Journal of Mathematical Research & Exposition
Jan., 2009, Vol. 29, No. 1, pp. 9–18
DOI:10.3770/j.issn:1000-341X.2009.01.002
Http://jmre.dlut.edu.cn

Construction of Authentication Codes with Arbitration from Singular Pseudo-Symplectic Geometry over Finite Fields

GAO You[1], *WANG Hong Li*[1,2]
(1. College of Science, Civil Aviation University of China, Tianjin 300300, China;
2. Mathematics and Information Science Department, Tangshan Teacher's College, Hebei 063000, China)
(E-mail: gao_you@263.net)

Abstract A construction of authentication codes with arbitration from singular pseudo-symplectic geometry over finite fields is given and the parameters of the code are computed. Under the assumption 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.

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

Document code A
MR(2000) Subject Classification 94A60
Chinese Library Classification O157.4

1. Introduction

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 symply (A^2-code) defined as follows:

Let S, E_T, E_R and M be four non-empty finite sets, and $f : S\times E_T \longmapsto M$ 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

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, $g(m, e_R) =\{\text{reject}\}$.

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 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.

Received date: 2007-01-14; **Accepted date**: 2008-01-02
Foundation item: the National Natural Science Foundation of China (No. 60776810); the Natural Science Foundation of Tianjin City (No. 08JCYBJC13900).

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

$$P_I = \max_{m\in M}\Big\{\frac{|\{e_R \in E_R | e_R \subset m\}|}{|E_R|}\Big\}.$$

2) The opponent's substitution attack: the largest probability of an opponent's successful substitution attack is P_S. Then

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

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

$$P_T = \max_{e_T\in E_T}\Big\{\frac{\max\limits_{m\,\text{can not be encoded by}\,e_T}|\{e_R \in E_R | e_R \subset m \ \text{and}\, p(e_R, e_T)\neq 0\}|}{|\{e_R \in E_R | p(e_R, e_T)\neq 0\}|}\Big\}.$$

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

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

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

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

In the 1990s, Wan, Feng, et al., constructed authentication codes without arbitration from geometry space of classical groups and special matrices over finite fields[2−5]. In the late 1990s, Ma, Li, et al., constructed A^2-code from geometry space of 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, and the parameters and the probabilities of successful attacks of these 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

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

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

Let $F_q^{(2\nu+\delta+l)}$ be the $(2\nu+\delta+l)$-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:

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

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

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 $M(m,2s+\tau,s)$ and P does not or does contain a vector of the form

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

corresponding to the cases $\varepsilon=0$ or 1, respectively. Let E be the subspace of $F_q^{(2\nu+\delta+l)}$ generated by $e_{2\nu+\delta+1},\ldots,e_{2\nu+\delta+l}$. 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 [9] 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 $P_{S_{2\nu+\delta+l,2\nu+\delta}}(F_q)$. Let P be a subspace of $F_q^{(2\nu+\delta+l)}$. We define the dual subspace of P as

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

2. Construction

Assume that $n=2\nu+1+l$, $1\le r<r+t<\nu$. Let P be a fixed subspace of type $(r+l,\,0,\,0,\,0,\,l)$ in the $(2\nu+1+l)$-dimensional singular pseudo-symplectic space $F_q^{(2\nu+1+l)}$. Then $P^{\perp}$ is a subspace of type $(2\nu-r+1+l,\,2(\nu-r)+1,\,\nu-r,\,1,\,l)$. Let $Q=\langle e_{2\nu+2}\rangle$, the set of source states $S=\{s|s$ is a subspace of type $(r-1+k,\,0,\,0,\,0,\,k)$ and $1\le k<l, Q\subset s\subset P\}$; the set of transmitter's encoding rules $E_T=\{e_T|e_T$ is a subspace of type $(2t+2,\,2t+1,\,t,\,1,\,1)$ and $e_T\cap P=Q$, $e_T\subset P^{\perp}\}$; the set of receiver's decoding rules $E_R=\{e_R|e_R$ is a subspace of type $(2t-1,\,2(t-1)+1,\,t-1,\,1,\,0)$, $e_R\subset P^{\perp}\}$; the set of messages $M=\{m|m$ is a subspace of type $(r+2t+k,\,2t+1,\,t,\,1,k)$ and $m\cap P$ is a subspace of type $(r-1+k,\,0,\,0,\,0,\,k)$; $Q\subset m\subset P^{\perp}\}$.

