Journal of Mathematical Research & Exposition
Mar., 2011, Vol. 31, No. 2, pp. 269–278
DOI:10.3770/j.issn:1000-341X.2011.02.010
Http://jmre.dlut.edu.cn

A Construction of Authentication Codes with Arbitration from Vector Spaces over Finite Fields

Wei Jia LI†, **Ji Zhu NAN***
School of Mathematical Sciences, Dalian University of Technology, Liaoning 116024, *P. R. China*

Abstract This paper is devoted to constructing an authentication code with arbitration using subspaces of vector spaces over finite fields. Moreover, if we choose the encoding rules of the transmitter and the decoding rules of the receiver according to a uniform probability distribution, then some parameters and the probabilities of successful attacks are computed.

Keywords authentication code with arbitration; vector space; finite field.

Document code A
MR(2010) Subject Classification 94A62
Chinese Library Classification O157.4

1. Introduction

Let (S, E_T, E_R, M) be four non-empty finite sets and $f : S \times E_T \to M$ and $g : M \times E_R \longrightarrow S \cup \{\text{reject}\}$ be two maps. The six-tuple (S, E_T, E_R, M, f, g) is called an authentication code with arbitration if it satisfies the following conditions:

(i) f and g are surjective;

(ii) For any $m \in M$ and $e_T \in E_T$, if there exists s in S such that $f(s, e_T) = m$, then s is uniquely determined by the given m and e_T;

(iii) If $e_T \in E_T$ and $e_R \in E_R$ are mutually relative (i.e., $s \in S$ encoded by e_T can be interpreted to itself by e_R), then $f(s, e_T) = m$ implies $g(m, e_R) = s$, where $m \in M$.

In an authentication code with arbitration (S, E_T, E_R, M, f, g), if $f(s, e_T) = m$, then we say that m is obtained by e_T encoding s and that e_T is contained in m; and if $g(m, e_R) = s$, we say that e_R is contained in m. The sets S, M, E_T, E_R are called the set of source states, the set of messages, the set of encoding rules of transmitter and the set of decoding rules of receiver, respectively. The cardinals $|S|$, $|M|$, $|E_T|$, $|E_R|$ are called parameters of this code.

The concept of authentication codes with arbitration was introduced by Simmons [1] to provide protection against deceptions from both outsiders (opponent) and insiders (transmitter and receiver). Sometimes, an authentication code with arbitration is simply called an A^2-model and it includes a fourth person, called the arbiter. The arbiter is assumed to be honest and he

Received June 18, 2009; Accepted April 26, 2010
Supported by the National Natural Science Foundation of China (Grant No. 10771023).
† Corresponding address: No. 13 Middle School of Dalian Developement Area, Liaoning 116650, P. R. China.
* Corresponding author
E-mail address: liwj871@yahoo.com.cn (W. J. LI); jznan@163.com (J. Z. NAN)

has access to all information, including e_T and e_R, but does not take part in any communication activities on the channel. His only task is to resolve possible disputes between the transmitter and the receiver whenever such occur.

It is well known that every authentication code with arbitration has the following five types of cheating attacks:

I, impersonation by the opponent. The opponent sends a message to the receiver and succeeds if this message is accepted by the receiver as authentic.

S, substitution by the opponent. The opponent observes a message that is transmitted and replaces this message with another. The opponent is successful if this other message is accepted by the receiver as authentic.

T, impersonation by the transmitter. The transmitter sends a message to the receiver and then denies having sent it. The transmitter succeeds if this message is accepted by the receiver as authentic and if this message is not one of the messages that the transmitter could have generated due to his encoding rule.

R_0, impersonation by the receiver. The receiver claims to have received a message from the transmitter. The receiver succeeds if this message could have been generated by the transmitter due to his encoding rule.

R_1, substitution by the receiver. The receiver receives a message from the transmitter, but claims to have received another message. The receiver succeeds if this other message could have been generated by the transmitter due to his encoding rule.

For the above five possible deceptions, we denote the probability of success in each attack by P_I, P_S, P_T, P_{R_0}, P_{R_1}, respectively.

Recently, some authentication codes based on geometry of the classical groups [2, 3, 5, 7] and normal form of matrices [4] over finite fields were constructed. In this paper, the vector spaces over finite fields will be applied to construct an authentication code with arbitration and moreover, its parameters and the serval probabilities of successful attacks are computed.

2. Matrix representations of vector spaces over finite fields

In this section we will recall some results for matrix representations of vector spaces over finite fields.

Definition 2.1 *Let $\mathbf{F}_q$ be a finite field and V be an n-dimensional vector space over $\mathbf{F}_q$. Suppose $a_1, a_2, \ldots, a_n$ is a basis of V, P is a subspace of V, $P = L(b_1, b_2, \ldots, b_t)$ and $A = (a_{ij})_{t\times n}$, where*

$$\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_t \end{pmatrix} = A \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}.$$

Then A is called a matrix representation of P on the basis $a_1, a_2, \ldots, a_n$. Clearly, $b_1, b_2, \ldots, b_t$ is a basis of P if and only if $\operatorname{rank}(A) = t$.

