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

Copyright © 2013 Xiuli Wang. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

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 $i$th sender $U_i$ ($i = 1, 2, \ldots, n$), secretly; then he calculates $e_R$ 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 \( P_L \) the largest probability of some opponent’s successful impersonation attack to receiver; it can be expressed as

\[
P_L = \max_{m \in M} \left\{ \frac{|e_R \in E_R \mid e_R \subset m|}{|E_R|} \right\}.
\] (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

\[
P_S = \max_{m \in M} \left\{ \max_{m' \in M} \left\{ \frac{|e_R \in E_R \mid e_R \subset m, m'|}{|E_R|} \right\} \right\}.
\] (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 \( E_L = \{E_{U_{i_1}}, E_{U_{i_2}}, \ldots, E_{U_{i_l}}\}. \) 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

\[
P_U(L) = \max_{e_t \in E_t} \max_{e_R \in E_R} \left\{ \frac{\max_{m \in M} \left\{ |e_R \in E_R \mid e_R \subset m, p(e_R, e_p) \neq 0 \right\}}{|E_R|} \right\}.
\] (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 \( F_q^* \) the nonzero elements set of \( F_q \). In this paper, we will use the following conclusions over finite fields.

Conclusion 1. A generator \( \alpha \) of \( F_q^* \) is called a primitive element of \( F_q \).

Conclusion 2. Let \( \alpha \in F_q \); if some polynomials contain \( \alpha \) 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 \( |F| = q^k \), then \( F \) is an \( n \)-dimensional vector space over \( F_q \). Let \( \alpha \) be a primitive element of \( F_q \), and \( g(x) \) the minimal polynomial about \( \alpha \) over \( F_q \); then \( \dim g(x) = n \) and \( 1, \alpha, \alpha^2, \ldots, \alpha^{n-1} \) is a basis of \( F \). Furthermore, \( 1, \alpha, \alpha^2, \ldots, \alpha^m-1 \) is linear independent, and \( \alpha \) is also linear independent; moreover, \( \alpha^p, \alpha^{2p}, \ldots, \alpha^{p^{m-1}}, \alpha^{p^m} \) is linear independent.

Conclusion 4. Consider \( (x_1 + x_2 + \cdots + x_m)^m = (x_1)^m + (x_2)^m + \cdots + (x_m)^m \), 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 \( q^{m(m-1)/2} \prod_{i=m-1}^{n} (q^i - 1) \).

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

3. Construction

Let the polynomial \( p(x) = a_1x^p + a_2x^{p^2} + \cdots + a_mx^{p^m} + 1 \geq j \leq k \), where the coefficient \( a_{ij} \in F_q \), \( 1 \leq i \leq n \), and these vectors by the composition of their coefficient are linearly independent. The set of source states \( S = F_q^* \); the set of \( i \)th 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 \( \alpha \) is a primitive element of \( F_q^* \); the set of \( i \)th 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 \( f_i : S \times E_i \to T_i \), \( f_i(s, e_i) = s p_i(x_i) + s^2 p_2(x_i) + \ldots + s^k p_k(x_i), 1 \leq i \leq n \).

The decoding map \( f : S \times E \to T \), \( f(s, e_R) = s p_1(\alpha) + s^2 p_2(\alpha) + \ldots + s^k p_k(\alpha) \).

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

The code works as follows.

Assume that \( q \) is larger than, or equal to, the number of the possible message and \( n \leq q \).

3.1. Key Distribution. The key distribution center randomly generates \( k (k \leq n) \) polynomials \( p_1(x), p_2(x), \ldots, p_k(x) \), where \( p_j(x) = a_{j1} x^{p_1} + a_{j2} x^{p_2} + \ldots + a_{jn} x^{p_n} (1 \leq j \leq k) \), and make these vectors by composed of their coefficient is linearly independent, it is equivalent to the column vectors of the matrix \( \begin{pmatrix} a_{i1} & a_{i2} & \cdots & a_{in} \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ a_{in} & a_{in} & \cdots & a_{in} \end{pmatrix} \) is linearly independent. He selects \( n \) distinct nonzero elements \( x_1, x_2, \ldots, x_n \in F_q \) again and makes \( x_i (1 \leq i \leq n) \) secret; then he sends privately \( p_1(x_i), p_2(x_i), p_3(x_i) \) to the sender \( U_i \) \((1 \leq i \leq n)\). The key distribution center also randomly chooses a primitive element \( \alpha \) of \( F_q \) satisfying \( x_1 + x_2 + \ldots + x_n = \alpha \) 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 \( t_i = f_i(s, e_{i}) = A_i(s_i) = sp_i(x_i) + s^2 p_2(x_i) + \ldots + s^k p_k(x_i), 1 \leq i \leq n \) and then sends \( A_i(s_i) = t_i \) to the synthesizer.

