The Construction of A^3-code from Singular Pseudo-symplectic Geometry over Finite Fields

LIU YANQIN
Civil Aviation University of China
College of Science
Dongli District, Tianjin
CHINA
yanqinliu1024@163.com

GAO YOU
Civil Aviation University of China
College of Science
Dongli District, Tianjin
CHINA
gao_you@263.net

ZHANG DAKE
Tianjin University of Sci & Tech
College of Science
HeXi District, Tianjin
CHINA
zhangdake@126.com

Abstract: A construction of A^3-code from singular pseudo-symplectic geometry over finite fields is presented. Under the assumption that the encoding rules of the transmitter, the receiver and the arbiter are chosen according to a uniform probability distribution, the parameters and the probabilities of success for different types of deceptions are computed.

Key–Words: A^3-codes, Singular Pseudo-symplectic Geometry , Finite fields.

1 Introduction

Security is very important in the process of information's transmission and storage, and the confidentiality and authentication become two important aspects of contemporary information systems. C.E.Shannon firstly researched confidentiality issues using the method of information theory in the 1940s [1], puting forward the concept of perfect security system. G.J.Simmons applied information theory to the research of authentication problem in the 1980s[2]. Authentication code has become the basic conditions of unconditionally secure authentication cryptography. Gilbert, Mac Williams and Sloane proposed the concept of authentication codes for the first time in a paper published in 1974, and constructed the first authentication code[3], which promoted the development of the message authentication. In 1992, Mr. Wan firstly constructed authentication codes without arbitration using the geometry of classical groups over finite fields[4].

There are three sides in usually authentication models, where the receiver and transmitter trust each other and they share a common key. But there are also other circumstances where the receiver and transmitter cheat each other, such as the transmitter sends an illegal message to the receiver, or the receiver claims to receive other messages after receiving legal messages. In order to solve the dispute between the transmitter and receiver, Simmons proposed the concept and construction method of authentication codes with arbitration[5, 6]. In this case, the arbiter is credible. When there is a dispute between the receiver and the transmitter, the arbiter is required to judge the legitimacy of the message. Authentication code with arbitration is also referred to A^2-code.

As to the construction of A^2-code, the domestic and foreign scholars have provided abundant research achievements, such as [7, 8, 9]. In many practical cases, the arbiter may also be incredible, he might attack the authentication system. Brickell and Stinson [10] introduced authentication code with dishonest arbiter, or A^3-code for short. In an A^3-code, each participant in the system has some secret key information which is used to protect him/her against attacks in the system. The code has been also studied in [11, 12, 13], where some constructions were given.

Let $\mathcal{S}, \mathcal{M}, \mathcal{E_T}, \mathcal{E_R}, \mathcal{E_A}$ be the set of source states, the set of messages, the sets of transmitter's, receiver's and arbiter's keys, respectively. Similar to A^2-code, the transmitter's key $e_t \in \mathcal{E_T}$ determines the encoding function $f : \mathcal{S} \times \mathcal{E_T} \to \mathcal{M}$. The receiver's key $e_r \in \mathcal{E_R}$ determines the decoding function $g : \mathcal{M} \times \mathcal{E_R} \to \mathcal{S} \cup \{\text{reject}\}$. If $g(m, e_r) \in \mathcal{S}$, the receiver will accept m as valid. The arbiter's key $e_a \in \mathcal{E_A}$ determines a subset $\mathcal{M}(e_a) \subseteq \mathcal{M}$. If $m \in \mathcal{M}(e_a)$, the arbiter will determine m as valid, where $\mathcal{M}(e_a)$ is the set of possible messages which are valid for the arbiter's key e_a. The transmitter T uses his key information e_t to encrypt a source state $s \in \mathcal{S}$ into a message $m \in \mathcal{M}$, i.e., $m = f(s, e_t)$, and then send m to the receiver R through a public channel. R uses his key information e_r to verify the authenticity of the received message m. The arbiter A who doesn't know the key information of T and R will resolve a dispute between the T and R using his key information.

Let $\mathcal{M}(e_t)$ be the set of possible messages for transmitter's key information e_t, then $\mathcal{M}(e_t) = \{m \in \mathcal{M} : f(s, e_t) = m, s \in \mathcal{S}\}$. Let $\mathcal{M}(e_r)$ be the set of possible messages for receiver's key information e_r, then $\mathcal{M}(e_r) = \{m \in \mathcal{M} : g(m, e_r) \in \mathcal{S}\}$. Let $\mathcal{E}_\mathcal{T}(e_r)$ be the set of possible transmitter's key information for a given receiver's key e_r, then $\mathcal{E}_\mathcal{T}(e_r) = \{e_t \in \mathcal{E}_\mathcal{T} : f(s, e_t) \in \mathcal{M}(e_r), s \in \mathcal{S}\}$. Let $\mathcal{E}_\mathcal{T}(e_a)$ be the set of possible transmitter's key information for a given arbiter's key e_a, then $\mathcal{E}_\mathcal{T}(e_a) = \{e_t \in \mathcal{E}_\mathcal{T} : f(s, e_t) \in \mathcal{M}(e_a), s \in \mathcal{S}\}$. For any message $m \in \mathcal{M}$, we assume that there exists at least one receiver's key $e_r \in \mathcal{E}_\mathcal{R}$ and one arbiter'k key $e_a \in \mathcal{E}_\mathcal{A}$ such that $m \in \mathcal{M}(e_r) \cap \mathcal{M}(e_a)$, otherwise the message m can be deleted from $\mathcal{M}$. Given a receiver's key e_r and an arbiter's key e_a, for any message $m \in \mathcal{M}(e_r) \cap \mathcal{M}(e_a)$ (if $\mathcal{M}(e_r) \cap \mathcal{M}(e_a) \neq \emptyset$), we assume that there exists at least one transmitter's key $e_t \in \mathcal{E}_\mathcal{T}(e_r) \cap \mathcal{E}_\mathcal{T}(e_a)$ such that $m \in \mathcal{M}(e_t)$, otherwise the message m can be deleted from $\mathcal{M}(e_r) \cap \mathcal{M}(e_a)$.

The receiver and the arbiter must recognize all the legal messages from the transmitter. Thus the participants' keys must have been chosen appropriately. This means that there is a dependence among the three participants' keys and all triple (e_t, e_r, e_a) will not be possible in general.

In the A^3-code the following seven types of cheating attacks are considered.

1. *Attack I*(Impersonation by the opponent). The opponent sends a message m to the receiver and succeeds if this message m is accepted as authentic by the receiver.

2. *Attack S*(Substitution by the opponent). Observing a legitimate message m ,the opponent places another message m' into the channel. He is successful if the receiver accept m' as an authentic message.

3. *Attack T*(Impersonation by the transmitter). Transmitter sends a fraudulent message m which is not valid under his key e_t. The transmitter succeeds if this message m is accepted by the receiver as authentic.

