Linear Authentication Codes: Bounds and Constructions

Huaxiong Wang, Chaoping Xing, and Rei Safavi-Naini

***Abstract*—In this paper, we consider a new class of unconditionally secure authentication codes, called *linear authentication codes* (or *linear A-codes*). We show that a linear A-code can be characterized by a family of subspaces of a vector space over a finite field. We then derive an upper bound on the size of source space when other parameters of the system, that is, the sizes of the key space and the authenticator space, and the deception probability, are fixed. We give constructions that are asymptotically close to the bound and show applications of these codes in constructing distributed authentication systems.**

***Index Terms*—Authentication codes (A-codes), distributed A-codes, linear A-codes.**

I. Introduction

UNCONDITIONALLY secure authentication codes (A-codes) allow two trusting parties to communicate in the presence of an opponent who may construct a fraudulent message, and/or substitute a transmitted message with a fraudulent one.

The construction of unconditionally secure A-codes relies on a number of theoretical areas including design theory, finite geometry, coding theory, and information theory. Previous research on authentication theory has been mainly focused on deriving bounds on parameters of A-codes and construction of codes with desirable properties such as having the minimum possible deception probabilities and the minimum number of keys. In general, to describe the model of A-codes and characterize optimal codes, a combinatorial approach is used. For example, numerous results are in the form "an A-code with certain properties exists if and only if a certain combinatorial structure exists."

In this paper, we introduce a new class of A-codes, called *linear A-codes*. *Linearity* requires some additional algebraic properties for the A-codes; that is, we require both the key space and the authenticator space of the codes be vector spaces, and a source state to induce a linear mapping between them. The main motivation of linear A-codes stems from the study of distributed authentication systems in which the functionality of authentication is to be distributed among a number of participants. The extra algebraic property allows more efficient constructions of such distributed systems.

We characterize linear A-codes in terms of a family vector spaces over finite fields such that the dimension of the intersection of a pair of such subspaces does not exceed a certain desired value (security parameter). We derive an upper bound on the number of possible source states of an A-code for given deception probabilities and number of keys, and give constructions that meet, or asymptotically meet, the bound.

The paper is organized as follows. In Section II, we give definitions and review known results on A-codes that will be required for the rest of the paper. In Section III, we introduce linear A-codes. Characterization of A-codes in terms of the families of subspaces of a vector space is given in Section IV, and bounds on the number of source states and constructions that asymptotically meet the bounds are given in Sections V and VI. We show how linear A-codes can be used to construct distributed authentication schemes in Section VII. Finally, we propose further research problems and conclude the paper in Section VIII.

II. Authentication Codes (A-Codes)

A-codes were first considered by Gilbert, MacWilliams, and Sloane [10]. Development of the general theory of unconditionally secure authentication systems has been initiated by Simmons [22], [23] and extended by a number of authors (see, for example, [1]–[3], [5], [7], [8], [11], [16], [19], [24]–[28]).

In the conventional model for unconditionally secure authentication system, there are three participants: a *transmitter*, a *receiver*, and an *opponent*. The transmitter wants to communicate a message to a receiver using a public channel which is subject to active attacks. That is, the opponent may impersonate the transmitter and insert a message into the channel, or replace a transmitted message with a fraudulent one. To protect against these attacks, the transmitter and the receiver share a secret key which is used to choose an authentication rule from an A-code.

A *systematic* A-code (or A-code *without secrecy*) is a code in which a *message* that is sent through the channel, consists of a *source state* (i.e., plaintext) concatenated with an *authenticator* (or a *tag*). Such a code is a triple $(\mathcal{S}, \mathcal{E}, \mathcal{A})$ of finite sets together with an (authentication) function $f: \mathcal{S} \times \mathcal{E} \to \mathcal{A}$. We sometimes also denote the A-code by $(\mathcal{S}, \mathcal{E}, \mathcal{A}, f)$. Here $\mathcal{S}$ is the set of source states, $\mathcal{E}$ is the set of keys, and $\mathcal{A}$ is the set of authenticators. When the transmitter wants to send the message $s \in \mathcal{S}$ using a key $e \in \mathcal{E}$, which is secretly shared with the receiver, he transmits the message (s, a), where $s \in \mathcal{S}$

Manuscript received August 11, 2001; revised November 15, 2002. The material in this paper was presented in part at Indocrypt 2001, The Second International Conference on Cryptology, Chennai, India, December 16–20, 2001.

H. Wang is with the Department of Computing, Macquarie University, Sydney, NSW 2109, Australia (e-mail: hwang@ics.mq.edu.au).

C. Xing is with the Department of Mathematics, National University of Singapore, Singapore. He is also with the University of Science and Technology of China, Hefei, Anhui, China (e-mail: matxcp@nus.edu.sg).

R. Safavi-Naini is with the School of Information Technology and Computer Science, University of Wollongong, Wollongong, Australia (e-mail: rei@uow.edu.au).

Communicated by P. Solé, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2003.809567

and $a = f(s, e) \in \mathcal{A}$. When the receiver receives (s, a), she checks the authenticity of the message by verifying whether $a = f(s, e)$ or not, using the secret key $e \in \mathcal{E}$. If the equality holds, she accepts s as authentic.

