Two Constructions of Multireceiver Authentication Codes from Singular Symplectic Geometry over Finite Fields

You Gao *, Yifan He

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

Abstract: In this paper, we constructed two multireceiver authentication codes from singular symplectic geometry over finite fields. Under the assumption that the probability distribution on the source states and sender's key space is uniform, the parameters and success probabilities of different types of deceptions are also computed .
Key words: Multireceiver authentication codes, Singular Symplectic Geometry, Construction, Security Analysis.

§1.Introduction

The construction of authentication codes is an important topic in cryptography , and multireceiver authentication codes(MRA-codes) are introduced by Desmedt, Frankel, and Yung [1] as an extension of Simmons model of unconditionally secure authentication[2], they also gave two constructions for MRA-codes: one based on polynomials and the other based on finite geometries. R.Safavi-Naini and H.Wang[3] generated the formal definition of multireceiver authentication codes. In the MRA-model, a sender wants to authenticate a message for a group of receivers such that each receiver can verify authenticity of the received message. There are three phases in an MRA-model[3]:

1.*Key distribution.*The KDC(key distribution center) privately transmits the key information to the sender and each receiver (the sender can also be the KDC).

2.*Broadcast.* For a source state, the sender generates the authenticated message using his/her key and broadcasts the authenticated message.

*Correspondence : College of Science, Civil Aviation University of China,Tianjin 300300, P.R.China; E-mail: gao_you@263.net

3. *Verification.* Each user can verify the authenticity of the broadcast message.

Denote by $X_1 \times \cdots \times X_2$ the direct product of sets $X_1, \cdots, X_2$ and by p_i projection mapping of $X_1 \times \cdots \times X_2$ on X_i. That is,$p_i : X_1 \times \cdots \times X_2 \to X_i$ defined by $p_i(x_1, x_2, \ldots, x_n)=x_i$ Let $g_1 : X_1 \to Y_1$ and $g_2 : X_2 \to Y_2$ be two mappings, we denote the direct product of g_1 and g_2 by $g_1 \times g_2$ where $g_1 \times g_2$: $X_1 \times X_2 \to Y_1 \times Y_2$ is defined by $(g_1 \times g_2)(x_1, x_2) = (g(x_1), g(x_2))$. The identity mapping on a set X is demoted by 1_X.

Let $C = (S, M, E, f)$ and $C_i = (S_i, M_i, E_i, f_i), i = 1, 2, \cdots n$ be authentication codes. We call $(C; C_1, C_2, \cdots, C_n)$ a multireceiver authentication code (MRA-codes)if there exit two mappings $\tau : E \to E_1 \times \cdots \times E_n$ and $\pi : M \to M_1 \times \cdots \times M_n$ such that for any $(s, e) \in S \times E$ and any $1 \leq i \leq n$, the following identity holds

$$p_i(\pi f(s, e)) = f_i((1_S \times p_i\tau)(s, e)).$$

Let $\tau_i = p_i\tau$ and $\pi_i = p_i\pi$. Then we have for each$(s, e) \in S \times E$

$$\pi_i f(s, e) = f_i(1_S \times \tau_i)(s, e).$$

We adopt Kerckhoff's principle that everything in the system except the actual keys of the sender and receivers is public. This includes the probability distribution of the source states and the sender's keys.

Attackers could be *outsiders* who do not have access to any key information, or *insiders* who have some key information. We only need to consider the latter group as it is at least as powerful as the former. We consider the systems that protect against the coalition of groups of up to a maximum size of receivers, and we study impersonation and substitution attacks.

Assume there are n receivers $R_1, \cdots, R_n$. Let $L = \{i_1 \cdots i_l\} \subseteq \{1, \ldots n\}$, $E_L = E_{R_{i_1}}, \times \cdots \times E_{R_{i_l}}$ and $R_L = \{R_{i_1}, \cdots R_{i_l}\}$. We consider the attack from R_L on a receiver R_i , where $i \notin L$.

Impersonation attack:R_L ,after receiving their secret keys, send a message m to R_i. R_L is successful if m is accepted by R_i as authentic. We denote by $P_I[i, L]$ the success probability of R_L in performing an impersonation attack on R_i This can be expressed as

$$P_I[i, L] = \max_{e_L \in E_L} \max_{m \in M} P(m \text{ is accepted by } R_i | e_L) \text{ where } i \notin L, e_L \in E_L$$

Substitution attack:R_L,after observing a message m that is transmitted by the sender, replace m with another message m'. $R_L$is successful if m' is accepted by R_i as authentic. We denote by $P_S[i, L]$ the success probability of R_L in performing a substitution attack on R_i. We have

$P_S[i,L] = \max_{e_L \in E_L} \max_{m \in M} \max_{m' \neq m \in M} P(R_i \text{ accepts } m' | m, e_L)$, where $i \notin L$

There are some constructions of multireceiver authentication codes are given in[3-7], and it is well known that authentication codes which are constructed by the geometry of classical groups over finite fields are easy to compute,see e.g.[8],[9],[10]. In this paper we construct two new multireceiver codes from singular symplectic geometry over finite fields, and the security analysis are also given.