Define the encoding map:

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

and the decoding map:

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

$$(m, e_R) \longmapsto \begin{cases} s, & \text{if } e_R \subset m, \text{where } s = m \cap P \\ \{\text{reject}\}, & \text{if } e_R \not\subset m. \end{cases}$$

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

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

and

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

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

Lemma 1 *The number of the source states is*

$$|S| = \frac{q^{(r-1)(l-k)}(q^r-1)\prod\limits_{i=l-k+1}^{l-1}(q^i-1)}{(q-1)\prod\limits_{i=1}^{k-1}(q^i-1)}.$$

Proof The number of the subspace of type $(r-1+k,\, 0,\, 0,\, 0,\, k)$ which contains Q and is contained in P is

$$q^{(r-1)(l-k)}N(r-1,r)N(k-1,l-1) = \frac{q^{(r-1)(l-k)}(q^r-1)\prod\limits_{i=l-k+1}^{l-1}(q^i-1)}{(q-1)\prod\limits_{i=1}^{k-1}(q^i-1)}.$$

Lemma 2 *The number of the transmitter's encoding rules is*

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

Proof Since $e_T \subset P^{\perp}$, and $e_T \cap P = Q$, the transmitter's encoding rules have the form as follows

$$\begin{pmatrix} R_1 & R_2 & 0 & R_4 & 0 & 0 & R_7 \\ 0 & 0 & 0 & 0 & 1 & 0 & L_7 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$
$$\begin{matrix} r & \nu-r & r & \nu-r & 1 & 1 & l-1 \end{matrix}$$

where (R_2, R_4) is a subspace of type $(2t,\ t)$ in the symplectic space ${F_q}^{(2(\nu-r))}$ and its number is $N(2t, t; 2(\nu-r))$. Therefore, the number of the transmitter's encoding rules is $q^{2tr+(2t+1)(l-1)}N(2t,\ t; 2(\nu-r))$.

Lemma 3 *The number of the receiver's decoding rules is*

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

Proof Since the receiver's decoding rules is a subspace of type $(2t-1,\ 2(t-1)+1,\ t-1,\ 1,\ 0)$ in $P^{\perp}$, it has the form as follows

$$\begin{array}{c}\left(\begin{array}{cccccc} R_1 & R_2 & 0 & R_4 & 0 & R_6 \\ 0 & 0 & 0 & 0 & 1 & L_6 \end{array}\right), \\ \begin{array}{cccccc} r & \nu-r & r & \nu-r & 1 & l \end{array}\end{array}$$

where (R_2, R_4) is a subspace of type $(2(t-1), t-1)$ in the symplectic space ${F_q}^{(2(\nu-r))}$ and its number is $N(2(t-1), t-1; 2(\nu-r))$. Then the number of the receiver's decoding rules is $q^{2(t-1)r+(2t-1)l}N(2(t-1), t-1; 2(\nu-r))$.

Lemma 4 *The number of the transmitter's encoding rules contained in a message is* $q^{2t(r-1)+(2t+1)(k-1)}$.

Proof Let P_1 be a message. Then $Q \subset P_1 \subset P^{\perp}$, P_1 is a subspace of type $(r+2t+k,\ 2t+1,\ t,\ 1, k)$ and $P \cap P_1$ is a subspace of type $(r-1+k,\ 0,\ 0,\ 0,\ k)$. Clearly, P_1 has a form as follows

$$P_1 = \begin{array}{c}\left(\begin{array}{cccccccc} Q_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ R_1 & R_2 & 0 & R_4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \end{array}\right), \\ \begin{array}{cccccccc} r & \nu-r & r & \nu-r & 1 & 1 & k-1 & l-k \end{array}\end{array}$$

and

$$P \cap P_1 = \begin{array}{c}\left(\begin{array}{ccccccc} Q_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I^{(k)} & 0 \end{array}\right) \\ \begin{array}{ccccccc} r & \nu-r & r & \nu-r & 1 & k & l-k \end{array}\end{array}$$

is a source state. If $e_T \subset P_1$, then we can assume

$$e_T = \begin{array}{c}\left(\begin{array}{cccccccc} R_1 & R_2 & 0 & R_4 & 0 & 0 & R_7 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & L_7 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{array}\right), \\ \begin{array}{cccccccc} r & \nu-r & r & \nu-r & 1 & 1 & k-1 & l-k \end{array}\end{array}$$

where (R_2, R_4) is a subspace of type $(2t,\ t)$ in the symplectic space ${F_q}^{(2(\nu-r))}$ and it is uniquely determined by the message P_1. Therefore, the number of the transmitter's encoding rules contained in a message is $q^{2t(r-1)+(2t+1)(k-1)}$.

