Linear Authentication Codes from Free Modules: Bounds and Constructions

Xiuli Wang
Civil Aviation University of China
Science College
Jinbei Road 2898, 300300 Tianjin
China
xlwang@cauc.edu.cn

Abstract: In this paper, we principally introduce a new class of unconditionally secure authentication codes, called linear authentication codes(or linear A-codes)from free modules. 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 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. We realize the generalization of linear authentication codes from vector space over field to free modules over ring.

Key–Words: Authentication codes(A-codes), Distributed A-codes, Multi-receiver A-codes, Multi-sender A-codes, Free modules, Ring

1 Introduction

Modules is a kind of algebra structure over ring, linear space is a kind of algebra structure over field, ring is the generalization of field, modules is the generalization of linear space, linear space and modules have a lot of similar properties. Linear space has a basis, but modules may not have a basis, so we introduce a kind of modules with a basis, it is called free modules. Thus the properties of linear space about basis can be generalized to free modules. In this paper, we generalize linear authentication codes over finite field to free modules over a commutative ring with a identity element 1 and having no zero divisor. Free modules have a basis and their algebraic structure is similar to vector space, the definition of modules is as follows:

Let R be a ring. A left $R-$module M is an additive abelian group M together with a mapping $M \times R \to M$ with $(m, r) \mapsto mr$, called module scalar multiplication, for which we have

(1) Associative law: $r(sm) = (rs)m$,

(2) Distributive laws:$r(m+n) = rm+rn$, $(m+n)r = mr+nr$,

(3) Unitary law:$1m = m$.

In the above m, n are arbitrary elements from M and r, s are arbitrary elements from R. If a nonempty subset N of a $R-$module M is closed for addition and scalar multiplication, then N is called a submodule of M. If a module has a basis, it is called a free module. More properties of modules, see [6]. R_q means a commutative ring R with q elements and identity element 1 and no zero divisors in this paper, that is a finite domain ring, it is clearly a principal ideal ring, a submodule of a free module over a principal ideal domain ring still is a free module[17]. 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 free modules, and a source state to induce a homomorphism (or 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 free modules over ring such that the dimension of the intersection of a pair of such free submodules does not exceed a certain desired value (security parameter). We derive an upper bound authentication systems. On the number of possible source states of an A-code for given 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.

A-codes were first considered by Gilbert, MacWilliams and Sloane. Development of the general theory of unconditionally secure authentication systems has been initiated by a number of authors(see, for example,[1-5]).

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 millage 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 $f:\mathcal{S}\times\mathcal{E}\rightarrow\mathcal{A}$. 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 message with the receiver, he transmits the message (s,a), where $s\in\mathcal{S}$ and $a=f(s,e)\in\mathcal{A}$. When the receiver receives (s,a), she checks the authenticity of the message by verifying whether $a=f(s,e)\in\mathcal{A}$ 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, the receiver and the transmitter will choose a probability distribution for $\mathcal{E}$. We will denote the probability of success of the opponent impersonation and substitution attacks by P_I and P_S, respectively. Then we have

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

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

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:

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

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

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.

2 LINEAR A-CODES OVER FREE MODULES

Consider an A-codes $(\mathcal{S},\mathcal{E},\mathcal{A},f)$. For each key $e\in\mathcal{E}$, the authentication function $f:S\times\mathcal{E}\rightarrow\mathcal{A}$ 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-codes $(\mathcal{S},\mathcal{E},\mathcal{A},f)$ can be characterized completely by the family of mappings $\{\Psi_e|e\in\mathcal{E}\}$, and vice versa.

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 Ψ_s from $\mathcal{E}$ to $\mathcal{A}$ defined by $\Psi_s(e)=f(s,e),\forall s\in\mathcal{S}$. Then, again, the A-code$(\mathcal{S},\mathcal{E},\mathcal{A},f)$ can be characterized by a family of mapping $\Psi=\{\Psi_s|s\in\mathcal{S}\}$. 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 free module over R_q, and Ψ is a family of R_q-homomorphism(or linear mapping) 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 1 *An A-code $(\mathcal{S},\mathcal{E},\mathcal{A},f)$ is linear over free modules if*

i) $\mathcal{E}$ and $\mathcal{A}$ are finite-dimensional free modules over R_q;

ii) for every $s\in\mathcal{S}$, defined by $\Psi_e(s)=f(s,e)$ is an R_q-homomorphism from $\mathcal{E}$ to $\mathcal{A}$.

