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

Copyright © 2011 Y. Gao and H. Yu. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

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 $f : S \times E_T \rightarrow M$ and $g : M \times E_R \rightarrow S \cup \{\text{reject}\}$ 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 $\nu$. $e_i$ ($1 \leq i \leq 2\nu + l$) is row vector in $V$ whose $i$th coordinate is 1 and all other coordinates are 0. Denote by $E$ the $l$-dimensional subspace of $V$ generated by $e_{2\nu+1}, e_{2\nu+2}, \ldots, e_{2\nu+l}$. $K_l$ denotes the matrix

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

(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 $P_l$. Then,

$$
P_l = \max_{m \in M} \left\{ \frac{|e_R \in E_R \mid e_R \subset m|}{|E_R|} \right\}. \quad (1.2)
$$

2. The opponent’s substitution attack: the largest probability of an opponent’s successful substitution attack is $P_S$. Then,

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

3. The transmitter’s impersonation attack: the largest probability of a transmitter’s successful impersonation attack is $P_T$. Then,

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

4. The receiver’s impersonation attack: the largest probability of a receiver’s successful impersonation attack is $P_R$. Then,

$$
P_R = \max_{e_T \in E_T} \left\{ \frac{\max_{m \in M} |\{e_T \in E_T \mid e_T \subset m, p(e_R, e_T) \neq 0\}|}{|\{e_T \in E_T \mid p(e_R, e_T) \neq 0\}|} \right\}. \quad (1.5)
$$
The receiver’s substitution attack: the largest probability of a receiver’s successful substitution attack is $P_{R_i}$. Then,

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

(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 $\langle v_1, v_2, e_{2^{2\nu+1}} \rangle$ 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

$$(S, E_T, E_R, M; f, g),$$  

(2.1)

where the set of source states

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

(2.2)

the set of transmitter’s encoding rules:

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

(2.3)

the set of receiver’s decoding rules:

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

(2.4)

the set of messages:

$$M = \{ m \mid m \text{ is a subspace of type } (2s + 3 + k, s + 1, k), \ P \subset m,$$

$$v_2 \notin m^\perp, m \cap P_0 \text{ is a subspace of type } (2s + 1 + k, s, k) \},$$  

(2.5)

the encoding function:

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

(2.6)
and the decoding function: $g : M \times E_R \to S \cup \{\text{reject}\}$,

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

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

$$E_k = \begin{pmatrix} e_{2v+1} \\ e_{2v+2} \\ \vdots \\ e_{2v+k} \end{pmatrix}, \quad Q = \begin{pmatrix} Q_0 \\ v_1 \\ v_2 \\ E_k \end{pmatrix}, \quad (2.8)$$

which satisfies

$$Q_k Q^T = \begin{pmatrix} 0 & I^{(s-1)} \\ -I^{(s-1)} & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & -1 & 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ k \end{pmatrix}. \quad (2.9)$$

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

$$Q_k Q^T = \begin{pmatrix} 0 & I^{(s-1)} \\ -I^{(s-1)} & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & * & * \\ -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ * & -1 & 0 & 0 & 0 \\ * & 0 & -1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ k \end{pmatrix}. \quad (2.10)$$
Journal of Applied Mathematics

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 \( \langle v_1, v_2, e_{2s+1} \rangle \), so \( P \subseteq M \cap P_0 = Q \), 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 \( R = \langle v_1, v_2, u_1, u_2, e_{2s+1} \rangle \) is a subspace of type \((5, 2, 1)\), hence a transmitter’s encoding rule.

