Two Constructions of Multireceiver Authentication Codes from Symplectic Geometry over Finite Fields

Chen Shangdi Zhao Dawei

College of Science, Civil Aviation University of China, Tianjin, 300300, P.R.China.

Abstract. Multireceiver authentication codes allow one sender to construct an authenticated message for a group of receivers such that each receiver can verify authenticity of the received message. In this paper, we constructed two multireceiver authentication codes from symplectic geometry over finite fields. The parameters and the probabilities of deceptions of the codes are also computed.

§1 Introduction

Multireceiver authentication codes (MRA-codes) are introduced by Desmedt, Frankel, and Yung (DFY) [1] as an extension of Simmons' model of unconditionally secure authentication. In an MRA-codes, a sender wants to authenticate a message for a group of receivers such that each receiver can verify authenticity of the received message. There are three phases in an MRA-codes:

1. *Key distribution.* The KDC (key distribution centre) privately transmits the key information to the sender and each receiver (the sender can also be the KDC).

2. *Broadcast.* For a source state, the sender generates the authenticated message using his/her key and broadcasts the authenticated message.

3. *Verification.* Each user can verify the authenticity of the broadcast message.

Denote by $X_1 \times \cdots \times X_n$ the direct product of sets $X_1, \cdots, X_n$, and by p_i the projection mapping of $X_1 \times \cdots \times X_n$ on X_i. That is, $p_i : X_1 \times \cdots \times X_n \rightarrow X_i$ defined by $p_i(x_1, x_2, \cdots, x_n) = x_i$. Let $g_1 : X_1 \rightarrow Y_1$ and $g_2 : X_2 \rightarrow Y_2$ be two mappings, we denote the direct product of g_1 and g_2 by $g_1 \times g_2$, where $g_1 \times g_2 : X_1 \times X_2 \rightarrow Y_1 \times Y_2$

Keywords: symplectic geometry, multireceiver authentication codes, finite fields.

Supported by the NNSF of China(60776810), the NSF of Tianjin(08JCYBJC13900).

Address: College of Science, Civil Aviation University of China, Tianjin 300300, P.R.China.

E-mail address: zhaodawei0411@163.com

is defined by $(g_1 \times g_2)(x_1, x_2) = (g_1(x_1), g_2(x_2))$. The identity mapping on a set X is denoted by 1_X.

Let $C = (S, M, E, f)$ and $C_i = (S, M_i, E_i, f_i), i = 1, 2, ..., n$, be authentication codes. We call $(C; C_1, C_2, \cdots, C_n)$ a multireceiver authentication code (MRA-code) if there exist two mappings $\tau : E \to E_1 \times \cdots \times E_n$ and $\pi : M \to M_1 \times \cdots \times Mn$ such that for any $(s, e) \in S \times E$ and any $1 \leq i \leq n$, the following identity holds

$$p_i(\pi f(s, e)) = f_i((1_S \times p_i \tau(s, e)).$$

Let $\tau_i = p_i \tau$ and $\pi_i = p_i \pi$. Then we have for each $(s, e) \in S \times E$

$$\pi_i f(s, e) = f_i(1_S \times \tau_i)(s, e).$$

We adopt Kerckhoff's principle that everything in the system except the actual keys of the sender and receivers is public. This includes the probability distribution of the source states and the sender's keys.

Attackers could be *outsiders* who do not have access to any key information, or *insiders* who have some key information. We only need to consider the latter group as it is at least as powerful as the former. We consider the systems that protect against the coalition of groups of up to a maximum size of receivers, and we study impersonation and substitution attacks.

Assume there are n receivers $R_1, \cdots, R_n$. Let $L = \{i_1, \cdots, i_l\} \subseteq \{1, \cdots, n\}, R_L = \{R_{i_1}, \cdots, R_{i_l}\}$ and $E_L = E_{R_{i_1}} \times \cdots \times E_{R_{i_l}}$. We consider the attack from R_L on a receiver R_i, where $i \notin L$.

Impersonation attack: R_L, after receiving their secret keys, send a message m to R_i. R_L is successful if m is accepted by R_i as authentic. We denote by $P_I[i, L]$ the success probability of R_L in performing an impersonation attack on R_i. This can be expressed as

$$P_I[i, L] = \max_{e_L \in E_L} \max_{m \in M} P(m \text{ is accepted by } R_i | e_L)$$

where $i \notin L$.

