A New Construction of A^2 Authentication Codes from Singular Pseudo-Symplectic Geometry over Finite Fields

You Gao *, Liwei Chang

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

Abstract: A new construction of authentication codes with arbitration using singular pseudo-symplectic geometry on finite fields is given. Some parameters and the probabilities of success for different types of deceptions are computed.

Keywords: authentication codes with arbitration; singular pseudo-symplectic geometry; finite fields.

1. Introduction and main results

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

Let S, E_T,E_R and M be four non-empty finite sets, $f : S \times E_T \to M$ and $g : M \times E_R \to S \cup \{reject\}$ 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

(1) The maps f and g are surjective;

(2) 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;

(3) $p(e_T, e_R) \neq 0$ and $f(s, e_T) = m$ implies $g(m, e_R) = s$, otherwise, $g(m, e_R)$

$= \{reject\}$.

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

*Correspondence : College of Science, Civil Aviation University of China,Tianjin,300300, P.R.China; E-mail:gao_you@263.net .

the set of 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 attendances: 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

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

3) The transmitter's impersonation attack: the largest probability of a transmitter's successful impersonation attack is P_T . Then

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

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

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

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

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

Notes: $p(e_R, e_T) \neq 0$ implies that any information s encoded by e_T can be authenticated by e_R.

In this paper, the ${}^tP$ denotes the transpose of a matrix P. Some concepts and notations refer to [2].

Suppose that $\mathbb{F}_q$ is a finite field of characteristic 2, $n = 2\nu + \delta + l$ and $\delta = 1, 2$. let

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

where S_δ is the $(2\nu + \delta) \times (2\nu + \delta)$ non-alternate symmetric matrix:

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

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

$$P_{S_{2\nu+\delta+l,2\nu+\delta}}(F_q) = \{g : gS_{\delta,l}g^T = S_{\delta,l}\}$$

denoted by $P_{S_{2\nu+\delta+l,2\nu+\delta}}(F_q)$.

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

$$F_q^{(2\nu+\delta+l)} \times P_{S_{2\nu+\delta+l,2\nu+\delta}}(F_q) \mapsto F_q^{(2\nu+\delta+l)}$$

$$((x_1, x_2, \cdots, x_{2\nu+\delta+l}), T) \mapsto (x_1, x_2, \cdots, x_{2\nu+\delta+l})T. \qquad (1)$$

The vector space $F_q^{(2\nu+\delta+l)}$ together with this action of the group $P_{S_{2\nu+\delta+l,2\nu+\delta}}(F_q)$ is called the singular pseudo -symplectic space of dimension $(2\nu + \delta + l)$ over F_q. An m-dimensional subspace P of $F_q^{(2\nu+\delta+l)}$ 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 $M(m, 2s + \tau, s)$. More properties of geometry of singular pseudo-symplectic groups over finite fields of characteristic 2 can be found in[2].

Wan Zhexian, Feng Rongquan, You Hong etc.constructed authentication codes without arbitration from geometry space of classical groups over finite fields [3–5]. Ma Wenping, Li Ruihu, Chen

Shangdi etc. constructed A^2-code from geometry space of non-singular classical groups over finite fields[6-8]. In the present paper, a new A^2-code will be constructed from singular pseudo-symplectic geometry over finite fields, the parameters and the probabilities of successful attacks of these codes are also computed.

2. Construction

Suppose that $n = 2\nu+2+l$, $2 \le r < t < \nu$, $\nu \ge 5$, *and* $1 \le k < l$. Let U be a fixed subspace of type $(r+2, 0, 0, 1, 1)$ and $U \cap E = \langle e_{2\nu+3} \rangle$ 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 $(2\nu-r+1+l, 2(v-r), v-r, 1, l)$; the set of source states $S = \{s | s$ is a subspace of type $(2t-r+1+k, 2(t-r), t-r, 1, k)$ and $U \subset S \subset U^\perp\}$; the set of transmitter's encoding rules $E_T = \{e_T | e_T$ is a subspace of type $(2r+2, 2r, r, 1, 1)$ and $U \subset e_T\}$; the set of receiver's decoding rules $E_R = \{e_R | e_R$ is a subspace of type $(2r, 2(r-2), r-2, 1, 1)$ and $U \subset e_R\}$; the set of messages $M = \{m | m$ is a subspace of type $(2t+1+k, 2t, t, 1, k)$ and $U \subset m$, $m \cap U^\perp$ is a subspace of type $(2t-r+1+k, 2(t-r), t-r, 1, k)\}$.
Define the encoding map:

$$f : S \times E_T \to M,\ (s, e_T) \to m = s + e_T$$

and the decoding map:

$$g : M \times E_R \to s \cup \{reject\}$$

$$(m, e_R) \longmapsto \begin{cases} s & \text{if } e_R \subset m, \text{where } s = m \cap U^\perp. \\ \{\text{reject}\} & \text{otherwise.} \end{cases}$$

We know the six tuple (S, E_T, E_R, M, f, g) is an authentication code with arbitration.
Assuming the transmitter's encoding rules and the receiver's decoding rules are chosen according to a uniform probability distribution, we can assume that

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

and

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

Lemma 2.1 The above construction of 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 $s \in S$, $e_T \in E_T$, from the definition of s, we can assume that

$$s = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & 0 & R_4 & 0 & 0 & 0 & 0 & R_9 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \end{pmatrix} \begin{matrix} r \\ 2(t-r) \\ 1 \\ 1 \\ k-1 \end{matrix}$$
$$\begin{matrix} r & \nu-r & r & \nu-r & 1 & 1 & 1 & k-1 & l-k \end{matrix}$$

then

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

since rank $(sS_{2,l}{}^t s) = 2(t-r)$, rank$(R_4{}^t R_2 + R_2{}^t R_4) = 2(t-r)$. Then we can assume that

$$e_T = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2' & R_3' & R_4' & 0 & 0 & 0 & R_8' \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} r \\ r \\ 1 \\ 1 \end{matrix}$$
$$\begin{matrix} r & \nu-r & r & \nu-r & 1 & 1 & 1 & l-1 \end{matrix}$$

then

$$e_T S_{2,l}{}^t e_T = \begin{pmatrix} 0 & {}^tR_3' & 0 & 0 \\ R_3' & R_4'\,{}^tR_2' + R_2'\,{}^tR_4' & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} r \\ r \\ 1 \\ 1 \end{matrix}$$
$$\begin{matrix} r & r & 1 & 1 \end{matrix}$$

and

$$e_T S_{2,l}{}^t e_T = \begin{pmatrix} 0 & I^{(r)} & 0 & 0 \\ I^{(r)} & R_4'\,{}^tR_2' + R_2'\,{}^tR_4' & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$
$$\sim \begin{pmatrix} 0 & I^{(r)} & 0 & 0 \\ I^{(r)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Hence we have

$$m = s + e_T = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & 0 & R_2 & 0 & 0 & 0 & 0 \\ 0 & R_2 & 0 & R_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(k)} & 0 \end{pmatrix} \begin{matrix} r \\ 2t-2r \\ r \\ 1 \\ k \end{matrix}$$
$$\begin{matrix} r & \nu-r & r & \nu-r & 1 & 1 & k & l-k \end{matrix}$$

thus m is a $2t + 1 + k$ dimensional subspace and

$$mS_{2,l}{}^t m = \begin{pmatrix} 0 & 0 & I^{(r)} & 0 & 0 \\ 0 & R_4{}^tR_2' + R_2{}^tR_4 & R_4'{}^tR_2' + R_2'{}^tR_4' & 0 & 0 \\ I^{(r)} & R_4{}^tR_2' + R_2{}^tR_4 & R_4'{}^tR_2' + R_2'{}^tR_4' & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\sim \begin{pmatrix} 0 & 0 & I^{(r)} & 0 & 0 \\ 0 & R_4{}^tR_2' + R_2{}^tR_4 & 0 & 0 & 0 \\ I^{(r)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

where $\mathrm{rank}(R_4{}^tR_2' + R_2{}^tR_4) = 2(t-r)$. Therefore, $\mathrm{rank}(mS_{2,l}{}^tm) = 2t$, $\dim(m \cap E) = k$. so m is a subspace of type$(2t+1+k, 2t, t, 1, k)$ containing U,i.e.,$m \in M$.

