# Two New Constructions of Multi-receiver Authentication Codes from Singular Pseudo- Symplectic Geometry over Finite Fields

GAO YOU
Civil Aviation University of China
College of Science
Jinbei Road 2898, 300300, Tianjin
CHINA
gao_you@263.net

CHANG LIWEI
Civil Aviation University of China
College of Science
Jinbei Road 2898, 300300, Tianjin
CHINA
changliwei002@163.com

*Abstract:* In this paper, two new constructions of multi-receiver authentication codes using singular pseudo-symplectic geometry on finite fields are described. Under the assumption that the encoding rules of the transmitter and the receiver are chosen according to a uniform probability distribution, the parameters and the probabilities of success for different types of deceptions are computed by the method of matrix and combinatorial enumeration.

*Key–Words:* Multi-receiver authentication codes, Singular pseudo-symplectic geometry, Finite fields, Construction, Combinatorial enumeration.

## 1 Introduction

Based on Simmons' model of unconditionally secure authentication, Desmedt, Frankel and Yung (DFY)[1] introduced an extended authentication model, here referred to as Multi-receiver authentication model, or simply the MRA-model. In the model, protection is provided against deceptions from both an opponent and an insider (transmitter and receiver). In the MRA-model, multi-receiver authentication codes allow a sender to construct an authenticated 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:

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.

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

Denote by $X_1 \times \cdots \times X_n$ the direct product of sets $X_1, \cdots, X_n$ 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 multi-receiver authentication code (MRA-code) 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 $1 \leq i \leq n$, 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 $L = \{i_1, \cdots, i_l\} \subseteq \{1, \cdots, n\}, R_L = \{R_{i_1}, \cdots, R_{i_l}\}$ 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 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

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

where $i \notin L$.

*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 $i \notin L$.

## 2 Preliminaries

Assume that $\mathbb{F}_q$ is a finite field of characteristic 2. Now let us introduce the singular pseudo-symplectic group. Let

$$S_{\delta,l} = \begin{pmatrix} S_\delta & \\ & 0^{(l)} \end{pmatrix}$$

where $S_\delta(\delta = 1 \; or \; 2)$ is the $(2\nu+\delta)\times(2\nu+\delta)$ non-alternate symmetric matrix:

$$S_1 = \begin{pmatrix} 0 & I^{(\nu)} & \\ I^{(\nu)} & 0 & \\ & & 1 \end{pmatrix}$$

or

$$S_2 = \begin{pmatrix} 0 & I^{(\nu)} & & \\ I^{(\nu)} & 0 & & \\ & & 0 & 1 \\ & & 1 & 1 \end{pmatrix}$$

The set of all $(2\nu+\delta+l)\times(2\nu+\delta+l)$ nonsingular matrices T satisfying

$$TS_{\sigma,l}{}^tT = S_{\sigma,l}$$

forms a group with respect to matrix multiplication, called the singular pseudo-symplectic group of degree $2\nu+\delta+l$ and rank $2\nu+\sigma$ over $\mathbb{F}_q$ and denoted by $P_{S_{2\nu+\delta+l,2\nu+\delta}}(\mathbb{F}_q)$.

Let $\mathbb{F}_q^{(2\nu+\delta+l)}$ be the $(2\nu+\delta+l)$-dimensional row vector space over $\mathbb{F}_q$, the singular pseudo-symplectic group $P_{S_{2\nu+\delta+l,2\nu+\delta}}(\mathbb{F}_q)$ has an action on the vector space $\mathbb{F}_q^{(2\nu+\delta+l)}$ defined as follows:

$$\mathbb{F}_q^{(2\nu+\delta+l)} \times P_{S_{2\nu+\delta+l,2\nu+\delta}}(\mathbb{F}_q) \longrightarrow \mathbb{F}_q^{(2\nu+\delta+l)}$$

$$((x_1,x_2\cdots,x_{2\nu+\delta+l}),T) \longmapsto (x_1,x_2\cdots,x_{2\nu+\delta+l})T$$

The vector space $\mathbb{F}_q^{(2\nu+\delta+l)}$ together with this action of the group $P_{S_{2\nu+\delta+l,2\nu+\delta}}(\mathbb{F}_q)$ is called the singular pseudo-symplectic space of dimension $(2\nu+\delta+l)$ over $\mathbb{F}_q$. An $m$ -dimensional subspace $P$ of $\mathbb{F}_q^{(2\nu+\delta+l)}$ is said to be of type $(m, 2s+\tau, s, \varepsilon)$, where $\tau = 0, 1$ or 2 and $\varepsilon = 0$ or 1, if $PS_{\delta,l}P^T$ is cogredient to $M(m, 2s+\tau, s)$ and $P$ does not or does contain a vector of the form

$$\begin{cases} (\underbrace{0,0\cdots 0}_{2\nu},1,x_{2\nu+2}\cdots,x_{2\nu+1+l}), & \text{where } \delta=1 \\ (\underbrace{0,0\cdots 0}_{2\nu},1,0,x_{2\nu+3}\cdots,x_{2\nu+2+l}), & \text{where } \delta=2 \end{cases}$$

corresponding to the cases $\varepsilon = 0$ or 1, respectively. Denote the set of subspaces of type $(m, 2s+\tau, s, \varepsilon)$ in $\mathbb{F}_q^{(2\nu+\delta+l)}$ by $\mathcal{M}(m,\ 2s+\tau,\ s,\ \varepsilon;\ 2\nu+\delta+l,\ 2\nu+\delta)$ and let

$$N(m,\ 2s+\tau,\ s,\ \varepsilon;\ 2\nu+\delta+l,\ 2\nu+\delta)$$

$$= \mathcal{M}(m,\ 2s+\tau,\ s,\ \varepsilon;\ 2\nu+\delta+l,\ 2\nu+\delta).$$

Let $E$ be the subspace of $\mathbb{F}_q^{(2\nu+\delta+l)}$ generated by $e_{2\nu+\delta+1},\cdots,e_{2\nu+\delta+l}$. Then $dimE = l$. An $m$-dimensional subspace $P$ of $\mathbb{F}_q^{(2\nu+\delta+l)}$ is called a subspace of type $(m, 2s+\tau, s, \varepsilon, k)$, if

