A New Construction of Multi-sender Authentication Codes from Polynomials over Finite Fields

Xiuli Wang

(College of Science, Civil Aviation University of China, Tianjin, 300300, P.R.China.)

Abstract: Multi-sender authentication codes allow a group of senders to construct an authenticated message for a receiver such that the receiver can verify authenticity of the received message. In this paper, we construct one multi-sender authentication codes from polynomials over finite fields. Some parameters and the probabilities of deceptions of this codes are also computed.

Keywords: polynomials, multi-sender authentication codes, primitive element, finite fields

2000 MR Subject Classification: 15A03; 94A60; 94A62

§1 Introduction

Multi-sender authentication codes were firstly constructed by Gilbert, Macwilliams and Sloane in [1] in 1974. Multi-sender authentication system refers to that a group of senders cooperatively send a message to a receiver, then the receiver should be able to ascertain that the message is authentic. About this case, many scholars and researchers had made a great contribution to multi-sender authentication codes, such as [2-6].

In the actual computer network communications, multi-sender authentication codes include sequential model and simultaneous model. Sequential model is that each sender uses his own encoding rules to encode a source state orderly, and the last sender sends the encoded 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 synthesizer respectively, then the

Supported by the NSF of China (61179026,11326060)and Fundamental Research of the Central Universities of China Civil Aviation University of Science special (3122014K015).

Address: College of Science, Civil Aviation University of China, Tianjin 300300, P.R.China.
E-mail: xlwangcauc@163.com, xlwang@cauc.edu.cn.

synthesizer forms an authenticated message and sends the authenticated message to the receiver, the receiver receives the message and verifies whether the message is legal or not. In this paper, we will adopt to the second model.

In a simultaneous model, there are four participants: a group of senders $U = \{U_1, U_2, \cdots, U_n\}$, the keys distribution center, he is 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 have their own Cartesian authentication code respectively. Let $(S, E_i, T_i; f_i)(i = 1, 2, \cdots, n)$ be the senders' Cartesian authentication code, $(S, E_R, T; g)$ be the receiver's Cartesian authentication code, $h : T_1 \times T_2 \times \cdots \times T_n \rightarrow T$ be the synthesis algorithm. $\pi_i : E \rightarrow E_i$ 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 an encoding rule $e \in E$ and sends $e_i = \pi_i(e)$ to the $i - th$ sender $U_i(i = 1, 2, \cdots, n)$ secretly, then he calculates e_R by e according to an 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, the sender U_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 $m = (s, t)$ to the receiver, 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 kerckhoff's principle which except the actual used keys, the other information of the whole system is public.

In a multi-sender authentication system, we assume that the whole senders are cooperation to form a valid message, that is, all senders as a whole and receiver are reliable. But there are some malicious senders which they together cheat the receiver, the part of senders and receiver are not credible, they can take impersonation attack and substitution attack. In the whole system, we assume$\{U_1, U_2, \cdots, U_n\}$ are senders, R is a receiver, E_i is the encoding rules set of the sender U_i, E_R is the decoding rules set of the receiver R. If the source state space S and the key space E_R of receiver R are according to a uniform distribution, then message space M and tag space T are determined by the probability distribution of S and E_R. $L = \{i_1, i_2, \cdots, i_l\} \subset \{1, 2, \cdots, n\}, l < n$, $U_L = \{U_{i_1}, U_{i_2}, \cdots, U_{i_l}\}, E_L = \{E_{U_{i_1}}, E_{U_{i_2}}, \cdots, E_{U_{i_l}}\}$. Now let us consider the attacks from malicious groups of senders. Here there are three kinds of attack:

The opponent's impersonation attack to receiver : U_L, after receiving their

secret keys, encodes a message and send it to receiver. U_L is successful if receiver accepts it as legitimate message. Denote P_I is the largest probability of some opponent's successful impersonation attack to receiver, it can be expressed as

$$P_I = \max_{m \in M} \left\{ \frac{|\{e_R \in E_R | e_R \subset m\}|}{|E_R|} \right\}$$

