A New Construction of Multisender Authentication Codes with Simultaneous Model from Singular Symplectic Geometry over Finite Fields

You Gao *, Gang Wang, Yifan He

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

Abstract: Multisender authentication codes allow a group of senders to construct an authenticated message for a receiver such that the receiver can verify authenticity of the received message. In this paper, a new multisender authentication codes with simultaneous model is constructed base on singular symplectic geometry over finite fields. The parameters and the maximum probabilities of deceptions are also computed.

Key words: Multisender authentication codes, Singular symplectic geometry, Construction, Finite fields.

§1.Introduction

The construction of authentication codes is an important topic in cryptography. Based on Simmons model of unconditionally secure authentication[1], authentication systems with multiple senders were introduced in [2], in the system ,there are multiple senders and construction of a codeword requires collaboration of a subset of them. In a simultaneous model, there are four participants: a group of senders $U = \{U_1, U_2, \cdots, U_n\}$; a Key Distribution Center (KDC), distribute keys to senders and receiver; a combiner C which is a public algorithm; a receiver which receives the authenticated message and verifies the message truth or not. In order to authenticate a message, there are four phases in a multisender model with simultaneous:

1. **Key Distribution**: KDC randomly selects an encoding rule $e \in E$ and secretly sends it to the receiver R , and sends $e_i = \pi_i(e)$ to the $i-$th sender U_i, $i = 1, 2, \cdots, n$;

*Correspondence : College of Science, Civil Aviation University of China,Tianjin 300300, P.R.China;

E-mail: gao_you@263.net

2. **Broadcast**: For a source state $s \in S$, if the transmitters $U_1, \cdots, U_n$ would like to send a source state s to the receiver R, U_i computes $t_i = f_i(s, e_{T_i})$, and sends $m_i = (s, t_i)$ to the combiner through a public channel;

3. **Combination**: The combiner receives the messages $m_i = (s, t_i), (i = 1, \cdots, n)$, and calculates $t = \varphi(t_1, \cdots, t_n)$using the combiner algorithm φ, then sends the message $m = (s, t)$ to the receiver R;

4. **Verification**: When the receiver receives the message $m = (s, t)$, he checks the authenticity by verifying whether $t = g(s, e)$ or not. If the equality holds, the message is regarded as authentic and is accepted. Otherwise, the message is rejected.

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

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.

Assume that $U_1, U_2, \cdots, U_n$ are transmitters, R is a receiver, E_{U_i} is the encoding rules of U_i, E_R is the decoding rules of receiver R. $D = \{i_1, i_2, \cdots, i_d\} \subset \{1, 2, \cdots, n\}$, $d < n$, $U_D = \{U_{i_1}, U_{i_2}, \cdots, U_{i_d}\}$, $E_D = \{E_{U_{i_1}}, E_{U_{i_2}}, \cdots, E_{U_{i_d}}\}$. Next we consider the attacks from malicious groups of transmitters.

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

$$P_I[D] = \max_{e_D \in E_D} \max_{m \in M} P(m \text{ is accepted by } R | e_D).$$

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

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

Many scholars have studied multi-receiver and multi-sender authentication codes, some constructions are given in[3-8], and it is well known that authentication codes which are constructed by the geometry of classical groups over finite fields are easy to compute, and a series of authentication codes with arbitration(A^2-codes) are constructed see [9-12]. There is a great relationship between A^2-codes and multi-receiver/multi-sender authentication codes. In this paper we construct a new multi-sender code

from singular symplectic geometry over finite fields, and parameters and the probabilities of deceptions of the code are also computed.

§2.Preliminaries

Singular symplectic geometry over finite fields is introduced in [13]. Let $n = 2\nu + l$ and define the $(2\nu + l) \times (2\nu + l)$ alternate matrix

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

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

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

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

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

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

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

Let v, u two non-zero vectors in $\mathbb{F}_q^{(2\nu+l)}$, they are said to be orthogonal(with respect to K_l) if $uK_lv^t = 0$, we say that u is orthogonal to v. Furthermore, for any subspace P we denote by $P^\perp$ the following set :

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

More properties of singular symplectic geometry over finite fields can be found in [13].