(i) $P$ is a subspace of type $(m, 2s+\tau, s, \varepsilon)$, and

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

Denote by $\mathcal{M}(m,\ 2s+\tau,\ s,\ \varepsilon,\ k;\ 2\nu+\delta+l,\ 2\nu+\delta)$ the set of subspaces of type $(m,\ 2s+\tau,\ s,\ \varepsilon,\ k)$ in $\mathbb{F}_q^{(2\nu+\delta+l)}$ and let

$$N(m,\ 2s+\tau,\ s,\ \varepsilon,\ k;\ 2\nu+\delta+l,\ 2\nu+\delta)$$

$$= |\mathcal{M}(m,\ 2s+\tau,\ s,\ \varepsilon,\ k;\ 2\nu+\delta+l,\ 2\nu+\delta)|.$$

From [2] we know that the set of all subspaces of type $(m, 2s+\tau, s, \varepsilon, k)$ in $\mathbb{F}_q^{(2\nu+\delta+l)}$ forms an orbit under $P_{S_{2\upsilon+\delta+l,2\nu+\delta}}(\mathbb{F}_q)$. Let $P$ is a subspace of $F_q^{(2\nu+\delta+l)}$, we define the dual subspace of $P$ is

$$P^\perp = \{x|x\in\mathbb{F}_q^{(2\nu+\delta+l)}, xS_{\delta,l}y^\top = 0, \forall y\in P\}.$$

In [3], Gao You, Shi Xinhua and Wang Hongli described one Construction of Authentication codes with Arbitration from singular Symplectic Geometry over Finite Fields. In [4], Desmedt, Frankel and Yung gave two constructions for MRA-codes: one is based on polynomials and the other based on finite geometries. There are other constructions of multireceiver authentication codes are given in [5]–[8]. It is well known that the construction of authentication codes is combinational design in its nature and the geometry of classical groups over finite fields, including symplectic geometry, pseudo-symplectic geometry, unitary geometry and orthogonal geometry can provide a better combination of structure and easy to count. In [9], Chen and Zhao constructed two multi-receiver authentication codes from Symplectic geometry over finite fields. In this paper we construct two new multi-receiver authentication codes from Singular Pseudo-Symplectic geometry over finite fields. The parameters and the probabilities of deceptions of the codes are also computed.

## 3 Construction

### 3.1 Construction I

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

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 $i$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 multi-receiver 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 any $s \in S$, $e_T \in E_T$, from the definition of $s$ and $e_T$, we can assume that

$$s = \begin{pmatrix} U \\ Q \end{pmatrix} \begin{matrix} n+1 \\ r+k-n-1 \end{matrix} \text{ and } e_T = \begin{pmatrix} U \\ V \end{pmatrix} \begin{matrix} n+1 \\ n \end{matrix},$$

then

$$\begin{pmatrix} U \\ Q \end{pmatrix} S_{2,l} {}^t\begin{pmatrix} U \\ Q \end{pmatrix} = \begin{pmatrix} 0^{(n)} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0^{(r-n+k-1)} \end{pmatrix}$$

and

$$\begin{pmatrix} U \\ V \end{pmatrix} S_{2,l} {}^t\begin{pmatrix} U \\ V \end{pmatrix} = \begin{pmatrix} 0 & 0 & I^{(n)} \\ 0 & 0 & 0 \\ I^{(n)} & 0 & 0 \end{pmatrix}.$$

Obviously

$$m = s + e_T = \begin{pmatrix} U \\ V \\ Q \end{pmatrix},$$

and

$$\begin{pmatrix} U \\ V \\ Q \end{pmatrix} S_{2,l} {}^t\begin{pmatrix} U \\ V \\ Q \end{pmatrix} = \begin{pmatrix} 0 & I^{(n)} & 0 \\ I^{(n)} & 0 & 0 \\ 0 & 0 & 0^{(r-n+k)} \end{pmatrix}.$$

From above, $m$ is a subspace of type $(r+n+k, 2n, n, 0, k)$ and $U \subset m$, i.e., $m \in M$.

(2) If $\forall m \in M$, let $s = m \cap U^{\perp}$, then $s$ is a subspace of type $(r+k, 0, 0, 0, k)$ , $U \subset m$ and $U \subset U^{\perp}$, i.e., $s \in S$ is a source state. Now let

$$s = \begin{pmatrix} U \\ Q \end{pmatrix} \begin{matrix} n+1 \\ r+k-n-1 \end{matrix}$$

then

$$s S_{2,l} {}^t s = \begin{pmatrix} 0^{(n)} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0^{(r-n+k-1)} \end{pmatrix}$$

Since $m \neq U^{\perp}$, therefore, there exist $V \in m \setminus U^{\perp}$ such that $m = s \oplus V$ and

$$\begin{pmatrix} U \\ V \\ Q \end{pmatrix} S_{2,l} \begin{pmatrix} U \\ V \\ Q \end{pmatrix}^T \sim \begin{pmatrix} 0 & I^{(n)} & 0 \\ I^{(n)} & 0 & 0 \\ 0 & 0 & 0^{(r-n+k)} \end{pmatrix}.$$

Let $e_T = U \oplus V$. Form above we deduce that $e_T$ is a subspace of type $(2n+1, 2n, n, 0, 1)$ and $e_T \cap U^{\perp} = U$. Therefore $e_T$ is an encoding rule of the transmitter and satisfying $s + e_T = m$.