(2) For $m \in M$, m is a subspace of type $(2t+1+k, 2t, t, 1, k)$ containing U. So there is subspace $V \subset m$, satisfying

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

Then we can assume that

$$m = \begin{pmatrix} U \\ V \\ P \end{pmatrix}$$

satisfying

$$\begin{pmatrix} U \\ V \\ P \end{pmatrix} S_{2,l} \begin{pmatrix} U \\ V \\ P \end{pmatrix}^T = \begin{pmatrix} 0 & I^{(r)} & 0 & 0 & 0 \\ I^{(r)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(t-r)} & 0 \\ 0 & 0 & I^{(t-r)} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Let $s = \begin{pmatrix} U \\ P \end{pmatrix}$, then s is a subspace of type $(2t-r+1+k, 2(t-r), t-r, 1, k)$ 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 $e_T = \begin{pmatrix} U \\ V \end{pmatrix}$, then e_T is a transmitter's encoding rule and satisfying $m = s + e_T$.

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

Lemma 2.2 The number of the source states is $|S| = q^{2(t-r)(l-k)} N(2(t-r), 2(t-r), t-r), 0; 2(v-r))N(k-1, l-1)$.

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

$$s = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & 0 & R_4 & 0 & 0 & 0 & 0 & R_9 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \\ r & \nu-r & r & \nu-r & 1 & 1 & 1 & k-1 & l-k \end{pmatrix} \begin{matrix} r \\ 2(t-r) \\ 1 \\ 1 \\ k-1 \end{matrix}$$

where (R_2, R_4) is a subspace of type $(2(t-r), 2(t-r), t-r, 0)$ in the pseudo-symplectic space $F_q^{2(\nu-r)}$. Therefore, the number of the source states is

$$|S| = q^{2(t-r)(l-k)} N(2(t-r), 2(t-r), t-r), 0; 2(v-r)) N(k-1, l-1).$$

Lemma2.3 The number of the encoding rules of transmitter is $|E_T| = N'(r+2, 0, 0, 1, 1; 2r+2, 2r, r, 1, 1; 2\nu+2+l, 2\nu+2)$.

Proof: Since e_T is a subspace of type $(2r+2, 2r, r, 1, 1)$ containing U.

Lemma 2.4 The number of the decoding rules of receiver is $|E_R| = N'(r+2, 0, 0, 1, 1; 2r, 2(r-2), r-2, 1, 1; 2\nu+2+l, 2\nu+2)$.

Proof: Since e_R is a subspace of type $(2r, 2(r-2), r-2, 1, 1)$ containing U.

Lemma 2.5 (1)The number of encoding rules e_T and e_R contained in m respectively is
$a = q^{2r(t-r)+r(k-1)}$ and $b = q^{2(r-2)(t-r)+(r-2)(k-1)} N(r-2, r)$;
(2)The number of the messages is $|M| = |S||E_T|/a$.

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

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

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

$$e_T = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & 0 & I^{(r)} & R_5 & 0 & 0 & 0 & 0 & R_{10} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} r \\ r \\ 1 \\ 1 \end{matrix}$$
$$\begin{matrix} r & t-r & \nu-t & r & t-r & \nu-t & 1 & 1 & 1 & k-1 & l-k \end{matrix}$$

where R_2, R_5, R_{10} arbitrarily. Therefore, the number of e_T containing U is $a = q^{2r(t-r)+r(k-1)}$. Like that if $e_R \subset m$, then we can assume that

$$e_R = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R'_2 & 0 & R'_4 & R'_5 & 0 & 0 & 0 & 0 & R'_{10} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} r \\ r-2 \\ 1 \\ 1 \end{matrix}$$
$$\begin{matrix} r & t-r & \nu-t & r & t-r & \nu-t & 1 & 1 & 1 & k-1 & l-k \end{matrix}$$

where R'_4 is a $r-2$ dimensional subspace of r dimensional subspace and R'_2, R'_5, R'_{10} arbitrarily. Therefore, the number of e_R containing U is $b = q^{2(r-2)(t-r)+(r-2)(k-1)}N(r-2,r)$.

