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

CHEN SHANGDI
Civil Aviation University of China
College of Science
Jinbei Road 2898, 300300, Tianjin
CHINA
11csd@163.com

AN LEI
Civil Aviation University of China
College of Science
Jinbei Road 2898, 300300, Tianjin
CHINA
anlei8712@yahoo.com.cn

Abstract: Multireceiver authentication codes allow one sender to construct an authenticated message for a group of receivers such that each receiver can verify authenticity of the received message. In this paper, two constructions of multireceiver authentication codes from singular symplectic geometry over finite fields are given. The parameters and the probabilities of success for different types of deceptions are computed.

Key–Words: Singular symplectic geometry, Multireceiver authentication codes, Finite fields, Construction, Probability

1 Introduction

As the flourish development of network communications and processing power of computer hardware, information security theory and technology have gradually been enriched and improved. Confidentiality and authentication are two important aspects of information security. Traditional two-user authentication codes are no longer suitable for network communication requirements, authentication codes with arbitration, multisender and multireceiver authentication systems come into being. This paper focuses on multireceiver authentication codes, two constructions of multireceiver authentication codes from singular symplectic geometry over finite fields are given. The parameters and the probabilities of success for different types of deceptions are computed.

Multireceiver authentication codes (MRA-codes) are introduced by Desmedt, Frankel, and Yung (DFY) [1] as an extension of Simmons' model of unconditionally secure authentication [2]. In an MRA-code, 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-code:

1. Key distribution. The KDC (key distribution centre) 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 an authenticated message using his/her key and broadcasts the authenticated message.

3. Verification. Each receiver can verify the authenticity of the received message.

Denote by $X_1\times\cdots\times X_n$ the direct product of sets $X_1, X_2, \cdots, X_n$, and by p_i the projection mapping of $X_1\times\cdots\times X_n$ on X_i. That is, $p_i : X_1\times\cdots\times X_n \to X_i$ defined by $p_i(x_1, x_2, \cdots, x_n) = x_i$. 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 $(g_1 \times g_2)(x_1, x_2) = (g_1(x_1), g_2(x_2))$. The identity mapping on a set X is denoted by 1_X.

Let $C = (S, M, E, f)$ and $C_i = (S, M_i, E_i, f_i)$, $i = 1, 2, ..., n$, be authentication codes. We call $(C; C_1, C_2, \cdots, C_n)$ a multireceiver authentication code (MRA-code) [3] if there exist two mappings $\tau : E \to E_1 \times\cdots\times E_n$ and $\pi : M \to M_1 \times\cdots\times Mn$ such that for any $(s, e) \in S \times E$ and any $1 \le i \le n$, 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 is public except the actual keys of the sender and receivers. 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 since it is at least as powerful as the former. We consider systems that work against the coalition of groups of up to a maximal size of receivers, and we study impersonation and substitution attacks.

Assume that there are n receivers $R_1, \cdots, R_n$. Let $L = \{i_1, \cdots, i_l\} \subseteq \{1, \cdots, n\}, R_L = \{R_{i_1}, \cdots, R_{i_l}\}$ 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 $i \notin L$.

Impersonation attack: R_L, after receiving its secret keys, sends a message m to R_i. The attack 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

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

where $i \notin L$.

Substitution attack: R_L, after observing a message m that is transmitted by the sender, replaces m with another message m'. The attack 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 . This can be expressed as

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

where $i \notin L$.

In [1] , Desmedt, Frankel and Yung gave two constructions of MRA-codes based on polynomials and finite geometries, respectively. In the case both of the sender and the receiver are not honest, Gao You [4], Chen Shangdi [5] constructed a series of authentication codes with arbitration. R. Safavi-Naini, Wang Huaxiong gave some results on authentication codes with one sender and multiple receivers [3] [6].R. Safavi-Naini also described the dynamics of authentication codes with one sender and multiple receivers. Ma Wenping, Wang Xinmei made great contributions on multisender authentication codes [7]. In this paper we construct two multireceiver authentication codes from singular symplectic geometry over finite fields. The parameters and the probabilities of deceptions of the codes are also computed.

2 Singular Symplectic Geometry

Let F_q be a finite field with q elements and

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

$$M(m, s) = \begin{pmatrix} 0 & I^{(s)} & \\ -I^{(s)} & 0 & \\ & & 0^{(m-2s)} \end{pmatrix}.$$

The singular symplectic group of degree $(2\nu + l)$ over F_q is defined to be the set of matrices

$$Sp_{2\nu+l,\nu}(F_q) = \{T \mid T K_l\, {}^tT = K_l\}$$

denoted by $Sp_{2\nu+l,\nu}(F_q)$.

Let $F_q^{(2\nu+l)}$ be the $(2\nu + l)$-dimensional row vector space over F_q. $Sp_{2\nu+l,\nu}(F_q)$ has an action on $F_q^{(2\nu+l)}$ defined as follows

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

$$((x_1, x_2, \ldots, x_{2\nu+l}), T) \mapsto (x_1, x_2, \ldots, x_{2\nu+l})T.$$

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

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

(i) $P K_l\, {}^tP$ is cogredient to $M(m, s)$;

(ii) $\dim(P \cap E) = k$.

Let $k \le l$ and $2s \le m - k \le \nu + s$. Denote the number of subspaces of type (m, s, k) in the $(2\nu + l)$-dimensional singular symplectic space over F_q by $N(m, s, k; 2\nu + l, \nu)$.

Denote by $P^\perp$ the set of vectors which are orthogonal to every vector of P, i.e.,

$$P^\perp = \{y \in F_q^{(2\nu+l)} | y K_l\, {}^tx = 0 \; for \; all \; x \in P\}.$$

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

More properties and undefined symbols of singular symplectic geometry over finite fields can be found in [8].

3 Constructions

3.1 Construction 1

Let F_q be a finite field with q elements and $e_i (1 \le i \le 2\nu + l)$ be the row vector in $F_q^{(2\nu+l)}$ whose i-th coordinate is 1 and all other coordinates are 0. Assume that $\nu \ge 3$, $2 \le n < t \le \nu$. $U = \langle e_1, e_2, \cdots, e_n, e_{2\nu+1}, e_{2\nu+2} \rangle$, i.e., U is a

$(n+2)$-dimensional subspace of $F_q^{(2\nu+l)}$ generated by $e_1, e_2, \cdots, e_n, e_{2\nu+1}, e_{2\nu+2}$, then $U^{\perp} = \langle e_1, \cdots, e_\nu, e_{\nu+n+1}, \cdots, e_{2\nu}, e_{2\nu+1}, e_{2\nu+2}, \cdots, e_{2\nu+l}\rangle$.

The set of source states S=$\{s | s$ is a subspace of type $(2t-n+k, t-n, k), 1 \leq k < l$ and $U \subset s \subset U^{\perp}\}$.