The opponent's substitution attack to the receiver: U_L replace m with another message m', after they observe a legitimate message m. U_L is successful if the receiver accept it as legitimate message, it can be expressed as

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

There might l malicious senders who together cheat the receiver, that is, the part of senders and the receiver are not credible, they can take impersonation attack. Let $L = \{i_1, i_2, \cdots, i_l\} \subset \{1, 2, \cdots, n\}, l < n$, $E_L = \{e_{i_1}, e_{i_2}, \cdots, e_{i_l}\}$. Assume $U_L = \{U_{i_1}, U_{i_2}, \cdots, U_{i_l}\}$, U_L, after receiving their secret keys, send a message m to the receiver R, U_L is successful if the receiver accepts it as legitimate message. Denote $P_U(L)$ is the maximum probability of success of the impersonation attack to the receiver. It can be expressed as

$$P_U(L) = \max_{e_I \in E_L} \max_{e_I \in e_U} \left\{ \frac{\max_{m \in M} |\{e_R \in E_R | e_R \subset m \text{ and } p(e_R, e_P) \neq 0\}|}{|\{e_R \in E_R | p(e_R, e_P) \neq 0\}|} \right\}$$

Notes: $p(e_R, e_U) \neq 0$ implies that any information s encoded by e_U can be authenticated by e_R.

In [2], Desmedt, Frankel and Yung gave two constructions for MRA-codes based on polynomials and finite geometries, respectively. To construct multi-sender or multi-receiver authentication by polynomials over finite fields, many researchers had done much work, for example [7-9]. There are other constructions of multi-sender authentication codes are given in [3 – 6]. The construction of authentication codes is combinational design in its nature. We know that the polynomial over finite fields can provide a better algebra structure and is easy to count. In this paper, we construct one multi-sender authentication codes from the polynomial over finite fields. Some parameters and the probabilities of deceptions of this codes are also computed. We realize the generalization and application of the similar idea and method of the article [6-9].

§2 Some results about finite field

Let F_q be the finite field with q elements, where q is a power of a prime p,

F is a filed containing F_q, denote F_q^* be the nonzero elements set of F_q. In this paper, we will use the following conclusions.

Definition 1[10]. A generator α of F_q^* is called a primitive element of F_q.

Theorem 1[10]. Let $|F| = q^n$, then F is a $n-dimension$ vector space over F_q. Let α be a primitive element of F_q, $g(x)$ is the minimal polynomial about α over F_q, then $dimg(x) = n$ and $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ is a basis of F. Furthermore, $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ is linear independent, it is equal to $\alpha, \alpha^2, \cdots, \alpha^{n-1}, \alpha^n$ (α is a primitive element, $\alpha \neq 0$) is also linear independent.

Theorem 2[11]. Let $m \leq n$. Then the number of $m \times n$ matrices of rank m over F_q is $q^{m(m-1)/2} \prod_{i=n-m+1}^{n} ($
$q^i - 1)$.

Definition 2[12]. $\varphi(q)$ is *Eulerfunction* of q, it represents the number of the elements which are prime to q.

Theorem 3[12]. Let α be an element of $q-1$ order in F_q^*, that is, α is a primitive element of F_q, then the order of α^r satisfying $Gcd(r, q-1) = 1$ is also $q-1$, so the number of all $q-1$ order elements in F_q^* is $\varphi(q-1)$

More results about finite fields can be found in [10-12].