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 uniquely source state contained in $m$.

From Lemma 1, we find this construction of multi-receiver authentication codes is reasonable. Next the parameters of this codes are computed. $\Box$

**Lemma 2** *The number of the source states is* $|S| = N(r-n,0,0,0;2\nu-2n+2)N(k-1,l-1)q^{(r-n)(l-k)}$.

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

$$s = \begin{array}{c} \left(\begin{array}{ccccccccc} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & Q_2 & 0 & Q_4 & Q_5 & Q_6 & 0 & 0 & Q_9 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \end{array}\right) \begin{array}{c} n \\ r-n \\ 1 \\ k-1 \end{array} \\ \begin{array}{ccccccccc} n & \nu-n & n & \nu-n & 1 & 1 & 1 & k-1 & l-k \end{array} \end{array},$$

where $(Q_2, Q_4, Q_5, Q_6)$ is a subspace of type $(r-n,0,0,0;2\nu-2n+2)$ in the pseudo-symplectic space $F_q^{(2(\nu-n)+2)}$. Therefore, the number of the source states is $|S| = N(r-n,0,0,0;2\nu-2n+2)N(k-1,l-1)q^{(r-n)(l-k)}$. $\Box$

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

**Proof:** Since $e_T$ is a subspace of type $(2n+1,n,0,0,1)$ containing $U$, then we can suppose that

$$e_T = \begin{array}{c} \left(\begin{array}{cccccccc} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & I^{(n)} & R_4 & R_5 & 0 & 0 & R_8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right) \begin{array}{c} n \\ n \\ 1 \end{array} \\ \begin{array}{cccccccc} n & \nu-n & n & \nu-n & 1 & 1 & 1 & l-1 \end{array} \end{array},$$

where $R_2, R_4, R_5, R_8$ is arbitrary. Therefore the number of $|e_T|$ containing $U$ is $q^{n(2\nu-2n+l)}$. $\Box$

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

**Proof:** Since the $i$th receiver's decoding rules $e_{R_i}$ is a subspace of type $(n+2,2,1,0,1)$ containing $U$ and $e_{R_i}$ is orthogonal to $\langle v_1, \cdots, v_{i-1}, v_{i+1}, \cdots, v_n\rangle$ and the transitivity properties of singular pseudo-symplectic group. So we can let $U = \langle e_1, e_2, \cdots, e_n, e_{2\nu+3}\rangle$, then $e_{R_i} = {}^t(e_1, \cdots, e_n, e_{2\nu+3}, u)$, where $u = (x_1\ x_2\ \cdots\ x_{2\nu}\ \cdots\ x_{2\nu+2+l})$. Obviously, $x_1 = \cdots = x_n = x_{\nu+1} = \cdots = x_{\nu+i-1} = x_{\nu+i+1} = \cdots = x_{\nu+n} = x_{2\nu+2} = x_{2\nu+3} = 0$, $x_{\nu+i} = 1$, and $x_{n+1}, \cdots, x_\nu, x_{\nu+n+1}, \cdots, x_{2\nu}, x_{2\nu+1}, \cdots, x_{2\nu+2+l}$ arbitrarily. Therefore, $|E_{R_i}| = q^{2(\nu-n)+l}$. $\Box$

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

*(2)The number of the messages is* $|M| = |S||E_T|/q^{n(r-n+k-1)}$.

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

$$m = \begin{array}{c} \left(\begin{array}{ccccccccccc} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \end{array}\right) \\ \begin{array}{ccccccccccc} n & r-n & \nu-r & n & r-n & \nu-r & 1 & 1 & 1 & k-1 & l-k \end{array} \end{array},$$

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

$$e_T = \begin{array}{c} \left(\begin{array}{ccccccccccc} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & 0 & I^{(n)} & 0 & 0 & 0 & 0 & 0 & R_{10} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{array}\right) \begin{array}{c} n \\ n \\ 1 \end{array} \\ \begin{array}{ccccccccccc} n & r-n & \nu-r & n & r-n & \nu-r & 1 & 1 & 1 & k-1 & l-k \end{array} \end{array},$$

where $R_2, R_{10}$ arbitrarily. Therefore, the number of $e_T$ contained in $m$ is $q^{n(r-n+k-1)}$.

(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 $q^{n(r-n+k-1)}$. Therefore we have $|M| = |S||E_T|/q^{n(r-n+k-1)}$. $\Box$

**Theorem 6** *The parameters of constructed multi-receiver authentication codes are*

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

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

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

$|M| = |S||E_T|/q^{n(r-n+k-1)}$.

Suppose 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 derive 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* $q^{(n-l)(2(\nu-n)+l)}$.

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

$$e_L = \begin{array}{c} \left(\begin{array}{cccccccccc} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & I^{(l)} & 0 & R_6 & R_7 & 0 & 0 & R_{10} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right) \\ \begin{array}{cccccccccc} l & n-l & \nu-n & l & n-l & \nu-n & 1 & 1 & 1 & l-1 \end{array} \end{array}.$$

Therefore, $e_T$ containing $e_L$ has the form as follows

$$e_T = \begin{array}{c} \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & I^{(l)} & 0 & R_6 & R_7 & 0 & 0 & R_{10} \\ 0 & 0 & R'_3 & 0 & I^{(n-l)} & R'_6 & R'_7 & 0 & 0 & R'_{10} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \\ \scriptstyle l \quad n-l \quad \nu-n \quad l \quad n-l \quad \nu-n \quad 1 \quad 1 \quad 1 \quad l-1 \end{array}$$

where $R'_3, R'_6, R'_7, R'_{10}$ arbitrarily. Therefore, the number of $e_T$ containing $e_L$ is $q^{(n-l)(2(\nu-n)+l)}$. $\square$