The set of the transmitter's encoding rules E_T=$\{e_T | e_T$ is a subspace of type $(2n+2, n, 2), U \subset e_T\}$.

The set of the i-th receiver's decoding rules E_{R_i}=$\{e_{R_i} | e_{R_i}$ is a subspace of type $(n+3, 1, 2)$ which is orthogonal to $\langle e_1, \cdots, e_{i-1}, e_{i+1}, \cdots, e_n\rangle$, $U \subset e_{R_i}\}, (1 \leq i \leq n)$.

The set of messages $M = \{m | m$ is a subspace of type $(2t+k, t, k), U \subset m\}$.

1. Key Distribution. The KDC randomly chooses a subspace $e_T \in E_T$, then privately sends e_T to the sender T. KDC randomly chooses a subspace $e_{R_i} \in E_{R_i}$ and $e_{R_i} \subset e_T$, then privately sends e_{R_i} to the i-th 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 $e_{R_i} \subset m$. R_i can get s from $s = m \cap U^{\perp}$.

Lemma 1 *The above construction of multireceiver 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 $m \in M$, $s = m \cap U^{\perp}$ is the unique source state contained in m and there is $e_T \in E_T$, such that $m = s + e_T$.

Proof: (1) For $s \in S$, $e_T \in E_T$, we can assume that

$$s = \begin{array}{cc} \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & Q_2 & 0 & Q_4 & 0 & 0 & 0 & Q_8 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-2)} & 0 \end{pmatrix} & \begin{matrix} n \\ 2(t-n) \\ 1 \\ 1 \\ k-2 \end{matrix} \\ \begin{matrix} n & \nu-n & n & \nu-n & 1 & 1 & k-2 & l-k \end{matrix} & \end{array},$$

then

$$sK_l\,{}^t s = \begin{array}{cc} \begin{pmatrix} 0 & 0 & 0 \\ 0 & -Q_4\,{}^tQ_2 + Q_2\,{}^tQ_4 & 0 \\ 0 & 0 & 0 \end{pmatrix} & \begin{matrix} n \\ 2(t-n) \\ k \end{matrix} \\ \begin{matrix} n & 2(t-n) & k \end{matrix} & \end{array}.$$

Since $\mathrm{rank}(sK_l\,{}^ts) = 2(t-n)$, $\mathrm{rank}(-Q_4\,{}^tQ_2 + Q_2\,{}^tQ_4) = 2(t-n)$. Then we can assume that

$$e_T = \begin{array}{cc} \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & I^{(n)} & R_4 & 0 & 0 & R_7 & R_8 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} & \begin{matrix} n \\ n \\ 1 \\ 1 \end{matrix} \\ \begin{matrix} n & \nu-n & n & \nu-n & 1 & 1 & k-2 & l-k \end{matrix} & \end{array},$$

and

$$e_T K_l\,{}^te_T = \begin{pmatrix} 0 & I^{(n)} & 0 \\ -I^{(n)} & -R_4\,{}^tR_2 + R_2\,{}^tR_4 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{matrix} n \\ n \\ 2 \end{matrix}$$

$$\sim \begin{array}{cc} \begin{pmatrix} 0 & I^{(n)} & 0 \\ -I^{(n)} & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} & \begin{matrix} n \\ n \\ 2 \end{matrix} \\ \begin{matrix} n & n & 2 \end{matrix} & \end{array}$$

We have

$m = s + e_T =$

$$\begin{array}{cc} \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & Q_2 & 0 & Q_4 & 0 & 0 & 0 & Q_8 \\ 0 & R_2 & I^{(n)} & R_4 & 0 & 0 & 0 & R_8 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-2)} & 0 \end{pmatrix} & \begin{matrix} n \\ 2(t-n) \\ n \\ 1 \\ 1 \\ k-2 \end{matrix} \\ \begin{matrix} n & \nu-n & n & \nu-n & 1 & 1 & k-2 & l-k \end{matrix} & \end{array}.$$

Thus m is a $2t+k$ dimensional subspace, and $mK_l\,{}^tm =$

$$\begin{pmatrix} 0 & 0 & I^{(n)} & 0 \\ 0 & -Q_4\,{}^tQ_2 + Q_2\,{}^tQ_4 & -Q_4\,{}^tR_2 + Q_2\,{}^tR_4 & 0 \\ -I^{(n)} & -R_4\,{}^tQ_2 + R_2\,{}^tQ_4 & -R_4\,{}^tR_2 + R_2\,{}^tR_4 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \sim$$

$$\begin{pmatrix} 0 & 0 & I^{(n)} & 0 \\ 0 & -Q_4\,{}^tQ_2 + Q_2\,{}^tQ_4 & 0 & 0 \\ -I^{(n)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0^{(k)} \end{pmatrix} \begin{matrix} n \\ 2(t-n) \\ n \\ k \end{matrix}$$

where $\mathrm{rank}(-Q_4\,{}^tQ_2 + Q_2\,{}^tQ_4) = 2(t-n)$. Therefore, $\mathrm{rank}(mK_l\,{}^tm) = 2t$, $\dim(m \cap E) = k$. So m is a subspace of type $(2t+k, t, k)$ containing U, i.e., $m \in M$.

(2) For $m \in M$, m is a subspace of type $(2t+k, t, k)$ containing U. So there is a subspace $V \subset m$, satisfying

$$\begin{pmatrix} U \\ V \end{pmatrix} K_l \, {}^t\begin{pmatrix} U \\ V \end{pmatrix} \sim \begin{array}{cc} \begin{pmatrix} 0 & I^{(n)} & 0 \\ -I^{(n)} & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} & \begin{matrix} n \\ n \\ 2 \end{matrix} \\ \begin{matrix} n & n & 2 \end{matrix} & \end{array}.$$

Then we can assume that $m = \begin{pmatrix} U \\ V \\ P \end{pmatrix}$, satisfying

$$\begin{pmatrix} U \\ V \\ P \end{pmatrix} K_l \, {}^t\begin{pmatrix} U \\ V \\ P \end{pmatrix} \sim \begin{pmatrix} 0 & I^{(n)} & 0 & 0 & 0 \\ -I^{(n)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(t-n)} & 0 \\ 0 & 0 & -I^{(t-n)} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0^{(k)} \end{pmatrix}.$$

Let $s = \begin{pmatrix} U \\ P \end{pmatrix}$, since $U \perp U$ and $U \perp P$, we have $s \perp U$. Therefore, s is a subspace of type $(2t-n+k, t-n, k)$ and $U \subset s \subset U^{\perp}$, i.e., $s \in S$ is a source state. For any $v \in V$ and $v \neq 0$, $v \notin s$ is obvious, i.e., $V \cap U^{\perp} = \{0\}$. Therefore, $m \cap U^{\perp} = \begin{pmatrix} U \\ P \end{pmatrix} = s$. Let $e_T = \begin{pmatrix} U \\ V \end{pmatrix}$, then e_T is a transmitter's encoding rule and satisfying $m = s + e_T$.