Theorem 2.2 ([5]) *Let A, B be $t \times n$ and $t_1 \times n$ matrices respectively ($t \leq t_1 \leq n$). Then the space represented by A is a subspace of the space represented by B if and only if there exists a $t\times$ t_1 matrix Q such that $A = QB$.*

Corollary 2.3 ([5]) *Let A, B be $t \times n$ matrices. Then the spaces represented by A and B respectively are the same if and only if there exists an invertible matrix Q in $GL_t(\mathbf{F}_q)$ such that $A = QB$.*

Corollary 2.4 ([5]) *Let the matrix $A_{k\times n}$ represent k-dimensional vector space P and $B_{k_1\times n}$ represent k_1-dimensional vector space Q. If $P \cap Q = \{0\}$, then the matrix $\binom{A}{B}$ represents the vector space $P \oplus Q$.*

Theorem 2.5 *Let P be a k-dimensional vector space with a basis $a_1, \ldots, a_k$ and $P \subset N$, where N is an n-dimensional vector space. Extend $a_1, a_2, \ldots, a_k$ to a basis $a_1, \ldots, a_k, a_{k+1}, \ldots, a_n$ of N, then V is a complementary subspace of P if and only if V has the matrix representation of the form $(A_{(n-k)\times k}, I_{n-k})$, where $A_{(n-k)\times k}$ is uniquely determined by the complementary subspace of P.*

Proof Assume that $(A_{(n-k)\times k}, I_{n-k})$ represents the vector space V, and

$$\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_{n-k} \end{pmatrix} = \begin{pmatrix} A_{(n-k)\times k} & I_{n-k} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix},$$

then $c_1, c_2, \ldots, c_{n-k}$ is a basis of V, and $\dim V = n - k$. If $x \in V \cap P$, then

$$x = \sum_{i=1}^{n-k} (l_i)(c_i) = m_1 a_1 + \cdots + m_k a_k + \sum_{i=1}^{n-k} (l_i)(a_{k+i}) \in P.$$

This means that

$$l_i = 0 \ (1 \leq i \leq n-k), \quad V \cap P = \{0\},$$

and V is a complementary subspace of P.

If V is a complementary subspace of P, then V has the matrix representation of the form $(A_{(n-k)\times k}, I_{n-k})$ (see the Proof of Lemma 3 in [5]).

Next we prove the uniqueness of $A_{(n-k)\times k}$. If (A, I) and (A_1, I) represent the same complementary subspace V of P, then there exists an invertible matrix D such that $(A, I) = D(A_1, I) = (DA_1, D)$. Consequently, $D = I$ and $A = A_1$. $\Box$

Theorem 2.6 ([6]) *Let $N(t, n)$ be the number of t-dimensional subspace of n-dimensional vector space V and $N(k, t; n)$ be the number of k-dimensional subspace contained in t-dimensional vector space of V. Then $N(t, n) = \frac{\prod_{i=n-t+1}^{n}(q^i-1)}{\prod_{i=1}^{t}(q^i-1)}$ and $N(k, t; n) = N(k, t)$.*

3. Construction of an authentication code with arbitration

Let $\mathbf{F}_q$ be a finite field with q elements, where q is a power of a prime and n is a positive integer. Let $\mathbf{F}_q^{(n)}$ be the n-dimensional vector space over $\mathbf{F}_q$. Suppose t and t_0 are two positive integers $(0 < 2t < t_0 < n-1)$, P_1 is a fixed (t_0+1)-dimensional subspace of $\mathbf{F}_q^{(n)}$, and P_0, contained in P_1, is a fixed t_0-dimensional subspace. We define the following sets:

$$\begin{aligned} S &:= \{s \mid s \subset P_0, \dim s = t\}, \\ M &:= \{m \mid m \subset \mathbf{F}_q^{(n)},\ m \cap P_0 \in S,\ \dim m = n - t_0 + t\}, \\ E_T &:= \{e_T \mid e_T \text{ is a complementary subspace of } P_0 \text{ in } \mathbf{F}_q^{(n)}\}, \\ E_R &:= \{e_R \mid e_R \text{ is a complementary subspace of } P_1 \text{ in } \mathbf{F}_q^{(n)}\}. \end{aligned}$$

For all $s \in S$, $e_T \in E_T$, we define the map

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

where $m \in M$, $e_R \in E_R$, and the map $g : M \times E_R \longrightarrow S \cup \{\text{reject}\}$ is defined by

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

Theorem 3.1 *The construction yields an authentication code with arbitration.*

Proof (i) For all $m \in M$, suppose $s = m \cap P_0$ and e_T is a complementary subspace of s in m, then $m = s + e_T$. Since $\dim m = n - t_0 + t$, $\dim e_T = n - t_0$, and $e_T \cap P_0 = \{0\}$, $e_T \in E_T$, and f is surjective.