Suppose the opponent has the ability to insert messages into the channel and/or to modify existing messages. An *impersonation attack* is when the opponent inserts a new message (s', a') into the channel. A *substitution attack* is when the opponent sees a message (s, a) and changes it to (s', a') where $s \neq s'$. A message (s, a) is called *valid* if there exists a key e such that $a = f(s, e)$. We assume that there is a probability distribution on the source states, which is known to all the participants. Given the probability distribution on the source states, the receiver and the transmitter will choose a probability distribution for $\mathcal{E}$. We will denote the probability of success of the opponent in impersonation and substitution attacks by P_I and P_S, respectively. Then we have

$$P_I = \max_{s, a} P((s, a) \text{ valid})$$

and

$$P_S = \max_{s, a} \max_{s \neq s', a'} P((s', a') \text{ valid} \mid (s, a) \text{ observed}).$$

In the remainder of the paper, we will always assume that the keys and the source states are uniformly distributed. In this case, we can represent P_I and P_S as follows:

$$P_I = \max_{s, a} \frac{|\{e \in \mathcal{E} \mid a = f(s, e)\}|}{|\mathcal{E}|},$$

$$P_S = \max_{s, a} \max_{s' \neq s, a'} \frac{|\{e \in \mathcal{E} \mid a = f(s, e), a' = f(s', e)\}|}{|\{e \in \mathcal{E} : a = f(s, e)\}|}.$$

Consider an A-code $(\mathcal{S}, \mathcal{E}, \mathcal{A})$, where $\mathcal{S}$ is a set of k source states, and $\mathcal{A}$ is a set of ℓ authenticators. For this code, it is known that $P_I \geq 1/\ell$ and $P_S \geq P_I$. Codes with $P_I = P_S = 1/\ell$ have been known to be equivalent to orthogonal arrays (see [26]). That is, suppose we have an A-code $(\mathcal{S}, \mathcal{E}, \mathcal{A})$ without secrecy with k source states and having ℓ authenticators in which $P_I = P_S = 1/\ell$. Then $|\mathcal{E}| \geq k(\ell - 1) + 1$ and equality occurs if and only if there exists an orthogonal array $OA(\ell, k, \lambda)$, where $\lambda = (k(\ell - 1) + 1)/\ell^2$.

One of the goals of authentication theory is to derive bounds on various parameters of A-codes and to construct A-codes with desired properties. For a review of different bounds and constructions for A-codes, refer to [11], , [14], [24], and [26].

III. Linear A-Codes

Consider an A-code $(\mathcal{S}, \mathcal{E}, \mathcal{A}, f)$. For each key $e \in \mathcal{E}$, the authentication function $f: \mathcal{S} \times \mathcal{E} \rightarrow \mathcal{A}$ induces a mapping ψ_e from $\mathcal{S}$ to $\mathcal{A}$ defined by $\psi_e(s) = f(s, e), \forall s \in \mathcal{S}$. Thus, the A-code $(\mathcal{S}, \mathcal{E}, \mathcal{A}, f)$ can be characterized completely by the family of mappings $\{\psi_e | e \in \mathcal{E}\}$, and *vice versa*. An attractive family of such mappings is obtained from an *almost strongly universal hash family*, which was introduced by Wegman and Carter [27] and has been the basis of the most combinatorial constructions. More details on the connections between almost strongly universal hash families and A-codes can be found in [2], [26], [27].

A source state $s \in \mathcal{S}$ in an A-code $(\mathcal{S}, \mathcal{E}, \mathcal{A}, f)$ can also be uniquely associated with a mapping ϕ_s from $\mathcal{E}$ to $\mathcal{A}$ defined by $\phi_s(e) = f(s, e), \forall e \in \mathcal{E}$. Then, again, the A-code $(\mathcal{S}, \mathcal{E}, \mathcal{A}, f)$ can be characterized by a family of mapping $\Phi = \{\phi_s \mid s \in \mathcal{S}\}$. In a conventional authentication system, the key space $\mathcal{E}$ and the authenticator space $\mathcal{A}$ do not have any algebraic structures. We will consider A-codes in which $\mathcal{E}$ and $\mathcal{A}$ have some additional algebraic structures. In particular, $\mathcal{E}$ and $\mathcal{A}$ are vector spaces over a finite filed $\boldsymbol{F}_q$, and Φ is a family of $\boldsymbol{F}_q$-linear mappings from $\mathcal{E}$ to $\mathcal{A}$. These codes are called *linear* A-codes. As will be shown in Section VII, linear A-codes are useful in constructing distributed authentication schemes.

Definition 3.1: An A-code $(\mathcal{S}, \mathcal{E}, \mathcal{A}, f)$ is *linear* over $\boldsymbol{F}_q$ if

i) $\mathcal{E}$ and $\mathcal{A}$ are finite-dimensional vector spaces over $\boldsymbol{F}_q$;

ii) for every $s \in \mathcal{S}$, ϕ_s defined by $\phi_s(e) = f(s, e)$ is an $\boldsymbol{F}_q$-linear mapping from $\mathcal{E}$ to $\mathcal{A}$.

We identify $\mathcal{S}$ with $\Phi = \{\phi_s \mid s \in \mathcal{S}\}$, and write the A-code as $(\Phi, \mathcal{E}, \mathcal{A}, f)$ to emphasize that the source states are represented as linear mappings. We may assume that $\mathcal{E} = \boldsymbol{F}_q^m$ and $\mathcal{A} = \boldsymbol{F}_q^m$. Given a basis $e_1, e_2, \ldots, e_n$ of $\mathcal{E}$ and a basis $a_1, a_2, \ldots, a_m$ of $\mathcal{A}$, a linear mapping $\phi \in \Phi$ can be represented by a *unique* $n \times m$ matrix A over $\boldsymbol{F}_q$ such that $\phi(e) = eA$, $\forall e \in \mathcal{E}$. If V and W are two vector spaces over $\boldsymbol{F}_q$, and ϕ is a linear mapping from V to W, we will denote $\mathbf{Ker}(\phi) = \{v \in V \mid \phi(v) = 0\}$. Obviously, $\mathbf{Ker}(\phi)$ is a subspace of V and its dimension is denoted by $\mathbf{dim}(\mathbf{Ker}(\phi))$.

Next, we compute the success probabilities of impersonation and substitution attacks for a linear A-code. For the impersonation attack, we have

$$\begin{aligned} P_I &= \max_{\phi \in \Phi} \max_{a \in \mathcal{A}} \frac{|\{e \mid \phi(e) = a\}|}{|\mathcal{E}|} \\ &= \max_{\phi \in \Phi} \frac{|\{e \mid \phi(e) = 0\}|}{|\mathcal{E}|} \\ &= \max_{\phi \in \Phi} 1/q^{\mathbf{dim}(\mathbf{Ker}(\phi)) - n} = q^{n - \gamma} \end{aligned}$$

where

$$\gamma = \max_{\phi \in \Phi} \{\mathbf{dim}(\mathbf{Ker}(\phi)) \mid \phi \in \Phi\}.$$

Clearly, $\gamma \leq n - m$, and if equality holds then P_I achieves the maximal value. In this case, each ϕ is onto, i.e., $\phi_s(\mathcal{E}) = \mathcal{A}$, $\forall s \in \mathcal{S}$.