4. *Attack* R_0 (Impersonation by the receiver). The transmitter didn't send any message, but the receiver claims to have received a message m from the transmitter. The receiver succeeds if the message m is valid under the arbiter's key e_a.

5. *Attack* R_1 (Substitution by the receiver). Receiving the legitimate message m and using his key e_r, the receiver claims to have received a message $m'(m' \neq m)$. He succeeds if the message m' is valid under the arbiter's key e_a.

6. *Attack* A_0 (Impersonation by the arbiter). This attack is similar to the Attack I. The arbiter sends a message m to the receiver using his key e_a and he succeeds if m is accepted as authentic by the receiver. The arbiter will have a better chance of success than the opponent for he has more information about the keys.

7. *Attack* A_1 (Substitution by the arbiter). This attack is similar to the Attack S. Knowing the legitimate message m and using his key e_a, the arbiter puts another message m' into the channel. He succeeds if the message m' is accepted by the receiver.

All parameters in the model except the actual choices of participants' keys are public information. The cheating person uses the optimal strategy when choosing the message. For the seven possible types of deceptions, we denote the probability of success in each attack by P_I, P_S, P_T, P_{R_0}, P_{R_1}, P_{A_0}, P_{A_1}, respectively. We introduce the following notations. Let $\mathcal{E}_\mathcal{T}, \mathcal{E}_\mathcal{R}, \mathcal{E}_\mathcal{A}$ be the set of transmitter's, receiver's and arbiter's keys, respectively.

$\mathcal{E}_\mathcal{X}(m) = \{e_x \in \mathcal{E}_\mathcal{X} : m \text{ is available for } e_x\}$.

$\mathcal{E}_\mathcal{X}(e_y) = \{e_x \in \mathcal{E}_\mathcal{X} : p(e_x, e_y) > 0\}$.

$\mathcal{M}(e_y) = \{m \in \mathcal{M} : m \text{ is available for } e_y\}$.

Using the above notations, we have the definition as:

Definition 1

$$P_I = \max_m \frac{|\mathcal{E}_\mathcal{R}(m)|}{|\mathcal{E}_\mathcal{R}|} \tag{1}$$

$$P_S = \max_{\substack{m,m' \\ m \neq m'}} \frac{|\mathcal{E}_\mathcal{R}(m) \cap \mathcal{E}_\mathcal{R}(m')|}{|\mathcal{E}_\mathcal{R}(m)|} \tag{2}$$

$$P_T = \max_{\substack{m,e_t \\ m \notin \mathcal{M}(e_t)}} \frac{|\mathcal{E}_\mathcal{R}(m) \cap \mathcal{E}_\mathcal{R}(e_t)|}{|\mathcal{E}_\mathcal{R}(e_t)|}, \tag{3}$$

$$P_{R_0} = \max_{m,e_r} \frac{|\mathcal{E}_\mathcal{A}(m) \cap \mathcal{E}_\mathcal{A}(e_r)|}{|\mathcal{E}_\mathcal{A}(e_r)|}, \tag{4}$$

$$P_{R_1} = \max_{\substack{m,m',e_r \\ m \neq m'}} \frac{|\mathcal{E}_\mathcal{A}(m) \cap \mathcal{E}_\mathcal{A}(m') \cap \mathcal{E}_\mathcal{A}(e_r)|}{|\mathcal{E}_\mathcal{A}(m) \cap \mathcal{E}_\mathcal{A}(e_r)|}, \tag{5}$$

where $P(m, e_r) \neq 0$.

$$P_{A_0} = \max_{m,e_a} \frac{|\mathcal{E}_\mathcal{R}(m) \cap \mathcal{E}_\mathcal{R}(e_a)|}{|\mathcal{E}_\mathcal{R}(e_a)|}, \tag{6}$$

$$P_{A_1} = \max_{\substack{m,m',e_a \\ m \neq m'}} \frac{|\mathcal{E}_\mathcal{R}(m) \cap \mathcal{E}_\mathcal{R}(m') \cap \mathcal{E}_\mathcal{R}(e_a)|}{|\mathcal{E}_\mathcal{R}(m) \cap \mathcal{E}_\mathcal{R}(e_a)|}, \tag{7}$$

where $P(m, e_a) \neq 0$.

It is then convenient to calculate the different probabilities using (1)-(7).

2 Preliminaries

We first make a brief introduction of the relevant knowledge of singular Pseudo-symplectic space, and the specific content can be found in [14]. Let $\mathbb{F}_q$ be a finite field. $n = 2\nu+\delta+l (\delta = 1, 2)$, let $S_{\delta,l} = \begin{pmatrix} S_\delta & \\ & 0^{(l)} \end{pmatrix}$, where S_δ is a $(2\nu+\delta)\times(2\nu+\delta)$ non-alternate symmetric matrix:

$$S_1 = \begin{pmatrix} 0 & I^{(\nu)} & \\ I^{(\nu)} & 0 & \\ & & 1 \end{pmatrix},$$

$$S_2 = \begin{pmatrix} 0 & I^{(\nu)} & & \\ I^{(\nu)} & 0 & & \\ & & 0 & 1 \\ & & 1 & 1 \end{pmatrix}.$$

The set of all $(2\nu+\delta+l)\times(2\nu+\delta+l)$ nonsingular matrices T satisfying $TS_{\delta,l}{}^tT = S_{\delta,l}$ forms a group with respect to matrix multiplication, called the singular pseudo-sympletic group of degree $2\nu+\delta+l$ and rank $2\nu+\delta$ over $\mathbb{F}_q$ and denoted by $Ps_{2\nu+\delta+l,2\nu+\delta}(\mathbb{F}_q)$. Let $\mathbb{F}_q^{(2\nu+\delta+l)}$ be $(2\nu+\delta+l)$-dimensional vector space over $\mathbb{F}_q$. $Ps_{2\nu+\delta+l,2\nu+\delta}(\mathbb{F}_q)$ has an action on the vector space $\mathbb{F}_q^{(2\nu+\delta+l)}$ defined as follows:

$$\mathbb{F}_q^{(2\nu+\delta+l)} \times Ps_{2\nu+\delta+l,2\nu+\delta}(\mathbb{F}_q) \to \mathbb{F}_q^{(2\nu+\delta+l)}$$
$$((x_1, x_2, \cdots, x_{2\nu+\delta+l}), T) \mapsto (x_1, x_2, \cdots, x_{2\nu+\delta+l})T.$$