For all $s \in S$, $e_R \in E_R$, there exists e_T in E_T, such that $e_R \subset e_T$. Denote $m = s + e_T$, then $m \cap P_0 = s$, and $\dim m = t + n - t_0$. Therefore, $m \in M$ and g is surjective.

(ii) For all $m \in M$, if there exist s_1 and s_2, such that $f(s_1, e_T) = f(s_2, e_T) = m$, then $m = s_1 + e_T = s_2 + e_T$ and $m \cap P_0 = (s_1 + e_T) \cap P_0 = (s_2 + e_T) \cap P_0$. Consequently, $s_1 = s_2$.

(iii) If e_T and e_R are mutually relative, $m = f(s, e_T)$ and $e_R \subset m$, then by the definition, we have $g(m, e_R) = m \cap P_0 = (s + e_T) \cap P_0 = s$, hence $g(m, e_R) = s$. □

4. Computation of parameters and P_I, P_S, P_T, P_{R_0}, P_{R_1}

Lemma 4.1 *The cardinal number of the set S is $|S| = \frac{\prod_{i=t_0-t+1}^{t_0}(q^i-1)}{\prod_{i=1}^{t}(q^i-1)}$.*

Proof It is easy to see $|S| = N(t, t_0; n) = N(t, t_0) = \frac{\prod_{i=t_0-t+1}^{t_0}(q^i-1)}{\prod_{i=1}^{t}(q^i-1)}$. □

Lemma 4.2 *The cardinal number of set E_T and E_R are $|E_T| = q^{t_0(n-t_0)}$ and $|E_R| = q^{(t_0+1)(n-t_0-1)}$.*

Proof Choose $a_1, a_2, \ldots, a_{t_0}, a_{t_0+1}, \ldots, a_n$ as a basis of $\mathbf{F}_q^{(n)}$, where $a_1, a_2, \ldots, a_{t_0}$ is a basis of P_0 and $a_1, a_2, \ldots, a_{t_0}, a_{t_0+1}$ is a basis of P_1. Thus by Theorem 2.5, for all $e_T \subset E_T$, it has the matrix representation of the form $(A_{(n-t_0)\times t_0}, I_{n-t_0})$, whence $|E_T| = q^{t_0(n-t_0)}$. Similarly, $|E_R| = q^{(t_0+1)(n-t_0-1)}$. □

Lemma 4.3 *The cardinal number of the set M is $|M| = q^{(n-t_0)(t_0-t)}\frac{\prod_{i=t_0-t+1}^{t_0}(q^i-1)}{\prod_{i=1}^{t}(q^i-1)}$.*

Proof Let $m \in M$, $s = m \cap P_0$ and $f(s, e_T) = m$. Then e_T is a complementary subspace of $m \cap P_0$ in m. Therefore, by Theorem 2.5, we know that the number of e_T in m is $q^{t\times(n-t_0)}$, whence $|M| = \frac{|\psi||e_T|}{q^{t\times(n-t_0)}}$. □

Theorem 4.4 *The parameters of the above construction are as follows:*

$$|S| = \frac{\prod_{i=t_0-t+1}^{t_0}(q^i-1)}{\prod_{i=1}^{t}(q^i-1)}, \quad |M| = q^{(n-t_0)(t_0-t)}\ \frac{\prod_{i=t_0-t+1}^{t_0}(q^i-1)}{\prod_{i=1}^{t}(q^i-1)},$$
$$|E_T| = q^{t_0(n-t_0)}, \quad |E_R| = q^{(t_0+1)(n-t_0-1)}.$$

Lemma 4.5 *e_T is related to e_R if and only if $e_R \subset e_T$.*

Proof If $e_R \subset e_T$, then for all $s \in S$, $e_R \subset s + e_T$, so e_T is related to e_R.

If e_T is related to e_R, then for all $s \in S$, $e_R \subset s + e_T$. Choose $a_1, a_2, \ldots, a_t$ as a basis of s and $a_{t+1}, \ldots, a_{n-t_0+t}$ as a basis of e_T. Since $0 < 2t < t_0$, there exist $b_1, b_2, \ldots, b_t$ in P_0 such that $a_1, a_2, \ldots, a_t, b_1, b_2, \ldots, b_t$ are linear independence. Let $s' = L(b_1, b_2, \ldots, b_t)$. Then $e_R \subset s' + e_T$. Consequently, for all $x \in e_R$, we have

$$x = \sum_{i=1}^{n-t_0+t} l_i a_i = \sum_{i=1}^{t} m_i b_i + \sum_{i=t+1}^{n-t_0+t} m_i a_i.$$