Assume that \( R = \langle v_1, v_2, u_1, u_2, e_{2s+1} \rangle \) 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 \( v_2K_iu_i^T \neq 0 \) or \( v_2K_iu_i^T \neq 0 \). Without loss of generality, let \( v_2K_iu_i^T = 1 \). If we also have \( v_2K_iu_i^T = 1 \), replacing \( u_1 \) by \( u_1 - u_2 \), we get \( v_2K_iu_i^T = 1 \) and \( v_2K_iu_i^T = 0 \). Since \( R \) is not a subspace of type \((5, 2, 1)\), certainly \( v_2K_iu_i^T = 0 \). 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 \( v_1K_iw^T = 1 \). Replacing \( u_1 \) by \( w + u_1 \), we have \( v_1K_iu_i^T = 1 \), \( v_2K_iu_i^T = 0 \) \( (v_2 \in Q^\perp) \). Then, \( R = \langle v_1, v_2, u_1, u_2, e_{2s+1} \rangle \) 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 \( Q' \subseteq M \cap P_0 = Q \), by \( Q' \subseteq M, Q' \subseteq P_0 \). 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 \( \langle v_2 \rangle^\perp \) containing \( P \), \( n_2 \), the number of subspaces of \((m_0 + l, s_0, l)\) contained in \( \langle v_2 \rangle^\perp \) containing a fixed subspace of type \((2s + 1 + k, s, k)\) as above, and \( n_3 \), the number of subspaces of \((m_0 + l, s_0, l)\) contained in \( \langle v_2 \rangle^\perp \) containing \( P \) and not contained in \( \langle v_1 \rangle^\perp \).

**Lemma 2.2.** One has

\[
n_1 = q^{2(v-s-1)} \cdot q^{(2s-1)(l-k)} \cdot N(2(s-1), s-1; 2(v-2)) \cdot N(k-1, l-1),
\]

\[
n_2 = N(m_0 - (2s + 1), s_0 - s; 2(v - s - 1)),
\]

\[
n_3 = q^{2(v-s-1)} \cdot q^{(2v-m_0-1)} \cdot N(m_0 - 3, s_0 - 1; 2(v - 2)).
\]

**Proof.** (1) Computation of \( n_1 \).

By the transitivity of \( Sp_{2s+1}(F_q) \) on the set of subspaces of the same type, we can assume that

\[
\begin{pmatrix}
v_1 \\
v_2
\end{pmatrix}
=egin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}
\begin{pmatrix}
1 & 1 & v-2 & 1 & 1 & v-2 & l
\end{pmatrix}
\]

Let \( Q \) be a subspace of type \((2s + 1 + k, s, k)\) contained in \( \langle v_2 \rangle^\perp \) containing \( P \). There exists a \( u \in Q \) such that \( v_1K_iu_i^T = 1 \). 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

\[
Q = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & R_1 & 1 & 0 & R_2 & 0 & 0 & R_3 \\
0 & 0 & Q_1 & 0 & 0 & Q_2 & 0 & 0 & Q_3 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & v-2 & 1 & 1 & v-2 & 1 & k-1 & l-k
\end{pmatrix}
\]

(2.13)
It is easy to verify that \( Q_1, Q_2 \) is a subspace of type \((2(s - 1), s - 1)\) in the \(2(\nu - 2)\)-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

\[
\begin{pmatrix}
I^{(s-1)} & 0 & 0 & 0 \\
0 & 0 & I^{(s-1)} & 0 \\
s - 1 & b & s - 1 & l - k
\end{pmatrix}
\]

(2.14)

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

\[
Q = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & a_4 & 1 & 0 & 0 & b_4 & 0 & 0 \\
0 & 0 & I^{(s-1)} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & I^{(s-1)} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & f^{(k-1)} & 0 \\
1 & 1 & a & b & 1 & 1 & a & b & k - 1 & l - k
\end{pmatrix},
\]

(2.15)

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

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

(2.16)

\((2)\) Computation of \(n_2\).

Let \(U\) be a subspace of type \((m_0 + l, s_0, l)\) contained in \(\langle \nu_2 \rangle\) 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

\[
U = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & I^{(s-1)} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & I^{(s-1)} & 0 & 0 & 0 \\
0 & 0 & 0 & P_1 & 0 & 0 & 0 & 0 & P_2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & f^{(l)} & 0 \\
1 & 1 & a & b & 1 & 1 & a & b & l
\end{pmatrix},
\]

(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 \(2(\nu - s - 1)\)-dimensional symplectic space. We have that

\[
n_2 = N(m_0 - (2s + 1), s_0 - s; 2(\nu - s - 1)).
\]

