A Construction of Multi-sender Authentication Codes from Pseudo-Symplectic Geometry over Finite Fields

Xiuli Wang

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

Abstract: Multi-sender authentication codes allow a group of senders to construct an authenticated message for a receiver such that the receiver can verify authenticity of the received message. In this paper, we constructed one multi-sender authentication codes from pseudo-symplectic geometry over finite fields. The parameters and the probabilities of deceptions of this codes are also computed.

Keywords: pseudo-symplectic geometry; multi-sender authentication codes; finite fields

2000 MR Subject Classification: 15A03; 94A60; 94A62

§1 Introduction

Multi-sender authentication code was firstly constructed by Gilbert, MacWilliams and Sloane in [1] in 1974. Multi-sender authentication system refers to that a group of senders cooperatively send a message to the receiver, then the receiver should be able to ascertain that the message is authentic. About this case, many scholars and researchers had made great contributions to multi-sender authentication codes [2-6].

In the actual computer network communications, multi-sender authentication codes include sequential model and simultaneous model. Sequential model is that each sender uses his own encoding rules to encode a source state orderly, and the last sender sends the encoded message to the receiver, the receiver receives the message and verifies whether the message is legal or not. Simultaneous model is that all senders use their own encoding rules to encode a source state, and each sender sends the encoded message to the synthesize respectively, then the

Supported by the NSF of China(61179026)and Fundamental Research of the Central Universities of China Civil Aviation University of Science special (ZXH2012k003).

Address: College of Science, Civil Aviation University of China, Tianjin 300300, P.R.China.
E-mail: xlwang@cauc.edu.cn, wangxiuli1999@tom.com

synthesizer forms an authenticated message and verifies whether the message is legal or not. In this paper, we will adopt to the second model.

In a simultaneous model, there are four participants: a group of senders $P = \{P_1, P_2, \cdots, P_n\}$, the keys distribution center, he responsible for the key distribution to senders and receiver, including solving the disputes between them, a receiver R, a synthesizer, he only runs the trusted synthesis algorithm. The code works as follows:each sender and receiver has their own cartesian authentication code respectively. Let $(S, E_i, T_i; f_i)(i = 1, 2, \cdots, n)$ be the sender's and Cartesian authentication code, $(S, E_R, T; g)$ be the receiver's cartesian authentication code, $h : T_1 \times T_2 \times \cdots \times T_n \rightarrow T$ be the synthesis algorithm. $\pi_i : E \rightarrow E_i$ be a subkey generation algorithm, where E is the key set of the key distribution center. When authenticating a message, the senders and the receiver should comply with the protocol: The key distribution center randomly selects a encoding rule $e \in E$ and sends $e_i = \pi_i(e)$ to the $i - th$ sender $P_i(i = 1, 2, \cdots, n)$ secretly, then he calculates e_R by e according to a effective algorithm, and secretly sends e_R to the receiver R; If the senders would like to send a source state s to the receiver R, P_i computes $t_i = f_i(s, e_i)(i = 1, 2, \cdots, n)$ and sends $m_i = (s, t_i)(i = 1, 2, \cdots, n)$ to the synthesizer through an open channel; The synthesizer receives the message $m_i = (s, t_i)(i = 1, 2, \cdots, n)$ and calculates $t = h(t_1, t_2, \cdots, t_n)$ by the synthesis algorithm h, then sends message $m = (s, t)$, he checks the authenticity by verifying whether $t = g(s, e_R)$ or not. If the equality holds, the message is authentic and is accepted. Otherwise, the message is rejected.

We assume that the key distribution center is credible, though he know the senders' and receiver's encoding rules, he will not participate in any communication activities. When transmitters and receiver are disputing, the key distribution center settles it. At the same time, we assume that the system follows the kerckhoff's principle which except the actual used keys, the other information of the whole system is public.

In a multi-sender authentication system, we assume that the whole senders are cooperation to form a valid message, that is, all senders as a whole and receiver are reliable. But there are some malicious senders which they together cheat the receiver, the part of senders and receiver are not credible, they can take impersonation attack and substitution attack. In the whole system, we assume $\{P_1, P_2, \cdots, P_n\}$ are senders, R is a receiver, E_i is the encoding rules set of the sender P_i, E_R is the decoding rules set of receiver R. If the source state space S and the key space E_R of receiver R are according to a uniform distribution of message space M and tag space T are determined by the probability distribution of S and E_R. $L = \{i_1, i_2, \cdots, i_l\} \subset \{1, 2, \cdots, n\}, l < n$, $P_L = \{p_1, p_2, \cdots, p_l\}, E_L = \{E_{p_1}, E_{p_2}, \cdots, E_{p_l}\}$. Now let us consider the attacks from malicious groups of senders. Here there still are two kinds of attack:

The opponent's impersonation attack: P_L send a message m to receiver. P_L is successful if the receiver accepts it as legitimate message. Denote $P_I(L)$ is the

largest probability of some opponent's successful impersonation attack, it can be expressed as

$$P_I(L) = \max_{e_L \in E_L} \max_{m \in M} P(m \text{ is accept by } R/e_L).$$

The opponent's substitution attack: the largest probability of some opponent's successful substitution attack, it can be expressed as

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

In this paper, we give a construction about multi-sender authentication code from Pseudo-Symplectic Geometry over finite fields.

