DOI:10.11916/j.issn.1005-9113.17021

A Construction of Multi-Sender Authentication Codes from Eigenvalues and Eigenvectors of the Matrix Over Finite Fields

Xiuli Wang, Lina Wang and Yakun Hao*

(*College of Science, Civil Aviation University of China, Tianjin 300300, China*)

Abstract: We construct one multi-sender authentication code by algebraic combination method from eigenvalues and eigenvectors of the matrix over finite fields. Some parameters and the probabilities of three kinds of successful attack of this code are also computed. For multi-sender authentication code, it allows a group of senders to construct an authenticated message for a receiver such that the receiver can verify authenticity of the received message.

Keywords: multi-sender authentication codes; nonsingular symmetric matrix; eigenvalues; eigenvectors; finite fields

CLC number: O157.4; O236.2 **Document code**: A **Article ID**: 1005-9113(2019)01-0051-10

1 Introduction

Multi-sender authentication code was given by Gilbert, Macwilliams and Sloane firstly in Ref.[1] in 1974. Multi-sender authentication system refers to that a group of senders cooperatively transmits a message to a receiver, and then the receiver should be able to ascertain that the message is authentic. The results of the study on authentication codes and Multi-sender authentication codes were very fruitful and many scholars made great contributions [2-16].

In the realistic computer network communications, Multi-sender authentication code includes two kinds of models, that is, sequential model and simultaneous model. Sequential model refers to that each sender uses his own encoding rules to encode a source state in order, and the final sender transmits the encoded message to the receiver, the receiver receives the message and identities whether the message is legal or not. Simultaneous model refers to that all senders use their own encoding rules to encode a source state, and each sender transmits the encoded message to the synthesizer respectively, then the synthesizer forms an authenticated message and transmits the authenticated message to the receiver, the receiver receives the message and identifies whether the message is legal or not. In this article, the second model is adopted.

In a simultaneous model, there are four participants: a group of senders $U = \{U_1, U_2, \cdots, U_n\}$, a receiver R, the keys distribution center and a synthesizer. The keys distribution center is responsible for the key distribution to senders and receiver, including settling the disputes between senders and receiver. The synthesizer only runs the reliable synthesis algorithm. 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 sender's 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 agreement: the key distribution center randomly selects an encoding rule $e \in E$ and transmits $e_i = \pi_i(e)$ to the ith sender $U_i(1, 2, \cdots, n)$ secretly, then it computes e_R by e according to an efficient algorithm, and secretly transmits e_R to the receiver R. If the senders would like to transmit a source state s to the receiver R, U_i computes $t_i = f_i(s, e_i)$ $(i = 1, 2, \cdots,$

Received 2017-02-16.

Sponsored by the National Natural Science Foundation of China (Grant No. 61179026) and the Fundamental Research of the Central Universities of China Civil Aviation University of Science Special (Grant No. 3122016L005).

* Corresponding author. E-mail: xlwangcauc@163.com.

n) and transmits $m_i = (s, t_i)(i = 1, 2, \cdots, n)$ to the synthesizer through an open channel. The synthesizer receives the message $m_i = (s, t_i)(i = 1, 2, \cdots, n)$ and computes $t = h(t_1, t_2, \cdots, t_n)$ by the synthesis algorithm h, then transmits the message $m = (s, t)$ to the receiver, it checks the authenticity by identifying whether $t = g(s, e_R)$ or not. If the equality holds, the message is authentic and is accepted. If not, the message is rejected.

Suppose the key distribution center is reliable, though he knows the senders' and receiver's encoding rules, it will not participate in any communication activities. When senders and receiver are disputing, the key distribution center solves it. At the same time, suppose the system follows the Kerckhoff's principle which excepts the actual used keys, the other information of the whole system is public.

In a Multi-sender authentication system, suppose that the whole senders are cooperated to form a valid message, that is, all senders as a whole and receiver are reliable. But there are some malicious senders, they unite to deceive the receiver, the part of senders and receiver are not reliable, they can take impersonation attack and substitution attack. In the whole system, suppose $\{U_1, U_2, \cdots, U_n\}$ 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 conform 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. We denote $L = \{i_1, i_2, \cdots, i_l\} \subset \{1, 2, \cdots, n\}$, $l < n$, $U_L = \{U_{i_1}, U_{i_2}, \cdots, U_{i_l}\}$, $E_L = \{E_{i_1}, E_{i_2}, \cdots, E_{i_l}\}$. Now study the attacks from malicious groups of transmitters. We consider three kinds of spoofing attack:

1) The opponent's impersonation attack to receiver. U_L, after receiving their secret keys, encodes a message and transmits it to receiver. U_L is successful if receiver accepts it as legitimate message. Denote P_I the largest probability of some opponent's successful impersonation attack to receiver, it can be represented as:

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

2) The opponent's substitution attack to the receiver. U_L uses another message m' instead of the message m, after they observe a legitimate message m. U_L is successful if the receiver accepts it as a legitimate message, it can be represented as:

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

3) There might be l malicious senders who unite to cheat the receiver, that is, the part of senders and the receiver are not reliable, 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, transmits a message m to the receiver R, U_L is successful if the receiver accepts it as a legitimate message. Denote $P_U(L)$ the maximum probability of success of the impersonation attack to the receiver. It can be represented as:

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

2 Preliminary Knowledge

2.1 Definition of Finite Fields and Some Relevant Conclusions

Definition 2.1.1 A finite field is a field that contains finite elements.

Theorem 2.1.2 Let F_q be the finite field with q elements, denote F_q^* all nonzero elements set of F_q, and F_q^* forms a cycle group.

Definition 2.1.3 A generator α of F_q^* is called a primitive element of F_q.

Definition 2.1.4 Let α be a primitive element of F_q, then $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ are linearly independent, furthermore, $\alpha, \alpha^2, \cdots, \alpha^n (n < q)$ are also linearly independent.

Theorem 2.1.5 Let α be a generator of F_q^*, and if k is an integer that is relatively prime to m, then α^k is also a generator of F_q^*.

The above conclusions come from the Ref.[17].

2.2 Eigenvalues and Eigenvectors of a Matrix and the Relevant Properties

Definition 2.2.1 Let $\boldsymbol{A}$ be a matrix over $F_q^{n \times n}$, $\boldsymbol{x}$ be a n dimension non-zero column vector over F_q, $\lambda \in F_q$ be a number, if the equation $\boldsymbol{Ax} = \lambda \boldsymbol{x}$ holds, then we call $\boldsymbol{x}$ an eigenvector of $\boldsymbol{A}$, and call λ

an eigenvalue of $\boldsymbol{A}$ corresponding to $\boldsymbol{x}$.

Theorem 2.2.2 A $n \times n$ matrix $\boldsymbol{A}$ is diagonalized if and only if $\boldsymbol{A}$ has n linearly independent eigenvectors.