**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 $q^{(n-l)(r-n+k-1)}$;*

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

**Proof:** (1) The matrix of $m$ is like lemma 5, then for any $e_L \subset m$, assume that

$$e_L = \begin{array}{c} \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & R_{12} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \\ \scriptstyle l \quad n-l \quad r-n \quad \nu-r \quad l \quad n-l \quad r-n \quad \nu-r \quad 1 \quad 1 \quad 1 \quad k-1 \quad l-k \end{array}$$

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

$$e_T = \begin{array}{c} \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & R_{12} & 0 \\ 0 & 0 & R'_3 & 0 & 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & R'_{12} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \\ \scriptstyle l \quad n-l \quad r-n \quad \nu-r \quad l \quad n-l \quad r-n \quad \nu-r \quad 1 \quad 1 \quad 1 \quad k-1 \quad l-k \end{array}$$

where $R'_3, R'_{12}$ arbitrarily. Therefore, the number of $e_T$ contained in $m$ and containing $e_L$ is $q^{(n-l)(r-n+k-1)}$.

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

**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 different source states, respectively. Assume that $s_0 = s_1 \cap s_2$, $dim\ s_0 = k_1$, then $n+1 \leq k_1 \leq r+k-1$. 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 $q^{(n-l-1)(k_1-n-1)}$.*

**Proof:** Since $m_1 = s_1 + e_T, m_2 = s_2 + e_T$ and $m_1 \neq m_2$, then $s_1 \neq s_2$. And for any $s \in S, s \supset U$, therefore, $n \leq k_1 \leq r+k-1$. 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

$$m_i = \begin{array}{cc} \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & h_{i_2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & h_{i_{10}} & 0 \\ 0 & 0 & 0 & I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & h'_{i_{10}} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} & \begin{array}{c} \scriptstyle n \\ \scriptstyle r-n \\ \scriptstyle n \\ \scriptstyle k-1 \\ \scriptstyle 1 \end{array} \\ \scriptstyle n \quad r-n \quad \nu-r \quad n \quad r-n \quad \nu-r \quad 1 \quad 1 \quad 1 \quad k-1 \quad l-k & \end{array},$$

Let

$m_1 \cap m_2$

$$= \begin{array}{cc} \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & Q_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & Q_{10} & 0 \\ 0 & 0 & 0 & I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & Q'_{10} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} & \begin{array}{c} \scriptstyle n \\ \scriptstyle r-n \\ \scriptstyle n \\ \scriptstyle k-1 \\ \scriptstyle 1 \end{array} \\ \scriptstyle n \quad r-n \quad \nu-r \quad n \quad r-n \quad \nu-r \quad 1 \quad 1 \quad 1 \quad k-1 \quad l-k & \end{array},$$

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,

$$dim \begin{array}{c} \begin{pmatrix} 0 & Q_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & Q_{10} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & Q'_{10} & 0 \end{pmatrix} \\ \scriptstyle n \quad r-n \quad \nu-r \quad n \quad r-n \quad \nu-r \quad 1 \quad 1 \quad 1 \quad k-1 \quad l-k \end{array},$$

$= k_1 - n - 1$

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

$$e_L = \begin{array}{c} \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & R_{10} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \\ \scriptstyle l \quad n-l \quad r-n \quad \nu-r \quad l \quad n-l \quad r-n \quad \nu-r \quad 1 \quad 1 \quad 1 \quad k-1 \quad l-k \end{array}$$

$$e_{R_i} = \begin{array}{c} \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R'_3 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & R'_{10} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \\ \scriptstyle l \quad n-l \quad r-n \quad \nu-r \quad i+l \quad 1 \quad n-i \quad \nu-n \quad 1 \quad 1 \quad 1 \quad k-1 \quad l-k \end{array}$$

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

$$\begin{array}{c} \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & R_{10} & 0 \\ 0 & 0 & h_3 & 0 & 0 & I^{(i)} & 0 & 0 & 0 & 0 & 0 & 0 & h_{10} & 0 \\ 0 & 0 & R'_3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & R'_{10} & 0 \\ 0 & 0 & h'_3 & 0 & 0 & 0 & 0 & I^{(n-i-l-1))} & 0 & 0 & 0 & 0 & h'_{10} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \\ \begin{array}{cccccccccccccc} l & n-l & r-n & \nu-r & l & i & 1 & n-l-i-1 & \nu-n & 1 & 1 & 1 & k-1 & l-k \end{array} \end{array}$$

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 $q^{(n-l-1)(k_1-n-1)}$. □

**Theorem 10** *In this multi-receiver authentication codes, under the assumption that the encoding rules of the transmitter and the receiver are chosen according to a uniform probability distribution , the largest probabilities of success for impersonation attack and substitution attack from $R_L$ on a receiver $R_i$ are*

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

$$P_S[i,L] = \frac{1}{q^{r-l+k-2}}.$$

*respectively, where $i \notin L$.*

**Proof:** $Impersonation\ attack$: $R_L$, commonly send a message $m$ to $R_i$. $R_L$ is successful if $m$ is accepted by $R_i$ as authentic. Therefore

$$P_I[i,L] = \max_{e_L \in E_L} \left\{ \frac{\max_{m \in M} |\{e_T \in E_T | e_T \subset m \text{ and } e_T \supset e_L, e_{R_i}\}|}{|\{e_T \in E_T | e_T \supset e_L\}|} \right\}$$

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

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

$Substitution\ attack$: $R_L$, 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. Therefore $P_S[i,L]$

