A New Construction of Multisender Authentication Codes from Symplectic Geometry over Finite Fields

Chen Shang-di[a] Yang Chun-li[b]

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

Abstract Multisender authentication codes allow a group of senders to construct an authenticated message for a receiver such that the receiver can verify authenticity of the received message. In this paper, we give the model of multisender authentication codes and the calculation formulas on probability of success in attacks by malicious groups of senders. A construction of multisender authentication codes from symplectic geometry over finite fields is given, and the parameters and the probabilities of deceptions are also calculated.

1. Introduction

Information security consists of confidentiality and authentication. Confidentiality is to prevent the confidential information from decrypting by adversary. The purpose of authentication is to ensure the sender is real and to verify the information is integrated. Digital signature and authentication codes are two important means of authenticating the information, and provide good service in the network. Digital signature is computationally secure, in practical, assume that the computing power of adversary is limited and a mathematical problem is intractable and complex. However, authentication codes are generally safe (unconditionally secure), relatively simple. In 1940s, C. E .Shannon first put forward the concept of perfect secrecy authentication system using the information theory. In 1980s, information theory method has been applied to the problem of authentication by G. J. Simmons, authentication codes became the foundation for constructing unconditionally secure authentication system. In 1974, Gilbert, MacWilliams and Sloane constructed the first authentication code[1], it is a landmark in the development of authentication theory. During the same period, Simmons independently studied the authentication theory and established three participants and

Keywords: symplectic geometry, multisender authentication codes, finite fields.

Supported By The NNSF of China(61179026).

Address: College of Science, Civil Aviation University of China, Tianjin 300300, P.R.China.

E-mail address: a. 11scd@163.com; b. yangchunli414@163.com

four participants certification models[2]. The famous mathematician Wan Zhexian constructed an authentication code without arbitration from the subspace of the classical geometry [3]. In the case of transmitter and receiver are not honestly, Ma Wenping, Wang Xinmei, Gao You, Chen Shangdi, Li Ruihu constructed a series of authentication codes with arbitration [4–7]. Xing Chaoping[8] and Ding Cunsheng[9] constructed authentication codes using algebraic curve, nonlinear functions. Safavi-Naini R gave some results on multireceiver authentication codes [10]. Ma Wenping, Y. Desmedt, Qi Yingchun, Du Qingling made great contributions on multisender authentication codes [11–14]. In this paper, we construct a multisender authentication code from symplectic geometry over finite fields, the parameters and the maximum probability of success in impersonation attack and substitution attack by group of senders are also computed.

2. The Model of Multisender Authentication Codes

Group cryptography is introduced by Boya and Desmedt, the basic idea is to change the single person into multiple persons in the communication users and has more practical value. Multiuser authentication codes are a generalization of traditional two users authentication codes, it changes the traditional single sender and single receiver into multiple senders and multiple receivers. Two cases of this authentication codes are studied mostly: multisender authentication codes and multireceiver authentication codes. In this paper, we only study the former. In the actual computer network communications, multisender authentication codes include sequential model and simultaneous model. Sequential model is that each sender uses their own encoding rules to encode a source state orderly, and the last sender sends the encoded message to the receiver, the receiver receives the message and verifies whether the message is legal or not; Simultaneous model is that all senders use their own encoding rules to encode a source state, then the synthesizer forms an authenticated message and sends it to the receiver, the receiver receives the message and verifies whether the message is legal or not.

In sequential model, there are three participants: a group of senders $U = \{U_1, U_2, \cdots, U_n\}$; a Key Distribution Center (KDC), for the distribution keys to senders and receiver; a receiver, he receives the authenticated message and verifies the message truth or not. The code works as follows: each sender and receiver has their own Cartesian authentication code, respectively. It used to generate part of the message and verify authenticity of the received message. Sender's authentication codes are called branch authentication codes, and receiver's authentication code is called channel authentication code. Let $(S_i, E_i, T_i; f_i)$, $i = 1, 2, \cdots, n$ be the sender's Cartesian authentication codes, and $T_{i-1} \subset S_i, 1 \leq i \leq n$, $(S, E, T; f)$ be the receiver's Cartesian authentication code, and $S = S_1, T = T_i, \pi_i : E \rightarrow E_i$ be a sub-key generation algorithm. For authenticating a message, the senders and the receiver should comply with protocols: 1) KDC randomly selects a $e \in E$ and secretly sends it to the receiver R, and sends $e_i = \pi_i(e)$ to the i–th sender U_i,

$i = 1,2,\cdots,n$; 2) If the senders would like to send a source state s to the receiver R, U_1 calculates $t_1 = f_1(s,e_1)$, and then sends to U_2 through an open channel, U_2 receives t_1 and calculates $t_2 = f_2(t_1,e_2)$, and then sends t_2 to U_3 through an open channel. In generally, U_i receives t_{i-1} and calculates $t_n = f_i(t_{i-1},e_i)$, and then sends t_i to U_{i+1} through an open channel, $1 < i < n$ .U_n receives t_{n-1} and calculates $t_n = f_n(t_{i-1},e_n)$, and then sends $m = (s,t_n)$ through an open channel to the receiver R ; 3) When the receiver receives the message $m = (s,t_n)$, he checks the authenticity by verifying whether $t_n = f(s,e)$ or not. If the equality holds, the message is regarded as authentic and is accepted. Otherwise, the message is rejected.

