Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2011, Article ID 675484, 18 pages
doi:10.1155/2011/675484

Research Article

Some New Constructions of Authentication Codes with Arbitration and Multi-Receiver from Singular Symplectic Geometry

You Gao and Huafeng Yu

College of Science, Civil Aviation University of China, Tianjin 300300, China

Correspondence should be addressed to You Gao, gao_you@263.net

Received 29 May 2011; Accepted 4 November 2011

Academic Editor: Junjie Wei

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

1. Introduction

Let S, E_T, E_R, and M be four nonempty finite sets, and let $f : S \times E_T \to M$ and $g : M \times E_R \to S \cup \{\text{reject}\}$ 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 a $s \in S$, 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.

In [1], Simmons introduced the A^2-code model to solve the transmitter and the receiver's distrust problem. In [2–4], some Cartesian authentication codes were constructed from symplectic and unitary geometry; in [5–7], authentication codes with arbitration based on symplectic and pseudosymplectic geometry were constructed.

The following notations will be fixed throughout this paper: p is a fixed prime. F_q is a field with q elements. $V = F_q^{(2\nu+l)}$ is a singular symplectic space over F_q with index ν. e_i $(1 \leq i \leq 2\nu + l)$ is row vector in V whose ith coordinate is 1 and all other coordinates are 0. Denote by E the l-dimensional subspace of V generated by $e_{2\nu+1}, e_{2\nu+2}, \dots, e_{2\nu+l}$. K_l denotes the matrix

$$\begin{pmatrix} 0 & I^{(\nu)} & 0 \\ -I^{(\nu)} & 0 & 0 \\ 0 & 0 & 0^{(l)} \end{pmatrix}. \tag{1.1}$$

For more concepts and notations used in this paper, refer to [8].

In an authentication system that permits arbitration, the 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,

$$P_I = \max_{m\in M}\left\{ \frac{|e_R \in E_R \mid e_R \subset m|}{|E_R|} \right\}. \tag{1.2}$$

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

$$P_S = \max_{m\in M}\left\{ \frac{\max_{m\neq m'\in M}|e_R \in E_R \mid e_R \subset m,\ e_R \subset m'|}{|e_R \in E_R \mid e_R \subset m|} \right\}. \tag{1.3}$$

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

$$P_T = \max_{e_T\in E_T}\left\{ \frac{\max_{m\in M,\ e_T\notin m}\left|\{e_R \in E_R \mid e_R \subset m,\ p(e_R, e_T) \neq 0\}\right|}{\left|\{e_R \in E_R \mid p(e_R, e_T) \neq 0\}\right|} \right\}. \tag{1.4}$$

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

$$P_{R_0} = \max_{e_R\in E_R}\left\{ \frac{\max_{m\in M}\left|\{e_T \in E_T \mid e_T \subset m,\ p(e_R, e_T) \neq 0\}\right|}{\left|\{e_T \in E_T \mid p(e_R, e_T) \neq 0\}\right|} \right\}. \tag{1.5}$$

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

$$P_{R_1} = \max_{e_R \in E_R,\, m \in M} \left\{ \frac{\max_{m' \in M} \left| \left\{ e_T \in E_T \mid e_T \subset m, m',\ p(e_R, e_T) \neq 0 \right\} \right|}{\left| \left\{ e_T \in E_T \mid p(e_R, e_T) \neq 0 \right\} \right|} \right\}. \tag{1.6}$$

Notes

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

2. The First Construction

In this section, we will construct an authentication code with arbitration from singular symplectic geometry over finite fields.

Assume that $2s \leq 2s_0 < m_0 \leq \nu + m_0$, $m_0 < 2\nu - 1$ and $1 \leq k < l$. Let P be a subspace $\langle v_1, v_2, e_{2\nu+1} \rangle$ of type $(3, 0, 1)$ in $F_q^{(2\nu+1)}$, and let P_0 be a fixed subspace of type $(m_0 + l, s_0, l)$ which contains P and orthogonal to v_2, but not orthogonal to v_1.

Our authentication code is a six-tuple

$$(S, E_T, E_R, M; f, g), \tag{2.1}$$

where the set of source states

$$S = \{ s \mid s \text{ is a subspace of type } (2s + 1 + k, s, k),\ p \subset s \subset P_0 \}, \tag{2.2}$$

the set of transmitter's encoding rules:

$$E_T = \{ e_T \mid e_T \text{ is a subspace of type } (5, 2, 1),\ e_T \cap P_0 = P \}, \tag{2.3}$$

the set of receiver's decoding rules:

$$E_R = \{ e_R \mid e_R \text{ is a subspace of type } (2, 1, 0),\ e_R \cap P_0 = \langle\ v_2 \rangle \}, \tag{2.4}$$

the set of messages:

$$\begin{aligned} M = \Big\{ m \mid m \text{ is a subspace of type } (2s + 3 + k, s + 1, k), P \subset m, \\ v_2 \notin m^{\perp}, m \cap P_0 \text{ is a subspace of type } (2s + 1 + k, s, k) \Big\}, \end{aligned} \tag{2.5}$$

the encoding function:

$$f : S \times E_T \longrightarrow M, \qquad (s, e_T) \longmapsto m = s + e_T \tag{2.6}$$

and the decoding function: $g : M \times E_R \rightarrow S \cup \{\text{reject}\}$,

$$(m, e_R) \longmapsto \begin{cases} s & \text{if } e_R \subset m, \text{where } s = m \cap P_0, \\ \{\text{reject}\} & \text{if } e_R \not\subset m. \end{cases} \tag{2.7}$$

Assuming that the transmitter's encoding rules and the receiver's decoding rules are chosen according to a uniform probability distribution, we can prove that the construction given above results in an A^2-code.

Lemma 2.1. *The six-tuple (S, E_T, E_R, M, f, g) is an authentication code with arbitration; that is*

(1) $s + e_T = m \in M$, *for all* $s \in S$ *and* $e_T \in E_T$;

(2) *for any* $m \in M$, $s = m \cap P_0$ *is uniquely information source contained in* m *and there is* $e_T \in E_T$, *such that* $m = s + e_T$.

