We use P_I and P_S to denote the maximum success probabilities with respect to the two attacks.

Combinatorial designs have been successfully used to construct certain optimal authentication codes [13], [15]. Certain algebraic curves give also very good authentication codes [3], [18], [20].

In this paper, we present a coding theory construction of Cartesian authentication codes. Our construction is a generalization of some known ones. Within this general framework, we construct several classes of authentication codes using certain classes of error-correcting codes. Our authentication codes are better than known ones with comparable parameters. We also show that our construction is related to certain combinatorial designs, such as difference matrices and generalized Hadamard matrices.

The generic construction presented in this paper is promising for several reasons. First, both linear and nonlinear error correcting codes can be used in the general framework. Second, it contains the constructions of good authentication codes in [6], [9], [20] as special cases. Third, by using certain classes of linear error codes, it gives new authentication codes that are better than the existing authentication codes with comparable parameters, as demonstrated in this paper.

II. A General Construction of Systematic Authentication Codes With Error-Correcting Codes

We use $\mathcal{S}$, $\mathcal{K}$, $\mathcal{T}$, and $\mathcal{E}$ to denote the source state space, key space, tag space, and encoding rule space, respectively. Throughout this paper, we assume that the key space and source state space have a uniform probability distribution. We shall also define our encoding rules such that $k \mapsto E_k$ is a one-to-one correspondence between the key space and encoding rule space. Hence, the encoding rule space has also a uniform probability distribution.

Let $\mathcal{C}$ be an (n, M) code over an alphabet B, i.e., $\mathcal{C}$ is a subset of B^n with size M, where $(B, +)$ is an Abelian group with q elements. We use $\boldsymbol{c}_i = (c_{i,0}, \ldots, c_{i,n-1})$ to denote a codeword of $\mathcal{C}$, $0 \leq i \leq M-1$. We define a Cartesian authentication code by

$$(\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{E}) = (\boldsymbol{Z}_M, B, \boldsymbol{Z}_n \times B, \{E_k : k \in \mathcal{K}\}) \quad (1)$$

where for any $k = (k_1, k_2) \in \mathcal{K}$ and $s \in \mathcal{S}$, $E_k(s) = c_{s,k_1} + k_2$.

This construction is very general, and contains several known constructions as special cases. We shall distinguish between the linear and nonlinear cases in the sequel.

Manuscript received August 1, 2006; revised January 30, 2007. The work of C. Ding was supported by the Research Grants Council of the Hong Kong Special Administration Region, China (Project 610425). The work of T. Helleseth and T. Kløve was supported by the Norwegian Research Council.

C. Ding and X. Wang are with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China (e-mail: cding,cswxs@cs.ust.hk; xswang@microsoft.com).

T. Helleseth and T. Kløve are with the Department of Informatics, University of Bergen, N-5020 Bergen, Norway (e-mail: torh@ii.uib.no; torleiv@ii.uib.no).

Communicated by A. Canteaut, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2007.896872

III. Constructions Using Linear Codes

In this section, we consider the special case that the code $\mathcal{C}$ used in the construction of (1) is linear. We present several classes of specific constructions of authentication codes based on several types of linear error-correcting codes, and show that our authentication codes are better than some existing ones.

A. The Case of Using Linear Codes

Let $\mathcal{C}$ be an $[n, \kappa, d]$ linear code over GF(q). Define $(B, +) =$ (GF(q), $+$). Then $M = q^\kappa$, and the authentication code of (1) becomes

$$(\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{E}) = (\boldsymbol{Z}_{q^\kappa}, \mathrm{GF}(q), \boldsymbol{Z}_n \times \mathrm{GF}(q), \{E_k : k \in \mathcal{K}\}) \tag{2}$$

where for any $k = (k_1, k_2) \in \mathcal{K}$ and $s \in \mathcal{S}$, $E_k(s) = c_{s,k_1} + k_2$.

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

$$P_I = \frac{1}{q} \text{ and } P_S = \max_{0 \neq \boldsymbol{c} \in \mathcal{C}} \max_{u \in \mathrm{GF}(q)} \frac{N(\boldsymbol{c}, u)}{n} \geq 1 - \frac{d}{n}$$

where $N(\boldsymbol{c}, u)$ denotes the number of times u occurs in the codeword $\boldsymbol{c}$. Furthermore

$$|\mathcal{S}| = q^\kappa, \quad |\mathcal{T}| = q, \quad |\mathcal{K}| = nq.$$

Proof: In the impersonation attack, the opponent wants to generate a message $m = (s, t)$ by choosing a source state s and a $k = (k_1, k_2) \in \mathcal{K}$ and computing $t = c_{s,k_1} + k_2$. The k_1 and k_2 are independent, and the opponent has no information about the key k. This is the same as selecting the pair (s, t) randomly. The message m is then inserted into the channel. This attack is successful if and only if $t = c_{s,k_1} + k_2$. Note that the keys and source states are equiprobable. We have

$$P_I = \max_{s,t} \frac{|\{k \in \mathcal{K} : t = c_{s,k_1} + k_2\}|}{|\{k \in \mathcal{K}\}|} = \frac{1}{q}.$$

