A New Construction of Authentication Code with Arbitration from $(2\nu+2+l)$-dimensional Singular Pseudo-Symplectic Space

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 from $(2\nu+2+l)$-dimensional singular pseudo-symplectic geometry on finite fields is given . Assuming that the encoding rules are chosen according to a uniform probability distribution, the parameters and the probabilities of success for different types of deceptions are also computed.

Keywords: authentication codes; arbitration; construction; singular pseudo-symplectic geometry

1. Introduction and main results

To solve the distrust problem of the transmitter and the receiver in the communications system, Simmons[1] introduced a model of authentication codes with arbitration, 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 the transmitter's encoding rules, the set of the receiver's decoding rules and 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 parameters of this code.

In an authentication system that permits arbitrations, this model includes four attendance: the transmitter, the receiver, the opponent and the arbiter, and includes five attacks: the opponent's impersonation attack, the

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

opponent's substitution attack, the transmitter's impersonation attack, the receiver's impersonation attack and the receiver's substitution attack.

Wan Zhexian , Feng Rongquan, You Hong etc. constructed authentication codes without arbitration from geometry space of classical groups over finite fields [2-4]. Ma Wenping, Li Ruihu Chen Shangdi etc. constructed A^2-code from geometry space of classical groups over finite fields[5-7]. 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 this authentication codes are also computed.

Assume that 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 pseudo-symplectic group of degree $2\nu+\delta+l$ over F_q is defined to be the set of matrices

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

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

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

$$F_q^{(2\nu+\delta+l)} \times Ps_{2\nu+\delta+l,2\nu+\delta}(F_q) \longrightarrow F_q^{(2\nu+\delta+l)}$$

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

The vector space $F_q^{(2\nu+\delta+l)}$ together with this action 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 $PS_{\delta,l}{}^tP$ is cogredient to $M(m, 2s+\tau, s)$ and P does not or does contain a vector of the form

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

corresponding to the cases $\varepsilon = 0$ or 1, respectively. Let E be the subspace of $F_q^{(2\nu+\delta+l)}$ generated by $e_{2\nu+\delta+1}, \cdots, e_{2\nu+\delta+l}$, then $dim E = l$. An m -dimensional subspace P of $F_q^{(2\nu+\delta+l)}$ is called a subspace of type $(m, 2s+\tau, s, \varepsilon, k)$, if

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

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

From [8] we know that the set of all subspaces of type $(m, 2s+\tau, s, \varepsilon, k)$ in $F_q^{(2\nu+\delta+l)}$ forms an orbit under $Ps_{2\nu+\delta+l, 2\nu+\delta}(F_q)$. Let P is a subspace of $F_q^{(2\nu+\delta+l)}$, we define the dual subspace of P is

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

2. Construction

Suppose that $n = 2\nu+2+l, 2 \leq r_2 < r_1 < \nu$, $\nu \geq 5$ and $1 \leq k_2 < k_1 < l$. Let U be a fixed subspace of type $(3,0,0,0,1)$ in the $(2\nu+2+l)$-dimensional singular pseudo-symplectic space $\mathbb{F}_q^{(2\nu+2+l)}$, then $U^{\perp}$ is a subspace of type $(2\nu+l, 2\nu-2, \nu-2, 1, l)$; P_0 is a fixed subspace of type $(r_1+k_1, 0, 0, 0, k_1)$ and $U \subset P_0 \subset U^{\perp}$; the set of source states $S = \{s | s$ is a subspace of type $(r_2+k_2, 0, 0, 0, k_2)$ and $U \subset S \subset P_0\}$; the set of the transmitter's encoding rules $E_T = \{e_T | e_T$ is a subspace of type $(5,4,2,0,1), U \subset e_T$ and $e_T \cap P_0 = U\}$; the set of the receiver's decoding rules $E_R = \{e_R | e_R$ is a subspace of type (4,2,1,0,1) and $U \subset e_R\}$; the set of messages $M = \{m | m$ is a subspace of type $(r_2+2+k_2, 4, 2, 0, k_2)$ and $U \subset m$, $m \cap P_0$ is a subspace of type $(r_2+k_2, 0, 0, 0, k_2)\}$.

Define the encoding map:

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

and the decoding map:

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

$$(m, e_R) \longmapsto \begin{cases} s & \text{if } e_R \subset m, where\, s = m \cap P_0. \\ \{\text{reject}\} & \text{otherwise.} \end{cases}$$

We know the six-tuple (S, E_T, E_R, M, f, g) is an authentication code with arbitration.