Proof. (1) Let s be a source state, that is, a subspace Q of type $(2s+1+k, s, k)$ containing p and contained in p_0. Write E_k, Q as

$$E_k = \begin{pmatrix} e_{2v+1} \\ e_{2v+i_2} \\ \vdots \\ {}_{2v+i_k} \end{pmatrix}, \qquad \mathrm{Q} = \begin{pmatrix} Q_0 \\ v_1 \\ v_2 \\ E_k \end{pmatrix}, \tag{2.8}$$

which satisfies

$$\mathrm{QK}_l\mathrm{Q}^{\mathrm{T}} = \begin{array}{c} \begin{pmatrix} 0 & I^{(s-1)} & & & & \\ -I^{(s-1)} & 0 & & & & \\ & & 0 & 1 & & \\ & & -1 & 0 & & \\ & & & & 0 & \\ & & & & & 0 \end{pmatrix} \\ \begin{matrix} s-1 & s-1 & 1 & 1 & 1 & k \end{matrix} \end{array}. \tag{2.9}$$

Let e_T be a transmitter's rule, that is, a subspace R of type $(5, 2, 1)$ containing P and $R \cap P_0 = P$. So, there exists $u_1, u_2 \in R$, such that $R = \langle v_1, v_2,\ u_1,\ u_2, e_{2v+1} \rangle$ and

$$\mathrm{QK}_l\mathrm{Q}^{\mathrm{T}} = \begin{array}{c} \begin{pmatrix} 0 & I^{(s-1)} & & & & & & \\ -I^{(s-1)} & 0 & & & & & & \\ & & 0 & 1 & 0 & * & * & \\ & & -1 & 0 & 0 & 1 & 0 & \\ & & 0 & 0 & 0 & 0 & 1 & \\ & & * & -1 & 0 & 0 & 0 & \\ & & * & 0 & -1 & 0 & 0 & \\ & & & & & & & 0 \end{pmatrix} \\ \begin{matrix} s-1 & s-1 & 1 & 1 & 1 & 1 & 1 & k \end{matrix} \end{array}. \tag{2.10}$$

Therefore, $M = Q + \langle u_1, u_2\rangle$ is a subspace of type $(2s+3+k, s+1, k)$ which contains P and $M\cap P_0 = Q$ is a subspace of type $(2s+1+k, s, k)$, and is not orthogonal to v_2, hence a message.

(2) Now, let m be a message; that is, m is a subspace M of type $(2s+3+k, s+1, k)$ which contains P and intersects P_0 at a subspace of type $(2s+1+k, s, k)$, and is not orthogonal to v_2. By definition, P_0 contains $\langle v_1, v_2, e_{2\nu+1}\rangle$, so $P \subset M\cap P_0 = Q$, so Q is a source state. Since $M \neq P_0$, there exists $u_1, u_2 \in M$ but $u_1, u_2 \notin P_0$ such that $M = Q + \langle u_1, u_2\rangle$. We have to show that there exists $u_1, u_2 \in M$ such that $R = \langle v_1, v_2, u_1, u_2, e_{2\nu+1}\rangle$ is a subspace of type $(5, 2, 1)$, hence a transmitter's encoding rule.

Assume that $R = \langle v_1, v_2, u_1, u_2, e_{2\nu+1}\rangle$ has been set; if R is a subspace of type $(5, 2, 1)$, then we are done. So, suppose that R is not a subspace of type $(5, 2, 1)$. Since $v_2 \in Q^{\perp}$ and $v_2 \notin M^{\perp}$, we must have that $v_2K_lu_1^T \neq 0$ or $v_2K_lu_2^T \neq 0$. Without loss of generality, let $v_2K_lu_2^T = 1$. If we also have $v_2K_lu_1^T = 1$, replacing u_1 by $u_1 - u_2$, we get $v_2K_lu_2^T = 1$ and $v_2K_lu_1^T = 0$. Since R is not a subspace of type $(5, 2, 1)$, certainly $v_1K_lu_1^T = 0$. Note that Q is a subspace of type $(2s+1+k, s, k)$, $v_1 \notin Q^{\perp}$, so there exists a vector $w \in Q$ such that $v_1K_lw^T = 1$. Replacing u_1 by $w + u_1$, we have $v_1K_lu_1^T = 1$, $v_2K_lu_1^T = 0$ $(v_2 \in Q^{\perp})$. Then, $R = \langle v_1, v_2, u_1, u_2, e_{2\nu+1}\rangle$ is a subspace of type $(5, 2, 1)$, and $M = Q + R$, hence R is a transmitter's encoding rule.

If there is another source state Q' such that $M = Q' + R'$, we have that $Q' \subset M\cap P_0 = Q$. by $Q' \subset M, Q' \subset P_0$. Since $\dim Q' = \dim Q = 2s+1+k$, so $Q' = Q$. This implies that the source state Q is uniquely determined by M. □

Let n_1 denote the number of subspaces of type $(2s+1+k, s, k)$ contained in $\langle v_2\rangle^{\perp}$ and containing P, n_2, the number of subspaces of type (m_0+l, s_0, l) contained in $\langle v_2\rangle^{\perp}$ and containing a fixed subspace of type $(2s+1+k, s, k)$ as above, and n_3, the number of subspaces of type (m_0+l, s_0, l) contained in $\langle v_2\rangle^{\perp}$ and containing P and not contained in $\langle v_1\rangle^{\perp}$.

Lemma 2.2. *One has*

$$\begin{aligned} n_1 &= q^{2(\nu-s-1)} \cdot q^{(2s-1)(l-k)} \cdot N(2(s-1), s-1;\ 2(\nu-2)) \cdot N(k-1, l-1),\\ n_2 &= N(m_0 - (2s+1), s_0 - s;\ 2(\nu - s - 1)),\\ n_3 &= q^{2(\nu-s-1)} \cdot q^{(2\nu-m_0-1)} \cdot N(m_0 - 3, s_0 - 1;\ 2(\nu-2)). \end{aligned} \tag{2.11}$$

Proof. (1) Computation of n_1.
By the transitivity of $Sp_{2\nu+l}(F_q)$ on the set of subspaces of the same type, we can assume that

$$\begin{array}{c} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \end{array} = \begin{array}{c} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \\ \begin{matrix} 1 & 1 & \nu-2 & 1 & 1 & \nu-2 & l \end{matrix} \end{array}. \tag{2.12}$$