We identify $\mathcal{S}$ with $\Psi=\{\Psi_s|s\in\mathcal{S}\}$, and write the A-code as $(\mathcal{S},\mathcal{E},\mathcal{A},f)$ to emphasize that the source states are represented as homomorphism. We may assume that $\mathcal{E}=R^n$ and $\mathcal{A}=R^m$. Given a basis $a_1,a_2,a_3,a_4...,a_n$ of $\mathcal{A}$, a homomorphism $\phi\in\Phi$ can be represented by a unique $n\times m$ matrix $\mathcal{A}$ over a commutative ring with a identity element 1 and having no zero divisor such that $\Psi(e)=eA,\forall e\in\mathcal{E}$. If V and W are two free modules over R_q, and is a homomorphism from V to W, we will denote $Ker(\Psi)=\{v\in V|\Psi(v)=0\}$. Obviously, $Ker(\Psi)$ is a free submodule of $FM(FM$ means free modules in this paper) and its dimension is denoted by $dimKer(\Psi)$.

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

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

where

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

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 attack, we have

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

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

Lemma 2 *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 $e_0 \in \{e|\phi(e) = a\} \cap \{\phi'(e) = a'\}$. 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 τ from $\{e|\phi(e) = 0\} \cap \{e|\phi'(e) = 0\}$ to $\{e|\phi(e) = a\} \cap \{e|\phi'(e) = a'\}$ by $\tau(e) = e + e_0$. Again, τ 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 2, P_S can be rewritten as

$$P_S = \max_{\phi,\phi' \in \Phi, \phi \neq \phi'} \max_{a,a' \in \mathcal{A}} \tfrac{|\{e|\phi(e)=0\} \cap \{e|\phi'(e)=0\}|}{|\{e|\phi(e)=0\}|}.$$

3 INTERPRETING A LINEAR A-CODE AS A FAMILY OF FREE SUBMODULES

Definition 3 *[12] An A-code$(\mathcal{S}, \mathcal{E}, \mathcal{A}, f)$ is called I-equitable if it has the additional property that $\forall s \in \mathcal{S}, a \in \mathcal{A}$, $P_I = \frac{|\{e|f(s,e)=a\}|}{|\mathcal{E}|}$.*

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

Lemma 4 *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 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

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

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

On the other hand,

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

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, 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 homomorphism from $\mathcal{E}$ to $\mathcal{A}$. Indeed, for a given $\phi_0 \in \Phi$, let $L_0 = Im(\phi_0) \subseteq \mathcal{A}$. If there exists $\phi \in \Phi$ and $\phi \neq \phi_0$ such that $Im(\phi) \neq L_0$, since the A-code is I-equitable, we know that $dim(Im(\phi)) = dim(L_0)$, It follows that there exists an isomorphism θ from $Im(\phi)$ to L_0 and $\theta\phi$ is an R_q-homomorphism from $\mathcal{E}$ to $\mathcal{A}$ and $Ker(\theta\phi) = Ker(\phi_0)$. 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 a surjective homomorphism from $\mathcal{E}$ to L_0.

Let $FM(n, q)$ denote the n-dimensional free module (whose basis has n linear independent elements) over R_q.

