A CONSTRUCTION OF CARTESIAN AUTHENTICATION CODE FROM ORTHOGONAL SPACES OVER A FINITE FIELD OF ODD CHARACTERISTIC

ZENGTI LI
Department of Mathematics, Langfang Normal College
Langfang, 065000, China

SUOGANG GAO*
Math. and Inf. College, Hebei Normal University
Shijiazhuang, 050016, China
sggao@hebtu.edu.cn

ZHONG WANG, BHAVANI THURAISINGHAM†
and WEILI WU‡
Department of Computer Science
University of Texas at Dallas, Richardson
Texas 75080, USA
†bxt043000@utdallas.edu
‡weiliwu@utdallas.edu

Accepted 14 January 2009

In this paper, we construct a Cartesian authentication code from subspaces of orthogonal space $F_{q}^{(2^e+1)}$ of odd characteristic and compute its parameters. Assuming that the encoding rules of the transmitter and the receiver are chosen according to a uniform probability distribution, the probabilities of successful impersonation attack and substitution attack are also computed.

Keywords: Authentication code; orthogonal space; classical groups.

Mathematics Subject Classification 2000: 05B25, 94A62

1. Introduction

We recall some terminology and definitions about authentication codes. For more theory about authentication codes, we would like to refer readers to [1, 4].

*Corresponding author. This paper was supported in part by Natural Science Foundation of Hebei Province, China (No. A2008000128), and Educational Committee of Hebei Province, China (No. 2007137).

†This paper was supported in part by National Science Foundation under grants CCF 0621829 and 0627233.
Let $S, E$ and $M$ denote three non-empty finite sets. Let $f : S \times E \rightarrow M$ be a map, the four tuple $(S, E, M; f)$ is called an authentication code, if

(i) the map $f : S \times E \rightarrow M$ is surjective and
(ii) for any $m \in M$ and $e \in E$, if there is an $s \in S$ satisfying $f(s, e) = m$, then such an $s$ is uniquely determined by the given $m$ and $e$.

Suppose that $(S, E, M; f)$ is an authentication code, then $S, E, M$ are called set of source states, set of encoding rules, and set of messages, respectively and $f$ is called encoding map. The cardinals $|S|, |E|, |M|$ are called size parameters of code. Moreover, if the authentication code satisfies the further requirement that given any message $m$ there is a unique source state $s$ such that $m = f(s, e)$ for every encoding rule $e$ contained in $m$, then the code is called a Cartesian authentication code.

Authentication codes are used in communication channels where besides the transmitter and the receiver there is an opponent who may play either impersonation attack or substitution attack. By an impersonation attack we mean that the opponent sends a message through the channel to the receiver and hopes the receiver will accept it as authentic, i.e., as a message sent by the transmitter. By a substitution attack we mean that after the opponent intercepts a message sent by the transmitter to the receiver, he sends another message instead and hopes the receiver will accept it as authentic. We denote by $P_I$ and $P_S$, respectively, the largest probabilities that could deceive the receiver when he play an impersonation attack and a substitution attack and call them the probability of a successful impersonation attack and of a successful substitution attack, respectively.

H. Wang, C. Xing and R. Safavi-Naini used the rank distance codes to construct some linear authentication codes [7]. Z. Wan constructed authentication codes from unitary space [5]. H. You and Y. Gao constructed some authentication codes from symplectic space [8]. S. Gao constructed two authentication codes from unitary space [3]. R. Feng, L. Hu and J. Kwak gave characterization of authentication codes in terms of bipartite graphs [2]. In this paper, we construct an authentication code from orthogonal spaces over a finite field of odd characteristic. Moreover, assuming that the encoding rules of the transmitter and the receiver are chosen according to a uniform probability distribution, we compute its parameters and probability of successful impersonation attack and substitution attack.