Let Q be a subspace of type $(2s+1+k, s, k)$ contained in $\langle v_2\rangle^{\perp}$ and containing P. There exists a $u \in Q$ such that $v_1K_lu^T = 1$. We may assume that $u = (0, 0, R_1, 1, 0, R_2, 0, 0, R_3)$. So, Q has a matrix representation of the form

$$\mathrm{Q} = \begin{array}{cc} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_1 & 1 & 0 & R_2 & 0 & 0 & R_3 \\ 0 & 0 & Q_1 & 0 & 0 & Q_2 & 0 & 0 & Q_3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \end{pmatrix} & \begin{matrix} 1 \\ 1 \\ 1 \\ 2s-2 \\ 1 \\ k-1 \end{matrix} \\ \begin{matrix} 1 & 1 & \nu-2 & 1 & 1 & \nu-2 & 1 & k-1 & l-k \end{matrix} & \end{array}. \tag{2.13}$$

It is easy to verify that Q_1, Q_2 is a subspace of type $(2(s-1), s-1)$ in the $2(v-2)$-dimensional symplectic space. The number of this kind of subspace is denoted by $N(2(s-1), s-1;\ 2(\nu-2))$, Q_3 arbitrarily. Furthermore, we may take (Q_1, Q_2, Q_3) as

$$\begin{array}{c}\begin{pmatrix} I^{(s-1)} & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(s-1)} & 0 & 0 \end{pmatrix} \\ \begin{matrix} s-1 & b & s-1 & b & l-k \end{matrix}\end{array} \tag{2.14}$$

to compute n_1, where $b = (\nu-2)-(s-1)$. Since Q has a matrix representation of the form

$$Q = \begin{array}{c}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a_4 & 1 & 0 & 0 & b_4 & 0 & 0 & c_3 \\ 0 & 0 & I^{(s-1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(s-1)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \end{pmatrix} \\ \begin{matrix} 1 & 1 & a & b & 1 & 1 & a & b & 1 & k-1 & l-k \end{matrix}\end{array}, \tag{2.15}$$

where $a = s-1$ and $b = \nu - s - 1$, we have that

$$n_1 = q^{2(\nu-s-1)} \cdot q^{(2s-1)(l-k)} \cdot N(2(s-1), s-1;\ 2(\nu-2)) \cdot N(k-1, l-1). \tag{2.16}$$

(2) Computation of n_2.

Let U be a subspaces of type $(m_0 + l, s_0, l)$ contained in $\langle v_2 \rangle^{\perp}$ and containing a fixed subspace of type $(2s+1+k, s, k)$ which contains P, similar to (1), we may assume that U has a matrix representation of the form

$$U = \begin{array}{c}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(s-1)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(s-1)} & 0 & 0 \\ 0 & 0 & 0 & P_1 & 0 & 0 & 0 & P_2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(l)} \end{pmatrix} \\ \begin{matrix} 1 & 1 & a & b & 1 & 1 & a & b & l \end{matrix}\end{array}, \tag{2.17}$$

where $a = s-1, b = \nu - s - 1$, so (P_1, P_2) is a subspace of type $(m_0 - (2s+1), s_0 - s)$ in the $2(v-s-1)$-dimensional symplectic space. We have that

$$n_2 = N(m_0 - (2s+1), s_0 - s;\ 2(\nu - s - 1)). \tag{2.18}$$

(3) Computation of n_3.

By the same method as that of (1) and (2), let U_0 be a subspaces of type (m_0+l, s_0, l) contained in $\langle v_2\rangle^{\perp}$, containing P and not contained in $\langle v_1\rangle^{\perp}$. We may assume that the subspace has a matrix representation of the form

$$U_0 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & A_1 & 1 & 0 & A_2 & 0 \\ 0 & 0 & Q_1 & 0 & 0 & Q_2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(l)} \end{pmatrix}. \tag{2.19}$$
$$\begin{matrix} 1 & 1 & v-2 & 1 & 1 & v-2 & l \end{matrix}$$

So, the number of the subspaces (Q_1, Q_2) is denoted by $N(m_0-3, s_0-1;\ 2(\nu-2))$. Then, by the transitivity of $Sp_{2\nu+l}(F_q)$ on the set of subspaces of the same type, we can assume that

$$U_0 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & a_5 & 1 & 0 & 0 & b_4 & b_5 & 0 \\ 0 & 0 & I^{(s_0-1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(s_0-1)} & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(a)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(l)} \end{pmatrix}, \tag{2.20}$$
$$\begin{matrix} 1 & 1 & c & a & b & 1 & 1 & c & a & b & l \end{matrix}$$

where $c = s_0 - 1, a = m_0 - 2s_0 - 1, b = \nu - m_0 + s_0, a_5, b_4, b_5$ arbitrarily. We may get

$$n_3 = q^{2(\nu-s-1)} \cdot q^{(2\nu-m_0-1)} \cdot N(m_0-3, s_0-1;\ 2(\nu-2)). \tag{2.21}$$

□

Lemma 2.3. *The number of the source states is*

$$|S| = q^{(m_0-2s-1)+(2s-1)(l-k)} \cdot \frac{N(2(s-1), s-1;\ 2(\nu-2)) \cdot N(m_0-(2s+1), s_0-s;\ 2(\nu-s-1)) \cdot N(k-1, l-1)}{N(m_0-3, s_0-1;\ 2(\nu-2))}. \tag{2.22}$$

Proof. Since $|S|$ is the number of subspaces of type $(2s+1+k, s, k)$ contained in P_0 and containing P, we have $|S| \cdot n_3 = n_1 \cdot n_2$. □

Lemma 2.4. *The number of the encoding rules of transmitter is*

$$|E_T| = q^{(m_0-3)+2(\nu-2)+2(l-1)} \cdot \left(q^{2\nu-m_0-1} - 1\right). \tag{2.23}$$

