Construction of Authentication Codes with Arbitration from Singular Symplectic Geometry

Hongli Wang *

Mathematics and Information Science Department, Tangshan Normal University, Tangshan, Hebei, 063000, China

Abstract: A construction of authentication codes with arbitration from singular symplectic geometry over finite fields is given and the parameters of the codes are computed. Assuming that the encoding rules of the transmitter and the receiver are chosen according to a uniform probability distribution, the probabilities of success for different types of deceptions are also computed.

Key words: finite fields, singular symplectic geometry, authentication codes with arbitration.

§1.Introduction

To solve the distrust problem of the transmitter and the receiver in the communications system, G. J. Simmons introduced a model of authentication codes with arbitration (see [1]), which we may write simply (A^2-code), defined as follows:

Let S, E_T, E_R, and M be four non-empty finite sets, $f : S \times E_T \longmapsto M$ and $g : M \times E_R \longmapsto S \cup \{\text{reject}\}$ be two maps. The six tuple (S, E_T, E_R, M, f, g) is called an authentication code with arbitration (A^2-code), if

(i) The maps f and g are surjective;

(ii) For any $m \in M$ and $e_T \in E_T$, if there is an $s \in S$, satisfying $f(s, e_T) = m$, then such an s is uniquely determined by the given m and e_T;

(iii) $p(e_T, e_R) \neq 0$ and $f(s, e_T) = m$ implies $g(m, e_R) = s$, otherwise $g(m, e_R) = \{\text{reject}\}$.

S, E_T, E_R, and M are called the set of source states, the set of transmitter's encoding rules, the set of receiver's decoding rules and the set of

*Biography: Mrs. Hongli Wang (1979-), associate professor, Master, interested in: algebra, code and cryptogram.

E-mail: tslily@163.com

messages, respectively. f and g are called the encoding map and decoding map, respectively. The cardinals $|S|, |E_T|, |E_R|$ and $|M|$ are called the size parameters of the code.

In an authentication system that permits arbitration, this model includes four attendance: the transmitter, the receiver, the opponent and the arbiter, and includes five attacks:

(1) The opponent's impersonation attack: the largest probability of an opponent's successful impersonation attack is P_I , then

$$P_I = \max_{m \in M} \left\{ \frac{|\{e_R \in E_R | e_R \subset m\}|}{|E_R|} \right\}$$

(2)The opponent's substitution attack: the largest probability of an opponent's successful substitution attack is P_S , then

$$P_S = \max_{m \in M} \left\{ \frac{\max\limits_{m' \in M} |\{e_R \in E_R | e_R \subset m \, and \, e_R \subset m'\}|}{|\{e_R \in E_R | e_R \subset m\}|} \right\}$$

(3)The transmitter's impersonation attack: the largest probability of a transmitter's successful impersonation attack is P_T ,then

$$P_T = \max_{e_T \in E_T} \left\{ \frac{\max\limits_{m \, can't \, be \, encoded \, by \, e_T} |\{e_R \in E_R | e_R \subset m \, and \, p(e_R, e_T) \neq 0\}|}{|\{e_R \in E_R | p(e_R, e_T) \neq 0\}|} \right\}$$

(4) The receiver's impersonation attack: the largest probability of a receiver's successful impersonation attack is P_{R_0} , then

$$P_{R_0} = \max_{e_R \in E_R} \left\{ \frac{\max\limits_{m \in M} |\{e_T \in E_T | e_T \subset m \, and \, p(e_R, e_T) \neq 0\}|}{|\{e_T \in E_T | p(e_R, e_T) \neq 0\}|} \right\}$$

(5) The receiver's substitution attack: the largest probability of a receiver's successful substitution attack is P_{R_1} , then

$$P_{R_1} = \max_{e_R \in E_R, m \in M} \left\{ \frac{\max\limits_{m' \in M} |\{e_T \in E_T | e_T \subset m, m' \, and \, p(e_R, e_T) \neq 0\}|}{|\{e_T \in E_T | e_T \subset m \, and \, p(e_R, e_T) \neq 0\}|} \right\}$$

In the 1990s, Wan Zhexian, Feng Rongquan etc. constructed authentication codes without arbitration from geometry space of classical groups over finite fields and special matrixes over finite fields (see [2]-[6]). From the late 90s, Ma Wenping, Li Ruihu etc. constructed A^2 -code from geometry space of classical groups over finite fields (see [7]-[10]). In the present

paper, a new A^2 -code will be constructed from singular pseudo-symplectic geometry over finite fields, and the parameters and the probabilities of successful attacks of the codes are also computed.