Let n_1 denote the number of subspaces of type $(r_2+k_2, 0, 0, 0, k_2)$ contained in $U^{\perp}$ and containing U; n_2 denote the number of subspaces of type $(r_1+k_1, 0, 0, 0, k_1)$ contained in $U^{\perp}$ and containing a fixed subspace of type $(r_2+k_2, 0, 0, 0, k_2)$ as above; and n_3 denote the number of subspaces of type $(r_1+k_1, 0, 0, 0, k_1)$ contained in $U^{\perp}$ and containing U.

Lemma 2.1 (1) $n_1 = N(r_2-2,0,0,0;2\nu-2)N(k_2-1,l-1)q^{(r_2-2)(l-k_2)}$;
(2) $n_2 = N(r_1-r_2,0,0,0;2\nu+2-2r_2)N(k_1-k_2,l-k_2)q^{(l-k_1)(r_1-r_2)}$;
(3) $n_3 = N(r_1-2,0,0,0;2\nu-2)N(k_1-1,l-1)q^{(r_1-2)(l-k_1)}$.

Proof. (1) We can assume that s is a subspace of type $(r_2+k_2,0,0,0,k_2)$ and $U \subset s \subset U^{\perp}$. Clearly, s has a form as follows

$$s = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k_2-1)} & 0 \\ 0 & 0 & R_3 & R_4 & 0 & 0 & R_7 & R_8 & R_9 & R_{10} & 0 & 0 & R_{13} \end{pmatrix} \begin{matrix} 1 \\ 1 \\ 1 \\ k_2-1 \\ r_2-2 \end{matrix}$$
$$\begin{matrix} 1 & 1 & r_2-2 & \nu-r_2 & 1 & 1 & r_2-2 & \nu-r_2 & 1 & 1 & 1 & k_2-1 & l-k_2 \end{matrix}$$

where $(R_3, R_4, R_7, R_8, R_9, R_{10})$ is a vector subspace of type $(r_2-2,0,0,0)$ in the pseudo-symplectic space $F_q^{(2\nu-2)}$ and R_{13} is arbitrary. Therefore, $n_1 = N(r_2-2,0,0,0;2\nu-2)N(k_2-1,l-1)q^{(r_2-2)(l-k_2)}$.

(2) Suppose that P is a subspace of type $(r_1+k_1,0,0,0,k_1)$ containing a fixed subspace of type $(r_2+k_2,0,0,0,k_2)$ as above and $P \subset U^{\perp}$. It is easy to know that P has a form as follows

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(r_2-2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k_2)} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k_1-k_2)} & 0 \\ 0 & 0 & 0 & R_4 & 0 & 0 & 0 & R_8 & R_9 & R_{10} & 0 & 0 & R_{13} \end{pmatrix} \begin{matrix} 1 \\ 1 \\ r_2-2 \\ k_2 \\ k_1-k_2 \\ r_1-r_2 \end{matrix}$$
$$\begin{matrix} 1 & 1 & r_2-2 & \nu-r_2 & 1 & 1 & r_2-2 & \nu-r_2 & 1 & 1 & k_2 & k_1-k_2 & l-k_1 \end{matrix}$$

where (R_4, R_8, R_9, R_{10}) is a subspace of type $(r_1-r_2,0,0,0)$ in the pseudo-symplectic space $F_q^{(2\nu+2-2r_2)}$ and R_{13} is arbitrary. Therefore, $n_2 = N(r_1-r_2,0,0,0;2\nu+2-2r_2)N(k_1-k_2,l-k_2)q^{(l-k_1)(r_1-r_2)}$.

(3) Similar to the proof of (1), we have $n_3 = N(r_1-2,0,0,0;2\nu-2)N(k_1-1,l-1)q^{(r_1-2)(l-k_1)}$.

Lemma 2.2 The number of the source states is

$$|S| = \frac{n_1 \cdot n_2}{n_3} = \frac{q^{(r_2-2)(2(r_2-r_1)+(k_1-k_2))}N(k_2-1,l-1)N(k_1-k_2,l-k_2)}{N(k_1-1,l-1)}$$

Lemma 2.3 The number of the encoding rules of the transmitter is

$$|E_T| = q^{2(2\nu-4+l)}$$

Proof. Since e_T is a subspace of type (5,4,2,0,1) and $e_T \cap P_0 = U$, hence $|E_T| = N'(3,0,0,0,1;5,4,2,0,1;2\nu+2+l,2\nu+2) = q^{2(2\nu-4+l)}$.