The vector space $\mathbb{F}_q^{(2\nu+\delta+l)}$ together with this action is called the singular pseudo-sympletic space of dimension $2\nu+\delta+l$ over $\mathbb{F}_q$. An m-dimensional subspace P of $\mathbb{F}_q^{(2\nu+\delta+l)}$ is said to be of type $(m, 2s+\tau, s, \varepsilon)$, where $\tau = 0, 1$, or 2 and $\varepsilon = 0$ or 1, if $PS_{\delta,l}{}^tP$ cogredient to $M(m, 2s+\tau, s)$ and P does not or does contain a vector of the form

$$\begin{cases} (\underbrace{0, 0, \ldots, 0}_{2\nu}, 1, x_{2\nu+2}, \ldots, x_{2\nu+1+l}), & \delta = 1 \\ (\underbrace{0, 0, \ldots, 0}_{2\nu}, 1, x_{2\nu+3}, \ldots, x_{2\nu+2+l}), & \delta = 2 \end{cases}$$

corresponding to the case $\varepsilon = 0$ or 1, respectively. Denote the set of subspaces of type $(m, 2s+\tau, s, \varepsilon)$ in $\mathbb{F}_q^{(2\nu+\delta+l)}$ by $\mathcal{M}(m, 2s+\tau, s, \varepsilon; 2\nu+\delta+l, 2\nu+\delta)$ and let

$$N(m, 2s+\tau, s, \varepsilon; 2\nu+\delta+l, 2\nu+\delta)$$
$$= |\mathcal{M}(m, 2s+\tau, s, \varepsilon; 2\nu+\delta+l, 2\nu+\delta)|.$$

Let E be the subspace of $\mathbb{F}_q^{(2\nu+\delta+l)}$ generated by $e_{2\nu+\delta+1}, \ldots, e_{2\nu+\delta+l}$. Then $\dim E = l$. An m-dimensional subspace P of $\mathbb{F}_q^{(2\nu+\delta+l)}$ is called a subspace of type $(m, 2s+\tau, s, \varepsilon, k)$ if
(1) P is a subspace of type $(m, 2s+\tau, s, \varepsilon)$, and
(2) $\dim(P \cap E) = k$.

Denote by $\mathcal{M}(m, 2s+\tau, s, \varepsilon, k; 2\nu+\delta+l, 2\nu+\delta)$ the set of subspaces of type $(m, 2s+\tau, s, \varepsilon, k)$ in $\mathbb{F}_q^{(2\nu+\delta+l)}$ and let

$$N(m, 2s+\tau, s, \varepsilon, k; 2\nu+\delta+l, 2\nu+\delta)$$
$$= |\mathcal{M}(m, 2s+\tau, s, \varepsilon, k; 2\nu+\delta+l, 2\nu+\delta)|.$$

Theorem 2 *$\mathcal{M}(m, 2s+\tau, s, \varepsilon, k; 2\nu+\delta+l, 2\nu+\delta)$ is non-empty if and only if*

$$\left.\begin{array}{l} (\tau,\varepsilon) = \begin{cases} (0,0), (1,0), (1,1), \text{ or } (2,0), & \text{when } \delta = 1, \\ (0,0), (0,1), (1,0), (2,0), \text{ or } (2,1), & \text{when } \delta = 2, \end{cases} \\ k \le l, \\ 2s + \max\{\tau,\varepsilon\} \le m-k \le \nu+s+[(\tau+\delta-1)/2]+\varepsilon \end{array}\right\}$$

hold simultaneously, and if and only if

$$\left.\begin{array}{l} (\tau,\varepsilon) = \begin{cases} (0,0), (1,0), (1,1), \text{ or } (2,0), & \text{when } \delta = 1, \\ (0,0), (0,1), (1,0), (2,0), \text{ or } (2,1), & \text{when } \delta = 2, \end{cases} \\ \max\{0, m-\nu-s-[(\tau+\delta-1)/2]-\varepsilon\} \le k \le \min\{l, m-2s-\max\{\tau,\varepsilon\}\} \end{array}\right\}$$

hold simultaneously.

3 Construction

Let $n \ge 1$ be an integer and $\mathbb{F}_q^{(n+1)}$ be the $(n+1)$-dimensional row vector space over $\mathbb{F}_q$. Let $n = 2\nu+2+l, 1 \le r < t < \nu$, $U = < e_1, e_2, \cdots, e_r, e_{2\nu+1}, e_{2\nu+3} >$ is a fixed subspace of type $(r+2, 0, 0, 1, 1)$, and its matrix representation is

$$U = \begin{array}{cc} \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} & \begin{array}{c} r \\ 1 \\ 1 \end{array} \\ \begin{array}{cccccccc} r & \nu-r & r & \nu-r & 1 & 1 & 1 & l-1 \end{array} & \end{array},$$

then $U^\perp$ is a subspace of type $(2\nu-r+1+l, 2(\nu-r), \nu-r, 1, l)$, and $U^\perp$ has the following matrix representation:

$$U^\perp = \begin{array}{c} \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I^{(\nu-r)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(\nu-r)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(l)} \end{pmatrix} \\ \begin{array}{ccccccc} r & \nu-r & r & \nu-r & 1 & 1 & l \end{array} \end{array}.$$

Let $\mathcal{S}, \mathcal{E_T}, \mathcal{E_R}, \mathcal{E_A}, \mathcal{M}$ be the set of source states, the set of transmitters' keys, the set of receivers' keys, the set of arbiter's keys and the set of messages, respectively. Then the construction of A^3-code is as follows:

$\mathcal{S} = \{$subspaces of type $(t+k, 0, 0, 1, k)$ containing U and contained in $U^{\perp}\}$

$\mathcal{E_T} = \{$subspaces of type $(2r+2, 2r, r, 1, 1)$ containing $U\}$

$\mathcal{E_R} = \{$ subspaces of type $(2r+1, 2(r-1), r-1, 1, 1)$ containing $U\}$

$\mathcal{E_A} = \{$subspaces of type $(2r+1, 2(r-1), r-1, 1, 1)$ containing $U\}$

$\mathcal{M} = \{$subspaces of type $(t+r+k, 2r, r, 1, k)$ containing $U\}$

Define the encoding function:

$$f : \mathcal{S} \times \mathcal{E_T} \to \mathcal{M}, \forall s \in \mathcal{S}, e_t \in \mathcal{E_T}, f(s, e_t) = s \cup e_t$$

Define the decoding function:

$$g : \mathcal{M} \times \mathcal{E_R} \to \mathcal{S} \cup \{\text{fraud}\}, \forall m \in \mathcal{M}, e_r \in \mathcal{E_R},$$

$$g(m, e_r) = \begin{cases} m \cap U^{\perp}\,; & e_r \subseteq m \\ \text{fraud}\,; & e_r \nsubseteq m \end{cases}$$

The triple (e_t, e_r, e_a) is valid if and only if e_r, e_a are contained in e_t. As a general rule, the Key Distribution Center (KDC) should choose different subspaces of type $(2r+1, 2(r-1), r-1, 1, 1)$ in the stage of key generation and distribution to be the receiver's key and the arbiter's key, respectively. That is $e_a \neq e_r$ in a communication.

Lemma 3 *The above construction is reasonable,*

(1) $\forall s \in \mathcal{S}, e_t \in \mathcal{E_T}, s \cup e_t = m \in \mathcal{M}$;

(2) $\forall m \in \mathcal{M}, s = m \cap U^{\perp}$ is the unique source state contained in the message m, and there is $e_t \in \mathcal{E_T}$, such that m=$s \cup e_t$.