§2.Fundamental Knowledge

Assume that F_q be a finite field with q elements of characteristic p, $q = p^\alpha$, p is a prime. Let $K_l = \begin{pmatrix} K & \\ & 0^{(l)} \end{pmatrix}$, where $K = \begin{pmatrix} 0 & I^{(\nu)} \\ -I^{(\nu)} & 0 \end{pmatrix}$. The set of all $(2\nu + l) \times (2\nu + l)$ nonsingular matrices T over F_q satisfying $TK_lT^t = K_l$ forms a group, called the singular symplectic group of degree $2\nu + l$ and index ν over F_q , denoted by $Sp_{2\nu+l,\nu}(F_q)$.

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

$$F_q^{(2\nu+l)} \times Sp_{2\nu+l,\nu}(F_q) \to F_q^{(2\nu+l)}$$
$$((x_1 \cdots, x_\nu \cdots, x_{2\nu+l}), T) \mapsto (x_1 \cdots, x_\nu \cdots, x_{2\nu+l})T.$$

The vector space $F_q^{(2\nu+l)}$ together with this action of $Sp_{2\nu+l,\nu}(F_q)$ is called the singular symplectic space over F_q . An m-dimensional subspace P of $F_q^{(2\nu+l)}$ is said to be of type(m, s), if PK_lP^t is cogredient to $M(m, s)$, where

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

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

From reference [11], we know all subspaces of type(m, s, k) in $F_q^{(2\nu+l)}$ form an orbit of subspaces under the action of $Sp_{2\nu+l,\nu}(F_q)$.

Let P be a subspace of $F_q^{(2\nu+l)}$, and define the dual subspace of P denoted by $P^\perp$:

$$P^\perp = \{x | x \in F_q^{(2\nu+l)}, xK_ly^t = 0, \forall y \in P\}.$$

§3.The Construction of A^2-code

Suppose that $n = 2\nu + l,\ \nu \geqslant 4, 1 \leqslant s < r < t < \nu$, Let U be a fixed subspace of type $(r+l, 0, 1)$ in the $(2\nu+l)$- dimensional singular symplectic space $F_q^{(2\nu+l)}$, and $U \cap E =< e_{2\nu+1} >$, then $U^{\perp}$ is a subspace of type $(2\nu - r + k, t - r, l,)$. Let the set of source states $S = \{s | s$ is a subspace of type $(2t-r+k, t-r, k)$ and $1 \leqslant k < l, U \subset s \subset U^{\perp}\}$; the set of transmitter's encoding rules $E_T = \{e_T | e_T$ is a subspace of type $(2r+1, r, 1)$ and $U \subset e_T\}$; the set of receiver's decoding rules $E_R = \{e_R | e_R$ is an m-dimensional subspace of $F_q^{(2\nu+l)}$ and $U + e_R$ is a supspace of type $(r+s+1, s, 1)\}$; the set messages $M = \{m | m$ is a subspace of type $(2t+k, t, k)$ and $U \subset m\}$.

Define the encoding map :

$$f : S \times E_T \longmapsto M,$$

$$(s, e_T) \longmapsto m = s + e_T$$

and the decoding map :

$$g : M \times E_R \longmapsto S \cup \{reject\}$$

$$(m, e_R) \longmapsto \begin{cases} s & if\ e_R \subset m, where\ s = m \cap U^{\perp} \\ reject, & if\ e_R \not\subset m \end{cases}$$

Assuming that the transmitters encoding rules and the receivers decoding rules are chosen according to a uniform probability distribution, we can assume that

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

then

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

First we prove this construction is an A^2-code.