Lemma 2.4 The number of the decoding rules of the receiver is

$$|E_R| = q^{2(\nu-2)+l}(q+1)$$

Proof. Since e_R is a subspace of type (4,2,1,0,1) in the $(2\nu+2+l)$-dimensional singular pseudo-symplectic space $F_q^{(2\nu+2+l)}$ and $U \subset e_R$, hence $|E_R| = N'(3,0,0,0,1;4,2,1,0,1;2\nu+2+l,2\nu+2) = q^{2(\nu-2)+l}(q+1)$.

Lemma 2.5 For any $m \in M$, let the number of e_T and e_R contained in m be a and b, respectively. Then $a = q^{2(r_2+k_2-3)}$, $b = q^{(r_2+k_2-3)}N(1,2)$.

Proof. Let m be a message, from the definition of m, we may take m as follows

$$m = \begin{pmatrix} I^{(2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(r_2-2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(2)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k_2)} & 0 \end{pmatrix}$$
$$\begin{array}{cccccccccc} 2 & r_2-2 & \nu-r_2 & 2 & r_2-2 & \nu-r_2 & 1 & 1 & k_2 & l-k_2 \end{array}$$

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

$$e_T = \begin{pmatrix} I^{(2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & h_2 & 0 & h_4 & 0 & 0 & 0 & 0 & 0 & h_{10} & 0 \end{pmatrix} \begin{array}{c} 2 \\ 1 \\ 2 \end{array}$$
$$\begin{array}{ccccccccccc} 2 & r_2-2 & \nu-r_2 & 2 & r_2-2 & \nu-r_2 & 1 & 1 & 1 & k_2-1 & l-k_2 \end{array}$$

where h_2 ,h_{10} arbitrarily and (h_4) is nonsingular. Therefore, $a = q^{2(r_2+k_2-3)}$.
If $e_R \subset m$, then we can assume

$$e_R = \begin{pmatrix} I^{(2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & h'_2 & 0 & h'_4 & 0 & 0 & 0 & 0 & 0 & h'_{10} & 0 \end{pmatrix} \begin{array}{c} 2 \\ 1 \\ 1 \end{array}$$
$$\begin{array}{ccccccccccc} 2 & r_2-2 & \nu-r_2 & 2 & r_2-2 & \nu-r_2 & 1 & 1 & 1 & k_2-1 & l-k_2 \end{array}$$

where h'_2, h'_{10} arbitrarily and (h'_4) is a 1 dimensional vector subspace of 2 dimensional vector space. Therefore, $b = q^{(r_2+k_2-3)}N(1,2)$.

Lemma 2.6 (1) For any $e_T \in E_T$, the number of e_R which is incidence with e_T is $c = N(1,2)$.

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

Proof. (1) Assume that $e_T \in E_T$, e_T is a subspace of type (5,4,2,0,1) and $e_T \cap P_0 = U$, we may take e_T as follows

$$e_T = \begin{pmatrix} I^{(2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & I^{(2)} & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{array}{c} 2 \\ 1 \\ 2 \end{array}$$
$$\begin{array}{cccccccccc} 2 & r_2-2 & \nu-r_2 & 2 & r_2-2 & \nu-r_2 & 1 & 1 & 1 & l-1 \end{array}$$

If $e_R \subset e_T$, then we can assume

$$e_R = \begin{pmatrix} I^{(2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & h_4 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} 2 \\ 1 \\ 1 \end{matrix}$$
$$\begin{matrix} 2 & r_2-2 & \nu-r_2 & 2 & r_2-2 & \nu-r_2 & 1 & 1 & 1 & l-1 \end{matrix}$$

where (h_4) is a 1 dimensional vector subspace of 2 dimensional vector space, hence $c = N(1,2)$.