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

3.4. Verification. When the receiver \( R \) receives \( m = (s, t) \), he calculates \( t' = g(s, e_R) = A_i(s_i) = sp_1(\alpha) + s^2 p_2(\alpha) + \ldots + s^k p_k(\alpha) \). 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 \( C_i = (S, E_R, T_i, f_i) \); then the code is an \( A \)-code, \( 1 \leq i \leq n \).

**Proof.** (1) For any \( e_{U_i} \in E_{U_i}, s \in S \), because \( E_{U_i} = \{ p_1(x_i), p_2(x_i), \ldots, p_k(x_i), x_i \in E_{U_i} \} \), so \( t_i = sp_i(x_i) + s^2 p_2(x_i) + \cdots + s^k p_k(x_i) \) is only defined; that is, \( f_i (1 \leq i \leq n) \) is a surjection.

(2) If \( s' \in S \) is another source state satisfying \( sp_1(x_i) + s^2 p_2(x_i) + \cdots + s^k p_k(x_i) = s' p_1(x_i) + s'^2 p_2(x_i) + \cdots + s'^k p_k(x_i) \), and let \( t_i = f_i(s, e_{i}) = sp_i(x_i) + s^2 p_2(x_i) + \cdots + s^k p_k(x_i) \); it is equivalent to
\[
\begin{pmatrix} x_1^{p_1}, x_1^{p_1-1}, \ldots, x_1^{p_1} \\ x_2^{p_2}, x_2^{p_2-1}, \ldots, x_2^{p_2} \\ \vdots \vdots \vdots \\ x_n^{p_n}, x_n^{p_n-1}, \ldots, x_n^{p_n} \end{pmatrix} = t_i.
\]
It follows that
\[
\begin{pmatrix} x_1^{p_1}, x_1^{p_1-1}, \ldots, x_1^{p_1} \\ x_2^{p_2}, x_2^{p_2-1}, \ldots, x_2^{p_2} \\ \vdots \vdots \vdots \\ x_n^{p_n}, x_n^{p_n-1}, \ldots, x_n^{p_n} \end{pmatrix} \times \begin{pmatrix} a_{i1} & a_{i2} & \cdots & a_{ik} \\ a_{i1} & a_{i2} & \cdots & a_{ik} \\ \vdots \vdots \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ik} \end{pmatrix} = \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_n \end{pmatrix}.
\]

Denote
\[
A = \begin{pmatrix} a_{i1} & a_{i2} & \cdots & a_{ik} \\ a_{i1} & a_{i2} & \cdots & a_{ik} \\ \vdots \vdots \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ik} \end{pmatrix},
\]
\[
X = \begin{pmatrix} x_1^{p_1}, x_1^{p_1-1}, \ldots, x_1^{p_1} \\ x_2^{p_2}, x_2^{p_2-1}, \ldots, x_2^{p_2} \\ \vdots \vdots \vdots \\ x_n^{p_n}, x_n^{p_n-1}, \ldots, x_n^{p_n} \end{pmatrix},
\]
\[
S = \begin{pmatrix} s \\ s^2 \\ \vdots \\ s^k \end{pmatrix}, \quad t = \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_n \end{pmatrix}.
\]

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 also defined; that is, \( f_i (1 \leq i \leq n) \) is a surjection.

(2) If \( s' \in S \) is another source state satisfying \( sp_1(x_i) + s^2 p_2(x_i) + \cdots + s^k p_k(x_i) = s' p_1(x_i) + s'^2 p_2(x_i) + \cdots + s'^k p_k(x_i) \), 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
\[
\begin{pmatrix} x_1^{p_1}, x_1^{p_1-1}, \ldots, x_1^{p_1} \\ \vdots \vdots \vdots \\ x_n^{p_n}, x_n^{p_n-1}, \ldots, x_n^{p_n} \end{pmatrix} \times \begin{pmatrix} a_{i1} & a_{i2} & \cdots & a_{ik} \\ a_{i1} & a_{i2} & \cdots & a_{ik} \\ \vdots \vdots \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ik} \end{pmatrix} = \begin{pmatrix} s-s' \\ s^2-s'^2 \\ \vdots \\ s^k-s'^k \end{pmatrix} = 0.
\]
Thus