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

$$P_S = \max_{s,s' \in \mathcal{S}, t, t' \in \mathcal{T}, s' \neq s} \frac{\left|\left\{k \in \mathcal{K} : t = c_{s,k_1} + k_2, t' = c_{s',k_1} + k_2\right\}\right|}{|\{k \in \mathcal{K} : t = c_{s,k_1} + k_2\}|}.$$

Note that $|\{k \in \mathcal{K} : t = c_{s,k_1} + k_2\}| = n$ for any fixed pair (s, t). On the other hand, the difference of any two distinct codewords is again a nonzero codeword. Therefore

$$\begin{aligned} &|\{k \in \mathcal{K} : t = c_{s,k_1} + k_2, t' = c_{s',k_1} + k_2\}| \\ &\quad = |\{k \in \mathcal{K} : t = c_{s,k_1} + k_2, t - t' = c_{s,k_1} - c_{s',k_1}\}| \\ &\quad = |\{k_1 \in \boldsymbol{Z}_n : t - t' = c_{s,k_1} - c_{s',k_1}\}| \\ &\quad = \text{the number of times } t - t' \text{ occurs in } \boldsymbol{c}_s - \boldsymbol{c}_{s'}. \end{aligned}$$

Note that t' is freely chosen and $s' \neq s$ is also freely chosen. Hence

$$\begin{aligned} P_S &= \max_{s \in \mathcal{S}, t \in \mathcal{T}} \max_{s' \neq s, t'} \frac{\left|\left\{k \in \mathcal{K} : \begin{matrix} t = c_{s,k_1} + k_2, \\ t' = c_{s',k_1} + k_2 \end{matrix}\right\}\right|}{n} \\ &= \max_{0 \neq \boldsymbol{c} \in \mathcal{C}} \max_{u \in \mathrm{GF}(q)} \frac{N(\boldsymbol{c}, u)}{n} \geq \max_{0 \neq \boldsymbol{c} \in \mathcal{C}} \frac{N(\boldsymbol{c}, 0)}{n} = 1 - \frac{d}{n}. \quad \square \end{aligned}$$

Our construction requires that in every nonzero codeword of the linear error-correcting code all the elements of the base field occur more or less equally often. Thus, large minimum distance does not give any good upper bound on P_S. However, it is necessary that the linear code has good minimum distance because $P_S \geq 1 - \frac{d}{n}$.

B. Authentication Codes From Irreducible Cyclic Codes

In this subection, we construct Cartesian authentication codes using irreducible cyclic codes. To this end, we need information about the structure of the codewords in an irreducible cyclic code. 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 α be a primitive element of GF(q), and let $\theta = \alpha^N$. For any $\beta \in$ GF(q), we define a vector

$$c(\beta) = (\mathrm{Tr}_{q/p}(\beta), \mathrm{Tr}_{q/p}(\beta\theta), \ldots, \mathrm{Tr}_{q/p}(\beta\theta^{n-1}))$$

where $\mathrm{Tr}_{q/p}$ is the trace function of GF(q)/GF(p). The set

$$C = \{c(\beta) : \beta \in \mathrm{GF}(q)\}$$

is called an *irreducible cyclic* $[n, m]$ code over GF(p).

Lemma 2: [2] Let C be the irreducible cyclic code with $N =$ 2. the distribution of elements from GF(p) in each nonzero codeword $c(\beta)$ is given as follows. For m even

$$\begin{aligned} N_0 &= \frac{q-1}{2p} + \frac{(1-p)(1 \pm \sqrt{q})}{2p} \\ N_i &= \frac{q-1}{2p} + \frac{1 \pm \sqrt{q}}{2p}, \qquad i = 1, \ldots, p-1 \end{aligned}$$

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

For m odd, one distribution is

$$\begin{aligned} N_0 &= \frac{q-1}{2p} + \frac{1-p}{2p} \\ N_a &= \frac{q-1}{2p} + \frac{1+\sqrt{pq}}{2p}, \ a \text{ nonzero square of GF}(p) \\ N_b &= \frac{q-1}{2p} + \frac{1-\sqrt{pq}}{2p}, \ b \text{ nonzero nonsquare of GF}(p) \end{aligned}$$

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

Theorem 3: Let $\mathcal{C}$ be the irreducible cyclic code with $N = 2$. Then for the authentication code of (2), we have

$$P_I = \frac{1}{p} \quad \text{and} \quad P_S = \begin{cases} \frac{1}{p} + \frac{p-1}{p(p^{m/2}+1)}, & \text{if } m \text{ is even} \\ \frac{1}{p} + \frac{1}{p^{m/2}-1}, & \text{if } m \text{ is odd.} \end{cases}$$

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

Proof: By Theorem 1, $P_I = \frac{1}{p}$. The conclusion on P_S follows from Lemma 2 and Theorem 1. □

We now compare a subclass of the codes of Theorem 3 with a subclass of codes in [3] with the following parameters:

$$|\mathcal{S}| = r^{s(1+r^{s-t})}, \quad |\mathcal{E}| = r^{2s+t}, \quad |\mathcal{T}| = r^t, \\ P_I = \frac{1}{r^t}, \quad P_S = \frac{2}{r^t} \tag{3}$$

