The Construction of A^3-Code from Projective Spaces over Finite Fields

GAO YOU
Civil Aviation University of China
College of Science
Jinbei Road 2898, 300300, Tianjin
CHINA
gao_you@263.net

LIU YANQIN
Civil Aviation University of China
College of Science
Jinbei Road 2898, 300300, Tianjin
CHINA
yanqinliu1024@163.com

Abstract: A^3-code has a dishonest arbiter who may disturb the communication compared with A^2-code, and the arbiter also has some secret key information used to arbitrate in the case of dispute between the senders and receivers. This paper firstly introduces the model of A^3-code and the seven types of possible cheating attacks as well as their computational formula. And then a construction of A^3-code is presented using the incidence relation of flats from projective spaces over finite fields. The parameters of the code and the probabilities of success in different attacks are also computed, assuming that the probability distributions of source states and participants keys are uniform.

Key–Words: A^3-codes, projective spaces , finite fields.

1 Introduction

The security of information system mainly has two aspects, confidentiality and authentication. Confidentiality is used to prevent enemies decoding the confidential information of the system, which can be solved by the cryptographic techniques. The authentication is to guard against the active attacks, such as falsification or manipulation of information. It plays an important role in protecting all kinds of communication systems in open environment. To promote the authentication technology, Simmons developed the information theory of the authentication system and introduced the concept of authentication channel which is used to deliver messages between two parties, called the *transmitter* and the *receiver*. Simmons firstly introduced the authentication model, A-codes for short, containing a transmitter and a receiver who share a common secret key in [1], to protect the transmitter and the receiver from active deceptions from a third party, often called the *opponent*. The receiver verifies whether the received message is authentic , i.e., originated by the transmitter, while the opponents mainly send the wrong message, tamper with or replace the correct message to make the receiver can't identify the authenticity of the message. The opponents' attacks have two different types, impersonation and substitution. The opponent has not seen any previous communication in impersonation, while in substitution, he has seen one transmitted message. In order to make the receiver identify the authenticity of the message with a high probability, the authentication code was restricted to be Cartesian authentication code, which has no security feature, and only the authentication feature.

The authentication model has been constructed in many ways. Since the transmitter and the receiver share the same key, they must be assumed trustworthy. In practice, this is unnatural in many situations where the transmitter and the receiver cannot trust each other. The transmitter may send a message but then later deny having sent any messages. Or the receiver may claim to have received a message that was never sent by the transmitter. Inspired by these problems, Simmons therefore introduced an extended authentication model, called *the authentication code with arbitration*, or simply A^2-code, in which the transmitter and the receiver do not trust each other [2] . Hence, disputes between them may occur. There is a third participant, called *arbiter*, to solve possible disputes between the transmitter and the receiver. The arbiter is assumed to be honest and have access to all key information. His sole task is to solve possible disputes between the two other participants and he does not take part in any communication activities.

Let $\mathcal{S}, \mathcal{M}, \mathcal{E}_{\mathcal{T}}, \mathcal{E}_{\mathcal{R}}$ be four nonempty finite sets, $f : \mathcal{S} \times \mathcal{E}_{\mathcal{T}} \to \mathcal{M}$ and $g : \mathcal{M} \times \mathcal{E}_{\mathcal{R}} \to \mathcal{S} \cup \{\text{reject}\}$ be two maps. The six-tuple $(\mathcal{S}, \mathcal{M}, \mathcal{E}_{\mathcal{T}}, \mathcal{E}_{\mathcal{R}}, f, g)$ is called an A^2-code, if:

1. The maps $f : \mathcal{S} \times \mathcal{E}_{\mathcal{T}} \to \mathcal{M}$ and $g : \mathcal{M} \times \mathcal{E}_{\mathcal{R}} \to$

$\mathcal{S} \cup \{\text{reject}\}$ are surjective.

2. For any $m \in \mathcal{M}$ and $e_t \in \mathcal{E}_\mathcal{T}$, if there exists an $s \in \mathcal{S}$ 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 $g(m, e_r) = \{\text{reject}\}$.

$\mathcal{S}, \mathcal{M}, \mathcal{E}_\mathcal{T}$, and $\mathcal{E}_\mathcal{R}$ are the set of source states, the set of messages, the set of transmitters' keys and the set of receivers' keys, respectively. f and g are called *encoding function* and *decoding function*, respectively.

The construction of authentication code with arbitration provides protection against deceptions both from an outsider (opponent) who do not have access to any key information and from the insiders (transmitter and receiver) who have some key information. As to the construction of codes for this model, the domestic and foreign scholars have made abundant achievements in authentication theory, such as [3, 4, 5], and Multi-receive Authentication Codes have been constructed in [6, 7].

In an A^2-model, the arbiter is by definition not cheating. This is an assumption which can be removed if we want to study the problem of constructing authentication models where the scenario is even worse than the A^2-model with a cheating arbiter. Brickell and Stinson introduced authentication codes with dishonest arbiter in [8], or A^3-code for short. An A^3-code is an extension of A^2-code in which none of the three participants, transmitter, receiver and arbiter, is assumed trusted.

The research about A^3-code also has a lot of achievements. Thomas Johansson [9] has given some bounds of A^3-code, optimal constructions of A^3-code and also an extended broadcast authentication system with multireceiver where transmitter can collude with unauthorised groups of receivers. Yejing Wang and Rei Safavi-Naini [10] extend the general attack model of A^3-codes by allowing transmitter and receiver not only to attack individually but also collude with the arbiter against the other. They also study the combinatorial structure of optimal A^3-code against collusion attacks and derive information theoretic lower bounds on success probability of various attacks, and combinatorial lower bounds on the size of key spaces. Then [11] provides the bounds on probability of the possible attacks and gives the construction of A^3-code with multiple senders that satisfy the bounds with equality.

The paper is organized as follows. In section 2 we introduce the model of A^3-code and the definition of various attacks. Section 3 gives the relevant knowledge of projective space and some important lemmas and theorems. In section 4 we show a construction of A^3-code from projective spaces over finite fields and the computation of the probabilities of success in different attacks. In section 5 we give a conclusion for this paper.

2 The Model of A^3-code

In an normal A^3-code, there are three participants: a transmitter T, a receiver R and an arbiter A, none of them is assumed trusted. Each participant has some secret key information used to protect himself against attacking in the system. The arbiter may disturb the communication but he will be assumed trusted during his arbitration. There is also an outsider O, who has no key information.

