Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 7, Issue, 05, pp.16459-16467, May, 2015

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

NEW CONSTRUCTION OF A²-MODEL FROM SYMPLECTIC SPACES OVER FINITE FIELD

***Boubacar Abba**

Department of Mathematics and Informatic, University of Science, Technics and Technologies,
Bamako BP:E3206, Mali

ARTICLE INFO

Article History:
Received 28th February, 2015
Received in revised form
23rd March, 2015
Accepted 05th April, 2015
Published online 31st May, 2015

Key words:

Authentication code with arbitration,
Symplectic Spaces,
Finite Field.

ABSTRACT

Many mathematicians have worked in this erea by using classical groups, normal form of matrices or some known vector spaces and came out some good results. But few of them have used symplectic spaces to construct authentication codes with arbitration. Then in this paper we give a new construction of authentication code with arbitration based on sympletic spaces and also compute parameters and probabilities from this code. The main objective of studying authentication codes with arbitration is to use them for the provision of better security in practical information communications. In the first part of this paper, we present and study the concept of authentication code with arbitration. The historical perspective of the development of authentication code with arbitration is also presented. In the part two of this paper some essential conceptions of symplectic spaces over finite field, which constitute the basic of this paper are introduced. In the same way several theorems are given, then parameters and probabilities of authentication code with arbitration are easily computed. In part three a new construction of authentication code with arbitration from symplectic geometry is presented. In our discussion, we describe the subspaces geometrical characteristics with matrices and use this method to deal with the counting problems in the computation of parameters and probabilities.

Citation: Boubacar Abba, 2015. "New construction of A^2-model from Symplectic spaces over finite field", *International Journal of Current Research*, 7, (5), 16459-16467.

INTRODUCTION

In the model of A-code the transmitter and the receiver are both honest and believe each other because they use the same encoding rules. So this system cannot protect the deception between them. For example when the receiver receives nothing, he can say he had received some legal information (because the receiver knows the encoding rule he can easily make a false information like this). Similarly, when the receiver receives legal information, he can also say that he had received other information. In the condition of these two things, the transmitter can only think that the opponent succeeds in his attack. Moreover, when the transmitter sends a piece of information, he can also say that he had never sent any information. During this time, the receiver can only regard that the opponent succeeds in the attack of the system. Then it is natural to see some disputes will occur between the transmitter and the receiver. However, it is not always the case that two parties want to trust each other. Inspired by this problem. Simmons introduced an extended model, called the A^2-code model in which there is a fourth person, called an arbiter. In this model, caution is taken against deception by the transmitter and the receiver as well as that by the opponent. The arbiter has access to all key information of the transmitter and the receiver, and solves disputes between them. Then there are essentially five different kinds of cheating, impersonation by the opponent, substitution by the opponent, impersonation by the transmitter, impersonation by the receiver and substitution by the receiver. So let us give first a mathematical description of authentication code with arbitration.

Definition

Suppose that S , M , E_T , E_R are four non-empty sets , let $g : S \times E_T \to M$ and $h : \mathrm{M} \times \mathrm{E}_R \to S \cup \{reject\}$ be to two maps , the six tuplet ,(S , M , E_T , E_R , g ,h)is called an authentication code with arbitration or A^2-code if

(1) $g : S \times E_T \to M$ is surjective and satisfies $g(s, e_T) = g(s', e_T) \Rightarrow s = s'$ where $m \in M$ $s, s' \in S, e_T \in E_T$

(2) $h : \mathrm{M} \times \mathrm{E}_R \to S \cup \{reject\}$ satisfies: $P(e_T, e_R) \neq 0$, we have $g(s, e_T) = m \Rightarrow h(m, e_R) = s$ where $s \in S$ and $m \in M$.

Corresponding author: Boubacar Abba,
Department of Mathematics and Informatic, University of Science, Technics and Technologies, Bamako BP:E3206, Mali