For the substitution attach, we have

$$\begin{aligned} P_S &= \max_{\substack{\phi, \phi' \in \Phi \\ \phi \neq \phi'}} \max_{a, a' \in \mathcal{A}} \frac{|\{e \mid \phi(e) = a, \phi'(e) = a'\}|}{|\{e \mid \phi(e) = a\}} \\ &= \max_{\substack{\phi, \phi' \in \Phi \\ \phi \neq \phi'}} \max_{a, a' \in \mathcal{A}} \frac{|\{e \mid \phi(e) = a\} \cap \{e \mid \phi'(e) = a'\}|}{|\{e \mid \phi(e) = 0\}|}. \end{aligned}$$

In order to compute P_S, we need the following lemma.

Lemma 3.1: For any $\phi, \phi' \in \Phi$ and any $a, a' \in \mathcal{A}$, we have either

i) $|\{e | \phi(e) = a\} \cap \{e | \phi'(e) = a'\}| = 0$; or

ii) $|\{e | \phi(e) = a\} \cap \{e | \phi'(e) = a'\}| = |\{e | \phi(e) = 0\} \cap \{e | \phi'(e) = 0\}|$.

Proof: Assume that $|\{e|\phi(e)=a\}\cap\{e|\phi'(e)=a'\}|\neq 0$, then there exists an $e_0\in\{e|\phi(e)=a\}\cap\{e|\phi'(e)=a'\}$. We define a function τ from $\{e|\phi(e)=a\}\cap\{e|\phi'(e)=a'\}$ to $\{e|\phi(e)=0\}\cap\{e|\phi'(e)=0\}$ by $\tau(e)=e-e_0$. It is easy to see that τ is one-to-one, which implies

$$|\{e|\phi(e)=a\}\cap\{e|\phi'(e)=a'\}|\leq|\{e|\phi(e)=0\}\cap\{e|\phi'(e)=0\}|.$$

On the other hand, we can define a function π from $\{e|\phi(e)=0\}\cap\{e|\phi'(e)=0\}$ to $\{e|\phi(e)=a\}\cap\{e|\phi'(e)=a'\}$ by $\pi(e)=e+e_0$. Again, π is one-to-one, which implies

$$|\{e|\phi(e)=0\}\cap\{e|\phi'(e)=0\}|\leq|\{e|\phi(e)=a\}\cap\{e|\phi'(e)=a'\}|$$

giving the proof of the lemma. □

From Lemma 3.1, P_S can be rewritten as

$$P_S=\max_{\substack{\phi,\phi'\in\Phi\\ \phi\neq\phi'}}\frac{|\{e\,|\,\phi(e)=0\}\cap\{e\,|\,\phi'(e)=0\}|}{|\{e\,|\,\phi(e)=0\}|}.$$

It follows that both P_I and P_S must be the reciprocals of a power q. That is, $P_I=q^{-t}$ and $P_S=q^{-d}$ for some integers t and d with $t\geq d$, and so performance of a linear A-code over $\boldsymbol{F}_q$ can be determined by the parameters $|\Phi|$, n, m, t and d. For given t and d (which correspond to the security level of the A-code), and n and m (which correspond to the key size and the length of tag), we would like to have $|\Phi|$ as large as possible. Equivalently, for given t, d, and $|\mathcal{S}|$ (the number of sources), we would like to construct linear A-code with $|\Phi|=|\mathcal{S}|$ such that n and m are as small as possible.

IV. Interpreting a Linear A-Code as a Family of Subspaces

Definition 4.1 [11]: An A-code $(\mathcal{S},\mathcal{E},\mathcal{A},f)$ is called *I-equitable* if it has the additional property that

$$\forall\, s\in\mathcal{S},\, a\in\mathcal{A},\qquad P_I=\frac{|\{e|f(s,e)=a\}|}{|\mathcal{E}|}.$$

Given an A-code $\mathcal{C}=(\mathcal{S},\mathcal{E},\mathcal{A},f)$, we may, without loss of generality,[1] assume $(\mathcal{A},+)$ is an Abelian group. Let $\mathcal{E}^*=\mathcal{E}\times\mathcal{A}$. We define a new A-code $C^*=(\mathcal{S},\mathcal{E}^*,\mathcal{A},f^*)$ with

$$f^*\colon\mathcal{S}\times(\mathcal{E}\times\mathcal{A})\to\mathcal{A}$$

defined by $f^*(s,(e,a))=f(s,e)+a$.

Lemma 4.1: Let $\mathcal{C}=(\mathcal{S},\mathcal{E},\mathcal{A},f)$ be an A-code. Then $\mathcal{C}^*=(\mathcal{S},\mathcal{E}^*,\mathcal{A},f^*)$ defined above is an I-equitable A-code and $P_S^*\leq P_S$, where P_S^* and P_S are the probabilities of substitution attacks in $\mathcal{C}^*$ and $\mathcal{C}$, respectively.

Proof: For any $s\in\mathcal{S}$ and $a\in\mathcal{A}$, we have

$$\begin{aligned}P_I^*&=\frac{|\{(e,b)\,|\,f^*(s,(e,b))=a\}|}{|\mathcal{E}\times\mathcal{A}|}\\&=\frac{\left|\bigcup_{b\in\mathcal{A}}\{e\in\mathcal{E}\,|\,f^*(s,e)=a-b\}\right|}{|\mathcal{E}|\,|\mathcal{A}|}\\&=\frac{|\mathcal{E}|}{|\mathcal{E}|\,|\mathcal{A}|}=\frac{1}{|\mathcal{A}|}.\end{aligned}$$

So $(\mathcal{S},\mathcal{E}^*,\mathcal{A},f^*)$ is I-equitable.