Theorem 5 *A linear A-code $(\mathcal{S}, \mathcal{E}, \mathcal{A})$ is called an $[n, M, t, d]$ linear A-code if and only if there exists a family of free submodules of $FM(n, q)$*

$$\mathcal{L} = \{L|L \textit{ is a free submodule of } FM(\alpha, q)\}$$

such that

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

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

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

Proof: Consider an $[n, M, t, d]$ linear A-code $\mathcal{C} = (\Phi, \mathcal{E}, \mathcal{A})$ and let $\mathcal{L}$=$\{Ker(\phi)|\phi \in \phi\}$. Since $\mathcal{C}$ is I-equitable, $P_I = \frac{1}{q^{n-dim(Ker(\phi))}} = q^{-t}$, and so $\dim(Ker(\phi)) = n - t, \forall \phi \in \Phi$. From lemma 2, we know

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

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

Conversely, if there is a family $\mathcal{L}$ of free submodule of $FM(\alpha, q)$ such that conditions i)-iii) are satisfied, then we take $\mathcal{E}$=$FM(n, q)$ and $\mathcal{A}$=$FM(t, q)$. For each free submodule $L \in \mathcal{L}$, there exists an R_q -homomorphism from $\mathcal{E}$ to $\mathcal{A}$ such that $L = Ker(\phi)$. Let Φ=$\{\phi_L|L \in \mathcal{L}\}$. Then it is straightforward to verify that $(\Phi, \mathcal{E}, \mathcal{A})$ is an linear A-code.

4 BOUNDS ON LINEAR A-CODES OVER FREE MODULES

In an $[n, M, t, d]$ linear A-code over R_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 R_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 free submodule of R_q is $\begin{bmatrix} n \\ k \end{bmatrix}_q$, which gives an upper bound for $M = (n, t, d, q)$.

Theorem 6 *For any integer* n, t, d *with* $n \geq t \geq d$ *and prime power q, we have*

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

Theorem 7 $M = (n, t, 1, q) = \begin{bmatrix} n \\ n-t \end{bmatrix}_q.$

Proof: Let $\mathcal{L}$ be the set of all $(n - t)$-dimensional subspaces of the n-dimensional free submodule $FM(n, q)$. Then $|\mathcal{L}|$=$\begin{bmatrix} \alpha \\ \alpha-\gamma \end{bmatrix}_q$. Since for any $L, L' \in \mathcal{L}, L \neq L'$,$\dim(L \cap L') \leq \alpha - \gamma - 1$, from Theorem 5, we know that there exists an $[n, \begin{bmatrix} n \\ n-t \end{bmatrix}_q, t, 1]$ linear A-code over R_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:

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

Choosing different values of t in Theorem 7 results in linear A-codes with different parameters.

The following result improve the bound in Theorem 6 when $d \geq 2$.

Theorem 8 *For an* $[n, M, t, d]$ *linear A-code over* R_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 5, we know that there is an $[n, M, t, d]$ linear A-code if and only if there is a family of free submodule of $FM(n, q)$, $\mathcal{L}$=$L_1, L_2, \cdots L_M$ with $dim((FM)_i) = n - t$ and $dim((FM)_i \cap (FM)_j) \leq n - (t + d)$. For each $i, 1 \leq i \leq M$, let R_i denote the family of free submodule $(FM)_i$ of dimension $n-(t+d)+1$. It follows that

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

We claim that $R_i \cap R_j = \emptyset, \forall i \neq j$. Otherwise, if $C \in R_i \cap R_j$ is a free submodule of dimension $n-(t+d)+1$, then C is a free submodule of both L_i and L_j which contradicts the assumption that $\dim((FM)_i \cap (FM)_j) \leq n - (t + d)$. We then have

$$\begin{aligned} \begin{bmatrix} n \\ n-(t+d)+1 \end{bmatrix}_q &\geq |\bigcup_{i=1}^{M} R_i| = M|R_i| \\ &= M \begin{bmatrix} n-t \\ n-(t+d)+1 \end{bmatrix}_q. \end{aligned}$$

The desired result follows immediately.

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

$$\left[\begin{array}{c} n \\ k \end{array}\right]_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)} \approx q^{(n-k)k}.$$

It follows that

$$M \leq \left[\begin{array}{c} n \\ n-(t+d)+1 \end{array}\right]_q \Big/ \left[\begin{array}{c} n-t \\ n-(t+d)+1 \end{array}\right]_q$$
$$\approx \frac{q^{(n-(t+d)+1)(t+d-1)}}{q^{(n-(t+d)+1)(d-1)}} = q^{(n-(t+d)+1)t}. \tag{1}$$