§3.Construction

Let $\mathbb{F}_q$ be a finite field with q elements. Assume that $1 < n' < n < \nu$, $n + n' < \nu$. $v_i (1 \leq i \leq 2\nu)$ be a row vector in $\mathbb{F}_q^{(2\nu+l)}$. $U' = \langle v_1, v_2, \cdots, v_{n'}, e_{2\nu+1} \rangle$ and U' is a fixed subspace of type$(n' + 1, 0, 1)$, U is a fixed subspace of type $(n+1, 0, 1)$, and $U' \subset U$,$W_i = \langle v_1, \cdots, v_{i-1}, v_{i+1} \cdots, v_{n'} \rangle$. The set of source states S=$\{s | s$ is a subspace of type $(2n+k, 0, k)$ and $U \subset s \subset U^{\perp}\}$; the set of $i-$th transmitter's encoding rules E_{U_i}=$\{e_{U_i} | e_{U_i}$ is a subspace of type $(n' + 2, 1, 1)$ and $U' \subset e_{U_i}$, $e_{U_i} \perp W_i\}$; the set of receiver's decoding rules E_R=$\{e_R | e_R$ is a subspace of type $(2n + 1, n, 1)$ and $U \subset e_R\}$; the set of $i-$th transmitter's tags T_i=$\{t_i | t_i$ is a subspace of type $(2n + k + 1, 1, k)$ and $U \subset t_i \subset W_i^{\perp}, t_i \not\subset U^{\perp}\}$; the set of receiver's tags T=$\{t | t$ is a subspace of type $(3n + k, n, k)$ and $U \subset t\}$.

Define the encoding map

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

The decoding map

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

The synthesizing map

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

where ω is a subspace and $t_1 + t_2 + \cdots + t_n + \omega$ is a subspace of type $(3n + k, n, k)$.

This code works as follows:

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

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

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

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

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

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

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

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

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

Lemma3.1 Let $C = (S, E_R, T; f)$, $C_i = (S, E_{U_i}, T_i; f_i)$, then C and C_i are Cartesian authentication codes, $1 \leq i \leq n$.

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

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

then

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

and

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

Obviously, for any $q \in Q$ and $q \neq 0$, we have $q \notin e_R$, therefore $t = s + e_R = \begin{pmatrix} U \\ Q \\ R \end{pmatrix}$, and

$$\begin{pmatrix} U \\ Q \\ R \end{pmatrix} K \begin{pmatrix} U \\ Q \\ R \end{pmatrix}^T = \begin{pmatrix} 0 & 0 & I^{(n)} & 0 \\ 0 & 0 & * & 0 \\ -I^{(n)} & * & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

so t is a subspace of type$(3n+k, n', k)$, and $U \subset t$.

On the other hand , for any $t \in T$, t is a subspace of type $(3n+k, n, k)$, so there is a subspace $V \subset t$, satisfying

$$\begin{pmatrix} U \\ V \end{pmatrix} K_l \begin{pmatrix} U \\ V \end{pmatrix}^T = \begin{pmatrix} 0 & I^{(n)} & 0 \\ -I^{(n)} & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{matrix} n \\ n \\ 1 \end{matrix}$$

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

$$\begin{pmatrix} U \\ V \\ P \end{pmatrix} K_l \begin{pmatrix} U \\ V \\ P \end{pmatrix}^T = \begin{pmatrix} 0 & I^{(n)} & 0 \\ -I^{(n)} & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{matrix} n \\ n \\ n+k \end{matrix}$$

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

If there is another source state s' contained in t, from the definition of s, we know $s' \subset t \cap U^{\perp} = s$, and dim (s') =dim (s), so $s' = s$,*ie.*, s is the unique source state contained in t. So C is Cartesian authentication code.

Similarly, we can prove that $C_i (1 \leq i \leq n)$ are also Cartesian authentication code.