(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 $(v_2)^\perp$, containing $P$ and not contained in $(v_1)^\perp$. We may assume that the subspace has a matrix representation of the form

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

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

$$U_0 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & a_5 & 1 & 0 & 0 & b_1 & b_5 & 0 \\ 0 & 0 & I^{(s_0 - 1)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(s_0 - 1)} & 0 & 0 \\ 0 & 0 & 0 & I^{(a)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(l)} \\ 1 & 1 & c & a & b & 1 & 1 & c & a & b & l \end{pmatrix},$$  \hfill (2.20)

where $c = s_0 - 1, a = m_0 - 2s_0 - 1, b = v - m_0 + s_0, a_5, b_1, b_5$ arbitrarily. We may get

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

$\Box$

Lemma 2.3. The number of the source states is

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

$\Box$

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

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

$$|E_T| = q^{m_0 - 3 + 2(v - 2) + 2(l - 1)} \cdot q^{2v - m_0 - 1} - 1).$$  \hfill (2.23)
Proof. Since $|E_T|$ is the number of subspaces of type $(5,2,1)$ contained in $P_0$ and containing $P$, let $R = \langle v_1, v_2, u_1, u_2, e_{2v+1} \rangle$, where $v_1 K_i u_1^T = 1, v_2 K_i u_2^T = 1$, and $\langle v_1, u_1 \rangle \perp \langle v_2, u_2 \rangle$. By the transitivity of $Sp_{2v+1}(F_q)$ on the set of subspaces of the same type, we can assume that

$$P_0 = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & I^{(s_0-1)} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & I^{(v)} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & I^{(i)} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & I^{(k)} & 0 & 0 & 0 \\
1 & 1 & c & a & b & 1 & 1 & c & a & b & l
\end{pmatrix}.$$ (2.24)

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

$$u_1 = (0, 0, a_3, a_4, a_5, 1, b_3, b_4, b_5, 0, f_2),$$

$$u_2 = (0, 0, c_3, c_4, c_5, 0, 1, d_3, d_4, d_5, 0, g_2).$$ (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 $q^{(m_0-3)+2(v-2)+2(l-1)}q^{2v-m_0-1-1}$ and that for $u_2$ is $q^{2v-2+2(l-1)}$; we may get

$$|E_T| = q^{(m_0-3)+2(v-2)+2(l-1)}q^{2v-m_0-1-1}.$$ (2.26)

\[\blacksquare]\]

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

$$|E_R| = q^{2v-2}q^l.$$ (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 $v_2 K_i u^T = 1$. Following the notion of Lemma 2.4, hence $u$ has the form

$$u = (a_1, 0, a_3, a_4, a_5, b_1, 1, b_3, b_4, b_6, c_1).$$ (2.28)

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

$$|E_R| = q^{2v-2}q^l.$$ (2.29)

\[\blacksquare]\]
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,
\[
a = q^{4s - 3 + 2(k - 1)} \cdot (q - 1), \quad b = q^{2s + 1} \cdot q^k.
\]

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 \( R = (v_1, v_2, u_1, u_2, e_{2s+1}) \). Here, \( M = Q + (u_1, u_2), v_2Ku_2^T = 1 \). Following the notation of Lemma 2.4, we can assume that \( Q \) has a matrix representation of the form
\[
Q = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & I^{(s-1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & d & c & a & b & 1 & 1 & d & c & a & b & k-1 & l-k
\end{pmatrix}
\]
(2.31)

where \( a = m_0 - 2s_0 - 1, b = v + s_0 - m, c = s_0 - s, \) and \( d = s - 1 \). By \( v_2Ku_2^T = 1 \) and \( R \) being the subspace of type \((5, 2, 1)\), we can assume
\[
u_1 = (0, 0, a_3, a_4, a_5, a_6, b_1, 0, b_3, b_4, b_5, b_6, 0, f_2, f_3),
\]
\[
u_2 = (0, 0, c_3, c_4, c_5, c_6, d_1, 1, d_3, d_4, d_5, d_6, 0, g_2, g_3),
\]
(2.32)