§2.Preliminaries

Singular symplectic geometry over finite fields is introduced in [11]. Let $n = 2\nu + l$ and define the $2\nu + l \times 2\nu + l$ alternate matrix

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

The set of all $(2\nu + l) \times (2\nu + l)$ nonsingular matrices T over $\mathbb{F}_q$ satisfying $TK_lT = K_l$ forms a group , called the singular symplectic group of $2\nu + l$ over the finite field $\mathbb{F}_q$, denoted by $Sp_{2\nu+l,\nu}(\mathbb{F}_q)$. There is an action of $Sp_{2\nu+l,\nu}(\mathbb{F}_q)$ on $\mathbb{F}_q^{(2\nu+l)}$ defined as follows:

$$\mathbb{F}_q^{(2\nu+l)} \times Sp_{2\nu+l,\nu}(\mathbb{F}_q) \to \mathbb{F}_q^{(2\nu+l)}$$

$$((x_1 \cdots, x_\nu \cdots, x_{2\nu+l}), T) \mapsto (x_1 \cdots, x_\nu \cdots, x_{2\nu+l})T$$

Then the vector space $\mathbb{F}_q^{(2\nu+l)}$ together with the above action of the group $S_{P_{2\nu+l,\nu}}(\mathbb{F}_q)$ is called the $2\nu + l$-dimensional singular symplectic space over $\mathbb{F}_q$.

Let $e_i (1 \leqslant i \leqslant 2\nu + l)$ be the row vector in $\mathbb{F}_q^{(2\nu+l)}$ whose i-th coordinate is 1 and all other coordinates are 0. Denote by E the l-dimensional subspace of $\mathbb{F}_q^{(2\nu+l)}$ generated by $e_{2\nu+1}, e_{2\nu+2}, \cdots, e_{2\nu+l}$. An m-dimensional subspace P of $\mathbb{F}_q^{(2\nu+l)}$ is called a subspace of $type(m,s,k)$ if

(i)PK_lP^t is cogredient to $M(m,s)$,and
(ii)$\dim(P \bigcap E) = k$, where

$$M(m,s) = \begin{pmatrix} 0 & I^{(s)} & \\ -I^{(s)} & 0 & \\ & & 0^{(m-s)} \end{pmatrix}$$

Let ν, u two non-zero vectors in $\mathbb{F}_q^{(2\nu+l)}$, they are said to be orthogonal(with respect to K_l) if $uK_l\nu^t = 0$, we say that u is orthogonal to ν.

Furthermore, for any subspace P we denote by $P^{\perp}$ the following set :

$$P^{\perp} = \{u \in \mathbb{F}_q^{(2\nu+l)} | uK_l\nu^t = 0, \text{ for all } \nu \in P\}$$

More properties of singular symplectic geometry over finite fields can be found in [11].

§3.Construction

Construction 1

Let $\mathbb{F}_q$ be a finite field with q elements and $v_i(1 \leq i \leq 2\nu)$ be the row vector in $\mathbb{F}_q^{(2\nu+l)}$. Assume that $2 \leq 2n < \nu, 1 < k \leq l$. $U = \langle v_1, v_2 \cdots, v_n, e_{2\nu+1} \rangle$, and U is a fixed subspace of type $(n+1, 0, 1)$. The set of source states $S = \{s \mid s$ is a subspace of type $(2n+k, 0, k)$ and $U \subset S \subset U^{\perp}\}$; The set of transmitter's encoding rules $E_T = \{e_T$ is a subspace of type $(2n+1, n, 1)$ and $U \subset e_t\}$; The set of ith receiver's decoding rules $E_{R_i} = \{e_{R_i}$ is a subspace of type $(n+2, 1, 1)$which is orthogonal to $\langle v_1, \cdots v_{i-1}, v_{i+1}, \cdots, v_n \rangle$ and $U \subset e_{R_i}\}$; The set of message $M = \{m | m$ is a subspace of type $(3n+k, n, k)$, and $U \subset m\}$.

1.*Key distribution.*The KDC randomly chooses a subspace $e_T \in E_T$, then privately sends e_T to the sender T. And the KDC randomly chooses a $e_{R_i} \in E_{R_i}$ and $e_{R_i} \in E_T$, then privately sends e_{R_i} to the ith receiver, where $1 \leq i \leq n$.

2.*Broadcast.*For a source state $s \in S$,the sender calculates $m = s + e_T$ and broadcast m.

3.*Verification.*Since the receiver R_i holds the decoding rule e_{R_i}, R_i accepts m as authentic if $e_{R_i} \in m$. R_i can get s from $s = m \bigcap U^{\perp}$.

We assume that the encoding rules of the transmitter and the receiver are chosen according to an uniform probability distribution. From the transitivity properties of singular symplectic group we can assume that

$$U = \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$
$$\begin{matrix} n & \nu-n & n & \nu-n & 1 & l-1 \end{matrix}$$

$$U^{\perp} = \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 \\ 0 & I^{(\nu-n)} & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(\nu-n)} & 0 \\ 0 & 0 & 0 & 0 & I^{(l)} \end{pmatrix}$$
$$\begin{matrix} n & \nu-n & n & \nu-n & l \end{matrix}$$

Lemma 1 The above construction of authentication codes is reasonable, that is

(1)$s + e_T = m \in M$, for all $s \in S$ and $e_T \in E_T$,

(2)for any $m \in M$, $s = m \bigcap U^{\perp}$ is an uniquely source state contained in m and there is $e_T \in E_T$, such that $m = s + e_T$.

