Two New Authentication Schemes from Singular Symplectic Geometry over Finite Fields*

Shangdi Chen† Minjuan Song

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

Abstract: Two kind of authentication schemes are constructed using singular symplectic geometry over finite fields in this paper. One is an authentication code with arbitration, another is a multi-receiver authentication code. The parameters of two kinds of codes have been computed. Under the assumption that the encoding rules of the transmitter and the receiver are chosen according to a uniform probability distribution, the maximum probabilities of success of different types of deceptions attacks are also computed.
Key words: authentication; arbitration; multi-receiver; singular symplectic geometry

1 Introduction

Authentication codes were invented by Gilbertetal[1] in 1974. Simmons [2] has developed the theory of unconditional authentication analogous to Shannon's theory of unconditional secrecy. The authentication codes without arbitration haven't valid to prevent transmitter and receiver from attacking mutual. In order to prevent the mutual deceit of the transmitter and the receiver, Simmons[3] put forward the concept of authentication codes with arbitration again. In Simmons' model there is only one receiver. As an extension of Simmons' unconditionally secure authentication, multireceiver authentication codes were introduced by Desmedt, Frankel, and Yung [4]. This paper makes use of the singular symplectic geometry to get a type of authentication codes with arbitration, at the same time, to construct a multi-receiver authentication code on this foundation, and the probabilities of success for different types of deceptions are also computed.

*The Project-sponsored by the National Natural Science Foundation of China(61179026) .
†E-mail: 11csd@163.com

To solve the distrust problem of the transmitter and the receiver in the communications system, Simmons introduced a model of authentication codes with arbitration, we symply write (A^2-code) defined as follows:

Definition 1.1 *Let S, E_T, E_R and M be four non-empty finite sets, and $f : S \times E_T \longmapsto M$ and $g : M \times E_R \longmapsto S \cup \{reject\}$ 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 an $s \in S$, 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, $g(m, e_R) = \{reject\}$.

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

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 an authentication system that permits arbitration, there are four participants: a transmitter, a receiver, an opponent, and an arbiter, and there are five attacks:

1) The opponent's impersonation attack: the largest probability of an opponent's successful impersonation attack is P_I. Then

$$P_I = \max_{m \in M} \frac{|\{e_R \in E_R | e_R \subset m\}|}{|E_R|}.$$

2) The opponent's substitution attack:

An opponent, after observing a message m that is transmitted by the sender, replace m with another m'. The opponent is successful if m' is accepted by the receiver. We denote by P_S the maximal probability of the opponent in performing a substitution attack on the receiver. Then

$$P_S = \max_{m \in M} \frac{\max\limits_{m \neq m' \in M} |\{e_R \in E_R | e_R \subset m \text{ and } e_R \subset m'\}|}{|\{e_R \in E_R | e_R \subset m\}|}.$$

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

$$P_T = \max_{e_T \in E_T} \frac{\max\limits_{m \in M, e_T \notin m} |\{e_R \in E_R | e_R \subset m \text{ and } p(e_R, e_T) \neq 0\}|}{|\{e_R \in E_R | p(e_R, e_T) \neq 0\}|}.$$

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

$$P_{R_0} = \max_{e_R \in E_R} \frac{\max_{m \in M} | \{e_T \in E_T | e_T \subset m \text{ and } p(e_R, e_T) \neq 0\} |}{| \{e_T \in E_T | p(e_R, e_T) \neq 0\} |}.$$

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

$$P_{R_1} = \max_{e_R \in E_R, m \in M} \frac{\max_{m' \in M} | \{e_T \in E_T | e_T \subset m, m' \text{ and } p(e_R, e_T) \neq 0\} |}{| \{e_T \in E_T | p(e_R, e_T) \neq 0\} |}.$$

The following notations will be fixed throughout this paper: p is a fixed prime and $q = p^\alpha$ is a fixed power of p. F_q is a field with q elements. $V = F_q^{2v+l}$ is a singular symplectic space over F_q with index v. $e_i (1 \leq i \leq 2v + l)$ 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 $e_{2v+1}, e_{2v+2}, \cdots, e_{2v+l}$. K_l denotes the matrix

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

$N(m,n)$ denotes the number of m-dimensional subspaces of F_q^n, $N(k,m,n)$ denotes the number of k-dimensional subspaces contained in a given m-dimensional subspace of F_q^n, $N'(k,m,n)$ denotes the number of m-dimensional subspaces containing a given k-dimensional subspace of F_q^n, $N(m,s;2v)$ denotes the number of subspaces of (m,s) in $2v$-dimensional symplectic spaces over F_q, $N(m_1,s_1;m,s:2v)$ denotes the number of subspaces of type (m_1,s_1) contained in a given subspace of type (m,s) in $2v$-dimensional symplectic spaces over F_q, $N'(m_1,s_1;m,s:2v)$ denotes the number of subspaces of type (m,s) containing a given subspace of type (m_1,s_1) in $2v$-dimensional symplectic spaces over F_q, $N(m,s,k;2v+l,v)$ denotes the number of subspaces of type (m,s,k) in $(2v+l)$-dimensional singular symplectic spaces over F_q, $N(m_1,s_1,k_1;m,s,k;2v+l,v)$ denotes the number of subspaces of type (m_1,s_1,k_1) contained a given subspace of type (m,s,k) in $(2v+l)$-dimensional singular symplectic spaces over F_q, $N'(m_1,s_1,k_1;m,s,k;2v+l,v)$ denotes the number of subspaces of type (m,s,k) containing a given subspace of type (m_1,s_1,k_1) in $(2v+l)$-dimensional singular symplectic spaces over F_q.

The reader is referred to [18], geometry of classical groups over finite fields, for notations and terminology.

2 The first Construction

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

Let $n = 2v+l$, $4 < r < t < v+1$, $v \geq 6$, $1 \leq k < l$, let U be a fixed subspace of type $(r+1,1,1)$ in V and let $U_0 = U \cap U^{\perp}$. Then $U^{\perp}$ and U_0 are subspaces of types $(2v-r+l, v+1-r, l)$ and $(r-1,0,1)$ in V, respectively.