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

5 CONSTRUCTIONS

We will show that linear A-code 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 [11]. Let $\Lambda = \{A_i\}$ be a set of m by r matrices over R_q. The distance $d(A,B)$ between two matrices A and B in Λ is defined by $d(A,B) = rank(A-B)$ and the minimum distance of Λ, denoted by $d(\Lambda)$, is defined as

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

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 9 *If there exists an $(m \times t, M, d)$ rank distance code over R_q, then there exists an $[m + t, M, t, d]$ linear A-code over R_q.*

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

$$\Phi = \left\{ \left(\begin{array}{c} I_t \\ A \end{array} \right) | A \in \Lambda \right\}$$

where I_t denotes the t by t identity matrix. For each $(I_t, A)^T \in \Phi$, we define

$$Ker \left(\begin{array}{c} I_t \\ A \end{array} \right)$$
$$= \left\{ (e_1, e_2) \in R_q^{t+m} | (e_1, e_2) \left(\begin{array}{c} I_t \\ A \end{array} \right) = 0 \right\}$$

where $e_1 \in R_q^t$ and $e_2 \in R_q^m$. We consider the set of free submodules of R_q^{t+m}.

$$\mathcal{L} = \{ Ker \left(\begin{array}{c} I_t \\ A \end{array} \right) | \left(\begin{array}{c} I_t \\ A \end{array} \right) \in \Phi \}.$$

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

$$\dim(Ker \left(\begin{array}{c} I_t \\ A \end{array} \right) \cap Ker \left(\begin{array}{c} I_t \\ B \end{array} \right)) \leq m - d.$$

Indeed

$$|L_A \cap L_B| = |Ker \left(\begin{array}{c} I_t \\ A \end{array} \right) \cap Ker \left(\begin{array}{c} I_t \\ B \end{array} \right)|$$
$$= |\{(e_1, e_2) \in R_q^{t+m} | (e_1, e_2) \left(\begin{array}{c} I_t \\ A \end{array} \right) = 0,$$
$$(e_1, e_2) \left(\begin{array}{c} I_t \\ B \end{array} \right) = 0\}|$$
$$= |\{(-e_2 A, e_2) \in R_q^{t+m} | e_2 A = e_2 B\}|$$
$$= |\{e_2 \in R_q^m | e_2(A-B) = 0\}|$$
$$= q^{m-rank(A-B)} \leq q^{m-d}.$$

From Theorem 5, we know that (Φ, R_q^{t+m}, R_q^t) is a $[t + m, M, t, d]$ linear A-code and the claimed result follows. □

Johansson[8] show that MRD-codes can be constructed from linearized polynomials.

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

$$c_{F(z)} = \left(\begin{array}{c} F(g_1) \\ F(g_2) \\ \vdots \\ F(g_m) \end{array} \right).$$

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 $a_{ij} \in R_q$.

Lemma 10 [9] *$\{A(c_{F(z)}) | F(z) \in P_{k,m,t}\}$ 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.*

Theorem 11 *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 9 and Lemma 10, we obtain the desired result. □

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 $P_I = P_S = \frac{1}{q}$. The code has the same parameters as the A-code $\mathcal{C} = (\mathcal{S}, \mathcal{E}, \mathcal{A}$,f), where $\mathcal{S} = R_q \times R_q$ and f defined as $f(s, (e_1, e_2)) = e_1 s + e_2, \forall s \in \mathcal{S}, (e_1, e_2) \in \mathcal{E}$. It is easy to verify that $\mathcal{C}$ is linear and $P_I = P_S = \frac{1}{q}$.

Comparing Theorem 11 with Bound (1), we get the following result.

Theorem 12 *The parameters given in Theorem 11 asymptotically meet the bounds in Theorem 8.*

The end of this section, we give the relation about orthogonal arrays and linear codes from free module over R_q. It is a generalization of linear codes from linear space over F_q(it means a field including q elements).

