Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2013, Article ID 320392, 7 pages
http://dx.doi.org/10.1155/2013/320392

Research Article

A New Construction of Multisender Authentication Codes from Polynomials over Finite Fields

Xiuli Wang

College of Science, Civil Aviation University of China, Tianjin 300300, China

Correspondence should be addressed to Xiuli Wang; xlwang@cauc.edu.cn

Received 3 February 2013; Accepted 7 April 2013

Academic Editor: Yang Zhang

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

1. Introduction

Multisender authentication code was firstly constructed by Gilbert et al. [1] in 1974. Multisender authentication system refers to who 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 great contributions to multisender authentication codes, such as [2–6].

In the actual computer network communications, multisender 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, the last sender sends the encoded message to the receiver, and 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 synthesizer forms an authenticated message and verifies whether the message is legal or not. In this paper, we will adopt the second model.

In a simultaneous model, there are four participants: a group of senders $U = \{U_1, U_2, \ldots, U_n\}$, the key distribution center, he is responsible for the key distribution to senders and receiver, including solving the disputes between them, a receiver R, and a synthesizer, where he only runs the trusted synthesis algorithm. The code works as follows: each sender and receiver has their own Cartesian authentication code, respectively. Let $(S, E_i, T_i; f_i)$ $(i = 1, 2, \ldots, n)$ be the senders' Cartesian authentication code, $(S, E_R, T; g)$ be the receiver's Cartesian authentication code, $h : T_1 \times T_2 \times \cdots \times T_n \to T$ be the synthesis algorithm, and $\pi_i : E \to E_i$ 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 an encoding rule $e \in E$ and sends $e_i = \pi_i(e)$ to the ith sender U_i $(i = 1, 2, \ldots, n)$, 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, U_i computes $t_i = f_i(s, e_i)$ $(i = 1, 2, \ldots, n)$ and sends $m_i = (s, t_i)$ $(i = 1, 2, \ldots, n)$ to the synthesizer through an open channel. The synthesizer receives the message $m_i = (s, t_i)$ $(i = 1, 2, \ldots, n)$ and calculates $t = h(t_1, t_2, \ldots, t_n)$ by the synthesis algorithm h and 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, and 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 principle in which, except the actual used keys, the other information of the whole system is public.

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

The opponent's impersonation attack to receiver: U_L, after receiving their secret keys, encode a message and send it to the receiver. U_L are successful if the receiver accepts it as legitimate message. Denote by P_I the largest probability of some opponent's successful impersonation attack to receiver; it can be expressed as

$$P_I = \max_{m \in M} \left\{ \frac{\left|\{e_R \in E_R \mid e_R \subset m\}\right|}{\left|E_R\right|} \right\}. \quad (1)$$

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 are successful if the receiver accepts it as legitimate message; it can be expressed as

$$P_S = \max_{m \in M} \left\{ \frac{\max_{m' \neq m \in M} \left|\{e_R \in E_R \mid e_R \subset m, m'\}\right|}{\left|\{e_R \in E_R \mid e_R \subset m\}\right|} \right\}. \quad (2)$$

There might be l malicious senders who together cheat the receiver; that is, the part of senders and the receiver are not credible, and they can take impersonation attack. Let $L = \{i_1, i_2, \ldots, i_l\} \subset \{1, 2, \ldots, n\}$, $l < n$ and $E_L = \{E_{Ui_1}, E_{Ui_2}, \ldots, E_{Ui_l}\}$. Assume that $U_L = \{U_{i_1}, U_{i_2}, \ldots, U_{i_l}\}$, after receiving their secret keys, send a message m to the receiver R; U_L are successful if the receiver accepts it as legitimate message. Denote by $P_U(L)$ the maximum probability of success of the impersonation attack to the receiver. It can be expressed as

$$P_U(L) = \max_{e_L \in E_L} \max_{e_L \in e_U} \left\{ \frac{\max_{m \in M} \left|\{e_R \in E_R \mid e_R \subset m, p(e_R, e_P) \neq 0\}\right|}{\left|\{e_R \in E_R \mid p(e_R, e_P) \neq 0\}\right|} \right\}. \quad (3)$$

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

In [2], Desmedt et al. gave two constructions for MRA-codes based on polynomials and finite geometries, respectively. To construct multisender or multireceiver authentication by polynomials over finite fields, many researchers have done much work, for example, [7–9]. There are other constructions of multisender authentication codes that 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 multisender authentication code from the polynomial over finite fields. Some parameters and the probabilities of deceptions of this code are also computed. We realize the generalization and the application of the similar idea and method of the paper [7–9].