In simultaneous model, there are four participants: a group of senders $U = \{U_1,U_2,\cdots,U_n\}$; a Key Distribution Center (KDC), for the distribution keys to senders and receiver; a synthesizer C, he only runs the trusted synthesis algorithm; a receiver,.he receives the authenticated message and verifies the message truth or not. The code works as follows: each sender and receiver has their own Cartesian authentication code, respectively. It used to generate part of the message and verify the received message. Sender's authentication codes are called branch authentication codes, and receiver's authentication code is called channel authentication code. Let $(S_i,E_i,T_i;f_i)$, $i = 1,2,\cdots,n$ be the sender's Cartesian authentication codes, $(S,E,T;f)$ be the receiver's Cartesian authentication code, $g : T_1 \times T_2 \times \cdots \times T_n \longrightarrow T$ be the synthesis algorithm, $\pi_i : E \longrightarrow E_i$ be a sub-key generation algorithm. For authenticating a message, the senders and the receiver should comply with protocols: 1) KDC randomly selects a encoding rule $e \in E$ and secretly sends it to the receiver R , and sends $e_i = \pi_i(e)$ to the i–th sender U_i, $i = 1,2,\cdots,n$; 2) If the senders would like to send a source state s to the receiver R , U_i computes $t_i = f_i(s,e_i)$, $i = 1,2,\cdots,n$ and sends $m_i = (s,t_i)$, $i = 1,2,\cdots,n$ to the synthesizer C through an open channel; 3) The synthesizer C receives the messages $m_i = (s,t_i)$, $i = 1,2,\cdots,n$, and calculates $t = g(t_1,t_2,\cdots,t_n)$ using the synthesis algorithm g , then sends message $m = (s,t)$ to the receiver R; 4) When the receiver receives the message $m = (s,t)$, he checks the authenticity by verifying whether $t = f(s,e)$ or not. If the equality holds, the message is regarded as authentic and is accepted. Otherwise, the message is rejected.

3. The calculation formulas

We assume that the arbitrator (KDC) and the synthesizer (C) are credible, though they know the senders' and receiver's encoding rules, they aren't participate in any communication activities. When transmitter and receiver are disputing, the arbitrator settles it. At the same time, assume that the system follows the Kerckhoff's principle which except the actual used keys, the other information of the whole system is public. Assume that the source state space S and the receiver's decoding rules space E_R are according to a uniform probability distribution, then the probability distribution of message space M and tag space T are determined by the probability distribution of S and E_R .

In a multisender authentication system, assume that the whole senders are cooperation to form a valid message, that is, all senders as a whole and receiver are reliable. But there are some malicious senders which they together cheat the receiver, the part of senders and receiver are not credible, they can take impersonation attack and substitution attack.

Assume that $U_1, U_2, \cdots, U_n$ are senders, R is a receiver, E_{U_i} is the encoding rules of U_i, E_R is the decoding rules of receiver R. $L = \{i_1, i_2, \cdots, i_l\} \subset \{1, 2, \cdots, n\}$, $l < n$, $U_L = \{U_{i_1}, U_{i_2}, \cdots, U_{i_l}\}$, $E_L = \{E_{U_{i_1}}, E_{U_{i_2}}, \cdots, E_{U_{i_l}}\}$. Next we consider the attacks from malicious groups of senders.

Impersonation attack: U_L, after receiving their secret keys, send a message m to receiver. U_L is successful if the receiver accepts it as legitimate message. Denote $P_I[L]$ is the maximum probability of success of the impersonation attack. It can be expressed as

$$P_I[L] = \max_{e_L \in E_L} \max_{m \in M} P(m \text{ is accepted by } R | e_L).$$

Substitution attack: U_L, after observing a legitimate message m, substitutes it with another message m'. U_L is successful if m' is accepted by receiver as authentic. Denote $P_S[L]$ is the maximum probability of success of the substitution attack. It can be expressed as

$$P_S[L] = \max_{e_L \in E_L} \max_{m \in M} \max_{m' \neq m \in M} P(m' \text{is accepted by } R | m, e_L).$$

4. Geometry of Symplectic Groups over Finite Fields

In this section, we give some definitions and properties on geometry of symplectic groups over finite fields, which can be extracted from [15] .

Let F_q be a finite field with q elements, $n = 2\nu$ and define the $2\nu \times 2\nu$ alternate matrix

$$K = \begin{pmatrix} 0 & I^{(\nu)} \\ -I^{(\nu)} & 0 \end{pmatrix}.$$

The symplectic group of degree 2ν over F_q, denote by $Sp_{2\nu}(F_q)$, is defined to be the set of matrices

$$Sp_{2\nu}(F_q) = \{T | TK^tT = K\},$$

with matrix multiplication as its group operation. Let $F_q^{(2\nu)}$ be the 2ν-dimensional row vector space over F_q. $Sp_{2\nu}(F_q)$ has an action on $F_q^{(2\nu)}$ defined as follows

$$F_q^{(2\nu)} \times Sp_{2\nu}(F_q) \to F_q^{(2\nu)}$$

$$((x_1, x_2, \ldots, x_{2\nu}), T) \to (x_1, x_2, \ldots, x_{2\nu})T.$$

The vector space $F_q^{(2\nu)}$ together with this action of $Sp_{2\nu}(F_q)$ is called the symplectic space over F_q.

Let P be an m–dimensional subspace of $F_q^{(2\nu)}$. We use the same latter P to denote a matrix representation of P, that is, P is an $m \times 2\nu$ matrix of rank m such that its rows form a basis of P. The $PK'P$ is alternate. Assume that it is of rank $2s$, then P is called a subspace of type (m, s). It is known that subspaces of type (m, s) exist in $F_q^{(2\nu)}$ if and only if

$$2s \leq m \leq \nu - s.$$

It is also known that subspaces of the same type form an orbit under $Sp_{2\nu}(F_q)$. Denote by $N(m, s; 2\nu)$ the number of subspaces of type (m, s) in $F_q^{(2\nu)}$.