Our authentication code is a six-tuple

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

where the set of source states

$$S = \{s | s \text{ is a subspace of type } (2t-r-2+k, t-r, k) \text{ in } V, U_0 \subset s \subset U^{\perp}\};$$

the set of transmitter's encoding rules

$$E_T = \{e_T | e_T \text{ is a subspace of type } (2r-1, r-1, 1) \text{ in V and } U \subset e_T\};$$

the set of receiver's decoding rules

$$E_R = \{e_R | e_R \text{ is a subspace of type } (2r-3, r-3, 1) \text{ in V and } U \subset e_R\};$$

the set of messages

$$\begin{aligned} M \quad = \quad & \{m | m \text{ is a subspace of type } (2(t-1)+k, t-1, k), U \subset m, \\ & m \cap U^{\perp} \text{ is a subspace of type } (2t-r-2+k, t-r, k) \text{ in V}\}; \end{aligned}$$

the encoding function:

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

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

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

Assuming the transmitter's encoding rules and the receiver's decoding rules are chosen according to a uniform probability distribution, we can suppose that

$$U = \begin{array}{c} \left(\begin{array}{cccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array} \right) \begin{array}{c} 1 \\ 1 \\ r-2 \\ 1 \end{array} \\ \begin{array}{cccccccc} 1 & r-2 & v+1-r & 1 & r-2 & v+1-r & 1 & l-1 \end{array} \end{array}.$$

Then

$$U^{\perp} = \begin{pmatrix} 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(v+1-r)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I^{(v+1-r)} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(l)} \end{pmatrix} \begin{matrix} r-2 \\ v+1-r \\ v+1-r \\ l \end{matrix}$$

$$\begin{matrix} 1 & r-2 & v+1-r & 1 & r-2 & v+1-r & l \end{matrix}$$

and

$$U_0 = \begin{pmatrix} 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} r-2 \\ l \end{matrix}$$

$$\begin{matrix} 1 & r-2 & v+1-r & 1 & r-2 & v+1-r & 1 & l-1 \end{matrix}$$

Lemma 2.1 *The six-tuple $(S, E_T, E_R, M; f, g)$ is a well-defined 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 $m \in M$, $s = m \cap U^{\perp}$ is uniquely information source contained in m and there is $e_T \in E_T$, such that $m = s + e_T$.

Proof. (1) For $s \in S$, we can suppose that

$$s = \begin{pmatrix} 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & 0 & R_6 & 0 & 0 & R_9 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \end{pmatrix} \begin{matrix} r-2 \\ 2(t-r) \\ 1 \\ k-1 \end{matrix},$$

$$\begin{matrix} 1 & r-2 & v+1-r & 1 & r-2 & v+1-r & 1 & k-1 & l-k \end{matrix}$$

where

$$sK_l\,{}^t s = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -R_6\,{}^t R_3 + R_3\,{}^t R_6 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{matrix} r-2 \\ 2(t-r) \\ k \end{matrix}.$$

$$\begin{matrix} r-2 & 2(t-r) & k \end{matrix}$$

Since $\operatorname{rank}(sK_l^t s) = 2(t-r)$, $\operatorname{rank}(-R_6\,{}^t R_3 + R_3\,{}^t R_6) = 2(t-r)$. For $e_T \in E_T$, we can suppose that

$$e_T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3' & 0 & R_5' & R_6' & 0 & R_8' \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} 1 \\ 1 \\ r-2 \\ r-2 \\ 1 \end{matrix},$$

$$\begin{matrix} 1 & r-2 & v+1-r & 1 & r-2 & v+1-r & 1 & l-1 \end{matrix}$$

where $\operatorname{rank}(R_3', R_5', R_6', R_8') = r-2$, and

$$e_T K_l {}^t e_T = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & R_5' & 0 \\ 0 & 0 & -R_5' & -R_6' {}^t R_3' + R_3' {}^t R_6' & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} 1 \\ 1 \\ r-2 \\ r-2 \\ 1 \end{matrix} .$$

Since e_T is a subspace of type $(2r-1, r-1, 1)$, $\operatorname{rank}(R_5') = r-2$. Let $R_5' = I^{(r-2)}$, we can assume that

$$e_T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3' & 0 & I^{(r-2)} & R_6' & 0 & R_8' \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} 1 \\ 1 \\ r-2 \\ r-2 \\ 1 \end{matrix}$$
$$\begin{matrix} 1 & r-2 & v+1-r & 1 & r-2 & v+1-r & 1 & l-1 \end{matrix} .$$

So

$$e_T K_l {}^t e_T = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(r-2)} & 0 \\ 0 & 0 & -I^{(r-2)} & -R_6' {}^t R_3' + R_3' {}^t R_6' & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} 1 \\ 1 \\ r-2 \\ r-2 \\ 1 \end{matrix}$$

$$\sim \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(r-2)} & 0 \\ 0 & 0 & -I^{(r-2)} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} 1 \\ 1 \\ r-2 \\ r-2 \\ 1 \end{matrix} ,$$

and

$$m = s + e_T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & 0 & R_6 & 0 & R_8 \\ 0 & 0 & R_3' & 0 & I^{(r-2)} & R_6' & 0 & R_8' \\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(k)} & 0 \end{pmatrix} \begin{matrix} 1 \\ r-2 \\ 1 \\ 2(t-r) \\ r-2 \\ k \end{matrix}$$
$$\begin{matrix} 1 & r-2 & v+1-r & 1 & r-2 & v+1-r & k & l-k \end{matrix} .$$