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 and F is a field containing F_q; denote by F_q^* be the nonzero elements set of F_q. In this paper, we will use the following conclusions over finite fields.

Conclusion 1. A generator α of F_q^* is called a primitive element of F_q.

Conclusion 2. Let $\alpha \in F_q$; if some polynomials contain α as their root and their leading coefficient are 1 over F_q, then the polynomial having least degree among all such polynomials is called a minimal polynomial over F_q.

Conclusion 3. Let $|F| = q^n$, then F is an n-dimensional vector space over F_q. Let α be a primitive element of F_q and $g(x)$ the minimal polynomial about α over F_q; then $\dim g(x) = n$ and $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ is a basis of F. Furthermore, $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ is linear independent, and it is equal to $\alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n$ (α is a primitive element, $\alpha \neq 0$) is also linear independent; moreover, $\alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{n-1}}, \alpha^{p^n}$ is also linear independent.

Conclusion 4. Consider $(x_1 + x_2 + \cdots + x_n)^m = (x_1)^m + (x_2)^m + \cdots + (x_n)^m$, where $x_i \in F_q$, $(1 \leq i \leq n)$ and m is a nonnegative power of character p of F_q.

Conclusion 5. Let $m \leq n$. Then, the number of $m \times n$ matrices of rank m over F_q is $q^{m(m-1)/2} \prod_{i=n-m+1}^{n} (q^i - 1)$.

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

3. Construction

Let the polynomial $p_j(x) = a_{j1}x^{p^n} + a_{j2}x^{p^{(n-1)}} + \cdots + a_{jn}x^p$ $(1 \leq j \leq k)$, where the coefficient $a_{il} \in F_q$, $(1 \leq l \leq n)$, and these vectors by the composition of their coefficient are linearly independent. The set of source states $S = F_q$; the set of ith transmitter's encoding rules $E_{U_i} = \{p_1(x_i), p_2(x_i), \ldots, p_k(x_i), x_i \in F_q^*\}$ $(1 \leq i \leq n)$; the set of receiver's encoding rules $E_R = \{p_1(\alpha), p_2(\alpha), \ldots, p_k(\alpha)$, where α is a primitive element of $F_q\}$; the set of ith transmitter's tags $T_i = \{t_i \mid t_i \in F_q\}$ $(1 \leq i \leq n)$; the set of receiver's tags $T = \{t \mid t \in F_q\}$.

Define the encoding map $f_i : S \times E_{U_i} \to T_i$, $f_i(s, e_{U_i}) = sp_1(x_i) + s^2 p_2(x_i) + \cdots + s^k p_k(x_i)$, $1 \le i \le n$.

The decoding map $f : S \times E_R \to T$, $f(s, e_R) = sp_1(\alpha) + s^2 p_2(\alpha) + \cdots + s^k p_k(\alpha)$.

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

The code works as follows.

Assume that q is larger than, or equal to, the number of the possible message and $n \le q$.

3.1. Key Distribution. The key distribution center randomly generates k ($k \le n$) polynomials $p_1(x), p_2(x), \ldots, p_k(x)$, where $p_j(x) = a_{j1}x^{p^n} + a_{j2}x^{p^{(n-1)}} + \cdots + a_{jn}x^p$ ($1 \le j \le k$), and make these vectors by composed of their coefficient is linearly independent, it is equivalent to the column vectors of the matrix $\begin{pmatrix} a_{11} & a_{21} & \cdots & a_{k1} \\ a_{12} & a_{22} & \cdots & a_{k2} \\ \vdots & \vdots & \vdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{kn} \end{pmatrix}$ is linearly independent. He selects n distinct nonzero elements $x_1, x_2, \ldots, x_n \in F_q$ again and makes x_i ($1 \le i \le n$) secret; then he sends privately $p_1(x_i), p_2(x_i), \ldots, p_k(x_i)$ to the sender U_i ($1 \le i \le n$). The key distribution center also randomly chooses a primitive element α of F_q satisfying $x_1 + x_2 + \cdots + x_n = \alpha$ and sends $p_1(\alpha), p_2(\alpha), \ldots, p_k(\alpha)$ to the receiver R.

3.2. Broadcast. If the senders want to send a source state $s \in S$ to the receiver R, the sender U_i calculates $t_i = f_i(s, e_{U_i}) = A_s(x_i) = sp_1(x_i) + s^2 p_2(x_i) + \cdots + s^k p_k(x_i)$, $1 \le i \le n$ and then sends $A_s(x_i) = t_i$ to the synthesizer.