(2) Assume that $e_R \in E_R$, e_R is a subspace of type (4,2,1,0,1) in the $(2\nu+2+l)$-dimensional singular pseudo-symplectic space $F_q^{(2\nu+2+l)}$, we may take e_R as follows

$$e_R = \begin{pmatrix} I^{(2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} 2 \\ 1 \\ 1 \end{matrix}$$
$$\begin{matrix} 2 & r_2-2 & \nu-r_2 & 1 & 1 & r_2-2 & \nu-r_2 & 1 & 1 & 1 & l-1 \end{matrix}$$

If $e_T \supset e_R$, then we can assume

$$e_T = \begin{pmatrix} I^{(2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & h_2 & h_3 & 0 & h_5 & h_6 & h_7 & h_8 & 0 & 0 & h_{11} \end{pmatrix} \begin{matrix} 2 \\ 1 \\ 1 \\ 1 \end{matrix}$$
$$\begin{matrix} 2 & r_2-2 & \nu-r_2 & 1 & 1 & r_2-2 & \nu-r_2 & 1 & 1 & 1 & l-1 \end{matrix}$$

where $\begin{pmatrix} 1 & 0 \\ 0 & h_5 \end{pmatrix}$ is nonsingular and $h_2, h_3, h_6, h_7, h_8, h_{11}$ arbitrarily, therefore $d = q^{2\nu-4+l}$.

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 $q^{r_2+k_2-3}$.

Proof. Similar to the proof of Lemma 2.6, we can obtain Lemma 2.7 .

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 $s_0 = s_1 \cap s_2$, $\dim s_0 = k$, then $3 \le k \le r_2 + k_2 - 1$ and

(1) The number of e_R contained in $m_1 \cap m_2$ is $q^{k-3}N(1,2)$;

(2) For any $e_R \subset m_1 \cap m_2$, the number of e_T contained in $m_1 \cap m_2$ and containing e_R is q^{k-3}.

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 $U \subset s_1, s_2$, therefore, $3 \le k \le r_2 + k_2 - 1$.

(1)Suppose 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 $s_i = m_i \cap P_0$ $(i = 1,2)$, we have $s_0 = (m_1 \cap P_0) \bigcap (m_2 \cap P_0) = m_1 \cap m_2 \cap P_0 = s_1 \cap m_2 =$

$s_2 \cap m_1$ 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 $s_1^{'} \cap m_2 \subsetneq s_1 \cap m_2 = s_0$, $m_1 \cap m_2 = s_0 + e_T^{'}$. Therefore $\dim(m_1 \cap m_2) = k+2$. From $e_T^{'} \subset m_1 \cap m_2$, we may take m_1 as follows

$$m_1 = \begin{array}{c}\left(\begin{array}{cccccccc} I^{(2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(2)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & R_2 & 0 & R_4 & R_5 & 0 & 0 & R_8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & R_8' \end{array}\right)\begin{array}{l} 2 \\ 2 \\ 1 \\ r_2-2 \\ k_2-1 \end{array} \\ \begin{array}{cccccccc} 2 & \nu-2 & 2 & \nu-2 & 1 & 1 & 1 & l-1 \end{array}\end{array}$$

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

$$m_1 \cap m_2 = \begin{array}{c}\left(\begin{array}{cccccccc} I^{(2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(2)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & P_2 & 0 & P_4 & P_5 & 0 & 0 & P_8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & P_8' \end{array}\right)\begin{array}{l} 2 \\ 2 \\ 1 \\ r_2-2 \\ k_2-1 \end{array} \\ \begin{array}{cccccccc} 2 & \nu-2 & 2 & \nu-2 & 1 & 1 & 1 & l-1 \end{array}\end{array}$$

and

$$\dim \left(\begin{array}{cccccccc} 0 & P_2 & 0 & P_4 & P_5 & 0 & 0 & P_8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & P_8' \end{array}\right) = k-3$$

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

$$e_R = \begin{array}{c}\left(\begin{array}{cccccccc} I^{(2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & h_2 & h_3 & h_4 & h_5 & 0 & 0 & h_8 \end{array}\right)\begin{array}{l} 2 \\ 1 \\ 1 \end{array} \\ \begin{array}{cccccccc} 2 & \nu-2 & 2 & \nu-2 & 1 & 1 & 1 & l-1 \end{array}\end{array}$$

where the number of h_3 is $N(1,2)$ and every row of $\left(\begin{array}{cccccccc} 0 & h_2 & 0 & h_4 & h_5 & 0 & 0 & h_8 \end{array}\right)$ is the linear combination of the base of $\left(\begin{array}{cccccccc} 0 & P_2 & 0 & P_4 & P_5 & 0 & 0 & P_8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & P_8' \end{array}\right)$. So it is easy to know that the number of e_R contained in $m_1 \cap m_2$ is $q^{k-3}N(1,2)$.