2. Orthogonal Space of Odd Characteristic

Let $F_q$ be a finite field of odd characteristic. For a fixed non-square element $z$ of $F_q^*$, let

$$S_{2\nu+\delta, \Delta} = \begin{pmatrix} 0 & f^{(e)} \\ f^{(e)} & 0 \\ \Delta \end{pmatrix},$$
where

\[
\Delta = \begin{cases} 
\emptyset, & \text{if } \delta = 0, \\
(1) \text{ or } (z), & \text{if } \delta = 1, \\
1 - z, & \text{if } \delta = 2.
\end{cases}
\]

The orthogonal group of degree \(2\nu + \delta\) over \(\mathbb{F}_q\), denoted by \(O_{2\nu+\delta,\Delta}(\mathbb{F}_q)\), consists of all \((2\nu+\delta)\times(2\nu+\delta)\) matrices \(T\) over \(\mathbb{F}_q\) satisfying \(T S_{2\nu+\delta,\Delta} T' = S_{2\nu+\delta,\Delta}\). There is an action of \(O_{2\nu+\delta,\Delta}(\mathbb{F}_q)\) on \(\mathbb{F}_q^{2\nu+\delta}\) as follows

\[
(\mathbb{F}_q^{2\nu+\delta}) \times O_{2\nu+\delta,\Delta}(\mathbb{F}_q) \to \mathbb{F}_q^{2\nu+\delta},
\]

\[
((x_1, x_2, \ldots, x_{2\nu+\delta}), T) \mapsto (x_1, x_2, \ldots, x_{2\nu+\delta}) T.
\]

The vector space \(\mathbb{F}_q^{2\nu+\delta}\) together with the above group action of the orthogonal group \(O_{2\nu+\delta,\Delta}(\mathbb{F}_q)\), is called the \((2\nu+\delta)\)-dimensional orthogonal space over \(\mathbb{F}_q\) of odd characteristic.

Let \(P\) be an \(m\)-dimensional subspace of \(\mathbb{F}_q^{2\nu+\delta}\). \(PS_{2\nu+\delta,\Delta} P'\) is cogredient to one of the following four forms

\[
M(m, 2r, r) = \begin{pmatrix} 0 & f(r) & 0 \\ f(r) & 0 & 0 \end{pmatrix},
\]

\[
M(m, 2r + 1, r, 1) = \begin{pmatrix} 0 & f(r) & 0 \\ f(r) & 1 & 0 \end{pmatrix},
\]

\[
M(m, 2r + 1, r, z) = \begin{pmatrix} 0 & f(r) & 0 \\ f(r) & z & 0 \end{pmatrix},
\]

and

\[
M(m, 2r + 2, r) = \begin{pmatrix} 0 & f(r) & 0 \\ f(r) & 1 & 0 \end{pmatrix}.
\]

We say that \(P\) is a subspace of type \((m, 2r + \gamma, r, \Gamma)\), if \(PS_{2\nu+\delta,\Delta} P'\) is cogredient to \(M(m, 2r + \gamma, r, \Gamma)\), where \(\Gamma = \emptyset\), if \(\gamma = 0\), and \(\Gamma = (1)\) or \((z)\), if \(\gamma = 1\), and \(\Gamma = (1 - z)\), if \(\gamma = 2\). In particular, subspaces of type \((m, 0, 0)\) are called \(m\)-dimensional totally isotropic subspaces and subspaces of type \((m, 2r + \gamma, r, \Gamma)\) with \(m = 2r + \gamma\) are called \(m\)-dimensional non-totally isotropic subspaces. The subspace
of type $(m, 2r + \gamma, r, \Gamma)$, which contains subspaces of type $(m_1, 2r_1 + \gamma_1, r_1, \Gamma_1)$, exists if and only if

$$2r + \gamma \leq m \leq \begin{cases} \nu + \delta, & \text{if } \gamma \neq \delta \text{ or } \gamma = \delta \text{ and } \Gamma = \Delta, \\ \nu + r, & \text{if } \gamma = \delta = 1 \text{ and } \Gamma \neq \Delta, \end{cases}$$

and

$$\min\{m - 2r - \gamma, m_1 - 2r_1 - \gamma_1\} \geq \begin{cases} \max\{0, m_1 - r - r_1 - \min\{\gamma, \gamma_1\}\}, & \text{if } \gamma_1 \neq \gamma, \text{ or } \gamma_1 = \gamma \text{ and } \Gamma_1 = \Gamma, \\ \max\{0, m_1 - r - r_1\}, & \text{if } \gamma_1 = \gamma = 1 \text{ and } \Gamma_1 \neq \Gamma. \end{cases}$$

It is known that the number of subspaces of type $(m, 2r + \gamma, r, \Gamma)$ in $\mathbb{F}_q^{2(\nu+1)}$, denoted by $N(m, 2r + \gamma, r, \Gamma; 2\nu + \delta, \Delta)$, is given by Theorem 6.26 of [6].