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

3.4. Verification. When the receiver R receives $m = (s, t)$, he calculates $t' = g(s, e_R) = A_s(\alpha) = sp_1(\alpha) + s^2 p_2(\alpha) + \cdots + s^k p_k(\alpha)$. If $t = t'$, he accepts t; otherwise, he rejects it.

Next, we will show that the above construction is a well defined multisender authentication code with arbitration.

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

Proof. (1) For any $e_{U_i} \in E_{U_i}$, $s \in S$, because $E_{U_i} = \{p_1(x_i), p_2(x_i), \ldots, p_k(x_i),\ x_i \in F_q^*\}$, so $t_i = sp_1(x_i) + s^2 p_2(x_i) + \cdots + s^k p_k(x_i) \in T_i = F_q$. Conversely, for any $t_i \in T_i$, choose $e_{U_i} = \{p_1(x_i), p_2(x_i), \ldots, p_k(x_i),\ x_i \in F_q^*\}$, where $p_j(x) = a_{j1}x^{p^n} + a_{j2}x^{p^{(n-1)}} + \cdots + a_{jn}x^p$ ($1 \le j \le k$), and let $t_i = f_i(s, e_{U_i}) = sp_1(x_i) + s^2 p_2(x_i) + \cdots + s^k p_k(x_i)$; it is equivalent to

$$\left(x_i^{p^n}, x_i^{p^{n-1}}, \ldots, x_i^p\right) \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{k1} \\ a_{12} & a_{22} & \cdots & a_{k2} \\ \vdots & \vdots & \vdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{kn} \end{pmatrix} \begin{pmatrix} s \\ s^2 \\ \vdots \\ s^k \end{pmatrix} = t_i. \tag{4}$$

It follows that

$$\begin{pmatrix} x_1^{p^n} & x_1^{p^{n-1}} & \cdots & x_1^p \\ x_2^{p^n} & x_2^{p^{n-1}} & \cdots & x_2^p \\ \vdots & \vdots & \vdots & \vdots \\ x_n^{p^n} & x_n^{p^{n-1}} & \cdots & x_n^p \end{pmatrix} \times \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{k1} \\ a_{12} & a_{22} & \cdots & a_{k2} \\ \vdots & \vdots & \vdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{kn} \end{pmatrix} \begin{pmatrix} s \\ s^2 \\ \vdots \\ s^k \end{pmatrix} = \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_n \end{pmatrix}. \tag{5}$$

Denote

$$A = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{k1} \\ a_{12} & a_{22} & \cdots & a_{k2} \\ \vdots & \vdots & \vdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{kn} \end{pmatrix},$$

$$X = \begin{pmatrix} x_1^{p^n} & x_1^{p^{n-1}} & \cdots & x_1^p \\ x_2^{p^n} & x_2^{p^{n-1}} & \cdots & x_2^p \\ \vdots & \vdots & \vdots & \vdots \\ x_n^{p^n} & x_n^{p^{n-1}} & \cdots & x_n^p \end{pmatrix}, \tag{6}$$

$$S = \begin{pmatrix} s \\ s^2 \\ \vdots \\ s^k \end{pmatrix}, \qquad t = \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_n \end{pmatrix}.$$

The above linear equation is equivalent to $XAS = t$, because the column vectors of A are linearly independent, X is equivalent to a Vandermonde matrix, and X is inverse; therefore, the above linear equation has a unique solution, 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 $sp_1(x_i) + s^2 p_2(x_i) + \cdots + s^k p_k(x_i) = s' p_1(x_i) + s'^2 p_2(x_i) + \cdots + s'^k p_k(x_i) = t_i$, and it is equivalent to $(s - s')p_1(x_i) + (s^2 - s'^2)p_2(x_i) + \cdots + (s^k - s'^k)p_k(x_i) = 0$, then

$$\left(x_i^{p^n}, x_i^{p^{n-1}}, \ldots, x_i^p\right) \times \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{k1} \\ a_{12} & a_{22} & \cdots & a_{k2} \\ \vdots & \vdots & \vdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{kn} \end{pmatrix} \begin{pmatrix} s - s' \\ s^2 - s'^2 \\ \vdots \\ s^k - s'^k \end{pmatrix} = 0. \tag{7}$$