Substitution attack: R_L, after observing a message m that is transmitted by the sender, replace m with another message m'. R_L is successful if m' is accepted by R_i as authentic. We denote by $P_S[i, L]$ the success probability of R_L in performing a substitution attack on R_i. We have

$$P_S[i, L] = \max_{e_L \in E_L} \max_{m \in M} \max_{m' \neq m \in M} P(R_i \text{ accepts } m' | m, e_L)$$

where $i \notin L$.

§2 Symplectic Geometry

Let $\mathbb{F}_q$ be a finite field with q elements, $n = 2\nu$ and define the $2\nu \times 2\nu$ alternate matrix

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

The symplectic group of degree 2ν over $\mathbb{F}_q$, denote by $Sp_{2\nu}(\mathbb{F}_q)$, is defined to be the set of matrices

$$Sp_{2\nu}(\mathbb{F}_q) = \{T|TK^tT = K\}$$

with matrix multiplication as its group operation. Let $\mathbb{F}_q^{(2\nu)}$ be the 2ν-dimensional row vector space over $\mathbb{F}_q$. $Sp_{2\nu}(\mathbb{F}_q)$ has an action on $\mathbb{F}_q^{(2\nu)}$ defined as follows

$$\mathbb{F}_q^{(2\nu)} \times Sp_{2\nu}(\mathbb{F}_q) \to \mathbb{F}_q^{(2\nu)}$$

$$((x_1, x_2, \ldots, x_{2\nu}), T) \to (x_1, x_2, \ldots, x_{2\nu})T.$$

The vector space $\mathbb{F}_q^{(2\nu)}$ together with this action of $Sp_{2\nu}(\mathbb{F}_q)$ is called the symplectic space over $\mathbb{F}_q$.

Let P be an m−dimensional subspace of $\mathbb{F}_q^{(2\nu)}$. We use the same latter P to denote a matrix representation of P, i.e., P is an $m \times 2\nu$ matrix of rank m such that its rows form a basis of P. The PK^tP is alternate. Assume that it is of rank $2s$, then P is called a subspace of type (m, s). It is known that (see [2]) subspaces of type (m, s) exist in $\mathbb{F}_q^{(2\nu)}$ if and only if

$$2s \leq m \leq \nu - s.$$

It is also known that subspaces of the same type form an orbit under $Sp_{2\nu}(\mathbb{F}_q)$. Denote by $N(m, s; 2\nu)$ the number of subspaces of type (m, s) in $\mathbb{F}_q^{(2\nu)}$.

Denote by $P^\perp$ the set of vectors which are orthogonal to every vector of P, i.e.,

$$P^\perp = \{y \in \mathbb{F}_q^{(2\nu)}|yK^tx = 0 \text{ for all } x \in P\}.$$

Obviously, $P^\perp$ is a $(2\nu - m)$-dimensional subspace of $\mathbb{F}_q^{(2\nu)}$.

More properties of symplectic geometry over finite fields can be found in [2].

In [3], Desmedt, Frankel and Yung gave two constructions for MRA-codes based on polynomials and finite geometries, respectively. There are other constructions of multireceiver authentication codes are given in [4], [5]. The construction of authentication codes is combinational design in its nature. We know that the geometry of classical groups over finite fields, including symplectic geometry, pseudo-symplectic geometry, unitary geometry and orthogonal geometry can provide a better composite structure and easy to count. In this paper we constructed two multireceiver authentication codes from symplectic geometry over finite fields. The parameters and the probabilities of deceptions of the codes are also computed.

§3 Construction

Construction I

Let $\mathbb{F}_q$ be a finite field with q elements and $e_i (1 \leq i \leq 2\nu)$ be the row vector in $\mathbb{F}_q^{(2\nu)}$ whose i−th coordinate is 1 and all other coordinates are 0. Assume that $1 < n < r < \nu$. $U = \langle e_1, e_2, \cdots, e_n \rangle$, i.e., U is an n−dimensional subspace of $\mathbb{F}_q^{(2\nu)}$ generated by $e_1, e_2, \cdots, e_n$, then $U^\perp = \langle e_1, \cdots, e_\nu, e_{\nu+n+1}, \cdots, e_{2\nu} \rangle$. The set of source states $S=\{s|s$ is a subspace of type $(2r-n, r-n)$ and $U \subset s \subset U^{\perp}\}$; the set of transmitter's encoding rules $E_T=\{e_T|e_T$ is a subspace of type $(2n, n)$, $U \subset e_T\}$; the set of ith receiver's decoding rules $E_{R_i}=\{e_{R_i}|e_{R_i}$ is a subspace of type $(n+1, 1)$ which is orthogonal to $\langle e_1, \cdots, e_{i-1}, e_{i+1}, \cdots, e_n\rangle$, $U \subset e_{R_i}\}$, $1 \le i \le n$; the set of messages $M=\{m|m$ is a subspace of type $(2r, r)$, $U \subset m\}$.