Two vectors $x$ and $y$ of $\mathbb{F}_q^{2(\nu+1)}$ are said to be orthogonal with respect to $S_{2\nu+\delta}$, if $xS_{2\nu+\delta}y' = 0$. Let $P$ be an $m$-dimensional subspace of $\mathbb{F}_q^{2(\nu+1)}$, we use the symbol $P^\perp$ to denote the set of vectors which are orthogonal to every vector of $P$ with respect to $S_{2\nu+\delta}$, i.e.

$$P^\perp = \{y \in \mathbb{F}_q^{2(\nu+1)} \mid yS_{2\nu+\delta}x' = 0 \text{ for all } x \in P\}.$$

3. Authentication Code Associated with Subspaces of Orthogonal Space of Odd Characteristic

Construction I In orthogonal space $\mathbb{F}_q^{2(\nu+1)}$, set $\Delta = \Gamma, 2r_0 + 1 \leq m_0 \leq \nu + r_0 + 1, r + r_0 + 2 \leq m_0, r \geq 1$. Let $(\nu_1, \nu_2)$ be a fixed 2-dimensional totally isotropic subspace, $P_0$ be a fixed subspace of type $(m_0, 2r_0 + 1, r_0, \Gamma)$, and $(\nu_1, \nu_2) \subset P_0 \subset (\nu_1, \nu_2)^\perp$. The source states are subspaces of type $(2r + 1, 2(r - 1) + 1, r - 1, \Gamma)$ containing $(\nu_1, \nu_2)$ in $P_0$. The encoding rules are subspaces of type $(3, 2, 1)$ which intersect $P_0$ at $(\nu_1, \nu_2)$ and are not orthogonal to $\nu_2$. The messages are subspaces of type $(2r + 2, 2r + 1, r, \Gamma)$ which intersect $P_0$ at subspace of type $(2r + 1, 2(r - 1) + 1, r - 1, \Gamma)$ containing $(\nu_1, \nu_2)$ and not orthogonal to $\nu_2$. Denote the set of source states, the set of encoding rules, and the set of messages by $S, E$ and $M$, respectively. Given a source state $s$ and an encoding rule $e$, the join $s + e$ of the subspaces $s$ and $e$ is regarded as the message into which the source state $s$ is encoded under $e$.


Proof. Let $s$ be an source state, i.e. $s$ is a subspace $Q$ of type $(2r + 1, 2(r - 1) + 1, r - 1, \Gamma)$ containing $(\nu_1, \nu_2)$ in $P_0$. Clearly, $Q$ has a matrix representation as follows

$$Q = \begin{pmatrix} Q_0 \\ \nu_1 \\ \nu_2 \end{pmatrix} = \begin{pmatrix} 2r - 1 \\ 1 \\ 1 \end{pmatrix} \quad (3.1)$$
such that

\[
QS_{2^\nu+1,\Delta}Q' = \begin{pmatrix}
  r - 1 & r - 1 & 1 & 1 & 1 \\
  0 & I^{(r-1)} & 0 & 0 & 0 \\
  0 & 0 & \Gamma & 0 & 0 \\
  0 & 0 & 0 & 0 & 1 \\
  0 & 0 & 0 & 0 & 1
\end{pmatrix}.
\]

(3.2)

Let \(e\) be an encoding rule, i.e. \(e\) is a subspace \(R\) of type \((3, 2, 1)\) which intersects \(P_0\) at \(\langle \nu_1, \nu_2 \rangle\) and is not orthogonal to \(\nu_2\). Therefore, there exists a \(u \in R\) such that \(\nu_2S_{2^\nu+\Delta}u' = 1\). It follows that \(R = \langle \nu_1, \nu_2, u\rangle\).

Since \(R\) is a subspace of type \((3, 2, 1)\), we have

\[
RS_{2^\nu+1,\Delta}R' = \begin{pmatrix}
  0 & 0 & 0 \\
  0 & 0 & 1 \\
  0 & 1 & 0
\end{pmatrix}.
\]

From (3.2), we have

\[
\begin{pmatrix}
  Q_0 \\
  \nu_1 \\
  \nu_2 \\
  u
\end{pmatrix}_{S_{2^\nu+1,\Delta}} = \begin{pmatrix}
  Q_0 \\
  \nu_1 \\
  \nu_2 \\
  u
\end{pmatrix}' = \begin{pmatrix}
  r - 1 & r - 1 & 1 & 1 & 1 \\
  0 & I^{(r-1)} & 0 & 0 & 0 \\
  0 & 0 & \Gamma & 0 & 0 \\
  0 & 0 & 0 & 0 & 1 \\
  0 & 0 & 0 & 0 & 1
\end{pmatrix}.
\]