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

$$= \max_{n+1 \le k_1 \le r+k-1} \frac{q^{(n-l-1)(k_1-n-1)}}{q^{(n-l)(r-n+k-1)}}$$

$$= \frac{1}{q^{r-l+k-2}}.$$

The desired result follows. □

## 3.2 Construction II

Suppose that $\mathbb{F}_q$ be a finite field with $q$ elements and $v_i (1 \le 3i \le 2\nu)$ be the row vector in $\mathbb{F}_q^{(2\nu+2+l)}$. Let $3 \le 3n < \nu$, $1 < k \le l$, $U = \langle v_1, v_2, \cdots, v_{3n}, e_{2\nu+3}\rangle$, i.e., $U$ is a fixed subspace of type $(3n+1, 0, 0, 0, 1)$ in the $(2\nu+2+l)$-dimensional singular pseudo-symplectic space $\mathbb{F}_q^{(2\nu+2+l)}$, then $U^\perp$ is a subspace of type $(2\nu - 3n + 2 + l, 2(\nu-3n)+2, \nu-3n, 1, l)$. The set of source states $S$={$s|s$ is a subspace of type $(2\nu-3n+k, 2(\nu-3n), \nu-3n, 0, k)$ and $U \subset s \subset U^\perp$}; the set of the transmitter's encoding rules $E_T$={$e_T|e_T$ is a 3n dimensional subspace and $U + e_T$ is a subspace of type $(6n+1, 6n, 3n, 0, 1)$}; the set of the $i$th receiver's decoding rules $E_{R_i}$={$e_{R_i}|e_{R_i}$ is a 3 dimensional subspace and $U + e_{R_i}$ is a subspace of type $(3n+4, 6, 3, 0, 1)$ which is orthogonal to $\langle v_1, \cdots, v_{3i-3}, v_{3i+1}, \cdots, v_{3n}\rangle$}; the set of messages $M$={$m|m$ is a subspace of type $(2\nu+k, 2\nu, \nu, 0, k)$, $U \subset m$ and $m \cap U^\perp$ is a subspace of type $(2\nu-3n+k, 2(\nu-3n), \nu-3n, 0, k)$}.

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 $i$th 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 multi-receiver 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 uniquely source state contained in $m$ and there is $e_T \in E_T$, such that $m = s + e_T$.*

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

$$s = \begin{array}{c} \begin{pmatrix} I^{(3n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & Q_2 & 0 & Q_4 & Q_5 & 0 & 0 & 0 & Q_9 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \end{pmatrix} \begin{array}{c} 3n \\ 2\nu-6n \\ 1 \\ k-1 \end{array} \\ \begin{array}{ccccccccc} 3n & \nu-3n & 3n & \nu-3n & 1 & 1 & 1 & k-1 & l-k \end{array} \end{array},$$

and

$$e_T = \begin{array}{c} \begin{pmatrix} X_1 & X_2 & I^{(3n)} & X_4 & X_5 & 0 & X_7 & X_8 & X_9 \end{pmatrix} \\ \begin{array}{ccccccccc} 3n & \nu-3n & 3n & \nu-3n & 1 & 1 & 1 & k-1 & l-k \end{array} \end{array},$$

then

$$sS_{\sigma,l}s^T = \begin{array}{c} \left(\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 0 & Q_4Q_2^T + Q_2Q_4^T & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right) \begin{array}{c} {\scriptstyle 3n} \\ {\scriptstyle 2\nu-6n} \\ {\scriptstyle 1} \\ {\scriptstyle k-1} \end{array} \\ \begin{array}{cccc} {\scriptstyle 3n} & {\scriptstyle 2\nu-6n} & {\scriptstyle 1} & {\scriptstyle k-1} \end{array} \end{array}.$$

Since $\mathrm{rank}(sS_{\sigma,l}s^T) = 2(\nu - 3n)$, $\mathrm{rank}(Q_4Q_2^T + Q_2Q_4^T) = 2(\nu - 3n)$. Then we can derive that

$$\begin{pmatrix} U \\ e_T \end{pmatrix} S_{2,l} \begin{pmatrix} U \\ e_T \end{pmatrix}^T = \begin{pmatrix} 0 & 0 & I^{(3n)} \\ 0 & 0 & 0 \\ I^{(3n)} & 0 & 0 \end{pmatrix}.$$

We have

$m = s + e_T$

$$= \begin{array}{c} \left(\begin{array}{ccccccccc} I^{(3n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & Q_2 & 0 & Q_4 & Q_5 & 0 & 0 & 0 & Q_9 \\ X_1 & X_2 & I^{(3n)} & X_4 & X_5 & 0 & X_7 & X_8 & X_9 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \end{array}\right) \begin{array}{c} {\scriptstyle 3n} \\ {\scriptstyle 2(\nu-3n)} \\ {\scriptstyle 3n} \\ {\scriptstyle 1} \\ {\scriptstyle k-1} \end{array} \\ \begin{array}{ccccccccc} {\scriptstyle 3n} & {\scriptstyle \nu-3n} & {\scriptstyle 3n} & {\scriptstyle \nu-3n} & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle k-1} & {\scriptstyle l-k} \end{array} \end{array}$$

Thus m is a $2\nu + k$ dimensional subspace and $mS_{2,l}m^T$

$$= \begin{pmatrix} 0 & 0 & I^{(3n)} & 0 & 0 \\ 0 & Q_4Q_2^T + Q_2Q_4^T & Q_4X_2^T + Q_2X_4^T & 0 & 0 \\ I^{(3n)} & X_4Q_2^T + X_2Q_4^T & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\sim \begin{pmatrix} 0 & 0 & I^{(3n)} & 0 & 0 \\ 0 & Q_4Q_2^T + Q_2Q_4^T & 0 & 0 & 0 \\ I^{(3n)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

where $\mathrm{rank}\,(Q_4Q_2^T + Q_2Q_4^T) = 2(\nu - 3n)$. Therefore, $\mathrm{rank}(mS_{2,l}m^T) = 2\nu$, $\dim(m \cap E) = k$. From above, $m$ is a subspace of type $(2\nu + k, 2\nu, \nu, 0, k)$ and $U \subset m$, i.e., $m \in M$.