\[
\begin{pmatrix}
    x_1^n & x_1^{n-1} & \cdots & x_1^1 \\
    x_2^n & x_2^{n-1} & \cdots & x_2^1 \\
    \vdots & \vdots & \ddots & \vdots \\
    x_n^n & x_n^{n-1} & \cdots & x_n^1
\end{pmatrix}
\times
\begin{pmatrix}
    a_{11} & a_{21} & \cdots & a_{kn} \\
    a_{12} & a_{22} & \cdots & a_{kn} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{1n} & a_{2n} & \cdots & a_{kn}
\end{pmatrix}
= \begin{pmatrix}
    0 \\
    0 \\
    \vdots \\
    0
\end{pmatrix},
\]

(8)

Similar to (1), we know that the homogeneous linear equation \( X \mathbf{s} = 0 \) has a unique solution; that is, there is only one zero solution, so \( s = s' \). So, \( s \) is the unique source state determined by \( e_U \) and \( t_j \); thus, \( C_i \) (1 ≤ \( i \) ≤ \( n \)) 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 \( \alpha \) is a primitive element of \( F_q, g(s, e_R) = sp_1(\alpha) + sp_2(\alpha) + \cdots + sp_k(\alpha) \in T = E_R \); on the other hand, for any \( t \in T \), choose \( e_R = \{ p_1(\alpha), p_2(\alpha), \ldots, p_k(\alpha) \} \), where \( \alpha \) is a primitive element of \( F_q \), \( g(s, e_R) = sp_1(\alpha) + sp_2(\alpha) + \cdots + sp_k(\alpha) = t \); it is equivalent to

\[
\left( \alpha^n, \alpha^{n-1}, \ldots, \alpha^1 \right)
\times
\begin{pmatrix}
    a_{11} & a_{21} & \cdots & a_{kn} \\
    a_{12} & a_{22} & \cdots & a_{kn} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{1n} & a_{2n} & \cdots & a_{kn}
\end{pmatrix}
= \begin{pmatrix}
    s \\
    s^2 \\
    \vdots \\
    s^k
\end{pmatrix} = t,
\]

(9)

that is, \( (\alpha^n, \alpha^{n-1}, \ldots, \alpha^1)A \left( \begin{pmatrix} s \\ \vdots \\ s^k \end{pmatrix} \right) = t \). From Conclusion 3, we know that \( (\alpha^n, \alpha^{n-1}, \ldots, \alpha^1) \) 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

\[
\left( \alpha^n, \alpha^{n-1}, \ldots, \alpha^1 \right)A \left( \begin{pmatrix} s' \\ \vdots \\ s^k \end{pmatrix} \right) = \left( \begin{pmatrix} s \\ \vdots \\ s^k \end{pmatrix} \right) = 0.
\]

This means \( (\alpha^n, \alpha^{n-1}, \ldots, \alpha^1)A = 0 \). Sim-

ilar to (1), we get that the homogeneous linear equation \( (\alpha^n, \alpha^{n-1}, \ldots, \alpha^1)A(S' - S) = 0 \) 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 \( t_j \); thus, \( C_i = (S, E_R, T, g) \) 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 \( t' = sp_1(\alpha) + sp_2(\alpha) + \cdots + sp_k(\alpha) \in T = \mathbb{F}_q \); from Conclusion 4, \( (x_1 + x_2 + \cdots + x_n)^{m} = (x_1)^{m} + (x_2)^{m} + \cdots + (x_n)^{m} \), where \( m \) is a nonnegative power of character \( p \) of \( E_q \), 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, \( t' = sp_1(\alpha) + sp_2(\alpha) + \cdots + sp_k(\alpha) = (sp_1(x_1) + sp_2(x_1) + \cdots + sp_k(x_1)) + (sp_1(x_2) + sp_2(x_2) + \cdots + sp_k(x_2)) + \cdots + (sp_1(x_n) + sp_2(x_n) + \cdots + sp_k(x_n)) = t_1 + t_2 + \cdots + t_n = t \), 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.
From Conclusion 5, we can conclude that the number of $A$ satisfying the condition is $q^{k(k-1)/2} \sum_{m=0}^{m+k+1} (q^k - 1)$. On the other hand, the number of distinct nonzero elements $x_1 (\leq i \leq n)$ in $F_q$ is $q-1$, so $|E_{q_i}| = q^{k(k-1)/2} \sum_{m=0}^{m+k+1} (q^k - 1)$. For $E_{R^q}, E_{R^q} = \{p_1(\alpha), p_2(\alpha), \ldots, p_k(\alpha)\}$, where $\alpha$ is a primitive element of $F_q$. For $\alpha$, from Conclusion 1, a generator of $F_q$ is called a primitive element of $F_q$ if $|E_{q_i}| = q-1$; by the theory of the group, we know that the number of generators of $F_q$ is $q(q-1)$; that is, the number of $\alpha$ is $q(q-1)$.