Furthermore, $P_0 \cap e_T = \{0\}$, therefore $l_i = m_i = 0$ $(i = 1, 2, \ldots, t)$, and $l_j = m_j$ $(j = t+1, \ldots, n-t_0+t)$, whence $x \in e_T, e_R \subset e_T$. □

Lemma 4.6 *(i) Given an encoding rule e_T, then the number of e_R related to it is $q^{(n-t_0-1)}$; (ii) Given a decoding rule e_R, then the number of e_T related to it is q^{t_0}.*

Proof (i) Choose $a_1, a_2, \ldots, a_{t_0}$ as a basis of P_0, and extend it to a basis $a_1, a_2, \ldots, a_{t_0}, a_{t_0+1}$ of P_1. Given an encoding rule e_T with a basis $\beta_{t_0+1}, \ldots, \beta_n$, then P_1 has the matrix representation of the form $\begin{pmatrix} I & 0 \\ \lambda_1 & \lambda_2 \end{pmatrix}$ on a basis $a_1, a_2, \ldots, a_{t_0}, \beta_{t_0+1}, \ldots, \beta_n$ of $\mathbf{F}_q^{(n)}$, and $\begin{pmatrix} I & 0 \\ 0 & \lambda_2 \end{pmatrix}$ is also a matrix representation of P_1. Hence $a_{t_0+1} \in e_T$, extend it to a basis $a_{t_0+1}, a_{t_0+2}, \ldots, a_n$ of e_T. Consequently, $a_1, a_2, \ldots, a_{t_0+1}, \ldots, a_n$ is a basis of $\mathbf{F}_q^{(n)}$.

If e_T is related to e_R, then $e_R \subset e_T$. Thus e_R has the matrix representation of the form

$$\begin{pmatrix} 0_{(n-t_0-1)t_0}, & A_{(n-t_0-1)(n-t_0)} \end{pmatrix} = \begin{pmatrix} 0_{(n-t_0-1)t_0}, & C_{(n-t_0-1)\times 1}, & D_{n-t_0-1} \end{pmatrix}.$$

Furthermore, e_R has the matrix representation of the form

$$\begin{pmatrix} B_{(n-t_0-1)(t_0+1)}, & I_{n-t_0-1} \end{pmatrix} = \begin{pmatrix} E_{(n-t_0-1)t_0}, & F_{(n-t_0-1)\times 1}, & I_{n-t_0-1} \end{pmatrix}.$$

So there exists an invertible matrix Q, such that

$$Q\begin{pmatrix} E_{(n-t_0-1)t_0}, & F_{(n-t_0-1)\times 1}, & I_{n-t_0-1} \end{pmatrix} = \begin{pmatrix} 0_{(n-t_0-1)t_0}, & C_{(n-t_0-1)\times 1}, & D_{n-t_0-1} \end{pmatrix}.$$

It is easy to see that $E = 0$, $QF = C$, $Q = D$. Obviously, e_R has the matrix representation of the form $\begin{pmatrix} 0_{(n-t_0-1)t_0}, & F_{(n-t_0-1)\times 1}, & I_{n-t_0-1} \end{pmatrix}$. Since F is uniquely determined by e_R, the number of e_R related to e_T is $q^{(n-t_0-1)}$.

(ii) Given a decoding rule e_R with a basis $a_{t_0+2}, \ldots, a_n$. Choose $a_1, a_2, \ldots, a_{t_0}, a_{t_0+1}, \ldots, a_n$ as a basis of $\mathbf{F}_q^{(n)}$, where $a_1, a_2, \ldots, a_{t_0}$ is a basis of P_0 and $a_1, a_2, \ldots, a_{t_0}, a_{t_0+1}$ is a basis of P_1. Then e_R has the matrix representation of the form

$$\begin{pmatrix} 0_{(n-t_0-1)(t_0+1)}, & I_{n-t_0-1} \end{pmatrix} = \begin{pmatrix} 0_{(n-t_0-1)t_0}, & 0_{(n-t_0-1)\times 1}, & I_{n-t_0-1} \end{pmatrix}.$$

Since e_T has the matrix representation of the form

$$\begin{pmatrix} A_{(n-t_0)t_0} & I_{n-t_0} \end{pmatrix} = \begin{pmatrix} B_{1\times t_0} & 1 & 0 \\ C_{(n-t_0-1)t_0} & 0 & I_{n-t_0-1} \end{pmatrix}$$

and $e_R \subset e_T$, there exists a matrix $\begin{pmatrix} Q_1 & Q_2 \end{pmatrix}$ such that

$$\begin{aligned} \begin{pmatrix} 0_{(n-t_0-1)t_0} & 0_{(n-t_0-1)\times 1} & I_{n-t_0-1} \end{pmatrix} &= \begin{pmatrix} Q_1 & Q_2 \end{pmatrix} \begin{pmatrix} B_{1\times t_0} & 1 & 0 \\ C_{(n-t_0-1)t_0} & 0 & I_{n-t_0-1} \end{pmatrix} \\ &= \begin{pmatrix} Q_1 B + Q_2 C & Q_1 & Q_2 \end{pmatrix}. \end{aligned}$$