[1]If $\mathcal{A}$ is not an Abelian group, we can define an operation on it to make it an Abelian group.

On the other hand

$$\begin{aligned}P_S^*&=\max_{\substack{s,s'\in\mathcal{S}\\ s\neq s'}}\max_{a,a'\in\mathcal{A}}\\&\quad\times\frac{|\{(e,b)|f(s,e)=a-b)\}\cup\{(e,b)|f(s',e)=a'-b\}|}{|\{(e,b)\,|\,f(s,e)=a-b)\}|}\\&\leq\max_{\substack{s,s'\in\mathcal{S}\\ s\neq s'}}\max_{c,c'\in\mathcal{A}}\frac{|\{e|f(s,e)=c\}\cup\{e|f(s',e)=c'\}|}{|\{e|f(s,e)=c)\}|}\\&=P_S.\end{aligned}$$

□

The I-equitable property means that for any choice of s and a, (s,a) has the least success chance for impersonation attack, and maximizes P_I. Using Lemma 4.1, we will only consider I-equitable A-codes.

We further assume that $P_S<1$. Then the source state $\phi\in\Phi$ of a linear A-code $(\Phi,\mathcal{E},\mathcal{A})$ can be interpreted as surjective linear mapping from $\mathcal{E}$ to $\mathcal{A}$. Indeed, for a given $\phi_0\in\Phi$, let $L_0=\mathbf{Im}(\phi_0)\subseteq\mathcal{A}$. If there exists $\phi\in\Phi$ and $\phi\neq\phi_0$ such that $\mathbf{Im}(\phi)\neq L_0$, since the A-code is I-equitable, we know that $\mathbf{dim}(\mathbf{Im}(\phi))=\mathbf{dim}(L_0)$. It follows that there exists an isomorphism θ from $\mathbf{Im}(\phi)$ to L_0 and $\theta\phi$ is an $\boldsymbol{F}_q$-linear mapping from $\mathcal{E}$ to $\mathcal{A}$ and $\mathbf{Ker}(\theta\phi)=\mathbf{Ker}(\phi_0)$. Notice that $\theta\phi\notin\Phi$. Otherwise, if ϕ is authenticated, the authenticated message $(\phi,\phi(e))$ can be substituted with $(\theta\phi,\theta(\phi(e)))$ that the receiver will always accept as authentic. This contradicts the assumption $P_S<1$. Thus, we can simply replace ϕ by $\theta\phi$ without changing the parameters of the A-code, and the procedure can be repeatedly carried out until each element in Φ^* is an onto linear mapping from $\mathcal{E}$ to L_0. We then take $\mathcal{A}$ to be L_0.

Let $V(n,q)$ denote the n-dimensional linear space over $\boldsymbol{F}_q$.

Definition 4.2: A linear A-code $(\mathcal{S},\mathcal{E},\mathcal{A})$ is called an $[n,M,t,d]$ linear A-code if $|\mathcal{S}|=M$, $|\mathcal{E}|=q^n$, $P_I=1/q^t$, and $P_S=1/q^d$.

Theorem 4.1: There exists an $[n,M,t,d]$ linear A-code if and only if there exists a family of subspaces of $V(n,q)$

$$\mathcal{L}=\{L\,|\,L\text{ is a subspace of }V(\alpha,q)\}$$

such that

i) $|\mathcal{L}|=M$;

ii) $\mathbf{dim}(L)=n-t,\forall\,L\in\mathcal{L}$;

iii) $\mathbf{dim}(L\cap L')\leq n-(t+d),\forall\,L,L'\in\mathcal{L},L\neq L'$.

Proof: Consider an $[n,M,t,d]$ linear A-code $\mathcal{C}=(\Phi,\mathcal{E},\mathcal{A})$ and let

$$\mathcal{L}=\{\mathbf{Ker}(\phi)\,|\,\phi\in\Phi\}.$$

Since $\mathcal{C}$ is I-equitable, $P_I=1/q^{n-\mathbf{dim}(\mathbf{Ker}(\phi))}=q^{-t}$, and so $\mathbf{dim}(\mathbf{Ker}(\phi))=n-t$, $\forall\phi\in\Phi$. From Lemma 3.1, we know

$$\begin{aligned}P_S&=\max_{\substack{\phi,\phi'\in\Phi\\ \phi\neq\phi'}}\frac{q^{\mathbf{dim}(\mathbf{Ker}(\phi)\cap\mathbf{Ker}(\phi'))}}{q^{\mathbf{dim}(\mathbf{Ker}(\phi))}}\\&=\max_{\substack{\phi,\phi'\in\Phi\\ \phi\neq\phi'}}q^{\mathbf{dim}(\mathbf{Ker}(\phi)\cap\mathbf{Ker}(\phi'))-n+t}=q^{-d}.\end{aligned}$$

It follows that $\mathbf{dim}(\mathbf{Ker}(\phi)\cap\mathbf{Ker}(\phi'))\leq n-(t+d)$, and the necessity follows.

Conversely, if there is a family $\mathcal{L}$ of subspaces of $V(\alpha,q)$ such that conditions i)–iii) are satisfied, then we take

$\mathcal{E} = V(n, q)$ and $\mathcal{A} = V(t, q)$. For each subspace $L \in \mathcal{L}$, there exists an $\boldsymbol{F}_q$-linear mapping ϕ_L from $\mathcal{E}$ to $\mathcal{A}$ such that $L = \mathbf{Ker}(\phi_L)$. Let $\Phi = \{\phi_L | L \in \mathcal{L}\}$. Then it is straightforward to verify that $(\Phi, \mathcal{E}, \mathcal{A})$ is an $[n, M, t, d]$ linear A-code. □

V. Bounds on Linear A-Codes

In an $[n, M, t, d]$ linear A-code over $\boldsymbol{F}_q$, given n, t, and d we would like to have M as large as possible. In this section, we will derive some upper bounds on M. We denote $M(n, t, d, q)$ the maximal M for which an $[n, M, t, d]$ linear A-code over $\boldsymbol{F}_q$ exists.