Lemma 5 *The number of the messages is*

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

Proof We easily know that a message contains a source state and the number of the transmitter's encoding rules contained in a message is $q^{2t(r-1)+(2t+1)(k-1)}$. Therefore, we have

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

Lemma 6 *The probability of an opponent's successful impersonation attack is*

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

Proof Let P_1 be a message and $Q \subset P_1 \subset P^{\perp}$. P_1 is a subspace of type $(r+2t+1+k,\ 2t+2,\ t,\ 1, k)$ and $P \cap P_1$ is a subspace of type $(r-1+k,\ 0,\ 0,\ 0,\ k)$. It is easy to know that P_1 has a form as follows

$$P_1 = \begin{pmatrix} Q_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ R_1 & R_2 & 0 & R_4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I^{(k)} & 0 \end{pmatrix}.$$
$$\begin{matrix} r & \nu-r & r & \nu-r & 1 & k & l-k \end{matrix}$$

We can assume that

$$e_R = \begin{pmatrix} R_1{}' & R_2{}' & 0 & R_4{}' & 0 & R_6{}' & 0 \\ 0 & 0 & 0 & 0 & 1 & L_6{}' & 0 \end{pmatrix},$$
$$\begin{matrix} r & \nu-r & r & \nu-r & 1 & k & l-k \end{matrix}$$

where $(R_1\, R_2\, 0\, R_4)$ is a subspace of type $(2t,\ t)$ in the symplectic space $F_q^{(2\nu)}$, and the number of subspaces of type $(2(t-1),\ t-1)$ contained in this subspace of type $(2t,\ t)$ is $N(2(t-1),t-1;2t,t;2(\nu-r))$, so the number of the receiver's decoding rules contained in the message P_1 is $q^{2(t-1)(r-1)+(2t-1)k}N(2(t-1),t-1;2t,t;2(\nu-r))$. Therefore, the probability of an opponent's successful impersonation attack is

$$\begin{aligned} P_I &= \frac{q^{2(t-1)(r-1)+(2t-1)k}N(2(t-1),t-1;2t,t;2(\nu-r))}{q^{2(t-1)r+(2t-1)l}N(2(t-1),t-1;2(\nu-r))} \\ &= \frac{q^{2t}-1}{q^{(2t-1)(l-k)}(q^2-1)N(2(t-1),t-1;2(\nu-r))}. \end{aligned}$$

Lemma 7 *The probability of an opponent's successful substitution attack is*

$$P_S = \frac{1}{q^{2(t-1)}}.$$

Proof It is easy to know that any two distinct messages contain $q^{2(t-1)(r-2)+(2t-1)k}$ $N(2(t-1),t-1;2t,t;2(\nu-r))$ receiver's decoding rules at most. Since the number of the receiver's decoding rules contained in any fixed message is $q^{2(t-1)(r-1)+(2t-1)k}N(2(t-1),t-1;2t,t;2(\nu-r))$. Therefore, the probability of an opponent's successful substitution attack is

$$P_S = \frac{q^{2(t-1)(r-2)+(2t-1)k}N(2(t-1),t-1;2t,t;2(\nu-r))}{q^{2(t-1)(r-1)+(2t-1)k}N(2(t-1),t-1;2t,t;2(\nu-r))} = \frac{1}{q^{2(t-1)}}.$$

Lemma 8 *The probability of a transmitter's successful impersonation attack is*

$$P_T = \frac{q^2-1}{q^{2t}-1}.$$

Proof Let e_T be the transmitter's secret encoding rules, s be a source state, and P_1 be the message corresponding to the source state s encoded by e_T. Then the number of the receiver's decoding rules contained in P_1 is $q^{2(t-1)(r-1)+(2t-1)k}N(2(t-1),t-1;2t,t;2(\nu-r))$. Assume that P_2 is a distinct message corresponding to s, but P_2 cannot be encoded by e_T. Then $P_1 \cap P_2$ contains $q^{2(t-1)(r-1)+(2t-1)k}N(2(t-1),t-1;2t-1,t-1;2(\nu-r))$ receiver's decoding rules at most. Therefore the probability of a transmitter's successful impersonation attack is

$$P_T = \frac{q^{2(t-1)(r-1)+(2t-1)k}N(2(t-1),t-1;2t-1,t-1;2(\nu-r))}{q^{2(t-1)(r-1)+(2t-1)k}N(2(t-1),t-1;2t,t;2(\nu-r))} = \frac{q^2-1}{q^{2t}-1}.$$