Proof. (1) $\forall s \in \mathcal{S}, e_t \in \mathcal{E_T}$, by the definition as above, s and e_t has the following form of matrix representation, respectively,

$$s = \begin{pmatrix} U \\ Q \end{pmatrix} \begin{matrix} r+2 \\ t+k-r-2 \end{matrix}, \quad e_t = \begin{pmatrix} U \\ V \end{pmatrix} \begin{matrix} r+2 \\ r \end{matrix}.$$

s and e_t satisfies the following condition, respectively,

$$\begin{pmatrix} U \\ Q \end{pmatrix} S_{2,l}{}^t \begin{pmatrix} U \\ Q \end{pmatrix} = \begin{pmatrix} US_{2,l}{}^tU & US_{2,l}{}^tQ \\ QS_{2,l}{}^tU & QS_{2,l}{}^tQ \end{pmatrix} = \begin{pmatrix} 0^{(r)} & 0 & 0 \\ 0 & 0^{(2)} & 0 \\ 0 & 0 & 0^{(t+k-r-2)} \end{pmatrix},$$

$$\begin{pmatrix} U \\ V \end{pmatrix} S_{2,l}{}^t \begin{pmatrix} U \\ V \end{pmatrix} = \begin{pmatrix} US_{2,l}{}^tU & US_{2,l}{}^tV \\ VS_{2,l}{}^tU & VS_{2,l}{}^tV \end{pmatrix} \sim \begin{pmatrix} 0^{(r)} & 0 & I^{(r)} \\ 0 & 0^{(2)} & 0 \\ I^{(r)} & 0 & 0 \end{pmatrix}.$$

Clearly, $Q \cap V = \{0\}$, that is

$$m = s \cup e_t = \begin{pmatrix} U \\ V \\ Q \end{pmatrix} \begin{matrix} r+2 \\ r \\ t+k-r-2 \end{matrix},$$

$$\begin{pmatrix} U \\ V \\ Q \end{pmatrix} S_{2,l}{}^t \begin{pmatrix} U \\ V \\ Q \end{pmatrix} = \begin{pmatrix} US_{2,l}{}^tU & US_{2,l}{}^tV & US_{2,l}{}^tQ \\ VS_{2,l}{}^tU & VS_{2,l}{}^tV & VS_{2,l}{}^tQ \\ QS_{2,l}{}^tU & QS_{2,l}{}^tV & QS_{2,l}{}^tQ \end{pmatrix} \sim \begin{pmatrix} 0 & I^{(r)} & 0 \\ I^{(r)} & 0 & 0 \\ 0 & 0 & 0^{(t+k-r)} \end{pmatrix}.$$

For $e_{2\nu+1} \in U \subset m, \dim(m \cap E) = k$, so m is a subspace of type $(t+r+k, 2r, r, 1, k)$, that is $m \in \mathcal{M}$.

(2) If $m \in \mathcal{M}$, then m is the subspace of type $(t+r+k, 2r, r, 1, k)$ containing U. Assume that

$$m = \begin{pmatrix} U \\ V \\ Q \end{pmatrix} \begin{matrix} r+2 \\ r \\ t+k-r-2 \end{matrix},$$

and

$$\begin{pmatrix} U \\ V \\ Q \end{pmatrix} S_{2,l}{}^t \begin{pmatrix} U \\ V \\ Q \end{pmatrix} \sim \begin{pmatrix} 0 & I^{(r)} & & \\ I^{(r)} & 0 & & \\ & & 0^{(2)} & \\ & & & 0^{(t+k-r-2)} \end{pmatrix},$$

where $\dim(Q \cap E) = k-1$.

Let $s = \begin{pmatrix} U \\ Q \end{pmatrix}$, then $U \subset s \subset U^{\perp}$, and s is a subspace of type $(t+k, 0, 0, 1, k)$, so $s \in \mathcal{S}$. $\forall v \in V, vS_{2,l}{}^tv \neq 0$, thus $v \notin U^{\perp}$, that is, $V \cap U^{\perp} = \{0\}$, then $s = m \cap U^{\perp}$.

Let $e_t = \begin{pmatrix} U \\ V \end{pmatrix}$, then e_t is a subspace of type $(2r+2, 2r, r, 1, 1)$, so e_t is a transmitter's key and $e_t + s = m$. Assume that s' is another source state contained in m, then $U \subset s' \subset U^{\perp}$, so $s' \subset m \cap U^{\perp} = s$. Since dim$s'$ =dim$s$, we have $s = s'$. That is, s is the unique source state contained in m.

By the discussions, the code constructed above is an A^3-code. $\square$

Lemma 4 *The number of source states of the constructed A^3-code is*

$$|\mathcal{S}| = q^{(l-k)(t-r-1)} N(t-r-1, 0; 2(\nu-r)) \cdot N(k-1, l-1).$$

Proof. According to the definition of source state, we can know that the source state s has the following matrix representation of the form

$$s = \begin{array}{cc} \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & 0 & R_4 & 0 & 0 & 0 & 0 & R_9 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \end{pmatrix} & \begin{matrix} r \\ t-r-1 \\ 1 \\ 1 \\ k-1 \end{matrix} \\ \begin{matrix} r & \nu-r & r & \nu-r & 1 & 1 & 1 & k-1 & l-k \end{matrix} & \end{array},$$

where (R_2, R_4) is a subspace of type $(t-r-1, 0)$ in $\mathbb{F}_q^{(2(\nu-r))}$, R_9 is random, so

$$|\mathcal{S}| = q^{(l-k)(t-r-1)} N(t-r-1, 0; 2(\nu-r)) \cdot N(k-1, l-1).$$

□

Lemma 5 *The number of transmitters' keys of the constructed A^3-code is*

$$|\mathcal{E}_{\mathcal{T}}| = q^{r(2(\nu-r)+l-1)}.$$

Proof. According to the definition of transmitter's key, we can know that e_t has the following matrix representation of the form

$$e_t = \begin{array}{cc} \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & I^{(r)} & R_4 & 0 & 0 & 0 & R_8 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} & \begin{matrix} r \\ r \\ 1 \\ 1 \end{matrix} \\ \begin{matrix} r & \nu-r & r & \nu-r & 1 & 1 & 1 & l-1 \end{matrix} & \end{array},$$

where R_2, R_4 and R_8 are random, so the number of transmitters' keys is

$$|\mathcal{E}_{\mathcal{T}}| = q^{r(2(\nu-r)+l-1)}.$$

□

Lemma 6 *The number of receivers' keys of the constructed A^3-code is*

$$|\mathcal{E}_{\mathcal{R}}| = q^{(r-1)(2(\nu-r)+l-1)} \cdot N(r-1, r).$$

Proof. According to the definition of receiver's key, we can know that e_r has the following matrix representation of the form

$$e_r = \begin{array}{cc} \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & R_3 & R_4 & 0 & 0 & 0 & R_8 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} & \begin{matrix} r \\ r-1 \\ 1 \\ 1 \end{matrix} \\ \begin{matrix} r & \nu-r & r & \nu-r & 1 & 1 & 1 & l-1 \end{matrix} & \end{array},$$

where R_3 is a $(r-1)$-dimensional vector subspace in the r-dimensional vector subspace, R_2, R_4 and R_8 are random, so the number of receivers' keys is

$$|\mathcal{E}_{\mathcal{R}}| = q^{(r-1)(2(\nu-r)+l-1)} \cdot N(r-1, r).$$

□

Lemma 7 *The number of arbiters' keys of the constructed A^3-code is*

$$|\mathcal{E}_{\mathcal{A}}| = q^{(r-1)(2(\nu-r)+l-1)} \cdot N(r-1, r).$$

Proof. By the construction of A^3-code, we can know

$$|\mathcal{E}_{\mathcal{A}}| = |\mathcal{E}_{\mathcal{R}}| = q^{(r-1)(2(\nu-r)+l-1)} \cdot N(r-1, r).$$