Let $\mathcal{S}, \mathcal{M}$, $\mathcal{E}_\mathcal{T}$, $\mathcal{E}_\mathcal{R}$ and $\mathcal{E}_\mathcal{A}$ be the set of source states, the set of messages, the set of transmitter's, receiver's and arbiter's keys, respectively. Here we denote an A^3-code by $A^3(T, R, A, \mathcal{S}, \mathcal{M}, \mathcal{E}_\mathcal{R}, \mathcal{E}_\mathcal{A})$.

Similar to A^2-code, the transmitter's key $e_t \in \mathcal{E}_\mathcal{T}$ determines the encoding function

$$f : \mathcal{S} \times \mathcal{E}_\mathcal{T} \to \mathcal{M}.$$

The receiver's key $e_r \in \mathcal{E}_\mathcal{R}$ determines the decoding function

$$g : \mathcal{M} \times \mathcal{E}_\mathcal{R} \to \mathcal{S} \cup \{\text{reject}\}$$

If $g(m, e_r) \in \mathcal{S}$, the receiver will accept m as valid.

The arbiter's key $e_a \in \mathcal{E}_\mathcal{A}$ 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.

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

$$\mathcal{E}_\mathcal{T}(e_a) = \{e_t \in \mathcal{E}_\mathcal{T} : f(s, e_t) \in \mathcal{M}(e_a), s \in \mathcal{S}\}.$$

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.

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 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 of 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.

The model has the following steps.

1. **Key Generation and Distribution:** The first step can be performed by an honest and trustworthy authority (such as the Key Distribution Center) who choose the valid triple (e_t, e_r, e_a) and securely deliver the keys $e_t,\ e_r,\ e_a$ to the three participants T, R and A, respectively. A valid triple has the property that if $f(s, e_t) = m$, then $g(m, e_r) = s$ and $m \in \mathcal{M}(e_a)$.

2. **Authentication:** To send a source state $s \in \mathcal{S}$, the transmitter T uses e_t to generate an authentic message $m = f(s, e_t)$, and then sends m to the receiver.

3. **Verification:** The receiver R uses e_r to verify the authenticity of a received message m. If $g(m, e_r) \in \mathcal{S}$, he accepts the message as the authentic, and conversely.

4. **Arbitration:** A dispute may occur between the transmitter and the receiver. In the case of disputes, the arbiter can decide whether the message m is generated by the transmitter T using his key e_a. If $m \in \mathcal{M}(e_a)$, he decide that m is generated by T, and conversely.

In the model of the authentication codes presented in this paper, the arbiter may also attack the system. So there are essentially seven types of possible cheating attacks. The attacks are the following:

1. *Attack I* (Impersonation by the opponent). The opponent places a message m into the channel. He succeeds if this message m is accepted as the 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 for his key e_t to the receiver. The transmitter succeeds if this message m is accepted by the receiver as the authentic.

4. *Attack* R_0 (Impersonation by the receiver). The transmitter doesn'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 for the arbiter's key e_a.

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

6. *Attack* A_0 (Impersonation by the arbiter). This attack is similar to the Attack I. The arbiter places a message m into the channel using his key e_a and he succeeds if m is accepted as the 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.

Authentication codes that take caution against all above seven different ways to cheat are referred to A^3-codes. We adopt Kerckhoffs principle that all parameters in the model except the actual choices of participants' keys are public information. This includes the probability distribution of the source states and the participants' keys. In all of these possible attacks to cheat, it is understood that the opponent is using an optimal strategy when choosing the message, or equivalently, that the opponent chooses the message that maximizes his chances of success.

For the seven possible types of deceptions, we denote the probability of success in each deception by P_I, P_S, P_T, P_{R_0}, P_{R_1}, P_{A_0}, P_{A_1}, respectively. According to the definition of the seven types of deceptions above, we can have the following definition.

Definition 1 *The general definitions of probability of success are as follows.*

$$P_I = \max_{m} P(m \text{ valid}), \tag{1}$$

$$P_S = \max_{\substack{m,m' \\ m \neq m'}} P(m' \text{ valid}|\ m), \tag{2}$$

$$P_T = \max_{\substack{m,e_t \\ m \notin \mathcal{M}(e_t)}} P(m \text{ valid}|\ e_t), \tag{3}$$

$$P_{R_0} = \max_{m,e_r} P(m \in \mathcal{M}(e_a)|\ e_r), \tag{4}$$

$$P_{R_1} = \max_{\substack{m,m',e_r \\ m\neq m'}} P(m' \in \mathcal{M}(e_a)|\ e_r, m), \tag{5}$$

$$P_{A_0} = \max_{m,e_a} P(m \text{ valid}|\ e_a), \tag{6}$$

$$P_{A_1} = \max_{\substack{m,m',e_a \\ m\neq m'}} P(m' \text{ valid}|\ e_a, m). \tag{7}$$

We further introduce some notations. Let $\mathcal{E}_{\mathcal{R}}(m)$ be the set of possible receiver's keys for a given message m, then

$$\mathcal{E}_{\mathcal{R}}(m) = \{e_r \in \mathcal{E}_{\mathcal{R}} : g(m, e_r) \in \mathcal{S}\}.$$

Let $\mathcal{E}_{\mathcal{A}}(m)$ be the set of possible arbiter's keys for a given message m, then

$$\mathcal{E}_{\mathcal{A}}(m) = \{e_a \in \mathcal{E}_{\mathcal{A}} : p(e_a, m) \neq 0\}.$$

Let $\mathcal{E}_{\mathcal{R}}(e_t)$ be the set of possible receiver's keys for a given transmitter's key e_t, then

$$\mathcal{E}_{\mathcal{R}}(e_t) = \{e_r \in \mathcal{E}_{\mathcal{R}} : g(m, e_r) \in \mathcal{S}, m \in \mathcal{M}(e_t)\}.$$

Let $\mathcal{E}_{\mathcal{R}}(e_a)$ be the set of possible receiver's keys for a given arbiter's key e_a, then

$$\mathcal{E}_{\mathcal{R}}(e_a) = \{e_r \in \mathcal{E}_{\mathcal{R}} : p(e_a, e_r) \neq 0\}.$$

Let $\mathcal{E}_{\mathcal{A}}(e_r)$ be the set of possible arbiter's keys for a given receiver's key e_r, then

$$\mathcal{E}_{\mathcal{A}}(e_r) = \{e_a \in \mathcal{E}_{\mathcal{A}} : p(e_a, e_r) \neq 0\}.$$

Using the above notations, we can rewrite the Definition 1 in the following form which are more specific.