From the Lemma 3.1, we know the construction is well defined. Next, we compute the parameters of the code.

Lemma 3.2 The number of the source states is

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

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

$$S = \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & X_1 & 0 & X_2 & 0 & 0 & X_3 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \end{pmatrix} \begin{matrix} n \\ n \\ 1 \\ k-1 \end{matrix}$$
$$\begin{matrix} n & \nu-n & n & \nu-n & 1 & k-1 & l-k \end{matrix}$$

where$(X_1 \quad X_2)$ is a subspace of type$(n, 0)$ in $\mathbb{F}_q^{2(\nu-n)}$ and X_3 arbitrarily. Therefore the number of the source states is

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

Lemma 3.3 The number of the $i-$th transmitter's encoding rules is $|E_{U_i}| = q^{2(\nu-n')+l-1}$, $1 \le i \le n'$.

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

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

where Y_2 has the form$(0, 0 \cdots, x_{\nu+i}, 0 \cdots 0)$,$x_{\nu+i} \neq 0$ and Y_1, Y_3, Y_4, Y_5 arbitrarily. So the number of the $i-$th transmitter's encoding rules is $|E_{U_i}| = q^{2(\nu-n')+l-1}$, $1 \le i \le n'$.

Lemma 3.4 For any $t_i \in T_i$, the number of t_i which containing e_{U_i} is $q^{2n-n'+k-1}$, $1 \le i \le n'$.

Proof: t_i is a subspace of type $(2n+k+1, 1, k)$, and $U \subset t_i$, so we can assume t_i has the form as the follows

$$t_i = \begin{pmatrix} I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 \end{pmatrix} \begin{matrix} i-1 \\ 1 \\ n-i \\ n \\ 1 \\ 1 \\ k-1 \end{matrix}$$
$$\begin{matrix} i-1 & 1 & n-i & n & \nu-2n & i-1 & 1 & n-i & n & \nu-2n & 1 & k-1 & l-k \end{matrix}$$

If $e_{U_i} \subset t_i$, then

$$e_{U_i} = \begin{pmatrix} I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & X_1 & X_2 & 0 & 0 & X_3 & 0 & 0 & 0 & 0 & X_4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} i-1 \\ 1 \\ n-i \\ 1 \\ 1 \end{matrix}$$
$$\begin{matrix} i-1 & 1 & n'-i & n-n' & n & \nu-2n & i-1 & 1 & n-i & n & \nu-2n & 1 & k-1 & l-k \end{matrix}$$

where $X_3 \neq 0$, and and X_1, X_2, X_4 arbitrarily, so the number of t_i which containing e_{U_i} is $q^{2n-n'+k-1}$.

Lemma 3.5 The number of the $i-$th transmitter's tags is

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

Proof: Since any t_i contains only one source state and the number of e_{U_i} contained in a t_i has been computed,we can compute $|T_i|$ by $|T_i| = |S||E_{U_i}|/q^{2n-n^{'}+k-1}$, then the number of the $i-$th transmitter's tags is $q^{n(l-k-2)+l-k-n^{'}+2\nu} N(n,0;2(\nu-n))N(k-1,l-1)$.

Lemma 3.6 The number of the receiver's decoding rules is $|e_R| = q^{n(2\nu-2n+l-1)}$.

Proof: The number of the receiver's decoding rules is $N^{'}(n+1,0,1;2n+1,n,1;2\nu+l,\nu)$, that is the number of subspaces of type$(2n+1,n,1)$ containing a given subspace of type $(n+1,0,1)$, and

$$\begin{aligned} & N^{'}(n+1,0,1;2n+1,n,1;2\nu+l,\nu) \\ &= \frac{N(n+1,0,1;2n+1,n,1;2\nu+l,\nu)N(2n+1,n,1;2\nu+l,\nu)}{N(n+1,0,1;2\nu+l,\nu)} \\ &= q^{n(2\nu-2n+l-1)}. \end{aligned}$$

Lemma 3.7 For any $t \in T$, the number of e_R which contained in t is $q^{n(n+k-1)}$.