Definition 13 *Let X be symbol set of cardinality $|X| = n \geq 1$ and let $k \geq 2$. An orthogonal array $OA(n, k)$ is an $N \times k$ array A with entries from X such that within any two column from A, every ordered pair of symbols from X occurs in exactly one row of A.*

A vector $u = (u_1, u_2, \cdots, u_k) \in S^k$, where S is a symbol set of cardinality $|S| = s \geq 1$, S^k is all s^k vectors, in which these vectors's length is k, any subset C of S^k is called a linear code, the vector is called codeword in C, these codewords are closed for addition and scalar multiplication. Nonzero elements number of a vector $u = (u_1, u_2, \cdots, u_k) \in S^k$ is defined as its Hamming weight $w(u)$. Hamming distance $dist(u, v)$ of two vectors $u, v \in S^k$ is defined as the number of different components of the two vectors. Minimum distance of code C is defined as $d = \min_{u,v \in C, u \neq v} dist(u, v)$. The above mentioned the distance $d(A, B)$ between two matrices A and B over R_q is a generalization of Hamming distance $dist(u, v)$ of two vectors $u, v \in R_q$. If C include N codewords, so we call C is a code, denoted by $(k, N, d)_s$, in which k is code length of C, N is the number of codewords in C, d is Minimum distance C and C is defined as a symbol set S.

Let a symbol set S be a R_q, as above, the linear code C from R_q is denoted by (k, N, d). If its dimension is n(non-negative integer), then the size of the code is $N = q^n, 0 \leq n \leq k$. Similarly, if the row of an orthogonal array is different from each other and form a free submodule of R_q^k, then we call the orthogonal array is linear.

For linear code C, its minimum distance is minimum weight of all nonzero codewords:

$$d = \min_{u \in C, u \neq 0} w(u).$$

Let G is a generator matrix of linear code C, that the matrix's row is a basis of linear code C, then all codewords is expressed as $u = xG$, where x is taken over all vectors in R_q^n. For example, the orthogonal array $OA(8, 4)$

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix},$$

its generator matrix is

$$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

Theorem 14 *Let a orthogonal array $OA(n, k)$ is defined as R_q, then any t column is linearly independent in R_q. Otherwise, if A is a $N \times k$ array, its row form a free submodule of R_q^k and any t column of A is linearly independent in R_q, then A is a orthogonal array.*

Proof: Take any t column $v_1, v_2, \cdots, v_t$ of a orthogonal array $OA(n, k)$, suppose

$$c_1 v_1 + c_2 v_2 + \cdots + c_t v_t = 0, c_1, \cdots, c_t \in R_q.$$

There is a row is $(1, 0, \cdots, 0)$ in matrix $(c_1, c_2, \cdots, c_t)$, from the above equation, we can deduce $c_1 = 0$. Similarly, we can deduce $c_2 = \cdots = c_t = 0$. So $v_1, v_2, \cdots, v_t$ is linearly independent in R_q.

Let A is a $N \times k$ array, its row form a free submodule of R_q^k, any t column of A is linearly independent in R_q. There exists an integer $0 \leq n \leq k$ such that $N = q^n$. Let G is a generator matrix of A, it is a $N \times k$ matrix, all row of A is expressed as $\xi G, \xi \in R_q^n$. Take any t column of A, G_1 is expressed as $N \times t$ matrix by corresponding t column in G, then t column of G_1 must be linearly independent in R_q, otherwise, A corresponds t column is linearly dependent, this is not possible. In the corresponding t column in A, the number of occurrences for any t topples z as row in A equal to the number of solutions for the equation $\xi G_1 = z, \xi \in R_q^n$, because the rank of G_1 is t, the number of solutions is q^{n-t}. Therefore, A is a orthogonal array.

Let C is a linear code over R_q, if it has the following property:

$$(c_0, c_1, \cdots, c_{k-1})$$

is a codeword of C, then

$$(c_{k-1}, c_0, \cdots, c_{k-2})$$

is also a codeword of C, we call the code is a circle code.