Thus

$$\begin{pmatrix} x_1^{p^n} & x_1^{p^{n-1}} & \cdots & x_1^{p} \\ x_2^{p^n} & x_2^{p^{n-1}} & \cdots & x_2^{p} \\ \vdots & \vdots & \vdots & \vdots \\ x_n^{p^n} & x_n^{p^{n-1}} & \cdots & x_n^{p} \end{pmatrix} \times \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{k1} \\ a_{12} & a_{22} & \cdots & a_{k2} \\ \vdots & \vdots & \vdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{kn} \end{pmatrix} \begin{pmatrix} s - s' \\ s^2 - s'^2 \\ \vdots \\ s^k - s'^k \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{8}$$

Similar to (1), we know that the homogeneous linear equation $XAS = 0$ has a unique solution; that is, there is only zero solution, so $s = s'$. So, 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 2. *Let $C = (S, E_R, T, g)$; then the code 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 $E_R = \{p_1(\alpha), p_2(\alpha), \ldots, p_k(\alpha)$, where α is a primitive element of $F_q\}$, $g(s, e_R) = sp_1(\alpha) + s^2 p_2(\alpha) + \cdots + s^k p_k(\alpha) \in T = F_q$; on the other hand, for any $t \in T$, choose $e_R = \{p_1(\alpha), p_2(\alpha), \ldots, p_k(\alpha)$, where α is a primitive element of $F_q\}$, $g(s, e_R) = sp_1(\alpha) + s^2 p_2(\alpha) + \cdots + s^k p_k(\alpha) = t$; it is equivalent to

$$\left(\alpha^{p^n}, \alpha^{p^{n-1}}, \cdots, \alpha^{p}\right) \times \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{k1} \\ a_{12} & a_{22} & \cdots & a_{k2} \\ \vdots & \vdots & \vdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{kn} \end{pmatrix} \begin{pmatrix} s \\ s^2 \\ \vdots \\ s^k \end{pmatrix} = t, \tag{9}$$

$$A = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{k1} \\ a_{12} & a_{22} & \cdots & a_{k2} \\ \vdots & \vdots & \vdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{kn} \end{pmatrix};$$

that is, $(\alpha^{p^n}, \alpha^{p^{n-1}}, \ldots, \alpha^{p}) A \begin{pmatrix} s \\ s^2 \\ \vdots \\ s^k \end{pmatrix} = t$. From Conclusion 3, we know that $(\alpha^{p^n}, \alpha^{p^{n-1}}, \ldots, \alpha^{p})$ is linearly independent and the column vectors of A are also linearly independent; therefore, the above linear equation has unique solution, so s is only defined; that is, g is a surjection.

(2) If s' is another source state satisfying $t = g(s', e_R)$, then

$$\left(\alpha^{p^n}, \alpha^{p^{n-1}}, \ldots, \alpha^{p}\right) A \begin{pmatrix} s' \\ s'^2 \\ \vdots \\ s'^k \end{pmatrix} = \left(\alpha^{p^n}, \alpha^{p^{n-1}}, \ldots, \alpha^{p}\right) A \begin{pmatrix} s \\ s^2 \\ \vdots \\ s^k \end{pmatrix}; \tag{10}$$

that is, $(\alpha^{p^n}, \alpha^{p^{n-1}}, \ldots, \alpha^{p}) A \left(\begin{bmatrix} s' \\ s'^2 \\ \vdots \\ s'^k \end{bmatrix} - \begin{bmatrix} s \\ s^2 \\ \vdots \\ s^k \end{bmatrix} \right) = 0$. Similar to (1), we get that the homogeneous linear equation $(\alpha^{p^n}, \alpha^{p^{n-1}}, \ldots, \alpha^{p}) A(S' - S) = 0$ has a unique solution; that is, there is only zero solution, so $S = S'$; that is, $s = s'$. 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 $m = (s, t)$, we have known that $\alpha = x_1 + x_2 + \cdots + x_n$, and it follows that $t' = sp_1(\alpha) + s^2 p_2(\alpha) + \cdots + s^k p_k(\alpha) = sp_1(x_1 + x_2 + \cdots + x_n) + s^2 p_2(x_1 + x_2 + \cdots + x_n) + \cdots + s^k p_k(x_1 + x_2 + \cdots + x_n)$. We also have known that $p_j(x) = a_{j1} x^{p^n} + a_{j2} x^{p^{(n-1)}} + \cdots + a_{jn} x^{p}$ $(1 \le j \le k)$; from Conclusion 4, $(x_1 + x_2 + \cdots + x_n)^{p^m} = (x_1)^{p^m} + (x_2)^{p^m} + \cdots + (x_n)^{p^m}$, where m is a nonnegative power of character p of F_q, and we get $p_j(x_1 + x_2 + \cdots + x_n) = p_j(x_1) + p_j(x_2) + \cdots + p_j(x_n)$; therefore, $t' = sp_1(\alpha) + s^2 p_2(\alpha) + \cdots + s^k p_k(\alpha) = (sp_1(x_1) + s^2 p_2(x_1) + \cdots + s^k p_k(x_1)) + (sp_1(x_2) + s^2 p_2(x_2) + \cdots + s^k p_k(x_2)) + \cdots + (sp_1(x_n) + s^2 p_2(x_n) + \cdots + s^k p_k(x_n)) = t_1 + t_2 + \cdots + t_n = t$, and the receiver R accepts m. □