Definition 2 *The probabilities of success in different deceptions are as follows.*

$$P_I = \max_{m} \frac{|\mathcal{E}_{\mathcal{R}}(m)|}{|\mathcal{E}_{\mathcal{R}}|}, \tag{8}$$

$$P_S = \max_{\substack{m,m' \\ m\neq m'}} \frac{|\mathcal{E}_{\mathcal{R}}(m) \cap \mathcal{E}_{\mathcal{R}}(m')|}{|\mathcal{E}_{\mathcal{R}}(m)|}, \tag{9}$$

$$P_T = \max_{\substack{m,e_t \\ m\notin\mathcal{M}(e_t)}} \frac{|\mathcal{E}_{\mathcal{R}}(m) \cap \mathcal{E}_{\mathcal{R}}(e_t)|}{|\mathcal{E}_{\mathcal{R}}(e_t)|}, \tag{10}$$

$$P_{R_0} = \max_{m,e_r} \frac{|\mathcal{E}_{\mathcal{A}}(m) \cap \mathcal{E}_{\mathcal{A}}(e_r)|}{|\mathcal{E}_{\mathcal{A}}(e_r)|}, \tag{11}$$

$$P_{R_1} = \max_{\substack{m,m',e_r \\ m\neq m'}} \frac{|\mathcal{E}_{\mathcal{A}}(m) \cap \mathcal{E}_{\mathcal{A}}(m') \cap \mathcal{E}_{\mathcal{A}}(e_r)|}{|\mathcal{E}_{\mathcal{A}}(m) \cap \mathcal{E}_{\mathcal{A}}(e_r)|}, \tag{12}$$

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

$$P_{A_0} = \max_{m,e_a} \frac{|\mathcal{E}_{\mathcal{R}}(m) \cap \mathcal{E}_{\mathcal{R}}(e_a)|}{|\mathcal{E}_{\mathcal{R}}(e_a)|}, \tag{13}$$

$$P_{A_1} = \max_{\substack{m,m',e_a \\ m\neq m'}} \frac{|\mathcal{E}_{\mathcal{R}}(m) \cap \mathcal{E}_{\mathcal{R}}(m') \cap \mathcal{E}_{\mathcal{R}}(e_a)|}{|\mathcal{E}_{\mathcal{R}}(m) \cap \mathcal{E}_{\mathcal{R}}(e_a)|}, \tag{14}$$

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

It is then convenient to calculate the probabilities of success in different deceptions using (8)-(14).

3 Preliminaries

We first make a brief introduction of the relevant knowledge of projective space, and the specific content can be found in [12]. Let $n \geq 1$ be an integer and $\mathbb{F}_q^{(n+1)}$ be the $(n+1)$-dimensional row vector space over $\mathbb{F}_q$. The 1-dimensional vector subspaces of $\mathbb{F}_q^{(n+1)}$ will now be called *points*, the 2-dimensional, 3-dimensional, and n-dimensional vector subspaces of $\mathbb{F}_q^{(n+1)}$ will be called *lines*, *planes*, and *hyperplanes*, respectively. The $(r+1)$-dimensional vector subspaces of $\mathbb{F}_q^{(n+1)}$ will be called *projective r-flats*, or simply r-flat($0 \leq r \leq n$). The 0-flats, 1-flats, 2-flats, and$(n-1)$-flats are points, lines, planes and hyperplanes, respectively. An r-flat is said to be *incident* with an s-flat, if the r-flat as a vector subspaces contains or is contained in the s-flat as a vector space. Then the set of 1-dimensional vector subspaces of $\mathbb{F}_q^{(n+1)}$, together with the r-flats ($0 \leq r \leq n$) and the incidence relation among them is called the n-dimensional *projective space* over $\mathbb{F}_q$ and is denoted by $PG(n, \mathbb{F}_q)$.

Let P be a point of $PG(n, \mathbb{F}_q)$, then P is a 1-dimensional vector subspace of $\mathbb{F}_q^{(n+1)}$. Let $(x_0, x_1, \ldots, x_n)$ be a non-zero vector in P, then

$$P = \{\lambda(x_0, x_1, \ldots, x_n)|\lambda \in \mathbb{F}_q\}.$$

For any $\lambda \in \mathbb{F}_q^*$, the non-zero vector $(\lambda x_0, \lambda x_1, \ldots, \lambda x_n)$ is called a *system of coordinates*, or simply the *coordinates* of the point P. Clearly, a system of coordinates of a point P is uniquely determined up to a non-zero constant multiple of $\mathbb{F}_q$.

According to the definition of $PG(n, \mathbb{F}_q)$ given above, we can know that the set of r-flats of $PG(n, \mathbb{F}_q)$ and the set of $(r+1)$-dimensional vector subspaces of $\mathbb{F}_q^{(n+1)}$ are in one-to-one correspondence. The r-flat F corresponding to an $(r+1)$-dimensional vector subspace U can be regarded as the set of points whose coordinates are the non-zero vectors of U.

Define the *dimension* of an r-flat in $PG(n,\mathbb{F}_q)$ to be r and denote dim $F = r$, but the corresponding $(r+1)$-dimensional vector subspace U is of dimension $r+1$. Moreover, we define the empty set $\emptyset$ of points in $PG(n,\mathbb{F}_q)$ to be of dimension -1 and denote dim $\emptyset = -1$. Let R_1 and R_2 be flats of $PG(n,\mathbb{F}_q)$. $R_1 \cap R_2$ which is called the *intersection* of R_1 and R_2 is the set of points contained in both R_1 and R_2. $R_1 \cup R_2$ called the *join* of R_1 and R_2 is the minimal flat containing both R_1 and R_2. From the dimension formula of $\mathbb{F}_q^{(n+1)}$, we can deduce the dimension formula of $PG(n,\mathbb{F}_q)$ immediately.