1. *Key Distribution*. The KDC randomly chooses a subspace $e_T \in E_T$, then privately sends e_T to the sender T. Then KDC randomly chooses a subspace $e_{R_i} \in E_{R_i}$ and $e_{R_i} \subset e_T$, then privately sends e_{R_i} to the ith receiver, where $1 \le i \le n$.

2. *Broadcast*. For a source state $s \in S$, the sender calculates $m = s + e_T$ and broadcast m.

3. *Verification*. Since the receiver R_i holds the decoding rule e_{R_i}, R_i accepts m as authentic if $e_{R_i} \subset m$. R_i can get s from $s = m \cap U^{\perp}$.

Lemma 3.1 The above construction of multireceiver authentication codes is reasonable, that is

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

(2) for any $m \in M$, $s = m \cap U^{\perp}$ is the uniquely source state contained in m and there is $e_T \in E_T$, such that $m = s + e_T$.

Proof: (1) For $s \in S$, $e_T \in E_T$, from the definition of s and e_T, we can assume that

$$s = \begin{pmatrix} U \\ Q \end{pmatrix} \begin{matrix} n \\ 2(r-n) \end{matrix} \quad \text{and} \quad \begin{pmatrix} U \\ Q \end{pmatrix} K \, {}^t\!\begin{pmatrix} U \\ Q \end{pmatrix} = \begin{pmatrix} 0^{(n)} & 0 & 0 \\ 0 & 0 & I^{(r-n)} \\ 0 & -I^{(r-n)} & 0 \end{pmatrix},$$

$$e_T = \begin{pmatrix} U \\ V \end{pmatrix} \begin{matrix} n \\ n \end{matrix} \quad \text{and} \quad \begin{pmatrix} U \\ V \end{pmatrix} K \, {}^t\!\begin{pmatrix} U \\ V \end{pmatrix} = \begin{pmatrix} 0 & I^{(n)} \\ -I^{(n)} & 0 \end{pmatrix}.$$

Obviously, for any $v \in V$ and $v \neq 0$, $v \notin s$, therefore,

$$m = s + e_T = \begin{pmatrix} U \\ V \\ Q \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} U \\ V \\ Q \end{pmatrix} K \, {}^t\!\begin{pmatrix} U \\ V \\ Q \end{pmatrix} = \begin{pmatrix} 0 & I^{(n)} & 0 & 0 \\ -I^{(n)} & 0 & * & * \\ 0 & * & 0 & I^{(r-n)} \\ 0 & * & -I^{(r-n)} & 0 \end{pmatrix}.$$

From above, m is a subspace of type $(2r, r)$ and $U \subset m$, i.e., $m \in M$.

(2) For $m \in M$, m is a subspace of type $(2r, r)$ containing U. So there is subspace $V \subset m$, satisfying

$$\begin{pmatrix} U \\ V \end{pmatrix} K \, {}^t\!\begin{pmatrix} U \\ V \end{pmatrix} = \begin{pmatrix} 0 & I^{(n)} \\ -I^{(n)} & 0 \end{pmatrix}.$$

Then we can assume that $m = \begin{pmatrix} U \\ V \\ Q \end{pmatrix}$, satisfying

$$\begin{pmatrix} U \\ V \\ Q \end{pmatrix} K \, {}^t\!\begin{pmatrix} U \\ V \\ Q \end{pmatrix} = \begin{pmatrix} 0 & I^{(n)} & 0 & 0 \\ -I^{(n)} & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(r-n)} \\ 0 & 0 & -I^{(r-n)} & 0 \end{pmatrix}.$$

Let $s = \begin{pmatrix} U \\ Q \end{pmatrix}$, then s is a subspace of type $(2r-n, r-n)$ and $U \subset s \subset U^{\perp}$, i.e., $s \in S$ is a source state. For any $v \in V$ and $v \neq 0$, $v \notin s$ is obvious, i.e., $V \cap U^{\perp} = \{0\}$. Therefore, $m \cap U^{\perp} = \begin{pmatrix} U \\ Q \end{pmatrix} = s$. Let $e_T = \begin{pmatrix} U \\ V \end{pmatrix}$, then e_T is a transmitter's encoding rule and satisfying $m = s + e_T$.

If s' is another source state contained in m, then $U \subset s' \subset U^{\perp}$. Therefore, $s' \subset m \cap U^{\perp} = s$, while dim$s'$=dim$s$, so s'=s, i.e., s is the uniquely source state contained in m.