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

In order for this subclass of codes to be comparable to the codes of Theorem 3, we set $s = t$ and $r = p$. Then (3) becomes

$$|\mathcal{S}| = p^{2t}, \quad |\mathcal{T}| = \sqrt{|\mathcal{S}|}, \quad |\mathcal{E}| = |\mathcal{S}||\mathcal{T}| = |\mathcal{M}|, \\ P_I = \frac{1}{|\mathcal{T}|}, \quad P_S = \frac{2}{|\mathcal{T}|} = \frac{2}{\sqrt{|\mathcal{S}|}}.$$

For the code of Theorem 3, we consider the case $m = 2$. For this subclass of codes, we have

$$|\mathcal{S}| = p^2, \quad |\mathcal{T}| = \sqrt{|\mathcal{S}|}, \quad |\mathcal{E}| = (|\mathcal{S}| - 1)|\mathcal{T}|/2 < |\mathcal{M}|/2, \\ P_I = \frac{1}{|\mathcal{T}|}, \quad P_S = \frac{2}{|\mathcal{T}| + 1} = \frac{2}{\sqrt{|\mathcal{S}|} + 1}.$$

In this case, we have $|\mathcal{E}| < |\mathcal{M}|/2$. Hence, in our subclass of codes, the number of keys is less than half of the size of the message space, while in the subclass of Bierbrauer's codes, the number of keys is the same as that of messages. On the other hand, the P_S for our codes is smaller than that for the subclass of Bierbrauer's codes. Therefore, our subclass of codes is better than the subclass of Bierbrauer's codes.

Lemma 4: [2] Let $\mathcal{C}$ be an $[n, m]$ irreducible cyclic code over GF(p) with $Nn = p^m - 1 = q - 1$, $N > 2$. If there exists a divisor j of $m/2$ for which $p^j \equiv -1 (\mathrm{mod} N)$, then there are only two distributions of elements from GF(p) which occur in the nonzero codewords of $\mathcal{C}$:

Class s (containing n codewords)

$$\begin{cases} N_0 = \frac{q-1}{Np} + \frac{1-p+u(1-p)(N-1)\sqrt{q}}{Np} \\ N_i = \frac{q-1}{Np} + \frac{1+u(N-1)\sqrt{q}}{Np}, \qquad i = 1, \ldots, p-1. \end{cases}$$

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

$$\begin{cases} N_0 = \frac{q-1}{Np} + \frac{1-p-u(1-p)\sqrt{q}}{Np} \\ N_i = \frac{q-1}{Np} + \frac{1+u\sqrt{q}}{Np}, \qquad i = 1, \ldots, p-1. \end{cases}$$

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.

The following lemma follows from Lemma 4.

Lemma 5: As for the constant u in Lemma 4, we have $u = 1$ if $(p^m - p)/(p-1)p^{m/2} \leq N - 1 \leq p^{m/2}$, and $u = -1$ if $N - 1 < (p^m - p)/(p-1)p^{m/2}$.

However, the semiprimitive condition implies that $N - 1 \leq p^{m/4}$. Note that

$$\frac{p^{m/2} - 1}{p - 1} < \frac{p^m - p}{(p-1)p^{m/2}} < \frac{p^{m/2} - 1}{p - 1} + 1.$$

Under the condition $N - 1 \leq p^{m/4}$, $u = -1$.

Theorem 6: Let $\mathcal{C}$ be the irreducible cyclic code with $N - 1 \leq p^{m/4}$. Then for the code of (2)

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

Furthermore, $|\mathcal{S}| = p^m$, $|\mathcal{T}| = p$, $|\mathcal{K}| = (p^m - 1)p/N$.

Proof: By Theorem 1, $P_I = \frac{1}{p}$. By Lemma 5 and the discussion following it, we know that the constant $u = -1$. Thus, all the constants N_i of Lemma 4 are determined. Hence

$$\max_{\substack{0 \neq \boldsymbol{c} \in \mathcal{C} \\ u \in \mathrm{GF}(p)}} N(\boldsymbol{c}, u) = \frac{q-1}{Np} + \frac{1 - p + (p-1)(N-1)\sqrt{q}}{Np}.$$

The conclusion on P_S then follows from Theorem 1. □

C. Authentication Codes From the Second Class of Linear Codes

Let p be an odd prime, and let α be a generating element of GF(q^m). For any $a, b \in$ GF(p^m), define

$$\boldsymbol{c}_{a,b} = \left(f_{a,b}(0), f_{a,b}(1), f_{a,b}(\alpha), \ldots, f_{a,b}(\alpha^{p^m - 2}) \right),$$

where $f_{a,b}(x) = \mathrm{Tr}_{p^m/p}(ax + bx^2)$.

We then define a $[p^m, 2m]$ linear code $\mathcal{C}$ over GF(p) as

$$\mathcal{C} = \{ \boldsymbol{c}_{a,b} : a, b \in \mathrm{GF}(p^m) \}. \tag{4}$$

The following theorem is a special case of a more general result in [21].