Proof: (1)For $s \in S$, $e_T \in E_T$, from the definition of s and e_T, we can assume that

$$S = \begin{pmatrix} U \\ Q \end{pmatrix} \begin{matrix} n+1 \\ n+k-1 \end{matrix} \quad \text{and } e_T = \begin{pmatrix} U \\ R \end{pmatrix} \begin{matrix} n+1 \\ n \end{matrix}$$

then

$$\begin{pmatrix} U \\ Q \end{pmatrix} K_l \begin{pmatrix} U \\ Q \end{pmatrix}^T = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

and

$$\begin{pmatrix} U \\ R \end{pmatrix} K_l \begin{pmatrix} U \\ R \end{pmatrix}^T = \begin{pmatrix} 0 & I^{(n)} & 0 \\ -I^{(n)} & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

obviously, for any $q \in Q$ and $q \neq 0$, we have $q \notin e_T$,therefore

$m = s+e_T = \begin{pmatrix} U \\ Q \\ R \end{pmatrix}$,and $\begin{pmatrix} U \\ Q \\ R \end{pmatrix} K \begin{pmatrix} U \\ Q \\ R \end{pmatrix}^T = \begin{pmatrix} 0 & 0 & I^{(n)} & 0 \\ 0 & 0 & * & 0 \\ -I^{(n)} & * & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$

so m is a subspace of type$(3n + k, n, k)$, and $U \subset m$.

(2)For any $m \in M$, m is a subspace of type $(3n + k, n, k)$,so there is a subspace $V \subset m$, satisfying $\begin{pmatrix} U \\ V \end{pmatrix} K_l \begin{pmatrix} U \\ V \end{pmatrix}^T = \begin{pmatrix} 0 & I^{(n)} & 0 \\ -I^{(n)} & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{matrix} n \\ n \\ 1 \end{matrix}$ We can assume that$m = \begin{pmatrix} U \\ V \\ P \end{pmatrix}$ satisfying $\begin{pmatrix} U \\ V \\ P \end{pmatrix} K_l \begin{pmatrix} U \\ V \\ P \end{pmatrix}^T = \begin{pmatrix} 0 & I^{(n)} & 0 \\ -I^{(n)} & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{matrix} n \\ n \\ n+k \end{matrix}$

denote $s = \begin{pmatrix} U \\ P \end{pmatrix}$, then s is a subspace of type$(2n + k, 0, k)$, and $U \subset S \subset U^{\perp}$, so $s \in S$. For any $v \in V$ and $v \neq 0$, we have $v \notin s$, so $s = m \bigcap U^{\perp}$, then $e_T = \begin{pmatrix} U \\ V \end{pmatrix}$ is an encoding rule and $m = s + e_T$.

If there is another source state s' contained in m, from the definition of s, we know $s' \subset m \bigcap U^{\perp} = s$, and dim (s') =dim (s), so $s' = s$,*ie.*, s is the uniquely source state contained in m.

Lemma 2 The number of the source states is $|S| = q^{n(l-k)}N(n, \nu - n)N(k-1, l-1)$.

Proof: From the definition of s, s is a subspace of type $(2n+k, 0, k)$ and $U \subset S \subset U^{\perp}$, so s has the form as follows

$$S = \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & X_1 & 0 & 0 & 0 & 0 & X_2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \end{pmatrix} \begin{matrix} n \\ n \\ 1 \\ k-1 \end{matrix}$$
$$\begin{matrix} n & \nu-n & n & \nu-n & 1 & k-1 & l-k \end{matrix}$$

whereX_1 is $\nu - n$ dimensional vector subspaces in $\mathbb{F}_q^{(n)}$ and X_2 arbitrarily. Therefore the number of the source states is $|S| = q^{n(l-k)}N(n, \nu-n)N(k-1, l-1)$.

Lemma 3 The number of encoding rules of transmitter is $|E_T| = N'(n+1, 0, 1; 2n+1, n, 1; 2\nu)$.

Proof: We can compute the number of encoding rules of transmitter by Theorem 3.29[11], $|E_T| = N'(n+1, 0, 1; 2n+1, n, 1; 2\nu)$.

Lemma 4 The number of the decoding rules of ith receiver is $|E_{R_i}| = q^{2\nu-2n+l-1}$.

Proof: From the definition of E_{R_i}, it has the form as follows

$$E_{R_i} = \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & Y_1 & Y_2 & Y_3 & 0 & Y_4 & Y_5 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} n \\ 1 \\ 1 \end{matrix}$$
$$\begin{matrix} n & \nu-n & n & \nu-n & 1 & k-1 & l-k \end{matrix}$$

where Y_2 has the form$(0, 0 \cdots, x_{\nu+i}, 0 \cdots 0)$,$x_{\nu+i} \neq 0$ and Y_1, Y_3, Y_4, Y_5 arbitrarily. So the number of the decoding rules of ith receiver is$|E_{R_i}| = q^{2\nu-2n+l-1}$.

Lemma 5(1)The number of encoding rules e_T contained in m is $q^{n(n+k-1)}$.

(2)The number of the messages is

$$|M| = q^{n(l-2k-n+1)}N(n, \nu-n)N(k-1, l-1)N'(n+1, 0, 1; 2n+1, n, 1; 2\nu).$$

Proof: m is a subspace of type$(3n+k, n, k)$, and $U \subset m$, so we can

assume m has the form as the follows

$$m = \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(n)} & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \end{pmatrix} \begin{matrix} n \\ n \\ n \\ 1 \\ k-1 \end{matrix}$$

$$\begin{matrix} n & n & \nu-2n & n & n & \nu-2n & 1 & k-1 & l-k \end{matrix}$$

if $e_T \subset m$, then $e_T = \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & Y_1 & 0 & I^{(n)} & 0 & 0 & 0 & Y_2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} n \\ n \\ 1 \end{matrix}$

$$\begin{matrix} n & n & \nu-2n & n & n & \nu-2n & 1 & k-1 & l-k \end{matrix}$$

where Y_1, Y_2 arbitrarily, then the number of encoding rules e_T contained in m is $q^{n(n+k-1)}$.