For a orthogonal array, we also introduce the same definition. For a linearly orthogonal array, if

$$(c_0, c_1, \cdots, c_{k-1})$$

is its row, then

$$(c_{k-1}, c_0, \cdots, c_{k-2})$$

is also its row, now the orthogonal array is called a circle array. The codeword

$$(c_0, c_1, \cdots, c_{k-1})$$

can be expressed as the polynomial

$$c_0 + c_1X + \cdots + c_{k-1}X^{k-1},$$

the codeword

$$(c_{k-1}, c_0, \cdots, c_{k-2})$$

can be expressed as the polynomial

$$X(c_0 + c_1X + \cdots + c_{k-1}X^{k-1})(modX^k - 1),$$

hence the code C is corresponding to a idea I of $R_q[x]/(X^k - 1)$, it is a principal idea, the polynomial $g(X)$ with minimum degree and the leading coefficient equal 1 is a generator of I. All codewords can be expressed as the polynomial $\alpha(X)g(X)$, where $\alpha(X)$ is taken over all polynomials with degree $\leq k - 1 - deg\{g(X)\}$ in R_q. Therefore, we can find the dimension of C is $k - deg\{g(X)\}$. The polynomial $g(X)$ must be a divisor of $X^k - 1$. Otherwise, the greatest common divisor of $g(X)$ and $X^k - 1$ is a polynomial whose degree no more than $deg\{g(X)\}$ in R_q, this contradicts that $g(X)$ is a generator of I.

Similar to the finite field[15], we can construct Reed-Solomon code by circle code in R_q, it is a kind of important linear code. We will do further work for concrete construction in future.

6 APPLICATIONS

Linear A-codes has been implicitly used in constructing distributed authentication schemes, for example, A^2-codes[8],group authentication schemes[7,9] and one-time fail-stop signatures[11]. 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 broadcast authentication systems.

Broadcast A-codes (also called multi-receiver A-codes)[2] 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.[1] 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 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 [1] 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 R_q. A (k, l) broadcast A-code using $(\mathcal{S}, \mathcal{E}, \mathcal{A}, f)$ can be constructed as follows. Let $R_1, \cdots R_l$ denote l receivers and let T be the sender. The key for the sender T is a k-tuple $(e_0, e_1 ..., e_{k-1}) \in \mathcal{E}^k$ and the key for $R_i, 1 \leq i \leq l$ is

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

where $x_1, x_2 \cdots x_l$ are l public distinct elements of $FM(n, q)$. To authenticate a message s, the sender broadcasts the authenticator $(a_0, a_1 \cdots a_{k-1}) \in \mathcal{A}^k$ to all receivers, where $a_j = f(s, e_j)$, for $j = 0, 1 \cdots k-1$. 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 [1], 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.

Multi-sender authentication code is also extension of conventional A-codes. Multi-sender authentication system refers to that a group of senders cooperatively send a message to the receiver, then the receiver should be able to ascertain that the message is authentic. About this case, many scholars had also much researches and had made great contributions to multi-sender authentication codes [1,9]

In the actual computer network communications, multi-sender authentication codes include sequential model and simultaneous model. Sequential model is that each sender uses their own encoding message to the receiver, the receiver receives the message and verifies whether the message is legal or not. Simultaneous model is that all senders use their own encoding rules to encode a source state, and each sender sends the encoded message to the synthesize respectively, then the synthesizer forms an authenticated message and verifies whether the message is legal or not. In this paper, we will adapt to the second model.

In a simultaneous model, there are four participants: a group of senders $P = \{P_1, P_2, \cdots, P_n\}$, the keys distribution center, he responsible for the key distribution to senders and receiver, including solving the disputes between them, a receiver R, a synthesizer, he only runs the trusted synthesis algorithm. The code works as follows: each sender and receiver has their own Cartesian authentication code respectively. Let $(S, E_i, T_i; f_i)(i = 1, 2, \cdots, n)$ be the sender's and Cartesian authentication code, $(S, E_R, T; g)$ be the receiver's Cartesian authentication code, $h : T_1 \times T_2 \times \cdots \times T_n \to T$ be the synthesis algorithm. $\pi_i : E \to E_i$ be a subkey generation algorithm, where E is the key set of the key distribution center. When authenticating a message, the senders and the receiver should comply with the protocol: The key distribution center randomly selects a encoding rule $e \in E$ and sends $e_i = \pi_i(e)$ to the ith sender $P_i(i = 1, 2, \cdots, n)$ secretly, then he calculates e_R by e according to a effective algorithm, and secretly sends e_R to the receiver R; If the senders would like to send a source state s to the receiver R, P_i computes $t_i = f_i(s, e_i)(i = 1, 2, \cdots, n)$ and sends $m_i = (s, t_i)(i = 1, 2, \cdots, n)$ to the synthesizer through an open channel; The synthesizer receives the message $m_i = (s, t_i)(i = 1, 2, \cdots, n)$ and calculates $t = h(t_1, t_2, \cdots, t_n)$ by the synthesis algorithm h, then sends message $m = (s, t)$, he checks the authenticity by verifying whether $t = g(s, e_R)$ or not. If the equality holds, the message is authentic and is accepted. Otherwise, the message is rejected.