Theorem 7: If m is even, the code $\mathcal{C}$ of (4) has parameters $[p^m, 2m, d = (p-1)p^{m-1} - (p-1)p^{m/2-1}]$ and has the following five nonzero weights:

$$(p-1)(p^{m-1} \pm p^{\frac{m}{2}-1}), (p-1)p^{m-1} \pm p^{\frac{m}{2}-1}, (p-1)p^{m-1}.$$

If m is odd, the code $\mathcal{C}$ of (4) has parameters $[p^m, 2m, d = (p-1)p^{m-1} - p^{(m-1)/2}]$ and has the following three nonzero weights: $(p-1)p^{m-1} \pm p^{(m-1)/2}$, $(p-1)p^{m-1}$.

Theorem 8: Let $\mathcal{C}$ be the code of (4). Then for the authentication code of (2), we have

$$P_I = \frac{1}{p} \quad \text{and} \quad P_S = \begin{cases} \frac{1}{p} + \frac{p-1}{p^{m/2+1}}, & \text{if } m \text{ even}, \\ \frac{1}{p} + \frac{1}{p^{(m+1)/2}}, & \text{if } m \text{ odd}. \end{cases}$$

Furthermore, we have $|\mathcal{S}| = p^{2m}$, $|\mathcal{T}| = p$, $|\mathcal{K}| = p^{m+1}$.

Proof: By Theorem 1, $P_I = \frac{1}{p}$. By Theorem 7 and its proof, we have

$$\max_{0\neq \boldsymbol{c}\in\mathcal{C}} \max_{u\in \mathrm{GF}(p)} N(\boldsymbol{c},u) = \begin{cases} p^{m-1}+(p-1)p^{m/2-1}, & \text{if } m \text{ even} \\ p^{m-1}+p^{(m-1)/2}, & \text{if } m \text{ odd.} \end{cases}$$

The conclusion on P_S then follows from Theorem 1. □

In [9], authentication codes with parameters

$$|\mathcal{S}| = q^{m(D-\lfloor D/p \rfloor)}, \quad |\mathcal{K}| = q^{m+1}, \quad |\mathcal{T}| = q, \quad P_I = \frac{1}{q}, \quad P_S = \frac{1}{q} + \frac{D-1}{\sqrt{q^m}}$$

are constructed using exponential sums, where D is an integer with $1 \leq D \leq \sqrt{q^m}$ and p is the characteristic of the finite field $\mathrm{GF}(q^m)$. When $D = 1$, the codes are optimal and are constructed using linear functions.

We now consider these codes for the case $q = p$ being odd and $D = 2$ with our authentication codes of Theorem 8. In this case, if $p = q > 2$, the subclass of codes in [9] has the parameters

$$|\mathcal{S}| = p^{2m}, \quad |\mathcal{K}| = p^{m+1} = \sqrt{|\mathcal{S}||\mathcal{T}|}, \quad |\mathcal{T}| = p, \quad P_I = \frac{1}{|\mathcal{T}|}, \quad P_S = \frac{1}{|\mathcal{T}|} + \frac{1}{|\mathcal{S}|^{1/4}}.$$

Our codes of Theorem 8 have parameters

$$|\mathcal{S}| = p^{2m}, \quad |\mathcal{K}| = p^m p = \sqrt{|\mathcal{S}||\mathcal{T}|}, \quad |\mathcal{T}| = p, \quad P_I = \frac{1}{|\mathcal{T}|}, \quad P_S = \begin{cases} \frac{1}{|\mathcal{T}|} + \frac{|\mathcal{T}|-1}{|\mathcal{T}|}\frac{1}{|\mathcal{S}|^{1/4}}, & m \text{ even} \\ \frac{1}{|\mathcal{T}|} + \frac{1}{|\mathcal{T}|}\frac{1}{|\mathcal{S}|^{1/4}}, & m \text{ odd.} \end{cases}$$

So the P_S of our codes of Theorem 8 is smaller. Thus, our codes of Theorem 8 are better in the case $D = 2$ and $p = q > 2$. Note that our authentication codes exist only for $p \neq 2$.

Hence, our authentication codes are better than the subclass of codes defined by $D = 2$ in [9]. If $D \neq 2$, the authentication codes in [9] cannot be compared with our codes, because the parameters are not comparable.

As will be made clear in Section V-A, our coding theory construction of authentication codes is different from the one in [10]. We now compare a subclass of our codes of Theorem 8 using our coding theory construction with a subclass of codes in [10].

In [10], authentication codes with parameters

$$|\mathcal{S}| = q^{\kappa}, \quad |\mathcal{K}| = q^2, \quad |\mathcal{T}| = q, \quad P_I = \frac{1}{q}, \quad P_S = \frac{\kappa}{q}$$

are constructed by applying the q-twisted construction to the Reed–Solomon codes. It is proven in [10] that these codes are *weakly optimal*. Note that Reed–Solomon codes cannot be used in our coding theory construction because it gives authentication codes with $P_S = 1$.