Proof. Since $|E_T|$ is the number of subspaces of type $(5,2,1)$ contained in P_0 and containing P, let $R = \langle v_1, v_2, u_1, u_2, e_{2\nu+1}\rangle$, where $v_1 K_l u_1^T = 1, v_2 K_l u_2^T = 1$, and $\langle v_1, u_1\rangle \perp \langle v_2, u_2\rangle$. By the transitivity of $Sp_{2\nu+1}(F_q)$ on the set of subspaces of the same type, we can assume that

$$\begin{gathered}
v_1 = (1,0,0,0,0,0,0,0,0,0,0,0), \\
v_2 = (0,1,0,0,0,0,0,0,0,0,0,0), \\
e_{2\nu+1} = (0,0,0,0,0,0,0,0,0,0,1,0), \\
P_0 = \begin{array}{c} \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & I^{(s_0-1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(s_0-1)} & 0 & 0 & 0 \\
0 & 0 & 0 & I^{(a)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(l)}
\end{pmatrix} \\
\begin{matrix} 1 & 1 & c & a & b & 1 & 1 & c & a & b & l \end{matrix}
\end{array},
\end{gathered} \tag{2.24}$$

where $c = s_0 - 1$, $a = m_0 - 2s_0 - 1$, and $b = \nu - m_0 + s_0$. Therefore, u_1 and u_2 have the respective forms:

$$\begin{aligned}
u_1 &= \left(0,0,a_3,a_4,a_5,1,0,b_3,b_4,b_5,0,f_2\right), \\
u_2 &= \left(0,0,c_3,c_4,c_5,0,1,d_3,d_4,d_5,0,g_2\right).
\end{aligned} \tag{2.25}$$

Note that $u_2 \notin P_0$ and $\dim(R \cap p_0) = 3$, so the vector u_1 cannot lie in P_0. Then, a_5, b_4, b_5 cannot equal zero at the same time. Thus, the number of u_1 is $q^{(m_0-3)+(l-1)}(q^{2\nu-m_0-1}-1)$ and that for u_2 is $q^{2(\nu-2)+(l-1)}$; we may get

$$|E_T| = q^{(m_0-3)+2(\nu-2)+2(l-1)} \cdot \left(q^{2\nu-m_0-1}-1\right). \tag{2.26}$$

□

Lemma 2.5. *The number of the encoding rules of receiver is*

$$|E_R| = q^{2\nu-2} \cdot q^l. \tag{2.27}$$

Proof. $|E_R|$ is the number of type $(2,1,0)$ intersecting P_0 at $\langle v_2\rangle$. Let $H = \langle v_2, u\rangle$, where $v_2 K_l u^T = 1$. Following the notion of Lemma 2.4, hence u has the form

$$u = (a_1, 0, a_3, a_4, a_5, b_1, 1, b_3, b_4, b_5, c_1). \tag{2.28}$$

Clearly, $u \notin P_0$. The number of u is $q^{2\nu-2} \cdot q^l$, that is,

$$|E_R| = q^{2\nu-2} \cdot q^l. \tag{2.29}$$

□

Lemma 2.6. *For any $m \in M$, let the number of e_T and e_R contained in m be a and b, respectively. Then,*

$$a = q^{4s-3+2(k-1)} \cdot (q-1), \qquad b = q^{2s+1} \cdot q^k. \tag{2.30}$$

Proof. Let M be a message, and $Q = M \cap P_0$, then Q is a source state contained in M. By Lemma 2.1, we may get a transmitter's encoding rule R contained in M. Let $R = \langle v_1, v_2, u_1, u_2, e_{2\nu+1} \rangle$. Here, $M = Q + \langle u_1, u_2 \rangle, v_2 K_l u_2^T = 1$. Following the notation of Lemma 2.4, we can assume that Q has a matrix representation of the form

$$Q = \begin{array}{c} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(s-1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(s-1)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \end{pmatrix} \\ \begin{matrix} 1 & 1 & d & c & a & b & 1 & 1 & d & c & a & b & 1 & k-1 & l-k \end{matrix} \end{array}, \tag{2.31}$$

where $a = m_0 - 2s_0 - 1, b = \nu + s_0 - m, c = s_0 - s,$ and $d = s - 1$. By $v_2 K_l u_2^T = 1$ and R being the subspace of type $(5, 2, 1)$, we can assume

$$\begin{aligned} u_1 &= (0, 0, a_3, a_4, a_5, a_6, b_1, 0, b_3, b_4, b_5, b_6, 0, f_2, f_3), \\ u_2 &= (0, 0, c_3, c_4, c_5, c_6, d_1, 1, d_3, d_4, d_5, d_6, 0, g_2, g_3), \end{aligned} \tag{2.32}$$

where $b_1 \neq 0$. Then,

$$M = \begin{array}{c} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(s-1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(s-1)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \\ 0 & 0 & a_3 & a_4 & a_5 & a_6 & b_1 & 0 & b_3 & b_4 & b_5 & b_6 & 0 & f_2 & f_3 \\ 0 & 0 & c_3 & c_4 & c_5 & c_6 & d_1 & 1 & d_3 & d_4 & d_5 & d_6 & 0 & g_2 & g_3 \end{pmatrix} \\ \begin{matrix} 1 & 1 & d & c & a & b & 1 & 1 & d & c & a & b & 1 & k-1 & l-k \end{matrix} \end{array}, \tag{2.33}$$

where $a = m_0 - 2s_0 - 1, b = \nu + s_0 - m, c = s_0 - s,$ and $d = s - 1$.

(1) Note that M is fixed, so, for u_1, the $a_4, a_5, a_6, b_4, b_5, b_6,$ and f_3 are fixed and, for u_2, the $c_4, c_5, c_6, d_4, d_5, d_6,$ and g_3 are fixed. Therefore, the number of u_1 is $q^{2(s-1)+(k-1)}$.

$(q-1)$ and the number of u_2 is $q^{2(s-1)+(k-1)+1}$. Then, the number of e_T contained in m is

$$a = q^{4s-3+2(k-1)} \cdot (q-1). \tag{2.34}$$

(2) Let $H = \langle v_2, u \rangle$ be a receiver's encoding rule contained in M, where $v_2 K_l u^T = 1$. Clearly, $u \notin Q$, then we can assume that u has the form

$$u = (h_1, 0, h_3, h_4, h_5, h_6, i_1, 1, i_3, i_4, i_5, i_6, j_1, j_2, j_3). \tag{2.35}$$