S , M , E_T , E_R denote respectively the set of source states, the set of all possible messages , the set of all encoding rules of transmitter , the set of encoding rules of receiver. The two map g and h are respectively encoding and decoding functions. If $g(s,e_T) = m$ we say that m is obtained by e_T encoding s and that e_T is contained in m, and if $h(m,e_R) = s$, we say that e_R is contained in m. The cardinals |S|. |M|, $|E_T|$, $|E_R|$ are called parameters of the A^2-code. In this model, the transmitter and the receiver are not mutually trust worthy, and hence disputes between them may occur, In order to solve possible disputes between the transmitter and the receiver , a fourth participant called arbiter is introduced. The arbiter has access to all key information and by definition, he doesn't cheat. He is only present to solve possible disputes and does not take part in any communication activities. Code for this model provide protection against deceptions both from an outsider (opponent) and from the insiders (transmitter and receiver). Recall that we only consider unconditional security, i.e., against attacks performed with unlimited computing power. As in A-code the transmitter wants to send some information, called a source state , to the receiver in such a way that the receiver can both recover the transmitted source state and verify that the transmitted message originates from the legitimate transmitter. The source state s , taken from the set S of possible source states , is encoded by the transmitter into a message m from the lager set M of possible messages. The message m is subsequently transmitted over the channel. The mapping from S to M is determined by transmitter's secret encoding rule e_T, chosen from the set E_T of possible encoding rules . We may assume that the transmitter uses a mapping $g : S \times E_T \to M$.

The mapping g satisfies $g(s,e_T) = g(s',e_T) \Rightarrow s = s'$. In other words, the source state can be recovered uniquely from a transmitted message. The mapping g is deterministic, i.e., a source state cannot be mapped into several messages for a given encoding rule (splitting is not allowed). This restriction is made for simplicity and most results that will be derived are also valid for A^2-model that use splitting. As usual, the opponent has access to the channel in the sense that he can either impersonate the transmitter and send a message, or replace a transmitted message with a different one. The receiver must decide whether a received message is valid or not. For this purpose the receiver uses a mapping, determined by his own secret encoding rule e_R, taken from the set E_R of possible encoding rules, that determines if the message is valid, and if so, also the source state. . So we may assume a mapping $h : \mathrm{M} \times \mathrm{E}_R \to S \cup \{reject\}$, where for all possible (e_T, e_R), i.e., $P(e_T,e_R) \neq 0$, we have $g(s,e_T) = m \Rightarrow h(m,e_R) = s$. For the receiver to accept all legal messages from the transmitter and to translate them to the correct source state, property (2) must hold for all pair (e_T, e_R). However, in general not all pairs (e_T, e_R) will be possible, i.e., have a positive probability. The arbiter is the supervisory person who has access to all information, including e_T and e_R, but does not take part in any communication activities on the channel. His only task is to solve possible disputes between the transmitter and the receiver whenever such occur. This is done in the following way. If the message m, received by the receiver, could have been generated by the transmitter according to his encoding rule e_T , then the arbiter decides that the message m was sent by the transmitter, and otherwise not. The arbiter assumed to be honest.

In the authentication code with arbitration the following five type of cheating attacks are considered.

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

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

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

Attack R_0 (Impersonation by the receiver). The receiver claims to have received a message from the transmitter. The receiver succeeds if this message could have generated by the transmitter according this encoding rule.

Attack R_1 (Substitution by the receiver). The receiver receives a message from the transmitter, but claims to have received another message. The receiver succeeds if this message could have been generated by the transmitter according to this encoding rule.

All parameters in the model except the actual choices of encoding rules are public information. In all possible attempts to cheat it is understood that the cheating person uses an optimal strategy when choosing a message, or equivalently, that the cheating person chooses the message that maximizes his chances of success. For the five types of deceptions, we denote these cheating probabilities by P_I , P_S , P_T , P_{R0} , P_{R1} respectively. The overall probability of deception is denoted by P_D and is defined to be $P_D = \max\{P_I, P_S, P_T, P_{R_0}, P_{R_1}\}$. Lot of authors used geometry of classical groups and normal form of matrices , involutions and idempotents over finite field to construction cartesian authentication codes and authentication codes with arbitration. In this paper we will use symplectic space over finite fields F_q to construct an authentication code with arbitration and compute the parameters and the probabilities of successful attacks in this construction.

2. Preliminaries: Let F_q , q is a power of odd prime , denote a finite field , and consider

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

The symplectic group of degree 2v over the finite field F_q is defined as $Sp_{2v}(F_q) = \{T \in GL_{2v}(F_q) / TK{}^tT = T\}$. Let

$V_{2v}(F_q)$ be the 2v-dimensional row vector space over F_q. There is a group action of $Sp_{2v}(F_q)$ on $V_{2v}(F_q)$ defined as follows:

$$V_{2v}(F_q)\times Sp_{2v}(F_q)\to V_{2v}(F_q)$$

$$((x_1,...,x_v,x_{v+1},....,x_{2v}),\mathrm{T})\to(x_1,....,x_v,....,x_{2v})T$$

The vector space $V_{2v}(F_q)$ together with the above group action of symplectic group $Sp_{2v}(F_q)$ is called the 2v-dimensional symplectic space over F_q with respect to K. Let P be an m-dimensional vector subspace of $V_{2v}(F_q)$. We often use the same letter P to denote a matrix representation of the vector subspace P , i.e., P is an $m\times 2v$ matrix of rank m whose rows form a basis of P. It is easy to see that PK^tP is an alternate matrix. Let the rank of PK^tP be 2s, then we call the vector subspace P a subspace of type (m,s). Clearly $s\le v$ and $2s\le m$ .From Dieudonne's generalization of Witt's theorem it follows that two subspaces belong to the same orbit under $Sp_{2v}(F_q)$ if and only if they are of the same type. It can be prove that the type (m, s) of a subspace satisfies the following inequality : $2s\le m\le v+s$ and that for any pair of nonnegative integers (m, s) satisfying the above inequality there exist subspaces of type (m, s). Thus the number of orbits of subspaces under $Sp_{2v}(F_q)$ is equal to the number of pairs of nonnegative integers (m, s) satisfying the above inequality . We computed that le latter is equal to $\frac{1}{2}(v+1)(v+2)$. By the same way we mention that the length N(m , s , 2v) of the orbit of subspaces of type (m , s) of $V_{2v}(F_q)$ is given by

$$N(m,s,2v)=q^{2s(v+s-m)}\frac{\prod_{i=v+s-m+1}^{v}(q^{2i}-1)}{\prod_{i=1}^{s}(q^{2i}-1)\prod_{i=1}^{m-2s}(q^{i}-1)}$$

In particular, subspaces of type (m, 0) are called m-dimensional totally isotropic subspaces and subspaces of type (2s, s) are called 2s-dimensional non-isotropic subspaces . It is clear that a subspace P is totally isotropic if and only if PK^tP=0, and it is non-isotropic if and only if PK^tP is nonsingular.

Two vectors x and y of $V_{2v}(F_q)$ are said to be orthogonal (with respect to K) , if $xK^ty=0$ .Furthermore, for any subspace P, define $P^{\perp}=\{y\in V_{2v}(F_q)\,|\,\mathrm{yK^tx}=0 \text{ for all } x\in P\}$.

Lemma 2.1 Let $A=\left(a_{ij}\right)_{m\times 2v}$ and $B=\left(b_{ij}\right)_{m_1\times 2v}$ denote m-dimensional and m_1-dimensional subspaces respectively. Then the subspace A is contained in the subspace B iff there is an $m\times m_1$ matrix Q such that $A=QB$ and $m\le m_1$. Furthermore A and B represent same subspace if there is an $m\times m$ (note m = m_1) invertible matrix Q such that A=QB.

Lemma 2.2 Let V be a 2v-dimensional symplectic space over F_q and P a subspace of type (m, 0) ($m\le v$) in V. Then $P^{\perp}$ contains a 2(v-m)-dimensional symplectic subspace Q which satisfies $Q\cap P=0$.

Proof Let $a_1,\dots,a_m$ be a basis of P. Then there exist $b_1,\dots,b_m$ in V such that $b_iKb_j^t=0, b_iKa_j^i=0\,(i\ne j)$ and $b_iKa_i^t=1$. And we have $V=\langle a_1,b_1\rangle\perp....\perp\langle a_m,b_m\rangle\perp W$. It is clear that $W\subseteq P^{\perp}$ and $P\subseteq P^{\perp}$. Note that $W\oplus P$ and $P^{\perp}$ both have dimension 2v-m . So $W\oplus P=P^{\perp}$, and W is the 2(v-m)-dimensional symplectic subspace contained in $P^{\perp}$ which satisfies that $Q\cap P=0$.

3.Construction of an A^2-model

Let $n=2v$, $m,m_0\in \mathrm{N}$ satisfy $1<m_0<m\le v$.

Let be P_0 a fixed subspace of type $(m_0,0)$ in $V_{2v}(F_q)$, and P_1 a fixed (m_0-1)-dimensional subspace contained in P_0. Define the set of all source states S = {s|s is a subspace of type (m , 0) containing P_0 in $V_{2v}(F_q)$}, the set of all possible messages $M=\{\eta\,|\,\eta$ is a subspace of type $(m-m_0,0)$ in $V_{2v}(F_q)$ and $\eta+P_0$ is a subspace of type (m , 0) in $V_{2v}(F_q)$ }, the set of all encoding rules of the transmitter $E_T=\{e_T\,|\,e_T$ is a complementary subspace of P_0 in $V_{2v}(F_q)$ },the set of all encoding rules of the receiver $E_R=\{e_R\,|\,e_R$ is a complementary subspace of P_1 in $V_{2v}(F_q)\}$

The encoding map f is defined as : $f(s,e_T)=s\cap e_T$, for all $s\in S$ and $e_T\in E_T$, the decoding map g is defined as :

$$g(\eta,e_R)=\begin{cases}\eta+P_0\,if & \eta\subseteq(\eta+P_0)\cap e_R\\ reject, otherwise.\end{cases}$$

To prove the above construction is indeed an A^2-model we need the following lemma.