Theorem 2.2.3 Let $\boldsymbol{A}$ be a $n \times n$ diagonalized matrix over F_q, $x_1, x_2, \cdots, x_n$ be n linearly independent unit eigenvectors (column vector) of $\boldsymbol{A}$, and $\lambda_1, \lambda_2, \cdots, \lambda_n$ be corresponding eigenvectors of $x_1, x_2, \cdots, x_n$ respectively. If we have the matrices

$$\boldsymbol{P} = [x_1, x_2, \cdots, x_n]$$

$$\boldsymbol{\Lambda} = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix}$$

then the equation $\boldsymbol{A} = \boldsymbol{P\Lambda P}^{-1}$ holds.

Theorem 2.2.4 A n order invertible symmetrical matrix must be diagonalized.

Lemma 2.2.5 If $\boldsymbol{A}$ is a $n \times n$ invertible symmetrical matrix, then the eigenvectors of corresponding different eigenvalues are orthogonal. Making these linearly independent eigenvector which are corresponding multiple eigenvalue of $\boldsymbol{A}$ are orthogonal to each other by Schmidt orthogonal method, and making them unitization again, we get a group of orthogonal unitization eigenvectors $\xi_1, \xi_2, \cdots, \xi_n$. Denote $\boldsymbol{P} = [\xi_1, \xi_2, \cdots, \xi_n]$, obviously, $\boldsymbol{P}$ is an orthogonal matrix and the equation $\boldsymbol{A} = \boldsymbol{P\Lambda P}^{-1}$ holds.

The above conclusions come from the Pef.[18].

Theorem 2.2.6[19] The number of invertible matrix over $F_q^{n\times n}$ is

$$\prod_{j=0}^{n-1}(q^n - q^j) = q^{\frac{n(n-1)}{2}} \prod_{j=1}^{n}(q^j - 1)$$

Theorem 2.2.7[18] If for any n order square matrix $\boldsymbol{A}$, a n order square matrix $\boldsymbol{P}$ satisfying the equation $\boldsymbol{AP} = \boldsymbol{PA}$, then $\boldsymbol{P}$ is a n order scalar matrix.

2.3 Related Definition of Authentication Codes

Definition 2.3.1[3] Let S, E and M be nonempty set. Assume $f: S \times E \to M$ is a surjective mapping from $S \times E$ to M, if for any given $e \in E$, $m \in M$, s satisfying $f(s,e) = m$ is uniquely determined by e and m, then we called the tetrad $(S, E, M; f)$ an authentication code.

2.4 Some Definition and Related Properties of Group Theory

Definition 2.4.1 Suppose $\boldsymbol{G}$ is a group, $\boldsymbol{H}$ is a subgroup of $\boldsymbol{G}$, then the number of left (or right) cosets of $\boldsymbol{H}$ in $\boldsymbol{G}$ is called index of $\boldsymbol{H}$ in $\boldsymbol{G}$, denoted by $[\boldsymbol{G}: \boldsymbol{H}]$.

Theorem 2.4.2 Let $\boldsymbol{G}$ be a finite group. If $\boldsymbol{H}$ is a subgroup of $\boldsymbol{G}$, then $|\boldsymbol{G}| = |\boldsymbol{H}|[\boldsymbol{G}: \boldsymbol{H}]$.

Definition 2.4.3 Suppose Ω be the object set and the group G effects on Ω, $a \in \Omega$, then $\Omega_a = \{g(a) \mid g \in G\}$ is called an orbit of Ω under G, a is called representative element of the orbit.

Definition 2.4.4 Let the group $\boldsymbol{G}$ effect on Ω, $a \in \Omega$, then $G_a = \{g \mid g \in \boldsymbol{G}, g(a) = a\}$ is called stable subgroup about the element a, denoted by $Stab_G^a$.

Theorem 2.4.5 For the group $\boldsymbol{G}$, the orbit Ω_a and the stable subgroup G_a, the orbit formula about them is as follows: $|\Omega_a| = [G: G_a]$.

The above conclusions come from the Ref.[20].

2.5 Some Definition and Properties of the Matrix Over Finite Fields

Definition 2.5.1 Let $\boldsymbol{S}$ be an $n \times n$ invertible symmetric matrix over F_q, a $n \times n$ invertible symmetric matrix $\boldsymbol{T}$ is called orthogonal with respect to $\boldsymbol{S}$, if the following equation holds: $\boldsymbol{TST}^{\mathrm{T}} = \boldsymbol{S}$.

Theorem 2.5.2 A $n \times n$ invertible symmetric matrix over F_q is cogredient to one and only one of the following four normal forms:

$$\boldsymbol{S}_{2\nu} = \begin{bmatrix} 0 & I^{(\nu)} \\ I^{(\nu)} & 0 \end{bmatrix}$$

$$\boldsymbol{S}_{2\nu+1,1} = \begin{bmatrix} 0 & I^{(\nu)} & 0 \\ I^{(\nu)} & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\boldsymbol{S}_{2\nu+1,z} = \begin{bmatrix} 0 & I^{(\nu)} & 0 \\ I^{(\nu)} & 0 & 0 \\ 0 & 0 & z \end{bmatrix}$$

$$\boldsymbol{S}_{2\nu+2} = \begin{bmatrix} 0 & I^{(\nu)} & 0 & 0 \\ I^{(\nu)} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -z \end{bmatrix}$$

The above is the corresponding form successively when $n = 2\nu$, $n = 2\nu + 1$, $n = 2\nu + 1$ and $n = 2\nu + 2$ respectively. In order to cover the four cases at the same time, we introduce the sign $\boldsymbol{S}_{2\nu+\delta,\Delta}$, where ν is its index, Δ denotes its definite part, the expression of Δ is as follows:

$$\Delta = \begin{cases} \phi, & \delta = 0 \\ (1) \text{ or } (z), & \delta = 1 \\ \begin{bmatrix} 1 & 0 \\ 0 & -z \end{bmatrix}, & \delta = 2 \end{cases}$$

Theorem 2.5.3 Denote the set of all matrices which is orthogonal with respect to $\boldsymbol{S}_{2\nu+\delta,\Delta}$ over F_q by $O_{2\nu+\delta,\Delta(F_q)}$, then,

$$O_{2\nu+\delta,\Delta(F_q)} = q^{\nu(\nu+\delta-1)} \prod_{i=1}^{\nu} (q^i - 1) \prod_{i=0}^{\nu+\delta-1} (q^i + 1)$$

The above conclusions come from the Ref.[19].