where \( b_1 \neq 0 \). Then,
\[
M = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & I^{(s-1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(s-1)} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & d & c & a & b & 1 & 1 & d & c & a & b & k-1 & l-k
\end{pmatrix}
\]
(2.33)

where \( a = m_0 - 2s_0 - 1, b = v + s_0 - m, c = s_0 - s, \) 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 \( q^{2(s-1)+(k-1)} \).
Lemma 2.8. (1) For any \( u_2 \) is \( q^{2(s-1)+(k-1)+1} \). Then, the number of \( e_T \) contained in \( m \) is
\[
a = q^{4s-3+2(k-1)} \cdot (q-1).
\]
(2) Let \( H = (v_2, u) \) be a receiver’s encoding rule contained in \( M \), where \( v_2K_iu^T = 1 \). Clearly, \( u \notin Q \), then we can assume that \( u \) has the form
\[
u = (h_1, 0, h_3, h_4, h_5, h_6, i_1, 1, i_3, i_4, i_5, i_6, j_1, j_2, j_3).
\]
Note that
\[
(h_1, h_5, h_6, i_4, i_5, i_6, j_3) = k(a_4, a_5, a_6, b_4, b_5, b_6, f_3) + (c_4, c_5, c_6, d_4, d_5, d_6, g_3),
\]
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
\[
b = q \cdot q^2 \cdot q^{2(s-1)} \cdot q^k = q^{2s+1+k}.
\]

Lemma 2.7. The number of the messages is
\[
|M| = \frac{|S||E_T|}{q^{4s-k+2(k-1)}(q-1)}.
\]
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,
\[
|M| = \frac{|S||E_T|}{a} = \frac{|S||E_T|}{q^{4s-k+2(k-1)}(q-1)}.
\]

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 \( e_R \) containing \( e_T \) is \( (q^{2q-4} - q^{m_q-3}) \cdot q^{l-1} \).

Proof. (1) Let \( R \) be a transmitter’s encoding rule; we can assume that \( R = (v_1, v_2, u_1, u_2, e_{2v+1}) \). Here, \( v_2K_iu_2^T = 1 \), \( v_1K_iu_1^T = 1 \), and \( (v_1, u_1) \perp (v_2, u_2) \). Then, the receiver’s encoding rule \( H \) contained in \( R \) should have the form \( H = (v_2, k_1v_1 + k_2u_1 + u_2 + k_3e_{2v+1}) \), 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 \( H = (v_2, u) \), where \( v_2K_iu^T = 1 \). Therefore, \( (v_1, v_2, u, e_{2v+1}) \) is a subspace of type \((4, 1, 1)\). The number of subspace \( (v_1, v_2, u, u_1, e_{2v+1}) \) of type \((5, 2, 1)\) is \( q^{2q-4} \cdot q^{l-1} \). Here, \( v_1K_iu_1^T \neq 0 \). Note that \( v_2 \in P^+ \) and \( v_1 \notin P^+ \). It is easy to see that
the number of \( u_1 \in P_0 \) such that \((v_1, v_2, u_1, e_{2v+1})\) 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 \((q^{2v-4} - q^{m_0-3}) \cdot q^{l-1}\). \(\square\)

**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

\[
q^{2(s-1)+(k-1)} \cdot (q-1).
\]

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

\[
M = \begin{pmatrix}
    1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
    0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
    0 & 0 & I^{(s-1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
    0 & 0 & 0 & 0 & 0 & I^{(s-1)} & 0 & 0 & 0 & 0 \\
    0 & 0 & a_3 & a_4 & b_1 & 0 & b_4 & f_2 & f_3 & 0 \\
    0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
    0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
    0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
    1 & 1 & a & b & 1 & 1 & a & b & 1 & k-1 \quad l-k
  \end{pmatrix},
\]

where \( b_1 \neq 0, a = s-1, \) and \( b = v-s-1 \).