Lemma 3.1: Let s be a subspace of type (m, 0) in $V_{2v}(\mathrm{F}_q)$ which contains P_0, and e_T a complementary subspace of P_0 in $V_{2v}(\mathrm{F}_q)$. Then $s\cap e_T$ is a subspace of type $(m-m_0,0)$ such that $(s\cap e_T)+P_0$ is a subspace of type (m , 0).

Proof Suppose the dimension of $s\cap e_T$ is l and $a_1,....,a_l$ it's basis . Let $b_1,.....,b_{m_0}$ be a basis of P_0. Since $s\cap e_T$ is contained in the complementary subspace of P_0, $b_1,.....,b_{m_0}$, $a_1,....,a_l$ are linearly independent. On the other hand , $\langle b_1,....,b_{m_0},a_1,....,a_l\rangle\subseteq s$, we have $m_0+l\le m$, i.e., $\dim(s\cap e_T)=l\le m-m_0$.

Extend the basis $b_1,.....,b_{m_0}$ of P_0 to a basis $b_1,.....,b_{m_0}$, $a_1,....,a_{m-m_0}$ of s if $a_i \notin e_T$, writing a_i as $a_i = x + y$ where $x \in P_0$ and $y \in e_T$, since $P_0 \oplus e_T = V_{2v}(F_q)$, we may find $y = a_i - x \in s$. Replace a_i by y, we obtain a new basis $b_1,.....,b_{m_0}$, $a_1,....,a_{i-1}$, y, $a_{1+1},....,a_{m-m_0}$ of s. In this way we may choose a_i $(1 \le i \le m - m_0)$ such that $a_i \in e_T$. Then $\langle a_1,....,a_{m-m_0}\rangle \subseteq s \cap e_T$ and $\dim(s \cap e_T) \ge m - m_0$. Above all, $\dim(s \cap e_T) = m - m_0$. And the proof implies that $\langle a_1,....,a_{m-m_0}\rangle = s \cap e_T$, and $s = (s \cap e_T) + P_0$. It is obvious that $s \cap e_T$ is a subspace of type $(m - m_0, 0)$ and $(s \cap e_T) + P_0$ is a subspace of type (m, 0).

Theorem 3.2 The construction provides us an A^2-model
Proof Let us verify the two conditions in the definition of authentication code with arbitration or A^2-model.

(1) f is surjective. In fact, for any $\eta \in M$,η is a subspace of type $(m - m_0, 0)$ and $\eta + P_0$ is a subspace of type (m , 0) in $V_{2v}(\mathrm{F}_q)$ (this implies that $\eta \cap P_0 = 0$ and there is a complementary subspace η' of P_0 such that $\eta' \supseteq \eta$). Let $s = \eta + P_0$, then $s \in S$. For any complementary subspace e_T of P_0 containing η, $s \cap e_T \supseteq \eta$. Then we have $s \cap e_T = \eta$ and $f(s, e_T) = \eta$ by Lemma 3.1.

For any $\eta \in M$, $e_T \in E_T$, if $s_1, s_2 \in S$ such that $f(s_1, e_T) = f(s_2, e_T) = \eta$ then by the proof of lemma 3.1we have $s_1 = s_2$

(2) It is clear that $P(e_T, e_R) \ne 0$. Let $f(s, e_T) = \eta$, $\eta \subseteq (\eta + P_0) \cap e_R$. Then $g(\eta, e_R) = \eta + P_0$ by the definition of g and $g(\eta, e_R) = s$ by the proof of lemma 3.1 .

3.1 Computation of parameters

Proposition 3.1.1 The number of source states is given by the following

$$|S| = \frac{\prod_{i=v-m+1}^{v-m_0} (q^{2i} - 1)}{\prod_{1=1} (q^i - 1)}$$

Proof Let $N'(m_0, 0; m, 0; 2v)$ denote the number of subspaces of type $(m, 0)$ containing a fixed subspace of type $(m_0, 0)$ in $V_{2v}(F_q)$. Then we may prove that $|S| = N'(m_0, 0; m, 0; 2v)$, so we need to give this lemma.