If s' is another source state contained in m, then $U \subset s' \subset U^{\perp}$. Therefore, $s' \subset m \cap U^{\perp} = s$, while dim$s'$=dim$s$, so s'=s, i.e., s is the unique source state contained in m.

From Lemma 1, we know that such construction of multireceiver authentication codes is well defined and there are n receivers in this system. Next we compute the parameters of the codes.

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

Proof: Since $U \subset s \subset U^{\perp}$, s has the form as follows

$$s = \begin{array}{c} \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & Q_2 & 0 & Q_4 & 0 & 0 & 0 & Q_8 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-2)} & 0 \end{pmatrix} \begin{matrix} n \\ 2(t-n) \\ 1 \\ 1 \\ k-2 \end{matrix} \\ \begin{matrix} n & \nu-n & n & \nu-n & 1 & 1 & k-2 & l-k \end{matrix} \end{array},$$

where (Q_2, Q_4) is a subspace of type $(2(t-n), t-n)$ in the symplectic space $F_q^{2(\nu-n)}$, Q_8 arbitrary. Therefore, the number of the source states is $|S| = q^{2(t-n)(l-k)}N(2(t-n), t-n; 2(\nu-n))N(k-2, l-2)$.

Lemma 3 *The number of the encoding rules of the transmitter is* $|E_T| = q^{n(2\nu-2n+l-2)}$.

Proof: Since e_T is a subspace of type $(2n+2, n, 2)$ containing U, e_T has the form as follows

$$e_T = \begin{array}{c} \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & I^{(n)} & R_4 & 0 & 0 & R_7 & R_8 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} n \\ n \\ 1 \\ 1 \end{matrix} \\ \begin{matrix} n & \nu-n & n & \nu-n & 1 & 1 & k-2 & l-k \end{matrix} \end{array},$$

where R_2, R_4, R_7, R_8 are arbitrary. Therefore, $|E_T| = q^{2(\nu-n)n+(k-2)n+(l-k)n} = q^{n(2\nu-2n+l-2)}$.

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

Proof: Since the i-th receiver's decoding rule e_{R_i} is a subspace of type $(n+3, 1, 2)$ containing U and e_{R_i} is orthogonal to $\langle e_1, \cdots, e_{i-1}, e_{i+1}, \cdots, e_n\rangle$. So we can assume that $e_{R_i} = {}^t(e_1 \cdots e_n\ e_{2\nu+1}\ e_{2\nu+2}\ u)$, where $u = (x_1\ x_2\ \cdots\ x_{2\nu+1}\ x_{2\nu+2}\ \cdots\ x_{2\nu+l})$. Obviously, $x_1 = \cdots = x_n = x_{\nu+1} = \cdots = x_{\nu+i-1} = x_{\nu+i+1} = \cdots = x_{\nu+n} = x_{2\nu+1} = x_{2\nu+2} = 0$, $x_{\nu+i} = 1$, and $x_{n+1}, \cdots, x_\nu, x_{\nu+n+1}, \cdots, x_{2\nu}, x_{2\nu+3}, \cdots, x_{2\nu+l}$ are arbitrary. Therefore, $|E_{R_i}| = q^{2\nu+l-2n-2}$.

Lemma 5 *(1)The number of encoding rules e_T contained in m is $q^{n(2t-2n+k-2)}$;*

(2)The number of the messages is $|M| = q^{2(t-n)(l-k)+n(2\nu-2t+l-k)}N(2(t-n), t-n; 2(\nu-n))N(k-2, l-2)$.

Proof: (1)Let m be a message. From the definition of m, we may take m as follows $m =$

$$\begin{array}{c} \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(t-n)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(n)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I^{(t-n)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(k)} & 0 \end{pmatrix} \begin{matrix} n \\ t-n \\ n \\ t-n \\ k \end{matrix} \\ \begin{matrix} n & t-n & \nu-t & n & t-n & \nu-t & k & l-k \end{matrix} \end{array}.$$

If $e_T \subset m$, then we can assume that $e_T =$

$$\begin{array}{c} \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & 0 & I^{(n)} & R_5 & 0 & 0 & 0 & R_9 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} n \\ n \\ 1 \\ 1 \end{matrix} \\ \begin{matrix} n & t-n & \nu-t & n & t-n & \nu-t & 1 & 1 & k-2 & l-k \end{matrix} \end{array}$$

where R_2, R_5, R_9 are arbitrary. Therefore, the number of e_T contained in m is $q^{n(t-n+t-n+k-2)} = q^{n(2t-2n+k-2)}$.

(2) We know that a message contains only one source state and the number of the transmitter's encoding rules contained in a message is $q^{n(2t-2n+k-1)}$. Therefore we have $|M| = |S||E_T|/q^{n(2t-2n+k-2)} = q^{2(t-n)(l-k)+n(2\nu-2t+l-k)}N(2(t-n), t-n; 2(\nu-n))N(k-2, l-2)$.

Theorem 6 *The parameters of constructed multireceiver authentication codes are*

$|S| = q^{2(t-n)(l-k)}N(2(t-n), t-n; 2(\nu-n))N(k-2, l-2)$;

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

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

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

Assume there are n receivers $R_1, \cdots, R_n$. Let $L = \{i_1, \cdots, i_l\} \subseteq \{1, \cdots, n\}$, $R_L =$

$\{R_{i_1}, \cdots, R_{i_l}\}$ and $E_L = E_{R_{i_1}} \times \cdots \times E_{R_{i_l}}$. We consider the impersonation attack and substitution 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 $1 \leq l \leq n-1$. First, we will prove the following results:

Lemma 7 *For any $e_L = (e_{R_1}, \cdots, e_{R_l}) \in E_L$, the number of e_T containing e_L is $q^{2(n-l)(\nu-n)+(l-2)(n-l)}$.*

Proof: For any $e_L = (e_{R_1}, \cdots, e_{R_l}) \in E_L$, since the transitivity property of singular symplectic group, we can assume that

$$e_L = \begin{array}{c} \left(\begin{array}{ccccccccc} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & I^{(l)} & 0 & R_6 & 0 & 0 & R_9 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right) \begin{array}{c} l \\ n-l \\ l \\ 1 \\ 1 \end{array} \\ \begin{array}{ccccccccc} l & n-l & \nu-n & l & n-l & \nu-n & 1 & 1 & l-2 \end{array} \end{array}.$$

Therefore, e_T containing e_L has the form as follows

$$e_T = \begin{array}{c} \left(\begin{array}{ccccccccc} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & I^{(l)} & 0 & R_6 & 0 & 0 & R_9 \\ 0 & 0 & R_3' & 0 & I^{(n-l)} & R_6' & 0 & 0 & R_9' \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right) \begin{array}{c} l \\ n-l \\ l \\ n-l \\ 1 \\ 1 \end{array} \\ \begin{array}{ccccccccc} l & n-l & \nu-n & l & n-l & \nu-n & 1 & 1 & l-2 \end{array} \end{array},$$

where R_3', R_6', R_9', are arbitrary. Therefore, the number of e_T containing e_L is $q^{2(n-l)(\nu-n)+(l-2)(n-l)}$.