It is not difficult to see that $Q_1 = 0$, $Q_2 = I$, $C = 0$. Hence e_T has the matrix representation of the form $\begin{pmatrix} B_{1\times t_0} & 1 & 0 \\ 0 & 0 & I_{n-t_0-1} \end{pmatrix}$. Since B is uniquely determined by e_T, the number of e_T related to e_R is q^{t_0}. $\square$

Lemma 4.7 *The probability of a successful impersonation attack by the opponent is* $P_I = \frac{1}{q^{(t_0-t)(n-t_0-1)}}$.

Proof For any $m \in M$, let $s = m \cap P_0$ and $m = s + e_T$. Choose $a_1, a_2, \ldots, a_{t_0}, a_{t_0+1}$ as a basis of P_1, where $a_1, a_2, \ldots, a_t$ is a basis of s and $a_1, a_2, \ldots, a_{t_0}$ is a basis of P_0. Thus by Theorem 4.6 (i), $a_{t_0+1} \in e_T$ and $a_{t_0+1}, a_{t_0+2}, \ldots, a_n$ is a basis of e_T. Therefore, m has the matrix representation of the form $\begin{pmatrix} I_{t+1} & 0 & 0 \\ 0 & 0 & I_{n-t_0-1} \end{pmatrix}$ on the basis

$$a_1, \ldots, a_t, a_{t_0+1}, a_{t+1}, \ldots, a_{t_0}, a_{t_0+2}, \ldots, a_n$$

of $\mathbf{F}_q^{(n)}$, whence e_R has the matrix representation of the form

$$\begin{pmatrix} A_{(n-t_0-1)(t_0+1)}, & I_{(n-t_0-1)} \end{pmatrix} = \begin{pmatrix} B_{(n-t_0-1)(t+1)}, & C_{(n-t_0-1)(t_0-t)}, & I_{(n-t_0-1)} \end{pmatrix}.$$

Since $e_R \subset m$, there exists a matrix $\begin{pmatrix} Q_1 & Q_2 \end{pmatrix}$ such that

$$\begin{aligned} \begin{pmatrix} B_{(n-t_0-1)(t+1)} & C_{(n-t_0-1)(t_0-t)} & I_{(n-t_0-1)} \end{pmatrix} &= \begin{pmatrix} Q_1 & Q_2 \end{pmatrix} \begin{pmatrix} I_{t+1} & 0 & 0 \\ 0 & 0 & I_{n-t_0-1} \end{pmatrix} \\ &= \begin{pmatrix} Q_1 & 0 & Q_2 \end{pmatrix}. \end{aligned}$$

Thus $Q_1 = B$, $Q_2 = I_{(n-t_0-1)}$, $C = 0$, and e_R has the matrix representation of the form $\begin{pmatrix} B_{(n-t_0-1)(t+1)}, & 0, & I_{(n-t_0-1)} \end{pmatrix}$. So the number of e_R in m is $q^{(t+1)(n-t_0-1)}$, and

$$P_I = \max_{m\in M} \left\{ \frac{\text{the number of } e_R \text{ in } m}{|E_R|} \right\} = \frac{1}{q^{(t_0-t)(n-t_0-1)}}. \quad \square$$

Lemma 4.8 *The probability of a successful substitution attack by the opponent is* $P_S = \frac{1}{q^{(n-t_0-1)}}$.

Proof Suppose $m, m' \in M$ where $m \cap P_0 = s$, $m' \cap P_0 = s'$, and $s \neq s'$. Choose $a_1, \ldots, a_{t_0}, a_{t_0+1}$ as a basis of P_1, where $a_1, a_2, \ldots, a_t$ is a basis of s and $a_1, a_2, \ldots, a_{t_0}$ is a basis of P_0. Thus by Theorem 4.7, m has the matrix representation of the form $\begin{pmatrix} I_{t+1} & 0 & 0 \\ 0 & 0 & I_{n-t_0-1} \end{pmatrix}$ on a basis $a_1, \ldots, a_t, a_{t_0+1}, a_{t+1}, \ldots, a_{t_0}, a_{t_0+2}, \ldots, a_n$ of $\mathbf{F}_q^{(n)}$. Since $e_R \subset m$, and also by Theorem 4.7, e_R has the matrix representation of the form $\begin{pmatrix} B_{(n-t_0-1)(t+1)}, & 0, & I_{(n-t_0-1)} \end{pmatrix}$. Since $e_R \subset m'$, extend $a_{t_0+2}, \ldots, a_n$ to a basis $b_1, \ldots, b_t, b_{t+1}, a_{t_0+2}, \ldots, a_n$ of m', and m' has the matrix representation of the form $\begin{pmatrix} D_{(t+1)(t_0+1)} & D_1 \\ 0 & I_{n-t_0-1} \end{pmatrix}$, whence