Lemma 3.1.2 Let P be a k-dimensional subspace in $V_{2v}(F_q)$ and $a_1,...,a_k$ a basis of P. Extend $a_1,...,a_k$ to a basis $a_1,...,a_k$, $a_{k+1},...,a_{2v}$ of $V_{2v}(F_q)$. Then any complementary subspace of P in $V_{2v}(F_q)$ has a matrix representation as $\begin{pmatrix} A_{(2v-k)\times k} & I_{(2v-k)} \end{pmatrix}$ on the above basis , where $A_{(2v-k)\times k}$ is determined uniquely by the complementary subspace of P.

Proof Let $C = \begin{pmatrix} C_1 & C_2 \end{pmatrix}$ where C$_1$ and C$_2$ are $(2v-k)\times k$ and $(2v-k)\times(2v-k)$ matrices respectively denote the matrix representation of a complementary subspace Q of P in $V_{2v}(F_q)$ with respect to the basis $a_1,...,a_k$, $a_{k+1},...,a_{2v}$. We claim that C$_2$ is invertible. Otherwise , no loss generality, suppose its first row is a linear combination of other rows (let λ be the row vector of representation coefficients), then we have $\begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix}\begin{pmatrix} C_1 & C_2 \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ C_3 & C_4 \end{pmatrix}$. Note that $\begin{pmatrix} \alpha & 0 \\ C_3 & C_4 \end{pmatrix}$ is full rank on rows, so $\alpha \ne 0$. Let $X = \begin{pmatrix} \alpha & 0 \end{pmatrix}\begin{pmatrix} a_1 \\ \vdots \\ a_{2v} \end{pmatrix} = \alpha \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix}$ Then $X \ne 0$ and $X \in P \cap Q$. But $P \cap Q = \{0\}$, this a contradiction , hence C$_2$ is invertible . Thus $C_2^{-1}\begin{pmatrix} C_1 & C_2 \end{pmatrix} = \begin{pmatrix} A & I \end{pmatrix}$ is also a representation of Q.

Suppose that $\begin{pmatrix} A & I \end{pmatrix}$ and $\begin{pmatrix} A_1 & I \end{pmatrix}$ both represent Q, then there is an invertible matrix D such that $\begin{pmatrix} A & I \end{pmatrix} = D\begin{pmatrix} A_1 & I \end{pmatrix}$, i.e., $\begin{pmatrix} A & I \end{pmatrix} = \begin{pmatrix} DA_1 & D \end{pmatrix}$, it is obvious that $D = I$, so A is determined uniquely by Q.

Proposition 3.1.2 The number of encoding rules of the transmitter is $|E_T| = \mathrm{q}^{m_0(2v-m_0)}$

Proof From lemma 3.1.2 we know that $e_T \in E_T$ has a matrix representation as the form $\begin{pmatrix} A_{(2v-m_0)\times m_0} & I_{(2v-m_0)} \end{pmatrix}$ where $A_{(2v-m_0)\times \mathrm{m}_0}$ is uniquely determined by e_T. Then we have the conclusion.

Proposition 3.1.3 The number of encoding rules of the receiver is $|E_R| = q^{(m_0-1)(2v-m_0+1)}$

Proof From Lemma 3.1.2 we know that $e_R \in E_R$ has a matrix representation as the form $\begin{pmatrix} A_{(2v-m_0+1)\times(m_0-1)} & I_{(2v-m_0+1)} \end{pmatrix}$ where $A_{(2v-m_0+1)\times(m_0-1)}$ is uniquely determined by e_R. Then we have the result.

Proposition 3.1.4 The number of messages is computed by

$$|M| = q^{m_0(m-m_0)} \frac{\prod_{i=v-m+1}^{v-m_0} (q^{2i}-1)}{\prod_{i=1}^{m-m_0} (q^{i}-1)}$$

Proof Given a message $\eta \in M$, we know that $\eta \cap P_0 = \{0\}$ and the source state corresponding to η is $\eta + P_0$ by definition of M and Theorem 3,2. Let $a_1, ..., a_{m_0}$ a basis of P_0, and $a_{m_0+1}, ..., a_m$ a basis of M. Then $a_1, ..., a_{m_0}$, $a_{m_0+1}, ..., a_m$ is a basis of $\eta + P_0$. Extend this basis to a basis $a_1, ..., a_{m_0}$, $a_{m_0+1}, ..., a_m$, $a_{m+1}, ..., a_{2v}$ of $V_{2v}(F_q)$. Then η has a representation $\begin{pmatrix} 0 & I_{(m-m_0)} & 0 \end{pmatrix}$ on the above basis. By lemma3.1.2,