It follows that \(M = Q + R = Q_0 \oplus \langle \nu_1, \nu_2, u\rangle\) is a subspace of type \((2^r + 2, 2^r + 1, r, \Gamma)\) and is not orthogonal to \(\nu_2\), and \(M \cap P_0\) is a subspace of type \((2^r + 1, 2(r - 1) + 1, r - 1, \Gamma)\). So \(M\) is a message.

Let \(M \in M\) be a subspace of type \((2^r + 2, 2^r + 1, r, \Gamma)\) which intersects \(P_0\) at subspace of type \((2^r + 2, 2(r - 1) + 1, r - 1, \Gamma)\), containing \(\langle \nu_1, \nu_2 \rangle\) and not orthogonal to \(\nu_2\). Set \(Q = M \cap P_0\), then \(\langle \nu_1, \nu_2 \rangle \subset Q\) and \(Q\) is a subspace of type \((2^r + 1, 2(r - 1) + 1, r - 1, \Gamma)\). So \(Q\) is a source state. Let \(M = Q \oplus \langle u\rangle\). Since \(M\) is not orthogonal to \(\nu_2\) and \(Q \subset P_0 \subset \langle \nu_1, \nu_2 \rangle^\perp\), we have \(\nu_2S_{2^\nu+\Delta}u' \neq 0\). It follows that \(R = \langle \nu_1, \nu_2, u\rangle\) is an encoding rule and \(M = Q + R\).

Suppose that \(Q^*\) is another source which is encoded into \(M\) under an encoding rule \(R^*\), i.e. \(M = Q^* + R^*\). As a source state, \(Q^* \subset P_0\), we have \(Q^* \subset M \cap P_0 = Q\) and \(\dim Q^* = \dim Q = 2^r + 1\). It follows that \(Q^* = Q\). This proves that the source state \(Q\) is uniquely determined by \(M\).

**Lemma 3.2.** Let \(n_1\) denote the number of subspaces of type \((2^r + 1, 2(r - 1) + 1, r - 1, \Gamma)\) containing \(\langle \nu_1, \nu_2 \rangle\) and contained in \(\langle \nu_1, \nu_2 \rangle^\perp\) and let \(n_2\) denote the number of subspaces of type \((m_0, 2r_0 + 1, r_0, \Gamma)\) containing a fixed subspace of type \((2^r + 1, 2(r - 1) + 1, r - 1, \Gamma)\) containing \(\langle \nu_1, \nu_2 \rangle\) and contained in \(\langle \nu_1, \nu_2 \rangle^\perp\). Assume
that \( n_3 \) is the number of subspaces of type \((m_0, 2r_0 + 1, r_0, \Gamma)\) containing \((\nu_1, \nu_2)\) and contained in \((\nu_1, \nu_2)^\perp\). Then

\[
\begin{align*}
n_1 &= N(2r - 1, 2(r - 1) + 1, r - 1, \Gamma; 2(\nu - 2) + 1), \\
n_2 &= N(m_0 - 2r - 1, 2(r_0 - r + 1), r_0 - r + 1; 2(\nu - r - 1)), \\
n_3 &= N(m_0 - 2, 2r_0 + 1, r_0, \Gamma; 2(\nu - 2) + 1).
\end{align*}
\]

**Proof.** (i) Since the orthogonal group \(O_{2\nu + \delta, \Delta}(F_q)\) acts transitively on each set of subspaces of the same type, we may assume that

\[
\begin{pmatrix}
\nu_1 \\
\nu_2
\end{pmatrix} = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}.
\]

Let \(Q\) be a subspace of type \((2r + 1, 2(r - 1) + 1, r - 1, \Gamma)\) containing \((\nu_1, \nu_2)\) and contained in \((\nu_1, \nu_2)^\perp\). We may assume that

\[
Q = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & Q_1 & 0 & 0 & Q_2 & Q_3
\end{pmatrix}.
\]

Clearly, \((Q_1, Q_2, Q_3)\) is a subspace of type \((2r - 1, 2(r - 1) + 1, r - 1, \Gamma)\) in \(F_q^{2(\nu - 2) + 1}\). Hence \(n_1 = N(2r - 1, 2(r - 1) + 1, r - 1, \Gamma; 2(\nu - 2) + 1)\).