3 Construction of the Multi-sender Authentication Code

3.1 Construction of the Multi-sender Authentication Code

Let F_q be a finite field of characteristic not 2, with $q \geqslant 5$, $\boldsymbol{A}$ be a nonsingular symmetric matrix over $\boldsymbol{F}_q^{n\times n}$, $\lambda_1, \lambda_2, \cdots, \lambda_n$ be eigenvalues of $\boldsymbol{A}$, $\xi_1, \xi_2, \cdots, \xi_n$ be corresponding orthogonal unit eigenvectors, $\boldsymbol{P} = [\xi_1, \xi_2, \cdots, \xi_n]$, obviously $\boldsymbol{P}$ is an orthogonal matrix, $\boldsymbol{\Lambda}$ be a diagonal matrix over $\boldsymbol{F}_q^{n\times n}$, its form is as follows:

$$\boldsymbol{\Lambda} = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix}$$

From Theorem 2.2.5, we know that $\boldsymbol{A} = \boldsymbol{P}\boldsymbol{\Lambda}\boldsymbol{P}^{-1}$, $\boldsymbol{\Lambda} = \boldsymbol{P}^{-1}\boldsymbol{A}\boldsymbol{P}$. Set α is a primitive element of F_q, $N = \{1, 2, \cdots, n\}$.

The source states set $S = F_q^*$;

The encoding rules set of the senders is $E_{U_i} = \{(\lambda_1, i) \mid \lambda_i \in F_q^*, i \in N\} (1 \leqslant i \leqslant n)$.

The decoding rules set of the receiver is $E_R = \{(\boldsymbol{P}, \boldsymbol{A}, \alpha) \mid P, \boldsymbol{A} \in F_q^{n\times n}, \alpha \text{ is a primitive element}\}$;

The label set of the sender $T_i = F_q^* (1 \leqslant i \leqslant n)$;

The label set of the receiver is $T = F_q^*$;

The encoding function of the sender U_i: f_i:

$S \times E_{U_i} \rightarrow T_i$, $f_i(s, e_{U_i}) = \lambda_i s^i, 1 \leqslant i \leqslant n$

The decoding function of the receiver R:

$$g: S \times E_R \rightarrow T$$

$$\boldsymbol{g}(s, e_R) = [s, s^2, \cdots, s^n] \boldsymbol{P}^{-1} \boldsymbol{A} \boldsymbol{P} \begin{bmatrix} \alpha \\ \alpha^2 \\ \vdots \\ \alpha^n \end{bmatrix}$$

The Multi-sender authentication code works as follows:

1) Key distribution. The key distribution center randomly generates a $n \times n$ nonsingular symmetric matrix $\boldsymbol{A}$ over F_q. He computes n eigenvalues and n corresponding orthogonal unit eigenvectors, and selects a eigenvalue randomly, denoted by λ_i. If λ_i is a k-tuples eigenvalue, then it is taken k times at most, and it selects a eigenvector from all these orthogonal unit eigenvectors belonging to λ_i, denoted by ξ_i, and it sends privately (λ_i, i) to the sender $U_i (1 \leqslant i \leqslant n)$, it means $e_{U_i} = (\lambda_i, i)$. After all e_{U_i} have been sent, $\xi_1, \xi_2, \cdots, \xi_n$ will be defined. When he generates the matrix $\boldsymbol{P} = [\xi_1, \xi_2, \cdots, \xi_n]$, he selects a primitive elements α of F_q, and sends $(\boldsymbol{A}, \boldsymbol{P}, \alpha)$ to the receiver R, it means $e_R = (\boldsymbol{A}, \boldsymbol{P}, \alpha)$.

2) Broadcast. If the senders would like to transmit a source state $s \in S$ to the receiver R, then the sender U_i computes $t_i = f_i(s, e_{U_i}) = \lambda_i s^i (1 \leqslant i \leqslant n)$ and sends t_i to the synthesizer H.

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

4) Verification. When the receiver R receives $m = (s, t)$, it calculates

$$t' = g(s, e_R) = [s, s^2, \cdots, s^n] \boldsymbol{P}^{-1} \boldsymbol{A} \boldsymbol{P} \begin{bmatrix} \alpha \\ \alpha^2 \\ \vdots \\ \alpha^n \end{bmatrix}$$

If $t = t'$, it accepts t; If not, it rejects it.

From the definition of these parameters, we know when there is no attack.

$$t' = [s, s^2, \cdots, s^n] \boldsymbol{P}^{-1} \boldsymbol{A} \boldsymbol{P} \begin{bmatrix} \alpha \\ \alpha^2 \\ \vdots \\ \alpha^n \end{bmatrix} =$$

$$[s, s^2, \cdots, s^n] \boldsymbol{\Lambda} \begin{bmatrix} \alpha \\ \alpha^2 \\ \vdots \\ \alpha^n \end{bmatrix} =$$

$$[s, s^2, \cdots, s^n] \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix} \begin{bmatrix} \alpha \\ \alpha^2 \\ \vdots \\ \alpha^n \end{bmatrix} =$$

$$\lambda_1 s\alpha + \lambda_2 s^2\alpha^2 + \cdots + \lambda_n s^n\alpha^n =$$

$$t_1\alpha + t_2\alpha^2 + \cdots + t_n\alpha^n = t$$

3.2 The Rationality of the Constructed Authentication Code

Lemma 3.2.1 Let $C_i = (S, E_{U_i}, T_i; f_i) (1 \leqslant i \leqslant n)$. Then the code is an A-code for the sender.

Proof For any $e_{U_i} \in E_{U_i}, s \in S$, because $E_{U_i} = (F_q^*, N), S = F_q^*$, so $t_i = \lambda_i s^i \in F_q^* = T_i$. For any $t_i \in T_i = F_q^*$, because F_q^* forms a cyclic group and the primitive element α of F_q is a generator of F_q^*, so we can assume $t_i = \alpha^k$. We choose $e_{U_i} = (\lambda_i, i) = (\alpha^{k-i}, i) \in (F_q^*, N) = E_{U_i}$, then there is $s = \alpha$ such that $f_i(s, e_{U_i}) = \lambda_i s^i = \alpha^{k-i} \cdot \alpha^i = \alpha^k = t_i$ holds, so f_i is surjective.

If $s' \in S$ is another source state satisfying $t_i = \lambda_i s^i (1 \leqslant i \leqslant n)$, that is,

$$[s', s'^2, \cdots, s'^n] \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix} = \begin{bmatrix} t \\ t^2 \\ \vdots \\ t^n \end{bmatrix}$$

then

$$[s', s'^2, \cdots, s'^n] \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix} = \begin{bmatrix} t \\ t^2 \\ \vdots \\ t^n \end{bmatrix} =$$

$$[s, s^2, \cdots, s^n] \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix}$$

and

$$[s - s', s^2 - s'^2, \cdots, s^n - s'^n] \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix} = 0$$

Because $\lambda_i \in F_q^*$, that is, $\lambda_i \neq 0$, so

$$\begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix}$$

is invertible. Therefore $[s - s', s^2 - s'^2, \cdots, s^n - s'^n] = [0, 0, \cdots, 0]$, then $s' = s$, that is, s is the unique source state determined by e_{Ui} and t_i.