Lemma 9 *The probability of a receiver's successful impersonation attack is*

$$P_{R_0} = \frac{1}{q^{2(l-k+1)}N(2,1;2(\nu-r-t+1))}.$$

Proof We can assume that the receiver's secret decoding rules are

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

Connecting with it gives the transmitter's encoding rules of the form:

$$e_T = \begin{pmatrix} 0 & I^{(t-1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ R_1 & 0 & R_3 & 0 & 0 & R_6 & 0 & 0 & R_9 \\ 0 & 0 & 0 & 0 & I^{(t-1)} & 0 & 0 & 0 & 0 \\ R_1{}' & 0 & R_3{}' & 0 & 0 & R_6{}' & 0 & 0 & R_9{}' \\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(2)} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \qquad (*)$$
$$\begin{matrix} r & t-1 & \nu-r-(t-1) & r & t-1 & \nu-r-(t-1) & 1 & 1 & l-1 \end{matrix}$$

where $\begin{pmatrix} R_3 & R_6 \\ R_3{}' & R_6{}' \end{pmatrix}$ is a subspace of type $(2,\,1)$ contained in the symplectic space $F_q^{2(\nu-r-(t-1))}$. So the number of transmitter's encoding rules as above is $q^{2r}N(2,1;2(\nu-r-t+1))q^{2(l-1)}$. A message containing e_R has $q^{2(r-1)}q^{2(k-1)}$ transmitter's encoding rules as above form, hence the probability of a receiver's successful impersonation attack is

$$P_{R_0} = \frac{q^{2(r-1)}q^{2(k-1)}}{q^{2r}N(2,1;2(\nu-r-t+1))q^{2(l-1)}} = \frac{1}{q^{2(l-k+1)}N(2,1;2(\nu-r-t+1))}.$$

Lemma 10 *The probability of a receiver's successful substitution attack is*

$$P_{R_1} = \frac{1}{q^2}.$$

Proof When the receiver received a message P_1, we know that P_1 contains $q^{2(r-1)}q^{2(k-1)}$

transmitter's encoding rules as form $(*)$. Substitute P_1 by message P_2 corresponding to the other source state. Then $P_1 \cap P_2$ contains $q^{2(r-2)}q^{2(k-1)}$ transmitter's encoding rules as form $(*)$ at most. Therefore the probability of a receiver's successful substitution attack is

$$P_{R_1} = \frac{q^{2(r-2)}q^{2(k-1)}}{q^{2(r-1)}q^{2(k-1)}} = \frac{1}{q^2}.$$

Theorem 1 *The A^2-code constructed as above has the following parameters:*

$$\begin{aligned}
|S| &= \frac{q^{(r-1)(l-k)}(q^r-1)\prod\limits_{i=l-k+1}^{l-1}(q^i-1)}{(q-1)\prod\limits_{i=1}^{k-1}(q^i-1)};\\
|E_T| &= q^{2tr+(2t+1)(l-1)}N(2t,t;2(\nu-r));\\
|E_R| &= q^{2(t-1)r+(2t-1)l}N(2(t-1),t-1;2(\nu-r));\\
|M| &= q^{(2t+1)(l-k)+2t}\ |S|\ N(2t,t;2(\nu-r));\\
P_I &= \frac{q^{2t}-1}{q^{(2t-1)(l-k)}(q^2-1)N(2(t-1),t-1;2(\nu-r))};\ P_S = \frac{1}{q^{2(t-1)}};\\
P_T &= \frac{q^2-1}{q^{2t}-1}\ ; P_{R_0} = \frac{1}{q^{2(l-k+1)}N(2,1;2(\nu-r-t+1))};\ P_{R_1} = \frac{1}{q^2}.
\end{aligned}$$

3. Realization of A^2-code

The receiver wants to prove whether the message m is an authentication, it suffices to prove $e_R \subset m$. If the equation $(k_1, k_2, \ldots, k_{r+2t+k})m = e_R$ has the solution, then m will be received as authentication, otherwise it will be regarded as deception.