We assume that the key distribution center is credible, though he know the senders' and receiver's encoding rules, he will not participate in any communication activities. When transmitters and receiver are disputing, the key distribution center settles it. At the same time, we assume that the system follows the Kirchhoffs principle which except the actual used keys, the other information of the whole system is public.

In the whole system, we assume$\{P_1, P_2, \cdots, P_n\}$ are senders, R is a receiver, E_i is the encoding rules set of the sender P_i, E_R is the decoding rules set of receiver R. If the source state space S and the key space E_R of receiver R are according to a uniform distribution of message space M and tag space T are determined by the probability distribution of S and E_R. Now let us consider various attacks. Here there still are two kinds of attack:

The opponent's impersonation attack: the largest probability of an opponent's successful impersonation attack

$$P_I = \max_{m \in M} \frac{|\{e_R \in E_R | e_R \in m\}|}{|E_R|}.$$

The opponent's substitution attack: the largest probability of an opponent's successful substitution attack

$$P_S = \max_{m \in M} \max_{m' \neq m \in M} \frac{|\{e_R \in E_R | e_R \in m, e_R \in m'\}|}{|\{e_R \in E_R | e_R \in m\}|}$$

The following gives a example for a construction about multi-sender authentication code.

Let the set of source states $S = R_q^*$, that is the nonzero elements set in R_q, The set of $i-$th transmitter's encoding rules $E_i = \{e_i | e_i \in R_q \times R_q^*\}$, the set of receiver's decoding rules $E_R = \{e_R | e_R \in R_q^k \times (R_q^k)^*\}$, where $(R_q^k)^*$ is the nonzero elements of R_q^k, the set of $i-$th transmitter's tags $T_i = \{t_i | t_i \in R_q\}$, the set of receiver's tags T is a linear code C over R_q, denoted by $C = [n, k]$. A $k \times n$ matrix G is a generator matrix of C. Let the encoding map

$f_i : S \times E_i \to T_i, f_i(s, e_i) = u_i + sv_i(1 \leq i \leq n)$, where $e_i = (u_i, v_i) \in E_i$.

The decoding map $g : S \times E_R \to T, G(s, e_R) = (\alpha + s\beta)G$, where $e_R = (\alpha, \beta) \in E_R$. The synthesizing map

$$h : T_1 \times T_2 \times \cdots \times T_n \to T,$$

$$h(t_1, t_2, \cdots, t_n) = (w_1 + sw_2) + (t_1, t_2, \cdots, t_n),$$

where $w_1, w_2 \in {R_q}^k$.

The scheme has the following steps:

1. Key distribution

The key distribution center randomly chooses an $e = (u, v) \in C \times C^*$, where C^* is nonzero codes in C, assume $u = (u_1, u_2, \cdots, u_n), v = (v_1, v_2, \cdots, v_n)$, then he calculates $e_i = \pi_i(e) = (u_i, v_i)$ and (α_1, β_1) satisfying
$\alpha_1(G) = (u_1, u_2, \cdots, u_n), \beta_1(G) = (v_1, v_2, \cdots, v_n)$. Again $v \neq 0$, so $\beta_1 \neq 0$, then $(\alpha_1, \beta_1) \in R_q^k \times (R_q^k)^*$; The key distribution center also randomly chooses an $(w_1, w_2) \in R_q^k \times R_q^k$ and calculates $e_R = (\alpha, \beta)$ such that $\alpha = w_1 + \alpha_1, \beta = w_2 + \beta_1$; He secretly sends e_R, e_i to the receiver R and sender $P_i (1 \leq i \leq n)$ respectively, at the same time, sends (w_1, w_2) to the synthesizer.