Let

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}.$$

denotes the *Gaussian coefficient*. Then, the number of k-dimensional subspaces of $V(n, q)$ is $\begin{bmatrix} n \\ k \end{bmatrix}_q$, which gives an upper bound for $M(n, t, d, q)$.

Theorem 5.1: For any integer n, t, d with $n \geq t \geq d$ and prime power q, we have

$$M(n, t, d, q) \leq \begin{bmatrix} n \\ n-t \end{bmatrix}_q.$$

For $d = 1$, the bound in Theorem 5.1 is tight as the following corollary shows.

Corollary 5.1:

$$M(n, t, 1, q) = \begin{bmatrix} n \\ n-t \end{bmatrix}_q.$$

Proof: Let $\mathcal{L}$ be the set of all $(n-t)$-dimensional subspaces of the n-dimensional vector space $V(n, q)$. Then $|\mathcal{L}| = \begin{bmatrix} \alpha \\ \alpha-\gamma \end{bmatrix}_q$. Since for any $L, L' \in \mathcal{L}$, $L \neq L'$, $\mathbf{dim}(L \cap L') \leq \alpha - \gamma - 1$, from Theorem 4.1, we know that there exists an $[n, \begin{bmatrix} n \\ n-t \end{bmatrix}_q, t, 1]$ linear A-code over $\boldsymbol{F}_q$. □

If we take $n = 2$ and $t = 1$, then $\begin{bmatrix} 2 \\ 1 \end{bmatrix}_q = q + 1$. We obtain a $[2, q+1, 1, 1]$ linear A-code. In other words, we have a linear A-code $(\mathcal{S}, \mathcal{E}, \mathcal{A})$ with the following parameters:

$$|\mathcal{S}| = q + 1, \quad |\mathcal{E}| = q^2, \quad |\mathcal{A}| = q, \quad \text{and} \quad P_I = P_S = 1/q.$$

We note that A-codes with these parameters were first constructed by Gilbert, MacWilliams, and Sloane [10]. Their construction uses projective planes and works as follows. Let q be a prime power. Consider the projective plane $\boldsymbol{PG}(2, \boldsymbol{F}_q)$ over the fields $\boldsymbol{F}_q$. Fix a line ℓ in $\boldsymbol{PG}(2, \boldsymbol{F}_q)$. The points on ℓ are regarded as source states, points not lying on ℓ are regarded as the encoding rules (i.e., key), and the lines different from ℓ are regarded as the messages $m = (s, e)$. This results in an A-code with $q+1$ source states, q^2 authentication keys, and q authenticators. The deception probabilities of this code are

$$P_I = P_S = 1/q.$$

On the other hand, choosing different values of t in Corollary 5.1 results in linear A-codes with different parameters.

The following result improves the bound in Theorem 5.1 when $d \geq 2$.

Theorem 5.2: For an $[n, M, t, d]$ linear A-code over $\boldsymbol{F}_q$, we have

$$M[n, t, d, q] \leq \frac{\begin{bmatrix} n \\ n-(t+d)+1 \end{bmatrix}_q}{\begin{bmatrix} n-t \\ n-(t+d)+1 \end{bmatrix}_q}.$$

Proof: From Theorem 4.1, we know that there is an $[n, M, t, d]$ linear A-code if and only if there is a family of subspaces of $V(n, q)$, $\mathcal{L} = \{L_1, L_2, \ldots, L_M\}$ with $\mathbf{dim}(V_i) = n - t$ and $\mathbf{dim}(V_i \cap V_j) \leq n - (t + d)$. For each i, $1 \leq i \leq M$, let $\mathcal{R}_i$ denote the family of subspace of V_i of dimension $n - (t + d) + 1$. It follows that

$$|\mathcal{R}_i| = \begin{bmatrix} n-t \\ n-(t+d)+1 \end{bmatrix}_q.$$

We claim that

$$\mathcal{R}_i \cap \mathcal{R}_j = \emptyset, \qquad \forall i \neq j.$$

Otherwise, if $C \in \mathcal{R}_i \cap \mathcal{R}_j$ is a subspace of dimension $n-(t+d)+1$, then C is a subspace of both L_i and L_j which contradicts the assumption that $\mathbf{dim}(V_i \cap V_j) \leq n - (t + d)$. We then have

$$\begin{bmatrix} n \\ n-(t+d)+1 \end{bmatrix}_q \geq \left| \bigcup_{i=1}^{M} \mathcal{R}_i \right| = M|\mathcal{R}_i| = M \begin{bmatrix} n-t \\ n-(t+d)+1 \end{bmatrix}_q.$$

The desired result follows immediately. □

For any fixed n and k, as $q \to \infty$ we have

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)} \approx q^{(n-k)k}.$$

It follows that

$$M \leq \begin{bmatrix} n \\ n-(t+d)+1 \end{bmatrix}_q \Big/ \begin{bmatrix} n-t \\ n-(t+d)+1 \end{bmatrix}_q \approx \frac{q^{(n-(t+d)+1)(t+d-1)}}{q^{(n-(t+d)+1)(d-1)}} = q^{(n-(t+d)+1)t}. \tag{1}$$

In the next section, we give a construction that meets the asymptotic bound in (1).

It is also worth pointing out that while in the general theory of A-codes it is possible that the size of source states grows exponentially with the size of the key, for example, the construction based on universal hash family (see, for example, [27], [2], [26], [28]). Because of the structure restriction, this will not be true for linear A-codes. In fact, from Theorem 4.1, it is easy to see that $\log_q |\mathcal{S}| \leq n^2 = (\log_q |\mathcal{E}|)^2$, and this bound can be asymptotically achieved. For example, if $(t+d) - 1 \approx t \approx n/2$, then, as we will show in the next section, we have a linear A-code with $\log_q M(n, t, d, q) \approx n^2/4$.

VI. Constructions

Rank distance codes [9] have been used to construct distributed authentication schemes such as A^2-codes by Johansson [12] and group authentication by van Dijk *et al.* [8]. Inspired by their work, we show that linear A-codes can be constructed

from rank distance codes. It turns out that such constructions result in linear A-codes that asymptotically meet the bound in the previous session.