(2)Since a message contains only one source state and the number of transmitter's encoding rules contained in a message has been computed,we can compute $|M|$ by $|M| = |S||E_T|/q^{n(n+k-1)}$, then the number of the messages is $|M| = q^{n(l-2k-n+1)}N(n, \nu-n)N(k-1, l-1)N'(n+1, 0, 1; 2n+1, n, 1; 2\nu)$.

Theorem 1 In the above construction of multireceiver authentication codes, the parameters are computed as follows
$|S| = q^{n(l-k)}N(n, \nu-n)N(k-1, l-1)$,
$|M| = q^{n(l-2k-n+1)}N(n, \nu-n)N(k-1, l-1)N'(n+1, 0, 1; 2n+1, n, 1; 2\nu)$,
$|E_T| = N'(n+1, 0, 1; 2n+1, n, 1; 2\nu)$,
$|E_{R_i}| = q^{2\nu-2n+l-1}$.

Assume there are n receivers $R_1, \cdots, R_n$. Let $L = \{i_1 \cdots i_{l'}\} \subseteq \{1, \ldots n\}$, $R_L = \{R_{i_1}, \cdots R_{i_{l'}}\}$ and $E_L = E_{R_{i_1}} \times \cdots \times E_{R_{i_{l'}}}$ We consider the attack from R_L on a receiver R_i ,where $i \notin L$. Without loss of generality, we can assume that $R_L = \{R_1, \cdots, R_{l'}\}, E_L = \{E_{R_1} \times \cdots \times E_{R_{l'}}\}$, where $1 \leq l' \leq n-1$. Now we give the security analysis about the above construction.

Lemma 6 For any $R_L = \{R_1, \cdots, R_{l'}\} \in E_L$, the number of e_T containing e_L is $q^{(2\nu-2n+l-1)(n-l')}$.

Proof: From the definition of e_{R_i}, we can assume that

$$e_L = \begin{pmatrix} I^{(n-l')} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(l')} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & Z_1 & I^{(l')} & 0 & Z_2 & 0 & Z_3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} n-l' \\ l' \\ l' \\ 1 \end{matrix}$$

$$\begin{matrix} n-l' & l' & \nu-n & l' & n-l' & \nu-n & 1 & l-1 \end{matrix}$$

if $e_L \subset e_T$, then

$$e_T = \begin{pmatrix} I^{(n-l')} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(l')} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & Z_1 & I^{(l')} & 0 & Z_2 & 0 & Z_3 \\ 0 & 0 & Y_1 & 0 & I^{(n-l')} & Y_2 & 0 & Y_3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ n-l' & l' & \nu-n & l' & n-l' & \nu-n & 1 & l-1 \end{pmatrix} \begin{matrix} n \\ n-l' \\ l' \\ l' \\ n-l' \\ 1 \end{matrix}$$

where Y_1, Y_2, Y_3 arbitrarily, so the number of e_T containing e_L is $q^{(2\nu-2n+l-1)(n-l')}$.

Lemma 7 For any $m \in M$ and $e_L, e_{R_i} \subset m$, where $i \notin L$.

(1)the number of e_T contained in m and containing e_L is $q^{(n+k-1)(n-l')}$;

(2)the number of e_T contained in m and containing e_L, e_{R_i} is $q^{(n+k-1)((n-l'-1)}$.

Proof:(1)If $e_L \subset m$(m has the same form as Lemma 5), then we can assume that

$$e_L = \begin{pmatrix} I^{(l')} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l')} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & Z_1 & 0 & I^{(l')} & 0 & 0 & 0 & 0 & Z_2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ l' & n-l' & n & \nu-2n & l' & n-l' & n & \nu-2n & 1 & k-1 & l-k \end{pmatrix} \begin{matrix} l' \\ n-l' \\ l' \\ 1 \end{matrix}$$

if $e_L \subset e_T \subset m$,then

$$e_T = \begin{pmatrix} I^{(l')} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l')} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & Z_1 & 0 & I^{(l')} & 0 & 0 & 0 & 0 & Z_2 & 0 \\ 0 & 0 & Z_1^* & 0 & 0 & I^{(n-l')} & 0 & 0 & 0 & Z_2^* & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ l' & n-l' & n & \nu-2n & l' & n-l' & n & \nu-2n & 1 & k-1 & l-k \end{pmatrix} \begin{matrix} l' \\ n-l' \\ l' \\ n-l' \\ 1 \end{matrix}$$

therefore the number of e_T contained in m and containing e_L is $q^{(n+k-1)((n-l')}$.

(2)Similarly, we can prove that the number of e_T contained in m and containing e_L, e_{R_i} is $q^{(n+k-1)((n-l'-1)}$.

Lemma 8 Assume that m_1 and m_2 are two distinct messages which commonly contain a transmitter's encoding rule e_T .s_1 and s_2 contained

in m_1 and m_2 are two source states,respectively,then for any $e_L, e_{R_i} \subset m_1 \cap m_2$,the number of e_T contained in $m_1 \cap m_2$ and containing e_L, e_{R_i} is $q^{(n-l'-1)(k_1-n-1)}$, where $k_1 = dim(s_1 \cap s_2)$.