(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 $a = q^{2r(t-r)+r(k-1)}$. Therefore we have $|M| = |S||E_T|/a$.

Lemma 2.6 (1) For any $e_T \in E_T$, the number of e_R which is incidence with e_T is $c = N(r-2,r)$.
(2) For any $e_R \in E_R$, the number of e_T which is incidence with e_R is $d = q^{4(\nu-r)+2(l-1)}$.

Proof. (1) Assume that $e_T \in E_T$, e_T is a subspace of type $(2r+2, 2r, r, 1, 1)$ containing U, we may take e_T as follows

$$e_T = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(r)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

If $e_R \subset e_T$ and e_R is a subspace of type $(2r, 2(r-2), r-2, 1, 1)$

containing U, then we can assume

$$e_R = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} r \\ r-2 \\ 1 \\ 1 \end{matrix}$$

where R_3 is a $r-2$ dimensional vector subspace of r dimensional vector space. Therefore the number of e_R which is incidence with e_T is $c = N(r-2, r)$.

(2)$\forall e_R \in E_R$, from the definition of e_R, we can assume that

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

If $e_T \supset e_R$ then

$$e_T = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & 0 & I^{(2)} & R_5 & 0 & 0 & 0 & R_9 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} r \\ r-2 \\ 2 \\ 1 \\ 1 \end{matrix}$$
$$\begin{matrix} r & \nu-r & r-2 & 2 & \nu-r & 1 & 1 & 1 & l-1 \end{matrix}$$

where R_2, R_5, R_9 arbitrarily, so the number of e_T which is incidence with e_R is $d = q^{4(\nu-r)+2(l-1)}$.

Lemma 2.7 For any $m \in M$ and $e_R \subset m$, the number of e_T contained in m and containing e_R is $q^{4(t-r)+2(k-1)}$.

Proof. The matrix of m is similar to lemma 2.5, then for any $e_R \subset m$, assume that

$$e_R = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & 0 & R_4 & R_5 & 0 & 0 & 0 & 0 & R_{10} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} r \\ r-2 \\ 1 \\ 1 \end{matrix}$$
$$\begin{matrix} r & t-r & \nu-t & r & t-r & \nu-t & 1 & 1 & 1 & k-1 & l-k \end{matrix}$$

where R_4 is a $r-2$ dimensional vector subspace of r dimensional vector subspace. If $e_T \subset m$ and $e_T \supset e_R$, therefore

$$e_T = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & 0 & R_4 & R_5 & 0 & 0 & 0 & 0 & R_{10} & 0 \\ 0 & R_2' & 0 & R_4' & R_5' & 0 & 0 & 0 & 0 & R_{10}' & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} r \\ r-2 \\ 2 \\ 1 \\ 1 \end{matrix}$$

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

where $\begin{pmatrix} R_4 \\ R_4' \end{pmatrix}$ is nonsingular, and R_2', R_5', R_{10}' arbitrarily, then the number of e_T contained in m and containing e_R is $q^{4(t-r)+2(k-1)}$.

Lemma 2.8 Suppose that m_1 and m_2 are two distinct messages which commonly contain a transmitter's encoding rule e_T'. s_1 and s_2 contained in m_1 and m_2 are two source states, respectively. Assume that $s_0 = s_1 \cap s_2$, dim $s_0 = k_1$, then $r+2 \leq k_1 \leq 2t-r+k$, and

(1) The number of e_R contained in $m_1 \cap m_2$ is $N(r-2,r)q^{(r-2)(k_1-r-2)}$;

(2) $\forall e_R \subset m_1 \cap m_2$, the number of e_T contained in $m_1 \cap m_2$ and containing e_R is $q^{2(k_1-r-2)}$.