Clearly, m is a $2(t-1)+k$ dimensional subspace, and $\dim(m \cap E) = k$. As

$$m K_l {}^t m$$

$$= \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I^{(r-2)} & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -R_6\,{}^tR_3 + R_3\,{}^tR_6 & -R_6\,{}^tR_3' + R_3\,{}^tR_6' & 0 \\ 0 & -I^{(r-2)} & 0 & -R_6'\,{}^tR_3 + R_3'\,{}^tR_6 & -R_6'\,{}^tR_3' + R_3'\,{}^tR_6' & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} 1 \\ r-2 \\ 1 \\ 2(t-r) \\ r-2 \\ k \end{matrix}$$

$$\sim \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I^{(r-2)} & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -R_6\,{}^tR_3 + R_3\,{}^tR_6 & 0 & 0 \\ 0 & -I^{(r-2)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} 1 \\ r-2 \\ 1 \\ 2(t-r) \\ r-2 \\ k \end{matrix},$$

where $rank(-R_6\,{}^tR_3 + R_3\,{}^tR_6) = 2(t-r)$, $\mathrm{rank}(mK_l\,{}^tm) = 2(t-1)$, so m is a subspace of type $(2(t-1)+k, t-1, k)$ containing U. Again,

$$m \cap U^{\perp} = \begin{pmatrix} 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & 0 & R_6 & 0 & R_8 \\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(k)} & 0 \end{pmatrix} \begin{matrix} r-2 \\ 2(t-r) \\ k \end{matrix}.$$

$$\begin{matrix} 1 & r-2 & v+1-r & 1 & r-2 & v+1-r & k & l-k \end{matrix}$$

this is a subspace of type $(2t-r-2+k, t-r, k)$. Hence, we have shown that $m \in M$.

(2) For any $m \in M$, let $P = m \cap U^{\perp}$. Then P is the subspace of type $(2t-r-2+k, t-r, k)$ containing U, and $U_0 = U \cap U^{\perp} \subset m \cap U^{\perp} = P$. Thus P is a source state contained in m.

Since U is a subspace of type $(r+1,1,1)$ and U_0 a subspace of type $(r-1,0,1)$, exist an isotropic subspace U_1 of type $(2,1,0)$ such that $U = U_0 \perp U_1$. While P is a subspace of type $(2(t-1)-r+k, t-r, k)$, exist a subspace Q_0 of type $(2(t-r)+k-1, t-r, k-1)$ such that $P = U_0 \perp Q_0$. Moreover, $Q_0 = Q_1 \perp Q_2$ where Q_1 is a subspace of type $(2(t-r), t-r, 0)$ and $Q_2 = Q_0 \cap E$. Hence Q_1 is a regular subspace of V, and

$$V = Q_1 \perp Q_1^{\perp},\ m = m \cap V = m \cap (Q_1 \perp Q_1^{\perp}) = Q_1 \perp (Q_1^{\perp} \cap m).$$

Notice that $Q_2, U_0, U_1 \subset Q_1^{\perp} \cap m$, so there is a subspace $V_0 \subset m$, satisfying $Q_1^{\perp} \cap m = Q_2 \oplus U_0 \oplus U_1 \oplus V_0$. Thus

$$\begin{aligned} m &= Q_1 \perp (Q_2 \oplus U_0 \oplus U_1 \oplus V_0) = (Q_1 \oplus Q_2) \oplus (U_0 \oplus U_1 \oplus V_0) \\ &= Q_0 \perp (U_0 \oplus U_1 \oplus V_0) = Q_0 \perp (U \oplus V_0). \end{aligned}$$

Let $e_T = U_0 \oplus U_1 \oplus V_0 = U \oplus V_0$. Since m is a subspace of type $(2(t-1)+k, t-1, k)$, e_T is a subspace of type$(2(r-1)+1, r-1, 1)$, and $U \subset e_T$. Thus e_T is an encoding rule of transmitter satisfying $m = P + e_T$.

Let s' be another source state contained in m. Then $s' \subset m \cap U^{\perp} = P$. Since $\dim s' = \dim P$, $s' = P$. That is, P is uniquely source state contained in m.

Hence, we have shown that the first construction is a well-defined authentication code with arbitration.

Next we compute the parameters of the code.

Lemma 2.2 *The number of the source states is* $|S| = q^{2(t-r)(l-k)} N(2(t-r), t-r; 2(v+1-r)) N(k-1, l-1)$.

Proof. Let $s \in S$. Since $U_0 \subset s \subset U^{\perp}$, s has the form

$$s = \begin{pmatrix} 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & 0 & R_6 & 0 & 0 & R_9 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \end{pmatrix} \begin{matrix} r-2 \\ 2(t-r) \\ 1 \\ k-1 \end{matrix},$$

$$\begin{matrix} 1 & r-2 & v+1-r & 1 & r-2 & v+1-r & 1 & k-1 & l-k \end{matrix}$$

where (R_3, R_6) is a subspace of type $(2(t-r), t-r)$ in the symplectic space $F_q^{2(v+1-r)}$, R_9 arbitrarily. Therefore, the number of the source states is

$$|S| = q^{2(t-r)(l-k)} N(2(t-r), t-r; 2(v+1-r)) N(k-1, l-1).$$

Lemma 2.3 *The number of the encoding rules of transmitter is*

$$|E_T| = \frac{N(r+1,1,1;2r-1,r-1,1;2v+l,v) N(2r-1,r-1,1;2v+l,v)}{N(r+1,1,1;2v+l,v)}.$$

Proof. Since each encoding rule is a subspace of type $(2r-1, r-1, 1)$ containing U in singular symplectic space $F_q^{(2v+l)}$,

$$\begin{aligned} E_T &= N'(r+1,1,1;2r-1,r-1,1;2v+l,v) \\ &= \frac{N(r+1,1,1;2r-1,r-1,1;2v+l,v) N(2r-1,r-1,1;2v+l,v)}{N(r+1,1,1;2v+l,v)}. \end{aligned}$$

Lemma 2.4 *The number of the decoding rules of receiver is*

$$|E_R| = \frac{N(r+1,1,1;2r-3,r-3,1;2v+l,v) N(2r-3,r-3,1;2v+l,v)}{N(r+1,1,1;2v+l,v)}.$$

Proof. Since each encoding rule is a subspace of type $(2r-3, r-3, 1)$ containing U in singular symplectic space $F_q^{(2v+l)}$,

$$\begin{aligned} |E_R| &= N'(r+1,1,1;2r-3,r-3,1;2v+l,v) \\ &= \frac{N(r+1,1,1;2r-3,r-3,1;2v+l,v) N(2r-3,r-3,1;2v+l,v)}{N(r+1,1,1;2v+l,v)}. \end{aligned}$$