To describe easily, we assume that $r = 2, t = 2, k = 1$ as example to explain the A^2-code's encoding and decoding process.

(1) The process of encoding.

Let

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

and

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

Then the transmitter's encoding rules e_T has the form:

$$e_T = \begin{pmatrix} X_1 & 1 & 0 & 0 & 0 & 0 & 0 & X_8 & 0 & 0 & X_{11} \\ X_1' & 0 & 1 & 0 & 0 & 0 & 0 & X_8' & 0 & 0 & X_{11}' \\ Y_1 & 0 & 0 & Y_4 & 0 & 1 & 0 & 0 & 0 & 0 & Y_{11} \\ Y_1' & 0 & 0 & Y_4' & 0 & 0 & 1 & 0 & 0 & 0 & Y_{11}' \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & Z_{11} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \beta_1 \\ \beta_2 \\ \gamma_1 \\ e_{2\nu+2} \end{pmatrix}$$
$$\begin{matrix} 2 & 1 & 1 & \nu-2 & 2 & 1 & 1 & \nu-2 & 1 & 1 & l-1 \end{matrix}$$

corresponding to e_T, and the receiver's decoding rules e_R has the form:

$$e_R = \begin{pmatrix} \alpha_1 + \lambda\alpha_2 \\ \beta_1 + \mu\beta_2 \\ \gamma_1 + be_{2\nu+2} \end{pmatrix},$$

where $(\alpha_1 + \lambda\alpha_2)K_l(\beta_1 + \mu\beta_2)^{\mathrm{T}} \neq 0$.

Let s be a source state. Then let

$$s = \begin{pmatrix} L_1 & 0 & 0 & 0 & 0 & 0 & L_7 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} \eta \\ e_{2\nu+2} \end{pmatrix},$$
$$\begin{matrix} 2 & \nu-2 & 2 & \nu-2 & 1 & 1 & l-1 \end{matrix}$$

and s be encoded to be $m = s + e_T$ by e_T.

(2) The process of decoding

If the receiver received a message m, then by the definition of m, we know that

$$m = \begin{pmatrix} N_1 & N_2 & 0 & N_4 & 0 & 0 & N_7 \\ Q_1 & Q_2 & 0 & Q_4 & 0 & 0 & Q_7 \\ R_1 & R_2 & 0 & R_4 & 0 & 0 & R_7 \\ 0 & 0 & 0 & 0 & 1 & 0 & Z_7 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$
$$\begin{matrix} 2 & \nu-2 & 2 & \nu-2 & 1 & 1 & l-1 \end{matrix}$$

If there are $k_i \in F_q (i = 1, 2, \ldots, 6)$, such that $(k_1, k_2, \ldots, k_6)m = e_R$, and every row has solution, then m will be accepted as authentication, and be decoded $s = m \cap P$, otherwise m will be seen as deception.

References

[1] SIMMONS G J. *Message authentication with arbitration of transmitter/receiverdisputes* [C]. In: Proc Eurocrypt'87, Lecture Notes in Computer Science 304, Berlin: 1987, 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 Sci. Math. Sci., 1994, **7**(4): 317–327.

[4] ZHENG Baodong. *A construction of authentication codes using involutory matrices over finite fields* [J]. J. Math. (Wuhan), 1999, **19**(3): 263–269. (in Chinese)

[5] GAO Suogang, LI Zengti. *A construction of Cartesian authentication code from symplectic geometry* [J]. Dongbei Shida Xuebao, 2002, **34**(4): 20–25. (in Chinese)
[6] MA Wenping, WANG Xinmei. *A construction of authentication codes with arbitration based on symplectic spaces* [J]. Chinese J. Comput., 1999, **22**(9): 949–952. (in Chinese)
[7] LI Zhihui, LI Ruihu. *Construction of authentication codes with arbitration from pseudo-symplectic geometry* [J]. J. Lanzhou Univ. Nat. Sci., 2005, **41**(5): 123–126. (in Chinese)
[8] LUO Jizhou, YOU Hong. *Construction of authentication codes with arbitration* [D]. Master's degree papers 2001,7. (in Chinese)
[9] WAN Zhexian. *Geometry of Classical Groups over Finite Fields (Second Edition)* [M]. Beijing/New York: Science Press, 2002.