Proof: t is a subspace of type $(3n+k,n,k)$, and $U \subset t$, so we can assume t has the form as the follows

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

If $e_R \subset t$, then

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

where X_1, X_2 arbitrarily, then the number of encoding rules e_R contained in t is $q^{n(n+k-1)}$.

Lemma 3.8 The number of the receiver's tags is

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

Proof: Similarly to Lemma 3.5.

Theorem 3.1 In the above construction of multisender authentication codes, the parameters are computed as follows

$|S| = q^{n(l-k)}N(n,0;2(\nu-n))N(k-1,l-1)$.
$|E_{U_i}| = q^{2(\nu-n')+l-1}$, $1 \le i \le n'$.
$|T_i| = q^{n(l-k-2)+l-k-n'+2\nu}\ N(n,0;2(\nu-n))N(k-1,l-1)$, $1 \le i \le n'$.
$|e_R| = q^{n(2\nu-2n+l-1)}$.
$|T| = q^{n(2\nu-3n+2l-2k)}N(n,0;2(\nu-n))N(k-1,l-1)$.

Without loss of generality, we assume that $U_D = \{U_1, U_2, \cdots, U_d\}$, $E_D = \{E_{U_1} \times E_{U_2} \times \cdots \times E_{U_d}\}$, where $d < n'$. Next we consider the attacks from U_D on R.

Lemma 3.9 For any $e_D = (e_{U_1}, e_{U_2}, \cdots, e_{U_d}) \in E_D$, the number of e_R containing e_D is $q^{(n-d)(2\nu-2n+l-1)}$.

Proof: For any $e_D = (e_{U_1}, e_{U_2}, \cdots, e_{U_d}) \in E_D$, we assume e_D as follows:

$$e_D = \begin{array}{c} \left(\begin{array}{cccccccccccc} I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & X_1 & X_2 & X_3 & I & 0 & X_4 & X_5 & X_6 & 0 & X_7 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right) \\ \begin{array}{cccccccccccc} d & n'-d & n-n' & n & \nu-2n & d & n'-d & n-n' & n & \nu-2n & 1 & l-1 \end{array} \end{array} \begin{array}{c} d \\ n'-d \\ d \\ 1 \end{array}$$

If $e_D \subset e_R$, then

$$e_R = \begin{array}{c} \left(\begin{array}{cccccccccccc} I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & X_1 & X_2 & X_3 & I & 0 & X_4 & X_5 & X_6 & 0 & X_7 \\ 0 & 0 & 0 & Y_2 & Y_3 & 0 & I & 0 & Y_5 & Y_6 & 0 & Y_7 \\ 0 & 0 & 0 & Z_2 & Z_3 & 0 & 0 & I & Z_5 & Z_6 & 0 & Z_7 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right) \\ \begin{array}{cccccccccccc} d & n'-d & n-n' & n & \nu-2n & d & n'-d & n-n' & n & \nu-2n & 1 & l-1 \end{array} \end{array} \begin{array}{c} d \\ n'-d \\ n-n' \\ d \\ n'-d \\ n-n' \\ 1 \end{array}$$

where $Y_2, Y_3, Y_5, Y_6, Y_7, Z_2, Z_3, Z_5, Z_6, Z_7$ arbitrarily, then the number of e_R containing e_D is $q^{(n-d)(2\nu-2n+l-1)}$.

Lemma 3.10 For any $t \in T$, $e_D = (e_{U_1}, e_{U_2}, \cdots, e_{U_d}) \in E_D$, $e_D \subset t$, the number of e_R which contained in t and containing e_D is $q^{(n+k-1)(n-d)}$.