□

Lemma 8 *For a given $m \in \mathcal{M}$, let $e_t(m)$ and $e_r(m)$ be the transmitters' and receivers' keys contained in m, respectively. Let $\mathcal{E}_{\mathcal{T}}(m)$ and $\mathcal{E}_{\mathcal{R}}(m)$ be the set of transmitters' keys and receivers' keys contained in the given message m, respectively. Then*

$$|\mathcal{E}_{\mathcal{T}}(m)| = q^{r(t+k-r-2)},$$

$$|\mathcal{E}_{\mathcal{R}}(m)| = q^{(r-1)(t+k-r-2)} \cdot N(r-1, r).$$

Proof. Let m be a message, a subspace of type $(t+r+k, 2r, r, 1, k)$ and $U \subset m$, then we can know m has the following matrix representation of the form

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

The transmitter's key is a subspace of type $(2r+2, 2r, r, 1, 1)$ containing U, then the transmitter's key contained in m has the following form

$$e_t(m)=\begin{array}{cc}\begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & R_2 & 0 & I^{(r)} & 0 & 0 & 0 & 0 & 0 & R_{10} & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} & \begin{matrix} r\\ r\\ 1\\ 1\end{matrix}\\ \begin{matrix} r & t-r-1 & \nu-t+1 & r & t-r-1 & \nu-t+1 & 1 & 1 & 1 & k-1 & l-k\end{matrix} & \end{array}.$$

When the message m is fixed, then R_2 and R_{10} are random, so we have

$$|\mathcal{E}_{\mathcal{T}}(m)|=q^{r(t+k-r-2)}.$$

The receiver's key is a subspace of type $(2r+1,2(r-1),r-1,1,1)$ containing U, then the receiver's key contained in m has the following form

$$e_r(m)=\begin{array}{cc}\begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & R'_2 & 0 & R'_4 & 0 & 0 & 0 & 0 & 0 & R'_{10} & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} & \begin{matrix} r\\ r\\ 1\\ 1\end{matrix}\\ \begin{matrix} r & t-r-1 & \nu-t+1 & r & t-r-1 & \nu-t+1 & 1 & 1 & 1 & k-1 & l-k\end{matrix} & \end{array}.$$

When the message m is fixed, R'_4 is an $(r-1)$-dimensional subspace contained in the r-dimensional subspace, R'_2 and R'_{10} are random, so

$$|\mathcal{E}_{\mathcal{R}}(m)|=q^{(r-1)(t+k-r-2)}\cdot N(r-1,r).$$

□

Lemma 9 *The number of messages in the constructed* A^3*-code is*

$$|\mathcal{M}|=q^{(t-1)(l-k+r)+r(2\nu-r)}\cdot N(t-r-1,0;2(\nu-r))\cdot N(k-1,l-1).$$

Proof. $\forall m\in\mathcal{M}$, there is an unique source state $s\in\mathcal{S}$ and some $e_t\in\mathcal{E}_{\mathcal{T}}$, such that m=$s\cup e_t$, where the number of e_t satisfying the previous condition is $|\mathcal{E}_{\mathcal{T}}(m)|$. Thus,

$$\begin{aligned}|\mathcal{M}|&=\frac{|\mathcal{S}|\cdot|\mathcal{E}_{\mathcal{T}}|}{|\mathcal{E}_{\mathcal{T}}(m)|}\\ &=\frac{q^{(l-k)(t-r-1)}N(t-r-1,0;2(\nu-r))\cdot N(k-1,l-1)\cdot q^{r(2(\nu-r)+l-1)}}{q^{r(t+k-r-2)}}\\ &=q^{(t-1)(l-k+r)+r(2\nu-r)}\cdot N(t-r-1,0;2(\nu-r))\cdot N(k-1,l-1).\end{aligned}$$

□

Lemma 10 $\forall e_t\in\mathcal{E}_{\mathcal{T}}$, *let* $\mathcal{E}_{\mathcal{R}}(e_t)$ *be the receivers' keys contained in* e_t, *then*

$$|\mathcal{E}_{\mathcal{R}}(e_t)|=q^{2(r-1)}\cdot N(r-1,r).$$

Proof. $\forall e_t\in\mathcal{E}_{\mathcal{T}}$, e_t is a subspace of type $(2r+2,2r,r,1,1)$ containing U, then we can assume

$$e_t=\begin{array}{cc}\begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & I^{(r)} & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\end{pmatrix} & \begin{matrix} r\\ r\\ 1\\ 1\end{matrix}\\ \begin{matrix} r & \nu-r & r & \nu-r & 1 & 1 & 1 & l-1\end{matrix} & \end{array}.$$

The receiver's key e_r is a subspace of type $(2r+1,2(r-1),r-1,1,1)$ containing U. If $e_r\subset e_t$, then we can assume

$$e_r(e_t)=\begin{array}{cc}\begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & R_3 & 0 & R_5 & 0 & R_7 & 0\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\end{pmatrix} & \begin{matrix} r\\ r-1\\ 1\\ 1\end{matrix}\\ \begin{matrix} r & \nu-r & r & \nu-r & 1 & 1 & 1 & l-1\end{matrix} & \end{array}$$

where R_3 is a $(r-1)$-dimensional vector subspace in the r-dimensional vector subspace, R_5 and R_7 are random, so

$$|\mathcal{E}_{\mathcal{R}}(e_t)|=q^{2(r-1)}\cdot N(r-1,r).$$

□

Lemma 11 *Assume that* m_1 *and* m_2 *are two distinct messages which commonly contain a transmitter's key* e_t. s_1 *and* s_2 *are two source states contained in* m_1 *and* m_2 *, respectively. Let* $s_0=s_1\cap s_2$, $\dim s_0=k_0$, *then* $r+2\le k_0\le t+k-1$, *and the number of receivers' keys contained in* $m_1\cap m_2$ *is*

$$|\mathcal{E}_{\mathcal{R}}(m_1)\cap\mathcal{E}_{\mathcal{R}}(m_2)|=q^{(r-1)(k_0-r-2)}\cdot N(r-1,r).$$