Lemma 1 (i) For any$s \in S$ and $e_T \in E_T$, then $s + e_T = m \in M$ (ii) For any $m \in M$, and $e_T \in E_T$, $s = m \cap U^{\perp}$ is the unique source state contained in m, such that $m = s + e_T$.

Proof. (i) For any $s \in S$, $e_T \in E_T$, then let

$$s = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & 0 & R_4 & 0 & 0 & R_7 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \end{pmatrix} \begin{matrix} r \\ 2(t-r) \\ 1 \\ k-1 \end{matrix}, \quad \begin{matrix} r & \nu-r & r & \nu-r & 1 & k-1 & l-k \end{matrix}$$

and

$$sK_ls^t = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -R_4R_2^t + R_2R_4^t & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{matrix} r \\ 2(t-r) \\ k \end{matrix}$$

$$\begin{matrix} r & 2(t-r) & k \end{matrix}$$

Since s is a subspace of type $(2t-r, t-r, k)$, $rank(-R_4R_2^t+R_2R_4^t) = 2(t-r)$, $rank(sK_ls^t) = 2(t-r)$.

$$e_T = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2' & 0 & R_4' & 0 & R_6' & R_7' \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} r \\ r \\ 1 \end{matrix}$$

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

and

$$e_TK_le_T^t = \begin{pmatrix} 0 & I^{(r)} & 0 \\ -I^{(r)} & -R_4'R_2'^t + R_2'R_4'^t & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\begin{matrix} r & r & 1 \end{matrix}$$

$$\sim \begin{pmatrix} 0 & I^{(r)} & 0 \\ -I^{(r)} & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

where $\sim$ denotes the two matrices are cogredient. Hence

$$m = s + e_T = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & 0 & R_4 & 0 & 0 & R_7 \\ 0 & R_2' & 0 & R_4 & 0 & 0 & R_7' \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \end{pmatrix} \begin{matrix} r \\ 2(t-r) \\ r \\ 1 \\ k-1 \end{matrix},$$

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

then m is $(2t+k)$-dimensional subspace.Also because

$$mK_lm^t = \begin{pmatrix} 0 & 0 & I^{(r)} & 0 \\ 0 & -R_4R_2^t + R_2R_4^t & -R_4R_2'^t + R_2R_4'^t & 0 \\ -I^{(r)} & -R_4'R_2^t + R_2'R_4^t & -R_4'R_2'^t + R_2'R_4'^t & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\begin{matrix} r & 2(t-r) & r & k \end{matrix}$$

$$\sim \begin{pmatrix} 0 & 0 & I^{(r)} & 0 \\ 0 & -R_4R_2^t + R_2R_4^t & 0 & 0 \\ -I^{(r)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

where $rank(-R_4R_2^t+R_2R_4^t)=2(t-r)$, then $rank(mK_lm^t) = 2t$ and $\dim(m\cap E) = k$. Therefore m is a subspace of type $(2t+k,t,k)$, i.e. $m \in M$.

(ii) If $m \in M$, m is a subspace of type $(2t+k,t,k)$, which contains U. Then $V \subset m$, such that

$$\begin{pmatrix} U \\ V \end{pmatrix} K_l \begin{pmatrix} U \\ V \end{pmatrix}^t = \begin{pmatrix} 0 & I^{(r)} & 0 \\ -I^{(r)} & 0 & 0 \\ 0 & 0 & 0 \\ r & r & 1 \end{pmatrix}.$$