From Lemma 3.1, we know that such construction of multireceiver authentication codes is reasonable and there are n receivers in this system. Next we compute the parameters of this codes.

Lemma 3.2 The number of the source states is $|S| = N(2(r-n), r-n; 2(\nu-n))$.

Proof: Since $U \subset s \subset U^{\perp}$, s has the form as follows

$$s = \begin{array}{c} \begin{pmatrix} I^{(n)} & 0 & 0 & 0 \\ 0 & Q_2 & 0 & Q_4 \end{pmatrix} \begin{array}{l} n \\ 2(r-n) \end{array} \\ \begin{array}{cccc} n & \nu-n & n & \nu-n \end{array} \end{array},$$

where (Q_2, Q_4) is a subspace of type $(2(r-n), r-n)$ in the symplectic space $F_q^{2(\nu-n)}$. Therefore, the number of the source states is $|S| = N(2(r-n), r-n; 2(\nu-n))$.

Lemma 3.3 The number of the encoding rules of transmitter is $|E_T| = q^{2n(\nu-n)}$.

Proof: Since e_T is a subspace of type $(2n, n)$ containing U, e_T has the form as follows

$$e_T = \begin{array}{c} \begin{pmatrix} I^{(n)} & 0 & 0 & 0 \\ 0 & R_2 & I^{(n)} & R_4 \end{pmatrix} \begin{array}{l} n \\ n \end{array} \\ \begin{array}{cccc} n & \nu-n & n & \nu-n \end{array} \end{array},$$

where R_2, R_4 arbitrarily. Therefore, $|E_T| = q^{2n(\nu-n)}$.

Lemma 3.4 The number of the decoding rules of ith receiver is $|E_{R_i}| = q^{2(\nu-n)}$.

Proof: Since the ith receiver's decoding rules e_{R_i} is a subspace of type $(n+1, 1)$ containing U and e_{R_i} is orthogonal to $\langle e_1, \cdots, e_{i-1}, e_{i+1}, \cdots, e_n \rangle$. So we can assume that $e_{R_i} = {}^t(e_1, \cdots, e_n, u)$, where $u = (x_1 \ x_2 \ \cdots \ x_{2\nu})$. Obviously, $x_1 = \cdots = x_n = x_{\nu+1} = \cdots = x_{\nu+i-1} = x_{\nu+i+1} = \cdots = x_{\nu+n} = 0$, $x_{\nu+i} = 1$, and $x_{n+1}, \cdots, x_\nu, x_{\nu+n+1}, \cdots, x_{2\nu}$ arbitrarily. Therefore, $|E_{R_i}| = q^{2(\nu-n)}$.

Lemma 3.5 (1)The number of encoding rules e_T contained in m is $q^{2n(r-n)}$;

(2)The number of the messages is $|M| = q^{2n(v-r)}N(2(r-n), r-n; 2(v-n))$.

Proof: (1) Let m be a message. From the definition of m, we may take m as follows

$$m = \begin{array}{c} \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-n)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(n)} & 0 & 0 \\ 0 & 0 & 0 & 0 & I^{(r-n)} & 0 \end{pmatrix} \\ \begin{matrix} n & r-n & v-r & n & r-n & v-r \end{matrix} \end{array}.$$

If $e_T \subset m$, then we can assume that

$$e_T = \begin{array}{cc} \begin{pmatrix} I^{(n)} & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & 0 & I^{(n)} & R_5 & 0 \end{pmatrix} & \begin{matrix} n \\ n \end{matrix} \\ \begin{matrix} n & r-n & v-r & n & r-n & v-r \end{matrix} & \end{array},$$

where R_2, R_5 arbitrarily. Therefore, the number of e_T contained in m is $q^{2n(r-n)}$.

(2) We know that a message contains only one source state and the number of the transmitter's encoding rules contained in a message is $q^{2n(r-n)}$. Therefore we have $|M| = |S||E_T|/q^{2n(r-n)} = q^{2n(v-r)}N(2(r-n), r-n; 2(v-n))$.

Theorem 3.1 The parameters of constructed multireceiver authentication codes are

$$\begin{gathered} |\ S\ | = N(2(r-n), r-n; 2(v-n)); \\ |E_T| = q^{2n(v-n)}; \\ |E_{R_i}| = q^{2(v-n)}; \\ |M| = q^{2n(v-r)}N(2(r-n), r-n; 2(v-n)). \end{gathered}$$

Assume there are n receivers $R_1, \cdots, R_n$. Let $L = \{i_1, \cdots, i_l\} \subseteq \{1, \cdots, n\}, R_L = \{R_{i_1}, \cdots, R_{i_l}\}$ and $E_L = E_{R_{i_1}} \times \cdots \times E_{R_{i_l}}$. We consider the *impersonation attack* and *substitution attack* from R_L on a receiver R_i, where $i \notin L$.