2) For $\forall m \in M$, $m$ is a subspace of type $(2\nu + k, 2\nu, \nu, 0, k)$ containing $U$. So there is a 3n-dimensional subspace $V \subset m$, satisfying

$$\begin{pmatrix} U \\ V \end{pmatrix} S_{2,l} \begin{pmatrix} U \\ V \end{pmatrix}^T = \begin{pmatrix} 0 & 0 & I^{(3n)} \\ 0 & 0 & 0 \\ I^{(3n)} & 0 & 0 \end{pmatrix}.$$

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

$$\begin{pmatrix} U \\ V \\ P \end{pmatrix} S_{2,l} \begin{pmatrix} U \\ V \\ P \end{pmatrix}^T$$

$$= \begin{pmatrix} 0 & 0 & I^{(3n)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ I^{(3n)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I^{(\nu-3n)} & 0 \\ 0 & 0 & 0 & I^{(\nu-3n)} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Let $s = \begin{pmatrix} U \\ P \end{pmatrix}$, then $s$ is a subspace of type $(2\nu - 3n + k, 2(\nu - 3n), \nu - 3n, 0, k)$ and $U \subset s \subset U^\perp$, i.e., $s \in S$ is a source state. For any $\nu \in V$ 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 $e_T = V$, 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 uniquely source state contained in $m$.

From Lemma 11, we know that this construction of multi-receiver authentication codes is reasonable and there are $n$ receivers in this system. Next the parameters of this codes was computed. □

**Lemma 12** *The number of the source states is* $|S| = N(2(\nu-3n), 2(\nu-3n), \nu-3n, 0; 2\nu-6n+2)N(k-1, l-1)q^{(2\nu-6n)(l-k)}$.

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

$$s = \begin{array}{c} \left(\begin{array}{ccccccccc} I^{(3n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & Q_2 & 0 & Q_4 & Q_5 & Q_6 & 0 & 0 & Q_9 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \end{array}\right) \begin{array}{c} {\scriptstyle 3n} \\ {\scriptstyle 2\nu-6n} \\ {\scriptstyle 1} \\ {\scriptstyle k-1} \end{array} \\ \begin{array}{ccccccccc} {\scriptstyle 3n} & {\scriptstyle \nu-3n} & {\scriptstyle 3n} & {\scriptstyle \nu-3n} & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle k-1} & {\scriptstyle l-k} \end{array} \end{array}$$

where $(Q_2, Q_4, Q_5, Q_6)$ is a subspace of type $(2(\nu - 3n), 2(\nu - 3n), \nu - 3n, 0; 2\nu - 6n + 2)$ in the pseudo-symplectic space $\mathbb{F}_q^{(2(\nu-n)+2)}$. Therefore, the number of the source states is $|S| = N(2(\nu - 3n), 2(\nu - 3n), \nu - 3n, 0; 2\nu - 6n + 2)N(k - 1, l - 1)q^{(2\nu-6n)(l-k)}$. □

**Lemma 13** *The number of the encoding rules of transmitter is* $|E_T| = q^{3n(2\nu-3n+1+l)}$.

**Proof:** Since $U + e_T$ is a subspace of type $(6n + 1, 6n, 3n, 0, 1)$, then we can suppose that

$$e_T = \begin{array}{c} \begin{pmatrix} X_1 & X_2 & I^{(3n)} & X_4 & X_5 & 0 & X_7 & X_8 & X_9 \end{pmatrix} \\ \begin{array}{ccccccccc} {\scriptstyle 3n} & {\scriptstyle \nu-3n} & {\scriptstyle 3n} & {\scriptstyle \nu-3n} & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle k-1} & {\scriptstyle l-k} \end{array} \end{array},$$

where $X_1, X_2, X_4, X_5, X_7, X_8$ and $X_9$ is arbitrary. Therefore the number of $e_T$ is $q^{3n(2\nu-3n+1+l)}$. □

**Lemma 14** *The number of the decoding rules of the $i$th receiver is $|E_{R_i}| = q^{3(2\nu-3n+1+l)}$.*

**Proof:** Since the $i$th receiver's decoding rules satisfying $U + e_{R_i}$ is a subspace of type $(3n+4, 6, 3, 0, 1)$ which is orthogonal to $\langle v_1, \cdots, v_{3i-3}, v_{3i+1}, \cdots, v_{3n}\rangle$ and the transitivity properties of singular pseudo-symplectic group. So we can assume that

$$e_{R_i} = \begin{pmatrix} X_1 & X_2 & 0 & I^{(3)} & 0 & X_6 & X_7 & 0 & X_9 & X_{10} & X_{11} \end{pmatrix}$$
$$\begin{matrix} 3n & \nu-3n & 3(i-1) & 3 & 3(n-i) & \nu-3n & 1 & 1 & 1 & k-1 & l-k \end{matrix}$$

where $X_1, X_2, X_6, X_7, X_9, X_{10}, X_{11}$ is arbitrary. Therefore the number of $|E_{R_i}|$ is $q^{3(2\nu-3n+1+l)}$. □

**Lemma 15** *(1)The number of encoding rules $e_T$ contained in $m$ is $q^{3n(2\nu-3n+k)}$;*

*(2)The number of the messages is $|M| = |S||E_T|/q^{3n(2\nu-3n+k)}$.*

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

$$m = \begin{pmatrix} I^{(3n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(\nu-3n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(3n)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(\nu-3n)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \end{pmatrix}$$
$$\begin{matrix} 3n & \nu-3n & 3n & \nu-3n & 1 & 1 & 1 & k-1 & l-k \end{matrix}$$

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

$$e_T = \begin{pmatrix} R_1 & R_2 & I^{(3n)} & R_4 & 0 & 0 & R_7 & R_8 & 0 \end{pmatrix},$$
$$\begin{matrix} 3n & \nu-3n & 3n & \nu-3n & 1 & 1 & 1 & k-1 & l-k \end{matrix}$$

where $R_1, R_2, R_4, R_7, R_8$ arbitrarily. Therefore, the number of $e_T$ contained in $m$ is $q^{3n(2\nu-3n+k)}$.