For $p_1(x), p_2(x), \ldots, p_k(x)$, from above, we have confirmed that the number of these polynomials is $q^{k(k-1)/2} \sum_{m=0}^{m+k+1} (q^k - 1)$; therefore, $|E_{R^q}| = [q^{k(k-1)/2} \sum_{m=0}^{m+k+1} (q^k - 1)] q(q-1)$. 

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

**Proof.** Let $m = (s, t) \in M$, $e_R = \{p_1(\alpha), p_2(\alpha), \ldots, p_k(\alpha)\}$, where $\alpha$ is a primitive element of $F_q$. If $e_R \subset m$, then $s_1 p_1(\alpha) + s_2 p_2(\alpha) + \ldots + s_k p_k(\alpha) = t$ implies $(\alpha^s, \alpha^{s-1}, \ldots, \alpha^t) A = t$. For any $\alpha$, suppose that there is another $A'$ such that $(\alpha^s, \alpha^{s-1}, \ldots, \alpha^t) A' = t$, then $(\alpha^s, \alpha^{s-1}, \ldots, \alpha^t) (A - A') = 0$, because $(\alpha^s, \alpha^{s-1}, \ldots, \alpha^t)$ is linearly independent, so $(A - A') = 0$, but $(\alpha^s, \alpha^{s-1}, \ldots, \alpha^t)$ is arbitrarily; therefore, $A - A' = 0$; that is, $A = A'$, and it follows that $A$ is only determined by $\alpha$. Therefore, as $\alpha \in E_{R^q}$ for any given $s$ and $t$, the number of $e_R$ contained in $m$ is $q(q-1)$.

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

**Proof.** Assume that $e_R = \{p_1(\alpha), p_2(\alpha), \ldots, p_k(\alpha)\}$, where $\alpha$ is a primitive element of $F_q$. If $e_R \subset m$ and $e_R \subset m'$, then $s_1 p_1(\alpha) + s_2 p_2(\alpha) + \ldots + s_k p_k(\alpha) = t$ implies $(\alpha^s, \alpha^{s-1}, \ldots, \alpha^t) A = t$. For any $\alpha$, suppose that there is another $A'$ such that $(\alpha^s, \alpha^{s-1}, \ldots, \alpha^t) A' = t$, then $(\alpha^s, \alpha^{s-1}, \ldots, \alpha^t) (A - A') = 0$, because $(\alpha^s, \alpha^{s-1}, \ldots, \alpha^t)$ is linearly independent, so $(A - A') = 0$, but $(\alpha^s, \alpha^{s-1}, \ldots, \alpha^t)$ is arbitrarily; therefore, $A - A' = 0$; that is, $A = A'$, and that follows that $A$ is only determined by $\alpha$. Therefore, as $\alpha \in E_{R^q}$ for any given $s$ and $t$, the number of $e_R$ contained in $m$ and $m'$ is 1.

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

**Proof.** For any fixed $e_U = \{p_1(x), p_2(x), \ldots, p_k(x)\}$, $x_i \in F_q^\ast (1 \leq i \leq n)$ containing a given $e_L$, we assume that $p_j(x) = \alpha_j x_i^{e_1} + \alpha_{j1} x_i^{e_2} + \ldots + \alpha_j x_i^{e_l}$ (for $1 \leq j \leq k, 1 \leq i \leq n$, $e_R = \{p_1(\alpha), p_2(\alpha), \ldots, p_k(\alpha)\}$, where $\alpha$ is a primitive element of $F_q$. From the definitions of $e_R$ and $e_L$, and Conclusion 4, we can conclude that $e_R$ is incidence with $e_L$, if and only if $x_1 + x_2 + \ldots + x_n = \alpha$. For any $\alpha$, since $\text{Rank}(1, 1, \ldots, 1) = \text{Rank}(1, 1, \ldots, 1, \alpha) = 1 < n$, so the equation $x_1 + x_2 + \ldots + x_n = \alpha$ always has a solution. From Theorem 3, we know the number of $e_R$ which is incidence with $e_U$ (i.e., the number of all $E_{R^q})$ is $[q^{k(k-1)/2} \sum_{m=0}^{m+k+1} (q^k - 1)] q(q-1)$.