Denote by $P^\perp$ the set of vectors which are orthogonal to every vector of P, that is,

$$P^\perp = \{y \in F_q^{(2\nu)} | yK'x = 0 \text{ for all } x \in P\}.$$

Obviously, $P^\perp$ is a $(2\nu - m)$-dimensional subspace of $F_q^{(2\nu)}$.

5. Construction

Let F_q be a finite field with q elements. Assume that $1 < n < n' < r < \nu$. $U = \langle e_1, e_2, \cdots, e_n \rangle$, then $U^\perp = \langle e_1, \cdots, e_\nu, e_{\nu+n+1}, \cdots, e_{2\nu} \rangle$. Let $W_i = \langle e_1, \cdots, e_{i-1}, e_{i+1} \cdots, e_n \rangle$, then $W_i^\perp = \langle e_1, \cdots, e_\nu, e_{\nu+i}, e_{\nu+n+1}, \cdots, e_{2\nu} \rangle$, $1 \leq i \leq n$. The set of source states $S = \{s | s$ is a subspace of type $(2r - n, r - n)$ and $U \subset s \subset U^\perp\}$; the set of i–th transmitter's encoding rules $E_{U_i} = \{e_{U_i} | e_{U_i}$ is a subspace of type $(n + 1, 1)$ and $U \subset e_{U_i}, e_{U_i} \perp W_i\}$; the set of receiver's decoding rules $E_R = \{e_R | e_R$ is a subspace of type $(2n', n')$ and $U \subset e_R\}$; the set of i–th transmitter's tags $T_i = \{t_i | t_i$ is a subspace of type $(2r - n + 1, r - n + 1)$ and $U \subset t_i \subset W_i^\perp, t_i \not\subset U^\perp\}$; the set of receiver's tags $T = \{t | t$ is a subspace of type $(2(r + n' - n), r + n' - n)$ and $U \subset t\}$.

Define the encoding map

$$f_i : S \times E_{U_i} \longrightarrow T_i, \; f_i(s, e_{U_i}) = s + e_{U_i}, \; 1 \leq i \leq n.$$

The decoding map

$$f : S \times E_R \longrightarrow T, \; f(s, e_R) = s + e_R.$$

The synthesizing map

$$g : T_1 \times T_1 \times \cdots \times T_n \longrightarrow T, \; g(t_1, t_2, \cdots, t_n) = t_1 + t_2 + \cdots + t_n + \omega,$$

where ω is a subspace and $t_1 + t_2 + \cdots + t_n + \omega$ is a subspace of type $(2(r + n' - n), r + n' - n)$.

This code works as follows:

1)KDC randomly chooses a $e_R \in E_R$ and selects a $(2n, n)$ subspace e such that $U \subset e$, and selects $e_{U_i} \in E_{U_i}$ so that $e_{U_1} + e_{U_2} + \cdots + e_{U_n} = e$. ω is a subspace and satisfying $e_R = \langle e, \omega \rangle$. KDC secretly sends e_R, e_{U_i} to the receiver and the senders, respectively, and sends ω to the synthesizer C.

2)If the senders want to send a source state $s \in S$, U_i calculates $t_i = f_i(s, e_{U_i}) = s + e_{U_i}$, and then sends t_i to the synthesizer C, $1 \leq i \leq n$.

3)The synthesizer receives $t_1, t_2, \cdots, t_n$, he calculates $t = g(t_1, t_2, \cdots, t_n) = t_1 + t_2 + \cdots + t_n + \omega$, and then sends (s, t) to the receiver R.

4)The receiver R receives (s, t), he calculates $t' = f(s, e_R) = s + e_R$. If $t = t'$, he accepts t, otherwise, he rejects it.

Assume that the sender's encoding rules and the receiver's decoding rules follow the uniform probability distribution. Let

$$U=\begin{array}{cc}\begin{pmatrix} I^{(i-1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(n-i)} & 0 & 0 & 0 & 0 & 0 \end{pmatrix} & \begin{array}{c} i-1 \\ 1 \\ n-i \end{array} \\ \begin{array}{cccccccc} i-1 & 1 & n-i & v-n & i-1 & 1 & n-i & v-n \end{array} & \end{array},$$

then

$$U^{\perp}=\begin{array}{c}\begin{pmatrix} I^{(i-1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(n-i)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(v-n)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(v-n)} \end{pmatrix} \\ \begin{array}{cccccccc} i-1 & 1 & n-i & v-n & i-1 & 1 & n-i & v-n \end{array} \end{array}.$$

$$W_i^{\perp}=\begin{array}{c}\begin{pmatrix} I^{(i-1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(n-i)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(v-n)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(v-n)} \end{pmatrix} \\ \begin{array}{cccccccc} i-1 & 1 & n-i & v-n & i-1 & 1 & n-i & v-n \end{array} \end{array}.$$

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

Lemma5.1 Let $C_i = (S, E_{U_i}, T_i; f_i)$, then C_i is a Cartesian authentication code, $1 \leq i \leq n$.