Lemma 2.5 *For any $m \in M$, let the number of encoding rules and decoding rules contained in m be a and b, respectively. Then*

$$a = q^{2(r-2)(t-r)+(r-2)(k-1)},\ b = q^{(r-4)(2(t-r)+k-1)}N(r-4,r-2).$$

Proof. Since m is a subspace of type $(2(t-1)+k,t-1,k)$ containing U and $m \cap U^{\perp}$ is a subspace of type $(2t-r-2+k,t-r,k)$ in V, we may take

$$m = \begin{array}{c} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(t-r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I^{(r-2)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(t-r)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k)} & 0 \end{pmatrix} \begin{matrix} 1 \\ r-2 \\ t-r \\ 1 \\ r-2 \\ t-r \\ k \end{matrix} \\ \begin{matrix} 1 & r-2 & t-r & v+1-t & 1 & r-2 & t-r & v+1-t & k & l-k \end{matrix} \end{array}.$$

Let $e_T \in E_T$ and $e_T \subset m$. Since e_T is the subspace of type $(2r-1,r-1,1)$ containing U,

$$e_T = \begin{array}{c} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & 0 & I^{(r-2)} & R_7 & 0 & 0 & R_{10} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} 1 \\ 1 \\ r-2 \\ r-2 \\ 1 \end{matrix} \\ \begin{matrix} 1 & r-2 & t-r & v+1-t & 1 & r-2 & t-r & v+1-t & 1 & k-1 & l-k \end{matrix} \end{array},$$

where R_3, R_7 and R_{10} are arbitrary. Thus the number of e_T contained in m is

$$a = q^{2(r-2)(t-r)+(r-2)(k-1)}.$$

Let $e_R \in E_R$ and $e_R \subset m$. Since e_R is a subspace of type $(2r-3,r-3,1)$ containing U,

$$e_R = \begin{array}{c} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & 0 & R_6 & R_7 & 0 & 0 & R_{10} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} 1 \\ 1 \\ r-2 \\ r-4 \\ 1 \end{matrix} \\ \begin{matrix} 1 & r-2 & t-r & v+1-t & 1 & r-2 & t-r & v+1-t & 1 & k-1 & l-k \end{matrix} \end{array},$$

where R_6 is a $(r-4)$-dimensional subspace in $(r-2)$-dimensional subspace, and R_3, R_7 and R_{10} are arbitrary. Thus the number of e_R contained in m is

$$b = q^{2(t-r)(r-4)+(k-1)(r-4)}N(r-4,r-2) = q^{(r-4)(2(t-r)+k-1)}N(r-4,r-2).$$

Lemma 2.6 *The number of the messages is* $|M| = \frac{|S||E_T|}{a}$.

Proof. Let $\Omega = \{(m, e_T) | m \in M, e_T \in E_T, e_T \subset m\}$. Then

$$|\Omega| = \sum_{m \in M} |\{e_T \in E_T | e_T \subset m\}| = |M|a,$$

and

$$|\Omega| = \sum_{e_T \in E_T} |\{m \in M | e_T \subset m\}|.$$

Since m only contains a source state for any $m \in M$, $|\{m \in M | e_T \subset m\}| = |S|$. Therefore,

$$|\Omega| = \sum_{e_T \in E_T} |S| = |S||E_T|.$$

Furthermore, $|M| = \frac{|S||E_T|}{a}$.

By Lemmas 2.1-2.6, we have Theorem 2.1.

Theorem 2.1 *The parameters of constructed authentication code with arbitration are*

$$|M| = \frac{|S||E_T|}{a};$$

$$|S| = q^{2(t-r)(l-k)} N(2(t-r), t-r; 2(v+1-r)) N(k-1, l-1);$$

$$|E_T| = \frac{N(r+1,1,1;2r-1,r-1,1;2v+l,v) N(2r-1,r-1,1;2v+l,v)}{N(r+1,1,1;2v+l,v)};$$

$$|E_R| = \frac{N(r+1,1,1;2r-3,r-3,1;2v+l,v) N(2r-3,r-3,1;2v+l,v)}{N(r+1,1,1;2v+l,v)}.$$

Lemma 2.7 *(1) For any $e_T \in E_T$, the number of decode rules e_R contained in e_T is $c = N(r-4, r-2)$.*

(2) For any $e_R \in E_R$, the number of encode rules e_T containing e_R is $d = q^{4(v+1-r)+2(l-1)}$.

Proof. (1) Let $e_T \in E_T$. Then e_T is a subspace of type $(2r-1, r-1, 1)$ containing U. We can suppose that

$$e_T = \begin{array}{c} \\ \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I^{(r-2)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \\ \begin{array}{cccccccc} 1 & r-2 & v+1-r & 1 & r-2 & v+1-r & 1 & l-1 \end{array} \end{array} \begin{array}{c} \\ 1 \\ 1 \\ r-2 \\ r-2 \\ 1 \end{array}.$$

For any $e_R \in E_R$. If $e_R \subset e_T$, for e_R is a subspace of type $(2r-3, r-3, 1)$ containing U, then we can suppose that

$$e_R = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & R_5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & r-2 & v+1-r & 1 & r-2 & v+1-r & 1 & l-1 \end{pmatrix} \begin{matrix} 1 \\ 1 \\ r-2 \\ r-4 \\ 1 \end{matrix},$$

where R_5 is a $(r-4)$-dimensional subspace in $(r-2)$-dimensional subspace. Thus the number of e_R contained in e_T is $c = N(r-4, r-2)$.

(2) Let $e_R \in E_R$. Then e_R is a subspace of type $(2r-3, r-3, 1)$ containing U. We can assume that

$$e_R = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I^{(r-4)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & r-2 & v+1-r & 1 & r-4 & 2 & v+1-r & 1 & l-1 \end{pmatrix} \begin{matrix} 1 \\ 1 \\ r-2 \\ r-4 \\ 1 \end{matrix}.$$

For any $e_T \in E_T$. If $e_T \supset e_R$, for e_T is a subspace of type $(2r-1, r-1, 1)$ containing U, then we can assume that

$$e_T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I^{(r-4)} & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & 0 & R_6 & R_7 & 0 & R_9 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & r-2 & v+1-r & 1 & r-4 & 2 & v+1-r & 1 & l-1 \end{pmatrix} \begin{matrix} 1 \\ 1 \\ r-2 \\ r-4 \\ 2 \\ 1 \end{matrix},$$

where R_3, R_7, R_9 arbitrarily, and $R_6 = I^{(2)}$. Thus the number of e_T containing e_R is $d = q^{4(v+1-r)+2(l-1)}$.