From Lemmas 1 and 2, we know that such construction of multisender authentication codes is reasonable and there are n senders in this system. Next, we compute the parameters of this code and the maximum probability of success in impersonation attack and substitution attack by the group of senders.

Theorem 3. *Some parameters of this construction are $|S| = q$, $|E_{U_i}| = [q^{k(k-1)/2} \prod_{i=n-k+1}^{n} (q^i - 1)] \binom{q-1}{1} = [q^{k(k-1)/2} \prod_{i=n-k+1}^{n} (q^i - 1)](q - 1)$ $(1 \le i \le n)$, $|T_i| = q$ $(1 \le i \le n)$, $|E_R| = [q^{k(k-1)/2} \prod_{i=n-k+1}^{n} (q^i - 1)] \varphi(q - 1)$, $|T| = q$. Where $\varphi(q - 1)$ is the Euler function of $q - 1$, it represents the number of primitive element of F_q here.*

Proof. For $|S| = q$, $|T_i| = q$, and $|T| = q$, the results are straightforward. For E_{U_i}, because $E_{U_i} = \{p_1(x_i), p_2(x_i), \ldots, p_k(x_i)$, $x_i \in F_q^*\}$, where $p_j(x) = a_{j1} x^{p^n} + a_{j2} x^{p^{(n-1)}} + \cdots + a_{jn} x^{p}$ $(1 \le j \le k)$, and these vectors by the composition of their coefficient are linearly independent, it is equivalent to the columns of $A = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{k1} \\ a_{12} & a_{22} & \cdots & a_{k2} \\ \vdots & \vdots & \vdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{kn} \end{pmatrix}$ is linear independent.

From Conclusion 5, we can conclude that the number of A satisfying the condition is $q^{k(k-1)/2}\prod_{i=n-k+1}^{n}(q^i-1)$. On the other hand, the number of distinct nonzero elements x_i $(1 \le i \le n)$ in F_q is $\binom{q-1}{1} = q-1$, so $|E_{U_i}| = [q^{k(k-1)/2}\prod_{i=n-k+1}^{n}(q^i-1)](q-1)$. For E_R, $E_R = \{p_1(\alpha), p_2(\alpha), \ldots, p_k(\alpha)$, where α is a primitive element of $F_q\}$. For α, from Conclusion 1, a generator of F_q^* is called a primitive element of F_q, $|F_q^*| = q-1$; by the theory of the group, we know that the number of generator of F_q^* is $\varphi(q-1)$; that is, the number of α is $\varphi(q-1)$. For $p_1(x), p_2(x), \ldots, p_k(x)$. From above, we have confirmed that the number of these polynomials is $q^{k(k-1)/2}\prod_{i=n-k+1}^{n}(q^i-1)$; therefore, $|E_R| = [q^{k(k-1)/2}\prod_{i=n-k+1}^{n}(q^i-1)]\varphi(q-1)$. □