Proof. Since $m_1 = s_1 + e_T', m_2 = s_2 + e_T'$ and $m_1 \neq m_2$, then $s_1 \neq s_2$. Because of $U \subset s_1, s_2$, therefore, $r+2 \leq k_1 \leq 2t-r+k$.

(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 $s_i = m_i \cap U^{\perp}$ $(i=1,2)$, we have $s_0 = (m_1 \cap U^{\perp}) \bigcap (m_2 \cap U^{\perp}) = m_1 \cap m_2 \cap U^{\perp} = s_1 \cap m_2 = s_2 \cap m_1$ and $m_1 \cap m_2 = (s_1 + e_T') \cap m_2 = (s_0 + s_1' + e_T') \cap m_2 = ((s_0 + e_T') + s_1') \cap m_2$. Because $s_0 + e_T' \subset m_2$, $m_1 \cap m_2 = (s_0 + e_T') + (s_1' \cap m_2)$. While $s_1' \cap m_2 \subseteq s_1 \cap m_2 = s_0$, $m_1 \cap m_2 = s_0 + e_T'$. Therefore dim $(m_1 \cap m_2) = k_1 + r$. From $e_T' \subset m_1 \cap m_2$ we can assume that

$$e_T' = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(r)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

and from the definition of the message, we may take m_1 as follows,

$$m_1 = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(r)} & 0 & 0 & 0 & 0 & 0 \\ 0 & A_2 & 0 & A_4 & 0 & 0 & 0 & A_8 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & A'_8 \end{pmatrix} \begin{matrix} r \\ r \\ 2(t-r) \\ 1 \\ 1 \\ k-1 \end{matrix}$$
$$\begin{matrix} r & \nu-r & r & \nu-r & 1 & 1 & 1 & l-1 \end{matrix}$$

because the type of m_2 is the same as m_1, therefore

$$m_1 \cap m_2 = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(r)} & 0 & 0 & 0 & 0 & 0 \\ 0 & C_2 & 0 & C_4 & 0 & 0 & 0 & C_8 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & C'_8 \end{pmatrix} \begin{matrix} r \\ r \\ 2(t-r) \\ 1 \\ 1 \\ k-1 \end{matrix}$$
$$\begin{matrix} r & \nu-r & r & \nu-r & 1 & 1 & 1 & l-1 \end{matrix}$$

since $\dim(m_1 \cap m_2) = k_1 + r$.

$$dim \begin{pmatrix} 0 & C_2 & 0 & C_4 & 0 & 0 & 0 & C_8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & C'_8 \end{pmatrix} = k_1 - r - 2$$

If for any $e_R \subset m_1 \cap m_2$, then

$$e_R = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & R_3 & R_4 & 0 & 0 & 0 & R_8 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} r \\ r-2 \\ 1 \\ 1 \end{matrix}$$

where the number of R_3 is $N(r-2, r)$ and every row of $(0\, R_2\, 0\, R_4\, 0\, 0\, 0\, R_8)$ is the linear combination of $\begin{pmatrix} 0 & C_2 & 0 & C_4 & 0 & 0 & 0 & C_8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & C'_8 \end{pmatrix}$. So it is easy to know that the number of e_R contained in $m_1 \cap m_2$ is $N(r-2, r)q^{(r-2)(k_1-r-2)}$.

(2) Suppose that $m_1 \cap m_2$ has the form of (1), then for any $e_R \subset m_1 \cap m_2$, we can assume that if $e_T \subset m_1 \cap m_2$ and $e_R \subset e_T$,

then e_T has the form as follows

$$e_T = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & R_3 & R_4 & 0 & 0 & 0 & R_8 \\ 0 & R_2' & R_3' & R_4' & 0 & 0 & 0 & R_8' \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} r \\ r-2 \\ 2 \\ 1 \\ 1 \end{matrix}$$

where $\begin{pmatrix} R_3 \\ R_3' \end{pmatrix}$ is nonsingular, every row of $(0\ R_2'\ 0\ R_4'\ 0\ 0\ 0\ R_8')$ is the linear combination of $\begin{pmatrix} 0 & C_2 & 0 & C_4 & 0 & 0 & 0 & C_8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & C_8' \end{pmatrix}$. Then the number of e_T contained in $m_1 \cap m_2$ and containing e_R is $q^{2(k_1-r-2)}$.