§3 Construction

Let the polynomial $p_j(x) = a_{1j}x + a_{2j}x^2 + \cdots + a_{nj}x^n$ $(1 \leq j \leq n)$, where the coefficient $a_{ni} \in F_q$ $(1 \leq i \leq n)$. The set of source states $S = F_q^*$; the set of i–th transmitter's encoding rules $E_{U_i} = \{a_{1i}, a_{2i}, \cdots, a_{ni}\}$ $(1 \leq i \leq n)$; the set of receiver's encoding rules $E_R = \{p_1(x), p_2(x), \cdots, p_n(x), \alpha\}$,where α is a primitive element of F_q; the set of i–th transmitter's tags $T_i = \{t_i | \, t_i \in F_q\}$ $(1 \leq i \leq n)$; the set of receiver's tags $T = \{t | \, t \in F_q^*\}$.

Define the encoding map $f_i : S \times E_{U_i} \to T_i, f_i(s, e_{U_i}) = sa_{1i} + s^2a_{2i} + \cdots + s^na_{ni} (1 \leq i \leq n)$.

The decoding map $f : S \times E_R \to T, g(s, e_R) = p_1(s)\alpha + p_2(s)\alpha^2 + \cdots + p_n(s)\alpha^n$.

The synthesizing map $h : T_1 \times T_2 \times \cdots \times T_n \to T, h(t_1, t_2, \cdots, t_n) = t_1\alpha + t_2\alpha^2 + \cdots + t_n\alpha^n$.

The code works as follows: assume q is larger than, or equal to , the number of possible message and $3 \leq q$.

1. Key distribution.

The key distribution center randomly generates n polynomials $p_j(x) = a_{1j}x + a_{2j}x^2 + \cdots + a_{nj}x^n$ $(1 \leq j \leq n)$, where the coefficient $a_{ni} \in F_q$ $(1 \leq i \leq n)$ and make these column vectors by composed of their coefficient are linearly independent, that is, the column vector groups$(a_{11}, a_{21}, \cdots, a_{n1})^T$,

$(a_{12}, a_{22}, \cdots, a_{n2})^T, \cdots, (a_{1n}, a_{2n}, \cdots, a_{nn})^T$ are linearly independent, we denote $A = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \cdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{pmatrix}$, so the column vectors of A are linearly independent, then he sends privately $\{a_{1i}, a_{2i}, \cdots, a_{ni}\}$ to the sender U_i $(1 \le i \le n)$. He selects a primitive element α of F_q secretly again and sends $\{p_1(x), p_2(x), \cdots, p_n(x), \alpha\}$ to the receiver R.

2. Broadcast. If the senders want to send a source state $s \in S$ to the receiver R, the sender U_i calculates $t_i = f_i(s, e_{U_i}) = sa_{1i} + s^2a_{2i} + \cdots + s^na_{ni}$ $(1 \le i \le n)$, then sends t_i to the synthesizer.

3. Synthesis. After the synthesizer receives $t_1, t_2, \cdots, t_n$, he calculates $h(t_1, t_2, \cdots, t_n) = t_1\alpha + t_2\alpha^2 + \cdots + t_n\alpha^n = t$ and then sends $m = (s, t)$ to the receiver R.

4.Verification. When the receiver R receives $m = (s, t)$, he calculates $t' = g(s, e_R) = p_1(s)\alpha + p_2(s)\alpha^2 + \cdots + p_n(s)\alpha^n$. If $t = t'$, he accepts t, otherwise, he rejects it.

Next we will show that the above construction is a well defined multi-sender authentication code with arbitration.

Lemma 3.1 Let $C_i = (S, E_{P_i}, T_i; f_i)$, the codes is an A-code, $1 \le i \le n$.