Proof: From the definition of source states, it is easy to know that $n+1 \leq k_1 \leq 2n+k-1$. Now we assume that

$$m_1 = \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(n)} & 0 & 0 & 0 & 0 \\ 0 & A_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & A_2 \end{pmatrix} \begin{matrix} n \\ n \\ n \\ 1 \\ k-1 \end{matrix}$$
$$\begin{matrix} n & n & \nu-2n & n & n & \nu-2n & 1 & l-1 \end{matrix}$$

$$m_2 = \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(n)} & 0 & 0 & 0 & 0 \\ 0 & B_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & B_2 \end{pmatrix} \begin{matrix} n \\ n \\ n \\ 1 \\ k-1 \end{matrix}$$
$$\begin{matrix} n & n & \nu-2n & n & n & \nu-2n & 1 & l-1 \end{matrix}$$

then

$$m_1 \bigcap m_2 = \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(n)} & 0 & 0 & 0 & 0 \\ 0 & C_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & C_2 \end{pmatrix} \begin{matrix} n \\ n \\ n \\ 1 \\ k-1 \end{matrix}$$
$$\begin{matrix} n & n & \nu-2n & n & n & \nu-2n & 1 & l-1 \end{matrix}$$

since $m_1 \bigcap m_2 = s_1 \bigcap s_2 + e_T$, then $\dim(m_1 \bigcap m_2) = k_1 + n$. And

$$dim \begin{pmatrix} 0 & C_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & C_2 \end{pmatrix} = k_1 - n - 1$$

for any $e_L, e_{R_i} \subset m_1 \bigcap m_2$, where $i \notin L$.

$$e_L = \begin{pmatrix} I^{(l')} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l')} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & X_1 & 0 & I^{(l')} & 0 & 0 & 0 & 0 & X_2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} l' \\ n-l' \\ l' \\ 1 \end{matrix}$$
$$\begin{matrix} l' & n-l' & n & \nu-2n & l' & n-l' & n & \nu-2n & 1 & k-1 & l-k \end{matrix}$$

and

$$e_{R_i} = \begin{pmatrix} I^{(l')} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l')} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & Y_1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & Y_2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} l' \\ n-l' \\ 1 \\ 1 \end{matrix}$$

$$\begin{matrix} l' & n-l' & n & \nu-2n & i-1 & i & n-i & n & \nu-2n & 1 & k-1 & l-k \end{matrix}$$

if $e_L, e_{R_i} \subset e_T \subset m_1 \bigcap m_2$, then

$$e_T = \begin{pmatrix} I^{(l')} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l')} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & X_1 & 0 & I^{(l')} & 0 & 0 & 0 & 0 & 0 & 0 & X_2 & 0 \\ 0 & 0 & Z_1^* & 0 & 0 & I^{(i-l'-1)} & 0 & 0 & 0 & 0 & 0 & Z_2^* & 0 \\ 0 & 0 & Y_1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & Y_2 & 0 \\ 0 & 0 & Z_1 & 0 & 0 & 0 & 0 & I^{(n-i)} & 0 & 0 & 0 & Z_2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} l' \\ n-l' \\ l' \\ i-l'-1 \\ 1 \\ n-i \\ 1 \end{matrix}$$

$$\begin{matrix} l' & n-l' & n & \nu-2n & l' & i-l'-1 & 1 & n-i & n & \nu-2n & 1 & k-1 & l-k \end{matrix}$$

so the number of e_T contained in $m_1 \cap m_2$ and containing e_L, e_{R_i} is $q^{(n-l'-1)(k_1-n-1)}$.

Theorem 2 In the above construction of multireceiver authentication codes, the largest probabilities of success for *Impersonation attack* and *Substitution attack* from R_L on a receiver R_i are

$$P_I[i, L] = \frac{1}{q^{2(\nu-n)+l-1+(n-l'-1)(2\nu-3n+l-k)}}, P_S[i, L] = \frac{1}{q^{2n-l'+k-2}}$$

Proof: *Impersonation attack:* after receiving their secret keys,R_L send a message m to R_i. R_L is successful if m is accepted by R_i as authentic:

$$\begin{aligned} P_I[i, L] &= \max_{e_L \in E_L} \max_{m \in M} P(m \text{ is accepted by } R_i | e_L) \text{ where } i \notin L \\ &= \max_{e_L \in E_L} \max_{m \in M} \left\{ \frac{\{e_T \in E_T | e_T \subset m, and\ e_T \supset e_L, e_{R_i}\}}{\{e_T \in E_T | e_L \subset e_T\}} \right\} \\ &= \frac{q^{(n+k-1)(n-l'-1)}}{q^{(2\nu-2n+l-1)(n-l')}} \\ &= \frac{1}{q^{2(\nu-n)+l-1+(n-l'-1)(2\nu-3n+l-k)}} \end{aligned}$$

Substitution attack: after observing a message m that is transmitted by the sender, replace m with another message m'.R_L is successful if m' is accepted by R_i as authentic:

$$
\begin{aligned}
P_S[i,L] &= \max_{e_L \in E_L} \max_{m \in M} \max_{m' \neq m \in M} P(R_i \text{ accepts } m' | m, e_L) \text{ where } i \notin L \\
&= \max_{e_L \in E_L} \max_{m \in M} \max_{m' \neq m \in M} \left\{ \frac{\{e_T \in E_T | e_T \subset m, m' \text{ and } e_T \supset e_L, e_{R_i}\}}{\{e_T \in E_T | e_L \subset e_T \text{ and } e_T \subset m\}} \right\} \\
&= \max \frac{q^{(k_1-n-1)(n-l'-1)}}{q^{(n-l')(n+k-1)}} \text{ where } n+1 \leq k_1 \leq 2n+k-1. \\
&= \frac{q^{(n+k-2)(n-l'-1)}}{q^{(n+k-1)(n-l')}} \\
&= \frac{1}{q^{2n-l'+k-2}}
\end{aligned}
$$