Lemma 2.8 *For any $m \in M$ and $e_R \in E_R$. If $e_R \subset m$, the the number of encode rules e_T containing e_R and contained in m is $q^{2(2t+k-2r-1)}$.*

Proof. Let the matrix representation of m be the same as Lemma 2.5. For any

$e_R \in E_R$. If $e_R \subset m$, then we write

$$e_R = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & 0 & R_6 & R_7 & 0 & 0 & R_{10} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} 1 \\ 1 \\ r-2 \\ r-4 \\ 1 \end{matrix}$$

$$\begin{matrix} 1 & r-2 & t-r & v+1-t & 1 & r-2 & t-r & v+1-t & 1 & k-1 & l-k \end{matrix}$$

where R_6 is a $(r-4)$-dimensional subspace in $(r-2)$-dimensional subspace. For any $e_T \in E_T$. If $e_T \subset m$ and $e_T \supset e_R$, then we can write

$$e_T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & 0 & R_6 & R_7 & 0 & 0 & R_{10} & 0 \\ 0 & 0 & R_3' & 0 & 0 & R_6' & R_7' & 0 & 0 & R_{10}' & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} 1 \\ 1 \\ r-2 \\ r-4 \\ 2 \\ 1 \end{matrix}$$

$$\begin{matrix} 1 & r-2 & t-r & v+1-t & 1 & r-2 & t-r & v+1-t & 1 & k-1 & l-k \end{matrix}$$

where $\begin{pmatrix} R_6 \\ R_6' \end{pmatrix}$ is a $(r-2)$-dimensional vector space, R_3', R_7' and R_{10}' arbitrarily. Thus the number of e_T containing e_R and contained in m is $q^{2(2t+k-2r-1)}$.

Lemma 2.9 *Assume that m_1 and m_2 are two distinct messages which commonly contain an encoding rule e_T' of the transmitter. Assume that s_1 and s_2 are two source states contained in m_1 and m_2, respectively. Let $s_0 = s_1 \cap s_2$, and $\dim s_0 = k_1$. Then*

(1) $r-1 \le k_1 \le 2t-r-3+k$;

(2) the number of e_R contained in $m_1 \cap m_2$ is $N(r-4, r-2)q^{(r-4)(k_1-r+1)}$; and

(3) the number of e_T containing e_R in $m_1 \cap m_2$ is $q^{2(k_1-r+1)}$ for any $e_R \subset m_1 \cap m_2$.

Proof. (1) Clearly, $m_1 = s_1 + e_T'$, and $m_2 = s_2 + e_T'$. For $m_1 \neq m_2$, $s_1 \neq s_2$. Again because of $s_1 \supset U_0$ and $s_2 \supset U_0$, $r-1 \le k_1 \le 2t-r-3+k$.

(2) Let s_i' be the complementary subspace of s_0 in s_i. Then $s_i = s_0 \oplus s_i'$ $(i = 1,2)$. For $s_i = m_i \cap U^{\perp} (i = 1,2)$,

$$s_0 = \left(m_1 \cap U^{\perp}\right) \cap \left(m_2 \cap U^{\perp}\right) = m_1 \cap m_2 \cap U^{\perp} = s_1 \cap m_2 = s_2 \cap m_1,$$

and

$$m_1 \cap m_2 = (s_1 + e_T') \cap m_2 = (s_0 + s_1' + e_T') \cap m_2 = ((s_0 + e_T') + s_1') \cap m_2.$$

Again, for $s_0 + e_T' \subset m_2$,

$$m_1 \cap m_2 = (s_0 + e_T') + (s_1' \cap m_2).$$

Furthermore, $m_1 \cap m_2 = s_0 + e_T'$ for $s_1' \cap m_2 \subseteq s_1 \cap m_2 = s_0$.

Since $\dim(m_i) = \dim(s_i) + \dim(e_T') - \dim(s_i \cap e_T')$,

$$\dim(s_i \cap e_T') = r - 1.$$

Due to $\dim(U_0) = r-1$, and $U_0 \subseteq s_i \cap e_T$, so $s_i \cap e_T = U_0$ $(i = 1,2)$. Therefore,

$$\dim(m_1 \cap m_2) = \dim(s_0) + \dim(e_T') - \dim\left(s_0 \cap e_T'\right) = k_1 + r.$$

Without loss of generality, we can assume

$$e_T' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I^{(r-2)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} 1 \\ 1 \\ r-2 \\ r-2 \\ 1 \end{matrix}$$
$$\begin{matrix} 1 & r-2 & v+1-r & 1 & r-2 & v+1-r & 1 & l-1 \end{matrix}$$

Then m_1 and m_2 have the matrix representations

$$m_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & A_3 & 0 & 0 & A_6 & 0 & A_8 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I^{(r-2)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & A_8' \end{pmatrix} \begin{matrix} 1 \\ r-2 \\ 2(t-r) \\ 1 \\ r-2 \\ 1 \\ k-1 \end{matrix}$$
$$\begin{matrix} 1 & r-2 & v+1-r & 1 & r-2 & v+1-r & 1 & l-1 \end{matrix}$$

and

$$m_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & B_3 & 0 & 0 & B_6 & 0 & B_8 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I^{(r-2)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & B_8' \end{pmatrix} \begin{matrix} 1 \\ r-2 \\ 2(t-r) \\ 1 \\ r-2 \\ 1 \\ k-1 \end{matrix}$$
$$\begin{matrix} 1 & r-2 & v+1-r & 1 & r-2 & v+1-r & 1 & l-1 \end{matrix}$$

respectively. Thus

$$m_1 \cap m_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & C_3 & 0 & 0 & C_6 & 0 & C_8 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I^{(r-2)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & C_8' \end{pmatrix} \begin{matrix} 1 \\ r-2 \\ 2(t-r) \\ 1 \\ r-2 \\ 1 \\ k-1 \end{matrix}$$
$$\begin{matrix} 1 & r-2 & v+1-r & 1 & r-2 & v+1-r & 1 & l-1 \end{matrix}$$