Note that

$$(h_4, h_5, h_6, i_4, i_5, i_6, j_3) = k(a_4, a_5, a_6, b_4, b_5, b_6, f_3) + (c_4, c_5, c_6, d_4, d_5, d_6, g_3), \tag{2.36}$$

where $k \in F_q$. Therefore, the number of $(h_4, h_5, h_6, i_4, i_5, i_6, j_3)$ is q. Then, the number of e_R contained in m is

$$b = q \cdot q^2 \cdot q^{2(s-1)} \cdot q^k = q^{2s+1+k}. \tag{2.37}$$

□

Lemma 2.7. *The number of the messages is*

$$|M| = \frac{|S||E_T|}{q^{4s-k+2(k-1)}(q-1)}. \tag{2.38}$$

Proof. For any $m \in M$, there is uniquely $s \in S$ and $e_T \in E_T$ satisfying $m = s + e_T$; the number of e_T is a. Thus,

$$|M| = \frac{|S||E_T|}{a} = \frac{|S||E_T|}{q^{4s-k+2(k-1)}(q-1)}. \tag{2.39}$$

□

Lemma 2.8. *(1) For any $e_T \in E_T$, the number of e_R contained in e_T is q^3.*

(2) For any $e_R \in E_R$, the number of e_T containing e_R is $(q^{2\nu-4} - q^{m_0-3}) \cdot q^{l-1}$.

Proof. (1) Let R be a transmitter's encoding rule; we can assume that $R = \langle v_1, v_2, u_1, u_2, e_{2\nu+1} \rangle$. Here, $v_2 K_l u_2^T = 1, v_1 K_l u_1^T = 1$, and $\langle v_1, u_1 \rangle \perp \langle v_2, u_2 \rangle$. Then, the receiver's encoding rule H contained in R should have the form $H = \langle v_2, k_1 v_1 + k_2 u_1 + u_2 + k_3 e_{2\nu+1} \rangle$, where $k_1, k_2, k_3 \in F_q$. So, the number of H is q^3.

(2) Let H be a receiver's encoding rule, and $H = \langle v_2, u \rangle$, where $v_2 K_l u^T = 1$. Therefore, $\langle v_1, v_2, u, e_{2\nu+1} \rangle$ is a subspace of type $(4, 1, 1)$. The number of subspace $\langle v_1, v_2, u, u_1, e_{2\nu+1} \rangle$ of type $(5, 2, 1)$ is $q^{2\nu-4} \cdot q^{l-1}$. Here, $v_1 K_l u_1^T \neq 0$. Note that $v_2 \in P_0^{\perp}$ and $v_1 \notin p_0^{\perp}$. It is easy to see that

the number of $u_1 \in P_0$ such that $\langle v_1, v_2, u_1, e_{2\nu+1}\rangle$ is a subspace of type $(4,1,1)$ is $q^{m_0-3} \cdot q^{l-1}$. So, the number of transmitter's encoding rules e_T containing H is $(q^{2\nu-4} - q^{m_0-3}) \cdot q^{l-1}$. $\square$

Lemma 2.9. *For any $m \in M$ and $e_R \subset m$, the number of e_T contained in m and containing e_R is*

$$q^{2(s-1)+(k-1)} \cdot (q-1). \tag{2.40}$$

Proof. Let M be a message, and let $H = \langle v_2, u\rangle$ be a receiver's encoding rule contained in M; we can assume that $u = (0,0,0,0,0,1,0,0,0,0,0,0)$, and M has a matrix representation of the form

$$M = \begin{array}{c}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(s-1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(s-1)} & 0 & 0 & 0 & 0 \\ 0 & 0 & a_3 & a_4 & b_1 & 0 & b_3 & b_4 & 0 & f_2 & f_3 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \end{pmatrix} \\ \begin{matrix} 1 & 1 & a & b & 1 & 1 & a & b & 1 & k-1 & l-k \end{matrix}\end{array}, \tag{2.41}$$

where $b_1 \neq 0, a = s-1,$ and $b = \nu - s - 1$.

Note that M is fixed, so a_4, b_4, f_3 are fixed. Assume that R is a transmitter's encoding rule contained in M and containing H. Let $R = \langle v_1, v_2, u, u_1, e_{2\nu+1}\rangle$, where $v_1 K_l u_1^T \neq 0$. Thus, u_1 has the form

$$u_1 = (0,0,c_3,c_4,d_1,0,d_3,d_4,0,g_2,g_3), \tag{2.42}$$

where $d_1 \neq 0$. Note that $(c_4, d_4, g_3) = k(a_4, b_4, f_3)$ and $u_1 \notin P_0$, so $k \neq 0$. Hence, u_1, $c_4, d_4,$ and g_3 are fixed. Then, the number of u_1 is $q^{2(s-1)+(k-1)} \cdot (q-1)$; that is, the number of R is $q^{2(s-1)+(k-1)} \cdot (q-1)$. $\square$

Lemma 2.10. *Assume 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 $s_0 = s_1 \bigcap s_2$, $\dim\ s_0 = k_1$, then $3 \leq k_1 \leq 2s + k$, and*

(1) *the number of e_R contained in $m_1 \bigcap m_2$ is q^{k_1};*

(2) *for any $e_R \subset m_1 \bigcap m_2$, the number of e_T containing e_R is q^{k_1-4}.*

Proof. Since $m_1 = s_1 + e'_T$, $m_2 = s_2 + e'_T$, and $m_1 \neq m_2$, then $s_1 \neq s_2$. Again because of $s_1 \supset P_0$ and $s_2 \supset P_0$, $3 \leq k_1 \leq 2s+k$. From $m_i = s_i + e'_T = s_0 + s'_i + e'_T$, it is easy to know that $m_1 \bigcap m_2 = s_0 + e'_T$. Therefore,

$$\dim\left(m_1 \bigcap m_2\right) = \dim s_0 + \dim e'_T - \dim\left(s_0 \bigcap e'_T\right) = k_1 + 5 - 3 = k_1 + 2. \tag{2.43}$$