Proof: For any $t \in T$, assume that

$$t = \begin{array}{c} \left(\begin{array}{cccccccccccccc} I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 \end{array}\right) \\ \begin{array}{cccccccccccccc} d & n'-d & n-n' & n & \nu-2n & d & n'-d & n-n' & n & \nu-2n & 1 & k-1 & l-k \end{array} \end{array} \begin{array}{c} d \\ n'-d \\ n-n' \\ n \\ d \\ n'-d \\ n-n' \\ 1 \\ k-1 \end{array}$$

Since $e_D \subset t$, then

$$e_D = \begin{array}{c} \left(\begin{array}{cccccccccccccc} I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & X_1 & X_2 & 0 & I & 0 & X_4 & 0 & 0 & 0 & X_5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{array}\right) \\ \begin{array}{cccccccccccccc} d & n'-d & n-n' & n & \nu-2n & d & n'-d & n-n' & n & \nu-2n & 1 & k-1 & l-k \end{array} \end{array} \begin{array}{c} d \\ n'-d \\ d \\ 1 \end{array}$$

If $e_D \subset e_R \subset t$, then

$$e_R = \begin{array}{c} \left(\begin{array}{cccccccccccccc} I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & X_1 & X_2 & 0 & I & 0 & X_4 & 0 & 0 & 0 & X_5 & 0 \\ 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & Z_2 & 0 & 0 & I & Z_4 & 0 & 0 & 0 & Z_6 & 0 \\ 0 & 0 & 0 & Q_2 & 0 & 0 & 0 & I & 0 & 0 & 0 & Q_6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{array}\right) \\ \begin{array}{cccccccccccccc} d & n'-d & n-n' & n & \nu-2n & d & n'-d & n-n' & n & \nu-2n & 1 & k-1 & l-k \end{array} \end{array} \begin{array}{c} d \\ n'-d \\ d \\ n-n' \\ n'-d \\ n-n' \\ 1 \end{array}$$

where $Z_2, Q_{2,}, Z_6, Q_6$ arbitrarily, so the number of the number of e_R which contained in t and containing e_D is $q^{(n+k-1)(n-d)}$.

Lemma 3.11 Assume that t' and t'' are two distinct tags are decoded by receiver's key e_R, s_1 and s_2 contained in t' and t'', respectively. Let $s_0 = s_1 \cap s_2$, $\dim s_0 = k_1$, then $n+1 \leq k_1 \leq 2n+k-1$, the number of e_R contained in $t' \cap t''$ and containing e_D is $q^{(k_1-n-1)(n-d)}$.

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

$$t^i = \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 \\ 0 & A_{i_1} & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(n)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & A_{i_2} \end{pmatrix} \begin{matrix} n \\ n \\ n \\ 1 \\ k-1 \end{matrix}$$
$$\begin{matrix} n & \nu-n & n & \nu-n & 1 & l-1 \end{matrix}$$

so

$$t' \cap t'' = \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 \\ 0 & A_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(n)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & A_2 \end{pmatrix} \begin{matrix} n \\ n \\ n \\ 1 \\ k-1 \end{matrix}$$
$$\begin{matrix} n & \nu-n & n & \nu-n & 1 & l-1 \end{matrix}$$

Since $\dim(t' \cap t'') = k_1 + n$, then

$$\dim \begin{pmatrix} 0 & A_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & A_2 \end{pmatrix} = k_1 - n - 1$$

For $e_D = (e_{U_1}, e_{U_2}, \cdots, e_{U_d}) \in E_D$, assume that

$$e_D = \begin{pmatrix} I^{(d)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n'-d)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & X_1 & X_2 & I^{(d)} & 0 & X_4 & 0 & 0 & X_5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$
$$\begin{matrix} d & n'-d & n-n' & \nu-n & d & n-d & n-n' & \nu-n & 1 & l-1 \end{matrix}$$

If $e_R \subset t' \cap t''$, and $e_D \subset e_R$, then

$$e_R = \begin{pmatrix} I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & X_1 & X_2 & I & 0 & X_4 & 0 & 0 & X_5 \\ 0 & 0 & 0 & Y_2 & 0 & I & Y_4 & 0 & 0 & Y_5 \\ 0 & 0 & 0 & Z_2 & 0 & 0 & I & 0 & 0 & Z_5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} d \\ n'-d \\ n-n' \\ d \\ n'-d \\ n-n' \\ 1 \end{matrix}$$
$$\begin{matrix} d & n'-d & n-n' & \nu-n & d & n-d & n-n' & \nu-n & 1 & l-1 \end{matrix}$$

Since

$$\dim \begin{pmatrix} 0 & A_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & A_2 \end{pmatrix} = k_1 - n - 1,$$

then the number of e_R which contained in $t' \cap t''$ and containing e_D is $q^{(k_1-n-1)(n-d)}$.