§2 Pseudo-Symplectic Geometry

Let F_q be the finite field with q elements, where q is a power of 2, $n = 2\nu + \delta$ and δ=1,2. Let

$$K = \begin{pmatrix} 0 & I^{(\nu)} \\ I^{(\nu)} & 0 \end{pmatrix}, \quad S_1 = \begin{pmatrix} K & \\ & 1 \end{pmatrix}, \quad S_2 = \begin{pmatrix} K & & \\ & 0 & 1 \\ & 1 & 1 \end{pmatrix}$$

and S_δ is an $(2\nu + \delta) \times (2\nu + \delta)$ non-alternate symmetric matrix.

The pseudo-symplectic group of degree $(2\nu + \delta)$ over F_q is defined to be the set of matrices $Ps_{2\nu+\delta}(F_q) = \{T | TS_\delta {}^tT = S_\delta\}$ denoted by $Ps_{2\nu+\delta}(F_q)$.

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

$$F_q^{(2\nu+\delta)} \times Ps_{2\nu+\delta}(F_q) \to F_q^{(2\nu+\delta)}$$
$$((x_1, x_2, \ldots, x_{2\nu+\delta}), T) \to (x_1, x_2, \ldots, x_{2\nu+\delta})T.$$

The vector space $F_q^{(2\nu+\delta)}$ together with this group action is called the pseudo-symplectic space over the finite field F_q of characteristic 2.

Let P be an m-dimensional subspace of $F_q^{(2\nu+\delta)}$, then $PS_\delta {}^tP$ is cogredient to one of the following three normal forms

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

$$M(m, 2s+1, s) = \begin{pmatrix} 0 & I^{(s)} & & \\ I^{(s)} & 0 & & \\ & & 1 & \\ & & & 0^{(m-2s-1)} \end{pmatrix}$$

$$M(m, 2s+2, s) = \begin{pmatrix} 0 & I^{(s)} & & & & \\ I^{(s)} & 0 & & & & \\ & & 0 & 1 & & \\ & & 1 & 1 & & \\ & & & & 0^{(m-2s-2)} & \end{pmatrix}$$

for some s such that $0 \leq s \leq [m/2]$. We say that P is a subspace of type $(m, 2s+\tau, s, \epsilon)$, where τ =0,1 or 2 and ϵ =0 or 1, if

(i) $PS_\delta\, {}^tP$ is cogredient to $M(m, 2s+\tau, s)$, and

(ii) $e_{2\nu+1} \notin P$ or $e_{2\nu+1} \in P$ according to $\epsilon = 0$ or $\epsilon = 1$, respectively.

Let P be an m-dimensional subspace of $F_q^{(2\nu+\delta)}$. Denote by $P^\perp$ the set of vectors which are orthogonal to every vector of P, i.e.,

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

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

More properties of pseudo-symplectic geometry over finite fields can be found in [7].

In [2], Desmedt, Frankel and Yung gave two constructions for MRA-codes based on polynomials and finite geometries, respectively. There are other constructions of multi-sender authentication codes are given in [3 – 6]. The construction of authentication codes is combinational design in its nature. We know that 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 this paper we constructed one multi-sender authentication codes from pseudo-symplectic geometry over finite fields. The parameters and the probabilities of deceptions of this codes are also computed. We realize the generalization and application of the similar idea and method of the article [9] from symplectic geometry to pseudo-symplectic geometry over Finite Fields.

§3 Construction

Let $\mathbb{F}_q$ be a finite field with q elements and $e_i (1 \leq i \leq 2\nu+2)$ be the row vector in $\mathbb{F}_q^{(2\nu+2)}$ whose $i-th$ coordinate is 1 and all other coordinates are 0. Assume that $2 < n+1 < r < \nu$. $U = \langle e_1, e_2, \cdots, e_n \rangle$, i.e., U is an n–dimensional subspace of $\mathbb{F}_q^{(2\nu+2)}$ generated by $e_1, e_2, \cdots, e_n$, then $U^\perp = \langle e_1, \cdots, e_\nu, e_{\nu+n+1}, \cdots, e_{2\nu+2} \rangle$. $W_i = \langle e_1, \cdots, e_{i-1}, e_{i+1}, \cdots, e_n \rangle, 1 \leq i \leq n$, then $W_i^\perp = \langle e_1, \cdots, e_\nu, e_{\nu+i}, e_{\nu+n+1}, \cdots, e_{2\nu+2} \rangle$. The set of source states $S = \{s | s$ is a subspace of type $(2\nu-2n+2, 2\nu-2n+2, \nu-n, 1)$ and $s \subset U^\perp\}$; the set of $i-th$ sender's decoding rules $E_{P_i} = \{e_{P_i} | e_{P_i}$ is a 1–dimensional subspace and $U + e_{P_i}$ is a subspace of type $(n+1, 0, 0, 0)$ which