Proof. By the definition of the A^3-code, we have $U\subset m_1\cap m_2$, thus $r+2\le k_0$. Clearly, $s_1\ne s_2$. For $\dim s_1=\dim s_2=t+k$, so $k_0\le t+k-1$. Let s'_i be the complement space of s_i in s_0, that is, $s_i=s_0+s'_i(i=1,2)$. $m_i=s_i+e_t=s_0+s'_i+e_t$ and $s_i=m_i\cap U^{\perp}$, then $s_0=(m_1\cap U^{\perp})\cap(m_2\cap U^{\perp})=m_1\cap m_2\cap U^{\perp}=s_1\cap m_2=s_2\cap m_1$, $m_1\cap m_2=(s_0+e_t+s'_i)\cap m_2$. $s_0+e_t\subset m_2$, thus $m_1\cap m_2=(s_0+e_t)+(s'_1\cap m_2)$. $s'_1\cap m_2\subset s_1\cap m_2=s_0$, so we have $m_1\cap m_2=s_0+e_t$ and $\dim(m_1\cap m_2)=k_0+r$. Assume that

$$m_i=\begin{array}{cc}\begin{pmatrix} I & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & A_{i2} & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & I & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & A_{i8}\end{pmatrix} & \begin{matrix} r\\ t-r-1\\ r\\ 1\\ 1\\ k-1\end{matrix}\\ \begin{matrix} r & \nu-r & r & \nu-r & 1 & 1 & 1 & l-1\end{matrix} & \end{array},$$

where $i = 1, 2$, then $m_1 \cap m_2$ has the following matrix representation of the form

$$m_1 \cap m_2 = \begin{array}{c} \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & B_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(r)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & B_8 \end{pmatrix} \begin{array}{l} r \\ \alpha \\ r \\ 1 \\ 1 \\ \beta \end{array} \\ \begin{array}{cccccccc} r & \nu-r & r & \nu-r & 1 & 1 & 1 & l-1 \end{array} \end{array},$$

where $\alpha + \beta = k_0 - r - 2$.

As for $\forall e_r \subset m_1 \cap m_2$, e_r has the following matrix representation of the form

$$e_r = \begin{array}{c} \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & R_3 & 0 & 0 & 0 & 0 & R_8 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{array}{l} r \\ r-1 \\ 1 \\ 1 \end{array} \\ \begin{array}{cccccccc} r & \nu-r & r & \nu-r & 1 & 1 & 1 & l-1 \end{array} \end{array},$$

where R_3 is a $(r-1)$-dimensional vector subspace in the r-dimensional vector subspace, R_2 and R_8 are decided by B_2 and B_8, respectively. Thus, the number of receivers' keys contained in $m_1 \cap m_2$ is

$$\begin{aligned} |\mathcal{E}_{\mathcal{R}}(m_1) \cap \mathcal{E}_{\mathcal{R}}(m_2)| &= q^{(r-1)(\alpha+\beta)} \cdot N(r-1, r) \\ &= q^{(r-1)(k_0-r-2)} \cdot N(r-1, r). \end{aligned}$$

□

Lemma 12 *$\forall e_r \in \mathcal{E}_{\mathcal{R}}$, let $e_a(e_r)$ be the arbiter's keys incident with e_r. e_r and e_a are said to be incident with each other, if they are contained in the same subspace of type $(2r+2, 2r, r, 1, 1)$. Then we can know e_r and e_a are incident with each other if and only if $e_r + e_a$ is a transmitter's key.*

Proof. If $e_r + e_a$ is a transmitter's key, clearly, $e_r + e_a$ is a subspace of type $(2r+2, 2r, r, 1, 1)$ containing e_r and e_a. Conversely, if e_r and e_a are incident with each other, by the definition, there exists a subspace X of type $(2r+2, 2r, r, 1, 1)$, such that $e_r \subset X$ and $e_a \subset X$, then $\dim(e_r + e_a) \leq 2r + 2$. For $\dim e_r = \dim e_a = 2r + 1$ and $e_r \neq e_a$, then we must have $\dim(e_r + e_a) = 2r + 2$, otherwise, $e_r = e_a$. $e_r + e_a \subset X$ and $\dim X = \dim(e_r + e_a)$, so $X = e_r + e_a$. $e_r + e_a$ is a subspace of type $(2r+2, 2r, r, 1, 1)$, and $U \subset e_r + e_a$, thus $e_r + e_a$ is a transmitter's key. □

Theorem 13 *let $\mathcal{E}_{\mathcal{A}}(e_r)$ be the set of arbiter's keys incident with the given receiver's key e_r, then*

$$|\mathcal{E}_{\mathcal{A}}(e_r)| = q^{(2\nu-r+l-3)} \cdot N(r-2, r-1).$$

Proof. $\dim e_r = \dim e_a = 2r + 1$, by the Lemma 12, if e_a and e_r are incident with each other, then $\dim(e_r + e_a) = 2r + 2$. By the dimension formula, we have $\dim(e_r \cap e_a) = 2r$. $\forall e_r \in \mathcal{E}_{\mathcal{R}}$, without loss of generality we can assume that e_r has the following matrix representation of the form

$$e_r = \begin{array}{c} \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I^{(r-1)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{array}{l} r \\ r-1 \\ 1 \\ 1 \end{array} \\ \begin{array}{ccccccccc} r & \nu-r & r-1 & 1 & \nu-r & 1 & 1 & 1 & l-1 \end{array} \end{array}.$$

Then we can assume

$$e_r \cap e_a = \begin{array}{c} \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R'_{31} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{array}{l} r \\ r-2 \\ 1 \\ 1 \end{array} \\ \begin{array}{ccccccccc} r & \nu-r & r-1 & 1 & \nu-r & 1 & 1 & 1 & l-1 \end{array} \end{array},$$

where R'_{31} is a $(r-2)$-dimensional vector subspace in the $(r-1)$-dimensional vector subspace. Assume that arbiter's key e_a incident with e_r has the following matrix representation of the form

$$e_a = \begin{array}{c} \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R'_{31} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & R_{31} & R_{32} & R_4 & 0 & 0 & 0 & R_8 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{array}{l} r \\ r-2 \\ 1 \\ 1 \\ 1 \end{array} \\ \begin{array}{ccccccccc} r & \nu-r & r-1 & 1 & \nu-r & 1 & 1 & 1 & l-1 \end{array} \end{array}.$$

e_a is a subspace of type $(2r+1, 2(r-1), r-1, 1, 1)$, R'_{31} is a $(r-2)$-dimensional vector subspace in the $(r-1)$-dimensional vector subspace. Let R_{32} be 1, R_{31} is generated by the vectors in R'_{31}. R_2, R_4 and R_8 are random. Thus

$$\begin{aligned} |\mathcal{E}_{\mathcal{A}}(e_r)| &= q^{(r-2)} \cdot q^{2(\nu-r)+(l-1)} \cdot N(r-2, r-1) \\ &= q^{(2\nu-r+l-3)} \cdot N(r-2, r-1). \end{aligned}$$