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 \( R = (v_1, v_2, u, u_1, e_{2v+1}) \), where \( v_1K_1u_1^T \neq 0 \). Thus, \( u_1 \) has the form

\[
u_1 = (0, 0, c_3, c_4, d_1, 0, d_3, d_4, 0, g_2, g_3),
\]

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

**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 \( s_0 = s_1 \cap s_2 \), \( \dim s_0 = k_1 \), then \( 3 \leq k_1 \leq 2s + k \), and

1. the number of \( e_R \) contained in \( m_1 \cap m_2 \) is \(q^{k_1}\);
2. for any \( e_R \subset m_1 \cap m_2 \), 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 \( m_1 \neq m_2 \), \( s_1 \neq s_2 \). Again because of \( s_1 \supset P_0 \) and \( s_2 \supset P_0 \), \( 3 \leq k_1 \leq 2s + k \). From \( m_1 = s_1 + e_T' = s_0 + s_1' + e_T' \), it is easy to know that \( m_1 \cap m_2 = s_0 + e_T' \). Therefore,

\[
\dim(m_1 \cap m_2) = \dim s_0 + \dim e_T' - \dim(s_0 \cap e_T') = k_1 + 5 - 3 = k_1 + 2.
\]
(1) By the definition of the message, we can assume that \( m_1 \) and \( m_2 \) have the form as follows, respectively:

\[
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & A_1 & 0 & 0 & A_2 & 0 \\
0 & 0 & a_3 & 0 & 1 & a_6 & 0 \\
0 & 0 & b_3 & b_4 & 0 & b_6 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & A_3 \\
1 & 1 & v - 2 & 1 & 1 & v - 2 & l
\end{pmatrix}
\]

\[
m_1 = \begin{pmatrix}
1 \\
1 \\
\end{pmatrix}
\]

\[
2(s - 1), \quad (2.44)
\]

where \( b_4 \neq 0 \),

\[
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & B_1 & 0 & 0 & B_2 & 0 \\
0 & 0 & c_3 & 0 & 1 & c_6 & 0 \\
0 & 0 & d_3 & d_4 & 0 & d_6 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & B_3 \\
1 & 1 & v - 2 & 1 & 1 & v - 2 & l
\end{pmatrix}
\]

\[
m_2 = \begin{pmatrix}
1 \\
1 \\
\end{pmatrix}
\]

\[
2(s - 1), \quad (2.45)
\]

where \( d_4 \neq 0 \). Thus,

\[
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & D_1 & 0 & 0 & D_2 & 0 \\
0 & 0 & f_3 & 0 & 1 & f_6 & 0 \\
0 & 0 & g_3 & g_4 & 0 & g_6 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & D_3 \\
1 & 1 & v - 2 & 1 & 1 & v - 2 & l
\end{pmatrix}
\]

\[
m_1 \cap m_2 = \begin{pmatrix}
1 \\
1 \\
\end{pmatrix}
\]

\[
2(s - 1), \quad (2.46)
\]

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

\[
\dim\begin{pmatrix}
0 & 0 & D_1 & 0 & 0 & D_2 & 0 \\
0 & 0 & f_3 & 0 & 1 & f_6 & 0 \\
0 & 0 & g_3 & g_4 & 0 & g_6 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & D_3
\end{pmatrix} = k_1 + 2 - 3 = k_1 - 1. \quad (2.47)
\]

If \( e_R \subset m_1 \cap m_2 \), then

\[
e_R = \begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
R_1 & 0 & R_4 & 1 & R_6 & R_7 \\
1 & 1 & v - 2 & 1 & 1 & v - 2 & l
\end{pmatrix}.
\]

\[
\quad (2.48)
\]
Since $R_1, R_4$ are arbitrary, every row of \((0 \ 0 \ R_3 \ 0 \ 1 \ R_6 \ R_7)\) 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 $m_1 \cap m_2$ is
\[
q^{k_1-2} \cdot q^2 = q^{k_1}.
\tag{2.50}
\]

(2) Assume that $m_1 \cap m_2$ has the form of (2.46), then, for any $e_R \subset m_1 \cap m_2$, we can assume that
\[
e_R = \begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
R_1 & 0 & R_3 & R_4 & 1 & R_6 & R_7 \\
1 & 1 & v-2 & 1 & 1 & v-2 & l
\end{pmatrix},
\tag{2.51}
\]
If $e_R \subset e_T$ and $e_T \subset m_1 \cap m_2$, then
\[
e_T = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & R_3 & R_4 & 1 & R_6 & 0 & R_7 \\
0 & 0 & R_3' & 1 & 0 & R_6' & 0 & R_7' \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & v-2 & 1 & 1 & v-2 & 1 & l-1
\end{pmatrix},
\tag{2.52}
\]
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 $q^{k_1-4}$. \qed
Theorem 2.11. The above construction yields an $A^2$-code with the following size parameters:

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

$$|E_T| = q^{(m_0-3)+2(v-2)+2(l-1)} \cdot \left(q^{2v-m_0-1} - 1\right),$$

$$|E_R| = q^{2v-2+l},$$

$$|M| = \frac{|S||E_T|}{q^{4s-3+2(k-1)} \cdot (q - 1)}. \tag{2.55}$$

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:

$$P_I = \frac{1}{q^{2v-2s-3} \cdot q^{l-k}}, \quad P_S = \frac{1}{q}, \quad P_T = \frac{1}{q^2},$$

$$P_{R_0} = \frac{q - 1}{q^{m_0-2s-1} \cdot q^{l-k}(q^{2v-m_0-1} - 1)}, \quad P_{R_1} = \frac{1}{q \cdot (q - 1)}. \tag{2.56}$$

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

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

(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 $\dim(s_1 \cap s_2) = k_1$, then

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

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 $R \cap M'$ 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

$$P_{R_0} = \frac{q^{2(s-1)(q-1)}q^{-1}}{(q^{2v-4} - q^{m_0-3})q^{-1}} = \frac{q - 1}{q^{m_0-2s-1}q^{-1-k}(q^{2v-m_0-1} - 1)}.$$  \hspace{1cm} (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 $e_R \subseteq e_T \subseteq m_1$, receiver is superior to select $e_T$, satisfying $e_R \subseteq e_T \subseteq m_1$, 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

$$P_{R_1} = \frac{q^{k_1-4}}{q^{2(s-1)(k-1)}(q-1)} = \frac{1}{q(q-1)}.$$  \hspace{1cm} (2.61)

where $k_1 = 2s + k$. \hfill \square

### 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 $2s \leq 2s_0 < m_0 \leq v + m_0$, $m_0 < 2v - 1$, and $1 \leq k < l$. Let $p$ be a subspace $\langle v_1, v_2, e_{2v+1} \rangle$ of type $(3,0,1)$ in $F_{2^{2v+1}}$, and let $P_0$ be a fixed subspace of type $(m_0 + l, s_0, l)$ which contains $P$ and orthogonal to $v_1$, but not orthogonal to $v_2$. Let $S = \{ s \mid s$ is a subspace of type $(2s + 1 + k, s, k) \}, P \subseteq s \subseteq P_0 \}$. Let $E = \{ e \mid e$ is a subspace of type $(5,2,1), e_T \cap P_0 = P \}$. Let $M = \{ m \mid m$ is a subspace of type $(2s + 3 + k, s + 1, k) \}, P \subseteq m, v_2 \not\subseteq m^\perp, m \cap P_0$ is a subspace of type $(2s + 1 + k, s, k) \},$ and let $M^* = \{(m_1, m_2, \ldots, m^k)\}m_1 \cup U^1 = m_2 \cup U^2 = \ldots = m_k \cup U^k$.

First, we construct $(\lambda + 1)^A$-codes. Let $C = (S, E^1, M^*, f)$, where $S, E^1, M^*$ are the sets of source states, keys, and authenticators of $C$, respectively, and $f : S \times E^1 \to M^*, f(s, e) = (s + e_1, s + e_2, \ldots, s + e_1)$ for $e = (e_1, e_2, \ldots, e_1) \in E^1$ 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 $\tau_i : E^1 \to E_i, \tau_i(e) = e_i$ for $e = (e_1, e_2, \ldots, e_1) \in E^1,$ and let $\pi_i : M^* \to M_i, \pi_i(m) = m_i$ for $m = (m_1, m_2, \ldots, m^k)$. Then,

$$\pi_i(f(s, e)) = \pi_i(s + e_1, s + e_2, \ldots, s + e_1) = s + e_i,$$

$$f_i((I_s \times \pi_i)(s, e)) = f_i(I_s(s), \pi_i(e)) = f_i(s, e_i) = s + e_i.$$