Lemma 3 *Let R_1 and R_2 be two flats of $PG(n,\mathbb{F}_q)$.Then*

$$\dim R_1 + \dim R_2 = \dim(R_1 \cap R_2) + \dim(R_1 \cup R_2).$$

Let $N(m,n)$ be the number of m-dimensional vector subspaces in $\mathbb{F}_q^{(n)}$, where $0 \le m \le n$. Then we have

$$N(m,n) = \begin{bmatrix} n \\ m \end{bmatrix}_q,$$

where $\begin{bmatrix} n \\ m \end{bmatrix}_q$ is called Gaussian coefficient, and

$$\begin{bmatrix} n \\ m \end{bmatrix}_q = \frac{\prod_{i=n-m+1}^{n} (q^i - 1)}{\prod_{i=1}^{m} (q^i - 1)}$$

and agree $\begin{bmatrix} n \\ 0 \end{bmatrix}_q = 1$ for all integer n.

The following lemmas and theorems will be used in the later proof process.

Lemma 4 *[12] Let $m \le n$. Then the number of $m \times n$ matrices of rank m over $\mathbb{F}_q$ is $q^{\frac{m(m-1)}{2}} \prod_{i=n-m+1}^{n} (q^i - 1)$.*

Theorem 5 *[12] In $PG(n,\mathbb{F}_q)$,*

(1) The number of m-flats ($0 \le m \le n$) is

$$N(m+1,n+1) = \begin{bmatrix} n+1 \\ m+1 \end{bmatrix}_q.$$

In particular, $PG(n,\mathbb{F}_q)$ has $q^n+q^{n+1}+\ldots\cdots+q+1$ points and $q^n+q^{n+1}+\ldots\cdots+q+1$ hyperplanes.

(2) The number of k-flats contained in a given m-flat ($0 \le k \le m \le n$) is

$$N(k+1,m+1) = \begin{bmatrix} m+1 \\ k+1 \end{bmatrix}_q.$$

(3) The number of m-flats containing a given k-flat ($0 \le k \le m \le n$) is

$$N(m-k,n-k) = \begin{bmatrix} n-k \\ m-k \end{bmatrix}_q.$$

Lemma 6 *[13] Let m,s,t be nonnegative integers and $\max\{0,m+s-n\} \le t \le \min\{m,s\}$. U is a random m-dimensional vector subspace of $\mathbb{F}_q^{(n)}$. Then the number of s-dimensional vector subspaces R satisfying $\dim(U \cap R) = t$, independent of the choice of U, is*

$$q^{(s-t)(m-t)} \begin{bmatrix} n-m \\ s-t \end{bmatrix}_q \begin{bmatrix} m \\ t \end{bmatrix}_q.$$

Corollary 7 *Let m,s be nonnegative integers and $\max\{-1,m+s-n\} \le t \le \min\{m,s\}$. P is a random m-flat of $PG(n,\mathbb{F}_q)$. Then the number of s-flats Q satisfying dim$(P \cap Q) = t$, independent of the choice of P, is*

$$q^{(s-t)(m-t)} \begin{bmatrix} n-m \\ s-t \end{bmatrix}_q \begin{bmatrix} m+1 \\ t+1 \end{bmatrix}_q.$$

In particular, if R is the given t-flat, the number of s-flats Q satisfying $P \cap Q = R$ is

$$q^{(s-t)(m-t)} \begin{bmatrix} n-m \\ s-t \end{bmatrix}_q.$$

Proof. P is an m-flat of $PG(n,\mathbb{F}_q)$, then P corresponds uniquely to an $(m+1)$-dimensional vector subspace U of $\mathbb{F}_q^{(n+1)}$. Similarly, Q corresponds uniquely to an $(s+1)$-dimensional vector subspace V of $\mathbb{F}_q^{(n+1)}$. Then $(U \cap V)$ is a $(t+1)$-dimensional vector subspace. According to Lemma refL-3-3, the number of V is independent of the choice of U. It's

$$q^{(s-t)(m-t)} \begin{bmatrix} n-m \\ s-t \end{bmatrix}_q \begin{bmatrix} m+1 \\ t+1 \end{bmatrix}_q.$$

The set of r-flats of $PG(n,\mathbb{F}_q)$ and the set of $(r+1)$-dimensional vector subspaces of $\mathbb{F}_q^{(n+1)}$ are in one-to-one correspondence, so we can deduce the conclusion directly. If the t-flat $P \cap Q = R$ is established, clearly the number of Q is

$$q^{(s-t)(m-t)} \begin{bmatrix} n-m \\ s-t \end{bmatrix}_q.$$

□

Lemma 8 *Let m,r,t be nonnegative integers and $0 \le t \le \min\{m,r\}$. Let R_0,P and Q be given t-dimensional, m-dimensional and r-dimensional vector subspace of $\mathbb{F}_q^{(n)}$, respectively. $P \cap Q = R_0$, then*

the number of s-dimensional vector spaces R which satisfy $P \cap R = R_0$ and $\dim(Q \cap R) = k$ is independent of the choice of R_0, P and Q, denoted by $p(m, r, t; s, k, n)$. Then

$$p(m,r,t;s,k,n) = \sum_{\substack{\beta+t=k \\ \alpha+\beta+\rho+t=s}} q^{\omega} \prod_{i=r-k-\alpha+1}^{r-k} (q^i - 1) \begin{bmatrix} m-t \\ \alpha \end{bmatrix}_q \begin{bmatrix} r-t \\ \beta \end{bmatrix}_q \begin{bmatrix} n-m-r+t \\ \rho \end{bmatrix}_q,$$

where $\omega = \rho(m + r - k - \alpha - t) + \frac{\alpha(\alpha-1)}{2}$.