□

Theorem 14 *Let m be the message containing the given receiver's key e_r. Let $\mathcal{E}_{\mathcal{A}}(m) \cap \mathcal{E}_{\mathcal{A}}(e_r)$ be the set of arbiter's keys contained in m and incident with e_r. Then*

$$|\mathcal{E}_{\mathcal{A}}(m) \cap \mathcal{E}_{\mathcal{A}}(e_r)| = q^{(t-3)} \cdot N(r-2, r-1).$$

Proof. Given the message m, assume that m has the following matrix representation of the form

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

Assume that the receiver's key contained in m has the following form

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

If e_a is the arbiter's key contained in m and incident with $e_r(m)$, then we can assume

$$e_r\cap e_a=\begin{array}{cc}\begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & R'_{31} & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} & \begin{array}{c} r\\ r-2\\ 1\\ 1 \end{array}\\ \begin{array}{ccccccccc} r & \nu-r & r-1 & 1 & \nu-r & 1 & 1 & 1 & l-1 \end{array} & \end{array},$$

where R'_{31} is a $(r-2)$-dimensional vector subspace in the $(r-1)$-dimensional vector subspace.

For $e_a \subset m$, we can assume e_a has the following matrix representation of the form

$$e_a=\begin{array}{cc}\begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & R'_{31} & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & R_2 & 0 & R_{31} & R_{32} & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} & \begin{array}{c} r\\ r-2\\ 1\\ 1\\ 1 \end{array}\\ \begin{array}{ccccccccccc} r & t-r-1 & \nu-t+1 & r-1 & 1 & t-r-1 & \nu-t+1 & 1 & 1 & 1 & l-1 \end{array} & \end{array}.$$

e_a is a subspace of type $(2r+1, 2(r-1), r-1, 1, 1)$ containing U, R'_{31} is a $(r-2)$-dimensional vector subspace in the $(r-1)$-dimensional vector subspace. Let R_{32} be 1, R_{31} is generated by the vectors in R'_{31}, R_2 is random. Thus

$$\begin{aligned}|\mathcal{E}_{\mathcal{A}}(m)\cap\mathcal{E}_{\mathcal{A}}(e_r)| =& q^{(r-2)}q^{(t-r-1)}N(r-2, r-1)\\ =& q^{(t-3)}\cdot N(r-2, r-1).\end{aligned}$$

□

Theorem 15 *Let m_1 and m_2 be two different messages containing receiver's key e_r. Let $\mathcal{E}_{\mathcal{A}}(m_1)\cap\mathcal{E}_{\mathcal{A}}(m_2)\cap\mathcal{E}_{\mathcal{A}}(e_r)$ be the set of arbiter's keys contained in m_1 and m_2 and incident with e_r. Let $m_1\cap m_2$ be as large as possible, then*

$$|\mathcal{E}_{\mathcal{A}}(m_1)\cap\mathcal{E}_{\mathcal{A}}(m_2)\cap\mathcal{E}_{\mathcal{A}}(e_r)| = q^{(t-4)}\cdot N(r-2, r-1).$$

Proof. If the message m has the following matrix representation of the form

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

there aren't any transmitters' keys, receivers' keys and arbiter's keys contained in m. Thus m is a invalid message. When $m_1\cap m_2$ is as large as possible, we can assume that

$$m_1\cap m_2=\begin{array}{c}\begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & I^{(t-r-2)} & 0 & & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & I^{(r-1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I^{(k-1)} & 0 \end{pmatrix}\\ \begin{array}{cccccccccccc} r & t-r-2 & \nu-t+2 & r-1 & 1 & t-r-2 & \nu-t+2 & 1 & 1 & 1 & k-1 & l-k \end{array}\end{array}.$$

Assume the receiver's key contained in m_1 and m_2 has the following form

$$e_r(m_1\cap m_2)=\begin{array}{c}\begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & I^{(r-1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}\\ \begin{array}{ccccccccccc} r & t-r-2 & \nu-t+2 & r-1 & 1 & t-r-2 & \nu-t+2 & 1 & 1 & 1 & l-1 \end{array}\end{array}.$$

If e_a is the arbiter's key contained in m_1 and m_2, and incident with $e_r(m_1\cap m_2)$, then the intersection of e_r and e_a contained in $m_1\cap m_2$ has the following matrix representation of the form

$$e_r \cap e_a = \begin{array}{cc} \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & R'_{31} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} & \begin{matrix} r \\ r-2 \\ 1 \\ 1 \end{matrix} \\ \begin{matrix} r & t-r-2 & \nu-t+2 & r-1 & 1 & t-r-2 & \nu-t+2 & 1 & 1 & 1 & l-1 \end{matrix} & \end{array},$$

where R'_{31} is a $(r-2)$-dimensional vector subspace in the $(r-1)$-dimensional vector subspace. Then we can further assume that the arbiter's key e_a has the following form

$$e_a = \begin{array}{cc} \begin{pmatrix} I^{(r)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & R'_{31} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R_2 & 0 & R_{31} & R_{32} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} & \begin{matrix} r \\ r-2 \\ 1 \\ 1 \\ 1 \end{matrix} \\ \begin{matrix} r & t-r-2 & \nu-t+2 & r-1 & 1 & t-r-2 & \nu-t+2 & 1 & 1 & 1 & l-1 \end{matrix} & \end{array}.$$

e_a is a subspace of type $(2r+1, 2(r-1), r-1, 1, 1)$ containing U and $e_r + e_a$ is a transmitter's key. R'_{31} is a $(r-2)$-dimensional vector subspace in the $(r-1)$-dimensional vector subspace. Let R_{32} be 1, R_{31} is generated by the vectors in R'_{31}, R_2 is random. Thus, when $m_1 \cap m_2$ is as large as possible, we have

$$\begin{aligned} &|\mathcal{E}_{\mathcal{A}}(m_1) \cap \mathcal{E}_{\mathcal{A}}(m_2) \cap \mathcal{E}_{\mathcal{A}}(e_r)| \\ =& q^{(r-2)} \cdot q^{(t-r-2)} \cdot N(r-2, r-1) \\ =& q^{(t-4)} \cdot N(r-2, r-1). \end{aligned}$$

□

Theorem 16 *Assume that the probability distribution of participants key set and source states set is uniform, the successful attacks probability of A^3-code in the construction program are as follows:*

$$\begin{aligned} P_I &= \frac{1}{q^{(r-1)(2\nu-r-m-k+l+1)}}, \\ P_S &= \frac{1}{q^{(r-1)}}, \\ P_T &= \frac{1}{q^{2(r-1)} \cdot N(r-1, r)}, \\ P_{A_0} = P_{R_0} &= \frac{1}{q^{2\nu-r-t+l}}, \\ P_{A_1} = P_{R_1} &= \frac{1}{q}. \end{aligned}$$