Let $m = \begin{pmatrix} U \\ V \\ P \end{pmatrix}$, such that

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

Write $s = \begin{pmatrix} U \\ P \end{pmatrix}$. Obviously, then $U \perp U$, $P \perp U$, $s \perp U$, i.e. $U \subset s \subset U^{\perp}$. s is a subspace of type $(2t-r+k, t-r, k)$, hence $s \in S$. Also because any $\nu \in V$ and $\nu \neq 0$, there always $\nu \notin s$, i.e. $V \cap U^{\perp} = \{0\}$, then $m \cap U^{\perp} = \begin{pmatrix} U \\ P \end{pmatrix} = s$. Let $e_T = \begin{pmatrix} U \\ V \end{pmatrix}$, then e_T is a transmitter's encoding rule, i.e. $e_T \in E_T$, such that $m = s + e_T$. Suppose s' is another source state contained in m. Since $U \subset s' \subset U^{\perp}$, then $s' \subset m \cap U^{\perp} = s$. And $\dim s' = \dim s$, then $s' = s$, i.e. $s = m \cap U^{\perp}$ is the unique source state contained in m.

From this lemma we know this construction is an A^2-code.

In the following we compute the parameters of this code and the probabilities of success for different types of attacks.

Lemma 2 The number of the source states is

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

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

$$\begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & 0 & R_4 & 0 & 0 & R_7 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \\ r & \nu-r & r & \nu-r & 1 & k-1 & l-k \end{pmatrix} \begin{matrix} \\ 2(t-r) \\ \\ \\ \end{matrix},$$

where $(R_2\ R_4)$ is a subspace of type $(2(t-r), t-r))$ in the $2(\nu-r)$-dimensional symplectic space and R_7 is arbitary. Hence

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

Where $N(m, s; 2\nu)$ denotes the subspace's number of type (m, s) in the 2ν-dimensional symplectic space, and $N(k, l)$ denotes the number of the k-dimensional subspaces in an l-dimensional vector space.

Lemma 3 The number of the transmitter's encoding rules is

$$|E_T| = \frac{N(r+1, 0, 1; 2r+1, r, 1; 2\nu) N(2r+1, r, 1; 2\nu)}{N(r+1, 0, 1; 2\nu)}$$

Proof. Since any transmitter's encoding rule is a subspace of type $(2r+1, r, 1)$ which contains U,

$$|E_T| = N'(r+1, 0, 1; 2r+1, r, 1; 2\nu+l, \nu)$$

$$= \frac{N(r+1, 0, 1; 2r+1, r, 1; 2\nu) N(2r+1, r, 1; 2\nu)}{N(r+1, 0, 1; 2\nu)}$$

Lemma 4 The number of the receiver's decoding rules is

$$|E_R| = q^{s(2\nu-r+l)} N(s, r)$$

Proof. e_R is an s-dimensional subspace of $F_q^{(2\nu+l)}$, and for any $e_R \in E_R, U + e_R$ is a subspace of type $(r+s+1, s, 1)$. Write e_R be

$$\begin{array}{c} \left(\begin{array}{ccccc} R_1 & R_2 & R_3 & R_4 & R_5 \\ r & \nu-r & r & \nu-r & l \end{array} \right)_s \end{array},$$

where R_3 is an s-dimensional subspace of a r- dimensional subspace, and R_1, R_2, R_4, R_5 are arbitary. Hence $|E_R| = q^{s(2\nu-r+l)} N(s, r)$.

Lemma 5 For any $m \in M$, write the number of e_T and e_R contained in m be a, b , respectively, then $a = q^{r(2t-2r+k-1)}, b = q^{s(2t-r+k)} N(s, r)$.

Proof. Let m be a message, i.e. m is a subspace of type$(2t+k, t, k)$ and $U \subset m$, m has the form as follows:

$$m = \begin{array}{c} \left(\begin{array}{cccccccc} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(t-r)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(r)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I^{(t-r)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(k)} & 0 \end{array} \right) \\ \begin{array}{cccccccc} r & t-r & \nu-t & r & t-r & \nu-t & k & l-k \end{array} \end{array}.$$