Proof. (1) For any $e_{U_i} \in E_{U_i}$, $s \in S$, because $e_{U_i} = \{a_{1i}, a_{2i}, \cdots, a_{ni}\}$, $a_{ij} \in F_q$ $(1 \le j \le n)$, so $t_i = sa_{1i} + s^2a_{2i} + \cdots + s^na_{ni} \in T_i = F_q$. Conversely, for any $t_i \in T_i$, choose $e_{U_i} = \{a_{1i}, a_{2i}, \cdots, a_{ni}\}$, $a_{ij} \in F_q, (1 \le j \le n)$, let $t_i =$

$$sa_{1i} + s^2a_{2i} + \cdots + s^na_{ni} \Leftrightarrow \begin{pmatrix} s, s^2, \cdots, s^n \end{pmatrix} \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \cdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{pmatrix} = \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_n \end{pmatrix},$$

$A = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \cdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{pmatrix}$, because the column vectors of A are linearly independent, so the above linear equation has unique solution, that is, $S = (s, s^2, \cdots, s^n)$ is only defined, so s is only defined, that is, f_i $(1 \le i \le n)$ is a surjection.

(2) If $s' \in S$ is another source state satisfying $sa_{1i} + s^2a_{2i} + \cdots + s^na_{ni} = s'a_{1i} + s'^2a_{2i} + \cdots + s'^na_{ni} = t_i$, it is equivalent to $(s - s')a_{1i} + (s^2 - s'^2)a_{2i} + \cdots + (s^n - s'^n)a_{ni} =$

0, that is, $(s - s', s^2 - s'^2, \cdots, s^n - s'^n)\begin{pmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \cdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{pmatrix} = (0, 0, \cdots, 0)$.

Similar to (1), the column vectors of A are linearly independent, A is invertible, we know the homogeneous linear equation $SA = 0$ has a unique solution and there is only zero solution, where $S = (s - s', s^2 - s'^2, \cdots, s^n - s'^n)$, that is, $(s - s', s^2 - s'^2, \cdots, s^n - s'^n) = (0, 0, \cdots, 0)$, so $s = s'$. Therefore, s is the unique source state determined by e_{U_i} and t_i, thus C_i $(1 \le i \le n)$ is an A-code.

Lemma 3.2 Let $C = (S, E_R, T; g)$, then the codes is an A-code.

Proof. (1) For any $s \in S$, $e_R \in E_R$, from the definition of e_R, we assume that $e_R = \{p_1(x), p_2(x), \cdots, p_n(x), \alpha\}$, where α is a primitive element of F_q, $t = g(s, e_R) = p_1(s)\alpha + p_2(s)\alpha^2 + \cdots + p_n(s)\alpha^n \in T = F_q^*$, otherwise, we suppose $p_1(s)\alpha + p_2(s)\alpha^2 + \cdots + p_n(s)\alpha^n = 0$, from theorem 1[10], we know $\alpha, \alpha^2, \cdots, \alpha^n$ are linearly independent, we can get $p_1(s) = p_2(s) = \cdots = p_n(s) = 0$, it is equivalent to

$$\left(s, s^2, \cdots, s^n \right)\begin{pmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \cdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{pmatrix} = \left(0, 0, \cdots, 0 \right),$$

similar to the proof of lemma 3.1(2), $A = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \cdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{pmatrix}$ is invertible, so $(s, s^2, \cdots, s^n) = (0, 0, \cdots, 0)$, that is, $s = 0$, because $s \in F_q^*$, it is a contradiction. On the other hand, for any $t \in T$, choose $e_R = \{p_1(x), p_2(x), \cdots, p_n(x), \alpha\}$, where α is a primitive element of F_q, $g(s, e_R) = p_1(s)\alpha + p_2(s)\alpha^2 + \cdots + p_n(s)\alpha^n = t$. It is equivalent to

$$\left(s, s^2, \cdots, s^n \right)\begin{pmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \cdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{pmatrix}\begin{pmatrix} \alpha \\ \alpha^2 \\ \vdots \\ \alpha^n \end{pmatrix} = t,$$

because $\alpha, \alpha^2, \cdots, \alpha^n$ are linearly independent and A is invertible, therefore, the above equation has unique solution, so s is only defined, that is, g is a surjection.