is orthogonal to $\langle e_1, \cdots, e_{i-1}, e_{i+1}, \cdots, e_n \rangle\}$, $1 \le i \le n$; the set of receiver's decoding rules E_R=$\{e_R | e_R$ an n–dimensional subspace and $U + e_R$ is a subspace of type $(2n, 2n, n, 0)\}$; the set of i–th transmitter's tags $T_i = \{t_i | t_i$ is a subspace of type $(2v - 2n + 3, 2(v - n + 1), v - n + 1, 1)$ and $t_i \not\subset U^{\perp}\}$; the set of receiver's tags T=$\{ t |\ t$ is a $(2v - n + 2)$-dimensional subspace and $m^{\perp} \in E_R\}$.

Define the encoding map $f_i : S \times E_{P_i} \to T_i, f_i(s, e_{P_i}) = s + e_{P_i}$, $1 \le i \le n$.

The decoding map $f : S \times E_R \to T, f(s, e_R) = s + e_R$.

The synthesizing map $g : T_1 \times T_2 \times \cdots \times T_n \to T, g(t_1, t_2, \cdots, t_n) = A(t_1 + t_2 + \cdots + t_n)$, where A is a nonsingular matrix and $A(t_1 + t_2 + \cdots + t_n)$ is a subspace of type $(2r + 1, 2r, r, 1)$.

The code works as follows:

1. Key distribution.

The key distribution center randomly chooses an $e_R \in E_R$ and selects a $(2n, n)$ subspace e such that $U \subset e$, and selects $\{e_{P_i} \in E_{P_i}$ so that $e_{P_1} + e_{P_2} + \cdots, + e_{P_n} = e$, A is a nonsingular matrix satisfying $e_R = \langle e, A \rangle$. The key distribution center randomly secretly sends e_R, e_{P_i} to the receiver and the senders respectively, and sends A to the synthesizer.

2. Broadcast. If the senders want to send a source state $s \in S$ to the receiver R, the sender P_i calculates $t_i = f_i(s, e_{P_i}) = s + e_{P_i}$, then sends $t_i (1 \le i \le n)$ to the synthesizer.

3. Synthesis. After the synthesizer receives $t_1, t_2, \cdots, t_n$, he calculates $h = (t_1, t_2, \cdots, t_n) = A(t_1 + t_2 + \cdots + t_n)$ and then sends $m = (s, t)$ to the receiver R.

4.Verification. When the receiver R receives $m = (s, t)$, he calculates $t' = g(s, e_R) = s + e_R$. If $t = t'$, he accepts t, otherwise, he rejects it.

Let

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

$$\begin{matrix} l & n-l & v-n & l & i-l-1 & 1 & n-i & v-n & 1 & 1 \end{matrix}$$

then

$$U^{\perp} = \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(v-n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(v-n)} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$\begin{matrix} l & n-l & v-n & l & i-l-1 & 1 & n-i & v-n & 1 & 1 \end{matrix}$$

$$W_i^{\perp} = \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(\nu-n)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(\nu-n)} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ l & n-l & \nu-n & l & i-l-1 & 1 & n-i & \nu-n & 1 & 1 \end{pmatrix}.$$

Lemma 3.1 Let $C_i = (S, E_{P_i}, T_i; f_i)$, the codes is a Cartesian authentication code, $1 \le i \le n$.

Proof. (1) For any $e_{p_i} \in E_{p_i}$, $s \in S$, Because e_{p_i} is a 1–dimensional subspace and $U + e_{P_i}$ is a subspace of type $(n+1, 0, 0, 0)$ which is orthogonal to $\langle e_1, \cdots, e_{i-1}, e_{i+1}, \cdots, e_n \rangle\}$, $1 \le i \le n$; we can assume that

$$e_{p_i} = \begin{pmatrix} R_1 & R_2 & 0 & 1 & 0 & 0 & R_7 & 0 \\ n & \nu-n & i-1 & 1 & n-i & \nu-n & 1 & 1 \end{pmatrix}.$$