In conclusion, $C_i (1 \leqslant i \leqslant n)$ is an A-code for the senders.

Lemma 3.2.2 Let $C = (S, E_R, T; g)$, then the code is an A-code for the receiver.

Proof (1) For any $s \in S$, $e_R \in E_R$, because $S = F_q^*$, $E_R = \{ (\boldsymbol{P}, \boldsymbol{A}, \alpha) \mid \boldsymbol{P}, \boldsymbol{A} \in \boldsymbol{F}_q^{n \times n}$, α is a primitive element$\}$, then

$$g(s, e_R) = [s, s^2, \cdots, s^n] \boldsymbol{P}^{-1} \boldsymbol{A} \boldsymbol{P} [\alpha, \alpha^2, \cdots, \alpha^n]^{\mathrm{T}} = t \in F_q^*$$

otherwise, we suppose

$$[s, s^2, \cdots, s^n] \boldsymbol{P}^{-1} \boldsymbol{A} \boldsymbol{P} [\alpha, \alpha^2, \cdots, \alpha^n]^{\mathrm{T}} = t = 0$$

Because $\alpha_1, \alpha_2, \cdots, \alpha_n$ is linearly independent, so $[s, s^2, \cdots, s^n] \boldsymbol{P}^{-1} \boldsymbol{A} \boldsymbol{P} = 0$, but $\boldsymbol{P}^{-1} \boldsymbol{A} \boldsymbol{P}$ is invertible, so $[s, s^2, \cdots, s^n] = [0, 0, \cdots, 0]$, that is, $s = 0$, it is a contradiction to $s \in S = F_q^*$. Meanwhile, for any $t \in T$, we choose $e_R \in E_R$. Since $s \in S$ such that $g(s, e_R) = t$ holds, then

$$[s, s^2, \cdots, s^n] \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix} \begin{bmatrix} \alpha \\ \alpha^2 \\ \vdots \\ \alpha^n \end{bmatrix} = t$$

It is equivalent to

$$[\alpha_1, \alpha_2, \cdots, \alpha_n] \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix} \begin{bmatrix} s \\ s^2 \\ \vdots \\ s^n \end{bmatrix} = t$$

Let $x_1 = s, x_2 = s^2, \cdots, x_n = s^n$ be unknown variable, getting the matrix $\boldsymbol{B}$ as follows:

$$\boldsymbol{B} = [\alpha_1, \alpha_2, \cdots, \alpha_n] \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix}$$

So getting a system of linear equations in the variables

$$x_1, x_2, \cdots, x_n : \boldsymbol{B} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = t$$

where $\boldsymbol{B}$ is the coefficient matrix of the system of linear equations. Obviously $\mathrm{rank}(\boldsymbol{B}) = 1, \bar{\boldsymbol{B}} = [B, t]$ is the augmented matrix the system of linear equations, from the definition of α, λ_i, t, we know $\mathrm{rank}(\bar{\boldsymbol{B}}) = 1$, that is, $\mathrm{rank}(\boldsymbol{B}) = \mathrm{rank}(\bar{\boldsymbol{B}}) = 1$. Therefore, from Theorem 2.2.8, the system of linear equations has solution, that is, there exists s satisfying $g(s, e_R) = t$. So g is surjective.

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

$$[s', s'^2, \cdots, s'^n] \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix} \begin{bmatrix} \alpha \\ \alpha^2 \\ \vdots \\ \alpha^n \end{bmatrix} = t =$$

$$[s, s^2, \cdots, s^n] \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix} \begin{bmatrix} \alpha \\ \alpha^2 \\ \vdots \\ \alpha^n \end{bmatrix}$$

$$[s - s', s^2 - s'^2, \cdots, s^n - s'^n] \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix} \begin{bmatrix} \alpha \\ \alpha^2 \\ \vdots \\ \alpha^n \end{bmatrix} = 0$$

$$[\alpha_1, \alpha_2, \cdots, \alpha_n] \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix} \begin{bmatrix} s - s' \\ s^2 - s'^2 \\ \vdots \\ s^n - s'^n \end{bmatrix} = 0 \quad (1)$$

Because α is primitive element, from Theorem 2.1.4, we know that $\alpha,\alpha^2,\cdots,\alpha^n$ linearly independent. So

$$\begin{bmatrix}\lambda_1 & 0 & \cdots & 0\\ 0 & \lambda_2 & \cdots & 0\\ \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & \cdots & \lambda_n\end{bmatrix}\begin{bmatrix}s-s'\\ s^2-s'^2\\ \vdots\\ s^n-s'^n\end{bmatrix}=0$$

Because $\lambda_i \neq 0\ (1 \leqslant i \leqslant n)$,

$$\begin{bmatrix}\lambda_1 & 0 & \cdots & 0\\ 0 & \lambda_2 & \cdots & 0\\ \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & \cdots & \lambda_n\end{bmatrix}$$

is invertible. Therefore, the above system of the Eq. (1) has only zero solution. Then

$$[s-s',s^2-s'^2,\cdots,s^n-s'^n]=[0,0,\cdots,0]$$

So $s-s'=0, s'=s$, that is, s satisfying $g(s,e_R)=t$ is the unique determined by e_R and t.

In conclusion, the code is an A-code for the receiver.

From Lemmas 3.2.1 and 3.2.2, it can be seen that the construction of this Multi-sender authentication code is reasonable. Next, we will begin to calculate the relevant parameters of constructed Multi-sender authentication code.

3.3 Computation of the Relevant Parameters About the Constructed Authentication Code

Lemma 3.3.1 Some relevant parameters of Multi-sender authentication code are as follows:

$$|S|=q-1,\ |T|=q-1,\ |T_i|=q-1$$
$$E_{U_i}=n(q-1)\ (1\leqslant i\leqslant n)$$

Proof From the definitions of S, T, T_i and E_{U_i}, these results are obvious.