(2) If s' is another source state satisfying

$$g(s', e_R) = (s, s^2, \cdots, s^n)\begin{pmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \cdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{pmatrix}\begin{pmatrix} \alpha \\ \alpha^2 \\ \vdots \\ \alpha^n \end{pmatrix}$$

$$= (s', s'^2, \cdots, s'^n) \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \cdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} \alpha \\ \alpha^2 \\ \vdots \\ \alpha^n \end{pmatrix} = t,$$

it is equivalent to

$$\left(s - s', s^2 - s'^2, \cdots, s^n - s'^n \right) \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \cdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} \alpha \\ \alpha^2 \\ \vdots \\ \alpha^n \end{pmatrix} = 0,$$

from $\alpha, \alpha^2, \cdots, \alpha^n$ are linearly independent and A is invertible again, the above equation has a unique solution, that is, $(s-s', s^2-s'^2, \cdots, s^n-s'^n) = (0, 0, \cdots, 0)$, furthermore, $s = s'$. So s is the unique source state determined by e_R and t, thus $C = (S, E_R, T; g)$ is an A-code.

At the same time, for any valid $m = (s, t)$, it follows that $t' = p_1(s)\alpha + p_2(s)\alpha^2 + \cdots + p_n(s)\alpha^n = (a_{11}s + a_{21}s^2 + \cdots + a_{n1}s^n)\alpha + (a_{12}s + a_{22}s^2 + \cdots + a_{n2}s^n)\alpha^2 + \cdots + (a_{1n}s + a_{2n}s^2 + \cdots + a_{nn}s^n)\alpha^n = t_1\alpha + t_2\alpha^2 + \cdots + t_n\alpha^n = t$, the receiver R accepts m.

From lemma 3.1 and 3.2, we know that such construction of multi-sender authentication codes is reasonable and there are n senders in this system. Next we compute the parameters of this codes and the maximum probability of success in impersonation attack and substitution attack by group of senders.

Theorem 3.3 Some parameters of this construction are $|S| = q - 1$; $|E_{U_i}| = q^n - q^{i-1} (1 \le i \le n)$; $|T_i| = q (1 \le i \le n)$; $|E_R| = [q^{n(n-1)/2} \prod_{i=1}^{n} (q^i - 1)]\varphi(q-1)$; $|T| = q - 1$.

Proof. For $|S| = q-1$, $|T_i| = q$ *and* $|T| = q-1$, the results are straightforward. For E_{U_i}, because $E_{U_i} = \{a_{1i}, a_{2i}, \cdots, a_{ni}\}$, $a_{ij} \in F_q$ $(1 \le j \le n)$,$(1 \le i \le n)$ and the column vector groups $(a_{11}, a_{21}, \cdots, a_{n1})^T, (a_{12}, a_{22}, \cdots, a_{n2})^T, \cdots, (a_{1n}, a_{2n}, \cdots, a_{nn})^T$ are linearly independent, so $|E_{U_1}| = q^n - 1, |E_{U_2}| = q^n - q$, and so on, we get $|E_{U_i}| = q^n - q^{i-1} (1 \le i \le n)$. For E_R, $E_R = \{p_1(x), p_2(x), \cdots, p_n(x), \alpha\}$, the polynomials $p_j(x) = a_{1j}x + a_{2j}x^2 + \cdots + a_{nj}x^n$ $(1 \le j \le n)$, where the coefficient $a_{ni} \in F_q$ $(1 \le i \le n)$ and these column vectors by composed of their coefficient are linearly independent, from theorem 2[11], we can get the number of these polynomials is $q^{n(n-1)/2} \prod_{i=1}^{n} (q^i - 1)$; For α, α is a primitive element of F_q, from theorem 3[12], we can get the number of α is $\varphi(q-1)$. Thus $|E_R| = [q^{n(n-1)/2} \prod_{i=1}^{n} (q^i - 1)]\varphi(q-1)$.

Lemma 3.4 For any $m \in M$, the number of e_R contained m is $\varphi(q-1)$.