Lemma 4. *For any $m \in M$, the number of e_R contained m is $\varphi(q-1)$.*

Proof. Let $m = (s,t) \in M$, $e_R = \{p_1(\alpha), p_2(\alpha), \ldots, p_k(\alpha)$, where α is a primitive element of $F_q\} \in E_R$. If $e_R \subset m$, then $sp_1(\alpha) + s^2p_2(\alpha) + \cdots + s^kp_k(\alpha) = t \Leftrightarrow (\alpha^{p^n}, \alpha^{p^{n-1}}, \ldots, \alpha^p)A\begin{pmatrix} s \\ s^2 \\ \vdots \\ s^k \end{pmatrix} = t$. For any α, suppose that there is another A' such that $(\alpha^{p^n}, \alpha^{p^{n-1}}, \ldots, \alpha^p)A'\begin{pmatrix} s \\ s^2 \\ \vdots \\ s^k \end{pmatrix} = t$, then $(\alpha^{p^n}, \alpha^{p^{n-1}}, \ldots, \alpha^p)(A - A')\begin{pmatrix} s \\ s^2 \\ \vdots \\ s^k \end{pmatrix} = 0$, because $\alpha^{p^n}, \alpha^{p^{n-1}}, \ldots, \alpha^p$ is linearly independent, so $(A-A')\begin{pmatrix} s \\ s^2 \\ \vdots \\ s^k \end{pmatrix} = 0$, but $\begin{pmatrix} s \\ s^2 \\ \vdots \\ s^k \end{pmatrix}$ is arbitrarily; therefore, $A - A' = 0$; that is, $A = A'$, and it follows that A is only determined by α. Therefore, as $\alpha \in E_R$, for any given s and t, the number of e_R contained in m is $\varphi(q-1)$. □

Lemma 5. *For any $m = (s,t) \in M$ and $m' = (s',t') \in M$ with $s \ne s'$, the number of e_R contained m and m' is* 1.

Proof. Assume that $e_R = \{p_1(\alpha), p_2(\alpha), \ldots, p_k(\alpha)$, where α is a primitive element of $F_q\} \in E_R$. If $e_R \subset m$ and $e_R \subset m'$, then $sp_1(\alpha) + s^2p_2(\alpha) + \cdots + s^kp_k(\alpha) = t \Leftrightarrow (\alpha^{p^n}, \alpha^{p^{n-1}}, \ldots, \alpha^p)A\begin{pmatrix} s \\ s^2 \\ \vdots \\ s^k \end{pmatrix} = t$, $s'p_1(\alpha) + s'^2p_2(\alpha) + \cdots + s'^kp_k(\alpha) = t \Leftrightarrow (\alpha^{p^n}, \alpha^{p^{n-1}}, \ldots, \alpha^p)A\begin{pmatrix} s' \\ s'^2 \\ \vdots \\ s'^k \end{pmatrix} = t$. It is equivalent to $(\alpha^{p^n}, \alpha^{p^{n-1}}, \ldots, \alpha^p)A\begin{pmatrix} s-s' \\ s^2-s'^2 \\ \vdots \\ s^k-s'^k \end{pmatrix} = t - t'$ because $s \ne s'$, so $t \ne t'$; otherwise, we assume that $t = t'$ and since $\alpha^{p^n}, \alpha^{p^{n-1}}, \ldots, \alpha^p$ and the column vectors of A both are linearly independent, it forces that $s = s'$; this is a contradiction. Therefore, we get

$$\left(t-t'\right)^{-1}\left[\left(\alpha^{p^n}, \alpha^{p^{n-1}}, \ldots, \alpha^p\right)A\begin{pmatrix} s-s' \\ s^2-s'^2 \\ \vdots \\ s^k-s'^k \end{pmatrix}\right] = 1, \quad (*)$$

since t, t' is given, $(t-t')^{-1}$ is unique, by equation $(*)$, for any given s, s' and t, t', we obtain that $(\alpha^{p^n}, \alpha^{p^{n-1}}, \ldots, \alpha^p)A$ is only determined; thus, the number of e_R contained m and m' is 1. □

Lemma 6. *For any fixed $e_U = \{p_1(x_i), p_2(x_i), \ldots, p_k(x_i)$, $x_i \in F_q^*\}$ $(1 \le i \le n)$ containing a given e_L, then the number of e_R which is incidence with e_U is $\varphi(q-1)$.*

Proof. For any fixed $e_U = \{p_1(x_i), p_2(x_i), \ldots, p_k(x_i)$, $x_i \in F_q^*\}$ $(1 \le i \le n)$ containing a given e_L, we assume that $p_j(x_i) = a_{j1}x_i^{p^n} + a_{j2}x_i^{p^{(n-1)}} + \cdots + a_{jn}x_i^p$ $(1 \le j \le k,\ 1 \le i \le n)$, $e_R = \{p_1(\alpha), p_2(\alpha), \ldots, p_k(\alpha)$, where α is a primitive element of $F_q\}$. From the definitions of e_R and e_U and Conclusion 4, we can conclude that e_R is incidence with e_U if and only if $x_1 + x_2 + \cdots + x_n = \alpha$. For any α, since $\mathrm{Rank}(1,1,\ldots,1) = \mathrm{Rank}(1,1,\ldots,1,\alpha) = 1 < n$, so the equation $x_1 + x_2 + \cdots + x_n = \alpha$ always has a solution. From the proof of Theorem 3, we know the number of e_R which is incident with e_U (i.e., the number of all E_R) is $[q^{k(k-1)/2}\prod_{i=n-k+1}^{n}(q^i-1)]\ \varphi(q-1)$. □