For $\dim(m_1 \cap m_2) = k_1 + r$,

$$\dim \begin{pmatrix} 0 & 0 & C_3 & 0 & 0 & C_6 & 0 & C_8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & C_8' \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} = k_1 - r + 2.$$

For any $e_R \in E_R$. If $e_R \subset m_1 \cap m_2$, then

$$e_R = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & R_5 & R_6 & 0 & R_8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} 1 \\ 1 \\ r-2 \\ r-4 \\ 1 \end{matrix},$$
$$\begin{matrix} 1 & r-2 & v+1-r & 1 & r-2 & v+1-r & 1 & l-1 \end{matrix}$$

where R_5 is a $(r-4)$-dimensional subspace in $(r-2)$-dimensional subspace while every row of $(0 \;\; 0 \;\; R_3 \;\; 0 \;\; 0 \;\; R_6 \;\; 0 \;\; R_8)$ is a linear combination of the base of subspace

$$\begin{pmatrix} 0 & 0 & C_3 & 0 & 0 & C_6 & 0 & C_8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & C_{8'} \end{pmatrix}.$$

Therefore, the number of e_R contained in $m_1 \cap m_2$ is

$$q^{(r-4)(k_1-r+2-1)} N(r-4, r-2) = q^{(r-4)(k_1-r+1)} N(r-4, r-2).$$

(3) Assume that $m_1 \cap m_2$ has the form as above. Then, for any $e_R \subset m_1 \cap m_2$, we can write

$$e_R = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & R_5 & R_6 & 0 & R_8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} 1 \\ 1 \\ r-2 \\ r-4 \\ 1 \end{matrix},$$
$$\begin{matrix} 1 & r-2 & v+1-r & 1 & r-2 & v+1-r & 1 & l-1 \end{matrix}$$

where R_5 is a $(r-4)$-dimensional subspace in $(r-2)$-dimensional subspace. For any $e_T \in E_T$. If $e_R \subset e_T$ and $e_T \subset m_1 \cap m_2$, then

$$e_T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & R_5 & R_6 & 0 & R_8 \\ 0 & 0 & R_3' & 0 & R_5' & R_6' & 0 & R_8' \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} 1 \\ r-2 \\ 1 \\ r-4 \\ 2 \\ 1 \end{matrix}$$

$$\begin{matrix} 1 & r-2 & v+1-r & 1 & r-2 & v+1-r & 1 & l-1 \end{matrix}$$

where $\begin{pmatrix} R_5 \\ R_5' \end{pmatrix}$ is a $(r-2)$-dimensional subspace while every row of

$$(0 \quad 0 \quad R_3' \quad 0 \quad 0 \quad R_6' \quad 0 \quad R_8')$$

is a linear combination of the base of subspace

$$\begin{pmatrix} 0 & 0 & C_3 & 0 & 0 & C_6 & 0 & C_8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & C_{8'} \end{pmatrix}.$$

Therefore, the number of e_T containing e_R in $m_1 \cap m_2$ is $q^{2(k_1-r+1)}$.

Theorem 2.2 *In the A^2 authentication code that we construct above, if the encoding rules of the transmitter and the receiver are chosen according to a uniform probability distribution, then the largest probabilities of success for different types of deceptions are $P_I = \frac{1}{q^{(r-4)(2(v-t+1)+l-k)}}$, $P_S = \frac{1}{q^{(r-4)}}$, $P_T = \frac{q^2-1}{q^{(r-2)}-1}$, $P_{R_0} = \frac{1}{q^{4(v-t)+2(l-k)+8}}$, and $P_{R_1} = \frac{1}{q^2}$, respectively.*

Proof. (1) Since the number of e_R contained in m is b by Lemma 2.5,

$$P_I = \max_{m \in M} \frac{|\{e_R \in E_R | e_R \subset m\}|}{|E_R|} = \frac{b}{|E_R|} = \frac{1}{q^{(r-4)(2(v-t+1)+l-k)}}.$$

(2) Because of $|\{e_R \in E_R | e_R \subset m, e_R \subset m'\}| = N(r-4, r-2)q^{(r-4)(k_1-r+1)}$ by Lemma 2.9, where $r-1 \le k_1 \le 2t-r-3+k$,

$$\begin{aligned} P_S &= \max_{m \in M} \frac{\max_{m \neq m' \in M} |\{e_R \in E_R | e_R \subset m \text{ and } e_R \subset m'\}|}{|e_R \in E_R | e_R \subset m|} \\ &= \frac{q^{(r-4)(k_2-r+1)} N(r-4, r-2)}{b} \\ &= \frac{1}{q^{(r-4)}}, \end{aligned}$$

where $k_2 = 2t - r - 3 + k$.

(3) Since

$$P_T = \max_{e_T \in E_T} \frac{\max_{m \in M, e_T \not\subset m} |\{e_R \in E_R | e_R \subset m \text{ and } p(e_R, e_T) \neq 0\}|}{|\{e_R \in E_R | p(e_R, e_T) \neq 0\}|}$$
$$= \max_{e_T \in E_T} \frac{\max_{m \in M, e_T \not\subset m} |\{e_R \in E_R | e_R \subset m \cap e_T\}|}{|\{e_R \in E_R | e_R \subset e_T\}|}.$$

Assume that $e_T \not\subset m$. Let $e_T = U \oplus W$, and $m = U \oplus \Omega$. Then $\dim(W) = (2r-1)-(r+1) = r-2$, and $\dim(\Omega) = 2(t-1)+k-(r+1) = 2t-r+k-3$. Because $U \subset e_R \subset e_T \cap m$,

$$\begin{aligned} e_R &= e_R \cap e_T = U \oplus (e_R \cap W) \\ &= e_R \cap m = U \oplus (e_R \cap \Omega) \\ &\supseteq U \oplus (e_R \cap W \cap \Omega). \end{aligned}$$

So $\dim(e_R \cap W \cap \Omega) \leq r-4$, and $e_R \cap W \cap \Omega$ is at most a $(r-4)$-dimensional subspace in $W \cap \Omega$ subspace. Since $e_T \not\subset m$, $\dim(W \cap \Omega) \leq r-3$. When $\dim(W \cap \Omega) = r-3$,

$$e_T = \begin{pmatrix} U \\ W \cap \Omega \\ e_{v+r-2} \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & I^{(r-3)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} 1 \\ 1 \\ r-2 \\ 1 \\ r-3 \\ 1 \end{matrix},$$
$$\begin{matrix} 1 & r-2 & v+1-r & 1 & r-3 & 1 & v+1-r & 1 & l-l \end{matrix}$$

where $e_T \cap m = \begin{pmatrix} U \\ W \cap \Omega \end{pmatrix}$, and $W \cap \Omega = (\,0\ \ 0\ \ 0\ \ 0\ \ I^{(r-3)}\ \ 0\ \ 0\ \ 0\ \ 0\,)$.