Lemma 8 *For any $m \in M$ and $e_L, e_{R_i} \subset m$,*

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

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

Proof: (1) The matrix of m is the same as that in lemma 5, then for any $e_L \subset m$, assume that

$e_L =$

$$\begin{array}{c} \left(\begin{array}{ccccccccccc} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & I^{(l)} & 0 & R_7 & 0 & 0 & 0 & R_{11} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right) \begin{array}{c} l \\ n-l \\ l \\ 1 \\ 1 \end{array} \\ \begin{array}{ccccccccccc} l & n-l & t-n & \nu-t & l & n-l & t-n & \nu-t & 1 & 1 & l-2 \end{array} \end{array}.$$

If $e_T \subset m$ and $e_T \supset e_L$, then

$e_T =$

$$\begin{array}{c} \left(\begin{array}{ccccccccccc} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & I^{(l)} & 0 & R_7 & 0 & 0 & 0 & R_{11} \\ 0 & 0 & R_3' & 0 & 0 & I^{(n-l)} & R_7' & 0 & 0 & 0 & R_{11}' \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right) \begin{array}{c} l \\ n-l \\ l \\ n-l \\ 1 \\ 1 \end{array} \\ \begin{array}{ccccccccccc} l & n-l & t-n & \nu-t & l & n-l & t-n & \nu-t & 1 & 1 & l-2 \end{array} \end{array}$$

where R_3', R_7', R_{11}' are arbitrary. Therefore, the number of e_T contained in m and containing e_L is $q^{2(t-n)(n-l)+(l-2)(n-l)}$.

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

Lemma 9 *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. Assume that $s_0 = s_1 \cap s_2$, dim $s_0 = k_1$, then $n+2 \leq k_1 \leq 2t-n+k-1$. 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 $q^{(n-l-1)(k_1-n-2)}$.*

Proof: Since $m_1 = s_1 + e_T, m_2 = s_2 + e_T$ and $m_1 \neq m_2, s_1 \neq s_2$. And for any $s \in S, s \supset U, n+2 \leq k_1 \leq 2t-n+k-1$. Assume that s_i' is the complementary subspace of s_0 in the s_i, then $s_i = s_0 + s_i'$ $(i = 1, 2)$. From $m_i = s_i + e_T = s_0 + s_i' + e_T$ and $s_i = m_i \cap U^\perp$, we have $s_0 = \left(m_1 \cap U^\perp\right) \bigcap \left(m_2 \cap U^\perp\right) = m_1 \cap m_2 \cap U^\perp = s_1 \cap m_2 = s_2 \cap m_1$ and $m_1 \cap m_2 = (s_1 + e_T) \cap m_2 = (s_0 + s_1' + e_T) \cap m_2 = ((s_0 + e_T) + s_1') \cap m_2$. Because $s_0 + e_T \subset m_2$, $m_1 \cap m_2 = (s_0 + e_T) + (s_1' \cap m_2)$. While $s_1' \cap m_2 \subseteq s_1 \cap m_2 = s_0$, $m_1 \cap m_2 = s_0 + e_T$.

From the definition of the message, we may take $m_i (i = 1, 2)$ as follows

$m_i =$

$$\begin{array}{c} \left(\begin{array}{ccccccc} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & p_{i_1} & 0 & p_{i_2} & 0 & 0 & 0 \\ 0 & 0 & I^{(n)} & 0 & 0 & 0 & 0 \\ 0 & p_{i_3} & 0 & p_{i_4} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & p_{i_5} \end{array}\right) \begin{array}{c} n \\ t-n \\ n \\ t-n \\ 1 \\ 1 \\ k-2 \end{array} \\ \begin{array}{ccccccc} n & \nu-n & n & \nu-n & 1 & 1 & l-2 \end{array} \end{array}.$$

Let

$$m_1 \cap m_2 = \begin{array}{cc} \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & p_1 & 0 & p_2 & 0 & 0 & 0 \\ 0 & 0 & I^{(n)} & 0 & 0 & 0 & 0 \\ 0 & p_3 & 0 & p_4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & p_5 \end{pmatrix} & \begin{matrix} n \\ t-n \\ n \\ t-n \\ 1 \\ 1 \\ k-2 \end{matrix} \\ \begin{matrix} n & \nu-n & n & \nu-n & 1 & 1 & l-2 \end{matrix} & \end{array},$$

from above we know that $m_1 \cap m_2 = s_0 + e_T$, then dim $(m_1 \cap m_2) = k_1 + n$, therefore,

$$\begin{aligned} &\dim \begin{pmatrix} 0 & P_1 & 0 & P_2 & 0 & 0 & 0 \\ 0 & P_3 & 0 & P_4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & P_5 \end{pmatrix} \\ &= k_1 + n - (2n + 2) \\ &= k_1 - n - 2. \end{aligned}$$

For any $e_L, e_{R_i} \subset m_1 \cap m_2$, we can assume that

$$e_L = \begin{array}{cc} \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & I^{(l)} & 0 & R_6 & 0 & 0 & R_9 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} & \begin{matrix} l \\ n-l \\ l \\ 1 \\ 1 \end{matrix} \\ \begin{matrix} l & n-l & \nu-n & l & n-l & \nu-n & 1 & 1 & l-2 \end{matrix} & \end{array},$$

$$e_{R_i} = \begin{array}{cc} \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3' & 0 & 1 & 0 & R_6' & 0 & 0 & R_9' \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} & \begin{matrix} l \\ n-l \\ l \\ 1 \\ 1 \end{matrix} \\ \begin{matrix} l & n-l & \nu-n & i-1 & 1 & n-i & \nu-n & 1 & 1 & l-2 \end{matrix} & \end{array}.$$

If $e_T \subset m_1 \cap m_2$ and $e_L, e_{R_i} \subset e_T$, then e_T has the form as follows
$e_T =$

$$\begin{array}{cc} \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & I^{(l)} & 0 & 0 & 0 & R_6 & 0 & 0 & R_9 \\ 0 & 0 & C_3 & 0 & I^{(i-l-1)} & 0 & 0 & C_6 & 0 & 0 & C_9 \\ 0 & 0 & R_3' & 0 & 0 & 1 & 0 & R_6' & 0 & 0 & R_9' \\ 0 & 0 & C_3' & 0 & 0 & 0 & I^{(n-i))} & C_6' & 0 & 0 & C_9' \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} & \begin{matrix} l \\ n-l \\ l \\ i-l-1 \\ 1 \\ n-i \\ 1 \\ 1 \end{matrix} \\ \begin{matrix} l & n-l & \nu-n & l & i-l-1 & 1 & n-i & \nu-n & 1 & 1 & l-2 \end{matrix} & \end{array}.$$

So it is easy to know that the number of e_T contained in $m_1 \cap m_2$ and containing e_L, e_{R_i} is $q^{(n-l-1)(k_1-n-2)}$.