Without loss of generality, we can assume that $R_L = \{R_1, \cdots, R_l\}$, $E_L = E_{R_1} \times \cdots \times E_{R_l}$, where $1 \leq l \leq n-1$. First, we will proof the following results:

Lemma 3.6 For any $e_L = (e_{R_1}, \cdots, e_{R_l}) \in E_L$, the number of e_T containing e_L is $q^{2(n-l)(v-n)}$.

Proof: For any $e_L = (e_{R_1}, \cdots, e_{R_l}) \in E_L$, we can assume that

$$e_L = \begin{array}{c} \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & I^{(l)} & 0 & R_6 \end{pmatrix} \\ \begin{matrix} l & n-l & v-n & l & n-l & v-n \end{matrix} \end{array}.$$

Therefore, e_T containing e_L has the form as follows

$$e_T = \begin{array}{c} \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & I^{(l)} & 0 & R_6 \\ 0 & 0 & R_3' & 0 & I^{(n-l)} & R_6' \end{pmatrix} \\ \begin{matrix} l & n-l & v-n & l & n-l & v-n \end{matrix} \end{array},$$

where R_3', R_6' arbitrarily. Therefore, the number of e_T containing e_L is $q^{2(n-l)(v-n)}$.

Lemma 3.7 For any $m \in M$ and $e_L, e_{R_l} \subset m$,

(1) the number of e_T contained in m and containing e_L is $q^{2(n-l)(r-n)}$;

(2) the number of e_T contained in m and containing e_L, e_{R_l} is $q^{2(n-l-1)(r-n)}$.

Proof: (1) The matrix of m is like lemma 3.5, then for any $e_L \subset m$, assume that

$$e_L = \begin{array}{c} \left(\begin{array}{cccccccc} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & I^{(l)} & 0 & R_7 & 0 \end{array}\right) \\ \begin{array}{cccccccc} l & n-l & r-n & v-r & l & n-l & r-n & v-r \end{array} \end{array}.$$

If $e_T \subset m$ and $e_T \supset e_L$, then

$$e_T = \left(\begin{array}{cccccccc} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & I^{(l)} & 0 & R_7 & 0 \\ 0 & 0 & R_3' & 0 & 0 & I^{(n-l)} & R_7' & 0 \end{array}\right),$$

where R_3', R_7' arbitrarily. Therefore, the number of e_T contained in m and containing e_L is $q^{2(n-l)(r-n)}$.

(2) Similarly, we can proof that the number of e_T contained in m and containing e_L, e_{R_l} is $q^{2(n-l-1)(r-n)}$.

Lemma 3.8 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 $s_0 = s_1 \cap s_2$, $\dim s_0 = k$, then $n \leq k \leq 2r - n - 1$. For any $e_L, e_{R_l} \subset m_1 \cap m_2$, the number of e_T contained in $m_1 \cap m_2$ and containing e_L, e_{R_l} is $q^{(n-l-1)(k-n)}$.

Proof: Since $m_1 = s_1 + e_T, m_2 = s_2 + e_T$ and $m_1 \neq m_2$, then $s_1 \neq s_2$. And for any $s \in S, s \supset U$, therefore, $n \leq k \leq 2r - n - 1$. Assume that s_i' is the complementary subspace of s_0 in the s_i, then $s_i = s_0 + s_i'$ $(i = 1, 2)$. From $m_i = s_i + e_T = s_0 + s_i' + e_T$ and $s_i = m_i \cap U^{\perp}$, we have $s_0 = (m_1 \cap U^{\perp}) \bigcap (m_2 \cap U^{\perp}) = m_1 \cap m_2 \cap U^{\perp} = s_1 \cap m_2 = s_2 \cap m_1$ and $m_1 \cap m_2 = (s_1 + e_T) \cap m_2 = (s_0 + s_1' + e_T) \cap m_2 = ((s_0 + e_T) + s_1') \cap m_2$. Because $s_0 + e_T \subset m_2$, $m_1 \cap m_2 = (s_0 + e_T) + (s_1' \cap m_2)$. While $s_1' \cap m_2 \subseteq s_1 \cap m_2 = s_0$, $m_1 \cap m_2 = s_0 + e_T$.