Since $e_R \subset e_T$,

$$e_R = \begin{pmatrix} U \\ e_R \cap W \cap \Omega \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & R_5 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} 1 \\ 1 \\ r-2 \\ 1 \\ r-4 \end{matrix},$$
$$\begin{matrix} 1 & r-2 & v+1-r & 1 & r-3 & 1 & v+1-r & 1 & l-1 \end{matrix}$$

where $e_R \cap W \cap \Omega = (\ 0\ \ 0\ \ 0\ \ 0\ \ R_5\ \ 0\ \ 0\ \ 0\ \ 0\ )$. So $e_R \cap W \cap \Omega$ is a $(r-4)$-dimensional subspace in $W \cap \Omega$, $\operatorname{rank}(R_5) = r-4$, and the number of R_5 is $N(r-4, r-3)$. The number of e_R is $N(r-4, r-3)$ at most. The number of e_R contained in e_T is c by Lemma 2.7. Thus

$$P_T = \frac{N(r-4, r-3)}{c} = \frac{q^2-1}{q^{r-2}-1}.$$

(4) For $m \in M$, we can assume

$$m = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(t-r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I^{(r-2)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(t-r)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k)} & 0 \end{pmatrix} \begin{matrix} 1 \\ r-2 \\ t-r \\ 1 \\ r-2 \\ t-r \\ k \end{matrix},$$
$$\begin{matrix} 1 & r-2 & t-r & v+1-t & 1 & r-2 & t-r & v+1-t & k & l-k \end{matrix}$$

For $e_R \in E_R$, if $e_R \subset m$, then e_R has form

$$e_R = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & 0 & R_6 & R_7 & 0 & 0 & R_{10} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} 1 \\ 1 \\ r-2 \\ r-4 \\ 1 \end{matrix},$$
$$\begin{matrix} 1 & r-2 & t-r & v+1-t & 1 & r-2 & t-r & v+1-t & 1 & k & l-k \end{matrix}$$

where $\operatorname{rank}(R_6) = r-4$. At the same time, for $e_T \in E_T$, if $e_R \subset e_T \subset m$, then e_T has form

$$e_T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(r-2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & 0 & R_6 & R_7 & 0 & 0 & R_{10} & 0 \\ 0 & 0 & R_3' & 0 & 0 & R_6' & R_7' & 0 & 0 & R_{10}' & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} 1 \\ 1 \\ r-2 \\ r-4 \\ 2 \\ 1 \end{matrix},$$
$$\begin{matrix} 1 & r-2 & t-r & v+1-t & 1 & r-2 & t-r & v+1-t & 1 & k-1 & l-k \end{matrix}$$

where rank $\begin{pmatrix} R_6 \\ R_6' \end{pmatrix} = r-2$, and R_3', R_7' and R_{10}' are arbitrary. The number of e_T containing e_R and contained in m is $q^{2(2(t-r)+k-1)}$. Thus

$$\begin{aligned} P_{R_0} &= \max_{e_R \in E_R} \left\{ \frac{\max\limits_{m \in M} |\{e_T \in E_T | e_T \subset m \text{ and } p(e_R, e_T) \neq 0\}|}{|\{e_T \in E_T | p(e_R, e_T) \neq 0\}|} \right\} \\ &= \max_{e_R \in E_R} \left\{ \frac{\max\limits_{m \in M} |\{e_T \in E_T | e_T \subset m \text{ and } e_R \subset e_T|}{|\{e_T \in E_T | e_R \subset e_T|} \right\} \\ &= \frac{q^{2(2t-2r+k-1)}}{d} \\ &= \frac{1}{q^{4(v-t)+2(l-k)+8}}. \end{aligned}$$

(5) Assume that the receiver declares to receive a message m_2 instead of m_1, when s_2 contained in m_1 is different from s_2 contained in m_2, the receiver's substitution attack can be successful. Since $e_R \subset e_T' \subset m_1$, receiver is superior to select e_T', satisfying $e_R \subset e_T' \subset m_1$, thus $m_2 = s_2 + e_T'$, and $\dim(s_1 \cap s_2) = k_1$ as large as possible. Therefore, the probability of a receiver's successful substitution attack is

$$P_{R_1} = \frac{q^{2(k_1-r+1)}}{q^{2(2(t-r)+k-1)}},$$

where $k_1 = 2t-r-3+k$. $P_{R_1} = \frac{1}{q^2}$ is the largest.

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. The definition of multireceiver authentication codes refer to [16].

Let $n = 2v+l, 4 < r < t < v+1, v \geq 6, 1 \leq k < l$. Let U be a fixed subspace of type $(r+1,1,1)$ in V, then $U^\perp$ is a subspace of type $(2v-r+l, v+1-r, l)$ in V. Let $U_0 = U \cap U^\perp$, then U_0 is a subspace of type $(r-1,0,1)$ in V. Let $S = \{s |\ s$ is a subspace of type $(2t-r-2+k, t-r, k)$ and $U_0 \subset s \subset U^\perp\}$; let $E = \{e \mid e$ is a subspace of type $(2r-1, r-1, 1)$ and $U \subset e\}$; let $M = \{m | m$ is a subspace of type $(2(t-1)+k, t-1, k), U \subset m, m \cap U^\perp$ is a subspace of type $(2t-r-2+k, t-r, k)\}$, and let $M^* = \{(m_1, m_2, \cdots, m_\lambda) \in M^\lambda | m_1 \cap U^\perp = m_2 \cap U^\perp = \cdots = m_\lambda \cap U^\perp\}$.