Theorem 10 *In the constructed multireceiver authentication codes, the largest probabilities of success for impersonation attack and substitution attack from R_L on a receiver R_i are*

$$\begin{aligned} P_I[i, L] &= \frac{1}{q^{(n-l-1)(2\nu-2t)+2(\nu-n)+(l-2)}}, \\ P_S[i, L] &= \frac{1}{q^{(n-l)(l-k+2)+2t-2n+k-4}}. \end{aligned}$$

respectively, where $i \notin L$.

Proof: Impersonation attack: R_L, after receiving its secret keys, sends a message m to R_i. The attack is successful if m is accepted by R_i as authentic. Therefore

$$\begin{aligned} &P_I[i, L] = \max_{e_L \in E_L} \\ &\left\{ \frac{\max_{m \in M} \mid \{e_T \in E_T | e_T \subset m \text{ and } e_T \supset e_L, e_{R_i}\} \mid}{\mid \{e_T \in E_T | e_T \supset e_L\} \mid} \right\} \\ &= \frac{q^{2(t-n)(n-l-1)+(l-2)(n-l-1)}}{q^{2(n-l)(\nu-n)+2(\nu-n)(n-l)}} \\ &= \frac{1}{q^{(n-l-1)(2\nu-2t)+2(\nu-n)+(l-2)}}. \end{aligned}$$

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

$$\begin{aligned} &P_S[i, L] = \max_{e_L \in E_L} \max_{m \in M} \max_{m' \in M} \\ &\quad \frac{\mid \{e_T \in E_T | e_T \subset m, m' \text{ and } e_T \supset e_L, e_{R_i}\} \mid}{\mid \{e_T \in E_T | e_T \subset m \text{ and } e_T \supset e_L\} \mid} \\ &= \max_{n+2 \le k_1 \le 2t-n+k-2} \frac{q^{(n-l-1)(k_1-n-2)}}{q^{2(t-n)(n-l)+(l-2)(n-l)}} \\ &= \frac{1}{q^{(n-l)(l-k+2)+2t-2n+k-4}}. \end{aligned}$$

3.2 Construction 2

Suppose that F_q is a finite field with q elements and $v_i (1 \le 2i \le 2\nu + l, l \ge 2)$ are the row vectors in $F_q^{(2\nu+l)}$. Let $2 \le 2n < \nu$, $1 < k \le l$,

$$U = \langle v_1, v_2, \cdots, v_{2n}, e_{2\nu+1}, e_{2\nu+2} \rangle,$$

i.e. U is a $(2n+2)$-dimensional subspace of $F_q^{(2\nu+l)}$ generated by $\nu_1, \nu_2, \cdots, \nu_{2n}, e_{2\nu+1}, e_{2\nu+2}$, i.e. U is a subspace of type$(2n+2, 0, 2)$, then $U^{\perp}$ is a subspace of type $(2\nu - n + l, \nu - n, l)$.

The set of source states

$$S = \left\{ s \;\middle|\; \begin{array}{c} s \text{ is a subspace of type} \\ (2\nu - 2n + k, \nu - 2n, k) \\ \text{and } U \subset s \subset U^{\perp} \end{array} \right\}.$$

The set of the transmitter's encoding rules E_T={$e_T|e_T$ is a 2n dimensional subspace and $U+e_T$ is a subspace of type $(4n+2,2n,2)$}.

The set of the i-th receiver's decoding rules E_{R_i}={$e_{R_i}|e_{R_i}$ is a 2 dimensional subspace and $U+e_{R_i}$ is a subspace of type $(2n+4,2,2)$ which is orthogonal to $\langle v_1,\cdots,v_{2i-3},v_{2i+1},\cdots,v_{2n}\rangle$}.

The set of messages M={$m|m$ is a subspace of type $(2\nu+k,\nu,k)$, $U\subset m$ and $m\cap U^{\perp}$=s }.

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

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 $e_{R_i}\subset m$. R_i can get s from $s=m\cap U^{\perp}$.

Lemma 11 *The above construction of Multireceiver 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 $m\in M$, $s=m\cap U^{\perp}$ is the unique 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

$$s=\begin{array}{c}\left(\begin{array}{cccccccc} I^{(2n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & Q_2 & 0 & Q_4 & 0 & 0 & 0 & Q_8\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-2)} & 0\end{array}\right)\begin{array}{c}2n\\ 2\nu-4n\\ 1\\ 1\\ k-2\end{array}\\ \begin{array}{cccccccc}2n & \nu-2n & 2n & \nu-2n & 1 & 1 & k-2 & l-k\end{array}\end{array},$$

then

$$sK_l\,{}^ts=\begin{array}{c}\left(\begin{array}{ccc}0 & 0 & 0\\ 0 & -Q_4\,{}^tQ_2+Q_2\,{}^tQ_4 & 0\\ 0 & 0 & 0\end{array}\right)\begin{array}{c}2n\\ 2(\nu-2n)\\ k\end{array}\\ \begin{array}{ccc}2n & 2(\nu-2n) & k\end{array}\end{array}.$$

Since rank$(sK_l\,{}^ts)=2(\nu-2n)$, rank$(-Q_4\,{}^tQ_2+Q_2\,{}^tQ_4)=2(\nu-2n)$. Then we can assume that

$$e_T=\begin{array}{c}\left(\begin{array}{cccccccc}X_1 & X_2 & I^{(2n)} & X_4 & X_5 & X_6 & X_7 & X_8\end{array}\right)\\ \begin{array}{cccccccc}2n & \nu-2n & 2n & \nu-2n & 1 & 1 & k-2 & l-k\end{array}\end{array},$$

and

$$\begin{pmatrix}U\\ e_T\end{pmatrix}K_l\,{}^t\begin{pmatrix}U\\ e_T\end{pmatrix}\sim\begin{array}{c}\left(\begin{array}{ccc}0 & I^{(2n)} & 0\\ -I^{(2n)} & 0 & 0\\ 0 & 0 & 0\end{array}\right)\begin{array}{c}2n\\ 2n\\ 2\end{array}\\ \begin{array}{ccc}2n & 2n & 2\end{array}\end{array}.$$