(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,

\[
P_i[i, J] = \frac{1}{q^{m_0+2v+2l-4s-2k-4} \cdot (q^{2v-m_0-1} - 1)},
\]

\[
P_S[i, J] = \frac{1}{q^{m_0+2v+2l-2s-k-5} \cdot (q^{2v-m_0-1} - 1)},
\]

where \( J = \{i_1, i_2, \ldots, i_j\}, i \notin J \).

Proof. Let \( e_j = (e_{i_1}, e_{i_2}, \ldots, e_{i_j}) \), then

\[
\tau_j(e) = e_j \iff e = (\ldots, e_{i_1}, \ldots, e_{i_j}, \ldots).
\]

It is easy to know that \(|e \in E^1 \mid \tau_j(e) = e_j| = |E|^{1-j} \), and

\[
f_i(s, e_i) = \pi_i(m), \quad s + e_i = m_i = \pi_i(m).
\]

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 \(|E|^{1-j-1} \). So,

\[
\left| \left\{ e \in E^1 \mid \tau_j(e) = e_j, \tau_i(e) = e_i, f_i(s, e_i) = \pi_i(m) \right\} \right| = |E|^{1-j-1}
\]

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

\[
P_i[i, J] = \max_{e_j \in E^J} \max_{s \in S} \max_{m \in M} \frac{\left| \left\{ e \in E^1 \mid \tau_j(e) = e_j, \tau_i(e) = e_i, f_i(s, e_i) = \pi_i(m) \right\} \right|}{\left| \left\{ e \in E^1 \mid \tau_j(e) = e_j \right\} \right|}
\]

\[
= \max_{e_j \in E^J} \max_{s \in S} \max_{m \in M} \frac{a}{|E|} = \frac{q^{4s+2k-5}}{q^{(m_0-3)+2(v-2)+2(l-1)} \cdot (q^{2v-m_0-1} - 1)}
\]

\[
= \frac{1}{q^{m_0+2v+2l-4s-2k-4} \cdot (q^{2v-m_0-1} - 1)}.
\]

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

\[
m = f(s, e) = (s + e_1, s + e_2, \ldots, s + e_j) = (m_1, m_2, \ldots, m_j)
\]
and $\tau_j(e) = (e_{1i}, e_{2i}, \ldots, e_{ki})$, whenever $e = (e_{1}, e_{2}, \ldots, e_{1i}, \ldots, e_{k}, \ldots, e_{\lambda})$, while

$$\left| \left\{ e \in E^k \mid m = f(s, e), \tau_j(e) = e_j \right\} \right| = |E|^{k-j},$$

$$\left| \left\{ e \in E^k \mid m = f(s, e), \tau_j(e) = e_j, \tau_i(e) = e_i \in E_{i}, f_{i}(s', e_i) = \tau_{i}(m) \right\} \right| = |E|^{k-i-1} \cdot d$$

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

$$P_S[i, j] = \max_{e_i \in E^k} \max_{\pi \in S, m \in M} \max_{s \in S, e \in E^k} \left| \left\{ e \in E^k \mid m = f(s, e), \tau_j(e) = e_j, \tau_i(e) = e_i \in E_{i}, f_{i}(s', e_i) = \tau_{i}(m') \right\} \right|$$

$$= \max_{e_i \in E^k} \max_{\pi \in S, m \in M} \max_{s \neq s' \in S, \pi \in M} \frac{d}{|E|}$$

$$= \max_{e_i \in E^k} \max_{\pi \in S, m \in M} \max_{s \neq s' \in S, \pi \in M} \frac{q^{k_i - 4}}{q^{m_{ij} + 2(s-2) + 2(l-1) - (q^{2s-1} - 1)}}$$

$$= \frac{1}{q^{m_{ij} + 2v + 2l - 2s - k - 5} \cdot (q^{2s-1} - 1)^4}$$

(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**


Submit your manuscripts at http://www.hindawi.com