(ii) Let \(P\) be a subspace of type \((m_0, 2r_0 + 1, r_0, \Gamma)\) containing a fixed subspace of type \((2r + 1, 2(r - 1) + 1, r - 1, \Gamma)\) containing \((\nu_1, \nu_2)\) and contained in \((\nu_1, \nu_2)^\perp\).

Since the orthogonal group \(O_{2\nu + \delta, \Delta}(F_q)\) acts transitively on each set of subspaces of the same type, we may assume that \(P\) has a matrix representation

\[
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & I^{(r-1)} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & I^{(r-1)} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & P_1 & 0 & 0 & 0 & P_2
\end{pmatrix}.
\]

It follows that

\[
PS_{2\nu + 1, \Delta}P' = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & I^{(r-1)} & 0 & 0 & 0 & 0 \\
0 & 0 & I^{(r-1)} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \Delta & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & P_2 P_1' + P_1 P_2'
\end{pmatrix}.
\]
where \((P_1,P_2)\) is a subspace of type \((m_0 - 2r - 1, 2(r_0 - r + 1), r_0 - r + 1)\) in \(\mathbb{F}^{(\nu - r - 1)}\). Therefore, \(n_2 = N(m_0 - 2r - 1, 2(r_0 - r + 1), r_0 - r + 1; 2(\nu - r - 1))\).

(iii) Similar to the proof of (i), we obtain
\[
  n_3 = N(m_0 - 2, 2r_0 + 1, r_0, \Gamma; 2(\nu - 2) + 1).
\]

**Lemma 3.3.** Let \(S\) be as in construction I. Then
\[
|S| = \frac{N(2(r - 1), (2r - 2) + 1, r - 1, \Gamma; 2(\nu - 2) + 1)N(m_0 - 2r - 1, 2(r_0 - r + 1), r_0 - r + 1; 2(\nu - r - 1))}{N(m_0 - 2, 2r_0 + 1, r_0, \Gamma; 2(\nu - 2) + 1)}.
\]

**Proof.** \(|S|\) is the number of subspaces of type \((2r + 1, 2(r - 1) + 1, r - 1, \Gamma)\) containing \(\langle \nu_1, \nu_2 \rangle\) in \(P_0\). Define a binary matrix, whose rows are indexed by all subspaces of type \((2r + 1, 2(r - 1) + 1, r - 1, \Gamma)\) containing \(\langle \nu_1, \nu_2 \rangle\) and contained in \(\langle \nu_1, \nu_2 \rangle^\perp\) (they are \(n_1\) in number), whose columns are indexed by all subspaces of type \((m_0, 2r_0 + 1, r_0, \Gamma)\) containing \(\langle \nu_1, \nu_2 \rangle\) and contained in \(\langle \nu_1, \nu_2 \rangle^\perp\) (they are \(n_3\) in number), with a 1 or 0 in the \((i, j)\) position of matrix, if the \(i\)-th subspace of type \((2r + 1, 2(r - 1) + 1, r - 1, \Gamma)\) is or is not contained in the \(j\)-th subspace of type \((m_0, 2r_0 + 1, r_0, \Gamma)\), respectively. Clearly, the number of each row containing 1 is equal to the number of subspaces of type \((m_0, 2r_0 + 1, r_0, \Gamma)\) containing a fixed subspace of type \((2r + 1, 2(r - 1) + 1, r - 1, \Gamma)\). This number equals \(n_2\). Similarly, the number of each column containing 1 is equal to the number of subspaces of type \((m_0, 2r_0 + 1, r_0, \Gamma)\) contained in a fixed subspace of type \((2r + 1, 2(r - 1) + 1, r - 1, \Gamma)\) contained in a fixed subspace of type \((m_0, 2r_0 + 1, r_0, \Gamma)\). This number equals \(|S|\). Counting the number of 1’s in the matrix by rows and columns, respectively, we get \(|S| \cdot n_3 = n_1 \cdot n_2\). By Lemma 3.2, the lemma holds.