Proof. For any $e_{U_i} \in E_{U_i}$, $s \in S$, we assume that

$$e_{U_i}=\begin{array}{cc}\begin{pmatrix} I^{(i-1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(n-i)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & R_4 & 0 & R_6 & 0 & R_8 \end{pmatrix} & \begin{array}{c} i-1 \\ 1 \\ n-i \\ 1 \end{array} \\ \begin{array}{cccccccc} i-1 & 1 & n-i & v-n & i-1 & 1 & n-i & v-n \end{array} & \end{array}.$$

For e_{U_i} is a subspace of type $(n+1, 1)$, therefore, $R_6 = 1$, R_4, R_8 arbitrarily. Obviously, $e_{U_i} \cap U^{\perp} = U$. Let $s \in S$, and

$$s=\begin{array}{cc}\begin{pmatrix} I^{(i-1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(n-i)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & H_4 & 0 & 0 & 0 & H_8 \end{pmatrix} & \begin{array}{c} i-1 \\ 1 \\ n-i \\ 2(r-n) \end{array} \\ \begin{array}{cccccccc} i-1 & 1 & n-i & v-n & i-1 & 1 & n-i & v-n \end{array} & \end{array}.$$

Because s is a subspace of type $(2r-n, r-n)$, (H_4, H_8) is a subspace of type $(2(r-n), r-n)$ in the symplectic space $F_q^{2(\nu-n)}$. Let $t_i = s + e_{U_i}$, then

$$t_i = \begin{array}{c} \left(\begin{array}{cccccccc} I^{(i-1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(n-i)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & R_4 & 0 & 1 & 0 & R_8 \\ 0 & 0 & 0 & H_4 & 0 & 0 & 0 & H_8 \end{array}\right) \begin{array}{c} i-1 \\ 1 \\ n-i \\ 1 \\ 2(r-n) \end{array} \\ \begin{array}{cccccccc} i-1 & 1 & n-i & \nu-n & i-1 & 1 & n-i & \nu-n \end{array} \end{array}.$$

and

$$t_iK^tt_i \sim \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I^{(r-n)} \\ 0 & 0 & 0 & 0 & -I^{(r-n)} & 0 \end{pmatrix}.$$

Obviously, $t_i \not\subset U^{\perp}$. So, t_i is a subspace of type $(2r-n+1, r-n+1)$ and satisfying $U \subset t_i \subset W_i^{\perp}$, that is $t_i \in T_i$. At the same time, we know $t_i \cap U^{\perp} = (s+e_{U_i}) \cap U^{\perp} = s + (e_{U_i} \cap U^{\perp}) = s + U = s$.

Conversely, for any $t_i \in T_i$, let $s = t_i \cap U^{\perp}$, $L \subset t_i$, satisfying $t_i = s \oplus L$. Obviously, $U \subset s \subset U^{\perp}$. For $U \subset t_i \subset W_i^{\perp}$, let

$$t_i = \begin{array}{c} \left(\begin{array}{cccccccc} I^{(i-1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(n-i)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & R_4' & 0 & R_6' & 0 & R_8' \end{array}\right) \begin{array}{c} i-1 \\ 1 \\ n-i \\ 2(r-n)+1 \end{array} \\ \begin{array}{cccccccc} i-1 & 1 & n-i & \nu-n & i-1 & 1 & n-i & \nu-n \end{array} \end{array}.$$

Because $t_i \not\subset U^{\perp}$, then $R_6' \neq 0$, therefore, one component of R_6' is not zero, through appropriate row transformation. Let

$$t_i = \begin{array}{c} \left(\begin{array}{cccccccc} I^{(i-1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(n-i)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & R_4 & 0 & 1 & 0 & R_8 \\ 0 & 0 & 0 & H_4 & 0 & 0 & 0 & H_8 \end{array}\right) \begin{array}{c} i-1 \\ 1 \\ n-i \\ 1 \\ 2(r-n) \end{array} \\ \begin{array}{cccccccc} i-1 & 1 & n-i & \nu-n & i-1 & 1 & n-i & \nu-n \end{array} \end{array}.$$

Obviously,

$$t_i \cap U^{\perp} = \begin{array}{c} \left(\begin{array}{cccccccc} I^{(i-1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(n-i)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & H_4 & 0 & 0 & 0 & H_8 \end{array}\right) \begin{array}{c} i-1 \\ 1 \\ n-i \\ 2(r-n) \end{array} \\ \begin{array}{cccccccc} i-1 & 1 & n-i & \nu-n & i-1 & 1 & n-i & \nu-n \end{array} \end{array}.$$

For t_i is a subspace of type $(2r-n+1, r-n+1)$, then $t_i \cap U^{\perp}$ is a subspace of type $(2r-n, r-n)$, that is, $s \in S$. Choose $L = (0\ 0\ 0\ R_4\ 0\ 1\ 0\ R_8)$, let $e_{U_i} = U + L$, then $e_{U_i} \in E_{U_i}$, and $t_i = s \oplus L = s + e_{U_i}$. Therefore, f_i is a surjection. For any $t_i \in T_i$, $e_{U_i} \in E_{U_i}$, if there exist $s \in S$ so that $t_i = s + e_{U_i}$, then $s \subset t_i \cap U^{\perp}$. However, dim$s$=$2r - n$=dim($t_i \cap U^{\perp}$), so, $s = t_i \cap U^{\perp}$, that is, s is determined by t_i and e_{U_i}.

Lemma5.2 Let $C = (S, E_R, T; f)$, then C is a Cartesian authentication code.

Proof. For any $s \in S$, $e_R \in E_R$, from the definition of s and e_R, we assume that

$$s = \begin{pmatrix} U \\ Q \end{pmatrix} \begin{matrix} n \\ 2(r-n) \end{matrix} \text{ and } \begin{pmatrix} U \\ Q \end{pmatrix} K {}^t\!\begin{pmatrix} U \\ Q \end{pmatrix} = \begin{pmatrix} 0^{(n)} & 0 & 0 \\ 0 & 0 & I^{(r-n)} \\ 0 & -I^{(r-n)} & 0 \end{pmatrix},$$

$$e_R = \begin{pmatrix} U \\ V \end{pmatrix} \begin{matrix} n \\ 2n'-n \end{matrix} \text{ and } \begin{pmatrix} U \\ V \end{pmatrix} K {}^t\!\begin{pmatrix} U \\ V \end{pmatrix} = \begin{pmatrix} 0 & I^{(n')} \\ -I^{(n')} & 0 \end{pmatrix}.$$

Obviously, for any $v \in V$ and $v \neq 0$, $v \notin s$. Therefore,

$$t = s + e_R = \begin{pmatrix} U \\ V \\ Q \end{pmatrix}, \text{ and } \begin{pmatrix} U \\ V \\ Q \end{pmatrix} K {}^t\!\begin{pmatrix} U \\ V \\ Q \end{pmatrix} = \begin{pmatrix} 0 & I^{(n')} & 0 & 0 \\ -I^{(n')} & 0 & * & * \\ 0 & * & 0 & I^{(r-n)} \\ 0 & * & -I^{(r-n)} & 0 \end{pmatrix}.$$

So, t is a subspace of type $(2(r + n' - n), r + n' - n)$ and $U \subset t$, that is, $t \in T$.