Theorem 3.3.2 Let $\boldsymbol{A}$ be $n\times n$ invertible symmetrical matrix over F_q. If $\boldsymbol{A}$ is cogredient to $S_{2v+\delta,\Delta}$ of Theorem 2.5.2, where $2v+\Delta=n$, then the number of such $\boldsymbol{A}$ is:

$$\Theta=\frac{q^{n(n-1)}\prod_{j=1}^{n}(q^j-1)}{q^{v(v+\delta-1)}\prod_{i=1}^{v}(q^i-1)\prod_{i=0}^{v+\delta-1}(q^i+1)}$$

Proof Let G be the set of all invertible matrix over $\boldsymbol{F}_q^{n\times n}$. Obviously, $(G,\times)$ is a group, where $\times$ is the multiplication with matrix, Ω be the set of all invertible symmetrical matrix over $\boldsymbol{F}_q^{n\times n}$. Choose $S_{2v+\delta}\in\Omega$. We assume that Ω forms an orbit under G, $\Omega_{S_{2v+\delta}}=\{\boldsymbol{T}(S_{2v+\delta},\Delta)\boldsymbol{T}\in G\}$, where $\boldsymbol{T}$ satisfies $\boldsymbol{T}(S)=\boldsymbol{T}\boldsymbol{S}\boldsymbol{T}^{\mathrm{T}}$. Obviously, $T(S)$ is cogredient to S, then the stable subgroup of $S_{2v+\delta,\Delta}$ is:

$$G_{S_{2v+\delta,\Delta}}=\{\boldsymbol{T}\mid \boldsymbol{T}\in G,\boldsymbol{T}(S_{2v+\delta,\Delta})=S_{2v+\delta,\Delta}\}$$

$\boldsymbol{T}$ contained in $G_{S_{2v+\delta,\Delta}}$ satisfies the equation $\boldsymbol{T}(S_{2v+\delta,\Delta})=\boldsymbol{T}S_{2v+\delta,\Delta}\boldsymbol{T}^{\mathrm{T}}=S_{2v+\delta,\Delta}$. According to Definition 2.5.1, $\boldsymbol{T}$ is orthogonal with respect to $S_{2v+\delta,\Delta}$, $G_{S_{2v+\delta,\Delta}}$ is composed of all $\boldsymbol{T}$ orthogonal with respect to $S_{2v+\delta,\Delta}$. Therefore, from Theorem 2.5.3, we know that

$$|G_{S_{2v+\delta,\Delta}}|=|O_{S_{2v+\delta,\Delta}}(F_q)|=q^{v(v+\delta-1)}\prod_{i=1}^{v}(q^i-1)\prod_{i=0}^{v+\delta-1}(q^i+1)$$

Therefore, by Theorem 2.4.4 and Theorem 2.4.7, we get

$$|\Omega_{S_{2v+\delta,\Delta}}|=|G:G_{S_{2v+\delta,\Delta}}|=\frac{|G|}{|G_{S_{2v+\delta,\Delta}}|}$$

Because G is the set of all invertible matrices over $\boldsymbol{F}_q^{n\times n}$ again, by Theorem 2.2.6, we know $|G|=q^{\frac{n(n-1)}{2}}\prod_{j=1}^{n}(q^j-1)$. Therefore,

$$|\Omega_{S_{2v+\delta,\Delta}}|=\frac{|G|}{|G_{S_{2v+\delta,\Delta}}|}=\frac{q^{n(n-1)}\prod_{j=1}^{n}(q^j-1)}{q^{v(v+\delta-1)}\prod_{i=1}^{v}(q^i-1)\prod_{i=0}^{v+\delta-1}(q^i+1)}$$

Since $\Omega_{S_{2v+\delta,\Delta}}$ is made up of all elements $\boldsymbol{A}$ which are cogredient to $S_{2v+\delta,\Delta}$, $|\Omega_{S_{2v+\delta,\Delta}}|$ is equal to the number of invertible symmetrical matrix over $\boldsymbol{F}_q^{n\times n}$ cogredienting to $S_{2v+\delta,\Delta}$, that is,

$$\Theta=\frac{q^{n(n-1)}\prod_{j=1}^{n}(q^j-1)}{q^{v(v+\delta-1)}\prod_{i=1}^{v}(q^i-1)\prod_{i=0}^{v+\delta-1}(q^i+1)}$$

Lemma 3.3.3 If α is a primitive element of F_q, then there are $\varphi(n-1)$ choices for α, where $\varphi(n-1)$ expresses the number of less than $q-1$ and relatively prime to $q-1$.

Proof Because α is a primitive element of F_q, by Definition 2.1.3, α is a generator of F_q^*, the order of α is m, from the properties of generator, $m=|F_q^*|=q-1$. If k is an integer that relatively prime to m, by Theorem 2.1.5, α^k is a generator of F_q^*, that is, α^k is a primitive element of F_q.

When $k>m, \alpha^k=\alpha^{k-m}$ and $k-m$ relatively prime to m, the number of generator in F_q^* is equal to the number of positive integer less than m and relatively prime with m, because $m=q-1$. Therefore, there are

$\varphi(n-1)$ choices of α.

Lemma 3.3.4

$$|E_R| = \Theta\varphi(q-1)n! \prod_{i=1}^{m} \frac{q^{s_i(s_i-1)/2}\prod_{j=1}^{s_i}(q^j-1)}{s_i!}$$

where Θ is given by Theorem 3.3.2, s_i means the multiple number of the eigenvalue λ_i and when $i \neq j$, $\lambda_i \neq \lambda_j, 1 \leqslant i,j \leqslant m, \sum_{i=1}^{m} s_i = n$.

Proof For any given $n \times n$ invertible symmetrical matrix $\boldsymbol{A}$ over F_q, it has m eigenvalues $\lambda_1,\lambda_2,\cdots,\lambda_m$ and they are different from each other, where λ_i is s_i multiple eigenvalues, $1 \leqslant i \leqslant m \leqslant n$ and $\sum_{i=1}^{m} s_i = n$. Because $\boldsymbol{A}$ is a symmetrical matrix, the eigenvalue λ_i has s_i linearly independent eigenvectors. In order to solve the corresponding eigenvectors of λ_i, need to solve the homogeneous linear equations $(\lambda_i\boldsymbol{E}-\boldsymbol{A})\boldsymbol{x}=0$. Since the rank of coefficient matrix $\lambda_i\boldsymbol{E}-\boldsymbol{A}$ is $n-s_i$, there are s_i free variables, the number of solutions of the homogeneous linear equations is equal to the number of invertible matrix, where the order of invertible matrix is s_i over F_q. By the theorem 2.2.5, the number of such invertible matrix is

$$\prod_{j=0}^{s_i-1}(q^{s_i}-q^j) = q^{s_i(s_i-1)/2}\prod_{j=1}^{s_i}(q^j-1)$$

Once the basic solutions system of $\lambda_i\boldsymbol{E}-\boldsymbol{A}$ is determined, then s_i linearly independent eigenvectors of λ_i are also unique determined and these eigenvectors are in order, when these eigenvectors are no order, suppose there are k_i possible choices for s_i eigenvectors, then there is the equation:

$$k_i s_i! = q^{s_i(s_i-1)/2}\prod_{j=1}^{s_i}(q^j-1)$$

so

$$k_i = \frac{q^{s_i(s_i-1)/2}\prod_{j=1}^{s_i}(q^j-1)}{s_i!}$$

By Schmidt orthogonal method, because the results of the orthogonality of the vector group $x_1,x_2,\cdots,x_n$ and the vector group $kx_1,kx_2,\cdots,kx_n(k\neq 0)$ are the same, so there are

$$\frac{k_i}{q-1} = \frac{q^{\frac{s_i(s_i-1)}{2}}\prod_{j=1}^{s_i}(q^j-1)}{(q-1)s_i!}$$

choice for s_i unit eigenvectors of corresponding to λ_i. Therefore, for any given matrix $\boldsymbol{A}$, the number of $\xi_1,\xi_2,\cdots,\xi_n$ possible choice is

$$\prod_{i=1}^{m}\frac{k_i}{q-1} = \prod_{i=1}^{m}\frac{q^{\frac{s_i(s_i-1)}{2}}\prod_{j=1}^{s_i}(q^j-1)}{(q-1)s_i!}$$

where $\xi_1,\xi_2,\cdots,\xi_n$ are no order.