Proof. Let

$$R_0 = \begin{pmatrix} I & 0 \\ t & n-t \end{pmatrix} \begin{matrix} t \\ \end{matrix}.$$

According to the given conditions, we can write the matrix representation of P and Q as follows,

$$P = \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ t & m-t & r-t & n-m-r+t \end{pmatrix} \begin{matrix} t \\ m-t \end{matrix},$$

$$Q = \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & 0 & I & 0 \\ t & m-t & r-t & n-m-r+t \end{pmatrix} \begin{matrix} t \\ r-t \end{matrix}.$$

Let R be the s-dimensional vector subspace of $\mathbb{F}_q^{(n)}$, and $P \cap R = R_0$, $\dim(Q \cap R) = k$. Write R as block matrix

$$R = \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & R_2 & R_3 & R_4 \\ t & m-t & r-t & n-m-r+t \end{pmatrix} \begin{matrix} t \\ s-t \end{matrix}.$$

Suppose $\text{rank}R_4 = \rho$, $\text{rank}(R_2, R_4) = \rho + \alpha$, denote $\beta = s - t - (\alpha + \rho)$. After multiplying by an appropriate $s \times s$ nonsingular matrix, R has matrix representation of the following form

$$R = \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & R_{22} & R_{23} & 0 \\ 0 & 0 & R_{33} & 0 \\ 0 & R_{42} & R_{43} & R_{44} \\ t & m-t & r-t & n-m-r+t \end{pmatrix} \begin{matrix} t \\ \alpha \\ \beta \\ \rho \end{matrix} \quad (15)$$

where $\text{rank}(R_{44}) = \rho$, $\text{rank}(R_{22}) = \alpha$, $\text{rank}(R_{33}) = \beta$. For the fixed ρ-dimensional vector subspace R_{44} of $\mathbb{F}_q^{(n-m-r+t)}$, let $M(R_{44})$ be the set of s-dimensional vector subspaces which (15) can represent. Let R_{44} and R'_{44} be two ρ-dimensional vector subspaces of $\mathbb{F}_q^{(n-m-r+t)}$, then there exists $T \in GL_{n-m-r+t}(\mathbb{F}_q)$, such that $R_{44}T = R'_{44}$. And thus there exists $\begin{pmatrix} I & \\ & T \end{pmatrix} \in GL_n(\mathbb{F}_q)$ transforming $M(R_{44})$ into $M(R'_{44})$. Therefore, $|M(R_{44})| = |M(R'_{44})|$ and $|M(R_{44})|$ is independent of the specific choice of R_{44}. For a fixed α-dimensional vector subspace R_{22} of $\mathbb{F}_q^{(m-t)}$, let $M(R_{44}, R_{22})$ be the set of s-dimensional vector subspaces in $M(R_{44})$. For a fixed β-dimensional vector subspace R_{33} of $\mathbb{F}_q^{(r-t)}$, let $M(R_{44}, R_{22}, R_{33})$ be the set of s-dimensional vector subspaces in $M(R_{44}, R_{22})$. Similarly, we can know that $|M(R_{44}, R_{22})|, |M(R_{44}, R_{22}, R_{33})|$ are independent of the specific choice of R_{22} and R_{33} respectively. Let

$$R_{22} = \begin{pmatrix} I^{(\alpha)} & 0 \end{pmatrix},$$

$$R_{33} = \begin{pmatrix} I^{(\beta)} & 0 \end{pmatrix},$$

$$R_{44} = \begin{pmatrix} I^{(\rho)} & 0 \end{pmatrix}.$$

Then R has matrix representation of the following form

$$R = \begin{pmatrix} I & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I & 0 & 0 & R_{232} & 0 & 0 \\ 0 & 0 & 0 & I & 0 & 0 & 0 \\ 0 & 0 & R_{422} & 0 & R_{432} & I & 0 \\ t & \alpha & m-t-\alpha & \beta & r-t-\beta & \rho & n-m-r+t-\rho \end{pmatrix} \begin{matrix} t \\ \alpha \\ \beta \\ \rho \end{matrix} \quad (16)$$

Since $P \cap R = R_0$, $\dim(R \cap Q) = k$, we have $k = \beta + t$ and $\text{rank}(R_{232}) = \alpha$. Clearly, the matrix representation of the form (16) is unique. So by the Lemma 4, the number of s-dimensional vector subspaces that (16) can represent is

$$q^{\rho(m+r-k-\alpha-t)+\frac{\alpha(\alpha-1)}{2}} \prod_{i=r-k-\alpha+1}^{r-k} (q^i - 1).$$

Then we can calculate $p(m, r, t; s, k, n)$ easily. □

Corollary 9 *Let $-1 \le t \le \min\{m, r\}$. Let R_0, P and Q be given t-flat, m-flat and r-flat of $PG(n, \mathbb{F}_q)$, respectively. $P \cap Q = R_0$, then the number of s-flats R which satisfy $P \cap R = R_0$ and $\dim(Q \cap R) = k$ is independent of the choice of R_0, P and Q, denoted by $p'(m, r, t; s, k, n)$. Then*

$$p'(m,r,t;s,k,n) = \sum_{\substack{\beta+t=k \\ \alpha+\beta+\rho+t=s}} q^{\omega} \prod_{i=r-k-\alpha+1}^{r-k} (q^i - 1) \begin{bmatrix} m-t \\ \alpha \end{bmatrix}_q \begin{bmatrix} r-t \\ \beta \end{bmatrix}_q \begin{bmatrix} n-m-r+t \\ \rho \end{bmatrix}_q,$$

where $\omega = \rho(m + r - k - \alpha - t) + \frac{\alpha(\alpha-1)}{2}$.

Proof. R_0 is a t-flat of $PG(n,\mathbb{F}_q)$, then R_0 corresponds uniquely to a $(t+1)$-dimensional vector subspace of $\mathbb{F}_q^{(n+1)}$, denoted by R_0 as well. Similarly, P and Q correspond uniquely to a $(m+1)$-dimensional vector subspace P and $(r+1)$-dimensional vector subspace Q of $\mathbb{F}_q^{(n+1)}$, respectively. Then $P\cap Q=R_0$, $P\cap R=R_0$ and $Q\cap R$ is a $(k+1)$-dimensional vector subspace of $\mathbb{F}_q^{(n+1)}$. According to Lemma 6, the number of $(s+1)$-dimensional vector subspace R is independent of the choice of R_0, P and Q. Then we have $p'(m,r,t;s,k,n)=p(m+1,r+1,t+1;s+1,k+1,n+1)$. So the number of r-flats can be deduced easily. □

4 Construction of A^3-code

Let $0\le t<r<m$. Let F be a fixed m-flat in $PG(n,\mathbb{F}_q)$ and let R be a fixed t-flat contained in F. Define the source state s to be the r-flat contained in F and containing R. Define the transmitter's key e_t to be the s-flat intersecting F at R. Define the receiver's and the arbiter's key to be the different $(s-1)$-flats intersecting F at R, respectively. Define the message m to be the $(r+s-t)$-flat intersecting F at a r-flat which contains R. Let $\mathcal{S},\mathcal{E}_\mathcal{T},\mathcal{E}_\mathcal{R},\mathcal{E}_\mathcal{A},\mathcal{M}$ be the set of source states, the set of transmitter's keys, the set of receiver's keys, the set of arbiter's keys and the set of messages, respectively.