Theorem 2.1 The parameters of constructed authentication codes with arbitration are
$|S| = q^{2(t-r)(l-k)} N(2(t-r), 2(t-r), t-r), 0; 2(v-r))N(k-1, l-1);$
$|E_T| = N'(r+2, 0, 0, 1, 1; 2r+2, 2r, r, 1, 1; 2\nu+2+l, 2\nu+2);$
$|E_R| = N'(r+2, 0, 0, 1, 1; 2r, 2(r-2), r-2, 1, 1; 2\nu+2+l, 2\nu+2);$
$|M| = |S||E_T|/a.$

Theorem 2.2 In the A^2 authentication codes, if the transmitter's encoding rules and the receiver's decoding rules are chosen according to a uniform probability distribution, the largest probabilities of success for different types of deceptions:

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

$$P_{R_0} = \frac{1}{q^{4(\nu-t)+2(l-k)}}; \quad P_{R_1} = \frac{1}{q^2}.$$

Proof. (1) The number of the transmitter's encoding rules contained in a message is b, then

$$P_I = \max_{m \in M} \left\{ \frac{|\{e_R \in E_R | e_R \subset m\}|}{|E_R|} \right\} = \frac{b}{|E_R|} = \frac{1}{q^{(r-2)(2\nu-2t+l-k+1)}}.$$

(2) Assume that opponent gets m_1 which is from transmitter and sends m_2 instead of m_1, when s_1 contained in m_1 is different from s_2 contained in m_2, the opponent's substitution attack can

success. Because $e_R \subset e_T \subset m_1$, thus the opponent select $e_T' \subset m_1$, satisfying $m_2 = s_2 + e_T'$ and $\dim(s_1 \bigcap s_2) = k$, then

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

$$= \frac{N(r-2,r)q^{(r-2)(k_1-r-2)}}{b},$$

where $k_1 = 2t - r + k, P_s == \frac{1}{q^{(r-2)}}$ is the largest.

(3) Let e_T be a transmitter's secret encoding rule, s be a source state and m_1 a the message corresponding to the source state s encoded by e_T. Then the number of the receiver's decoding rules contained in m_1 is e_R. Assume that m_2 is a distinct message corresponding to s, but m_2 cannot be encoded by e_T. Then $m_1 \cap m_2$ contains $N(r-2, r-1)$ receiver's decoding rules at most.

We can assume that $e_T = U \oplus \omega$, $\dim(\omega) = 2r+2-r-2 = r$ and $m = U \oplus \Omega$, $\dim(\Omega) = 2t - 1 + k - r$; since $U \subset e_R \subset e_R \cap m$, then $e_R = e_R \cap e_T = U \oplus (e_R \cap \omega) = e_R \cap m = U \oplus (e_R \cap \Omega) = U \oplus (e_R \cap \omega \cap \Omega)$ where $\dim(e_R \cap \omega \cap \Omega) = r-2$, $e_R \cap \omega \cap \Omega$ is a $r-2$ dimensional subspace of $\omega \cap \Omega$, and $e_T \subsetneq m$, then $\dim(\omega \cap \Omega) \leq r-1$ when $\dim(\omega \cap \Omega) = r-1$, we can assume

$$e_T = \begin{pmatrix} U \\ \omega \cap \Omega \\ e_{v+r} \end{pmatrix} = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & I^{(r-1)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} r \\ 1 \\ 1 \\ r-1 \\ 1 \end{matrix},$$

where $e_T \cap m = \begin{pmatrix} U \\ \omega \cap \Omega \end{pmatrix}$ and $\omega \cap \Omega = (0\ 0\ I^{(r-1)}\ 0\ 0\ 0\ 0\ 0\ 0)$ since $e_R \subset e_T$,

$$e_R = \begin{pmatrix} U \\ e_R \cap \omega \cap \Omega \end{pmatrix} = \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} r \\ r-2 \\ 1 \\ 1 \end{matrix},$$

where $e_R \cap \omega \cap \Omega = (\ 0\ \ 0\ \ R_3\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ )$, then $e_R \cap \omega \cap$