From the construction method of $\boldsymbol{P}$ from the above, every possible choice of $\boldsymbol{P}$ all is a permutation for $\xi_1,\xi_2,\cdots,\xi_n$, therefore, for any given $\xi_1,\xi_2,\cdots,\xi_n$, there are $n!$ possible choice of $\boldsymbol{P}$. So for any given $\boldsymbol{A}$, the number of all possible cases of $\boldsymbol{P}$ is

$$n!\prod_{i=1}^{m}\frac{q^{\frac{s_i(s_i-1)}{2}}\prod_{j=1}^{s_i}(q^j-1)}{(q-1)s_i!}$$

Because $e_R = (A,P,\alpha)$, where there are Θ possible cases for $\boldsymbol{A}$, the number of P is

$$n!\prod_{i=1}^{m}\frac{q^{\frac{s_i(s_i-1)}{2}}\prod_{j=1}^{s_i}(q^j-1)}{(q-1)s_i!}$$

and there are $\varphi(n-1)$ choice for α. Therefore, there are

$$\Theta n!\prod_{i=1}^{m}\frac{q^{\frac{s_i(s_i-1)}{2}}\prod_{j=1}^{s_i}(q^j-1)}{(q-1)s_i!}$$

choice for $e_R = (A,P,\alpha)$. That is,

$$|E_R| = \Theta\varphi(q-1)n!\prod_{i=1}^{m}\frac{q^{\frac{s_i(s_i-1)}{2}}\prod_{j=1}^{s_i}(q^j-1)}{(q-1)s_i!}$$

Lemma 3.3.5 For each $m \in M$, the number of e_R contained in m is $2\varphi^3(q-1)$.

Proof For each

$$m=(s,t)\in M, e_R=(P,A,\alpha)\in E_R$$

if $e_R \subset m$, then

$$g(s,e_R) = [s,s^2,\cdots,s^n]\boldsymbol{P}^{-1}\boldsymbol{A}\boldsymbol{P}[\alpha,\alpha^2,\cdots,\alpha^n]^{\mathrm{T}} = [s,s^2,\cdots,s^n]\boldsymbol{\Lambda}[\alpha,\alpha^2,\cdots,\alpha^n]^{\mathrm{T}} = t$$

For any α, suppose there is another $\boldsymbol{\Lambda}'$ such than $[s,s^2,\cdots,s^n]\boldsymbol{\Lambda}'[\alpha,\alpha^2,\cdots,\alpha^n]^{\mathrm{T}} = t$. We have

$$[s,s^2,\cdots,s^n](\boldsymbol{\Lambda}-\boldsymbol{\Lambda}')[\alpha,\alpha^2,\cdots,\alpha^n]^{\mathrm{T}} = 0$$

Because $\alpha,\alpha^2,\cdots,\alpha^n$ are linearly independent, we get $[s,s^2,\cdots,s^n](\boldsymbol{\Lambda}-\boldsymbol{\Lambda}')=0$, from $[s,s^2,\cdots,s^n]$ is arbitrarily, we have $\boldsymbol{\Lambda}-\boldsymbol{\Lambda}'=0$, that is, $\boldsymbol{\Lambda}=\boldsymbol{\Lambda}'$. Therefore, $\boldsymbol{\Lambda}$ is only determined by α, so the number of α is $\varphi(q-1)$.

In the following, we will discuss when $\boldsymbol{\Lambda}$ is determined, the number of $\boldsymbol{A}$ and $\boldsymbol{P}$ satisfying $\boldsymbol{P}^{-1}\boldsymbol{A}\boldsymbol{P}$. Let G be the set of all invertible matrix over $\boldsymbol{F}_q^{n\times n}$. Obviously, $(G,\times)$ is a group, where "$\times$" is

multiplication with matrix. Let Ω be the set of all invertible symmetrical matrix over $\boldsymbol{F}_q^{n\times n}$. We choose $\boldsymbol{A}\in\Omega$ and assume Ω forms an orbit Ω_A under the action of G: $\Omega_A=\{\boldsymbol{P}(\boldsymbol{A})\mid \boldsymbol{P}\in G\}$, where $\boldsymbol{P}(\boldsymbol{A})=\boldsymbol{P}^{-1}\boldsymbol{A}\boldsymbol{P}$, then stable subgroup of $\boldsymbol{A}$ is $G_A=\{\boldsymbol{P}\mid \boldsymbol{P}\in G,\boldsymbol{P}(\boldsymbol{A})=\boldsymbol{A}\}$, $\boldsymbol{P}$ contained in G_A satisfies the equation $\boldsymbol{P}(\boldsymbol{A})=\boldsymbol{P}^{-1}\boldsymbol{A}\boldsymbol{P}=\boldsymbol{A}$ i.e. $\boldsymbol{A}\boldsymbol{P}=\boldsymbol{P}\boldsymbol{A}$. By Theorem 2.2.7, such $\boldsymbol{P}$ is scalar matrix $\lambda\boldsymbol{E}$, because $\boldsymbol{P}\in G$ is an orthogonal matrix, $\boldsymbol{P}\boldsymbol{P}^{\mathrm{T}}=\boldsymbol{E}$. So $\lambda=\pm 1,\boldsymbol{P}=\pm\boldsymbol{E}$, where $\boldsymbol{E}$ is a n order unit matrix. Then $\mid G_A\mid=2$.

From the orbit formula and the Lagrange theorem, we know that $\mid G\mid=\mid\Omega_A\mid\cdot\mid G_A\mid$. Now because the elements of Ω_A taking the form $\boldsymbol{P}(\boldsymbol{A})=\boldsymbol{P}^{-1}\boldsymbol{A}\boldsymbol{P}$ and $\boldsymbol{P}^{-1}\boldsymbol{A}\boldsymbol{P}$ is only determined by α, for $\boldsymbol{P}^{-1}\boldsymbol{A}\boldsymbol{P}$, there are $\varphi(q-1)$ possible cases, that is, $\mid\Omega_A\mid=\varphi(q-1)$. So $\mid G\mid=2\varphi(q-1)$, that is, there are $2\varphi(q-1)$ possible choices for $\boldsymbol{P}$.