Define the encoding function:

$$f:\mathcal{S}\times\mathcal{E}_\mathcal{T}\to\mathcal{M}$$

$$\forall s\in\mathcal{S},e_t\in\mathcal{E}_\mathcal{T},f(s,e_t)=s\cup e_t$$

Define the decoding function:

$$g:\mathcal{M}\times\mathcal{E}_\mathcal{R}\to\mathcal{S}\cup\{\text{fraud}\}$$

$$\forall m\in\mathcal{M},e_r\in\mathcal{E}_\mathcal{R},g(m,e_r)=\begin{cases} m\cap F\ ; & e_r\subseteq m\\ \text{fraud}\ ; & e_r\nsubseteq m\end{cases}$$

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 $(s-1)$-flats in the stage of key generation and distribution to be the the receiver's key and the arbiter's key, respectively. That is $e_a\neq e_r$ in a communication.

Lemma 10 *The above construction of A^3-code is reasonable,*

(1) $\forall s\in\mathcal{S},e_t\in\mathcal{E}_\mathcal{T},s\cup e_t\in\mathcal{M}$;

(2) $\forall m\in\mathcal{M},s=m\cap F$ is the unique source state contained in the message m.

Proof. (1) $\forall s\in\mathcal{S},e_t\in\mathcal{E}_\mathcal{T}$, by the definition as above, we can know $s\cap e_t=R$. Then dim($s\cup e_t$)=dim(s)+dim(e_t)−dim($s\cap e_t$) $=r+s-t$, dim($s\cup e_t\cup F$)=dim($e_t\cup F$)=dim(e_t)+dim$F$−dim($e_t\cap F$) $=s+m-t$. So we have dim($(s\cup e_t)\cap F$) $=r$. Clearly, $R\subseteq(s\cup e_t)\cap F$. Thus $s\cup e_t$ is a $(r+s-t)$-flat intersecting F at a r-flat containing R. That is $s\cup e_t\in\mathcal{M}$.

(2) By the construction, $m\cap F$ is a r-flat containing R, thus $s=m\cap F\in\mathcal{S}$. Assume that s' is another source state contained in m, then $s'\subseteq m\cap F=s$. Since dim(s') =dim(s), we have $s=s'$. That is, s is the unique source state contained in m. □

Theorem 11 *The parameters of the constructed A^3-code are*

$$|\mathcal{S}|=\begin{bmatrix} m-t\\ r-t\end{bmatrix}_q,$$

$$|\mathcal{E}_\mathcal{T}|=q^{(s-t)(m-t)}\begin{bmatrix} n-m\\ s-t\end{bmatrix}_q,$$

$$|\mathcal{E}_\mathcal{R}|=|\mathcal{E}_\mathcal{A}|=q^{(s-t-1)(m-t)}\begin{bmatrix} n-m\\ s-t-1\end{bmatrix}_q,$$

$$|\mathcal{M}|=q^{(s-t)(m-r)}\begin{bmatrix} n-m\\ s-t\end{bmatrix}_q\begin{bmatrix} m-t\\ r-t\end{bmatrix}_q.$$

Proof. According to the construction of the authentication code, $|\mathcal{S}|,|\mathcal{E}_\mathcal{T}|,|\mathcal{E}_\mathcal{R}|$ and $|\mathcal{E}_\mathcal{A}|$ can be can be directly derived from Corollary 7. By the definition of the message, m is the $(r+s-t)$-flat intersecting F at a r-flat which contains R. On the basis of Corollary 7, we can know that the number of $(r+s-t)$-flats intersecting F at a fixed r-flat in $PG(n,\mathbb{F}_q)$ is

$$q^{(s-t)(m-r)}\begin{bmatrix} n-m\\ s-t\end{bmatrix}_q.$$

Then by Theorem 5, the number of r-flats containing the given t-flat R in the m-flat F is

$$N(r-t,m-t)=\begin{bmatrix} m-t\\ r-t\end{bmatrix}_q.$$

So we can deduce that

$$|\mathcal{M}|=q^{(s-t)(m-r)}\begin{bmatrix} n-m\\ s-t\end{bmatrix}_q\begin{bmatrix} m-t\\ r-t\end{bmatrix}_q.$$

□

Lemma 12 *Let m be a random message. Then the number of receiver's keys contained in m is*

$$|\mathcal{E}_\mathcal{R}(m)|=q^{(s-t-1)(r-t)}\begin{bmatrix} s-t\\ s-t-1\end{bmatrix}_q.$$

Proof. By the Lemma 10(2), we can know that $s = m \cap F$ is the only source state contained in m. We assert that e_r is the receiver's key contained in m if and only if e_r is the $(s-1)$-flat contained in m, and $e_r \cap s = R$. In fact, if e_r is the receiver's key, then $e_r \cap s \subseteq e_r \cap F = R$. By the construction of the A^3-code, we know that $R \subseteq s \cap e_r$. Hence we have $e_r \cap s = R$. Conversely, if $e_r \subseteq m$ and $e_r \cap s = R$, then we have $e_r \cap F \subseteq m \cap F = s$. Thus $e_r \cap F \subseteq e_r \cap s = R$ and $e_r \cap F = R$. That is, e_r is the receiver's key contained in m. From the Corollary 7 we can know that

$$|\mathcal{E}_{\mathcal{R}}(m)| = q^{(s-t-1)(r-t)} \begin{bmatrix} s-t \\ s-t-1 \end{bmatrix}_q .$$

□

Lemma 13 *Assume that m and m' are two distinct messages which commonly contain a transmitter's key e_t. s and s' are two source states contained in m and m' , respectively. Then e_r is the receiver's key contained in both m and m' if and only if e_r is the $(s-1)$-flat contained in $m \cap m'$ and $e_r \cap (s \cap s') = R$.*