**Lemma 3.4.** Let \(E\) be as in construction I. Then
\[
|E| = q^{2\nu - 2}.
\]

**Proof.** \(|E|\) is the number of subspaces of type \((3, 2, 1)\) which intersect \(P_0\) at \(\langle \nu_1, \nu_2 \rangle\) and not orthogonal to \(\nu_2\). Set \(R = \langle \nu_1, \nu_2 \rangle \in E\), then \(\nu_2 S_{2\nu + 1, \Delta} u' \neq 0\). So we obtain
\[
\begin{array}{cccccc}
1 & 1 & \nu - 2 & 1 & 1 & \nu - 2 & 1 \\
1 & a_1 & a_2 & a_3 & a_4 & \\
u & 0 & 0 & 0 & 0 & 0
\end{array}
\]
Therefore, \(|E| = q^{2\nu - 2}\).

**Lemma 3.5.** The number of encoding rules contained in a massage is \(q^{2r - 1}\).

**Proof.** Let \(M\) be a message, i.e. \(M\) is a subspace of type \((2r + 2, 2r + 1, r, \Gamma)\) which intersects \(P_0\) at a subspace of type \((2r + 1, 2(r - 1) + 1, r - 1, \Gamma)\), is not orthogonal to \(\nu_2\) and containing \(\langle \nu_1, \nu_2 \rangle\). Set \(Q = M \cap P_0\), then \(Q\) is a source state contained in \(M\). By the proof of Lemma 3.1, there exists an encoding rules \(R \subset M\). Let \(R = \langle \nu_1, \nu_2, u \rangle\), where \(\nu_2 S_{2\nu + 1, \Delta} u' = 1\), then \(u \in Q\) and \(M = Q \oplus \langle u \rangle\). Since the orthogonal group \(O_{2\nu + 4, \Delta}(\mathbb{F}_q)\) acts transitively on each set of subspaces of the same
type, we may assume that
\[ Q = \begin{pmatrix}
1 & 1 & r - 1 & \nu - r - 1 & 1 & 1 & r - 1 & \nu - r - 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & I^{(r-1)} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}. \]

Since \( \nu_2 S_{2^\nu+1, \Delta u'} = 1 \), we may assume that
\[ u = \begin{pmatrix}
1 & 1 & r - 1 & \nu - r - 1 & 1 & 1 & r - 1 & \nu - r - 1 & 1 \\
0 & 0 & a_1 & a_2 & a_3 & 1 & a_4 & a_5 & a_6
\end{pmatrix}. \]

Thus
\[ M = \begin{pmatrix}
1 & 1 & r - 1 & \nu - r - 1 & 1 & 1 & r - 1 & \nu - r - 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & I^{(r-1)} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(r-1)} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & a_1 & a_2 & a_3 & 1 & a_4 & a_5 & a_6
\end{pmatrix}. \]

Since \( M \) is a fixed message, \( a_2, a_3, a_5 \) are fixed. It follows that the number of encoding rules contained in a message is \( q^{2r-1} \).

**Lemma 3.6.** Let \( M, S \) and \( E \) be as in construction \( I \). Then
\[ |M| = q^{2\nu-2r-1} |S|. \]

**Proof.** By Lemma 3.1, each message contains a unique source state. By Lemma 3.5, each message contains \( q^{2r-1} \) encoding rules. Thus
\[ |M| \cdot q^{2r-1} = |S| \cdot |E|. \]

Therefore, \( |M| = q^{2\nu-2r-1} |S| \).

**Lemma 3.7.** Let \( M_1 \) and \( M_2 \) be two distinct messages and let \( Q_1 \) and \( Q_2 \) be the source states contained in \( M_1 \) and \( M_2 \), respectively. Assume \( \dim(Q_1 \cap Q_2) = s \). Then \( 2 \leq s \leq 2r \), and the number of encoding rules contained in \( M_1 \cap M_2 \) is \( q^s \).

**Proof.** Let \( Q_0 = Q_1 \cap Q_2 \). Clearly, \( 2 \leq s \leq 2r \) and \( \langle \nu_1, \nu_2 \rangle \subset Q_0 \). If \( R = \langle \nu_1, \nu_2, u \rangle \) is an encoding rule contained in \( M_1 \cap M_2 \), then
\[ M_1 = Q_1 + R = Q_1 \oplus \langle u \rangle, \quad M_2 = Q_2 + R = Q_2 \oplus \langle u \rangle. \]
Since $M_1 \neq M_2$, we have $Q_1 \neq Q_2$. So, there exist subspace $Q_1'$ of $Q_1$ and subspace $Q_2'$ of $Q_2$, such that

$$Q_1 = Q_0 \oplus Q_1', \quad Q_2 = Q_0 \oplus Q_2'.$$

It follows that

$$M_1 = Q_0 \oplus Q_1' \oplus \langle u \rangle, \quad M_2 = Q_0 \oplus Q_2' \oplus \langle u \rangle,$$

where $u \in R$ and $\nu_2 S_{2v+1, \Delta} u' = 1$. Clearly, $\langle \nu_1, \nu_2, \alpha + u \rangle$ is an encoding rule contained in $M_1 \cap M_2$, where $\alpha \in Q_0$.