Let $s \in S$, since $s \subset U^{\perp}$, s has the form as follows:

$$s = \begin{pmatrix} A_1 & I^{(\nu-n)} & 0 & 0 & 0 & 0 \\ B_1 & 0 & 0 & I^{(\nu-n)} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ D_1 & 0 & 0 & 0 & 0 & 1 \\ n & \nu-n & n & \nu-n & 1 & 1 \end{pmatrix}.$$

Let $t_i = s + e_{p_i}$, then

$$t_i = \begin{pmatrix} A_1 & I^{(\nu-n)} & 0 & 0 & 0 & 0 & 0 & 0 \\ B_1 & 0 & 0 & 0 & 0 & I^{(\nu-n)} & 0 & 0 \\ R_1 & R_2 & 0 & 1 & 0 & 0 & R_7 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ D_1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ n & \nu-n & i-1 & 1 & n-i & \nu-n & 1 & 1 \end{pmatrix} \sim$$

$$\begin{pmatrix} A_1 & I^{(\nu-n)} & 0 & 0 & 0 & 0 & 0 & 0 \\ B_1 & 0 & 0 & 0 & 0 & I^{(\nu-n)} & 0 & 0 \\ R_1 & R_2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ D_1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ n & \nu-n & i-1 & 1 & n-i & \nu-n & 1 & 1 \end{pmatrix}$$

and

$$t_i S_2 {}^t t_i \sim \begin{pmatrix} 0 & I^{(\nu-n)} & 0 & 0 & * \\ I^{(\nu-n)} & 0 & 0 & 0 & * \\ 0 & 0 & 0 & 1 & * \\ 0 & 0 & 1 & 1 & * \\ * & * & * & * & 0 \end{pmatrix}.$$

Obviously, t_i is a subspace of type $(2\nu-2n+3, 2(\nu-n+1), \nu-n+1, 1)$ and $t_i \not\subset U^{\perp}$, that is $t_i \in T_i$. Furthermore we know $t_i \cap U^{\perp} = (s + e_{p_i}) \cap U^{\perp} = s + (e_{p_i} \cap U^{\perp}) = s + \emptyset = s$.

Conversely, for any $t_i \in T_i$, let $s = t_i \cap U^{\perp}, L \subset t_i$, satisfying $t_i = s \oplus L$. Obviously, $s \subset U^{\perp}$. For $t_i \subset W_i^{\perp}$ and $t_i \not\subset U^{\perp}$, let

$$t_i = \begin{pmatrix} A_1 & I^{(\nu-n)} & 0 & 0 & 0 & 0 & 0 & 0 \\ B_1 & 0 & 0 & 0 & 0 & I^{(\nu-n)} & 0 & 0 \\ R_1 & R_2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ D_1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ n & \nu-n & i-1 & 1 & n-i & \nu-n & 1 & 1 \end{pmatrix}.$$

Obviously,

$$t_i \cap U^{\perp} = \begin{pmatrix} A_1 & I^{(\nu-n)} & 0 & 0 & 0 & 0 \\ B_1 & 0 & 0 & I^{(\nu-n)} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ D_1 & 0 & 0 & 0 & 0 & 1 \\ n & \nu-n & n & \nu-n & 1 & 1 \end{pmatrix}.$$

For t_i is a subspace of type $(2\nu - 2n + 3, 2(\nu - n + 1), \nu - n + 1, 1)$, then $t_i \cap U^{\perp}$ is a subspace of type $(2(\nu - n) + 1, 2(\nu - n + 1), \nu - n, 1)$, that is $s \in S$. Choose

$$L = \begin{pmatrix} R_1 & R_2 & 0 & 1 & 0 & 0 & R_7 & 0 \end{pmatrix},$$

so $L \in e_{P_i}$, $s \oplus L = s \oplus e_{P_i}$. Therefore, f_i is a surjection. For any $t_i \in T_i, e_{P_i} \in E_{P_i}$, if there exist $s \in S$ so that $t_i = s + e_{P_i}$, then $s \in t_i \cap U^{\perp}$. However, $dim s = 2(\nu - n) + 2 = dim(t_i \cap U^{\perp})$, so $s = t_i \cap U^{\perp}$, that is, s is determined by t_i and e_{P_i}.

Lemma 3.2 Let $C = (S, E_R, T; g)$, the codes is a Cartesian authentication code.