$$\begin{pmatrix} D & 0 \\ 0 & I_{n-t_0-1} \end{pmatrix} = \begin{pmatrix} E_{(n-t_0-1)(t+1)} & F_{t_0-t} & 0 \\ 0 & 0 & I_{n-t_0-1} \end{pmatrix}$$

also represents m'. Consequently, by $e_R \subset m'$, there exists a matrix $\begin{pmatrix} M_1 & M_2 \end{pmatrix}$ such that

$$\begin{pmatrix} B_{(n-t_0-1)(t+1)} & 0 & I_{(n-t_0-1)} \end{pmatrix} = \begin{pmatrix} M_1 & M_2 \end{pmatrix} \begin{pmatrix} E_{(n-t_0-1)(t+1)} & F_{t_0-t} & 0 \\ 0 & 0 & I_{n-t_0-1} \end{pmatrix}$$

$$= \begin{pmatrix} M_1 E & M_1 F & M_2 \end{pmatrix}.$$

Therefore, $M_1 D = \begin{pmatrix} B, & 0 \end{pmatrix}$, $M_2 = I_{(n-t_0-1)}$, and the space represented by

$$\begin{pmatrix} B, & 0_{(n-t_0-1)(n-t-1)} \end{pmatrix}$$

is a subspace of the space represented by $\begin{pmatrix} D, & 0_{(t+1)(n-t_0-1)} \end{pmatrix}$, that is to say, it is the best way for opponent to make $\dim(m \cap m')$ as much as possible. Since $s \neq s'$, $\max \dim(s \cap s') = t - 1$, and $\max \dim(m \cap m') = n - t_0 + t - 1$, which means that one column of the first t columns of B is 0 , so the number of e_R in m and m' is at most $q^{(n-t_0-1)t}$, and

$$P_S = \max_{m \in M} \left\{ \frac{\max\limits_{m' \in M} \{\text{the number of } e_R \text{in } m \text{ and } m'\}}{\text{the number of } e_R \text{ in } m} \right\} = \frac{1}{q^{(n-t_0-1)}}. \quad \square$$

Lemma 4.9 *The probability of a successful impersonation attack by the transmitter is* $P_T = \frac{1}{q^{(n-t_0-1)}}$.

Proof Given an encoding rule e_T and $m \in M$, where m cannot be encoded by e_T. Assume that $m \cap P_0 = s$ and choose $a_1, a_2, \ldots, a_{t_0}, a_{t_0+1}$ as a basis of P_1, where $a_1, a_2, \ldots, a_t$ is a basis of s and $a_1, a_2, \ldots, a_{t_0}$ is a basis of P_0. Consequently, by Lemma 4.6 (i), $a_1, a_2, \ldots, a_{t_0+1}, \ldots, a_n$ is a basis of $\mathbf{F}_q^{(n)}$, and $e_T = L(a_{t_0+1}, \ldots, a_n)$, whence e_R has the matrix representation of the form

$$\begin{aligned} &\begin{pmatrix} 0_{(n-t_0-1)(t_0)}, & F_{(n-t_0-1)\times 1}, & I_{n-t_0-1} \end{pmatrix} \\ &= \begin{pmatrix} 0_{(n-t_0-1)t}, & 0_{(n-t_0-1)(t_0-t)}, & F_{(n-t_0-1)\times 1}, & I_{n-t_0-1} \end{pmatrix}. \end{aligned}$$

Since $m=(m\cap P_0)\oplus e'_T$, where $e'_T\subset E_T$, m has the matrix representation of the form

$$\begin{pmatrix} I_t & 0_{n-t} \\ A_{(n-t_0)t_0} & I_{n-t_0} \end{pmatrix} = \begin{pmatrix} I_t & 0_{t_0-t} & 0_{n-t_0} \\ C_1 & C_2 & I_{n-t_0} \end{pmatrix}.$$

Hence

$$\begin{pmatrix} I_t & 0_{t_0-t} & 0_{n-t_0} \\ 0 & C_2 & I_{n-t_0} \end{pmatrix} = \begin{pmatrix} I_t & 0 & 0 & 0_{n-t_0-1} \\ 0 & A_1 & 1 & 0 \\ 0 & A_2 & 0 & I_{n-t_0-1} \end{pmatrix}$$

also represents the vector space m. Since $\begin{pmatrix} I_t & 0_{t_0-t} & 0_{n-t_0} \\ 0 & 0 & I_{n-t_0} \end{pmatrix}$ represents the space $(m\cap P_0)+e_T$, $C_2=\begin{pmatrix} A_1 \\ A_2 \end{pmatrix}\neq 0$. Otherwise $m=(m\cap P_0)+e_T$, which is contradictory. Since $e_R\subset m$, there exists a matrix $\begin{pmatrix} Q_1 & Q_2 & Q_3 \end{pmatrix}$ such that