On the other hand, For any $t \in T$, t is a subspace of type $(2(r+n'-n), r+n'-n)$ containing U, then there exist a subspace $V \subset t$, satisfying

$$\begin{pmatrix} U \\ V \end{pmatrix} K {}^t\!\begin{pmatrix} U \\ V \end{pmatrix} = \begin{pmatrix} 0 & I^{(n')} \\ -I^{(n')} & 0 \end{pmatrix}.$$

Let $t = \begin{pmatrix} U \\ V \\ Q \end{pmatrix}$, and satisfying

$$\begin{pmatrix} U \\ V \\ Q \end{pmatrix} K {}^t\!\begin{pmatrix} U \\ V \\ Q \end{pmatrix} = \begin{pmatrix} 0 & I^{(n')} & 0 & 0 \\ -I^{(n')} & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(r-n)} \\ 0 & 0 & -I^{(r-n)} & 0 \end{pmatrix}.$$

Let $s = \begin{pmatrix} U \\ Q \end{pmatrix}$, then s is a subspace of type $(2r - n, r - n)$ and $U \subset s \subset U^{\perp}$, that is, $s \in S$. For any $v \in V$ and $v \neq 0$, then $v \notin s$, that is, $V \cap U^{\perp} = \{0\}$. So, $t \cap U^{\perp} = \begin{pmatrix} U \\ Q \end{pmatrix} = s$. Let $e_R = \begin{pmatrix} U \\ V \end{pmatrix}$, then $e_R \in E_R$, and satisfying $t = s + e_R$.

If s' is another source state contained in t, then $s' \subset t \cap U^{\perp} = s$, while dim$s'$=dim$s$, so, s'=s. Therefore, s is the uniquely source state contained in t.

From the above two lemmas, we know this construction is well defined. Next, we compute the parameters and the maximum probability of success in impersonation attack and substitution attack by group of senders.

Lemma 5.3 The number of the source states is $|S| = N(2(r-n), r-n; 2(v-n))$.

Proof. For any $s \in S$, since $U \subset s \subset U^{\perp}$ and s is a subspace of type $(2r-n, r-n)$, assume that

$$s=\begin{array}{cc}\begin{pmatrix} I^{(n)} & 0 & 0 & 0\\ 0 & Q_2 & 0 & Q_4\end{pmatrix} & \begin{array}{c} n\\ 2(r-n)\end{array}\\ \begin{array}{cccc} n & v-n & n & v-n\end{array} & \end{array},$$

where (Q_2, Q_4) is a subspace of type $(2(r-n), r-n)$ in the symplectic space $F_q^{2(v-n)}$. Therefore, $|S| = N(2(r-n), r-n; 2(v-n))$.

Lemma 5.4 The number of the i–th transmitter's encoding rules is $|E_{U_i}| = q^{2(v-n)}$, $1 \le i \le n$.

Proof. Let $e_{U_i} \in E_{U_i}$, then

$$e_{U_i}=\begin{array}{cc}\begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0\\ 0 & R_2 & 0 & 1 & 0 & R_4\end{pmatrix} & \begin{array}{c} n\\ 1\end{array}\\ \begin{array}{cccccc} n & v-n & i-1 & 1 & n-i & v-n\end{array} & \end{array},$$

where R_2, R_4 arbitrarily. Therefore, $|E_{U_i}| = q^{2(v-n)}$, $1 \le i \le n$.

Lemma 5.5 For any $t_i \in T_i$, the number of t_i which containing e_{U_i} is a_i, then $a_i = q^{2(r-n)}$, $1 \le i \le n$.

Proof. Since the transitivity properties of the same type subspaces under the symplectic groups, we choose

$$t_i=\begin{array}{cc}\begin{pmatrix} I^{(i-1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & I^{(n-i)} & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & I^{(r-n)} & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(r-n)} & 0\end{pmatrix} & \begin{array}{c} i-1\\ 1\\ n-i\\ 1\\ r-n\\ r-n\end{array}\\ \begin{array}{cccccccccc} i-1 & 1 & n-i & r-n & v-r & i-1 & 1 & n-i & r-n & v-r\end{array} & \end{array}.$$

If $e_{U_i} \subset t_i$, then we assume that

$$e_{U_i}=\begin{array}{cc}\begin{pmatrix} I^{(i-1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & I^{(n-i)} & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & R_4 & 0 & 0 & R_7 & 0 & R_9 & 0\end{pmatrix} & \begin{array}{c} i-1\\ 1\\ n-i\\ 1\end{array}\\ \begin{array}{cccccccccc} i-1 & 1 & n-i & r-n & v-r & i-1 & 1 & n-i & r-n & v-r\end{array} & \end{array}.$$

For e_{U_i} is a subspace of type $(n+1, 1)$, so, $R_7 = 1$, while R_4, R_9 arbitrarily. Therefore, $a_i = q^{2(r-n)}$, $1 \le i \le n$.

Lemma 5.6 The number of the i–th transmitter's tags is $|T_i| = N(2(r-n), r-n; 2(v-n))q^{2(v-r)}$, $1 \le i \le n$.