Proof. (1) For any $s \in S$, $e_R \in E_R$, from the definition of s and e_R, we assume that

$$s = \begin{pmatrix} A_1 & I^{(\nu-n)} & 0 & 0 & 0 & 0 \\ B_1 & 0 & 0 & I^{(\nu-n)} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ D_1 & 0 & 0 & 0 & 0 & 1 \\ n & \nu-n & n & \nu-n & 1 & 1 \end{pmatrix}$$

and

$$e_R = \begin{pmatrix} H_1 & H_2 & I^{(n)} & 0 & H_5 & 0 \\ n & \nu-n & n & \nu-n & 1 & 1 \end{pmatrix}.$$

$$t = s + e_R = \begin{pmatrix} A_1 & I^{(\nu-n)} & 0 & 0 & 0 & 0 \\ B_1 & 0 & 0 & I^{(\nu-n)} & 0 & 0 \\ H_1 & H_2 & I^{(n)} & 0 & H_5 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ D_1 & 0 & 0 & 0 & 0 & 1 \\ n & \nu-n & n & \nu-n & 1 & 1 \end{pmatrix} \sim$$

$$\begin{pmatrix} A_1 & I^{(\nu-n)} & 0 & 0 & 0 & 0 \\ B_1 & 0 & 0 & I^{(\nu-n)} & 0 & 0 \\ H_1 & H_2 & I^{(n)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ D_1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$
$$\begin{matrix} n & \nu-n & n & \nu-n & 1 & 1 \end{matrix}$$

is an $(2\nu - n + 2)$– dimensional subspace.

But $t^{\perp} = ({}^tH_1, {}^tB_1, I^{(n)}, {}^tA_1, {}^tD_1, {}^t0) \in E_R$, so $B_1 = 0$, therefore we take

$$t = \begin{pmatrix} A_1 & I^{(\nu-n)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(\nu-n)} & 0 & 0 \\ H_1 & H_2 & I^{(n)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ D_1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$
$$\begin{matrix} n & \nu-n & n & \nu-n & 1 & 1 \end{matrix}$$

Obviously $t \in T$.

(2) For $t \in T$, t is an $(2\nu - n + 2)$– dimensional subspace, and $t^{\perp} \in E_R$,

$$t \cap U^{\perp} = \begin{pmatrix} A_1 & I^{(\nu-n)} & 0 & 0 & 0 & 0 \\ B_1 & 0 & 0 & I^{(\nu-n)} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ D_1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$
$$\begin{matrix} n & \nu-n & n & \nu-n & 1 & 1 \end{matrix}$$

$(t \cap U^{\perp})^{\perp} = t^{\perp} + U$ is a subspace of type $(2n, 2n, 2n, 0)$, $t \cap U^{\perp}$ is a subspace of type $(2\nu - 2n + 2, 2\nu - 2n + 2, \nu - n, 1)$, so we take $s = t \cap U^{\perp}$, i.e., $s \in S$. Let

$$e_R = \begin{pmatrix} H_1 & H_2 & I^{(n)} & 0 & H_5 & 0 \end{pmatrix},$$
$$\begin{matrix} n & \nu-n & n & \nu-n & 1 & 1 \end{matrix}$$

therefore e_R is an n–dimensional subspace and $U + e_R$ is a subspace of type $(2n, 2n, n, 0)$, then e_R is a transmitter's decoding rule and satisfying $t = s + e_R$.

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

From Lemma 3.1 and 3.2, we know that such construction of multisender authentication codes is reasonable and there are n senders in this system. Next we compute the parameters of this codes and the maximum probability of success in impersonation attack and substitution attack by group of senders.

Lemma 3.3 Some parameters of this construction are

$$|S| = q^{n(2\nu-2n+1)}; \quad |E_{P_i}| = q^{\nu+1}.$$

Proof. Since $s \subset U^{\perp}$ and s is a subspace of type $(2\nu-2n+2, 2\nu-2n+2, \nu-n, 1)$,

s has the form as follows:

$$s = \begin{pmatrix} A_1 & I^{(v-n)} & 0 & 0 & 0 & 0 \\ B_1 & 0 & 0 & I^{(v-n)} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ D_1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{matrix} v-n \\ v-n \\ 1 \\ 1 \end{matrix},$$

$$\begin{matrix} n & v-n & n & v-n & 1 & 1 \end{matrix}$$

where A_1, B_1, D_1 arbitrarily. So $|S| = q^{n(2v-2n+1)}$.

For any $e_{p_i} \in E_{p_i}$, we can assume that e_{P_i} has the form as follows:

$$e_{p_i} = \begin{pmatrix} R_1 & R_2 & 0 & 1 & 0 & 0 & R_7 & 0 \end{pmatrix},$$
$$\begin{matrix} n & v-n & i-1 & 1 & n-i & v-n & 1 & 1 \end{matrix}$$

where R_1, R_2, R_7 arbitrarily. Therefore, $|E_{P_i}| = q^{v+1}$.

Lemma 3.4 (1) For any $t_i \in T_i$, the number of t_i containing e_{P_i} is $q^{v-n+1}(1 \le i \le n)$;

(2) The number of the $i-th$ transmitter's tag is $|T_i| = q^{2n(v-n+1)}$.