Since e_T is a subspace of type $(2r+1, r, 1)$which contains U, and $e_T \subset m$, then

$$e_T = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & 0 & I^{(r)} & R_5 & 0 & 0 & R_8 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} r \\ t-r \\ \nu-t \end{matrix} \quad \begin{matrix} r & t-r & \nu-t & 1 & k-1 & l-k \end{matrix},$$

where R_2, R_5, R_8 are arbitary. Therefore the number of e_T contained in m is

$$a = q^{2r(t-r)+r(k-1)} = q^{r(2t-2r+k-1)}.$$

Since e_R is an s-dimensional subspace and $U + e_R$ is a subspace of type $(r+s+1, s, 1)$, and $e_R \subset m$, then

$$e_R = \begin{pmatrix} R_1 & R_2 & 0 & R_4 & R_5 & 0 & R_7 & 0 \end{pmatrix} s \quad \begin{matrix} r & t-r & \nu-t & r & t-r & \nu-t & k & l-k \end{matrix},$$

where R_4 is an s-dimensional subspace of a r-dimensional subspace, and R_1, R_2, R_5, R_7 are arbitary. Hence the number of e_R contained in m is

$$b = q^{s[2(t-r)+r+k]} N(s,r) = q^{s(2t-r+k)} N(s,r).$$

Lemma 6 The number of the messages is

$$|M| = \frac{|S||E_T|}{q^{r(2t-2r+k-1)}}.$$

Proof. For any $m \in M$, it contains a unique source state $s \in S$ and $a = q^{r(2t-2r+k-1)}$ encoding rules $e_T \in E_T$, such that $m = s + e_T$. Hence $|M| = \frac{|S||E_T|}{a} = \frac{|S||E_T|}{q^{r(2t-2r+k-1)}}$.

Theorem 1 The parameters of the A^2-code are:
$|S| = q^{2(t-r)(l-k)} N(2(t-r), t-r; 2(\nu-r)) N(k-1, l-1)$.
$|M| = \frac{|S||E_T|}{q^{r(2t-2r+k-1)}}$.
$|E_T| = \frac{N(r+1,0,1;2r+1,r,1;2\nu) N(2r+1,r,1;2\nu)}{N(r+1,0,1;2\nu)}$.
$|E_R| = q^{s(2\nu-r+l)} N(s,r)$.

Lemma 7 (i) For any $e_T \in E_T$, the number of e_R contained in e_T is $c = q^{(r+1)s} N(s,r)$.(ii) For any $e_R \in E_R$, the number of e_T which contains e_R is $d = q^{(2\nu-2r+l-1)(r-s)}$.

Proof. (i) For any $e_T \in E_T$, since e_T is a subspace of type $(2r+1, r, 1)$ which contains U, assume that

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

Since e_R is an s-dimensional subspace of $F_q^{(2\nu+l)}$ and $e_R \subset e_T, U + e_R$ is a subspace of type $(r+s+1, s, 1)$. Suppose that

$$e_R = \begin{pmatrix} R_1 & 0 & R_3 & 0 & R_5 & 0 \end{pmatrix} \begin{matrix} s \end{matrix} ,$$
$$\begin{matrix} r & \nu-r & r & \nu-r & 1 & l-1 \end{matrix}$$

where R_3 is an s-dimensional subspace of a r-dimensional subspace, and R_1, R_5 are arbitary. Then the number of e_R contained in e_T is $c = q^{(r+1)s}N(s,r)$.

(ii) For any $e_R \in E_R$, suppose that

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

If $e_T \supset e_R$, then let

$$e_T = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(s)} & 0 & 0 & 0 & 0 \\ 0 & R_2 & 0 & I^{(r-s)} & R_5 & 0 & R_7 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} r \\ s \\ r-s \\ 1 \end{matrix} ,$$
$$\begin{matrix} r & \nu-r & s & r-s & \nu-r & 1 & l-1 \end{matrix}$$

where R_2, R_5, R_7 are arbitary. Then the number of e_T which contains e_R is $d = q^{(2\nu-2r+l-1)(r-s)}$.

Lemma 8 For any $m \in M$ and any $e_R \subset M$, the number of e_T which contains e_R in m is $q^{(r-s)(2t-2r+k-1)}$.