Because $\mid\Omega_A\mid$ is the number of all $\boldsymbol{A}$ turned into diagonal matrix by the similarity transformation $\boldsymbol{P}^{-1}\boldsymbol{A}\boldsymbol{P}$, therefore, the number of $\boldsymbol{A}$ is $\varphi(q-1)$ now. So when $\boldsymbol{P}^{-1}\boldsymbol{A}\boldsymbol{P}$ is determined, the number of $(\boldsymbol{A},\boldsymbol{P})$ is $2\varphi^2(q-1)$. In summary, the number of the triple $(\boldsymbol{A},\boldsymbol{P},\alpha)$ satisfying the known condition is $2\varphi^3(q-1)$, that is, the number of e_R which is contained in m is $2\varphi^3(q-1)$.

Lemma 3.3.6 For each $m=(s,t)\in M$, and $m'=(s',t')\in m'$ with $s\neq s'$, the number of e_R which is contained m and m' is $2\varphi^2(q-1)$.

Proof We assume $e_R=(P,A,\alpha)$. If $e_R\subset m$ and $e_R\subset m'$, then

$$g(s',e_R)=[s',s'^2,\cdots,s'^n]\boldsymbol{P}^{-1}\boldsymbol{A}\boldsymbol{P}[\alpha,\alpha^2,\cdots,\alpha^n]^{\mathrm{T}}=[s',s'^2,\cdots,s'^n]\boldsymbol{\Lambda}[\alpha,\alpha^2,\cdots,\alpha^n]^{\mathrm{T}}=t'$$

Furthermore, we obtain

$$[s-s',s^2-s'^2,\cdots,s^n-s'^n]\boldsymbol{\Lambda}[\alpha,\alpha^2,\cdots,\alpha^n]^{\mathrm{T}}=t-t'$$

If $t=t'$, then $t-t'=0$. Since $\alpha,\alpha^2,\cdots,\alpha^n$ is linearly independent,

$$[s-s',s^2-s'^2,\cdots,s^n-s'^n]\boldsymbol{\Lambda}=0$$

Because $\boldsymbol{\Lambda}$ is invertible, we get

$$[s-s',s^2-s'^2,\cdots,s^n-s'^n]=0$$

so $s=s'$, it is contradiction with the known conditions. So $t\neq t',t-t'\neq 0$. We obtain

$$(t-t')^{-1}\lfloor[s-s',s^2-s'^2,\cdots,s^n-s'^n]\boldsymbol{\Lambda}[\alpha,\alpha^2,\cdots,\alpha^n]^{\mathrm{T}}\rfloor=1$$

For any given $m=(s,t)$, $m'=(s',t')$, where s, s', t and t' are only determined. From the uniqueness of inverse element over finite fields, $\boldsymbol{\Lambda}[\alpha,\alpha^2,\cdots,\alpha^n]^{\mathrm{T}}$ is only determined. From the properties of $\boldsymbol{\Lambda}$ and α, we know that such $\boldsymbol{\Lambda}$ and α are also only determined respectively. Similar to the proof of Lemma 3.3.5, the number of two-tuple $(\boldsymbol{A},\boldsymbol{P})$ is $2\varphi^2(q-1)$. So the number of e_R which is contained m and m' is $2\varphi^2(q-1)$.

Lemma 3.3.7 For each e_U containing a given e_L, the number of e_R which is incidence with e_U is

$$\mid E_R\mid=\Theta\varphi(q-1)n!\prod_{i=1}^{m}\frac{q^{s_i(s_i-1)/2}\prod_{j=1}^{s_i}(q^j-1)}{(q-1)s_i!}$$

Proof From the above construction methods and the properties of e_U and e_R, we know that for any source state s,

$$\mid E_R\mid=\Theta\varphi(q-1)n!\prod_{i=1}^{m}\frac{q^{s_i(s_i-1)/2}\prod_{j=1}^{s_i}(q^j-1)}{(q-1)s_i!}$$

Lemma 3.3.8 For each e_U 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 $2\varphi^2(q-1)$.

Proof For any $s\in S$, $e_R\in E_R$, from Lemma 3.3.7, we know that for any given e_U, all of e_R are incidence with e_U Because $e_R\subset m$, so

$$g(s,e_R)=[s,s^2,\cdots,s^n]\boldsymbol{P}^{-1}\boldsymbol{A}\boldsymbol{P}[\alpha,\alpha^2,\cdots,\alpha^n]^{\mathrm{T}}=[s,s^2,\cdots,s^n]\boldsymbol{\Lambda}[\alpha,\alpha^2,\cdots,\alpha^n]^{\mathrm{T}}=t$$

Furthermore, $t^{-1}[s,s^2,\cdots,s^n]\boldsymbol{\Lambda}[\alpha,\alpha^2,\cdots,\alpha^n]^{\mathrm{T}}=1$.

Similar to Lemma 3.3.6, it can be seen that $\boldsymbol{\Lambda}[\alpha,\alpha^2,\cdots,\alpha^n]^{\mathrm{T}}$ is uniquely determined. Therefore, the number of e_R which is incidence with e_U and contained in m is $2\varphi^2(q-1)$.

3.4 Computation of the Attack Probability About the Authentication Code

Theorem 3.4.1 In the constructed Multi-sender authentication code, if the senders' encoding rules and the receiver's decoding rules are chosen conforming to a uniform probability distribution, then the largest probabilities of success for different types of spoofing attack respectively are:

$$P_I=\frac{2\varphi^2(q-1)}{n!\dfrac{q^{n(n-1)/2}\prod_{j=1}^{n}(q^j-1)}{q^{v(v+\delta-1)}\prod_{i=1}^{v}(q^i-1)\prod_{i=0}^{v+\delta-1}(q^i+1)}\prod_{i=1}^{m}\dfrac{q^{s_i(s_i-1)/2}\prod_{j=1}^{s_i}(q^j-1)}{(q-1)s_i!}}$$

$$P_S = \frac{1}{\varphi(n-1)}$$

$$P_U(L) = \frac{2\varphi(q-1)}{n! \dfrac{q^{n(n-1)/2}\prod_{j=1}^{n}(q^j-1)}{q^{v(v+\delta-1)}\prod_{i=1}^{v}(q^i-1)\prod_{i=0}^{v+\delta-1}(q^i+1)}\prod_{i=1}^{m}\dfrac{q^{s_i(s_i-1)/2}\prod_{j=1}^{s_i}(q^j-1)}{(q-1)s_i!}}$$