an encoding rule e_T of the transmitter which contains η has a representation $\begin{pmatrix} A_{(2v-m_0)\times m_0} & I_{(2v-m_0)} \end{pmatrix}$ where $A_{(2v-m_0)\times \mathrm{m}_0}$ is uniquely determined by e_T. Rewrite $\begin{pmatrix} A & I \end{pmatrix}$ as $\begin{pmatrix} B & I_{(m-m_0)} & 0 & 0 \\ C & 0 & I_{(2v-m)} & 0 \end{pmatrix}$. Note that $\eta \subseteq e_T$, by Lemma 2.1, there is a matrix $\begin{pmatrix} Q_1 & Q_2 \end{pmatrix}$ such that $\begin{pmatrix} 0 & I_{(m-m_0)} & 0 \end{pmatrix} =$ $\begin{pmatrix} Q_1 & Q_2 \end{pmatrix} \begin{pmatrix} B & I_{(m-m_0)} & 0 & 0 \\ C & 0 & I_{(2v-m)} & 0 \end{pmatrix}$ $= \begin{pmatrix} Q_1A + Q_2B & Q_1 & Q_2 \end{pmatrix}$ It is obvious that $Q_1 = I$, $Q_2 = 0$ and thus $B = 0$. So any encoding rule e_T contained in η has a representation $\begin{pmatrix} 0 & I_{(m-m_0)} & 0 & 0 \\ C & 0 & I_{(2v-m)} & 0 \end{pmatrix}$ on the above basis and the number of encoding rules of the transmitter , which contained in η is $\mathrm{q}^{m_0(2v-m)}$. Since $|\mathrm{M}| = \frac{|S||E_T|}{q^{m_0(2v-m)}}$, we get the consequence.

3.2 Computation of probabilities

Proposition 3.2.1 The probability of a successful impersonation attack is $P_I = \frac{1}{q^{(m_0-1)(m-m_0)}}$

Proof From the definition of the message set (set of all possible messages), any η message satisfies that $\eta \cap P_0 = \{0\}$ and that $\eta + P_0$ is a source state corresponding to η (see the proof of Theorem 3.2).

Let $a_1, ..., a_{m_0}$ a basis of P_0 such that $a_1, ..., a_{m_0-1}$ is a basis of P_1 and extend it to a basis $a_1, ..., a_{m_0-1}$, a_{m_0}, $a_{m_0+1}, ..., a_m$ of $\eta + P_0$ such that $a_{m_0+1}, ..., a_m$ is a basis of η. At last extend this basis of $\eta + P_0$ to a basis $a_1, ..., a_{m_0-1}$, $a_{m_0}, ..., a_m$, $a_{m+1}, ..., a_{2v}$ of $V_{2v}(F_q)$. Then η has a matrix representation

$$\begin{pmatrix} 0_{(m-m_0)\times(m_0-1)} & 0_{(m-m_0)\times 1} & I_{(m-m_0)} & 0_{(m-m_0)\times(2v-m)} \end{pmatrix}$$

on the above basis. Applying Lemma 3.1.2 we know that e_R which is contained in η (i.e.,$\eta \subseteq e_R$) must have a representation in the form $\begin{pmatrix} A_{(2v-m_0+1)\times(\mathrm{m}_0-1)} & I_{(2v-m_0+1)} \end{pmatrix}$, where $A_{(2v-m_0+1)\times(\mathrm{m}_0-1)}$ is determined uniquely by e_R. Block it into $\begin{pmatrix} \beta_3 & 1 & 0 & 0 \\ A & 0 & I_{(m-m_0)} & 0 \\ B & 0 & 0 & I_{(2v-m)} \end{pmatrix}$. Since $\eta \subseteq e_R$, we know that $\begin{pmatrix} 0 & 0 & I & 0 \end{pmatrix}$ is a linear combination of rows of $\begin{pmatrix} \beta_3 & 1 & 0 & 0 \\ A & 0 & I_{(m-m_0)} & 0 \\ B & 0 & 0 & I_{(2v-m)} \end{pmatrix}$. Thus we may get $A = 0$ and the number of e_R in η is $q^{(m_0-1)(2v-m+1)}$ (i.e., the number of $\begin{pmatrix} \beta_3 \\ B \end{pmatrix}$). Then $P_I = \max_{\eta \in M} \left\{ \frac{the \quad number \quad of \quad e_R \quad in \quad \eta}{|E_R|} \right\}$

$$= \frac{q^{(m_0-1)(2v-m+1)}}{q^{(m_0-1)(2v-m_0+1)}}$$

$$= \frac{1}{q^{(m_0-1)(m-m_0)}}$$

To compute other probabilities , choose $a_1, ..., a_{m_0}$ a basis of P_0 such that $a_1, ..., a_{m_0-1}$ is a basis of P_1. By lemma 3.1 we know that $P_0^{\perp} = P_0 \oplus W$ where W is 2(v-m$_0$)-dimensional symplectic subspace in $V_{2v}(F_q)$