Proof. Write m be the form as in lemma 5. For any $e_R \subset m$, let

$$e_R = \begin{pmatrix} R_1 & R_2 & 0 & R_4 & R_5 & 0 & R_7 & R_8 & 0 \end{pmatrix} \begin{matrix} s \end{matrix} ,$$
$$\begin{matrix} r & t-r & \nu-t & r & t-r & \nu-t & 1 & k-1 & l-k \end{matrix}$$

where R_4 is an s-dimensional subspace of a r-dimensional subspace. If $e_T \subset m$ and $e_T \supset e_R$,then

$$e_T = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & 0 & R_4 & R_5 & 0 & 0 & R_8 & 0 \\ 0 & R_2' & 0 & R_4' & R_5' & 0 & 0 & R_8' & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} r \\ s \\ r-s \\ 1 \end{matrix} ,$$
$$\begin{matrix} r & t-r & \nu-t & r & t-r & \nu-t & 1 & k-1 & l-k \end{matrix}$$

where $\begin{pmatrix} R_4 \\ R_4' \end{pmatrix}$ is a r-dimensional subspace, and R_2', R_5', R_8' are arbitary. Then the number of e_T which contains e_R in m is

$$q^{2(r-s)(t-r)+(r-s)(k-1)} = q^{(r-s)(2t-2r+k-1)}.$$

Lemma 9 Suppose m_1 and m_2 are two distinct messages which contain a transmitter's encoding rule e_T' in common, s_1 and s_2 are the source states which contained in m_1 and m_2, respectively. Let $s_0 = s_1 \cap s_2$,dim $s_0 = k_1$, then $r+1 \leqslant k_1 \leqslant 2t-r+k-1$, and also (i) The number of e_R contained in $m_1 \cap m_2$ is $q^{k_1 s} N(s,r)$. (ii) For any $e_R \subset m_1 \cap m_2$, the number of e_T which contains e_R in $m_1 \cap m_2$ is $q^{(r-s)(k_1-r-1)}$.

Proof. For $m_1 = s_1 + e_T'$, $m_2 = s_2 + e_T'$,$m_1 \neq m_2$, therefore $s_1 \neq s_2$. Also because $s_1 \supset U, s_2 \supset U$, then $r+1 \leqslant k_1 \leqslant 2t-r+k-1$. Let s_i' be complemented subspace of s_0 in s_i , then $s_i = s_0 + s_i'.(i = 1,2)$. Since $m_i = s_i + e_T' = s_0 + s_i' + e_T'$, it is easy to know $m_1 \cap m_2 = s_0 + e_T'$.

(i) From the definition of message, suppose that m_1 and m_2 have the form as follows:

$$m_1 = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 \\ 0 & A_2 & 0 & 0 & 0 \\ 0 & 0 & I^{(r)} & 0 & 0 \\ 0 & 0 & 0 & A_4 & 0 \\ 0 & 0 & 0 & 0 & A_5 \end{pmatrix} \begin{matrix} r \\ t-r \\ r \\ t-r \\ k \end{matrix}$$
$$\begin{matrix} r & \nu-r & r & \nu-r & l \end{matrix}$$

$$m_2 = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 \\ 0 & B_2 & 0 & 0 & 0 \\ 0 & 0 & I^{(r)} & 0 & 0 \\ 0 & 0 & 0 & B_4 & 0 \\ 0 & 0 & 0 & 0 & B_5 \end{pmatrix} \begin{matrix} r \\ t-r \\ r \\ t-r \\ k \end{matrix}$$
$$\begin{matrix} r & \nu-r & r & \nu-r & l \end{matrix}$$

then

$$m_1 \cap m_2 = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 \\ 0 & C_2 & 0 & 0 & 0 \\ 0 & 0 & I^{(r)} & 0 & 0 \\ 0 & 0 & 0 & C_4 & 0 \\ 0 & 0 & 0 & 0 & C_5 \end{pmatrix} \begin{matrix} r \\ t-r \\ r \\ t-r \\ k \end{matrix} \quad . \quad (*)$$
$$\begin{matrix} r & \nu-r & r & \nu-r & l \end{matrix}$$