From the definition of the message, we may take $m_i (i = 1, 2)$ as follows

$$m_i = \begin{array}{c} \left(\begin{array}{cccc} I^{(n)} & 0 & 0 & 0 \\ 0 & P_{i2} & 0 & 0 \\ 0 & 0 & I^{(n)} & 0 \\ 0 & 0 & 0 & P_{i4} \end{array}\right) \begin{array}{c} n \\ r-n \\ n \\ r-n \end{array} \\ \begin{array}{cccc} n & v-n & n & v-n \end{array} \end{array}.$$

Let

$$m_1 \cap m_2 = \begin{array}{cc} \begin{pmatrix} I^{(n)} & 0 & 0 & 0 \\ 0 & P_2 & 0 & 0 \\ 0 & 0 & I^{(n)} & 0 \\ 0 & 0 & 0 & P_4 \end{pmatrix} & \begin{array}{c} n \\ r-n \\ n \\ r-n \end{array} \\ \begin{array}{cccc} n & v-n & n & v-n \end{array} & \end{array},$$

from above we know that $m_1 \cap m_2 = s_0 + e_T$, then $\dim(m_1 \cap m_2) = k+n$, therefore,

$$\dim \begin{pmatrix} 0 & P_2 & 0 & 0 \\ 0 & 0 & 0 & P_4 \end{pmatrix} = k-n.$$

For any $e_L, e_{R_i} \subset m_1 \cap m_2$, we can assume that

$$e_L = \begin{array}{c} \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & I^{(l)} & 0 & R_6 \end{pmatrix} \\ \begin{array}{cccccc} l & n-l & v-n & l & n-l & v-n \end{array} \end{array},$$

$$e_{R_i} = \begin{array}{cc} \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3' & 0 & 1 & 0 & R_6' \end{pmatrix} & \begin{array}{c} l \\ n-l \\ 1 \end{array} \\ \begin{array}{ccccccc} l & n-l & v-n & i-1 & 1 & n-i & v-n \end{array} & \end{array}.$$

If $e_T \subset m_1 \cap m_2$ and $e_L, e_{R_i} \subset e_T$, then e_T has the form as follows

$$e_T = \begin{array}{cc} \begin{pmatrix} I^{(l)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(n-l)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & I^{(l)} & 0 & 0 & 0 & R_6 \\ 0 & 0 & C_3 & 0 & I^{(i-l-1)} & 0 & 0 & C_6 \\ 0 & 0 & R_3' & 0 & 0 & 1 & 0 & R_6' \\ 0 & 0 & C_3' & 0 & 0 & 0 & I^{(n-i)} & C_6' \end{pmatrix} & \begin{array}{c} l \\ n-l \\ l \\ i-l-1 \\ 1 \\ n-i \end{array} \\ \begin{array}{cccccccc} l & n-l & v-n & l & i-l-1 & 1 & n-i & v-n \end{array} & \end{array}.$$

So it is easy to know that the number of e_T contained in $m_1 \cap m_2$ and containing e_L, e_{R_i} is $q^{(n-l-1)(k-n)}$.

Theorem 3.2 In the constructed multireceiver authentication codes, the largest probabilities of success for *impersonation attack* and *substitution attack* from R_L on a receiver R_i are

$$P_I[i,L] = \frac{1}{q^{2(n-l)(v-r)+2(r-n)}}, \qquad P_S[i,L] = \frac{1}{q^{2r-n-l-1}}$$

respectively, where $i \notin L$.

Proof: *Impersonation attack*: R_L, after receiving their secret keys, send a message m to R_i. R_L is successful if m is accepted by R_i as authentic. Therefore

$$P_I[i,L] = \max_{e_L \in E_L} \left\{ \frac{\max_{m \in M} |\{e_T \in E_T | e_T \subset m \text{ and } e_T \supset e_L, e_{R_i}\}|}{|\{e_T \in E_T | e_T \supset e_L\}|} \right\}$$

$$= \frac{q^{2(n-l-1)(r-n)}}{q^{2(n-l)(v-n)}}$$

$$= \frac{1}{q^{2(n-l)(v-r)+2(r-n)}}.$$

Substitution attack: R_L, after observing a message m that is transmitted by the sender, replace m with another message m'. R_L is successful if m' is accepted by R_i as authentic. Therefore

$$P_S[i,L] = \max_{e_L \in E_L} \max_{m \in M} \left\{ \frac{\max\limits_{m' \in M} |\{e_T \in E_T | e_T \subset m, m' \text{ and } e_T \supset e_L, e_{R_i}\}|}{|\{e_T \in E_T | e_T \subset m \text{ and } e_T \supset e_L\}|} \right\}$$