Lemma 7. *For any fixed $e_U = \{p_1(x_i), p_2(x_i), \ldots, p_k(x_i)$, $x_i \in F_q^*\}$ $(1 \le i \le n)$ containing a given e_L and $m = (s,t)$, the number of e_R which is incidence with e_U and contained in m is* 1.

Proof. For any $s \in S$, $e_R \in E_R$, we assume that $e_R = \{p_1(\alpha), p_2(\alpha), \ldots, p_k(\alpha)$, where α is a primitive element of $F_q\}$. Similar to Lemma 6, for any fixed $e_U = \{p_1(x_i), p_2(x_i), \ldots, p_k(x_i)$, $x_i \in F_q^*\}$, $(1 \le i \le n)$ containing a given e_L, we have known that e_R is incident with e_U if and only if

$$x_1 + x_2 + \cdots + x_n = \alpha. \quad (11)$$

Again, with $e_R \subset m$, we can get

$$sp_1(\alpha) + s^2p_2(\alpha) + \cdots + s^kp_k(\alpha) = t. \quad (12)$$

By (11) and (12) and the property of $p_j(x)$ $(1 \le j \le k)$, we have the following conclusion:

$$sp_1\left(\sum_{i=1}^{n}x_i\right) + s^2p_2\left(\sum_{i=1}^{n}x_i\right) + \cdots + s^kp_k\left(\sum_{i=1}^{n}x_i\right) = t \Longleftrightarrow \left(p_1\left(\sum_{i=1}^{n}x_i\right), p_2\left(\sum_{i=1}^{n}x_i\right), \ldots, p_k\left(\sum_{i=1}^{n}x_i\right)\right)$$

$$\times \begin{pmatrix} s \\ s^2 \\ \vdots \\ s^k \end{pmatrix}$$

$$= t \Longleftrightarrow \left(\sum_{i=1}^{n} p_1(x_i), \sum_{i=1}^{n} p_2(x_i), \ldots, \sum_{i=1}^{n} p_k(x_i) \right) \begin{pmatrix} s \\ s^2 \\ \vdots \\ s^k \end{pmatrix}$$

$$= t \Longleftrightarrow \left(\left(\sum_{i=1}^{n} x_i \right)^n, \left(\sum_{i=1}^{n} x_i \right)^{n-1}, \ldots, \left(\sum_{i=1}^{n} x_i \right) \right) A \begin{pmatrix} s \\ s^2 \\ \vdots \\ s^k \end{pmatrix}$$

$$= t \Longleftrightarrow \left[\left(\sum_{i=1}^{n} p_1(x_i), \sum_{i=1}^{n} p_2(x_i), \ldots, \sum_{i=1}^{n} p_k(x_i) \right) - \left(\left(\sum_{i=1}^{n} x_i \right)^n, \left(\sum_{i=1}^{n} x_i \right)^{n-1}, \ldots, \left(\sum_{i=1}^{n} x_i \right) \right) A \right] \times \begin{pmatrix} s \\ s^2 \\ \vdots \\ s^k \end{pmatrix} = 0, \tag{13}$$

because s is any given. Similar to the proof of Lemma 4, we can get $(\sum_{i=1}^{n} p_1(x_i), \sum_{i=1}^{n} p_2(x_i), \ldots, \sum_{i=1}^{n} p_k(x_i)) - ((\sum_{i=1}^{n} x_i)^n, (\sum_{i=1}^{n} x_i)^{n-1}, \ldots, (\sum_{i=1}^{n} x_i))A = 0$; that is, $((\sum_{i=1}^{n} x_i)^n, (\sum_{i=1}^{n} x_i)^{n-1}, \ldots, (\sum_{i=1}^{n} x_i))A = (\sum_{i=1}^{n} p_1(x_i), \sum_{i=1}^{n} p_2(x_i), \ldots, \sum_{i=1}^{n} p_k(x_i))$, but $p_1(x_i), p_2(x_i), \ldots, p_k(x_i)$ and x_i $(1 \le i \le n)$ also are fixed; thus, α and $A$are only determined, so the number of e_R which is incident with e_U and contained in m is 1. □