We now consider a subclass of these codes for the case $q = p$ being prime and $\kappa = 2$. This subclass of codes has parameters

$$|\mathcal{S}| = p^2, \quad |\mathcal{K}| = p^2, \quad |\mathcal{T}| = p, \quad P_I = \frac{1}{p}, \quad P_S = \frac{2}{p}.$$

A subclass of the authentication codes of Theorem 8 defined by $m = 1$ has parameters

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

So the P_S and P_I of our codes of Theorem 8 are the same as those of that subclass of codes in [10]. However, our subclass of codes uses fewer keys, and thus is better than the subclass of codes in [10] which is proved to be weakly optimal.

D. Authentication Codes From the Third Class of Linear Codes

Let χ be a nontrivial additive character of $\mathrm{GF}(q^m)$ and let $a = (a_1, \ldots, a_r) \in \mathrm{GF}(q^m)^r$, $b \in \mathrm{GF}(q^m)$. Then the sum

$$K(\chi; a, b) = \sum_{(x_1,\ldots,x_r)\in(\mathrm{GF}(q^m)^*)^r} \chi\left(\sum_{i=1}^{r} a_i x_i + b x_1^{-1}\cdots x_r^{-1}\right)$$

is called the multiple Kloosterman sum.

Lemma 9: If χ is a nontrivial additive character of $\mathrm{GF}(q^m)$, $a \in \mathrm{GF}(q^m)^r$ and $b \in \mathrm{GF}(q^m)$ with $(a, b) \neq (0, 0)$, then

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

We now define a function

$$f_{a,b}(x) = \mathrm{Tr}_{q^m/q}\left(a_1 x_1 + \cdots + a_r x_r + b x_1^{-1}\cdots x_r^{-1}\right)$$

where $\mathrm{Tr}_{q^m/q}$ is the trace function from $\mathrm{GF}(q^m)$ to $\mathrm{GF}(q)$ and $x = (x_1, \ldots, x_r)$. We define

$$N(a, b; u) = |\{x \in (\mathrm{GF}(q^m)^*)^r : f_{a,b}(x) = u\}|$$

for any $(a, b) \in \mathrm{GF}(q^m)^r \times \mathrm{GF}(q^m)$ and $u \in \mathrm{GF}(q)$.

We now give a lower bound on $N(a, b; u)$ for any $(a, b) \neq (0, 0)$. Let $q = p^h$ for some h, where p is a prime. We use $\mathrm{Tr}_{q/p}$ to denote the trace function from $\mathrm{GF}(q)$ to $\mathrm{GF}(p)$, and let ϵ denote a complex p-th root of unity. Then

$$\begin{aligned} qN(a,b;u) &= \sum_{x\in(\mathrm{GF}(q^m)^*)^r} \sum_{y\in\mathrm{GF}(q)} \epsilon^{\mathrm{Tr}_{q/p}[y(f_{a,b}(x)-u)]} \\ &= (q^m-1)^r + \sum_{y\in\mathrm{GF}(q)^*} \sum_{x\in(\mathrm{GF}(q^m)^*)^r} \epsilon^{\mathrm{Tr}_{q/p}[y(f_{a,b}(x)-u)]} \\ &= (q^m-1)^r + \sum_{y\in\mathrm{GF}(q)^*} \epsilon^{\mathrm{Tr}_{q/p}[-yu]} \sum_{x\in(\mathrm{GF}(q^m)^*)^r} \epsilon^{\mathrm{Tr}_{q/p}[y(f_{a,b}(x))]} \end{aligned}$$

By Lemma 9

$$\begin{aligned} |qN(a,b;u) - (q^m-1)| &\leq \sum_{y\in\mathrm{GF}(q)^*} \left| \sum_{x\in(\mathrm{GF}(q^m)^*)^r} \epsilon^{\mathrm{Tr}_{q/p}[y(f_{a,b}(x))]} \right| \\ &\leq (r+1)(q-1)q^{mr/2}. \end{aligned}$$

Hence

$$\begin{cases} N(a,b;u) \geq \frac{(q^m-1)^r-(r+1)(q-1)q^{mr/2}}{q} \\ N(a,b;u) \leq \frac{(q^m-1)^r+(r+1)(q-1)q^{mr/2}}{q}. \end{cases} \tag{5}$$

For any $a, b \in \mathrm{GF}(q^m)$, we define a vector

$$\boldsymbol{c}_{a,b} = \big(f_{a,b}(\gamma_0), f_{a,b}(\gamma_1), \ldots, f_{a,b}(\gamma_{(q^m-1)^r-1})\big)$$

where $\gamma_0, \gamma_1, \ldots, \gamma_{(q^m-1)^r-1}$ are all the elements of $\mathrm{GF}(q^m)^*$. We then define a $[(q^m-1)^r, (r+1)m]$ linear code $\mathcal{C}$ over $\mathrm{GF}(q)$ as

$$\mathcal{C} = \{\boldsymbol{c}_{a,b} : a, b \in \mathrm{GF}(q^m)\}. \tag{6}$$

Lemma 10: If $(q^m-1)^r > (r+1)q^{mr/2}$, the code $\mathcal{C}$ of (6) has parameters $[(q^m-1)^r, (r+1)m, d]$ with minimum distance

$$d \geq \frac{(q-1)(q^m-1)^r-(r+1)(q-1)q^{mr/2}}{q}.$$

Proof: If $(q^m-1)^r > (r+1)q^{mr/2}$, by (5) $N(a,b;u) < (q^m-1)^r$ for any $(a,b) \neq (0,0)$ and u. Thus, the $q^{(r+1)m}$ codewords are pairwise distinct, and $\mathcal{C}$ has dimension $(r+1)m$. The lower bound on the minimum distance d also follows from (5). □