Construction 2

Let $\mathbb{F}_q$ be a finite field with q elements and $v_i (1 \leq i \leq 2\nu)$ be the row vector in $\mathbb{F}_q^{(2\nu+l)}$. Assume that $2 < r < s, r+s < \nu, 1 \leq k \leq l$. $U = \langle v_1, v_2 \cdots, v_r, e_{2\nu+1} \rangle$, and U is a fixed subspace of type $(r+1, 0, 1)$. The set of source states $S = \{s \mid s$ is a subspace of type $(r+2s+k, s, k)$ and $U \subset S \subset U^{\perp}\}$; The set of transmitter's encoding rules $E_T = \{e_T$ is a r-dimensional subspace in $\mathbb{F}_q^{(2\nu+l)}$ and $U + e_T$ is a subspace of type $(2r+1, r, 1)\}$; The set of *ith* receiver's decoding rules $E_{R_i} = \{e_{R_i}$ is 1-dimensional subspace $\mathbb{F}_q^{(2\nu+l)}$, and $U + e_{R_i}$ is a subspace of type $(r+2, 1, 1)$ which is orthogonal to $\langle v_1, \cdots v_{i-1}, v_{i+1}, \cdots, v_r \rangle\}$; The set of message $M = \{m | m$ is a subspace of type $(2(r+s)+k, r+s, k)$, and $U \subset m$, $m \bigcap U^{\perp}$ is a subspace of type$(r+2s+k, s, k)$ $\}$.

1.*Key distribution.*The KDC randomly chooses a subspace $e_T \in E_T$, and privately sends e_T to the sender T. Then the KDC randomly chooses a $e_{R_i} \in E_{R_i}$ and $e_{R_i} \in E_T$, then privately sends e_{R_i} to the *ith* receiver, where $1 \leq i \leq n$.
2.*Broadcast.*For a source state $s \in S$,the sender calculates $m = s + e_T$ and broadcasts m.
3. *Verification.*Since the receiver R_i holds the decoding rule e_{R_i},R_i accepts m as authentic if $e_{R_i} \in m$. R_i can get s from $s = m \bigcap U^{\perp}$.

We assume that the encoding rules of the transmitter and the receiver are chosen according to an uniform probability distribution. From the transitivity properties of singular symplectic group we can assume that

$$
U = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}
\begin{matrix} \\ \\ r & \nu-r & r & \nu-r & 1 & l-1 \end{matrix}
$$

$$U^{\perp} = \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 \\ 0 & I^{(\nu-r)} & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(\nu-r)} & 0 \\ 0 & 0 & 0 & 0 & I^{(l)} \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix}$$
$$\begin{matrix} n & \nu-r & r & \nu-r & l \end{matrix}$$

Lemma 9 The above construction of authentication codes is reasonable, that is

(1)$s + e_T = m \in M$, for all $s \in S$ and $e_T \in E_T$

(2)for any $m \in M$, $s = m \bigcap U^{\perp}$ is uniquely source state contained in m and there is $e_T \in E_T$, such that $m = s + e_T$.

The proof of the lemma is straightforward, so the proof is omitted.

Lemma 10 The number of encoding rules e_T contained in m is $q^{r(r+2s+k)}$.

Proof: If m is a message, then m is a subspace of type $(2(r+s)+k, r+s, k)$, and $U \subset m$, we can assume that

$$m = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(s)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I^{(s)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \\ 0 & 0 & 0 & I^{(r)} & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} r \\ s \\ s \\ 1 \\ k-1 \\ r \end{matrix}$$
$$\begin{matrix} r & s & \nu-r-s & r & s & \nu-r-s & 1 & k-1 & l-k \end{matrix}$$

if $e_T \subset m$, then

$$e_T = \begin{pmatrix} Q_1 & Q_2 & 0 & I^{(r)} & Q_3 & 0 & Q_4 & Q_5 & 0 \end{pmatrix} r$$
$$\begin{matrix} r & s & \nu-r-s & r & s & \nu-r-s & 1 & k-1 & l-k \end{matrix}$$

where Q_1, Q_2, Q_3, Q_4, Q_5 arbitrarily, so the number of encoding rules e_T contained in m is $q^{r(r+2s+k)}$.

Theorem 3 In the above construction of multireceiver authentication codes, the parameters are computed as follows

$|S| = q^{2s(l-k)} N(k-1, l-1) N(2s, s; 2(\nu - r))$

$|E_T| = q^{(2\nu-r+l)r}$

$|E_{R_i}| = q^{2\nu-r+l}$

$|M| = q^{r(2\nu-2r-2s+l-k)} q^{2s(l-k)} N(k-1, l-1) N(2s, s; 2(\nu - r))$

Proof: (1) For any $s \in S$, s has the form as follows

$$s = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_1 & 0 & R_2 & 0 & 0 & R_3 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \\ r & \nu-r & r & \nu-r & 1 & k-1 & l-k \end{pmatrix} \begin{matrix} r \\ 2s \\ 1 \\ k-1 \end{matrix}$$

where $(R_1 R_2)$ is a subspace of type$(2s, s)$ in $\mathbb{F}_q^{(2(\nu-r))}$, R_3 arbitrarily, so $|S| = q^{2s(l-k)} N(k-1, l-1) N(2s, s; 2(\nu-r))$.