We have

$$m=s+e_T=$$

$$\begin{array}{c}\left(\begin{array}{cccccccc} I^{(2n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & Q_2 & 0 & Q_4 & 0 & 0 & 0 & Q_8\\ X_1 & X_2 & I^{(2n)} & X_4 & X_5 & X_6 & X_7 & X_8\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-2)} & 0\end{array}\right)\begin{array}{c}2n\\ 2(\nu-2n)\\ 2n\\ 1\\ 1\\ k-2\end{array}\\ \begin{array}{cccccccc}2n & \nu-2n & 2n & \nu-2n & 1 & 1 & k-2 & l-k\end{array}\end{array}.$$

Thus m is a $2\nu+k$ dimensional subspace, and

$$mK_l\,{}^tm=$$

$$\begin{pmatrix}0 & 0 & I^{(2n)} & 0\\ 0 & -Q_4\,{}^tQ_2+Q_2\,{}^tQ_4-Q_4\,{}^tR_2+Q_2\,{}^tR_4 & & 0\\ -I^{(2n)} & -R_4\,{}^tQ_2+R_2\,{}^tQ_4-R_4\,{}^tR_2+R_2\,{}^tR_4 & & 0\\ 0 & 0 & 0 & 0\end{pmatrix}\sim$$

$$\left(\begin{array}{cccc}0 & 0 & I^{(2n)} & 0\\ 0 & -Q_4\,{}^tQ_2+Q_2\,{}^tQ_4 & 0 & 0\\ -I^{(2n)} & 0 & 0 & 0\\ 0 & 0 & 0 & 0^{(k)}\end{array}\right)\begin{array}{c}2n\\ 2(\nu-2n)\\ 2n\\ k\end{array}$$

where rank$(-Q_4\,{}^tQ_2+Q_2\,{}^tQ_4)=2(\nu-2n)$. Therefore, rank$(mK_l\,{}^tm)=2\nu$, dim$(m\cap E)=k$. From above, m is a subspace of type $(2\nu+k,\nu,k)$ containing U, i.e., $m\in M$.

(2) For $m\in M$, m is a subspace of type $(2\nu+k,\nu,k)$ containing U. So there is subspace $V\subset m$, satisfying

$$\begin{pmatrix}U\\ V\end{pmatrix}K_l\,{}^t\begin{pmatrix}U\\ V\end{pmatrix}\sim\begin{array}{c}\left(\begin{array}{ccc}0 & 0 & I^{(2n)}\\ 0 & 0 & 0\\ -I^{(2n)} & 0 & 0\end{array}\right)\begin{array}{c}2n\\ 2\\ 2n\end{array}\\ \begin{array}{ccc}2n & 2 & 2n\end{array}\end{array}$$

then we can assume that $m=\begin{pmatrix}U\\ V\\ P\end{pmatrix}$, satisfying

$$\begin{pmatrix}U\\ V\\ P\end{pmatrix}K_l\,{}^t\begin{pmatrix}U\\ V\\ P\end{pmatrix}\sim\begin{pmatrix}0 & 0 & I^{(2n)} & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0\\ -I^{(2n)} & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & I^{(\nu-2n)} & 0\\ 0 & 0 & 0 & -I^{(\nu-2n)} & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0^{(k-2)}\end{pmatrix}.$$

Let $s=\begin{pmatrix}U\\ P\end{pmatrix}$, since $U\perp U$ and $U\perp P$, we have $s\perp U$. Therefore, s is a subspace of type $(2\nu-2n+k,t-n,k)$ and $U\subset s\subset U^{\perp}$, i.e., $s\in S$ is a source state. For any $v\in V$ and $v\neq 0$, $v\notin s$ is obvious, i.e.,

$V \cap U^{\perp} = \emptyset$. Therefore, $m \cap U^{\perp} = \begin{pmatrix} U \\ P \end{pmatrix} = s$. Let $e_T = \begin{pmatrix} U \\ V \end{pmatrix}$, then e_T is a transmitter's encoding rule and satisfying $m = s + e_T$.

If s' is another source state contained in m, then $U \subset s' \subset U^{\perp}$. Therefore, $s' \subset m \cap U^{\perp} = s$, while dim$s'$=dim$s$, so s'=s, i.e., s is the unique source state contained in m.

From Lemma11, we know that such construction of multireceiver authentication codes is well defined and there are n receivers in this system. Next we compute the parameters of this codes.

Lemma 12 *The number of the source states is* $| S |= q^{2(\nu-2n)(l-k)} N(2(\nu-2n), \nu-2n; 2(\nu-2n)) N(k-2, l-2)$.

Proof: Since $U \subset s \subset U^{\perp}$, s has the form as follows

$$s = \begin{array}{c} \begin{pmatrix} I^{(2n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & Q_2 & 0 & Q_4 & 0 & 0 & 0 & Q_8 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-2)} & 0 \end{pmatrix} \begin{array}{l} 2n \\ 2\nu-4n \\ 1 \\ 1 \\ k-2 \end{array} \\ \begin{array}{cccccccc} 2n & \nu-2n & 2n & \nu-2n & 1 & 1 & k-2 & l-k \end{array} \end{array},$$

where (Q_2, Q_4) is a subspace of type $(2(\nu-2n), \nu-2n)$ in the symplectic space $F_q^{(2(\nu-2n))}$, Q_8 arbitrary. Therefore, the number of the source states is$| S |= q^{2(\nu-2n)(l-k)} N(2(\nu-2n), \nu-2n; 2(\nu-2n)) N(k-2, l-2)$.

Lemma 13 *The number of the encoding rules of the transmitter is* $|E_T| = q^{2n(2\nu-2n+l)}$.

Proof: Since $U + e_T$ is a subspace of type $(4n+2, 2n, 2)$, then we can suppose that

$$e_T = \begin{array}{c} \begin{pmatrix} X_1 & X_2 & I^{(2n)} & X_4 & X_5 & X_6 & X_7 & X_8 \end{pmatrix} \\ \begin{array}{cccccccc} 2n & \nu-2n & 2n & \nu-2n & 1 & 1 & k-2 & l-k \end{array} \end{array},$$

where $X_1, X_2, X_4, X_5, X_6, X_7, X_8$ is arbitrary. Therefore the number of e_T is $q^{2n(2\nu-2n+l)}$.

Lemma 14 *The number of the decoding rules of the i-th receiver is* $|E_{R_i}| = q^{2(2\nu-2n+l)}$.

Proof: Since the i-th receiver's decoding rule $U+e_{R_i}$ is a subspace of type $(2n+4, 2, 2)$ which is orthogonal to $\langle v_1, \cdots, v_{2i-2}, v_{2i+1}, \cdots, v_{2n}\rangle$ and by the transitivity property of singular symplectic group, we can assume that $e_{R_i} =$

$$\begin{array}{c} \begin{pmatrix} X_1 & X_2 & 0 & I^{(2)} & 0 & X_6 & X_7 & X_8 & X_9 & X_{10} \end{pmatrix} \\ \begin{array}{cccccccccc} 2n & \nu-2n & 2(i-1) & 2 & 2(n-i) & \nu-2n & 1 & 1 & k-2 & l-k \end{array} \end{array},$$

where $X_1, X_2, X_6, X_7, X_8, X_9, X_{10}$ are arbitrary. Therefore the number of $|E_{R_i}|$ is $q^{2(2\nu-2n+l)}$.