Theorem 11: Let $\mathcal{C}$ be the $[(q^m-1)^r, (r+1)m]$ code of Lemma 10. Then for the authentication code of (2), we have

$$P_I = \frac{1}{q} \text{ and } P_S \leq \frac{1}{q} + \frac{(r+1)(q-1)q^{mr/2}}{q(q^m-1)^r}.$$

Furthermore, $|\mathcal{S}| = q^{(r+1)m}$, $|\mathcal{T}| = q$, $|\mathcal{K}| = (q^m-1)^r q$.

Proof: By Theorem 1, $P_I = \frac{1}{p}$. By (5) we have

$$\max_{\substack{0 \neq \boldsymbol{c} \in \mathcal{C} \\ u \in \mathrm{GF}(p)}} N(\boldsymbol{c}, u) \leq \frac{(q^m-1)^r+(r+1)(q-1)q^{mr/2}}{q}.$$

The conclusion on P_S then follows from Theorem 1. □

Note that our construction here is based on the multiple Kloosterman sum, which is different from the construction based on some exponential sums given in [9].

In [9], authentication codes with parameters

$$|\mathcal{S}| = q^{m(D-\lfloor D/p \rfloor)}, \quad |\mathcal{K}| = q^{m+1}, \quad |\mathcal{T}| = q,$$
$$P_I = \frac{1}{q}, \quad P_S = \frac{1}{q} + \frac{D-1}{\sqrt{q^m}}$$

are constructed using exponential sums, where D is an integer with $1 \leq D \leq \sqrt{q^m}$ and p is the characteristic of the finite field $\mathrm{GF}(q^m)$. When $D = 1$, the codes are optimal and are constructed using linear functions.

We first consider a subclass of the codes defined by $D = 3$, $m = 1$, and $p = 2$ or 3 with a subclass of our authentication codes of Theorem 11 defined by $m = r = 1$ and q being a power of 2 or 3.

In the case that $D = 3$, $m = 1$, and $p = 2$ or 3, the subclass of codes in [9] have the parameters

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

In the case $m = r = 1$ and q being a power of 2 or 3, our codes of Theorem 11 have parameters

$$|\mathcal{S}| = q^2, \quad |\mathcal{K}| = (q-1)q < |\mathcal{S}|, \quad |\mathcal{T}| = q,$$
$$P_I = \frac{1}{q}, \quad P_S = \frac{1}{q} + \frac{2}{\sqrt{q}}.$$

So the P_I and P_S of the subclass of the codes of Theorem 11 are the same as the subclass of codes in [9] and both subclasses of codes have the same tag space and source state space. But our subclass of codes uses fewer keys, and are thus better.

When $D = 3$, $m = 1$, and $p > 3$, the probabilities P_I and P_S are the same for the subclass of codes in [9]. However, the subclass of codes in [9] has a larger source state space and key space. In this case, the parameters of the subclass of codes in [9] cannot be compared with our subclass of codes.

For all the remaining cases, the parameters of our codes are not comparable with those of the codes in [9]. So we have made a full comparison of our authentication codes of Theorem 11 with those in [9]. The conclusion is that whenever the parameters are comparable, our codes are better.

E. Special Cases

It can be shown that the construction using exponential sums by Helleseth and Johansson [9] and the construction using algebraic curves by Xing, Wang, and Lam [20] can be viewed as special cases of the generic construction of this paper.

IV. Constructions Using Nonlinear Codes

The generic coding-theory construction of (1) in Section II allows the use of both linear and nonlinear codes. In Section III, we demonstrated that linear codes could give very good authentication codes with this construction. In this section, we will show that this construction could also produce good and optimal authentication codes when certain nonlinear codes are employed.

Let $(A, +)$ be a group of order q. A $(q, k; \lambda)$ *difference matrix* is a $k \times q\lambda$ matrix $D = (d_{ij})$ with entries from A, so that for each $1 \leq h < j \leq k$, the list

$$d_{h,1} - d_{j,1}, d_{h,2} - d_{j,2}, \ldots, d_{h,q\lambda} - d_{j,q\lambda}$$

contains every element of A λ times, see [7]. A generalized Hadamard matrix $\mathrm{GH}(q, \lambda)$ is a $(q, q\lambda; \lambda)$ difference matrix. Hence Hadamard difference matrices are special difference matrices. In particular, a Hadamard matrix $H(4n)$ is a $\mathrm{GH}(2, 2n)$ over the group $(\{1, -1\}, \cdot)$.