$$\begin{aligned} &\begin{pmatrix} 0_{(n-t_0-1)t} & 0_{(n-t_0-1)(t_0-t)} & F_{(n-t_0-1)\times 1} & I_{n-t_0-1} \end{pmatrix} \\ &= \begin{pmatrix} Q_1 & Q_2 & Q_3 \end{pmatrix} \begin{pmatrix} I_t & 0 & 0 & 0_{n-t_0-1} \\ 0 & A_1 & 1 & 0 \\ 0 & A_2 & 0 & I_{n-t_0-1} \end{pmatrix} \\ &= \begin{pmatrix} Q_1 & Q_2A_1+Q_3A_2 & Q_2 & Q_3 \end{pmatrix}. \end{aligned}$$

Thus $Q_1=0$, $Q_2=F$, $Q_3=I$, $FA_1+A_2=0$, $A_1^{\mathrm{T}}F^{\mathrm{T}}=-A_2^{\mathrm{T}}$, and $A_1\neq 0$, otherwise $A_2=0$, $C_2=0$, which is contradictory. Since A_1^{T} is of the type $(t_0-t)\times 1$ and F^{T} is of the type $1\times(n-t_0-1)$, every column of F^{T} is a solution of a non-homogeneous equations. Therefore, F^{T} has at most one choice and the number of e_R in m related to e_T is at most 1, and

$$P_T=\max_{e_T}\left\{\frac{\max\limits_{e_T\not\subseteq m}\{\text{the number of } e_R \text{ in } m \text{ related to } e_T\}}{\text{the number of } e_R \text{ related to } e_T}\right\}=\frac{1}{q^{(n-t_0-1)}}.\ \square$$

Lemma 4.10 *The probability of a successful impersonation attack by the receiver is* $P_{R_0}=\frac{1}{q^{t_0-t}}$.

Proof Given a decoding rule e_R with a basis $a_{t_0+2},\ldots,a_n$ and $m\in M$, where $e_R\subset m$ and $m\cap P_0=s$. Choose $a_1,a_2,\ldots,a_t$ as a basis of s, and extend it to a basis $a_1,a_2,\ldots,a_{t_0}$ of P_0. If we choose $a_1,a_2,\ldots,a_t,a_{t_0+1},\ldots,a_n$ as a basis of m, then m has the matrix representation of the form $\begin{pmatrix} I_t & 0 & 0 \\ 0 & 0 & I_{n-t_0} \end{pmatrix}$ on a basis $a_1,a_2,\ldots,a_{t_0+1},\ldots,a_n$ of $\mathbf{F}_q^{(n)}$. If e_T related to e_R is contained in m, then $e_R\subset e_T\subset m$, and e_T has the matrix representation of the form $\begin{pmatrix} B_{(n-t_0)t_0}, & I_{n-t_0} \end{pmatrix}=\begin{pmatrix} C_{(n-t_0)t}, & D_{(n-t_0)(t_0-t)}, & I_{n-t_0} \end{pmatrix}$. Therefore, referring to $e_T\subset m$, there exists a matrix $\begin{pmatrix} Q_1 & Q_2 \end{pmatrix}$ such that

$$\begin{aligned} \begin{pmatrix} C_{(n-t_0)t} & D_{(n-t_0)(t_0-t)} & I_{n-t_0} \end{pmatrix} &= \begin{pmatrix} Q_1 & Q_2 \end{pmatrix}\begin{pmatrix} I_t & 0 & 0 \\ 0 & 0 & I_{n-t_0} \end{pmatrix} \\ &= \begin{pmatrix} Q_1 & 0 & Q_2 \end{pmatrix}, \end{aligned}$$

whence $C = Q_1$, $D = 0$, $Q_2 = I_{n-t_0}$ and e_T has the matrix representation of the form

$$\begin{pmatrix} C_{(n-t_0)t}, & 0_{(n-t_0)(t_0-t)}, & I_{n-t_0} \end{pmatrix}.$$

Furthermore, by Lemma 4.7 (ii), we know that e_T has the matrix representation of the form $\begin{pmatrix} B_{1\times t_0} & 1 & 0 \\ 0 & 0 & I_{n-t_0-1} \end{pmatrix}$. Therefore e_T has the matrix representation of the form

$$\begin{pmatrix} E_{1\times t} & 0_{1\times(t_0-t)} & 1 & 0 \\ 0 & 0 & 0 & I_{n-t_0-1} \end{pmatrix},$$

and the number of e_T in m related to e_R is q^t. Finally

$$P_{R_0} = \max_{e_R}\left\{\frac{\max\limits_{m}\{\text{the number of } e_T \text{ in } m \text{ related to } e_R\}}{\text{the number of } e_T \text{ related to } e_R}\right\} = \frac{1}{q^{t_0-t}}. \quad \square$$

Lemma 4.11 *The probability of a successful substitution attack by the receiver is* $P_{R_1} = \frac{1}{q}$.