Proof. Since f_i is a surjection, then $|T_i| \le |S \times E_{U_i}|$. For every t_i containing a unique source state $t_i \cap U^{\perp}$, and from lemma 5.5, the number of t_i which containing e_{U_i} is $q^{2(r-n)}$, then $|S \times E_{U_i}| = |T_i \times a_i|$. Therefore,

$$|T_i| = \frac{|S \times E_{U_i}|}{a_i} = \frac{N(2(r-n), r-n; 2(v-n))q^{2(v-n)}}{q^{2(r-n)}} = N(2(r-n), r-n; 2(v-n))q^{2(v-r)}.$$

Lemma 5.7 The number of the receiver's decoding rules is $|E_R| = q^{2n'(v-n')}$.

Proof. For $e_R \in E_R$, then

$$e_R = \begin{array}{c} \left(\begin{array}{cccc} I^{(n')} & 0 & 0 & 0 \\ 0 & R_2 & I^{(n')} & R_4 \end{array}\right)\begin{array}{c} n' \\ n' \end{array} \\ \begin{array}{cccc} n' & v-n' & n' & v-n' \end{array} \end{array},$$

where R_2, R_4 arbitrarily. So, $|E_R| = q^{2n'(v-n')}$.

Lemma 5.8 For any $t \in T$, the number of e_R which contained in t is a, then $a = q^{2n'(r-n)}$.

Proof. Since the transitivity properties of the same type subspace under the symplectic groups, we choose

$$t = \begin{array}{c} \left(\begin{array}{cccccc} I^{(n')} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(n')} & 0 & 0 \\ 0 & I^{(r-n)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I^{(r-n)} & 0 \end{array}\right)\begin{array}{c} n' \\ n' \\ r-n \\ r-n \end{array} \\ \begin{array}{cccccc} n' & r-n & v-r-n'+n & n' & r-n & v-r-n'+n \end{array} \end{array}.$$

If $e_R \subset t$, then

$$e_R = \begin{array}{c} \left(\begin{array}{cccccc} I^{(n')} & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & 0 & I^{(n')} & R_5 & 0 \end{array}\right)\begin{array}{c} n' \\ n' \end{array} \\ \begin{array}{cccccc} n' & r-n & v-r-n'+n & n' & r-n & v-r-n'+n \end{array} \end{array}.$$

where R_2, R_5 arbitrarily. Therefore, $a = q^{2n'(r-n)}$.

Lemma 5.9 The number of the receiver's tags is $|T| = N(2(r-n), r-n; 2(v-n))q^{2n'(v-r-n'+n)}$.

Proof. Similarly to Lemma 5.6,

$$\begin{aligned} |T| &= \frac{|S \times E_R|}{a} \\ &= \frac{N(2(r-n), r-n; 2(v-n))q^{2n'(v-n')}}{q^{2n'(r-n)}} \\ &= N(2(r-n), r-n; 2(v-n))q^{2n'(v-r-n'+n)}. \end{aligned}$$

Theorem 5.1 The parameters of this code are: $|\ S\ | = N(2(r-n), r-n; 2(v-n))$; $|E_{U_i}| = q^{2(v-n)}$; $|T_i| = N(2(r-n), r-n; 2(v-n))q^{2(v-r)}$; $|E_R| = q^{2n'(v-n')}$; $|T| = N(2(r-n), r-n; 2(v-n))q^{2n'(v-r-n'+n)}$.

Without loss of generality, we assume that $U_L = \{U_1, U_2, \cdots, U_l\}$, $E_L = \{E_{U_1} \times E_{U_2} \times \cdots \times E_{U_l}\}$, where $l < n$. Next we consider the attacks from U_L on R.

Lemma 5.10 For any $e_L = (e_{U_1}, e_{U_2}, \cdots, e_{U_l}) \in E_L$, the number of e_R containing e_L is $q^{2(v-n')(n'-l)}$.

Proof. For any $e_L = (e_{U_1}, e_{U_2}, \cdots, e_{U_l}) \in E_L$, we assume e_L as follows;

$$e_L = \begin{array}{c} \left(\begin{array}{cccccccc} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & R_4 & I^{(l)} & 0 & R_7 & R_8 \end{array} \right) \\ \begin{array}{cccccccc} l & n-l & n'-n & v-n' & l & n-l & n'-n & v-n' \end{array} \end{array} .$$

If $e_L \subset e_R$, then e_R assumed as

$$e_R = \begin{array}{cc} \left(\begin{array}{cccccccc} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(n'-n)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & R_4 & I^{(l)} & 0 & R_7 & R_8 \\ 0 & 0 & 0 & H_4 & 0 & I^{(n-l)} & 0 & H_8 \\ 0 & 0 & 0 & Q_4 & 0 & 0 & I^{(n'-n)} & Q_8 \end{array} \right) & \begin{array}{c} l \\ n-l \\ n'-n \\ l \\ n-l \\ n'-n \end{array} \\ \begin{array}{cccccccc} l & n-l & n'-n & v-n' & l & n-l & n'-n & v-n' \end{array} & \end{array} .$$

where H_4, H_8, Q_4, Q_8 arbitrarily. Therefore, the number of e_R containing e_L is $q^{2(v-n')(n'-l)}$.

Lemma 5.11 For any $t \in T$, $e_L = (e_{U_1}, e_{U_2}, \cdots, e_{U_l}) \in E_L$, the number of e_R which contained in t and containing e_L is $q^{2(r-n)(n'-l)+(n'-n)(n-l)}$.