Ω is a $r-2$ dimensional subspace of $\omega \cap \Omega$, the number of R_3 is $N(r-2,r-1)$, so the largest number of the e_R is $N(r-2,r-1)$, the number of e_R which is incidence with e_T is $c = N(r-2,r)$. Therefore the probability of transmitter's successful impersonation attack is

$$P_T = \max_{e_T \in E_T} \left\{ \frac{\max\limits_{m \in M, e_T \not\subset m} | \{e_R \in E_R | e_R \subset m \cap e_T\} |}{| \{e_R \in E_R | e_R \subset e_T\} |} \right\}$$

$$= \frac{N(r-2,r-1)}{N(r-2,r)} = \frac{q^2-1}{q^r-1}.$$

(4) Let e_R be a the receiver's decoding rule, we have known that the number of transmitter's encoding rules containing e_R is $d = q^{4(\nu-r)+2(l-1)}$ and a message containing e_R has $q^{4(t-r)+2(k-1)}$ transmitter's encoding rules. Hence the probability of receiver's successful impersonation attack is

$$P_{R_0} = \max_{e_R \in E_R} \left\{ \frac{\max\limits_{m \in M} | \{e_T \in E_T | e_T \subset m \text{ and } e_R \subset e_T\} |}{| \{e_T \in E_T | e_R \subset e_T\} |} \right\}$$

$$= \frac{q^{4(t-r)+2(k-1)}}{q^{4(\nu-r)+2(l-1)}} = \frac{1}{q^{4(\nu-t)+2(l-k)}}.$$

(5) Assume that the receiver declares to receive a message m_2 instead of m_1, when s_1 contained in m_1 is different from s_2 contained in m_2, the receiver's substitution attack can be successful. Since $e_R \subset e_T \subset m_1$, the receiver is superior to select $e_T^{'}$, satisfying $e_R \subset e_T^{'} \subset m_1$, thus $m_2 = s_2 + e_T^{'}$ and $\dim(s_1 \cap s_2) = k_1$ as large as possible. Therefore, the probability of a receiver's successful substitution attack is

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

$$= \frac{q^{2(k_1-r-2)}}{q^{2(2(t-r)+k-1)}},$$

where $k_1 = 2t - r + k$, $P_{R_1} = \frac{1}{q^2}$ is the largest.

Acknowledgements

This work is supported by the National Natural Science Foundation of China under Grant No. 61179026 and the Natural Science Foundation of Tianjin City in China under Grant No. 08JCYBJC13900.

References

[1] G.J. Simmons. Message authentication with arbitration of transmitter/receiver disputes. Proc. Eurcrypt 87. Lecture Notes in Computer Science, 1987(304):151-165.

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

[3] Wan ZheXian, Feng Rongquan. Construction of Cartesian Authentication Codes from pseudo-Symplectic Geometry [C].CHNACRYPT'94,Beijing:1994,82-86.

[4] 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.

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

[6] Ma Wenping,Wang Xinmei. A Construction of Authentication Codes with Arbitration Based on Symplectic Space (in Chinese)[J].Chinese Journal of Computers, 1999,229:949-952.

[7] Li Zhihui,Li Ruihu.Construction of Authentication Codes with Arbitration from Pseudo-Symplectic Geometry(in Chinese)[J].Journal of Lanzhou University (Natural Sciences), 2005,415:123-126.

[8] Chen Shangdi, Zhao Dawei.New Construction of Authentication Codes with Arbitration from Pseudo-Symplectic Geometry over Finite Fields[J].ARS COMBINTARIA 97A.2010:453-465.