(1) By the definition of the message, we can assume that m_1 and m_2 have the form as follows, respectively:

$$m_1 = \begin{array}{cc} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & A_1 & 0 & 0 & A_2 & 0 \\ 0 & 0 & a_3 & 0 & 1 & a_6 & 0 \\ 0 & 0 & b_3 & b_4 & 0 & b_6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & A_3 \end{pmatrix} & \begin{array}{c} 1 \\ 1 \\ 1 \\ 2(s-1) \\ 1 \\ 1 \\ l \end{array}, \\ \begin{array}{ccccccc} 1 & 1 & v-2 & 1 & 1 & v-2 & l \end{array} & \end{array} \tag{2.44}$$

where $b_4 \neq 0$,

$$m_2 = \begin{array}{cc} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & B_1 & 0 & 0 & B_2 & 0 \\ 0 & 0 & c_3 & 0 & 1 & c_6 & 0 \\ 0 & 0 & d_3 & d_4 & 0 & d_6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & B_3 \end{pmatrix} & \begin{array}{c} 1 \\ 1 \\ 1 \\ 2(s-1) \\ 1 \\ 1 \\ l \end{array}, \\ \begin{array}{ccccccc} 1 & 1 & v-2 & 1 & 1 & v-2 & l \end{array} & \end{array} \tag{2.45}$$

where $d_4 \neq 0$. Thus,

$$m_1 \bigcap m_2 = \begin{array}{cc} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & D_1 & 0 & 0 & D_2 & 0 \\ 0 & 0 & f_3 & 0 & 1 & f_6 & 0 \\ 0 & 0 & g_3 & g_4 & 0 & g_6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & D_3 \end{pmatrix} & \begin{array}{c} 1 \\ 1 \\ 1 \\ 2(s-1) \\ 1 \\ 1 \\ l \end{array}, \\ \begin{array}{ccccccc} 1 & 1 & v-2 & 1 & 1 & v-2 & l \end{array} & \end{array} \tag{2.46}$$

where $g_4 \neq 0$. Since $\dim(m_1 \cap m_2) = k_1 + 2$, therefore

$$\dim \begin{pmatrix} 0 & 0 & D_1 & 0 & 0 & D_2 & 0 \\ 0 & 0 & f_3 & 0 & 1 & f_6 & 0 \\ 0 & 0 & g_3 & g_4 & 0 & g_6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & D_3 \end{pmatrix} = k_1 + 2 - 3 = k_1 - 1. \tag{2.47}$$

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

$$e_R = \begin{array}{c} \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ R_1 & 0 & R_3 & R_4 & 1 & R_6 & R_7 \end{pmatrix}. \\ \begin{array}{ccccccc} 1 & 1 & v-2 & 1 & 1 & v-2 & l \end{array} \end{array} \tag{2.48}$$

Since R_1, R_4 are arbitrary, every row of $(0 \quad 0 \quad R_3 \quad 0 \quad 1 \quad R_6 \quad R_7)$ is the linear combination of the base

$$\begin{pmatrix} 0 & 0 & D_1 & 0 & 0 & D_2 & 0 \\ 0 & 0 & f_3 & 0 & 1 & f_6 & 0 \\ 0 & 0 & g_3 & g_4 & 0 & g_6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & D_3 \end{pmatrix}, \tag{2.49}$$

thus the number of it is q^{k_1-2}. So, it is easy to know that the number of e_R contained in $m_1 \bigcap m_2$ is

$$q^{k_1-2} \cdot q^2 = q^{k_1}. \tag{2.50}$$

(2) Assume that $m_1 \bigcap m_2$ has the form of (2.46), then, for any $e_R \subset m_1 \bigcap m_2$, we can assume that

$$e_R = \begin{array}{c} \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ R_1 & 0 & R_3 & R_4 & 1 & R_6 & R_7 \end{pmatrix} \\ \begin{matrix} 1 & 1 & v-2 & 1 & 1 & v-2 & l \end{matrix} \end{array}. \tag{2.51}$$

If $e_R \subset e_T$ and $e_T \subset m_1 \bigcap m_2$, then

$$e_T = \begin{array}{cc} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & R_4 & 1 & R_6 & 0 & R_7 \\ 0 & 0 & R_3' & 1 & 0 & R_6' & 0 & R_7' \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} & \begin{matrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{matrix} \\ \begin{matrix} 1 & 1 & v-2 & 1 & 1 & v-2 & 1 & l-1 \end{matrix} & \end{array}, \tag{2.52}$$

where

$$\begin{pmatrix} 0 & 0 & R_3' & 0 & 0 & R_6' & 0 & R_7' \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \tag{2.53}$$

is the linear combination on the basis of

$$\begin{pmatrix} 0 & 0 & D_1 & 0 & 0 & D_2 & 0 \\ 0 & 0 & f_3 & 0 & 1 & f_6 & 0 \\ 0 & 0 & g_3 & g_4 & 0 & g_6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & D_3 \end{pmatrix}, \tag{2.54}$$

then the number of e_T containing e_R is q^{k_1-4}. □

Theorem 2.11. *The above construction yields an* A^2*-code with the following size parameters:*

$$
\begin{aligned}
|S| &= q^{(m_0-2s-1)+(2s-1)(l-k)} \\
&\quad \cdot \frac{N(2(s-1), s-1;\ 2(\nu-2)) \cdot N(m_0-(2s+1), s_0-s;\ 2(\nu-s-1)) \cdot N(k-1, l-1)}{N(m_0-3, s_0-1;\ 2(\nu-2))}, \\
|E_T| &= q^{(m_0-3)+2(\nu-2)+2(l-1)} \cdot \left(q^{2\nu-m_0-1}-1\right), \\
|E_R| &= q^{2\nu-2+l}, \\
|M| &= \frac{|S||E_T|}{q^{4s-3+2(k-1)} \cdot (q-1)}.
\end{aligned}
\tag{2.55}
$$

Moreover, assume that the encoding rules e_T *and* e_R *are chosen according to a uniform probability distribution, the largest probabilities of success for different types of deceptions:*

$$
\begin{aligned}
P_I &= \frac{1}{q^{2\nu-2s-3} \cdot q^{l-k}}, \qquad P_S = \frac{1}{q}, \qquad P_T = \frac{1}{q^2}; \\
P_{R_0} &= \frac{q-1}{q^{m_0-2s-1} \cdot q^{l-k}\left(q^{2\nu-m_0-1}-1\right)}, \qquad P_{R_1} = \frac{1}{q \cdot (q-1)}.
\end{aligned}
\tag{2.56}
$$

Proof. (1) The number of m containing e_R is b, then

$$
P_I = \frac{q^{2s+1} \cdot q^k}{q^{2\nu-2} \cdot q^l} = \frac{1}{q^{2\nu-2s-3} \cdot q^{l-k}}.
\tag{2.57}
$$

(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 be successful. Because $e_R \subset e_T \subset m_1$, the opponent selects $e'_T \subset m_1$ satisfying $m_2 = s_2 + e'_T$ and $\dim(s_1 \bigcap s_2) = k_1$, then

$$
P_S = \frac{q^{k_1}}{q^{2s+1} \cdot q^k} = \frac{1}{q},
\tag{2.58}
$$

where $k_1 = 2s + k$.