Theorem 3.2 The maximum probability of success in impersonation attack and substitution attack from U_D on R are

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

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

$$\begin{aligned} P_I(D) &= \max_{e_D \in E_D} \max_{t \in T} \left\{ \frac{|\{e_R \in E_R | e_D \subset e_R,\ e_R \subset t'\}|}{|\{e_R \in E_R | e_D \subset e_R\}|} \right\} \\ &= \frac{q^{(n+k-1)(n-d)}}{q^{(n-d)(2\nu-2n+l-1)}} \\ &= \frac{1}{q^{2\nu-3n+l-k}}. \end{aligned}$$

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

$$\begin{aligned} P_S(D) &= \max_{e_D \in E_D} \max_{t \in T} \max_{t \neq t' \in T} \left\{ \frac{|\{e_R \in E_R | e_D \subset e_R,\ e_R \subset t'_1 \cap t'_2\}|}{|\{e_R \in E_R | e_D \subset e_R,\ e_R \subset t'\}|} \right\} \\ &= \frac{q^{(k_1-n-1)(n-d)}}{q^{(n+k-1)(n-d)}} \\ &= \max_{k_1} \frac{1}{q^{2n+k-k_1}} \\ &= \frac{1}{q}. \end{aligned}$$

Acknowledgements

This work is supported by the National Natural Science Foundation of China under Grant No.61179026 and the Fundamental Research Funds for the Central Universities under Grant No.3122014K015.

References

[1] Simmons G.J. Authentication theory/coding theory[C]. lecture Notes in Computer Science, Springer, 1985, 411-491.

[2] Y.Desmedt and Yair Frankel. Shared generation of authentications and signatures.Advances in Cryptology-Cryptology'91, Lecture Notes in Computer Science, Springer-Verlag. 1992,vol.576,pp.457-469.

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

[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] Ma Wenping, Wang Xinmei. Several New Constructions on Multitransmitters Authentication Codes[J]. Acta Electronica Sinica. 28(4), 2000, pp. 117-119.

[6] Du Qingling, Lv Shuwang. Bounds and Construction for Multisender Authentication Code [J]. Computer Engineering and Applications. 2004.10 ,9 -10, 29.

[7] Safavi-Naini R, Wang Huaxiong. Broadcast Authentication for roup Communication[J]. Theoretical Computer Science. 269(1/2), 2001, pp. 1-21.

[8] Chen Shangdi, Zhao Dawei. Two Constructions of Multireceiver Authentication Codes from Symplectic Geometry over Finite Fields. Ars Combinatoria. 2011,98, pp. 193-203.

[9] Gao You, Shi xinhua, Wang hongli. A Constructions of Authentication codes with Arbitration from singular Symplectic Geometry over Finite Fields[j]. Acta Scientiarum Naturalium Universitatis Nankaiensis. 2008,41(6), pp.72-77.

[10] Wang Hong-li,Gao You. Construction of Authentication codes with Arbitration from Singular Pseudo-symplectic Geometry. Journal of Hebei Polytechnic University (Natural Science Edition). 2008,30(2), pp. 65-70.

[11] Li Ruihu. Construction of Authentication Codes with Arbitration from Symplectic Geometry[J].Appl.Math.J. Chinese Univ.Ser.B,1999,14(4), pp.475-480.

[12] Li Ruihu,Li Zun xian. Construction of Authentication Codes with Arbitration from Sympletic Geometry .Journal of china institute of communications. 1999, 20(7), pp.21-26.

[13] Wan Zhexian. Geometry of Classical Groups over Finite Fields (Second Edition) [M]. Beijing/New York: Science Press, 2002.