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

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

$$\pi_i(f(s,e))=\pi(s+e_1,s+e_2,\cdots,s+e_{\lambda})=s+e_i,$$

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

Therefore, $\pi_i(f(s,e))=f_i((I_s\times\tau_i)(s,e))$. 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:*

$$P_I[i,J]=\frac{1}{q^{(r-2)(2(v-t)+l-k+2)}},P_S[i,J]=\frac{1}{q^{(r-2)(2v-2t+l-k+5)}}.$$

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

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

$$\tau_J(e)=e_J\Longleftrightarrow e=(\cdots,e_{i_1},\cdots,e_{i_j},\cdots).$$

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

$$f_i(s,e_i)=\pi_i(m),s+e_i=m_i=\pi_i(m). \tag{1}$$

From Lemma 2.5, we know the number of e_i satisfying (1) is a. For any e_i satisfying (1), the number of e satisfying $\tau_J(e)=e_J$ and $\tau_i(e)=e_i$ is $|\,E\,|^{\lambda-j-1}$. So

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

And $a=q^{(r-2)(2t-2r+l-1)}$, thus

$$\begin{aligned}P_I[i,J] &= \max_{e_J\in E^J}\max_{s\in S}\max_{m\in M}\frac{|\,\{e\in E^{\lambda}|\tau_J(e)=e_J,\tau_i(e)=e_i,f_i(s,e_i)=\pi_i(m)\}\,|}{|\,\{e\in E^{\lambda}|\tau_J(e)=e_J\}\,|}\\ &= \max_{e_J\in E^J}\max_{s\in S}\max_{m\in M}\frac{a}{|\,E\,|}\end{aligned}$$

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

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

Now we compute the probability of substitution attack. We know

$$m = f(s,e) = (s+e_1, s+e_2, \cdots, s+e_\lambda) = (m_1, m_2, \cdots, m_\lambda).$$

and $\tau_J(e) = (e_{i_1}, e_{i_2}, \cdots, e_{i_j})$, whenever $e = (e_1, e_2, \cdots, \underbrace{e_{i_1}, \cdots, e_{i_j}}_{j}, e_k, \cdots, e_\lambda)$. While

$$| \{e \in E^\lambda | m = f(s,e), \tau_J(e) = e_J\} | = | E |^{\lambda - j},$$

$| \{e \in E^\lambda | m = f(s,e), \tau_J(e) = e_J, \tau_i(e) = e_i \in E_i, f_i(s', e_i) = \pi_i(m)\} | = | E |^{\lambda-j-1} \times b,$
and $b = q^{(r-2)(k_1-r+1)}$. Therefore,

$$P_s[i,J]$$

$$= \max_{e_J \in E^J} \max_{s \in S, m \in M} \max_{s \neq s' \in S} \frac{|\{e \in E^\lambda | m = f(s,e), \tau_J(e) = e_J, \tau_i(e) = e_i \in E_i, f_i(s', e_i) = \pi_i(m')\}|}{|\{e \in E^\lambda | m = f(s,e), \tau_J(e) = e_J\}|}$$

$$= \max_{e_J \in E^J} \max_{s \in S, m \in M} \max_{s \neq s' \in S} \frac{b}{|E|}$$

$$= \max_{e_J \in E^J} \max_{s \in S, m \in M} \max_{s \neq s' \in S} \frac{q^{(r-2)(k_1-r-1)}}{q^{(r-2)(2v-2r+l+1)}}$$

$$= \frac{1}{q^{(r-2)(2v-2t+l-k+5)}}$$

where $k_1 = 2t - r - 3 + k$.

The results about multi-receiver authentication codes based on geometry of classical groups over finite fields are fewer.

References

[1] E.N. Gilbert, F.J. Mac Williams, N.J.A. Slone. Codes which detect deception, Bell Syst. Tech.J. 1974(53):405-424.

[2] G.J. Simmons. Authentication theorey/coging theorey. Advance in Cryptology: Proc. of Crypto 84, Lecture Notes in Computer Science, 1985(196):411-432.

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

[4] Desmedt,Y., Frankel,Y., Yung,M.. Multer-receiver/Multi-sender network security: efficient authenticated multicast/feedback, in IEEE infocom'92: 2045-2054.

[5] Wan Zhexian. Construction of Cartesian Authentication Codes from Unitary Geometry. Designs, Codes and cryptology. 1992, 2:333-356.

[6] Feng Rongquan.Construction of Cartesian Authentication Codes from Geometry of Classical Groups. Northeast Mathematical Journal. 1999, 15(1): 103-114.

[7] You Hong, Gao You. Some new Constructions of Cartesian Authentication Codes from Symplectic Geometry. System Science and Mathematical Science. 1994, 7(4):317-327.

[8] Gao You, Zou Zengjia. Some Constructions of Cartesian Authentication Codes from Pseudo- Symplectic Geometry[J]. Northeast. Math.J 1995, 11(1):47-55.

[9] Gao You, Wang Yuandong. Two New Constructions of Cartesian Authentication Codes from Symplectic Geometry. Applied Mathematics Journal of Chinese Univerties, 1995, 10(3), B:345-356.

[10] Gao You, Shi Xinhua, Wang Hongli. Construction of Authentication Codes with Arbitration from Singular Symplectic Geometry over Finite Fields. Acta Scientiarum Naturalium Universitatis Nankaiensis. 2008,6:72-77 .

[11] Wang Hongli, Gao You. Construction of Authentication Codes with Arbitration from Singular Pseudo-Symplectic Geometry. Acta Scientiarum Naturalium Science and Engineering UniversityOf Hebei 2008, 2:65-70.

[12] Qi Yingchun, Zhou Tong.Talking Multi-sender Authentication Codes and Construction of Method.Zhong Zhou University, 2003, 20(1):118-120.

[13] Ma WenPing, Wang XinMei.A Few New Structure methods of Multi-sender Authentication Codes. Electronics College Journal, 2000, 28(4):117-119.

[14] Li Xiyang, Qin Cong. New Constructions of Multi-receiver Authentication Codes. Calculator Engineering, 2008,34(15):138-139.

[15] Du Qingling, Zhang LiMin.The Relevant Boundary and Construction Of Multi-receiver Authentication Codes .Electronics Information College Journal, 2002, 24(8): 1109-1112.

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

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

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