Let $\gamma_1, ..., \gamma_{2(v-m_0)}$ be a basis of W, then $a_1, ..., a_{m_0-1}$ a_0, , $\gamma_1, ..., \gamma_{2(v-m_0)}$ is a basis of $P_0^{\perp}$. Extend it to a basis $a_1, ..., a_{m_0-1}, a_0, \gamma_1, ..., \gamma_{2(v-m_0)}$, $\gamma_{2(v-m_0)+1}, ..., \gamma_{2v-m_0}$ $V_{2v}(F_q)$.

Then P_0 has a matrix representation $\begin{pmatrix} I_{(m-1)} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ on this basis. For any source state $s \in S$, since $P_0 \subseteq s$ and $s \subseteq P_0^{\perp}$, s has a matrix representation $\begin{pmatrix} I_{(m_0-1)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ X_2 & X_2 & X & 0 \end{pmatrix}$, where X is a $(m-m_0)\times[2(\mathrm{v}-\mathrm{m}_0)]$ matrix on this basis. Furthermore

$$\begin{pmatrix} I & 0 & 0 \\ 0 & 1 & 0 \\ -X_1 & -X_2 & I \end{pmatrix}\begin{pmatrix} I & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ X_1 & X_2 & X & 0 \end{pmatrix} = \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & X & 0 \end{pmatrix}.$$

So the matrix representation of s on the basis should be $\begin{pmatrix} I & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & X & 0 \end{pmatrix}$, where $\begin{pmatrix} 0 & 0 & X & 0 \end{pmatrix}$ denotes a subspace of type $(m-m_0,0)$ in $V_{2v}(F_q)$. For any $e_T \in E_T$ and $e_R \in E_R$, we know that they have a matrix representation $\begin{pmatrix} A_{2(v-m_0)\times(m_0-1)} & \alpha & I_{2(v-m_0)} & 0 \\ C_{m_0\times(m_0-1)} & \beta & 0 & I_{m_0} \end{pmatrix}$ and $\begin{pmatrix} \delta & 1 & 0 & 0 \\ B_{2(v-m_0)\times(m_0-1)} & 0 & I_{2(v-m_0)} & 0 \\ D_{m_0\times(m_0-1)} & 0 & 0 & I_{m_0} \end{pmatrix}$ respectively by lemma 3.1.2

For any $\eta \in M$, since $\eta \in P_0^{\perp} = P_0 \oplus W$, η has a matrix representation $\begin{pmatrix} Y_{(m-m_0)\times(2v-m_0)} & 0_{(m-m_0)\times m_0} \end{pmatrix}$ on this basis. Because $\eta + P_0$ has a matrix representation $\begin{pmatrix} I_{(m_0-1)} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ X_1 & X_2 & X & 0 \end{pmatrix}$ on this basis, we may think the source state which corresponds to η is a subspace with the representation $\begin{pmatrix} I & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & X & 0 \end{pmatrix}$ where $\begin{pmatrix} 0 & 0 & X & 0 \end{pmatrix}$ denotes a subspace of type $(m-m_0,0)$.

Proposition 3.2.2 The probability of a successful substitution attack is $P_S = \dfrac{1}{q^{m_0-1}}$

Proof Let η and η' be two messages corresponding to different source states, and $\begin{pmatrix} X_1 & X_2 & X & 0 \end{pmatrix}$ and $\begin{pmatrix} X_1' & X_2' & X' & 0 \end{pmatrix}$ the matrix representation of η and η' respectively, where X and X' are two different subspaces of type $(m-m_0,0)$ in W. It is obvious that rank $\begin{pmatrix} X \\ X' \end{pmatrix} \geq m-m_0+1$. Let e_R be the encoding rule of receiver contained in η and η'(that is to say, $\eta \subseteq e_R$ and $\eta' \subseteq e_R$). So the subspace represented by $\begin{pmatrix} X_1 & X_2 & X & 0 \end{pmatrix}$ is contained in a subspace represented by $\begin{pmatrix} \delta & 1 & 0 & 0 \\ B_{2(v-m_0)\times(m_0-1)} & 0 & I_{2(v-m_0)} & 0 \\ D_{m_0\times(m_0-1)} & 0 & 0 & I_{m_0} \end{pmatrix}$. Then there exist a matrix $\begin{pmatrix} Q_1 & Q_2 & Q_3 \end{pmatrix}$ such that

$$\begin{pmatrix} X_1 & X_2 & X & 0 \end{pmatrix} = \begin{pmatrix} Q_1 & Q_2 & Q_3 \end{pmatrix}$$

$$\begin{pmatrix} \delta & 1 & 0 & 0 \\ B_{2(v-m_0)\times(m_0-1)} & 0 & I_{2(v-m_0)} & 0 \\ D_{m_0\times(m_0-1)} & 0 & 0 & I_{m_0} \end{pmatrix}$$