Theorem 8. *In the constructed multisender 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*

$$P_I = \frac{1}{q^{k(k-1)/2} \prod_{i=n-k+1}^{n} (q^i - 1)},$$

$$P_S = \frac{1}{\varphi(q-1)}, \tag{14}$$

$$P_U(L) = \frac{1}{[q^{k(k-1)/2} \prod_{i=n-k+1}^{n} (q^i - 1)] \varphi(q-1)}.$$

Proof. By Theorem 3 and Lemma 4, we get

$$P_I = \max_{m \in M} \left\{ \frac{|\{e_R \in E_R \mid e_R \subset m\}|}{|E_R|} \right\} = \frac{\varphi(q-1)}{[q^{k(k-1)/2} \prod_{i=n-k+1}^{n} (q^i - 1)] \ \varphi(q-1)} = \frac{1}{q^{k(k-1)/2} \prod_{i=n-k+1}^{n} (q^i - 1)}. \tag{15}$$

By Lemmas 4 and 5, we get

$$P_S = \max_{m \in M} \left\{ \frac{\max_{m' \neq m \in M} |\{e_R \in E_R \mid e_R \subset m, m'\}|}{|\{e_R \in E_R \mid e_R \subset m\}|} \right\} = \frac{1}{\varphi(q-1)}. \tag{16}$$

By Lemmas 6 and 7, we get

$$P_U(L) = \max_{e_L \in E_L} \max_{e_L \in e_U} \left\{ \frac{\max_{m \in M} |\{e_R \in E_R \mid e_R \subset m, p(e_R, e_P) \neq 0\}|}{|\{e_R \in E_R \mid p(e_R, e_P) \neq 0\}|} \right\} = \frac{1}{[q^{k(k-1)/2} \prod_{i=n-k+1}^{n} (q^i - 1)] \varphi(q-1)}. \tag{17}$$

□

Acknowledgments

This paper is supported by the NSF of China (61179026) and the Fundamental Research of the Central Universities of China Civil Aviation University of Science special (ZXH2012k003).

References

[1] E. N. Gilbert, F. J. MacWilliams, and N. J. A. Sloane, "Codes which detect deception," *The Bell System Technical Journal*, vol. 53, pp. 405–424, 1974.

[2] Y. Desmedt, Y. Frankel, and M. Yung, "Multi-receiver/multi-sender network security: efficient authenticated multicast/feedback," in *Proceedings of the the 11th Annual Conference of the IEEE Computer and Communications Societies (Infocom '92)*, pp. 2045–2054, May 1992.

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

[4] W. Ma and X. Wang, "Several new constructions of multi trasmitters authentication codes," *Acta Electronica Sinica*, vol. 28, no. 4, pp. 117–119, 2000.

[5] G. J. Simmons, "Message authentication with arbitration of transmitter/receiver disputes," in *Advances in Cryptology—EUROCRYPT '87, Workshop on the Theory and Application of of Cryptographic Techniques*, vol. 304 of *Lecture Notes in Computer Science*, pp. 151–165, Springer, 1988.

[6] S. Cheng and L. Chang, "Two constructions of multi-sender authentication codes with arbitration based linear codes to be published in ," *WSEAS Transactions on Mathematics*, vol. 11, no. 12, 2012.

[7] R. Safavi-Naini and H. Wang, "New results on multi-receiver authentication codes," in *Advances in Cryptology—EUROCRYPT '98 (Espoo)*, vol. 1403 of *Lecture Notes in Comput. Sci.*, pp. 527–541, Springer, Berlin, Germany, 1998.

[8] R. Aparna and B. B. Amberker, "Multi-sender multi-receiver authentication for dynamic secure group communication," *International Journal of Computer Science and Network Security*, vol. 7, no. 10, pp. 47–63, 2007.

[9] R. Safavi-Naini and H. Wang, "Bounds and constructions for multireceiver authentication codes," in *Advances in cryptology—ASIACRYPT'98 (Beijing)*, vol. 1514 of *Lecture Notes in Comput. Sci.*, pp. 242–256, Springer, Berlin, Germany, 1998.

[10] S. Shen and L. Chen, *Information and Coding Theory*, Science press in China, 2002.

[11] J. J. Rotman, *Advanced Modern Algebra*, High Education Press in China, 2004.

[12] Z. Wan, *Geometry of Classical Group over Finite Field*, Science Press in Beijing, New York, NY, USA, 2002.