$$= \max_{n \le k \le 2r-n-1} \frac{q^{(n-l-1)(k-n)}}{q^{2(n-l)(r-n)}}$$

$$= \frac{1}{q^{2r-n-l-1}}.$$

Construction II

Assume that $1 < n < v$, $U = \langle e_1, e_2, \cdots, e_n \rangle$, i.e., U is an n–dimensional subspace of $\mathbb{F}_q^{(2v)}$ generated by $e_1, e_2, \cdots, e_n$, then $U^\perp = \langle e_1, \cdots, e_v, e_{v+n+1}, \cdots, e_{2v} \rangle$. The set of source states $S = \{s | s$ is a subspace of type $(2(v-n), v-n)$ and $s \subset U^\perp\}$; the set of transmitter's encoding rules $E_T = \{e_T | e_T$ is an n–dimensional subspace and $U + e_T$ is a subspace of type $(2n, n)\}$; the set of ith receiver's decoding rules $E_{R_i} = \{e_{R_i} | e_{R_i}$ is an 1–dimensional subspace and $U + e_{R_i}$ is a subspace of type $(n+1, 1)$ which is orthogonal to $\langle e_1, \cdots, e_{i-1}, e_{i+1}, \cdots, e_n \rangle\}$, $1 \le i \le n$; the set of messages $M = \{m | m$ is an $(2v-n)$–dimensional subspace and $m^\perp \in E_T\}$.

1. *Key Distribution.* The KDC randomly chooses a subspace $e_T \in E_T$, then privately sends e_T to the sender T. Then KDC randomly chooses a subspace $e_{R_i} \in E_{R_i}$ and $e_{R_i} \subset e_T$, then privately sends e_{R_i} to the ith receiver, where $1 \le i \le n$.

2. *Broadcast.* For a source state $s \in S$, the sender calculates $m = s + e_T$ and broadcast m.

3. *Verification.* Since the receiver R_i holds the decoding rule e_{R_i}, R_i accepts m as authentic if $e_{R_i} \subset m$.

Lemma 3.9 The construction II is reasonable.

Proof: For $s \in S$, $e_T \in E_T$, from the definition of s and e_T, we can assume that

$$s = \begin{array}{c} \begin{pmatrix} A & I^{(v-n)} & 0 & 0 \\ B & 0 & 0 & I^{(v-n)} \end{pmatrix}, \\ \begin{array}{cccc} n & v-n & n & v-n \end{array} \end{array}$$

$$e_T = \begin{array}{c} \begin{pmatrix} X_1 & X_2 & I^{(n)} & X_4 \end{pmatrix}. \\ \begin{array}{cccc} n & v-n & n & v-n \end{array} \end{array}$$

Then

$$m = s + e_T = \begin{pmatrix} A & I^{(v-n)} & 0 & 0 \\ B & 0 & 0 & I^{(v-n)} \\ Y & 0 & I^{(n)} & 0 \end{pmatrix},$$

where $Y = X_1 - X_2A - X_4B$. Therefore, m is an $(2\nu - n)$–dimensional subspace and $m^\perp = ({}^tY \quad {}^tB \quad I^{(n)} \quad -{}^tA) \in E_T$, i.e., $m \in M$.

For $m \in M, m^\perp \in E_T$, then $(m \cap U^\perp)^\perp = m^\perp + U$ is a subspace of type $(2n, n)$. Therefore, $m \cap U^\perp$ is a subspace of type $(2(\nu - n), \nu - n)$. Let $s = m \cap U^\perp$, then $s \in S$. We can assume that

$$m = \begin{pmatrix} A & I^{(\nu-n)} & 0 & 0 \\ B & 0 & 0 & I^{(\nu-n)} \\ Y & 0 & I^{(n)} & 0 \end{pmatrix}, \quad s = m \cap U^\perp = \begin{pmatrix} A & I^{(\nu-n)} & 0 & 0 \\ B & 0 & 0 & I^{(\nu-n)} \end{pmatrix}.$$

Let $e_T = \begin{pmatrix} Y & 0 & I^{(n)} & 0 \end{pmatrix}$, then e_T is an n–dimensional subspace and $U + e_T$ is a subspace of type $(2n, n)$. Therefore, e_T is an encoding rule of transmitter and satisfying $s + e_T = m$.

If s' is another source state contained in m, similar to the proof of the lemma 3.1, we have s'=s, i.e., s is the uniquely source state contained in m.