Proof. Let $m = (s,t) \in M$, $e_R = \{p_1(x), p_2(x), \cdots, p_n(x), \alpha\} \in E_R$. If $e_R \subset m$, then

$$p_1(s)\alpha + p_2(s)\alpha^2 + \cdots + p_n(s)\alpha^n = t$$

$$\Leftrightarrow \quad (s, s^2, \cdots, s^n) \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \cdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} \alpha \\ \alpha^2 \\ \vdots \\ \alpha^n \end{pmatrix} = t \ ,$$

where $A = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \cdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{pmatrix}$. For any α, suppose there is another matrix A' such that $(s, s^2, \cdots, s^n)\ A' \begin{pmatrix} \alpha \\ \alpha^2 \\ \vdots \\ \alpha^n \end{pmatrix} = t$, furthermore, we have $(s, s^2, \cdots, s^n)\ (A - A') \begin{pmatrix} \alpha \\ \alpha^2 \\ \vdots \\ \alpha^n \end{pmatrix} = 0$, from $\alpha, \alpha^2, \cdots, \alpha^n$ are linearly independent, we get $(s, s^2, \cdots, s^n)$ $(A - A') = 0$. Because $(s, s^2, \cdots, s^n)$ is arbitrarily, so $A - A' = 0$, that is, $A = A'$, therefore, A is only determined by α. For any given s and t, so the number of e_R contained m is equal to the number of α, that is, the number of e_R contained m is equal to $\varphi(q-1)$.

Lemma 3.5 For any $m = (s,t) \in M$ and $m' = (s',t') \in M$ with $s \neq s'$, then the number of e_R contained m and m' is 1.

Proof. Assume $e_R = \{p_1(x), p_2(x), \cdots, p_n(x), \alpha\} \in E_R$. If $e_R \subset m$ and $e_R \subset m'$, then $p_1(s)\alpha + p_2(s)\alpha^2 + \cdots + p_n(s)\alpha^n = t$ and $p_1(s')\alpha + p_2(s')\alpha^2 + \cdots + p_n(s')\alpha^n = t'$, they are equivalent to $(s, s^2, \cdots, s^n)\ A \begin{pmatrix} \alpha \\ \alpha^2 \\ \vdots \\ \alpha^n \end{pmatrix} = t$, $(s', s'^2, \cdots, s'^n)\ A \begin{pmatrix} \alpha \\ \alpha^2 \\ \vdots \\ \alpha^n \end{pmatrix} = t'$ respectively. Furthermore, we have $(s - s', s^2 - s'^2, \cdots, s^n - s'^n)\ A \begin{pmatrix} \alpha \\ \alpha^2 \\ \vdots \\ \alpha^n \end{pmatrix} = t - t'$, because $s \neq s'$, so $t \neq t'$. Otherwise, we assume $t = t'$, then $t - t' = 0$. From $\alpha, \alpha^2, \cdots, \alpha^n$ are linearly independent and A is invertible, similar to lemma 3.2, it must be $s = s'$, it is contradiction to $s \neq s'$. Therefore, $t - t' \neq 0$. Furthermore, $(t -$

$t')^{-1}\ (s-s', s^2-s'^2, \cdots, s^n-s'^n)\ A\begin{pmatrix}\alpha\\ \alpha^2\\ \vdots\\ \alpha^n\end{pmatrix} = 1$ (*). For any given t, t', $(t-t')^{-1}$ is only defined, and s, s' are also any given, from above the identical equation (*), we obtain $A\begin{pmatrix}\alpha\\ \alpha^2\\ \vdots\\ \alpha^n\end{pmatrix}$ is only determined, because $\alpha, \alpha^2, \cdots, \alpha^n$ are linearly independent and A is invertible again, so α and A are only determined respectively. Therefore, now the number of $\{p_1(x), p_2(x), \cdots, p_n(x), \alpha\}$ is equal to the number of such α and A, it is 1. So the number of e_R contained m and m' is 1.