Let $\mathcal{C}$ be an (n, M) code over an alphabet A, where $(A, +)$ is an Abelian group with q elements. We use $\boldsymbol{c}_i = (c_{i,0}, \ldots, c_{i,n-1})$ to denote a codeword of $\mathcal{C}$, $0 \leq i \leq M-1$. Define an $M \times n$ matrix $C = [\boldsymbol{c}_0^T \boldsymbol{c}_2^T \cdots \boldsymbol{c}_{M-1}^T]^T$.

With a proof similar to that of Theorem 1, we can prove the following.

Theorem 12: The authentication code of (1) has $P_I = P_S = \frac{1}{q}$ if and only if C is a $(q, M; n/q)$ differenc matrix over A

Clearly, the row vectors of a difference matrix usually form a nonlinear code, and certain nonlinear codes give difference matrices. It is known that for any $(q, k; \lambda)$ difference matrix, we have $q\lambda \geq k$, and the equality here holds if and only if it is a generalized Hadamard matrix. With our construction of (1), Hadamard matrices give in fact optimal authentication codes.

Theorem 13: The authentication code of (1) has $P_I = P_S = \frac{1}{q}$ and is optimal if C is a $(q, n; n/q)$ generalized Hadamard matrix over A.

Proof: The optimality of an authentication code with such parameters is proved in [6] □

Let f be a mapping from a finite Abelian group $(A, +)$ to another one $(B, +)$. We use $a_0, a_1, \ldots, a_{n-1}$ to denote all the elements of A. We now define an (n, n) code $\mathcal{C}$ over the alphabet B, with the codewords defined by

$$\boldsymbol{c}_i = (f(a_0 + a_i), \ldots, f(a_{n-1} + a_i)) \tag{7}$$

for all i with $0 \leq i \leq n-1$. If f is nonlinear, the code $\mathcal{C}$ is also nonlinear.

When f has optimal nonlinearity, the authentication codes of (1) corresponding to the nonlinear codes $\mathcal{C}$ of (7) become the authentication codes constructed from highly nonlinear functions by Chanson, Ding, and Salomaa [6]. The construction using generalized Hadamard difference matrices is closely related to the one using perfect nonlinear mappings. In particular, some generalized Hadamard matrices can be constructed with perfect nonlinear mappings [5]. The purpose of this subsection is to point out that the construction by Chanson, Ding, and Salomaa is a special case of the general construction presented in this paper.

V. Comparison With Other Related Constructions

In this section, we review some other related constructions and point out how they differ from the generic construction of Section II.

A. The Kabatianskii–Smeets–Johansson Construction

The q-twisted construction given in [10] uses an (n, M, d) code over GF(q) with some special property to construct an authentication code with parameters

$$|\mathcal{S}| = M/q, \quad |\mathcal{E}| = nq, \quad |\mathcal{T}| = q, \quad P_I = \frac{1}{q}, \quad P_S = 1 - \frac{d}{n}.$$

Thus, the maximum probability P_S is completely determined by the minimum distance of the error-correcting code. Furthermore, the larger the minimum distance of the code, the smaller the probability P_S of the obtained authentication code.

However, for authentication codes from our construction, the maximum probability P_S cannot be determined by the minimum distance of the error-correcting code. On contrast, a linear code with very large minimum distance could give a very bad authentication code. For example, consider the maximum-distance separable (MDS) $[n, 1, n]$ linear code generated by the all-one vector $\mathbf{1}$ and the authentication code using this linear code with our construction. The maximum probability $P_S = 1$, which shows that the obtained authentication code is the worst.

Furthermore, the coding theory construction of authentication codes in [10] requires an (n, M, d) code $\mathcal{C}$ such that if $\boldsymbol{c} \in \mathcal{C}$, then $\boldsymbol{c} + \lambda\mathbf{1} \in \mathcal{C}$ for all λ, where $\mathbf{1}$ is the all-one codeword. While such a code cannot be used in our construction at all because it will give an authentication code with $P_S = 1$.

B. The Composition Construction

This construction has been considered in [3], [4], and [16]. Briefly, its basic idea is equivalent to combining an authentication code with an error-correcting code to obtain a new authentication code. This construction is different from the generic construction of Section II.

C. The Wang–Xing–Safavi-Naini Construction

Wang, Xing, and Safavi-Naini introduced a class of authentication codes, called linear authentication codes [18]. An authentication code $(\mathcal{S}, \mathcal{T}, \mathcal{K}, \{E_k : k \in \mathcal{K}\})$ is called *linear* if

1. $\mathcal{K}$ and $\mathcal{T}$ are finite dimensional spaces over GF(q);
2. for each $s \in \mathcal{S}$, the function $f(k)$ defined by $f(k) = E_k(s)$ is a GF(q)-linear mapping from $\mathcal{K}$ to $\mathcal{T}$.

Wang, Xing, and Safavi-Naini used the rank distance codes to construct some linear authentication codes [18]. This construction seems different from the generic construction of Section II and also other constructions based on error-correcting codes.