2. Broadcast. If the senders want to send a source state $s \in S$ to the receiver R , the sender P_i calculates $t_i = f_i(s, e_i) = u_i + sv_i$, then sends $(s, t_i)(1 \leq i \leq n)$ to the synthesizer.

3. Synthesis. After the synthesizer receives $(s, (t_1, t_2, \cdots, t_n))$, he calculates $h = (t_1, t_2, \cdots, t_n) = (w_1 + sw_2) + (t_1, t_2, \cdots, t_n)$ and then sends $m = (s, t)$ to the receiver R.

4. Verification. When the receiver R receives $m = (s, t)$, he calculates $t' = g(s, e_R) = (\alpha + s\beta)G$. If $t = t'$, he accepts t, otherwise, he rejects it.

The same as above multi-receiver, using a proof similar to [14], it is not difficult to prove the security of the above construction. Where

$$P_I = \max_{m \in M} \frac{|\{e_R \in E_R | e_R \in m\}|}{|E_R|} = \frac{1}{q^k},$$

$$P_S = \max_{m \in M} \max_{m' \neq m \in M} \frac{|\{e_R \in E_R | e_R \in m, e_R \in m'\}|}{|\{e_R \in E_R | e_R \in m\}|}$$
$$= \frac{1}{q^{k-1}},$$

we can see that the chances of success in the corresponding attacks would be greatly reduced when the number n and k are large enough.

7 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 free module of over a commutative ring R_q with a identity element 1 and no zero divisors. 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 of R_q, is sufficiently large. An interesting research problem is whether the bound in Theorem 8 can be met for general q, and in particular, when is small. In this paper, we realizes the generalization of a linear A-code $\mathcal{C} = (\mathcal{S}, \mathcal{E}, \mathcal{A}, f)$ defined using vector spaces over finite field to free modules over R_q, but these results still need further to improve according to the differences of algebra structure between vector space and free modules in future.

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

Acknowledgements: The research was partially supported by NSF of China(61179026) and Fundamental Research of the Central Universities of China Civil Aviation University of Science special (ZXH2012k003).

References:

[1] Y. Desmedt, Y. Frankel, and M. Yung, Multi-receiver/Multi-sender network security: Efficient authenticated multicast/feedback, *IEEE INFOCOM′92*, 1992, pp. 2045-2054.

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

[3] R.Safavi-Naini and H. Wang, New results on multi-receiver authentication codes, in Advances in CryptologyłEurocrypt 98 *Lecture Notes in Computer Science*, Berlin, Germany: Springer-Verlag,1438,1998,pp.527-541.

[4] R. Safavi-Naini and H. Wang, Multireceiver authentication codes: Models, bounds, constructions and extensions, *Inform. Comput.*, 151, no.1/2, 1999, pp.148-172.

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

[6] J. Rotman, *An introduction to homological algebra*, San-Francisco London: Academic Press New York,1979.

[7] M. Vandijk, C. Gehrmann, and B. Smeets, Unconditionally secure group authentication, *Design, Codes and Cryptograph*, 14, 1998, pp.281-296.

[8] T. Johansson, Authentication codes for non trusting parties obtained from rank metric codes, *Design, Codes and Cryptograph*, 6,1995,pp.205-218.

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

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

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

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

[13] A. Shamir, How to share a secret, *Commun. ACM.*, 22, 1979, pp.612-613.

[14] Cheng Shangdi, Chang Lizhen, Two Constructions of Multi-sender Authentication Codes with arbitration Based Linear Codes, *WSEAS Transactions on Mathematics*, vol.11, isuue12, 2012, pp.1103-1113

[15] Pei Dingyi, *Message Authentication Codes*, China Science and Technology University Press, 2009.

[16] Wan Zhexian, *Design Theory*, Higher Education Press, 2009.

[17] Joseph J. Rotman, *Advanced Mordern Algebra*, Higher Education Press, 2004.