Proof. (1) By the definition 1, Lemma 6 and Lemma 8, we can directly get

$$\begin{aligned} P_I =& \max_m \frac{|\mathcal{E}_{\mathcal{R}}(m)|}{|\mathcal{E}_{\mathcal{R}}|} \\ =& \frac{q^{(r-1)(t+k-r-2)} \cdot N(r-1, r)}{q^{(r-1)(2(\nu-r)+l-1)} \cdot N(r-1, r)} \\ =& \frac{1}{q^{(r-1)(2\nu-r-m-k+l+1)}}. \end{aligned}$$

(2) Suppose that opponent intercept the legitimate message $m (m = s \cup e_t)$ and replace it with m'. The source state s in m is different from s' in m'. For $e_r \subseteq e_t \subseteq m$, so the opponents optimal strategy is to select m' containing the transmitters key e_t, such that $m' = s' \cup e_t$. By the Lemma 11, we have $\dim(s \cap s') = k_0 (r+2 \leq k_0 \leq t+k-1)$. When $e_t \subseteq (m \cap m')$, $|\mathcal{E}_{\mathcal{R}}(m) \cap \mathcal{E}_{\mathcal{R}}(m')| = q^{(r-1)(k_0-r-2)} \cdot N(r-1, r)$. Let $k_0 = t+k-1$, then

$$P_S = \frac{q^{(r-1)(t+k-1-r-2)} \cdot N(r-1, r)}{q^{(r-1)(t+k-r-2)} \cdot N(r-1, r)} = \frac{1}{q^{(r-1)}}.$$

(3) The transmitter sends a message $m \notin \mathcal{M}(e_t)$ to the receiver. The receiver accepts the message if and only if m contains the receiver's key e_r. For $e_r \subseteq e_t$, the transmitter must select m which contain e_r as much as possible and $e_t \nsubseteq m$. Clearly, $\dim(e_t \cap m) \leq 2r+1$. That is, there is at most one $e_r (e_r \subseteq e_t)$ in m, i.e. $|\mathcal{E}_{\mathcal{R}}(m) \cap \mathcal{E}_{\mathcal{R}}(e_t)| \leq 1$. Then

$$\begin{aligned} P_T =& \max_{\substack{m, e_t \\ m \notin \mathcal{M}(e_t)}} \frac{|\mathcal{E}_{\mathcal{R}}(m) \cap \mathcal{E}_{\mathcal{R}}(e_t)|}{|\mathcal{E}_{\mathcal{R}}(e_t)|} \\ =& \frac{1}{q^{2(r-1)} \cdot N(r-1, r)}. \end{aligned}$$

(4) The receiver claims to have received a message $m (e_r \subseteq m)$, he succeeds if $e_a \subseteq m$. By the Theorem 13 and Theorem 14, we have

$$\begin{aligned} P_{R_0} =& \max_{m, e_r} \frac{|\mathcal{E}_{\mathcal{A}}(m) \cap \mathcal{E}_{\mathcal{A}}(e_r)|}{|\mathcal{E}_{\mathcal{A}}(e_r)|} \\ =& \frac{q^{(t-3)} \cdot N(r-2, r-1)}{q^{(2\nu-r+l-3)} \cdot N(r-2, r-1)} \\ =& \frac{1}{q^{2\nu-r-t+l}}. \end{aligned}$$

By the construction of A^3-code and Lemma 3.10, we can know

$$P_{A_0} = P_{R_0} = \frac{1}{q^{2\nu-r-t+l}}.$$

(5) The transmitter sends a legitimate message m to a receiver, but the receiver claims to have received

m'. Let e_r be the receiver's key, then clearly we have $e_r \subseteq m \cap m'$. The attack is successful when the arbiter's key e_a is associated with receiver's key e_r and contained in both m and m'. By the Theorem 14 and Theorem 15, we have

$$P_{R_1} = \max_{\substack{m,m',e_r \\ m \neq m'}} \frac{|\mathcal{E}_{\mathcal{A}}(m) \cap \mathcal{E}_{\mathcal{A}}(m') \cap \mathcal{E}_{\mathcal{A}}(e_r)|}{|\mathcal{E}_{\mathcal{A}}(m) \cap \mathcal{E}_{\mathcal{A}}(e_r)|}$$

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

By the construction of A^3-code and Lemma 12 we can know

$$P_{A_1} = P_{R_1} = \frac{1}{q}.$$

□

Acknowledgements: This work is supported by the National Natural Science Foundation of China under Grant No.61179026 and the Natural Science Foundation of the Education Department of Hebei Province, China No. Z2013085.

References:

[1] C. E. Shannon, Communication Theory of Secrecy Systems, *Bell System Technical Journal*, 28(4), 1949, pp. 656-715.

[2] G. J. Simmons, *Authentication theory/coding theory*, Advances in Cryptology. Springer Berlin Heidelberg, 1985, pp. 411-431.

[3] E. N. Gilbert, F. J. MacWilliams, N. J. Sloane, Codes which detect deception, *Bell System Technical Journal*, 53(3), 1974, pp. 405-424.

[4] Z. Wan, Construction of Cartesian authentication codes from unitary geometry, *Designs, Codes and Cryptography*, 2(4), 1992, pp. 333-356.

[5] G. J. Simmons, *Message Authentication with Arbitration of Transmitter/Receiver Disputes*, Springer Berlin Heidelberg, 1988, pp. 151-165.

[6] G. J. Simmons, A Cartesian product construction for unconditionally secure authentication codes that permit arbitration, *Journal of Cryptology*, 2(2), 1990, pp. 77-104.

[7] T. Johansson, Lower bounds on the probability of deception in authentication with arbitration, *IEEE Transactions on Information Theory*, 40(5), 1994, pp. 1573-1585.

[8] S. Chen, L. An, Two Constructions of Multireceiver Authentication Codes from Singular Symplectic Geometry over Finite Fields, *WSEAS Transactions On Mathematics*, 11(1), 2012, pp. 54C63.

[9] Y. Gao, L. Chang, Two New Constructions of Multi-receiver Authentication Codes from Singular Pseudo-Symplectic Geometry over Finite Fields, *WSEAS Transactions on Mathematics*, 11(1), 2012, pp. 44C53.

[10] E. F. Brickell, D. R. Stinson, *Authentication Codes with Multiple Arbiters*, Springer Berlin Heidelberg, 1988, pp. 51-55.

[11] Y. Desmedt, M. Yung, *Arbitrated unconditionally secure authentication can be unconditionally protected against arbiters attacks*. Springer Berlin Heidelberg, 1991, pp. 177-188.

[12] T. Johansson, Further results on asymmetric authentication schemes, *Information and Computation*, 151(1), 1999, pp. 100-133.

[13] Y. Gao Y, Y. Liu, The construction of A^3-code from projective spaces over finite fields, *WSEAS Transactions on Mathematics*, 12(10), 2013, pp. 1024-1033.

[14] Z. Wan, *Geometry of classical groups over finite fields*, 2nd edition, Science Press, Beijing/New York, 2002.