Lemma 3.6 For any fixed $e_U = \{a_{1i}, a_{2i}, \cdots, a_{ni}\}(1 \le i \le n)$ containing a given e_L, then the number of e_R which is incidence with e_U is $[q^{n(n-1)/2}\prod_{i=1}^{n}(q^i - 1)]\varphi(q-1)$.

Proof. For any fixed $e_U = \{a_{1i}, a_{2i}, \cdots, a_{ni}\}(1 \le i \le n)$ containing a given e_L, $p_j(x) = a_{1j}x + a_{2j}x^2 + \cdots + a_{nj}x^n$ $(1 \le j \le n)$, we assume $e_R = \{p_1(x), p_2(x), \cdots, p_n(x), \alpha\} \in E_R$, where α is a primitive element of F_q, from the definition of e_R and e_U, we can conclude that e_R is incidence with e_U if and only if $p_1(s)\alpha + p_2(s)\alpha^2 + \cdots + p_n(s)\alpha^n = (a_{11}s + a_{21}s^2 + \cdots + a_{n1}s^n)\alpha + (a_{12}s + a_{22}s^2 + \cdots + a_{n2}s^n)\alpha^2 + \cdots + (a_{1n}s + a_{2n}s^2 + \cdots + a_{nn}s^n)\alpha^n = t_1\alpha + t_2\alpha^2 + \cdots + t_n\alpha^n = t$. From this, we can know the number of e_R which is incidence with e_U is equal to the number of all E_R. Therefore, the number of e_R which is incidence with e_U is $[q^{n(n-1)/2}\prod_{i=1}^{n}(q^i - 1)]\varphi(q-1)$.

Lemma 3.7 For any fixed $e_U = \{a_{1i}, a_{2i}, \cdots, a_{ni}\}(1 \le i \le n)$ containing a given e_L and $m = (s, t)$, then the number of e_R which is incidence with e_U and contained in m is 1.

Proof. For any $s \in S, e_R \in E_R$, $p_j(x) = a_{1j}x + a_{2j}x^2 + \cdots + a_{nj}x^n$ $(1 \le j \le n)$, we assume $e_R = \{p_1(x), p_2(x), \cdots, p_n(x), \alpha\} \in E_R$, where α is a primitive element of F_q. Similar to lemma 3.6, for any fixed $e_U = \{a_{1i}, a_{2i}, \cdots, a_{ni}\}(1 \le i \le n)$ containing a given e_L, we have known all e_R are incidence with e_U. Since e_R is contained in m again, we can get $p_1(s)\alpha + p_2(s)\alpha^2 + \cdots + p_n(s)\alpha^n = t \Leftrightarrow (s, s^2, \cdots, s^n)\ A\begin{pmatrix}\alpha\\ \alpha^2\\ \vdots\\ \alpha^n\end{pmatrix} = t \Leftrightarrow t^{-1}(s, s^2, \cdots, s^n)\ A\begin{pmatrix}\alpha\\ \alpha^2\\ \vdots\\ \alpha^n\end{pmatrix} = 1$, we can con-

clude that $t^{-1}(s, s^2, \cdots, s^n)$ and $A\begin{pmatrix} \alpha \\ \alpha^2 \\ \vdots \\ \alpha^n \end{pmatrix}$ are mutually inverse. Because s, t is any given, so $t^{-1}(s, s^2, \cdots, s^n)$ is only determined. Furthermore, $A\begin{pmatrix} \alpha \\ \alpha^2 \\ \vdots \\ \alpha^n \end{pmatrix}$ is also only determined. Similar to the proof of lemma 3.5, from the properties of A and α, we know such A and α are also only determined respectively. So the number of e_R which is incidence with e_U and contained in m is equal to the number of such A and α, that is, 1.