From above, $m_1 \cap m_2 = s_0 + e_T'$, then $\dim(m_1 \cap m_2) = k_1 + r$ .Hence

$$\dim \begin{pmatrix} 0 & C_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & C_4 & 0 \\ 0 & 0 & 0 & 0 & C_5 \end{pmatrix} = k_1 - r \ .$$

If $e_R \subset m_1 \cap m_2$, then from the definition of e_R,

$$e_R = \begin{pmatrix} R_1 & R_2 & R_3 & R_4 & R_5 \\ r & \nu-r & r & \nu-r & l \end{pmatrix}_s ,$$

where R_3 is an s-dimensional subspace of a r-dimensional subspace, and R_1, R_2, R_4, R_5 are arbitary. Hence the number of e_R in $m_1 \cap m_2$ is

$$q^{s(r+k_1-r)}N(s,r) = q^{k_1 s}N(s,r).$$

(ii) Let the represent matrix of $m_1 \cap m_2$ be as(*).Then for $e_R \subset m_1 \cap m_2$, let

$$e_R = \begin{pmatrix} R_1 & R_2 & R_3 & R_4 & R_5 \\ r & \nu-r & r & \nu-r & l \end{pmatrix}_s ,$$

where R_3 is an s-dimensional subspace of a r-dimensional subspace. If $e_T \supset e_R$ and $e_T \subset m_1 \cap m_2$, then

$$e_T = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & R_3 & R_4 & 0 & R_6 \\ 0 & R_2' & R_3' & R_4' & 0 & R_6' \\ 0 & 0 & 0 & 0 & 1 & 0 \\ r & \nu-r & r & \nu-r & 1 & l-1 \end{pmatrix} \begin{matrix} r \\ s \\ r-s \\ 1 \end{matrix} .$$

where $\begin{pmatrix} R_3 \\ R_3' \end{pmatrix}$ is r-dimensional subspace, and R_2', R_4', R_6' are arbitary. Hence the number of e_T which contains e_R in $m_1 \cap m_2$ is $q^{(r-s)(k_1-r-1)}$.

Theorem 2. In this A^2 -code, if e_T and e_R are chosen according to a uniform probability distribution, then the maximum probability of all kinds of successful attacks are:

$$P_I = \frac{1}{q^{(2\nu-2t+l-k)s}}. \quad P_S = \frac{1}{q^s}. \quad P_T = \frac{q^{r-s}-1}{q^r-1}.$$

$$P_{R_0} = \frac{1}{q^{(r-s)(2\nu-2t+l-k)}}. \quad P_{R_1} = \frac{1}{q^{r-s}}.$$

Proof. (i) Suppose that the opponents use the message m to cheat the receiver, the receiver's impersonation attack is successful if and only if the message m contains the receiver's decoding rules.Since the number of e_R contained in m is b, $P_I = \dfrac{q^{(2t-r+k)s}N(s,r)}{q^{(2\nu-r+l)s}N(s,r)} = \dfrac{1}{q^{(2\nu-2t+l-k)s}}$.

(ii) Suppose that the opponents intercept the transmitter's message m_1 and then transmit m_2 to receiver. Only if the source state s_1 which contained in the message m_1 is different to the source state s_2 contained in

the message m_2, the opponent's substitution attack is successful. Since $e_R \subset e_T \subset m_1$, the opponent's best tactics is to choose $e'_T \subset m_1$, such that $m_2 = s_2 + e'_T$, and dim $s_1 \cap s_2 = k_1$, k_1 is as large as possible. Then $P_S = \frac{q^{k_1 s} N(s,r)}{q^{(2t-r+k)s} N(s,r)}$, where when $k_1 = 2t - r + k - 1$, $P_S = \frac{1}{q^s}$ is maximum.

(iii) Suppose that the transmitter send a message m and $m \not\supset e_T$. If and only if $m \supset e_R$, the transmitter's impersonation attack is successful. Since $e_R \subset e_T$, the transmitter should select m such that the number of e_R contained in m is as much as possible, and $m \not\supset e_T$. It is easy to know the number of e_R is $q^{(r+1)s} N(s, r-1)$ at most. Since the number of e_R contained in e_T is c, $P_T = \frac{q^{(r+1)s} N(s,r-1)}{q^{(r+1)s} N(s,r)} = \frac{q^{r-s}-1}{q^r-1}$.