VI. Concluding Remarks

We presented a construction of authentication codes based on error-correcting codes, and described several classes of authentication codes based on several types of linear error-correcting codes. We showed that some subclasses of our authentication codes are better than some subclasses of existing good authentication codes or the parameters of our codes are not comparable with them. We remark that the construction of this paper is different from that of [8], although the same set of error-correcting codes are employed in both constructions. On the other hand, the parameters of the authentication codes in this paper and those of the authentication codes in [8] can never be the same.

Note that a Cartesian authentication code has five parameters. In order to be able to compare two classes of authentication codes, we need to fix at least three of the five parameters and then compare the remaining parameters for the two classes. In many cases this is impossible, and hence it is not possible to compare two classes of authentication codes. We mention that we are not able to compare our authentication codes with those in [20], since the parameters are not comparable.

We showed that the general construction described in this paper is closely related to difference matrices and generalized Hadamard matrices. We also demonstrated that our construction is a generalization of several earlier constructions, and on the other hand different from several other earlier constructions.

Clearly, with our construction every error-correcting code gives an authentication code. It is obvious that this construction gives both good and bad authentication codes. The main task is

to find classes of error-correcting codes with special properties that give good authentication codes within the framework of this construction.

Finally, we invite the reader to check if there is any connection between the constructions of authentication codes in this paper and the constructions of error-correcting codes using pseudo-random graphs in [1].

ACKNOWLEDGMENT

The authors wish to thank the reviewers for their comments that improved the presentation of this paper.

REFERENCES

[1] N. Alon, J. Bruck, J. Naor, M. Naor, and R. M. Roth, "Construction of asymptotically good low-rate error-correcting codes through pseudo-random graphs," *IEEE Trans. Inf. Theory*, vol. 38, no. 2, pp. 509–516, Mar. 1992.

[2] L. D. Baumert and R. J. McEliece, "Weights of irreducible codes," *Info. Comput.*, vol. 20, pp. 158–175, 1972.

[3] J. Bierbrauer, "Universal hashing and geometric codes," *Des., Codes Cryptogr.*, vol. 11, pp. 207–221, 1997.

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

[5] C. Carlet and C. Ding, "Highly nonlinear mappings," *J. Complexity*, vol. 20, no. 2, pp. 205–244, 2004.

[6] S. Chanson, C. Ding, and A. Salomaa, "Cartesian authentication codes from functions with optimal nonlinearity," *Theor. Comp. Sci.*, vol. 290, pp. 1737–1752, 2003.

[7] C. J. Colbourn and W. De Launey, "Difference matrices," in *CRC Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz, Eds. Boca Raton, FL: CRC, 1996, pp. 287–297.

[8] C. Ding and X. Wang, "A coding theory construction of new systematic authentication codes," *Theor. Comp. Sci.*, vol. 330, pp. 81–99, 2005.

[9] T. Helleseth and 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)*. New York: Springer-Verlag, 1997, vol. 1109, pp. 31–44.

[10] G. A. Kabatianskii, B. Smeets, and T. Johansson, "On the cardinality of systematic authentication codes via error-correcting codes," *IEEE Trans. Inf. Theory*, vol. 42, no. 2, pp. 566–578, Mar. 1996.

[11] R. Lidl and H. Niederreiter, *Finite Fields*, ser. Encyclopedia of Mathematics and Its Application . Cambridge, U.K.: Cambridge University Press, 1997, vol. 20.

[12] C. Mitchell, M. Walker, and P. Wild, "The combinatorics of perfect authentication schemes," *SIAM J. Discr. Math.*, vol. 7, pp. 102–107, 1994.

[13] R. S. Rees and D. R. Stinson, "Combinatorial characterizations of authentication codes II," in *Des., Codes Cryptogr.y*, 1996, vol. 7, pp. 239–259.

[14] G. J. Simmons, "Authentication theory/coding theory," in *Advances in Cryptology—Crypto' 84 (Lecture Notes in Computer Science)*. New York: Springer-Verlag, 1984, vol. 196, pp. 411–431.

[15] D. R. Stinson, "Combinatorial characterizations of authentication codes," *Des., Codes Cryptogr.*, vol. 2, pp. 175–187, 1992.

[16] D. R. Stinson, "Universal hashing and authentication codes," *Des., Codes Cryptogr.*, vol. 2, pp. 74–85, 1992.

[17] D. R. Stinson, "On the connections between universal hashing, combinatorial designs and error-correcting codes," in *Congressus Numerantium*, 1996, vol. 114, pp. 7–27.

[18] H. Wang, C. Xing, and R. Safavi-Naini, "Linear authentication codes: Bounds and constructions," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 866–872, Apr. 2003.

[19] M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality," *J. Comp. Syst. Sci.*, vol. 22, pp. 265–279, 1981.

[20] C. Xing, H. Wang, and K. Y. Lam, "Construction of authentication codes from algebraic curves over finite fields," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 886–892, May 2000.

[21] J. Yuan, C. Carlet, and C. Ding, "The weight distribution of a class of linear codes from perfect nonlinear functions," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 712–717, Feb. 2006.