Proof. Clearly we have $R \subseteq e_r \cap (s \cap s')$. If e_r is the receiver's key contained in both m and m', by the proof of Lemma 12, we have $e_r \cap s = R$ and $e_r \cap s' = R$. Then we can deduce $e_r \cap (s \cap s') = R$. Conversely, if $e_r \subseteq m \cap m'$ and $e_r \cap (s \cap s') = R$, then $e_r \cap F \subseteq m \cap m' \cap F \subseteq m \cap F = s$. Similarly, we have $e_r \cap F \subseteq s'$. Thus $e_r \cap F \subseteq (s \cap s' \cap e_r) = R$, so $e_r \cap F = R$, i.e. e_r is the receiver's key contained in $m \cap m'$. □

Lemma 14 *Let e_r and e_a be receiver's key and arbiter's key respectively. e_r and e_a are said to be incident with each other, if they are contained in the same s-flat which intersects F at R. Then e_r and e_a are incident with each other if and only if dim$(e_r \cap e_a) = s-2$.*

Proof. Since e_r and e_a are receiver's key and arbiter's key respectively, dim(e_r) =dim(e_a) =$s-1$ and $e_r \neq e_a$. If e_r and e_a are incident with each other, dim$(e_r \cup e_a) = s$. By the dimension formula, we have dim$(e_r \cap e_a) = s-2$. Conversely, if dim$(e_r \cap e_a) = s-2$, by the dimension formula, dim$(e_r \cup e_a) = s$. It is sufficient to prove $(e_r \cup e_a) \cap F = R$. dim$(e_r \cup e_a \cup F)$ =dim(e_r)+dim(e_a)+dim (F)−dim$(e_r \cap F)$−dim$(e_a \cap F)$−dim$(e_r \cap e_a)$+dim$(e_r \cap e_a \cap F) = s+m-t$, so dim$((e_r \cup e_a) \cap F)$ =dim$(e_r \cup e_a)$+dim(F)−dim$(e_r \cup e_a \cup F) = t$, i.e. $(e_r \cup e_a) \cap F = R$. □

Theorem 15 *Assume that the probability distributions of the set of participants' keys and the set of source states are uniform, then the successful attacks probability of A^3-code in the construction program are as follows:*

$$P_I = \frac{(q^2-1)(q^3-1)\cdots(q^{s-t}-1)}{q^{(s-t-1)(m-r)}(q^{n-m-s+t+2}-1)(q^{n-m-s+t+3}-1)\cdots(q^{n-m}-1)},$$

$$P_S = \frac{1}{q^{s-t-1}},$$

$$P_T = \frac{1}{q^s + q^{s-1} \cdots + q + 1},$$

$$P_{R_0} = P_{A_0} = \frac{p'(r, s-1, t; s-1, s-2, r+s-t)}{p'(m, s-1, t; s-1, s-2, n)},$$

$$P_{R_1} = P_{A_1} = \frac{p'(r-1, s-1, t; s-1, s-2, r+s-t-1)}{p'(r, s-1, t; s-1, s-2, r+s-t)}.$$

Proof. (1) By the Definition 2, Theorem 11 and Lemma 12, we can directly get

$$P_I = \frac{(q^2-1)(q^3-1)\cdots(q^{s-t}-1)}{q^{(s-t-1)(m-r)}(q^{n-m-s+t+2}-1)(q^{n-m-s+t+3}-1)\cdots(q^{n-m}-1)}.$$

(2) Suppose that opponent intercepts the legitimate message $m(m = s \cup e_t)$ and replaces 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 opponent's optimal strategy is to select m' containing the transmitter's key e_t, such that $m' = s' \cup e_t$. Let dim$(s \cap s') = l(-1 \leq l \leq r-1)$, then dim$(m \cup m')$ =dim$(s \cup s' \cup e_t)$ =dim(s)+dim(s')+dim(e_t)−dim$(s \cap e_t)$−dim$(s' \cap e_t)$-dim$(s \cap s')$+dim$(s \cap s' \cap e_t) = 2r+s-t-l$. so we have dim$(m \cap m') = s+l-t$. By the Lemma 13 and Corollary 7, when $e_t \subseteq (m \cap m')$,

$$|\mathcal{E}_{\mathcal{R}}(m) \cap \mathcal{E}_{\mathcal{R}}(m')| = q^{(s-t-1)(l-t)} \begin{bmatrix} s-t \\ s-t-1 \end{bmatrix}_q .$$

Let $l = r-1$, then

$$P_S = \frac{q^{(s-t-1)(l-t)} \begin{bmatrix} s-t \\ s-t-1 \end{bmatrix}_q}{q^{(s-t-1)(r-t)} \begin{bmatrix} s-t \\ s-t-1 \end{bmatrix}_q} = \frac{1}{q^{s-t-1}}.$$

(3) The transmitter send a message $m \notin \mathcal{M}(e_t)$ to the receiver. The receiver accept 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, $\dim(e_t \cap m) \leq s-1$. That is , there is at most one $e_r \subseteq e_t$ in m, i.e.

$|\mathcal{E}_{\mathcal{R}}(m) \cap \mathcal{E}_{\mathcal{R}}(e_t)| \leq 1$. The number of e_r associated with e_t is

$$|\mathcal{E}_{\mathcal{R}}(e_t)| = \begin{bmatrix} s-t \\ s-t-1 \end{bmatrix}_q.$$

Then

$$P_T = \frac{1}{\begin{bmatrix} s-t \\ s-t-1 \end{bmatrix}_q} = \frac{1}{q^{s-t-1} + q^{s-t-2} \cdots + q + 1}.$$