(3) Assume that R is transmitter's encoding rules, Q is a source state, and $M = R + Q$. Therefore, the number of receiver's encoding rules contained in R is q^3. Let M' be another message, such that $M' = R' + Q$ and $R \neq R'$. Then, e_R contained $R \bigcap M'$ is at most q. So,

$$
P_T = \frac{q}{q^3} = \frac{1}{q^2}.
\tag{2.59}
$$

(4) From Lemmas 2.8 and 2.9, thus

$$P_{R_0} = \frac{q^{2(s-1)\cdot(q-1)\cdot q^{k-1}}}{\left(q^{2\nu-4} - q^{m_0-3}\right)\cdot q^{l-1}} = \frac{q-1}{q^{m_0-2s-1}\cdot q^{l-k}\left(q^{2\nu-m_0-1}-1\right)}. \tag{2.60}$$

(5) Assume that the receiver declares to receive a message m_2 instead of m_1, when s_2 contained in m_1 is different from s_2 contained in m_2; the receiver's substitution attack can be successful. Since $e_R \subset e_T \subset m_1$, 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

$$P_{R_1} = \frac{q^{k_1-4}}{q^{2(s-1)+(k-1)}\cdot(q-1)} = \frac{1}{q(q-1)}, \tag{2.61}$$

where $k_1 = 2s + k$. □

3. The Second Construction

In this section, from singular symplectic geometry and the first construction, we construct an authentication code with a transmitter and multi-receivers and compute the probabilities of success for different types of deceptions. For the definition of multi-receiver authentication codes, refer to [9].

Let $2s \le 2s_0 < m_0 \le \nu + m_0$, $m_0 < 2\nu - 1$, and $1 \le k < l$. Let p be a subspace $\langle v_1, v_2, e_{2\nu+1}\rangle$ of type $(3,0,1)$ in $F_q^{(2\nu+l)}$, and let P_0 be a fixed subspace of type $(m_0 + l, s_0, l)$ which contains P and orthogonal to v_2, but not orthogonal to v_1. Let $S = \{s \mid s\ is\ a\ subspace\ of\ type\ (2s+1+k, s, k), P \subset s \subset P_0\}$, Let $E = \{e \mid e\ is\ a\ subspace\ of\ type\ (5,2,1), e_T \bigcap P_0 = P\}$, Let $M = \{m \mid m\ is\ a\ subspace\ of\ type\ (2s+3+k, s+1, k), P \subset m,\ v_2 \notin m^{\perp}, m \bigcap P_0\ is\ a\ subspace\ of\ type\ (2s+1+k, s, k)\}$, and let $M^* = \{(m_1, m_2, \ldots, m^{\lambda}) | m_1 \bigcap U^{\perp} = m_2 \bigcap U^{\perp} = \ldots = m_{\lambda} \bigcap U^{\perp}\}$.

First, we construct $(\lambda+1)A$-codes. Let $C = (S, E^{\lambda}, M^*, f)$, where S, E^{λ}, and M^* are the sets of source states, keys, and authenticators of C, respectively, and $f : S \times E^{\lambda} \to M^*, f(s,e) = (s+e_1, s+e_2, \ldots, s+e_{\lambda})$ for $e = (e_1, e_2, \ldots, e_{\lambda}) \in E^{\lambda}$ is the authentication mapping of C. Let $C_i = (S, E_i, M_i; f_i)$, where $S, E_i = E$ and $M_i = M$ are the sets of source states, keys, and authenticators of C_i, respectively, and $f_i : S \times E_i \to M_i, f_i(s, e_i) = s + e_i$ for $e_i \in E_i$, is the authentication mapping of C_i. It is easy to know that C and C_i are well-defined A-codes.

Our authentication scheme is a $(\lambda+1)$-tuple $C; C_1, C_2, \ldots, C_{\lambda}$. Let $\tau_i : E^{\lambda} \to E_i, \tau_i(e) = e_i$ for $e = (e_1, e_2, \ldots, e_{\lambda}) \in E^{\lambda}$, and let $\pi_i : M^* \to M_i, \pi_i(m) = m_i$ for $m = (m_1, m_2, \ldots, m_{\lambda})$. Then,

$$\begin{gathered}\pi_i\left(f(s,e)\right) = \pi(s+e_1, s+e_2, \ldots, s+e_{\lambda}) = s+e_i,\\ f_i((I_s \times \tau_i)(s,e)) = f_i(I_s(s), \tau_i(e)) = f_i(s, e_i) = s + e_i.\end{gathered} \tag{3.1}$$

Therefore, $\pi_i(f(s,e)) = f_i((I_s \times \pi_i)(s,e))$. Thus, our scheme is indeed a well-defined authentication code with a transmitter and multi-receivers.

Theorem 3.1. *In the construction of multi-receiver authentication codes, if the encoding rules are chosen according to a uniform probability distribution, then the probabilities of impersonation attack and substitution attack are, respectively,*

$$P_I[i, J] = \frac{1}{q^{m_0+2\nu+2l-4s-2k-4} \cdot \left(q^{2\nu-m_0-1} - 1\right)},$$
$$P_S[i, J] = \frac{1}{q^{m_0+2\nu+2l-2s-k-5} \cdot \left(q^{2\nu-m_0-1} - 1\right)}, \tag{3.2}$$

where $J = \{i_1, i_2, \dots, i_j\}, i \notin J$.