Proof. (1) Since the transitivity properties of the same subspaces under the pseudo-symplectic groups, we may take t_i as follows:

$$t_i = \begin{pmatrix} A_1 & I^{(v-n)} & 0 & 0 & 0 & 0 & 0 & 0 \\ B_1 & 0 & 0 & 0 & 0 & I^{(v-n)} & 0 & 0 \\ R_1 & R_2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ D_1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$
$$\begin{matrix} n & v-n & i-1 & 1 & n-i & v-n & 1 & 1 \end{matrix}$$

if $e_{P_i} \subset t_i$, then we assume that

$$e_{p_i} = \begin{pmatrix} R_1 & R_2 & 0 & 1 & 0 & 0 & R_7 & 0 \end{pmatrix},$$
$$\begin{matrix} n & v-n & i-1 & 1 & n-i & v-n & 1 & 1 \end{matrix}$$

where R_2, R_7 arbitrarily, therefore the number of t_i containing e_{P_i} is $q^{v-n+1}(1 \le i \le n)$;

(2) We know that every t_i contains only one source state $t_i \cap U^{\perp}$ and the number of t_i containing e_{P_i}. Therefore we have $|t_i| = |S||E_{P_i}|/q^{r-n+1} = |S|q^{n(v-n+1)}|/q^{v-n+1} = q^{2n(v-n+1)}$.

Lemma 3.5 (1) The number of the receiver's decoding rules is $|E_R| = q^{n(v+1)}$;

(2) For any $t \in T$, the number of e_R which contained t is $q^{n(v-n+1)}(1 \le i \le n)$;

(3) The number of the receiver's tag is $|T| = q^{n(2v-2n+1)}$.

Proof. (1) Let $e_R \in E_R$, e_R has the form as follows:

$$e_R = \begin{pmatrix} H_1 & H_2 & I^{(n)} & 0 & H_5 & 0 \end{pmatrix},$$
$$\begin{matrix} n & v-n & n & v-n & 1 & 1 \end{matrix}$$

where H_1, H_2, H_5 arbitrarily. Therefore $|E_R| = q^{n(\nu+1)}$.

(2) Since the transitivity properties of the same subspaces under the pseudo-symplectic groups, we may choose t as follows:

$$t = \begin{pmatrix} A_1 & I^{(\nu-n)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(\nu-n)} & 0 & 0 \\ H_1 & H_2 & I^{(n)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ D_1 & 0 & 0 & 0 & 0 & 1 \\ n & \nu-n & n & \nu-n & 1 & 1 \end{pmatrix}.$$

If $e_R \subset t$, then

$$e_R = \begin{pmatrix} H_1 & H_2 & I^{(n)} & 0 & H_5 & 0 \\ n & \nu-n & n & \nu-n & 1 & 1 \end{pmatrix},$$

where H_2, H_5 arbitrarily. Therefore the number of e_R which contained t is $q^{n(\nu-n+1)}$;

(3) Similarly to Lemma 3.4(2), $|T| = |S||E_R|/q^{r-n+1} = |S|q^{n(\nu+1)}/q^{\nu-n+1} = q^{n(2\nu-n+1)}$.

Without loss of generality, we assume that $L = \{i_1, i_2, \cdots, i_l\} \subset \{1, 2, \cdots, n\}, l < n$, $P_L = \{p_1, p_2, \cdots, p_l\}, E_L = \{E_{p_1}, E_{p_2}, \cdots, E_{p_l}\}$. Now let us consider the attacks on R from malicious groups of senders.

Lemma 3.6 For any $e_L = \{E_{p_1}, E_{p_2}, \cdots, E_{p_l}\} \in E_L$, the number of e_R containing e_L is $q^{(\nu-n+1)(n-l)}$.

Proof. For any $e_L = \{E_{p_1}, E_{p_2}, \cdots, E_{p_l}\} \in E_L$, we assume e_L as follows:

$$e_L = \begin{pmatrix} R_1 & R_2 & R_3 & I^{(l)} & 0 & 0 & R_7 & 0 \\ l & n-l & \nu-n & l & n-l & \nu-n & 1 & 1 \end{pmatrix}.$$

If $e_R \supset e_L$, then e_R has the form as follows:

$$e_R = \begin{pmatrix} R_1 & R_2 & R_3 & I^{(l)} & 0 & 0 & R_7 & 0 \\ H_1 & H_2 & H_3 & 0 & I^{(n-l)} & 0 & H_7 & 0 \\ l & n-l & \nu-n & l & n-l & \nu-n & 1 & 1 \end{pmatrix},$$

where H_1, H_2, H_3, H_7 arbitrarily. Therefore, the number of e_R containing e_L is $q^{(\nu+1)(n-l)}$.