Conversely, let $\langle \nu_1, \nu_2, w \rangle$ be an encoding rule contained in $M_1 \cap M_2$, where $\nu_2 S_{2v+1, \Delta} w' = 1$. Write

$$w = \alpha_1 + w_1 + \lambda_1 u, \quad \alpha_1 \in Q_0, \quad w_1 \in Q_1', \quad \lambda_1 \in \mathbb{F}_q,$$

$$w = \alpha_2 + w_2 + \lambda_2 u, \quad \alpha_2 \in Q_0, \quad w_2 \in Q_2', \quad \lambda_2 \in \mathbb{F}_q.$$

Since $Q_1 \oplus \langle u \rangle$ and $Q_2 \oplus \langle u \rangle$ are direct sum, we obtain $\lambda_1 = \lambda_2 = \lambda$. It follows that $\alpha_1 + w_1 = \alpha_2 + w_2$. Hence $w_1 = w_2 = 0, \alpha_1 = \alpha_2 = \alpha$. Therefore, $w = \alpha + \lambda u$. Since $\nu_2 S_{2v+1, \Delta} w' = 1$, we have $\lambda = 1$. So $\langle \nu_1, \nu_2, w \rangle = \langle \nu_1, \nu_2, \alpha + u \rangle$, where $\alpha \in Q_0$.

Let $R = \langle \nu_1, \nu_2, \alpha + u \rangle$ and $R' = \langle \nu_1, \nu_2, \alpha^* + u \rangle$. Note that $R = R'$ if and only if $\alpha - \alpha^* = \lambda_1 \nu_1 + \lambda_2 \nu_2, \lambda_1, \lambda_2 \in \mathbb{F}_q$. Hence the number of encoding rules contained in $M_1 \cap M_2$ is $\frac{q^2}{q^2} = q^{-2}$.

Assuming now that the encoding rules are chosen according to a uniform probability distribution, let us compute $P_I$ and $P_S$. By Lemma 3.4 and Lemma 3.5, we have

$$P_I = \frac{q^{2r-1}}{q^{2v-2}} = \frac{1}{q^{2v-2r-1}}.$$ 

By Lemma 3.5 and Lemma 3.7, we have

$$P_S(M_2|M_1) = \frac{q^{s-2}}{q^{2v-1}} = \frac{1}{q^{2v-s+1}}.$$ 

Clearly, given any source state $Q_1$ there is a source state $Q_2$ such that $\dim(Q_1 \cap Q_2) = 2r$. Hence $P_S = \frac{1}{q}$. Summarizing, we obtain

**Theorem 3.8.** Construction I yields a Cartesian authentication code with parameters

$$N(2r - 1, (2r - 2) + 1, r - 1, \Gamma; 2(\nu - 2) + 1)N(m_0 - 2r - 1, 2(r_0 - r + 1),$$

$$|S| = \frac{N(m_0 - 2, 2r_0 + 1, r_0, \Gamma; 2(\nu - 2) + 1)}{N(m_0 - 2r - 1, 2(r_0 - r + 1)},$$

$$|\mathcal{E}| = q^{2r-2},$$

$$|\mathcal{M}| = q^{2v-2r-1}|S|,$$
where

\[
N(2r - 1, (2r - 2) + 1, r - 1, \Gamma; 2(\nu - 2) + 1), N(m_0 - 2r - 1, 2(r_0 - r + 1), r_0 - r + 1; 2(\nu - r - 1)), N(m_0 - 2, 2r_0 + 1, r_0, \Gamma; 2(\nu - 2) + 1)
\]

are given by Theorem 6.26 of [6]. Moreover, assume that the encoding rules are chosen according to a uniform probability distribution. Then

\[
P_I = \frac{1}{q^{2\nu - 2r - 1}}, \quad P_S = \frac{1}{q}.
\]

References