Proof. Let $e_J = (e_{i_1}, e_{i_2}, \dots, e_{i_j})$, then

$$\tau_J(e) = e_J \Longleftrightarrow e = \left(\dots, e_{i_1}, \dots, e_{i_j}, \dots\right). \tag{3.3}$$

It is easy to know that $|e \in E^{\lambda} \mid \tau_J(e) = e_J| = |E|^{\lambda - j}$, and

$$f_i(s, e_i) = \pi_i(m), \quad s + e_i = m_i = \pi_i(m). \tag{3.4}$$

From Lemma 2.6, we know that the number of e_i satisfying (3.4) is a. For any e_i satisfying (3.4), the number of e satisfying $\tau_J(e), \tau_i(e) = e_i$ is $|E|^{\lambda - J - 1}$. So,

$$\left|\left\{e \in E^{\lambda} \mid \tau_J(e) = e_J, \tau_i(e) = e_i, f_i(s, e_i) = \pi_i(m)\right\}\right| = |E|^{\lambda - j - 1} \tag{3.5}$$

and $a = q^{4s+2k-5}$, thus

$$\begin{aligned} P_I[i, J] &= \max_{e_J \in E^J} \max_{s \in S} \max_{m \in M} \frac{\left|\left\{e \in E^{\lambda} \mid \tau_J(e) = e_J, \tau_i(e) = e_i, f_i(s, e_i) = \pi_i(m)\right\}\right|}{\left|\left\{e \in E^{\lambda} \mid \tau_J(e) = e_J\right\}\right|} \\ &= \max_{e_J \in E^J} \max_{s \in S} \max_{m \in M} \frac{a}{|E|} = \frac{q^{4s+2k-5}}{q^{(m_0-3)+2(\nu-2)+2(l-1)} \cdot \left(q^{2\nu-m_0-1} - 1\right)} \\ &= \frac{1}{q^{m_0+2\nu+2l-4s-2k-4} \cdot \left(q^{2\nu-m_0-1} - 1\right)}. \end{aligned} \tag{3.6}$$

Now, we compute the probability of substitution attack: we know that

$$m = f(s, e) = (s + e_1, s + e_2, \dots, s + e_{\lambda}) = (m_1, m_2, \dots, m_{\lambda}) \tag{3.7}$$

and $\tau_J(e) = (e_{i_1}, e_{i_2}, \ldots, e_{i_j})$, whenever $e = (e_1, e_2, \ldots, \underbrace{e_{i_1}, \ldots, e_{i_j}}, e_k, \ldots, e_\lambda)$, while

$$\left|\left\{e \in E^\lambda \mid m = f(s,e), \tau_J(e) = e_J\right\}\right| = |E|^{\lambda - j},$$
$$\left|\left\{e \in E^\lambda \mid m = f(s,e), \tau_J(e) = e_J, \tau_i(e) = e_i \in E_i, f_i(s', e_i) = \pi_i(m)\right\}\right| = |E|^{\lambda - j - 1} \cdot d \tag{3.8}$$

and $d = q^{k_1 - 4}$, therefore

$$\begin{aligned}
&P_S[i, J] \\
&= \max_{e_j \in E^J} \max_{s \in S,\ m \in M} \max_{s \neq s' \in S,\ m \in M} \frac{\left|\left\{e \in E^\lambda \mid m = f(s,e), \tau_J(e) = e_J, \tau_i(e) = e_i \in E_i, f_i(s', e_i) = \pi_i(m')\right\}\right|}{\left|\left\{e \in E^\lambda \mid m = f(s,e), \tau_J(e) = e_J\right\}\right|} \\
&= \max_{e_j \in E^J} \max_{s \in S,\ m \in M} \max_{s \neq s' \in S,\ m \in M} \frac{d}{|E|} \\
&= \max_{e_j \in E^J} \max_{s \in S,\ m \in M} \max_{s \neq s' \in S,\ m \in M} \frac{q^{k_1 - 4}}{q^{(m_0 - 3) + 2(\nu - 2) + 2(l - 1) \cdot (q^{2\nu - m_0 - 1} - 1)}} \\
&= \frac{1}{q^{m_0 + 2\nu + 2l - 2s - k - 5} \cdot \left(q^{2\nu - m_0 - 1} - 1\right)},
\end{aligned} \tag{3.9}$$

where $k_1 = 2s + k$. □

Two types of construction of authentication codes from singular symplectic geometry over finite fields are given. Among them, in the first construction, based on singular symplectic geometry structure of the authentication code with arbitration, the greatest probabilities of success for different types of deceptions are relatively lower, therefore there are some advantages. In addition, the second construction is based on singular symplectic geometry and is a multi-receiver authentication code. The probabilities of success for different types of deceptions are also computed. The results about multi-receiver authentication codes based on singular symplectic geometry are fewer. Thus, the structure of authentication code and the theory for further discussion are very meaningful.

Acknowledgments

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

References

[1] G. J. Simmons, “Message authentication with arbitration of transmitter/receiver disputes,” in *Proceedings of the Workshop on the Theory and Application of of Cryptographic Techniques (EUROCRYPT ’87)*, vol. 304 of *Lecture Notes in Computer Science*, pp. 151–165, 1987.

[2] Z. X. Wan, "Construction of Cartesian authentication codes from unitary geometry," *Designs, Codes and Cryptography*, vol. 2, no. 4, pp. 333–356, 1992.

[3] H. You and Y. Gao, "Some new constructions of Cartesian authentication codes from symplectic geometry," *Systems Science and Mathematical Sciences*, vol. 7, no. 4, pp. 317–327, 1994.

[4] T. Yayuan, "Construction of cartesian authentication codes from symplectic geometry," *Journal of Hebei Polytechnic University (Natual Science Edition)*, vol. 30, no. 1, pp. 49–53, 2008 (Chinese).

[5] G. You, S. Xinhua, and W. Hongli, "Constructions of authentication codes with arbitration from singular sympleetic geometry over finite fields," *Acta Scientiarum Naturalium Universitatis Nankaiensis*, vol. 41, no. 6, pp. 72–77, 2008.

[6] R. Li and L. Guo, "Construction of authentication codes with arbitration from unitary geometry," *Applied Mathematics Series B*, vol. 14, no. 4, pp. 475–480, 1999.

[7] G. You and W. Hong-Li, "Construction of authentication codes with arbitration from singular pseudo-symplectic geometry," in *Proceedings of the 7th International Conference on Machine Learning and Cybernetics (ICMLC '08)*, vol. 2, pp. 1183–1188, Kunming, China, 2008.

[8] W. Zhexian, *Geometry of Classical Groups over Finite Fields*, Science Press, Beijing, China, 2nd edition, 2002.

[9] R. Safavi-Naini and H. Wang, "Multireceiver authentication codes: models, bounds, constructions, and extensions," *Information and Computation*, vol. 151, no. 1-2, pp. 148–172, 1999.