Proof Given a decoding rule e_R with a basis $a_{t_0+2}, \ldots, a_n$. Suppose m and m' are two messages from different source states, $m \cap P_0 = s$, $m' \cap P_0 = s'$ and $a_1, a_2, \ldots, a_t$ is a basis of s. Extend it to a basis $a_1, a_2, \ldots, a_{t_0}$ of P_0. If we choose $a_1, a_2, \ldots, a_t, a_{t_0+1}, \ldots, a_n$ as a basis of m, then $a_1, a_2, \ldots, a_{t_0+1}, \ldots, a_n$ is a basis of $\mathbf{F}_q^{(n)}$. Since $e_R \subset e_T \subset m$, and also by Lemma 4.10., we know that e_T has the matrix representation of the form

$$\begin{pmatrix} B_{1\times t} & 0_{1\times(t_0-t)} & 1 & 0 \\ 0 & 0 & 0 & I_{n-t_0-1} \end{pmatrix} = \begin{pmatrix} E_{(n-t_0)\times t_0} & I_{n-t_0} \end{pmatrix}.$$

Therefore, by $e_T \subset m$ and $e_T \subset m'$, if $\beta_1, \beta_2, \ldots, \beta_t, a_{t_0+1}, \ldots, a_n$ is a basis of m', then m' has the matrix representation of the form $\begin{pmatrix} A_{t\times t_0} & 0 \\ 0 & I_{n-t_0} \end{pmatrix}$. Since $e_T \subset m'$, there exists a matrix $\begin{pmatrix} Q_1 & Q_2 \end{pmatrix}$ such that

$$\begin{pmatrix} E & I_{n-t_0} \end{pmatrix} = \begin{pmatrix} Q_1 & Q_2 \end{pmatrix}\begin{pmatrix} A_{t\times t_0} & 0 \\ 0 & I_{n-t_0} \end{pmatrix}.$$

Hence $E = Q_1 A$, $Q_2 = I_{n-t_0}$, and the space represented by $\begin{pmatrix} E, & 0_{n-t_0} \end{pmatrix}$ is a subspace of the space represented by $\begin{pmatrix} A, & 0_{t\times(n-t_0)} \end{pmatrix}$. Since $E = \begin{pmatrix} B_{1\times t} & 0 \\ 0 & 0 \end{pmatrix}$, whence it is the best way for opponent to make $\dim(s \cap s')$ as much as possible. Consequently, from $s \neq s'$, we have $\max\dim(s \cap s') = t - 1$. That is to say , one column of the first t columns of B is 0, therefore the number of e_T in m and m' related to e_R is at most q^{t-1}, whence

$$P_{R_1} = \max_{e_R, m}\left\{\frac{\max\limits_{m'\in M}\{\text{the number of } e_T \text{ in } m \text{ and } m' \text{ related to } e_R\}}{\text{the number of } e_T \text{ in } m \text{ related to } e_R}\right\} = \frac{1}{q}. \quad \square$$

Theorem 4.12 *The probabilities of successful attacks of the authentication code with arbitration gotten from the above construction are as follows:*

$$P_I = \frac{1}{q^{(t_0-t)(n-t_0-1)}},\ P_S = \frac{1}{q^{(n-t_0-1)}},\ P_T = \frac{1}{q^{(n-t_0-1)}},\ P_{R_0} = \frac{1}{q^{t_0-t}},\ P_{R_1} = \frac{1}{q}.$$

References

[1] SIMMONS G J. *A Cartesian product construction for unconditionally secure authentication codes that permit arbitration* [J]. J. Cryptology, 1990, **2**(2): 77–104.
[2] WAN Zhexian. *Construction of Cartesian authentication codes from unitary geometry* [J]. Des. Codes Cryptogr., 1992, **2**(4): 333–356.
[3] WAN Zhexian. *Further constructions of Cartesian authentication codes from symplectic geometry* [J]. Northeast. Math. J., 1992, **8**(1): 4–20.
[4] YOU Hong, NAN Jizhu. *Using normal form of matrices over finite fields to construct cartesian authentication codes* [J]. J. Math. Res. Expisition, 1998, **18**(3): 341–346.
[5] GAO You, XU Wenyan, JING Jingjing. *A construction of authentication codes with arbitration from vector space over finite fields* [J]. J. Civil Aviation University of China, 2005, **23**(6): 56–63.
[6] WAN Zhexian. *Geometry of Classical Groups over Finite Fields* [M]. Studentlitteratur, Lund; Chartwell-Bratt Ltd., Bromley, 1993.
[7] ABBA B, YOU Hong. *Using pseudo-symplectic spaces to construct Cartesian authentication codes with arbitration* [J]. J. Helongjiang Univ. Natur. Sci., 2006, **23**(5): 681–689.