(2) Since e_T is a r-dimensional subspace in $\mathbb{F}_q^{(2\nu+l)}$ and $U + e_T$ is a subspace of type $(2r+1, r, 1)$, so we can assume that

$$e_T = \begin{pmatrix} Q_1 & Q_2 & I^{(r)} & Q_3 & Q_4 \\ r & \nu-r & r & \nu-r & l \end{pmatrix} r$$

where Q_1, Q_2, Q_3, Q_4 arbitrarily, so $|E_T| = q^{(2\nu-r+l)r}$

(3) From the definition of e_{R_i},

$$e_{R_i} = \begin{pmatrix} Q_1 & Q_2 & 0 & 1 & 0 & Q_3 & Q_4 \\ r & \nu-r & i-1 & 1 & n-i & \nu-r & l \end{pmatrix} 1$$

where Q_1, Q_2, Q_3, Q_4 arbitrarily, so $|e_{R_i}| = q^{2\nu-r+l}$

(4) Since a message contains only one source state and the number of transmitter's encoding rules contained in a message has been computed, we can compute $|M|$ by $|M| = |S||E_T|/q^{r(r+2s+k)}$, so $|M| = q^{r(2\nu-2r-2s+l-k)} q^{2s(l-k)} N(k-1, l-1) N(2s, s; 2(\nu-r))$.

Lemma 11 For any $R_L = \{R_1, \cdots, R_{l'}\} \in E_L$, the number of e_T containing e_L is $q^{(2\nu-r+l)(r-l')}$, where $l' < r$.

Proof: From the definition of e_{R_i}, we can assume that

$$e_L = \begin{pmatrix} X_1 & X_2 & I^{(l')} & 0 & X_3 & X_4 \\ r & \nu-r & l' & r-l' & \nu-r & l \end{pmatrix} l'$$

where X_1, X_2, X_3, X_4 arbitrarily, if $e_L \subset e_T$, then

$$e_T = \begin{pmatrix} X_1 & X_2 & I^{l'} & 0 & X_3 & X_4 \\ Y_1 & Y_2 & 0 & I^{(r-l')} & Y_3 & Y_4 \\ r & \nu-r & l' & r-l' & \nu-r & l \end{pmatrix} \begin{matrix} l' \\ r-l' \end{matrix}$$

so the number of e_T containing e_L is $q^{(2\nu-r+l)(r-l')}$.

Lemma 12 For any $m \in M$ and $e_L, e_{R_i} \subset m$,, where $i \notin L$.

(1)the number of e_T contained in m and containing e_L is $q^{(r+2s+k)((r-l')}$;

(2)the number of e_T contained in m and containing e_L, e_{R_i} is $q^{(r+2s+k)((r-l'-1)}$.

Proof: (1) If $e_L \subset m$(m has the same form as Lemma 10), then we can assume that

$$e_L = \begin{pmatrix} \underset{l'}{Y_1} & \underset{r-l'}{Y_2} & \underset{s}{Y_3} & \underset{v-r-s}{0} & \underset{l'}{I^{(l')}} & \underset{r-l'}{0} & \underset{s}{Y_4} & \underset{v-r-s}{0} & \underset{1}{Y_5} & \underset{k-1}{Y_6} & \underset{l-k}{0} \end{pmatrix} l'$$

where $Y_1, Y_2, Y_3, Y_4, Y_5, Y_6$ arbitrarily, if $e_L \subset e_T \subset m$ then

$$e_T = \begin{pmatrix} \underset{l'}{Y_1} & \underset{r-l'}{Y_2} & \underset{s}{Y_3} & \underset{v-r-s}{0} & \underset{l'}{I^{(l')}} & \underset{r-l'}{0} & \underset{s}{Y_4} & \underset{v-r-s}{0} & \underset{1}{Y_5} & \underset{k-1}{Y_6} & \underset{l-k}{0} \\ \underset{l'}{Z_1} & \underset{r-l'}{Z_2} & \underset{s}{Z_3} & \underset{v-r-s}{0} & \underset{l'}{0} & \underset{r-l'}{I^{(r-l')}} & \underset{s}{Z_4} & \underset{v-r-s}{0} & \underset{1}{Z_5} & \underset{k-1}{Z_6} & \underset{l-k}{0} \end{pmatrix} \begin{matrix} l' \\ r-l' \end{matrix}$$

where $Z_1, Z_2, Z_3, Z_4, Z_5, Z_6$ arbitrarily, so the number of e_T contained in m and containing e_L is $q^{(r+2s+k)((r-l')}$.

(2) Similarly,we can prove that the number of e_T contained in m and containing e_L, e_{R_i} is $q^{(r+2s+k)((r-l'-1)}$.

Lemma 13 Assume that m_1 and m_2 are two distinct messages which commonly contain a transmitter's encoding rule e_T .s_1 and s_2 contained in m_1 and m_2 are two source states, respectively, then for any $e_L, e_{R_i} \subset m_1 \cap m_2$, the number of e_T contained in $m_1 \cap m_2$ and containing e_L, e_{R_i} $(i \notin L)$is $q^{(r-l'-1)(k_1-r-2s-1)}$, where $k_1 = dim(s_1 \cap s_2)$.