Proof. For any $t \in T$, we assume t as follows;

$$t = \begin{array}{cc} \left(\begin{array}{cccccccccc} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(n'-n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(r-n)} & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I^{(l)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(n-l)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(n'-n)} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(r-n)} & 0 \end{array} \right) & \begin{array}{c} l \\ n-l \\ n'-n \\ r-n \\ l \\ n-l \\ n'-n \\ r-n \end{array} \\ \begin{array}{cccccccccc} l & n-l & n'-n & r-n & v+n-r-n' & l & n-l & n'-n & r-n & v+n-r-n' \end{array} & \end{array} .$$

If $e_L \subset t$, then

$$e_L = \left(\begin{array}{cccccccccc} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & R_4 & 0 & I^{(l)} & 0 & R_8 & R_9 & 0 \end{array} \right),$$

Since $e_L \subset e_R \subset t$, then e_R assumed as

$$e_R = \begin{array}{cc} \left(\begin{array}{cccccccccc} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(n'-n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & R_4 & 0 & I^{(l)} & 0 & R_8 & R_9 & 0 \\ 0 & 0 & 0 & H_4 & 0 & 0 & I^{(n-l)} & H_8 & H_9 & 0 \\ 0 & 0 & 0 & N_4 & 0 & 0 & 0 & I^{(n'-n)} & N_9 & 0 \end{array} \right) & \begin{array}{c} l \\ n-l \\ n'-n \\ l \\ n-l \\ n'-n \end{array} \\ \begin{array}{cccccccccc} l & n-l & n'-n & r-n & v+n-r-n' & l & n-l & n'-n & r-n & v+n-r-n' \end{array} & \end{array} ,$$

where H_4, H_8, H_9, N_4, N_9 arbitrarily, then the number of e_R contained in t and containing e_L is $q^{2(r-n)(n'-l)+(n'-n)(n-l)}$.

Lemma 5.12 Assume that t_1 and t_2 are two distinct tags which decoded by receiver's key e_R, s_1 and s_2 contained in t_1 and t_2, respectively. Let $s_0 = s_1 \cap s_2$, $\dim s_0 = k$, then $n \leq k \leq 2r - n - 1$, the number of e_R which contained in $t_1 \cap t_2$ and containing e_L is $q^{(n'-l)(k+2n'-3n)}$.

Proof. Since $t_1 = s_1 + e_R$, $t_2 = s_2 + e_R$, and $t_1 \neq t_2$, then $s_1 \neq s_2$. For any $s \in S, U \subset s$, so, $n \leq k \leq 2r-n-1$. Assume that s_i' is the complementary subspace of s_0 in the s_i, then $s_i = s_0 + s_i'$ $(i = 1,2)$. Because of $t_i = s_i + e_R = s_0 + s_i' + e_R$ and $s_i = t_i \cap U^{\perp}$, we know $s_0 = (t_1 \cap U^{\perp}) \cap (t_2 \cap U^{\perp}) = t_1 \cap t_2 \cap U^{\perp} = s_1 \cap t_2 = s_2 \cap t_1$, and $t_1 \cap t_2 = (s_1 + e_R) \cap t_2 = (s_0 + s_1' + e_R) \cap t_2 = ((s_0 + e_R) + s_1') \cap t_2$. Since $s_0 + e_R \subseteq t_2$, then $t_1 \cap t_2 = (s_0 + e_R) + (s_1' \cap t_2)$, while $s_1' \cap t_2 \subseteq s_1 \cap t_2 = s_0$, so $t_1 \cap t_2 = s_0 + e_R$. From the definition of t, we assume $t_i (i = 1,2)$ as follows:

$$t_i = \begin{array}{cc} \left(\begin{array}{cccc} I^{(n)} & 0 & 0 & 0 \\ 0 & P_{i_2} & 0 & 0 \\ 0 & 0 & I^{(n)} & 0 \\ 0 & 0 & 0 & P_{i_4} \end{array}\right) & \begin{array}{c} n \\ r+n'-2n \\ n \\ r+n'-2n \end{array} \\ \begin{array}{cccc} n & v-n & n & v-n \end{array} & \end{array} .$$

Let

$$t_1 \cap t_2 = \begin{array}{cc} \left(\begin{array}{cccc} I^{(n)} & 0 & 0 & 0 \\ 0 & P_2 & 0 & 0 \\ 0 & 0 & I^{(n)} & 0 \\ 0 & 0 & 0 & P_4 \end{array}\right) & \begin{array}{c} n \\ r+n'-2n \\ n \\ r+n'-2n \end{array} \\ \begin{array}{cccc} n & v-n & n & v-n \end{array} & \end{array} .$$

From $t_1 \cap t_2 = s_0 + e_R$, we know $\dim(t_1 \cap t_2) = k + 2n' - n$. So,

$$\dim\begin{pmatrix} 0 & P_2 & 0 & 0 \\ 0 & 0 & 0 & P_4 \end{pmatrix} = k + 2n' - 3n.$$

For any $e_L = (e_{U_1}, e_{U_2}, \cdots, e_{U_l}) \in E_L$, we assume e_L as follows:

$$e_L = \begin{array}{cc} \left(\begin{array}{cccccccc} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & R_4 & I^{(l)} & 0 & R_7 & R_8 \end{array}\right) & \begin{array}{c} l \\ n-l \\ l \end{array} \\ \begin{array}{cccccccc} l & n-l & n'-n & v-n' & l & n-l & n'-n & v-n' \end{array} & \end{array} ,$$

If $e_R \subset t_1 \cap t_2$ and $e_L \subset e_R$, then

$$e_R = \begin{array}{cc} \left(\begin{array}{cccccccc} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(n'-n)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & R_4 & I^{(l)} & 0 & R_7 & R_8 \\ 0 & 0 & 0 & B_4 & 0 & I^{(n-l)} & 0 & B_8 \\ 0 & 0 & 0 & B_4' & 0 & 0 & I^{(n'-n)} & B_8' \end{array}\right) & \begin{array}{c} l \\ n-l \\ n'-n \\ l \\ n-l \\ n'-n \end{array} \\ \begin{array}{cccccccc} l & n-l & n'-n & v-n' & l & n-l & n'-n & v-n' \end{array} & \end{array} .$$

So, every row of $\begin{pmatrix} 0 & B_4 & 0 & B_8 \\ 0 & B'_4 & 0 & B'_8 \end{pmatrix}$ is the linear combination of

$$\begin{pmatrix} 0 & P_2 & 0 & 0 \\ 0 & 0 & 0 & P_4 \end{pmatrix}.$$

Therefore, the number of e_R which contained in $t_1 \cap t_2$ and containing e_L is $q^{(n'-l)(k+2n'-3n)}$.