(4) By the lemma 14, we can know $|\mathcal{E}_{\mathcal{R}}(e_a)| = |\mathcal{E}_{\mathcal{A}}(e_r)|$, so it is sufficient to compute $|\mathcal{E}_{\mathcal{A}}(e_r)|$. $\forall e_a \in \mathcal{E}_{\mathcal{A}}(e_r)$, $\dim(e_a \cap e_r) = s-2$ and $e_a \cap F = R$, where F and e_r are m-flat and $(s-1)-$flat respectively, and $e_r \cap F = R$. By the Corollary 3.2, we have

$$|\mathcal{E}_{\mathcal{A}}(e_r)| = p'(m, s-1, t; s-1, s-2, n).$$

Receiver claims to have receive a message $m(e_r \subseteq m)$, he succeeds if $e_a \subseteq m$. Now we compute the probability of P_{R_0}. Let $s = m \cap F$ be the unique source state contained in m. e_a contained in m is the arbiter's key incident with receiver's key e_r if and only if e_a is the $(s-1)$-flat contained in m satisfying both $e_a \cap s = R$ and $\dim(e_a \cap e_r) = s-2$. In fact, if $e_a \subseteq m$ is the arbiter's key and $p(e_r, e_a) \neq 0$, by the Lemma 14, it is clear that $\dim(e_r \cap e_a) = s-2$. $e_a \cap s \subseteq e_a \cap F = R$, so $e_a \cap s = R$. Conversely, it is sufficient to prove $e_a \cap F = R$. $e_a \subseteq m$, thus $e_a \cap F \subseteq m \cap F = s$. So we have $e_a \cap F \subseteq e_a \cap s = R$, i.e. $e_a \cap F = R$. By the Corollary 9, if $e_r \subseteq m$, then $|\mathcal{E}_{\mathcal{A}}(m) \cap \mathcal{E}_{\mathcal{A}}(e_r)| = p'(r, s-1, t; s-1, s-2, r+s-t)$ and

$$P_{R_0} = P_{A_0} = \frac{p'(r, s-1, t; s-1, s-2, r+s-t)}{p'(m, s-1, t; s-1, s-2, n)}.$$

(5) Transmitter sends a legitimate message m to receiver , but the receiver claims to have received m'. Let $s = m \cap F$ and $s' = m' \cap F$ be two different source states contained in m and m', respectively. Let e_r be the receiver's key, then clearly we have $e_r \subseteq m \cap m'$. e_a contained in both m and m' is the arbiter's key incident with receiver's key e_r if and only if e_a is the $(s-1)$-flat contained in $m \cap m'$ satisfying both $e_a \cap (s \cap s') = R$ and $\dim(e_a \cap e_r) = s-2$. In fact, if $e_a \subseteq m \cap m'$ is the arbiter's key and $p(e_r, e_a) \neq 0$, by the Lemma 14, it is clear that $\dim(e_r \cap e_a) = s-2$. Similar to the above proof, $e_a \cap s \subseteq e_a \cap F = R$, so we have $e_a \cap s = R$. Similarly, $e_a \cap s' = R$. Thus we can deduce $e_a \cap (s \cap s') = R$. Conversely, it is sufficient to prove $e_a \cap F = R$. $e_a \cap F \subseteq m \cap F = s$, $e_a \cap F \subseteq m' \cap F = s'$, so $e_a \cap F \subseteq e_a \cap s \cap s' = R$, i.e. $e_a \cap F = R$. Suppose $\dim(s \cap s') = l$, then $-1 \leq l \leq r-1$. By the Corollary 9, if $e_r \subseteq m \cap m'$, then $|\mathcal{E}_{\mathcal{A}}(m) \cap \mathcal{E}_{\mathcal{A}}(m') \cap \mathcal{E}_{\mathcal{A}}(e_r)| = p'(l, s-1, t; s-1, s-2, s+l-t)$ and

$$P_{R_1} = P_{A_1} = \frac{p'(r-1, s-1, t; s-1, s-2, r+s-t-1)}{p'(r, s-1, t; s-1, s-2, r+s-t)}.$$

□

5 Conclusion

The main result in this paper is the new construction of A^3-code and the calculation of the probabilities of success in different attacks. A^3-code is the extension of A^2-code and is constructed based on A^2-code, but there are remarkable differences between them, i.e., A^3-code has a dishonest arbiter compared with the A^2-code and he will also attack the system, that is, A^3-code has at least two more attacks (impersonation and substitution by the arbiter) than A^2-code. In A^2-code model, the arbiter decides whether the message is authentic or not by judging whether the message is valid under the senders key information when theres a dispute between the sender and the receiver, while in A^3-code, he decides it by his or her own key information. Thus in A^3-code, the computation of probabilities of success in different attacks is more complicated compared with A^2-code. The defect of this paper is that the construction of A^3-code is restricted to theoretical basis. Actually, we should further consider the broadcast model and collusion model, associating with practical applications.

Acknowledgements: This work is supported by the National Natural Science Foundation of China under Grant No.61179026 and the Fundamental Research Funds for the Central Universities under Grant No.3122013k001.

References:

[1] G. J. Simmons, *Authentication theory/coding theory*. lecture Notes in Computer Science, 196, Springer, 1985, pp. 411–491.

[2] G. J. Simmons, A Cartesian Product Construction for Unconditionally Secure Authentication Codes that Permit Arbitration, *J. Cryptology* 2, 1990, pp. 77–104.

[3] G. J. Simmons, *Message authentication with arbitration of transmitter\receiver disputes*. proc Eurocrypt'87, Lecture Notes in Computer Science 304, Berlin: 1987, pp. 151–165.

[4] J. Guo, Construction of authentication codes with arbitration from finite affine geometry, *Journal of Science of Teachers' College and University* 27,2007, pp. 1-4

[5] Y. Gao, X. Shi, H. Wang, A Construction of authentication codes with arbitration from singular symplectic geometry over Finite Fields, *Acta Scientiarum Naturalium Universitatis Nankaiensis*,41(6), 2008, pp. 72–77.

[6] 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. 44–53.

[7] 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. 54–63.

[8] E. F. Brickell, D. R. Stinson *Authentication codes with multiple arbiters,* In Advances in Cryptology-EUROCRYPT88, Lecture Notes in Computer Science, volume 330, pages 51-55. Springer-Verlag, Berlin, Heidelberg, New York, 1988, pp. 390–397

[9] T. Johansson, Further results on asymmetric authentication schemes, *Information and Computation*, 151, 1999, pp. 100–133.

[10] Y. Wang, R. Safavi-Naini, A3-codes under collusion attack, *Asiacrypt 99, Lecture Notes in Computer Science*, 1716,1999, pp. 390–399.

[11] R. Safavi-Naini, Y. Wang, Bounds and constructions for A^3-code with multi-senders, *Information Security and Privacy Lecture Notes in Computer Science*, 1438, 1998, pp. 159–168

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

[13] J. Guo, Y. Huo, D. Zhao, An Anzahl formula of subspaces in finite vector spaces and its application, *Joural of Hebei Normal University (Natural Science Edition)*,28(6),2004, pp. 561–564.