We first review rank distance codes studied by Gabidulin in [9]. Let $\Lambda = \{A_i\}$ be a set of m by r matrices over $\boldsymbol{F}_q$. The distance $d(A, B)$ between two matrices A and B in Λ is defined by $d(A, B) = \mathbf{rank}(A - B)$ and the minimum distance of Λ, denoted by $d(\Lambda)$, is defined as

$$d(\Lambda) = \min_{\substack{A, B \in \Lambda \\ A \neq B}} d(A, B).$$

Let $d = d(\Lambda)$ and $M = |\Lambda|$. We call Λ an $(m \times t, M, d)$ *rank distance code*. The following theorem establishes the relation between linear A-codes and rank distance codes.

Theorem 6.1: If there exists an $(m \times t, M, d)$ rank distance code over $\boldsymbol{F}_q$, then there exists an $[m+t, M, t, d]$ linear A-code over $\boldsymbol{F}_q$.

Proof: Let Λ be an $(m \times t, M, d)$ rank distance code. We define a set of $t + m$ by t matrices

$$\Phi = \left\{ \begin{pmatrix} I_t \\ A \end{pmatrix} \middle| A \in \Lambda \right\}$$

where I_t denotes the t by t identity matrix. For each $\binom{I_t}{A} \in \Phi$, we define

$$\mathbf{Ker}\begin{pmatrix} I_t \\ A \end{pmatrix} = \left\{ (e_1, e_2) \in \boldsymbol{F}_q^{t+m} \middle| (e_1, e_2)\begin{pmatrix} I_t \\ A \end{pmatrix} = 0 \right\}$$

where $e_1 \in \boldsymbol{F}_q^t$ and $e_2 \in \boldsymbol{F}_q^m$. We consider the set of subspaces of $\boldsymbol{F}_q^{r+m}$

$$\mathcal{L} = \left\{ \mathbf{Ker}\begin{pmatrix} I_t \\ A \end{pmatrix} \middle| \begin{pmatrix} I_t \\ A \end{pmatrix} \in \Phi \right\}.$$

Clearly, $|\mathcal{L}| = M$ and $\mathbf{dim}\left(\mathbf{Ker}\binom{I_t}{A}\right) = m$, we show that for any $A, B \in \Lambda$

$$\mathbf{dim}\left(\mathbf{Ker}\begin{pmatrix} I_t \\ A \end{pmatrix} \bigcap \mathbf{Ker}\begin{pmatrix} I_t \\ B \end{pmatrix}\right) \leq m - d.$$

Indeed

$$\begin{aligned} \left| L_A \bigcap L_B \right| &= \left| \mathbf{Ker}\begin{pmatrix} I_t \\ A \end{pmatrix} \bigcap \mathbf{Ker}\begin{pmatrix} I_t \\ B \end{pmatrix} \right| \\ &= \left| \left\{ (e_1, e_2) \in \boldsymbol{F}_q^{t+m} \middle| (e_1, e_2)\begin{pmatrix} I_t \\ A \end{pmatrix} = 0, \right. \right. \\ &\qquad \left. \left. (e_1, e_2)\begin{pmatrix} I_t \\ B \end{pmatrix} = 0 \right\} \right| \\ &= |\{(-e_2 A, e_2) \in \boldsymbol{F}_q^{t+m} \,|\, e_2 A = e_2 B\}| \\ &= |\{e_2 \in \boldsymbol{F}_q^m | e_2(A - B) = 0\}| \\ &= q^{m - \mathbf{rank}(A-B)} \leq q^{m-d}. \end{aligned}$$

From Theorem 4.1, we know that $(\Phi, \boldsymbol{F}_q^{t+m}, \boldsymbol{F}_q^t)$ is a $[t + m, M, t, d]$ linear A-code and the claimed result follows. □

As shown in [12], in an $(m \times t, M, d)$ rank distance code, we always have $d \leq m - k + 1$, where $k = \log_{q^t} M$. Codes for which the equality holds are called *maximum-rank-distance codes* (or MRD-codes for short). Johansson [12] showed that MRD-codes can be constructed from linearlized polynomials.

Recall that a polynomial of the form $F(z) = \sum_{i=0}^{m} f_i z^{q^i}$, where $f_i \in \boldsymbol{F}_{q^t}$ is called a *linearized polynomial* over $\boldsymbol{F}_{q^t}$. Let k, m, t be integers satisfying $0 < k \leq m \leq t$. By $P_{k,m,t}$, we denote the set of all linearized polynomials of degree at most q^{k-1}. Assume that $g_1, g_2, \ldots, g_m$ are specified elements of the field $\boldsymbol{F}_{q^t}$ which are linearly independent over $\boldsymbol{F}_q$. For each $F(z) \in P_{k,m,t}$, set

$$c_{F(z)} = \begin{pmatrix} F(g_1) \\ F(g_2) \\ \vdots \\ F(g_m) \end{pmatrix}.$$

We associate $c_{F(z)}$ with an $m \times t$ matrix $A(c_{F(z)}) = (a_{ij})$, which is obtained by writing $F(g_i)$ (expressed in a fixed base) as a row vector with entries $a_{ij} \in \boldsymbol{F}_q$.

Lemma 6.1 [12]: $\{A(c_{F(z)}) | F(z) \in P_{k,m,t}\}$ is an MRD-code. That is, $\{A(c_{F(z)}) \,|\, F(z) \in P_{k,m,t}\}$ is an $(m \times r, q^{tk}, m - k + 1)$ rank distance code.

Corollary 6.1: Let n, t, d be integers satisfying $0 < t + d \leq n$ and let q be a prime. The above construction from linearized polynomials results in a $[n, q^{t(n-t-d+1)}, t, d]$ linear A-code.