Theorem 3.8 In the constructed multi-sender authentication codes, if the senders' encoding rules and the receiver's decoding rules are chosen according to a uniform probability distribution, then the largest probabilities of success for different types of deceptions respectively are:

$$P_I = \frac{1}{q^{n(n-1)/2}\prod_{i=1}^{n}(q^i-1)};\quad P_S = \frac{1}{\varphi(q-1)};\quad P_U(L) = \frac{1}{[q^{n(n-1)/2}\prod_{i=1}^{n}(q^i-1)]\varphi(q-1)}.$$

Proof. By theorem 3.3 and lemma 3.4, we get

$$\begin{aligned} P_I &= \max_{m\in M}\left\{\frac{|\{e_R \in E_R | e_R \subset m\}|}{|E_R|}\right\} \\ &= \frac{\varphi(q-1)}{q^{n(n-1)/2}\prod_{i=1}^{n}(q^i-1)\varphi(q-1)} \\ &= \frac{1}{q^{n(n-1)/2}\prod_{i=1}^{n}(q^i-1)}; \end{aligned}$$

By lemma 3.4 and lemma 3.5, we get

$$P_S = \max_{m\in M}\left\{\frac{\max_{m'\neq m\in M}|\{e_R \in E_R | e_R \subset m, m'\}|}{|\{e_R \in E_R | e_R \subset m\}|}\right\} = \frac{1}{\varphi(q-1)};$$

By lemma 3.6 and lemma 3.7, we get

$$\begin{aligned} P_U(L) &= \max_{e_I\in E_I}\max_{e_I\in e_U}\left\{\frac{\max_{m\in M}|\{e_R \in E_R | e_R \subset m \text{ and } p(e_R, e_P)\neq 0\}|}{|\{e_R \in E_R | p(e_R, e_P)\neq 0\}|}\right\} \\ &= \frac{1}{[q^{n(n-1)/2}\prod_{i=1}^{n}(q^i-1)]\varphi(q-1)}. \end{aligned}$$

References

[1] Gilbert E N, MacWilliams F J, Sloan N J. Codes which detect deception. *Bell System Technical Journal*, 53:405-424,1974.

[2] Y. Desmedt, Y. Frankel and M. Yung. Multer-receiver/multi-sender network security: efficient authenticated multicast/feedback. *IEEE Infocom'92*: 2045-2054,1992.

[3] 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*, 1334:130-143,1997.

[4] Ma Wenping, Wang Xinmei. Several new constructions of multitrasmitters authentication codes. *ACTA ELECTRONIC SINICA*, 28(4):117-119,2000.

[5] G.J.Simmons. Message authentication with arbitration of transmitter/receiver disputes. *Proc. Eurcrypt 87. Lecture Notes in Computer Science*, 304:151-165,1985.

[6] Cheng Shangdi,Chang Lizhen. Two constructions of multi-sender authentication codes with arbitration based linear codes. Wseas Transactions on mathematics, vol. 11, no. 12, pp.1103-1113, 2012.

[7] R.Safavi-Naini, H.Wang. New results on multi-receiver authentication codes. *In Advances in Crptology-Eurocrypt'98, LNCS*, 1403:527-541,1998.

[8] R.Aparna, B.B.Amberker. Multi-sender multi-receiver authentication for dynamic secure group communication. *International journal of computer science and network security*, 7(10):47-63, 2007.

[9] R.Safavi-Naini, H.Wang. Multireceiver authentication codes:models, bounds,constructions and extensions.*In Advances in Crptology-Asiacrypt'98, LNCS*, 1514:242-256, 1998.

[10] Shen shiyi, Chen lushen. Information and coding theory. *Science press in China*, 2002.

[11] Wan Zhexian. Geometry of classical group over finite field. *Science press in Beijing/New York*, 2002.

[12] Joseph J. Rotman. Advanced modern algebra. *High education press in China*, 2004.