(2) Assume 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

$$e_R = \begin{array}{c}\left(\begin{array}{cccccccc} I^{(2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & h_2 & h_3 & h_4 & h_5 & h_6 & 0 & h_8 \end{array}\right)\begin{array}{l} 2 \\ 1 \\ 1 \end{array} \\ \begin{array}{cccccccc} 2 & \nu-2 & 2 & \nu-2 & 1 & 1 & 1 & l-1 \end{array}\end{array}$$

If $e_T \subset m_1 \cap m_2$ and $e_R \subset e_T$, then e_T has the form as follows

$$e_T = \begin{pmatrix} I^{(2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & h_2 & h_3 & h_4 & h_5 & 0 & 0 & h_8 \\ 0 & h_2' & h_3' & h_4' & h_5' & h_6' & 0 & h_8' \end{pmatrix} \begin{matrix} 2 \\ 1 \\ 1 \\ 1 \end{matrix}$$
$$\begin{matrix} 2 & \nu-2 & 2 & \nu-2 & 1 & 1 & 1 & l-1 \end{matrix}$$

where $\begin{pmatrix} h_3 \\ h_3' \end{pmatrix}$ is nonsingular and every row of $\begin{pmatrix} 0 & h_2' & h_3' & h_4' & h_5' & 0 & 0 & h_8' \end{pmatrix}$ is the linear combination of the base of $\begin{pmatrix} 0 & P_2 & 0 & P_4 & P_5 & 0 & 0 & P_8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & P_8' \end{pmatrix}$ then the number of e_T contained in $m_1 \cap m_2$ and containing e_R is q^{k-3}.

Theorem 2.1 The parameters of constructed authentication codes with arbitration are

$$|S| = \frac{q^{(r_2-2)(2(r_2-r_1)+(k_1-k_2))}N(k_2-1, l-1)N(k_1-k_2, l-k_2)}{N(k_1-1, l-1)};$$

$$|E_T| = q^{2(2\nu-4+l)}; \qquad |E_R| = q^{2(\nu-2)+l}(q+1); \qquad M = |S||E_T|/a.$$

Theorem 2.2 In the A^2−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:

$$P_I = \frac{1}{q^{2\nu-r_2-k_2+l-1}}; \quad P_S = \frac{1}{q}; \quad P_T = \frac{1}{q+1};$$

$$P_{R_0} = \frac{1}{q^{2\nu+l-r_2-k_2-1}}; \quad P_{R_1} = \frac{1}{q}$$

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

$$P_I = \max_{m \in M}\left\{\frac{|\{e_R \in E_R | e_R \subset m\}|}{|E_R|}\right\}$$
$$= \frac{b}{|E_R|} = \frac{1}{q^{2\nu-r_2-k_2+l-1}}.$$

(2) Suppose that opponent get m_1 which is from the transmitter and send 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 the probability of opponent' substitution attack is

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

where $k = r_2 + k_2 - 1, P_s = \frac{1}{q}$ is the largest.

(3) Let e_T be a transmitter's encoding rules, s be a source state and m_1 be a 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 c. 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 1 receiver's decoding rules which is incidence with e_T at most. Therefore the probability of transmitter's successful impersonation attack is

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

$$= 1/(q+1)$$

(4) Let e_R be a receiver's decoding rule, we have known that the number of transmitter's encoding rules containing e_R is $q^{2\nu-4+l}$ and a message has $q^{r_2+k_2-3}$ transmitter's encoding rules containing e_R. Hence the probability of receiver's successful impersonation attack is

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

$$= 1/q^{(2\nu+l-r_2-k_2-1)}$$

(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 $\dim(s_1 \cap s_2) = k$ as large as possible. Therefore, the probability of receiver's successful substitution attack is

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

$$= q^{(k-3)}/q^{(r_2+k_2-3)}$$

where $k = r_2 + k_2 - 1$, $P_{R_1} = \frac{1}{q}$ is the largest.

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.ZXH2012K003.

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, Feng Rongquan. Construction of Cartesian Authentication Codes from pseudo-Symplectic Geometry [C].CHNACRYPT'94,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 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

[5] 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.

[6] 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.

[7] 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.

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