Proof: Put $k = n - t - d + 1$ and $m = n - t$. Applying Theorem 6.1 and Lemma 6.1, we obtain the desired result. □

Example 6.1: Choosing $n = 2$ and $t = d = 1$, we have a linear A-code $(\mathcal{S}, \mathcal{E}, \mathcal{A})$ with $|\mathcal{S}| = q$, $|\mathcal{E}| = q^2$, and $|\mathcal{A}| = q$, with $P_I = P_S = 1/q$. The code has the same parameters as the A-code $\mathcal{C} = (\mathcal{S}, \mathcal{E}, \mathcal{A}, F)$, where $\mathcal{S} = \boldsymbol{F}_q$, $\mathcal{A} = \boldsymbol{F}_q$, $\mathcal{E} = \boldsymbol{F}_q \times \boldsymbol{F}_q$, and f defined as $f(s, (e_1, e_2)) = e_1 \cdot s + e_2$, $\forall s \in \mathcal{S}$, $(e_1, e_2) \in \mathcal{E}$. It is easy to verify that $\mathcal{C}$ is linear and $P_I = P_S = 1/q$.

Comparing Corollary 6.1 with Bound (1), we get the following result.

Corollary 6.2: The parameters given in Corollary 6.1 asymptotically meet the bounds in Theorem 5.2.

VII. Applications

Linear A-codes have been implicitly used in constructing distributed authentication schemes, for example, A^2-codes [12], group authentication schemes [16], [8] and one-time fail-stop signatures [20]. With appropriate modification, these constructions can be generalized to *any* linear A-codes. In this section, we show how linear A-codes can be used as a building block for constructing group authentication schemes and broadcast authentication systems.

A. Group Authentication Schemes

Group authentication schemes, also known as *threshold authentication* schemes, were introduced by Desmedt *et al.* [7] to generalize conventional A-codes. In a group authentication scheme, there are multiple senders and the generation of authenticator requires collaboration of an authorized subset of senders. In a (k, ℓ) threshold authentication scheme, there are ℓ senders and generation of authenticator for a message requires collaboration of at least k senders. A general method of constructing a

threshold authentication system is by combining a (k, ℓ) secret sharing scheme [21] and an A-code, by sharing the authentication key among the n senders. It is known that a direct combination will fail to fulfill the security requirement of such systems; and caution must be exercised in regard to the authentication operation for the generation of authenticator such that one cannot recover the underlying authentication key even if he/she has seen the authenticated message from the authorized group. To the best of our knowledge, all the previous constructions use Shamir's secret sharing and some particular examples of linear A-codes [7], [8]. We show that this construction method is generic in the sense that one can always construct group authentication schemes by combining *any* linear A-codes and a (linear) secret sharing scheme.

The construction of a (k, ℓ) group authentication scheme proceeds as follows. Let $(\mathcal{S}, \mathcal{E}, \mathcal{A}, f)$ be an $[n, M, t, d]$ linear A-code over $\boldsymbol{F}_q$. Assume that there are n senders $P_1, \ldots, P_\ell$ and a receiver R. Assume $q > \ell$ and $x_1, x_2, \ldots, x_\ell$ are ℓ distinct elements of $\boldsymbol{F}_q$ (x_i is associated to P_i). Let $e_0, e_1, \ldots, e_{k-1}$ be k random values in $\mathcal{E}$. The key of R is e_0 and the key of P_i is

$$\alpha_i = \sum_{j=0}^{k-1} x_i^j e_j. \tag{2}$$

Since $\mathcal{E}$ is an n-dimensional vector space over $\boldsymbol{F}_q$, the right-hand side of (2) is well defined. Assume that k senders $P_{i_1}, \ldots, P_{i_t}$ want to authenticate a message $s \in \mathcal{S}$. Each P_{i_j} computes

$$b_{i_j} = \prod_{u \in B,\, u \neq i_j} \frac{-x_u}{(x_{i_j} - x_u)} \cdot \alpha_{i_j}$$

and sends $a_{i_j} = f(s, b_{i_j})$ to the receiver R, where $B = \{i_1, \ldots i_k\}$. The receiver computes $a = \sum_{j=1}^{k} a_{i_j}$ and accepts s as authentic if $a = f(s, e_o)$.

The security proof of the above schemes is similar to [8]. Thus, various group A-codes can be obtained through different choices of the underlying linear A-codes. In general, we can always combine a linear A-code and a linear secret sharing scheme to construct a group A-code.

B. Broadcast Authentication Schemes

Broadcast A-codes (also called *multireceiver A-codes*) [7] are another extension of conventional A-codes. In a broadcast A-code, there are multiple receivers, and a sender can authenticate a message to all receivers by broadcasting a message in such a way that each receiver can individually verify the authenticity of the message. An obvious solution is to use a conventional A-code and give all receivers the same key of the A-code. The sender can just broadcast the authenticated messages of the A-code. This is not secure because a receiver can impersonate the sender and send fraudulent messages to other receiver. Another solution is to choose individual authentication keys for each receiver to share with the sender. To authenticate a message, the sender generates all the authenticators for all the keys, and broadcasts the concatenation of them which each receiver can verify its authenticity through his/her corresponding component. This solution, although secure, is very inefficient when the group of receivers is large as the number of keys and the length of broadcast increase linearly with the number of receivers.

Desmedt *et al.* [7] gave a solution that achieves both efficiency and security. To guarantee the efficiency, they relaxed the security requirement to the threshold security; namely, it is assumed that the number of the malicious receivers (who might collude to attack the system) is bounded by some threshold parameter. More precisely, in a (k, ℓ) broadcast A-code, there are ℓ receivers in which at most $k-1$ malicious receivers might try to attack the system. A (k, ℓ) broadcast A-code was constructed in [7] using the linear A-code of Example 6.1. We will generalize this construction method for general linear A-codes.