Theorem 3.3 The parameters of this construction are

$$|S| = q^{2n(\nu-n)}; \quad |E_T| = q^{n(2\nu-n)}; \quad |E_{R_i}| = q^{2\nu-n}; \quad |M| = q^{n(2\nu-n)}.$$

Proof: From the proof of the lemma 3.9, for any $s \in S, e_T \in E_T$, s, e_T have the form as follows

$$s = \begin{pmatrix} A & I^{(\nu-n)} & 0 & 0 \\ B & 0 & 0 & I^{(\nu-n)} \end{pmatrix}, \quad e_T = \begin{pmatrix} X_1 & X_2 & I^{(n)} & X_4 \end{pmatrix}$$

respectively. Therefore, $|S| = q^{2n(\nu-n)}$, $|E_T| = q^{n(2\nu-n)}$. Since $m \in M$ if and only if $m^\perp \in E_T$, we have $|M| = |E_T| = q^{n(2\nu-n)}$.

For any $e_{R_i} \in E_{R_i}$,

$$e_{R_i} = \begin{array}{c} \begin{pmatrix} R_1 & R_2 & 0 & 1 & 0 & R_4 \end{pmatrix} \\ \begin{array}{cccccc} n & \nu-n & i-1 & 1 & n-i & \nu-n \end{array} \end{array}.$$

Therefore, $|E_{R_i}| = q^{2\nu-n}$.

Similar to the lemma 3.6-3.8, we have the following three lemmas.

Lemma 3.10 For any $e_L = (e_{R_1}, \cdots, e_{R_l}) \in E_L$, the number of e_T containing e_L is $q^{(n-l)(2\nu-n)}$.

Lemma 3.11 For any $m \in M$ and $e_L, e_{R_i} \subset m$,

(1) the number of e_T contained in m and containing e_L is $q^{2(n-l)(\nu-n)}$;

(2) the number of e_T contained in m and containing e_L, e_{R_i} is $q^{2(n-l-1)(\nu-n)}$.

Lemma 3.12 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 $s_0 = k$, then $0 \le k \le 2(\nu - n) - 1$. For any $e_L, e_{R_i} \subset m_1 \cap m_2$, the number of e_T contained in $m_1 \cap m_2$ and containing e_L, e_{R_i} is $q^{k(n-l-1)}$.

Theorem 3.4 In the construction II, the largest probabilities of success for *impersonation attack* and *substitution attack* from R_L on a receiver R_i are

$$P_I[i, L] = \frac{1}{q^{n(n-l)+2(v-n)}}, \qquad P_S[i, L] = \frac{1}{q^{2v-n-l-1}}$$

respectively, where $i \notin L$.

Proof: *Impersonation attack*:

$$\begin{aligned} P_I[i, L] &= \max_{e_L \in E_L} \left\{ \frac{\max\limits_{m \in M} |\{e_T \in E_T | e_T \subset m \text{ and } e_T \supset e_L, e_{R_i}\}|}{|\{e_T \in E_T | e_T \supset e_L\}|} \right\} \\ &= \frac{q^{2(n-l-1)(v-n)}}{q^{(n-l)(2v-n)}} \\ &= \frac{1}{q^{n(n-l)+2(v-n)}}. \end{aligned}$$

Substitution attack:

$$\begin{aligned} P_S[i, L] &= \max_{e_L \in E_L} \max_{m \in M} \left\{ \frac{\max\limits_{m' \in M} |\{e_T \in E_T | e_T \subset m, m' \text{ and } e_T \supset e_L, e_{R_i}\}|}{|\{e_T \in E_T | e_T \subset m \text{ and } e_T \supset e_L\}|} \right\} \\ &= \max_{0 \le k \le 2(v-n)-1} \frac{q^{k(n-l-1)}}{q^{2(n-l)(v-n)}} \\ &= \frac{1}{q^{2v-n-l-1}}. \end{aligned}$$

References

[1] Safavi-Naini R, Wang H. Multi-receiver Authentication Codes: Models, Bounds, Constructions and Extensions[J]. Information and Computation, 1999, 151(1): 148- 172.

[2] WAN Zhexian. Geometry of Classical Groups over Finite Fields (Second Edition) [M]. Beijing/New York: Science Press, 2002.

[3] Y. Desmedt, Y. Frankel and M. Yung, Multer-receiver/Multi-sender network security: efficient authenticated multicast/feedback, *IEEE infocom'92*, (1992) 2045-2054.

[4] G.J.Simmons. Message authentication with arbitration of transmitter/receiver disputes. Proc. Eurcrypt 87. Lecture Notes in Computer Science, 1985 (304):151-165.

[5] Safavi-Naini R, Wang Huaxiong. Broadcast Authentication for Group Communication[J]. Theoretical Computer Science, 2001,269(1/2): 1-21.