Lemma 15 *(1)The number of encoding rules e_T contained in m is $q^{2n(2\nu-2n+k)}$;*

(2)The number of the messages is $|M| = q^{2(\nu-n)(l-k)} N(2(\nu-2n), \nu-2n; 2(\nu-2n)) N(k-2, l-2)$.

Proof: (1) Let m be a message, since $U \subset m$ and from the definition of m, we may take m as follows

$$m = \begin{array}{c} \begin{pmatrix} I^{(2n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(\nu-2n)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(2n)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(\nu-2n)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-2)} & 0 \end{pmatrix} \\ \begin{array}{cccccccc} 2n & \nu-2n & 2n & \nu-2n & 1 & 1 & k-2 & l-k \end{array} \end{array},$$

if $e_T \subset m$, then we can assume that

$$e_T = \begin{array}{c} \begin{pmatrix} R_1 & R_2 & I^{(2n)} & R_4 & R_5 & R_6 & R_7 & 0 \end{pmatrix} \\ \begin{array}{cccccccc} 2n & \nu-2n & 2n & \nu-2n & 1 & 1 & k-2 & l-k \end{array} \end{array}$$

where $R_1, R_2, R_4, R_5, R_6, R_7$ are arbitrary. Therefore, the number of e_T contained in m is $q^{2n(2\nu-2n+k)}$.

(2) We know that a message contains only one source state and the number of the transmitter's encoding rules contained in a message is $q^{2n(2\nu-2n+k)}$. Therefore we have $|M| = |S||E_T|/q^{2n(2\nu-2n+k)} = q^{2(\nu-n)(l-k)} N(2(\nu-2n), \nu-2n; 2(\nu-2n)) N(k-2, l-2)$.

Theorem 16 *The parameters of constructed multireceiver authentication codes are*

$|S| = q^{2(\nu-2n)(l-k)} N(2(\nu-2n), \nu-2n; 2(\nu-2n)) N(k-2, l-2)$.

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

$|E_{R_i}| = q^{2(2\nu-2n+l)}$;

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

Assume that there are n receivers $R_1, \cdots, R_n$. Let $L = \{i_1, \cdots, i_l\} \subseteq \{1, \cdots, n\}, R_L = \{R_{i_1}, \cdots, R_{i_l}\}$ and $E_L = E_{R_{i_1}} \times \cdots \times E_{R_{i_l}}$. We consider the impersonation attack and substitution 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 $1 \le l \le n-1$. First, we will prove the following results:

Lemma 17 *For any $e_L = (e_{R_1}, \cdots, e_{R_l}) \in E_L$, the number of e_T containing e_L is $q^{(2n-2l)(2\nu-2n+l)}$.*

Proof: For any $e_L = (e_{R_1}, \cdots, e_{R_l}) \in E_L$, we can assume that

$$e_L = \begin{array}{c} \begin{pmatrix} R_1 & R_2 & I^{(2l)} & 0 & R_5 & R_6 & R_7 & R_8 & R_9 \end{pmatrix} \\ \begin{matrix} 2n & \nu-2n & 2l & 2n-2l & \nu-2n & 1 & 1 & k-2 & l-k \end{matrix} \end{array}.$$

Therefore, e_T containing e_L has the form as follows

$$e_T = \begin{array}{c} \begin{pmatrix} R_1 & R_2 & I^{(2l)} & 0 & R_5 & R_6 & R_7 & R_8 & R_9 \\ R_1' & R_2' & 0 & I^{(2n-2l)} & R_5' & R_6' & R_7' & R_8' & R_9' \end{pmatrix} \\ \begin{matrix} 2n & \nu-2n & 2l & 2n-2l & \nu-2n & 1 & 1 & k-2 & l-k \end{matrix} \end{array},$$

where $R_1', R_2', R_5', R_6', R_7', R_8', R_9'$ are arbitrary. Therefore, the number of e_T containing e_L is $q^{(2n-2l)(2\nu-2n+l)}$.

Lemma 18 *For any $m \in M$ and $e_L, e_{R_i} \subset m$,*

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

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

Proof: (1) The matrix of m is the same as that in lemma 15, then for any $e_L \subset m$, assume that

$$e_L = \begin{array}{c} \begin{pmatrix} R_1 & R_2 & I^{(2l)} & 0 & R_5 & R_6 & R_7 & R_8 & 0 \end{pmatrix} \\ \begin{matrix} 2n & \nu-2n & 2l & 2n-2l & \nu-2n & 1 & 1 & k-2 & l-k \end{matrix} \end{array}.$$

If $e_T \subset m$ and $e_T \supset e_L$, then

$$e_T = \begin{array}{c} \begin{pmatrix} R_1 & R_2 & I^{(2l)} & 0 & R_5 & R_6 & R_7 & R_8 & 0 \\ R_1' & R_2' & 0 & I^{(2n-2l)} & R_5' & R_6' & R_7' & R_8' & 0 \end{pmatrix} \\ \begin{matrix} 2n & \nu-2n & 2l & 2n-2l & \nu-2n & 1 & 1 & k-2 & l-k \end{matrix} \end{array},$$

where $R_1', R_2', R_5', R_6', R_7', R_8'$ are arbitrary. Therefore, the number of e_T contained in m and containing e_L is $q^{(2n-2l)(2\nu-2n+k)}$.

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

Lemma 19 *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. Assume that $s_0 = s_1 \cap s_2$, $\dim s_0 = k_1$, then $2n+2 \leq k_1 \leq 2\nu - 2n + k - 1$. 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 $q^{2(n-l-1)(k_1-2n-2)}$.*

Proof: Since $m_1 = s_1 + e_T, m_2 = s_2 + e_T$ and $m_1 \neq m_2$, $s_1 \neq s_2$, for any $s \in S, s \supset U$, $2n+2 \leq k_1 \leq 2\nu - 2n + k - 1$. Assume that s_i' is the complementary subspace of s_0 in the s_i, then $s_i = s_0 + s_i'$ $(i = 1, 2)$. From $m_i = s_i + e_T = s_0 + s_i' + e_T$ and $s_i = m_i \cap U^\perp$, we have $s_0 = (m_1 \cap U^\perp) \bigcap (m_2 \cap U^\perp) = m_1 \cap m_2 \cap U^\perp = s_1 \cap m_2 = s_2 \cap m_1$ and $m_1 \cap m_2 = (s_1 + e_T) \cap m_2 = (s_0 + s_1' + e_T) \cap m_2 = ((s_0 + e_T) + s_1') \cap m_2$. Because $s_0 + e_T \subset m_2$, $m_1 \cap m_2 = (s_0 + e_T) + (s_1' \cap m_2)$. While $s_1' \cap m_2 \subseteq s_1 \cap m_2 = s_0$, $m_1 \cap m_2 = s_0 + e_T$.