Let $(\mathcal{S}, \mathcal{E}, \mathcal{A}, f)$ be a linear A-code over $\boldsymbol{F}_q$. A (k, ℓ) broadcast A-code using $(\mathcal{S}, \mathcal{E}, \mathcal{A}, f)$ can be constructed as follows. Let $R_1, \ldots, R_\ell$ denote ℓ receivers and let T be the sender. The key for the sender T is a k-tuple $(e_0, e_1, \ldots, e_{k-1}) \in \mathcal{E}^k$, and the key for R_i, $1 \leq i \leq \ell$ is

$$\alpha_i = \sum_{j=0}^{k-1} x_i^j e_j$$

where $x_1, x_2, \ldots, x_\ell$ are ℓ public, distinct elements of $\boldsymbol{F}_q$. To authenticate a message s, the sender broadcasts the authenticator $(a_0, a_1, \ldots a_{k-1}) \in \mathcal{A}^k$ to all receivers, where $a_j = f(s, e_j)$, for $j = 0, 1, \ldots, k-1$. Upon receiving the broadcast message, R_i accepts s as authentic if

$$\sum_{j=0}^{k-1} x_i^j a_j = f(s, \alpha_i).$$

Again, using a proof similar to [7], it is not difficult to prove the security of the above construction. We emphasize that in this construction the key size of the sender and the size of broadcast grows linearly with k, the security parameter of the system, rather than ℓ, the number of receivers in the previous trivial solution. By choosing efficient underlying linear A-codes, we obtain more efficient broadcast A-codes than previous known schemes.

VIII. Conclusion

Linear A-codes are a new, interesting class of A-codes. We have shown that such A-codes can be characterized in terms of families of subspaces of vector spaces over finite fields. We derived an upper bound on the number of source states of these codes and gave constructions that asymptotically meet the bound. However, the construction that is closed to the asymptotic bound is only when q, the size field, is sufficiently large. An interesting research problem is whether the bound in Theorem 5.2 can be met for general q, and in particular, when q is small.

A linear A-code $\mathcal{C} = (\mathcal{S}, \mathcal{E}, \mathcal{A}, f)$ is defined using vector spaces over finite fields. Another interesting question is: if we relax the underlying algebraic structure from a finite field to an Abelian group (or modules over a ring), can we improve the bound of Theorem 5.2 or give other nontrivial constructions?

We believe linear A-codes can be used in other distributed systems in which A-codes play a role and so exploring such applications needs further work.

ACKNOWLEDGMENT

The authors wish to thank H. Niederreiter for useful discussions that led to the proof of Theorem 5.2, and C. Ding for his interest in this work. The also wish to thank the reviewer for his/her insightful suggestions which improved the presentation of the paper.

REFERENCES

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

[2] 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.

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

[4] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *J. Comput. Syst. Sci.*, vol. 18, pp. 143–154, 1979.

[5] B. den Boer, "A simple and key-economical unconditional authentication scheme," *J. Comput. Security*, vol. 2, pp. 65–71, 1993.

[6] Y. Desmedt, "Society and group oriented cryptology: A new concept," in *Advances in Cryptography—CRYPTO '87 (Lecture Notes in Computer Science)*. Berlin, Germany: Sprilnger-Verlag, 1988, vol. 293, pp. 120–127.

[7] Y. Desmedt, Y. Frankel, and M. Yung, "Multi-receiver/Multi-sender network security: Efficient authenticated multicast/feedback," in *Proc. IEEE INFOCOM'92*, 1992, pp. 2045–2054.

[8] M. van Dijk, C. Gehrmann, and B. Smeets, "Unconditionally secure group authentication," *Des., Codes Cryptogr.*, vol. 14, pp. 281–296, 1998.

[9] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Probl. Inform. Transm.*, vol. 21, no. 1, pp. 1–12, 1985.

[10] E. N. Gilbert, F. J. MacWilliams, and N. J. A. Sloane, "Codes which detect deception," *Bell Syst. Tech. J.*, vol. 33, pp. 405–424, 1974.

[11] T. Johansson, "Contributions to unconditionally secure authentication," Ph.D. dissertation, Lund Univ., Lund, Sweden, 1994.

[12] ——, "Authentication codes for nontrusting parties obtained from rank metric codes," *Des., Codes Cryptogr.*, vol. 6, pp. 205–218, 1995.

[13] ——, "Further results on asymmetric authentication schemes," *Inform. Comput.*, vol. 151, no. 1/2, pp. 100–133, 1999.

[14] G. Kabatianskii, B. Smeets, and T. Johansson, "On the cardinality of systematic authentication codes via error correcting," *IEEE Trans. Inform. Theory*, vol. 42, pp. 566–578, Mar. 1996.

[15] F. J. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[16] K. Martin and R. Safavi-Naini, "Multisender authentication schemes with unconditional security," in *Information and Communications Security (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1997, vol. 1334, pp. 130–143.

[17] R. Safavi-Naini, "Three systems for shared generation of authenticators," *Des., Codes Cryptogr.*, vol. 13, 1998.

[18] R. Safavi-Naini and H. Wang, "New results on multi-receiver authentication codes," in *Advances in Cryptology—Eurocrypt '98 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1998, vol. 1438, pp. 527–541.

[19] ——, "Multireceiver authentication codes: Models, bounds, constructions and extensions," *Inform. Comput.*, vol. 151, no. 1/2, pp. 148–172, 1999.

[20] R. Safavi-Naini, W. Susilo, and H. Wang, "Fail-stop signature for long messages," in *Indocrypt'00 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2000, vol. 1977, pp. 165–177.

[21] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, pp. 612–613, 1979.

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

[23] ——, "A survey of information authentication," in *Contemporary Cryptology, The Science of Information Integrity*, G. J. Simmons, Ed. Piscataway, NJ: IEEE Press, 1992, pp. 379–419.

[24] B. Smeets, P. Vanroose, and Z.-X. Wan, "On the construction of authentication codes with secrecy and codes withstanding spoofing attacks of order $L \geq 2$," in *Advances in Cryptology—Eurocrypt '90 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1990, vol. 473, pp. 306–312.

[25] D. R. Stinson, "The combinatorics of authentication and secrecy codes," *J. Cryptol.*, vol. 2, pp. 23–49, 1990.

[26] ——, "Universal hashing and authentication codes," *Codes Cryptogr.*, vol. 4, pp. 369–380, 1994.

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

[28] C. Xing, H. Wang, and K. Y. Lam, "Constructions of authentication codes from algebraic curves over finite fields," *IEEE Trans. Inform. Theory*, vol. 46, pp. 886–892, May 2000.