(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 $q^{3n(2\nu-3n+k)}$. Therefore we have $|M| = |S||E_T|/q^{3n(2\nu-3n+k)}$. □

**Theorem 16** *The parameters of constructed multi-receiver authentication codes are*

$|S| = N(2(\nu-3n), 2(\nu-3n), \nu-3n, 0; 2\nu-6n+2)N(k-1, l-1)q^{(2\nu-6n)(l-k)}$;

$|E_T| = q^{3n(2\nu-3n+1+l)}$;

$|E_{R_i}| = q^{3(2\nu-3n+1+l)}$;

$|M| = |S||E_T|/q^{3n(2\nu-3n+k)}$.

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 $1 \le l \le n-1$. First, we will proof 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 $q^{(3n-3l)(2\nu-3n+1+l)}$.*

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

$$e_L = \begin{pmatrix} R_1 & R_2 & I^{(3l)} & 0 & R_5 & R_6 & 0 & R_8 & R_9 & R_{10} \end{pmatrix}.$$
$$\begin{matrix} 3n & \nu-3n & 3l & 3n-3l & \nu-3n & 1 & 1 & 1 & k-1 & l-k \end{matrix}$$

Therefore, $e_T$ containing $e_L$ has the form as follows

$$e_T = \begin{pmatrix} R_1 & R_2 & I^{(3l)} & 0 & R_5 & R_6 & 0 & R_8 & R_9 & R_{10} \\ R_1' & R_2' & 0 & I^{(3n-3l)} & R_5' & R_6' & 0 & R_8' & R_9' & R_{10}' \end{pmatrix}$$
$$\begin{matrix} 3n & \nu-3n & 3l & 3n-3l & \nu-3n & 1 & 1 & 1 & k-1 & l-k \end{matrix}$$

where $R_1'$, $R_2'$, $R_5'$, $R_6'$, $R_8'$, $R_9'$, $R_{10}'$ arbitrarily. Therefore, the number of $e_T$ containing $e_L$ is $q^{(3n-3l)(2\nu-3n+1+l)}$. □

**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 $q^{(3n-3l)(2\nu-3n+k)}$;*

*(2) the number of $e_T$ contained in $m$ and containing $e_L, e_{R_i}$ is $q^{(3n-3l-3)(2\nu-3n+k)}$.*

**Proof:** (1) The matrix of $m$ is like lemma 15, then $\forall e_L \subset m$, we can assume that

$$e_L = \begin{pmatrix} R_1 & R_2 & I^{(3l)} & 0 & R_5 & 0 & 0 & R_8 & R_9 & 0 \end{pmatrix}.$$
$$\begin{matrix} 3n & \nu-3n & 3l & 3n-3l & \nu-3n & 1 & 1 & 1 & k-1 & l-k \end{matrix}$$

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

$$e_T = \begin{pmatrix} R_1 & R_2 & I^{(3l)} & 0 & R_5 & 0 & 0 & R_8 & R_9 & 0 \\ R_1' & R_2' & 0 & I^{(3n-3l)} & R_5' & 0 & 0 & R_8' & R_9' & 0 \end{pmatrix}.$$
$$\begin{matrix} 3n & \nu-3n & 3l & 3n-3l & \nu-3n & 1 & 1 & 1 & k-1 & l-k \end{matrix}$$

where $R_1', R_2', R_5', R_8', R_9'$ arbitrarily. Therefore, the number of $e_T$ contained in $m$ and containing $e_L$ is $q^{(3n-3l)(2\nu-3n+k)}$.

(2) Similarly, we can derive that the number of $e_T$ contained in $m$ and containing $e_L, e_{R_i}$ is $q^{(3n-3l-3)(2\nu-3n+k)}$. □

**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 different source states, respectively. Assume that $s_0 = s_1 \cap s_2$, dim $s_0 = k_1$, then $3n+1 \le k_1 \le 2\nu - 3n + k - 1$. 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 $q^{3(n-l-1)(k_1-3n-1)}$.*

**Proof:** Since $m_1 = s_1 + e_T, m_2 = s_2 + e_T$, and $m_1 \neq m_2$, then $s_1 \neq s_2$. And for any $s \in S, s \supset U$, therefore, $3n+1 \le k_1 \le 2\nu - 3n + k - 1$. 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

$$m_i = \begin{array}{c} \begin{pmatrix} I^{(3n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & h_{i_2} & 0 & h_{i_4} & 0 & 0 & 0 & h_{i_8} & 0 \\ X_1 & X_2 & I^{(3n)} & X_4 & 0 & 0 & X_7 & X_8 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & h_{i_8}' & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{array}{c} 3n \\ 2(\nu-3n) \\ 3n \\ k-1 \\ 1 \end{array} \\ \begin{array}{ccccccccc} 3n & \nu-3n & 3n & \nu-3n & 1 & 1 & 1 & k-1 & l-k \end{array} \end{array}$$