Lemma 3.7 For any $t \in T$, and $e_L = \{E_{p_1}, E_{p_2}, \cdots, E_{p_l}\} \in E_L$, the number of e_R which contained in t and containing e_L is $q^{(\nu-n+1)(n-l)}$.

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

$$t=\begin{pmatrix} A_1 & A_2 & I^{(\nu-n)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I^{(\nu-n)} & 0 & 0 \\ R_1 & R_2 & 0 & I^{(l)} & 0 & 0 & 0 & 0 \\ H_1 & H_2 & 0 & 0 & I^{(n-l)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ D_1 & D_2 & 0 & 0 & 0 & 0 & 0 & 1 \\ l & n-l & \nu-n & l & n-l & \nu-n & 1 & 1 \end{pmatrix},$$

If $e_L \subset t$, then e_L has the form as follows:

$$e_L=\begin{pmatrix} R_1 & R_2 & R_3 & I^{(l)} & 0 & 0 & R_7 & 0 \\ l & n-l & \nu-n & l & n-l & \nu-n & 1 & 1 \end{pmatrix},$$

Since $e_L \subset e_R \subset t$, then we assume e_R as follow:

$$e_R=\begin{pmatrix} R_1 & R_2 & R_3 & I^{(l)} & 0 & 0 & R_7 & 0 \\ H_1 & H_2 & H_3 & 0 & I^{(n-l)} & 0 & H_7 & 0 \\ l & n-l & \nu-n & l & n-l & \nu-n & 1 & 1 \end{pmatrix},$$

where G_3 and G_7 arbitrarily. Therefore, the number of e_R which contained in t and containing e_L is $q^{(n-l)(\nu-n+1)}$.

Lemma 3.8 Assume that t_1 and t_2 are two distinct tags ($t_1, t_2 \in T$) which decoded by receiver's key e_R, s_1 and s_2 contained in t_1 and t_2 are two source states, respectively. Let $s_0 = s_1 \cap s_2$, dim $s_0 = k$, then $1 \le k \le 2(\nu - n) + 1$, the number of e_R which contained in $t_1 \cap t_2$ and containing e_L is $q^{(k+n-\nu-1)(n-1)}$.

Proof. Since $t_1 = s_1 + e_R, t_2 = s_2 + e_R$ and $t_1 \neq t_2$, then $s_1 \neq s_2$. For any $s \in S$, $U \in s$,obviously $n \le k \le 2r - n$. 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 $t_i = s_i + e_R = s_0 + s_i' + e_R$ and $s_i = t_i \cap U^{\perp}$, we know $s_0 = (t_1 \cap U^{\perp}) \cap (t_2 \cap U^{\perp}) = t_1 \cap t_2 \cap U^{\perp} = s_1 \cap t_2 = s_2 \cap t_1$, and $t_1 \cap t_2 = (s_1 + e_R) \cap t_2 = (s_0 + s_1' + e_R) \cap t_2 = ((s_0 + e_R) + s_1') \cap t_2$, since $s_0 + e_R \subseteq t_2$, then $t_1 \cap t_2 = (s_0 + e_R) + (s_1' \cap t_2)$, while $s_1' \cap t_2 \subseteq s_1 \cap t_2 = s_0$, so we have $t_1 \cap t_2 = s_0 + e_R$.

From the definition of t_i, we may take $t_i, i = 1, 2$ as follows:

$$t=\begin{pmatrix} A_{i_1} & A_{i_2} & A_{i_3} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I^{(\nu-n)} & 0 & 0 \\ R_{i_1} & R_{i_2} & R_{i_3} & I^{(l)} & 0 & 0 & 0 & 0 \\ H_{i_1} & H_{i_2} & H_{i_3} & 0 & I^{(n-l)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ D_{i_1} & D_{i_2} & D_{i_3} & 0 & 0 & 0 & 0 & 1 \\ l & n-l & \nu-n & l & n-l & \nu-n & 1 & 1 \end{pmatrix},$$

Let

$$t_1 \cap t_2 = \begin{pmatrix} A_1 & A_2 & A_3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I^{(v-n)} & 0 & 0 \\ R_1 & R_2 & R_3 & I^{(l)} & 0 & 0 & 0 & 0 \\ H_1 & H_2 & H_3 & 0 & I^{(n-l)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ D_1 & D_2 & D_3 & 0 & 0 & 0 & 0 & 1 \\ l & n-l & v-n & l & n-l & v-n & 1 & 1 \end{pmatrix},$$

from above we know that $t_1 \cap t_2 = s_0 + e_R$, then $dim(t_1 \cap t_2) = k + 2n - n = k + n$, therefore,

$$dim\begin{pmatrix} A_1 & A_2 & A_3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} = k + n - (v - n + n + 1) = k + n - v - 1.$$