From the definition of the message, we may take $m_i (i = 1, 2)$ as follows $m_i =$

$$\begin{array}{cc} \begin{pmatrix} I^{(2n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & h_{i_2} & 0 & h_{i_4} & 0 & 0 & h_{i_7} & 0 \\ X_1 & X_2 & I^{(2n)} & X_4 & X_5 & X_6 & X_7 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & h_{i_7}' & 0 \end{pmatrix} & \begin{matrix} 2n \\ 2(\nu-2n) \\ 2n \\ 1 \\ 1 \\ k-2 \end{matrix} \\ \begin{matrix} 2n & \nu-2n & 2n & \nu-2n & 1 & 1 & k-2 & l-k \end{matrix} & \end{array}.$$

Let $m_1 \cap m_2 =$

$$\begin{array}{cc} \begin{pmatrix} I^{(2n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & Q_2 & 0 & Q_4 & 0 & 0 & Q_7 & 0 \\ X_1 & X_2 & I^{(2n)} & X_4 & X_5 & X_6 & X_7 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & Q_7' & 0 \end{pmatrix} & \begin{matrix} 2n \\ 2(\nu-2n) \\ 2n \\ 1 \\ 1 \\ k-2 \end{matrix} \\ \begin{matrix} 2n & \nu-2n & 2n & \nu-2n & 1 & 1 & k-2 & l-k \end{matrix} & \end{array},$$

from above we know that $m_1 \cap m_2 = s_0 + e_T$, then dim $(m_1 \cap m_2) = k_1 + 2n$, therefore,

$$dim = \begin{pmatrix} 0 & Q_2 & 0 & Q_4 & 0 & 0 & Q_7 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & Q_7' & 0 \end{pmatrix}$$

$= k_1 - 2n - 2$.

For any $e_L, e_{R_i} \subset m_1 \cap m_2$, we can assume that $e_L =$

$$\begin{array}{c} \begin{pmatrix} R_1 & R_2 & I^{(2l)} & 0 & 0 & 0 & R_7 & R_8 & R_9 & R_{10} & 0 \end{pmatrix} \\ \begin{matrix} 2n & \nu-2n & 2l & 2(i-1-l) & 2 & 2(n-i) & \nu-2n & 1 & 1 & k-2 & l-k \end{matrix} \end{array},$$

and

$e_{R_i} =$

$$\begin{array}{c} \begin{pmatrix} X_1 & X_2 & 0 & 0 & I^{(2)} & 0 & X_7 & X_8 & X_9 & X_{10} & 0 \end{pmatrix} \\ \begin{matrix} 2n & \nu-2n & 2l & 2(i-1-l) & 2 & 2(n-i) & \nu-2n & 1 & 1 & k-2 & l-k \end{matrix} \end{array}.$$

If $e_T \subset m_1 \cap m_2$ and $e_L, e_{R_i} \subset e_T$, then e_T has the form as follows e_T=

$$\begin{array}{c} \begin{pmatrix} R_1 & R_2 & I^{(2l)} & 0 & 0 & 0 & R_7 & R_8 & R_9 & R_{10} & 0 \\ H_1 & H_2 & 0 & I^{(2(i-l-1))} & 0 & 0 & H_7 & H_8 & H_9 & H_{10} & 0 \\ X_1 & X_2 & 0 & 0 & I^{(2)} & 0 & X_7 & X_8 & X_9 & X_{10} & 0 \\ N_1 & N_2 & 0 & 0 & 0 & I^{(2(n-i))} & N_7 & N_8 & N_9 & N_{10} & 0 \end{pmatrix} \\ \begin{matrix} 2n & \nu-2n & 2l & 2(i-1-l) & 2 & 2(n-i) & \nu-2n & 1 & 1 & k-2 & l-k \end{matrix} \end{array}$$

So it is easy to know that the number of e_T contained in $m_1 \cap m_2$ and containing e_L, e_{R_i} is $q^{2(n-l-1)(k_1-2n-2)}$.

Theorem 20 *In the constructed multireceiver authentication codes, the largest probabilities of success for impersonation attack and substitution attack from R_L on a receiver R_i are,respectively,*

$$P_I[i,L] = \frac{1}{q^{2(n-l)(l-k)+2(2\nu-2n+k)}},$$
$$P_S[i,L] = \frac{1}{q^{2(n-l)(2n+3)+2(2\nu-4n+k-3)}}.$$

where $i \notin L$.

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

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

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

$$\begin{aligned} P_S[i,L] &= \max_{e_L \in E_L} \max_{m \in M} \max_{m' \in M} \\ &\frac{\mid \{e_T \in E_T | e_T \subset m, m' \text{ and } e_T \supset e_L, e_{R_i}\} \mid}{\mid \{e_T \in E_T | e_T \subset m \text{ and } e_T \supset e_L\} \mid} \\ &= \max_{2n+2 \le k_1 \le 2\nu-2n+k-1} \frac{q^{2(n-l-1)(k_1-2n-2)}}{q^{(2n-2l)(2\nu-2n+k)}} \\ &= \frac{1}{q^{2(n-l)(2n+3)+2(2\nu-4n+k-3)}}. \end{aligned}$$

Acknowledgements: The research was supported by the NNSF of China(61179026) and The Research Funds For The Central University (ZXH2010C008).

References:

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

[2] G. J. Simmons, Authentication thery/coding theory, *Lecture Notes in Comput.Vol.* 196, pp. 411–431.

[3] R. Safavi-Naini, H. Wang, Multi-receiver Authentication Codes: Models, Bounds, Constructions and Extensions, *Information and Computation*, 1999, pp. 148–172.

[4] Y. Gao, Z. J. Zou, Some Constructions of Cartesian Authentication Codes from Pseudo-Sympletic Geometry, *Nortneast. Math. J,* Vol.11, 1995, No.1, pp. 47-55.

[5] S. D. Chen, D. W. Zhao, New Construction of Authentication Codes with Arbitration from Pseudo-Sympletic Geometry over Finite Fields, *Ars Combinatoria*, 2010, 97A, pp. 453-465.

[6] R. Safavi-Naini, H. Wang, New Results on Multirecerver Authentication Codes, *Theoretical Computer Science,* 2001,269(1/2), pp. 1-21.

[7] W. P. Ma, X. M. Wang, A Few New Structure Methods of Multi-sender Authentication Codes, *Electronics College Journal*, Vol.28, 2000, No.4, pp. 117-119

[8] Z. X. Wan, *Geometry of Classical Groups over Finite Fields*, (Second Edition), Beijing/New York: Science Press, 2002.