Let

$m_1 \cap m_2$

$$= \begin{array}{c} \begin{pmatrix} I^{(3n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & Q_2 & 0 & Q_4 & 0 & 0 & 0 & Q_8 & 0 \\ X_1 & X_2 & I^{(3n)} & X_4 & 0 & 0 & X_7 & X_8 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & Q_8' & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{array}{c} 3n \\ 2(\nu-3n) \\ 3n \\ k-1 \\ 1 \end{array} \\ \begin{array}{ccccccccc} 3n & \nu-3n & 3n & \nu-3n & 1 & 1 & 1 & k-1 & l-k \end{array} \end{array}$$

from above we know that $m_1 \cap m_2 = s_0 + e_T$, then dim $(m_1 \cap m_2) = k_1 + 3n$, therefore,

$$dim \begin{pmatrix} 0 & Q_2 & 0 & Q_4 & 0 & 0 & 0 & Q_8 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & Q_8' & 0 \end{pmatrix}$$

$$= k_1 - 3n - 1.$$

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

$$e_L = \begin{array}{c} \begin{pmatrix} R_1 & R_2 & I^{(3l)} & 0 & 0 & 0 & R_7 & 0 & 0 & R_{10} & R_{11} & 0 \end{pmatrix}, \\ \begin{array}{cccccccccccc} 3n & \nu-3n & 3l & 3(i-1-l) & 3 & 3(n-i) & \nu-3n & 1 & 1 & 1 & k-1 & l-k \end{array} \end{array}$$

$$e_{R_i} = \begin{array}{c} \begin{pmatrix} X_1 & X_2 & 0 & 0 & I^{(3)} & 0 & X_7 & 0 & 0 & X_{10} & X_{11} & 0 \end{pmatrix}, \\ \begin{array}{cccccccccccc} 3n & \nu-3n & 3l & 3(i-1-l) & 3 & 3(n-i) & \nu-3n & 1 & 1 & 1 & k-1 & l-k \end{array} \end{array}$$

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

$$\begin{array}{c} \begin{pmatrix} R_1 & R_2 & I^{(3l)} & 0 & 0 & 0 & R_8 & 0 & 0 & R_{11} & R_{12} & 0 \\ H_1 & H_2 & 0 & I^{(3(i-l-1))} & 0 & 0 & H_8 & 0 & 0 & H_{11} & H_{12} & 0 \\ X_1 & X_2 & 0 & 0 & I^{(3)} & 0 & X_7 & 0 & 0 & X_{10} & X_{11} & 0 \\ N_1 & N_2 & 0 & 0 & 0 & I^{(3(n-i))} & N_7 & 0 & 0 & N_{10} & N_{11} & 0 \end{pmatrix} \\ \begin{array}{cccccccccccc} 3n & \nu-3n & 3l & 3(i-1-l) & 3 & 3(n-i) & \nu-3n & 1 & 1 & 1 & k-1 & l-k \end{array} \end{array}$$

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 $q^{3(n-l-1)(k_1-3n-1)}$. $\square$

**Theorem 20** *In this multireceiver authentication codes, under the assumption that the encoding rules of the transmitter and the receiver are chosen according to a uniform probability distribution, the largest probabilities of success for $impersonation\ attack$ and $substitution\ attack$ from $R_L$ to a receiver $R_i$ are*

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

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

*respectively, where $i \notin L$.*

**Proof:** $Impersonation\ attack$: $R_L$, 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. Therefore

$$P_I[i, L] = \max_{e_L \in E_L} \left\{ \frac{\max_{m \in M} |\{e_T \in E_T | e_T \subset m \text{ and } e_T \supset e_L, e_{R_i}\}|}{|\{e_T \in E_T | e_T \supset e_L\}|} \right\}$$

$$= \frac{q^{(3n-3l-3)(2\nu-3n+k)}}{q^{(3n-3l)(2\nu-3n+1+l)}}$$

$$= \frac{1}{q^{(3n-3l-3)(l-k+1)+3(2\nu-3n++l+1)}}.$$

$Substitution\ attack$: $R_L$, 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. Therefore

$P_S[i, L]$

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

$$= \max_{3n+1 \le k_1 \le 2\nu-3n+k-1} \frac{q^{3(n-l-1)(k_1-3n-1)}}{q^{(3n-3l)(2\nu-3n+k)}}$$

$$= \frac{1}{q^{3(n-l-1)(3n+2)+3(2\nu-3n+k)}}.$$

This completes the proof. $\square$

**Acknowledgements:** This work is supported by the National Natural Science Foundation of China under Grant No. 61179026.

*References:*


[1] R. Safavi-Naini, H. Wang, Multi-receiver Authentication Codes: Models, Bounds, Constructions and Extensions, *Information and Computation*, Vol.151,1999, 1: pp.148–172.

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

[3] Y. Gao, X. H. Shi, H. L. Wang, A Constructions of Authentication codes with Arbitration from singular Symplectic Geometry over Finite Fields, *Acta Scientiarum Naturalium Universitatis Nankaiensis*, Vol.41, 2008, 6:pp. 72–77.

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

[5] G. J. Simmons, Message authentication with arbitration of transmitter/receiv- er disputes, *Proc. Eurcrypt 87. Lecture Notes in Computer Science*, Vol.304, 1985, pp. 151–165.

[6] R. Safavi-Naini, H. X. Wang, Broadcast Authentication for Group Communication, *Theoretical Computer Science*, Vol.269, 2001, (1&2):pp. 1–21.

[7] W. P. Ma, X. M. Wang, A Few New Structure Methods of Multi-sender uthentication Codes,*Acta Electronica Sinica*, Vol.28, 2000, 4:pp. 117–119.

[8] Li Xiyang,Qin Cong. New Constructions of Multi-receiver Authentication Codes, *Computer Engineering*, Vol.34, 2008, 15:pp. 138–139.

[9] S. D. Chen, D. W. Zhao, Two Constructions of Multireceiver Authentication Codes from Symplectic Geometry over Finite Fields, *ARS Combinatoria*, Vol.98, 2011, pp. 193–203.