**Lemma 7.** For any fixed $e_U = \{p_1(x), p_2(x), \ldots, p_k(x)\}$, $x_i \in F_q^\ast (1 \leq i \leq n)$ 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 $s \in S$, $e_R \subset E_{R^q}$, we assume that $e_R = \{p_1(x), p_2(x), \ldots, p_k(x)\}$, where $\alpha$ is a primitive element of $F_q$. Similar to Lemma 6, for any fixed $e_U = \{p_1(x), p_2(x), \ldots, p_k(x)\}$, $x_i \in F_q^\ast (1 \leq i \leq n)$ containing a given $e_L$, we have known that $e_R$ is incidence with $e_U$ if and only if

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

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

$$s p_1(\alpha) + s_2 p_2(\alpha) + \ldots + s_k p_k(\alpha) = t. \quad (12)$$

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

$$s p_1(\sum_{i=1}^{n} x_i) + s_2 p_2(\sum_{i=1}^{n} x_i) + \ldots + s_k p_k(\sum_{i=1}^{n} x_i) = t \iff \left( p_1(\sum_{i=1}^{n} x_i), p_2(\sum_{i=1}^{n} x_i), \ldots, p_k(\sum_{i=1}^{n} x_i) \right).$$
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, \((\sum_{i=1}^{n} x_{i})^{n}, (\sum_{i=1}^{n} x_{i})^{n-1}, \ldots, (\sum_{i=1}^{n} x_{i})) A = 0\). Therefore, \( \{e_{R} \in E_{R} | m \subseteq m' \} = \{e_{R} \in E_{R} | e_{R} \subseteq m \} \).

By Lemmas 4 and 5, we get

\[
P_{S} = \max_{m \subseteq m' \in M} \left\{ \frac{\max_{e_{R} \in E_{R}} \{e_{R} \in E_{R} | e_{R} \subseteq m, m' \}}{\max_{e_{R} \in E_{R}} \{e_{R} \in E_{R} | e_{R} \subseteq m \}} \right\} \]

(16)

By Lemmas 6 and 7, we get

\[
P_{U} (L) = \max_{e_{R} \in E_{R}} \left\{ \frac{\max_{e_{R} \in E_{R}} \{e_{R} \in E_{R} | e_{R} \subseteq m, p(e_{R}, e_{R}) \neq 0 \}}{\max_{e_{R} \in E_{R}} \{e_{R} \in E_{R} | p(e_{R}, e_{R}) \neq 0 \}} \right\} \]

(17)

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

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

\[
(15)
\]

\[
\begin{aligned}
= t & \iff \left( \sum_{i=1}^{n} p_{1}(x_{i}), \sum_{i=1}^{n} p_{2}(x_{i}), \ldots, \sum_{i=1}^{n} p_{k}(x_{i}) \right) \left( \begin{array}{c}
\sum_{i=1}^{n} x_{i} \\
\sum_{i=1}^{n} x_{i}^{2} \\
\vdots \\
\sum_{i=1}^{n} x_{i}^{k}
\end{array} \right) \\
= t & \iff \left( \sum_{i=1}^{n} p_{1}(x_{i}), \sum_{i=1}^{n} p_{2}(x_{i}), \ldots, \sum_{i=1}^{n} p_{k}(x_{i}) \right) A \left( \begin{array}{c}
\sum_{i=1}^{n} x_{i} \\
\sum_{i=1}^{n} x_{i}^{2} \\
\vdots \\
\sum_{i=1}^{n} x_{i}^{k}
\end{array} \right)
\end{aligned}
\]

(13)

**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

\[
P_{I} = \frac{1}{q^{k(k-1)/2} \prod_{i=1}^{n} (q^{i} - 1)},
\]

\[
P_{S} = \frac{1}{\phi(q - 1)},
\]

\[
P_{U} (L) = \frac{1}{q^{k(k-1)/2} \prod_{i=1}^{n} (q^{i} - 1)} \phi(q - 1).
\]

(14)

**Proof.** By Theorem 3 and Lemma 4, we get

\[
P_{I} = \max_{m \subseteq E_{R}} \left\{ \frac{|e_{R} \in E_{R} | e_{R} \subseteq m|}{|E_{R}|} \right\}
\]

\[
(12)
\]

**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**


Submit your manuscripts at http://www.hindawi.com