Proof: From the definition of source states, it is easy to know that $r+1 \leq k_1 \leq r+2s+k-1$. we choose m_1, m_2 as follows

$$m_1 = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 \\ 0 & A_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & A_2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & A_3 \\ 0 & 0 & I^{(r)} & 0 & 0 & 0 \end{pmatrix} \begin{matrix} r \\ s \\ s \\ 1 \\ k-1 \\ r \end{matrix}$$

$$m_2 = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 \\ 0 & B_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & B_2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & B_3 \\ 0 & 0 & I^{(r)} & 0 & 0 & 0 \end{pmatrix} \begin{matrix} r \\ s \\ s \\ 1 \\ k-1 \\ r \end{matrix}$$

and $m_1 \bigcap m_2 = s_1 \bigcap s_2 + e_T$, $\dim(m_1 \bigcap m_2) = k_1 + r$, so

$$m_1 \bigcap m_2 = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 \\ 0 & C_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & C_2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & C_3 \\ 0 & 0 & I^{(r)} & 0 & 0 & 0 \end{pmatrix} \begin{matrix} r \\ s \\ s \\ 1 \\ k-1 \\ r \end{matrix}$$
$$\begin{matrix} r & \nu-r & r & \nu-r & 1 & l-1 \end{matrix}$$

and $\dim \begin{pmatrix} 0 & C_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & C_2 & 0 \\ 0 & 0 & 0 & 0 & C_3 \end{pmatrix} = k_1 - r - 1$. Similar to lemma 8 we can derive the number of e_T contained in $m_1 \cap m_2$ and containing e_L, e_{R_i} is $q^{(r-l'-1)(k_1-r-1)}$.

Theorem 4 In the construction 2 of multireceiver authentication codes, the largest probabilities of success for *Impersonation attack* and *Substitution attack* from R_L on a receiver R_i are

$$P_I[i,L] = \frac{1}{q^{2\nu-r+l+(r-l'-1)(2\nu-2r-2s+l-k)}}, P_S[i,L] = \frac{1}{q^{(r-l'-1)(r+2)+r+2s+k}}$$

Proof: *Impersonation attack:* after receiving their secret keys,R_L send a message m to R_i.R_L is successful if m is accepted by R_i as authentic:

$$P_I[i,L] = \max_{e_L \in E_L} \max_{m \in M} P(m \text{ is accepted by } R_i | e_L) \text{ where } i \notin L$$

$$= \max_{e_L \in E_L} \max_{m \in M} \left\{ \frac{\{e_T \in E_T | e_T \subset m, and\ e_T \supset e_L, e_{R_i}\}}{\{e_T \in E_T | e_L \subset e_T\}} \right\}$$

$$= \frac{q^{(r+2s+k)(r-l'-1)}}{q^{(2\nu-r+l)(r-l')}}$$

$$= \frac{1}{q^{2\nu-r+l+(r-l'-1)(2\nu-2r-2s+l-k)}}$$

Substitution attack: after observing a message m that is transmitted by the sender ,replace m with another message m'.R_L is successful if m' is accepted by R_i as authentic:

$$P_S[i,L] = \max_{e_L \in E_L} \max_{m \in M} \max_{m' \neq m \in M} P(R_i \text{ accepts } m' | m, e_L) \text{ where } i \notin L$$

$$= \max_{e_L \in E_L} \max_{m \in M} \max_{m' \neq m \in M} \left\{ \frac{\{e_T \in E_T | e_T \subset m, m' \text{ and } e_T \supset e_L, e_{R_i}\}}{\{e_T \in E_T | e_L \subset e_T \text{ and } e_T \subset m\}} \right\}$$

$$= \max \frac{q^{(k_1-r-1)(r-l'-1)}}{q^{(r-l')(r+2s+k)}} \quad \text{where } r+1 \leq k_1 \leq r+2s+k-1.$$

$$= \frac{q^{(2s+k-2)(r-l'-1)}}{q^{(r-l')(r+2s+k)}}$$

$$= \frac{1}{q^{(r-l'-1)(r+2)+r+2s+k}}$$

Acknowledgements

This work is supported by the National Natural Science Foundation of China under Grant No.61179026, the Fundamental Research Funds for the Central Universities under Grant No.ZXH2012K003 and the Graduate Science and Technology Innovation Fund of Civil Aviation University of China under Grant No.YJSCX12-17.

References

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

[2] G.J.Simmons. Authentication theory/Coding theory, Advances in Cryptology, Proceedings of Crypto 84. Lecture Notes in Computer Science 196[C]. Berlin:Springer-Verlag, 1985:411-431.

[3] R. Safavi-Naini and H. Wang, Bounds and constructions for multireceiver authentication codes, Advances in Cryptology C Asiacrypt 98, Lecture Notes in Computer Science, 242-256.

[4] Li Xiyang,Qin Cong. New Constructions of Multi-receiver Authentication Codes[J]. Computer Engineering. 2008,34(15):138-139.

[5] R. Safavi-Naini and H. Wang, New results on multi-receiver authentication codes, Advances in Cryptology -Eurocrypt'98,Lecture Notes in Comp.Sci.1998,1403:527-541.

[6] K. Kurosawa and S.Obana, Characterisation of (k;n) multi-receiver authentication, Information Security and Privacy, ACISP'97,Lecture Notes in Cpmput.Sci.1997,1270:204-215.
[7] Du Qingling, Zhang Limin. Bounds and Construction for Multiple Authentication Codes with Mutlireceiver[J]. Journal of electronics and information technology. 2002, 24(8):1109-1112.
[8] Gao You and Huo Liqun. Construction of new authentication codes with arbitration from Singual Geometry over Finite Fields[J].Chinese Journal of Engineering Mathematics, 2011,28(5):629-640.
[9] Li Ruihu. Construction of Authentication Codes with Arbitration from Symplectic Geometry[J].Appl.Math.J. Chinese Univ.Ser.B,1999,14(4):475-480.
[10] Chen Shangdi, Zhao Dawei.Two Constructions of Multireceiver Authentication Codes from Symplectic Geometry over Finite Fields. Ars Combinatoria, 2011,98:193-203.
[11] Z.Wan, Geometry of classical groups over finite fields, 2nd edition, Science Press, Beijing/New York, 2002.