(iv) Suppose that the receiver claimed that it has received the message m in the case of receiving no message. If $m \supset e_T$, the receiver's impersonation attack is successful. Since $e_R \subset e_T$, the receiver should choose m such that $m \supset e_R$. Since the number of e_T which contains e_R in m is $q^{(r-s)(2t-2r+k-1)}$, $P_{R_0} = \frac{q^{(r-s)(2t-2r+k-1)}}{q^{(r-s)(2\nu-2r+l-1)}} = \frac{1}{q^{(r-s)(2\nu-2t+l-k)}}$.

(v) Suppose that the receiver after having received the message m_1, but claimed to have received another message m_2 . Only if the source state s_1 contained in m_1 must be different to the source state s_2 contained in m_2, then the receiver's substitution's attack is successful. Since $e_R \subset e_T \subset m_1$, the receiver's best tactics is to choose e'_T to meet $e_R \subset e'_T \subset m_1$, such that $m_2 = s_2 + e'_T$, and $\dim(s_1 \cap s_2) = k_1$, k_1 is as large as possible. Hence $P_{R_1} = \frac{q^{(r-s)(k_1-r-1)}}{q^{(r-s)(2t-2r+k-1)}}$, where when $k_1 = 2t - r + k - 1$, $P_{R_1} = \frac{1}{q^{r-s}}$ is maximum.

Acknowledgements

Project supported by the natural science foundation of the education department of Hebei province, China (No.Z2013085), the foundation of Tangshan science and technology bureau (No.13130245z) and the science development foundation of Tangshan Normal University (No.2013E03).

References

[1] Simmons G. J. Message authentication with arbitration of transmitter/receiver disputes[A]. In: Proc Eurocrypt87, Lecture Notes in Computer Science 304[C]. Berlin: 1987, 151-165.

[2] Wan Zhexian, Feng Rongquan. Construction of Cartesian Authentication Codes from pseudo-Symplectic Geometry [A]. HNACRYPT94[C]. Beijing: 1994. 82-86.

[3] You Hong, Gao You. Some new constructions of Cartesian authentication codes from symplectic geometry[J]. Systems Science and Mathematical Sciences, 1994, 7(4): 317-327.

[4] Gao You, Tao Yayuan. Construction of Cartesian Authentication Codes from alternate matrices over Finite Fields[J]. Applied Mathematics A Journal of Chinese Universities(Ser.A), 2007, 22A(4): 385-390.

[5] Gao Suogang, Li Zengti. Construction of Cartesian Authentication Codes from Symplectic Geometry over Finite Fields [J]. Journal of Northeast Normal University (Natural Sciences) , 2002, 34(4): 20-25.

[6] Wang Hongli. The Construction of Cartesian Authentication Code from the Vector Space over Finite Fields [J]. Computer Engineering and Applications, 2012, 48(1), 114 -115, 149.

[7] Ma Wenping, Wang Xinmei. A Construction of Authentication Codes with Arbitration Over Symplectic Space [J]. Chinese Journal of Computers1999, 22(9): 949-952.

[8] Li Zhihui, Li Ruihu. Construction of Authentication Codes with Arbitration from Pseudo-Symplectic Geometry [J]. Journal of Lanzhou University (Natural Sciences), 2005, 41(5), 123-126.

[9] Yu Huafeng, Gao You. Construction of authentication codes with arbitration from alternate matrices over finite fields [J]. Journal of Natural Science of Heilongjiang University, 2012,29(1), 42-50.

[10] Yue Mengtian, Li Zengti. Construction of Authentication Codes with Arbitration from Orthogonal Geometries in odd characteristic[J]. Journal of Hebei Normal University(Natural Science Edition), 2013,37(3),217-221. 2008,30(2), pp. 65-70.

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