For any $e_L, e_R \subset t_1 \cap t_2$, we can assume that

$$e_L = \begin{pmatrix} R_1 & R_2 & R_3 & I^{(l)} & 0 & 0 & R_7 & 0 \\ l & n-l & v-n & l & n-l & v-n & 1 & 1 \end{pmatrix},$$

$$e_R = \begin{pmatrix} R_1 & R_2 & R_3 & I^{(l)} & 0 & 0 & R_7 & 0 \\ H_1 & H_2 & H_3 & 0 & I^{(n-l)} & 0 & H_7 & 0 \\ l & n-l & v-n & l & n-l & v-n & 1 & 1 \end{pmatrix},$$

so where every row of

$$\begin{pmatrix} H_1 & H_2 & H_3 & 0 & H_7 & 0 \end{pmatrix}$$

is the linear combination of

$$\begin{pmatrix} A_1 & A_2 & A_3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Therefore, the number of $e_R \subset t_1 \cap t_2$ and containing e_L is $q^{(k+n-v-1)(n-l)}$.

Theorem 3.1 In the constructed multisender authentication codes, the largest probabilities of success for *impersonation attack* and *substitution attack* from E_L on a receiver R are

$$P_I(L) = \frac{1}{q^{n(n-l)}}, \quad P_S(L) = \frac{1}{q^{n-l}}$$

respectively.

Proof. *Impersonation attack*: E_L, after receiving their secret keys, encodes a message and send it to reveiver. E_L is successful if the receiver accepts it as legitimate message. So

$$\begin{aligned} P_I(L) &= \max_{e_L \in E_L} \max_{m \in M} \left\{ \frac{\max_{t \in T} |\{e_R \in E_R | e_L \subset e_R \text{ and } e_R \subset t\}|}{|\{e_R \in E_R | e_L \subset e_R\}|} \right\} \\ &= \frac{q^{(n-l)(v-n+1)}}{q^{(n-l)(v+1)}} = \frac{1}{q^{n(n-l)}}. \end{aligned}$$

Substitution attack: E_L replace t with another message t', after they observe a legitimate message t. E_L is successful if the receiver accept it as legitimate message. So

$$P_S(L) = \max_{e_L \in E_L} \max_{m \in M} \max_{m' \neq m \in M} \left\{ \frac{\max_{t' \in T} |\{e_R \in E_R | e_R \subset t, t' \text{ and } e_L \subset e_R\}|}{|\{e_R \in E_R | e_R \subset t \text{ and } e_L \subset e_R\}|} \right\}$$

$$= \max_{1 \leq k \leq 2(v-n)+1} \frac{q^{(n-l)(k+n-v-1)}}{q^{(n-l)(v-n+1)}} = \max_{1 \leq k \leq 2(v-n)+1} \frac{1}{q^{(2v-2n+2-k)(n-l)}} = \frac{1}{q^{n-l}}.$$

References

[1] Gilbert E N, MacWilliams F J, Sloan N J. Codes Which Detect Deception. *Bell System Technical Journal*, 1974, 53, pp.405-424.

[2] Y. Desmedt, Y. Frankel, M. Yung. Multi-receiver/Multi-sender Network Security: Efficient Authenticated Multicast/Feedback. *IEEE Infocom'92*, 1992, pp. 2045-2054.

[3] K. Martin, R. Safavi-Naini. Multisender Authentication Schemes with Unconditional Security. *Information and Communications Security (Lecture Notes in Computer Science), Berlin, Germany:Springer-Verlag*, 1997, 1334, pp.130-143.

[4] Ma Wenping, Wang Xinmei. Several New Constructions of Multitrasmitters Authentication Codes. *Acta Eletronic Sinica*, 2000, 28(4), pp.117-119.

[5] G.J.Simmons. Message Authentication with Arbitration of Transmitter/Receiver Disputes. *Proc. Eurcrypt 87. Lecture Notes in Computer Science*, 1985, 304, pp.151-165.

[6] Cheng Shangdi, Chang Lizhen. Two Constructions of Multi-sender Authentication Codes with Arbitration Based Linear Codes. To be published in Wseas Trans. Math..

[7] Wan Zhexian. *Geometry of Classical Groups over Finite Fields (2nd Edition)*. Science Press, Beijing/New York, 2002.

[8] Satoshi Obana, Kaoru Kurosawa. Bounds and Combinatorial Structure of (k,n) Multi-receiver A-Codes. *Designs,Codes and Cryptography*, 2001, 22, pp.47-63.

[9] Cheng Shangdi, Zhao Dawei. Two Constructions of Multireceiver Authentication Codes from Symplectic Geometry over Fields. *Ars Combinatoria*, 2011, 99, pp.193-203.