Theorem 5.2 The maximum probability of success in impersonation attack and substitution attack from U_L on R are:

$$P_I(L) = \frac{1}{q^{2(n'-l)(v+n-n'-r)-(n'-n)(n-l)}}, \qquad P_S(L) = \frac{1}{q^{(n'-l)(2n-2n'+l)+(n'-n)(n-l)}}.$$

Proof. (1) Impersonation attack: U_L, after receiving keys, encodes a message and sends it to the receiver, U_L is successful if the receiver accepts it as legitimate message. Denote $P_I(L)$ is the maximum probability of success of the impersonation attack, it can be expressed as

$$\begin{aligned} P_I(L) &= \max_{e_L \in E_L} \max_{m \in M} \left\{ \frac{|\{e_R \in E_R | e_L \subset e_R,\ e_R \subset t\}|}{|\{e_R \in E_R | e_L \subset e_R\}|} \right\} \\ &= \frac{q^{2(r-n)(n'-l)+(n'-n)(n-l)}}{q^{2(v-n')(n'-l)}} \\ &= \frac{1}{q^{2(n'-l)(v+n-n'-r)-(n'-n)(n-l)}}. \end{aligned}$$

(2) Substitution attack: U_L, after observing a legitimate message m, substitutes it with another message m'. U_L is successful if the receiver accepts it as legitimate message. Denote $P_S(L)$ is the maximum probability of success of the substitution attack, it can be expressed as

$$\begin{aligned} P_S(L) &= \max_{e_L \in E_L} \max_{m \in M} \max_{m \neq m' \in M} \left\{ \frac{|\{e_R \in E_R | e_L \subset e_R, e_R \subset t, e_R \subset t'\}|}{|\{e_R \in E_R | e_L \subset e_R, e_R \subset t\}|} \right\} \\ &= \max_{n \leq k \leq 2r-n-1} \frac{q^{(n'-l)(k+2n'-3n)}}{q^{2(r-n)(n'-l)+(n'-n)(n-l)}} \\ &= \frac{1}{q^{(n'-l)(2n-2n'+1)+(n'-n)(n-l)}}. \end{aligned}$$

References

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

[2] Simmons. G. J. Message Authentication with Arbitration of Transmitter/Receiver Disputes Advances in Cryptology-Crypto'87, Lecture Notes in Computer Science 304, Berlin:Springer-Verlag, 1988: 151-165.

[3] Wan Zhexian. Construction of Cartesian Authentication Codes from Unitary Geometry. Designs, Codes and cryptology. 1992, 2:333-356.

[4] MA Wenping, WANG Xinmei. A Construction of Authentication Codes with Arbitration Based on Symplectic Spaces. CHINESE J. COMPUTERS, 1999, 22(9):949-952.

[5] Gao You, Shi Xinhua, Wang Hongli. Construction of Authentication Codes with Arbitration from Symplectic Geometry over Finite Fields. Acta Scientiarum Naturalium Universitatis Nankaiensis, 2008, 41(6):72-77.

[6] Chen Shangdi, Zhao Dawei. New Construction of Authentication Codes with Arbitration from Pseudo-Sympletic Geometry over Finite Fields. ARS COMBINATORIA 2010, 97A:453-465.

[7] LI Ruihu, LI Zunxian. Construction of A^2-codes from symplectic geometry. Journal of Shanxi Normal University(Natural Science Edition), 1998, 26(4):10-15.

[8] Chaoping Xing, Huaxiong Wang, Kwok-Yan Lam. Constructions of authentication codes from algebraic curves over finite fields, IEEE Trans. Inform. Theory.2000,46: 886-892.

[9] Claude Carlet, Cunsheng Ding, Harald Niederreiter. Authentication Schemes from Highly Nonlinear Functions. Designs, Codes and Cryptology.2006,40(1): 71-79.

[10] R.Safavi-Naini,H.Wang. Multireceiver Authentication Codes: Models, Bounds, Constructions and Extensions . Information and Computation, 1999, 151(1): 148-172.

[11] Y.Desmedt, Y.Frankle and M.Yung. Multi-receiver/Multi-sender network security: efficient authenticated multicast/feedback. IEEE Infocom'92, 1992, 2045-2054.

[12] QI Yingchun, ZHOU Tong. Multiple Authentication Code with Multi-transmitter and Its Constructions . JOURNAL OF ZHONGZHOU UNIVERSITY, 2003, 20(1):118-120.

[13] MA Wenping, WANG Xinmei. Several New Constructions on Multitransmitters Authentication Codes . ACTA ELECTRONICA SINICA, vol.28, No.4, 2000,117-119.

[14] DU Qingling, LV Shuwang. Bounds and Construction for Multisender Authentication Code . Computer Engineering and Applications, 2004.10,9 -10,29.

[15] WAN Zhexian. Geometry of Classical Groups over Finite Fields.(Second Edition) Beijing: Science Press, 2002.