Proof By Lemma 3.3.4 and Lemma 3.3.5,

$$P_I = \max_{m\in M}\left\{\frac{|\{e_R \in E_R \mid e_R \subset m\}|}{|E_R|}\right\} = \frac{2\varphi^3(q-1)}{\Theta\varphi(q-1)\,n!\prod_{i=1}^{m}\dfrac{q^{s_i(s_i-1)/2}\prod_{j=1}^{s_i}(q^j-1)}{(q-1)\,s_i!}} =$$

$$\frac{2\varphi^2(q-1)}{n! \dfrac{q^{n(n-1)/2}\prod_{j=1}^{n}(q^j-1)}{q^{v(v+\delta-1)}\prod_{i=1}^{v}(q^i-1)\prod_{i=0}^{v+\delta-1}(q^i+1)}\prod_{i=1}^{m}\dfrac{q^{s_i(s_i-1)/2}\prod_{j=1}^{s_i}(q^j-1)}{(q-1)s_i!}}$$

By Lemma 3.3.5 and Lemma 3.3.6, we get

$$P_S = \max_{m\in M}\left\{\frac{\max_{m\neq m'\in M}|\{e_R \in E_R \mid e_R \subset m, m'\}|}{|\{e_R \in E_R \mid e_R \subset m\}|}\right\} = \frac{2\varphi^2(q-1)}{2\varphi^3(q-1)} = \frac{1}{\varphi(q-1)}$$

By Lemma 3.3.7 and Lemma 3.3.8, we get

$$P_U(L) = \max_{e_L\in E_L,\ e_L\in e_u}\max\left\{\frac{\max_{m\in M}|\{e_R \in E_R \mid e_R \subset m, \text{and } p(e_R,e_U)\neq 0\}|}{|\{e_R \in E_R \mid p(e_R,e_U)\neq 0\}|}\right\} = \frac{2\varphi^2(q-1)}{\Theta\varphi(q-1)\,n!\prod_{i=1}^{m}\dfrac{q^{s_i(s_i-1)/2}\prod_{j=1}^{s_i}(q^j-1)}{(q-1)\,s_i!}} =$$

$$\frac{2\varphi(q-1)}{n! \dfrac{q^{n(n-1)/2}\prod_{j=1}^{n}(q^j-1)}{q^{v(v+\delta-1)}\prod_{i=1}^{v}(q^i-1)\prod_{i=0}^{v+\delta-1}(q^i+1)}\prod_{i=1}^{m}\dfrac{q^{s_i(s_i-1)/2}\prod_{j=1}^{s_i}(q^j-1)}{(q-1)s_i!}}$$

References

[1] Gilbert E N, Macwiliams F J , Sloan N J. Codes which detect deception. Bell Labs Technical Journal, 1974, 53(3): 405 - 424. DOI: 10. 1002/j. 1538 - 7305. 1974. tb02751.x.

[2] Desmedt Y, Frankel Y, Yung M. Multer-receiver/ Multi-sender network security: Efficient authenticated multicast/ feedback. INFOCOM ′92. Eleventh Annual Joint Conference of the IEEE Computer and Communications Societies. Piscataway: IEEE, 1992. 2045-2054. DOI: 10. 1109/INFCOM.1992.263476.

[3] Pei Dingyi. Message Authentication Codes. AnHui: China University of Science and Technology Press, 2009.

[4] Chen Shangdi, Chang Lizhen. Two constructions of Multi-sender authentication codes with arbitration based linear codes. Wseas Transactions on Mathematics, 2012, 11 (12): 1103-1113.

[5] Safavi-Naini R, Wang H. New results on multi-receiver authentication codes. Advances in Cryptology-EUROCRYPT'98, International Conference on the Theory and Application of Cryptographic Techniques. 1998, 1403: 527-541. DOI: 10. 1007/BFb0054151.

[6] Gao You, Yu Huafeng. Constructions of authenticationn codes with arbitration from alternate matrix over finite fields. Journal of Nature Science of Heilongjiang University, 2015, 29(1): 42-50.

[7] Liu Yanqin, Gao You, Zhang Dake. The construction of

A^3-code from singular pseudo-symple ctic geometry over finite fields. Wseas Transactions on Mathematics, 2015,14: 77-86.

[8] Gao You, Wang Gang, He Yifan. A new construction of multisender authentication codes with simultaneous model from singular symplectic geometry over finite fields. Ars Combinatoria,2015,118:95-107.

[9] Chen Shangdi, Zhang Xiaolian, Ma Hao. Two constructions of A^3-codes from projective geometry in finite fields. Journal of China Universities of Posts and Telecommunications,2015,22(2):52-59.DOI: 10.1016/S1005-8885(15)60639-2.

[10] Chen Shangdi, Zhang Xiaolian. Three constructions of perfect authentication codes from projective geometry over finite fields. Applied Mathematics and Computation, 2015,253:308-317.DOI: 10.1016/j.amc.2014.12.088.

[11] Chen Shangdi, Chang Lizhen. A construction of multi-receiver authentication codes with dynamic sender from linear codes. Applied Mathematics and Computation, 2016,129:227-236.

[12] Chen Shangdi, Song Minjuan. Two new authentication schemes from singular symplectic geometry over finite fields. J. Comb. Math. Comb. Comp., 2014, 88: 169-190.

[13] Chen Shangdi, Zhang Xiaolian, Ma Hao. Construction of authentication codes with double arbiters over symplectic geometry. Acta Mathematics Applicate Sinica (English Series),2015,31(4):1141-1152.DOI:10.1007/s10255-015-0511-3.

[14] Liang Miao, Li Mingchao, Du Beiliang. A construction for *t*-fold perfect authentication codes with arbitration. Designs, Codes and Cryptography, 2014, 73(3): 781-790. DOI:10.1007/s10623-013-9826-3.

[15] Li Mingchao, Liang Miao, Du Beiliang. A construction of *t*-fold perfect splitting authentication codes with equal deception probabilities.Cryptography and Communications, 2015,7(2): 207-215. DOI: 10.1007/s12095-014-0107-4.

[16] Liang Miao, Ji Lijun, Zhang Jingcai. Some new classes of 2-fold optimal or perfect splitting authentication codes. Cryptography and Communications, 2017, 9(3): 407-430. DOI:10.1007/s12095-015-0179-9.

[17] Shen Shiyi, Chen Lushen. Theory of Information and Coding. Beijing: Science Press, 2002.

[18] Wang E F, Shi S M. Advanced Algebra. Beijing:Higher Education Press, 2003.

[19] Wan Zhexian. Geometry of Classical Group over Finite Field. Beijing: Science Press, 2002.

[20] Zhang Herui. Modern Algebra Foundation. Beijing:High Education Press, 1978.