$= \begin{pmatrix} Q_1\delta + Q_2B + Q_3D & Q_1 & Q_2 & Q_3 \end{pmatrix}$. We have $\begin{pmatrix} X_1 & X_2 & X & 0 \end{pmatrix} = \begin{pmatrix} X_2\delta + XB & X_2 & X & 0 \end{pmatrix}$. Similarly $\begin{pmatrix} X_1' & X_2' & X' & 0 \end{pmatrix} = \begin{pmatrix} X_2'\delta + X'B & X_2' & X' & 0 \end{pmatrix}$.

Combining the two equalities, we have $\begin{pmatrix} X \\ X' \end{pmatrix} B + \begin{pmatrix} X_2 \\ X_2' \end{pmatrix}\delta = \begin{pmatrix} X_1 \\ X_1' \end{pmatrix}$, i.e., $\begin{pmatrix} X \\ X' \end{pmatrix} B - \begin{pmatrix} X_1 \\ X_1' \end{pmatrix} = \begin{pmatrix} X_2 \\ X_2' \end{pmatrix}\delta$. From ranck $\begin{pmatrix} X \\ X' \end{pmatrix} \geq m-m_0+1$ we know that the dimension of the solution space of $\begin{pmatrix} X \\ X' \end{pmatrix}\gamma^t = 0$ is less than or equal to $2(v-m_0)-(m-m_0+1) = 2v-m-m_0+1$. For a fixed δ, a column of B as a solution of the system of non-homogeneous linear equations may have $q^{(2v-m-m_0-1)}$ choices at most, so there are at most $\left(q^{(2v-m-m_0-1)}\right)^{m_0-1}$ choices for B.Thus the number of e_R in η and η' is at most $q^{(m_0-1)}q^{(m_0-1)(2v-m-m_0+1)}q^{m_0(m_0-1)} = q^{(m_0-1)(2v-m)}$ (namely the number of $\begin{pmatrix} \delta \\ B \\ D \end{pmatrix}$). From the process of P$_1$'s calculation we know that the number of encoding rules e_R , which is contained in message η is $q^{(m_0-1)(2v-m+1)}$. Therefore

$$P_S = \max_{\eta \in M} \left\{ \frac{\max\limits_{\eta'} \{the \quad number \quad of \quad e_R \quad in \quad \eta \quad and\, \eta'\}}{thenumber \quad of \quad e_R \quad in \quad \eta} \right\}$$

$$= \frac{q^{(m_0-1)(2v-m)}}{q^{(m_0-1)(2v-m+1)}} = \frac{1}{q^{m_0-1}}.$$

Lemma 3.3.3 Let $\begin{pmatrix} I & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & X & 0 \end{pmatrix}$ denote a source state s , $\begin{pmatrix} A & \alpha & I_{2(v-m_0)} & 0 \\ C & \beta & 0 & I_{m_0} \end{pmatrix}$ a encoding rule e_T and $\begin{pmatrix} \delta & 1 & 0 & 0 \\ B_{2(v-m_0)\times(m_0-1)} & 0 & I_{2(v-m_0)} & 0 \\ D_{m_0\times(m_0-1)} & 0 & 0 & I_{m_0} \end{pmatrix}$ an encoding rule e_R. Then

(1) The message obtained by e_T encoding s (that is the intersection of the subspaces that e_T and s represent) has a matrix representation $\begin{pmatrix} XA & X\alpha & X & 0 \end{pmatrix}$;

(2) The subspace $e_R \cap s$ has a matrix representation $\begin{pmatrix} \delta & 1 & 0 & 0 \\ XB & 0 & X & 0 \end{pmatrix}$.

Proof Let $\begin{pmatrix} Y_1 & Y_2 & Y & 0 \end{pmatrix}$ be a matrix representation of the message η obtained by e_T encoding s. Since $\eta \subseteq e_T$, by lemma 2.1 there is a matrix $\begin{pmatrix} Q_1 & Q_2 \end{pmatrix}$ such that

$$\begin{pmatrix} Y_1 & Y_2 & Y & 0 \end{pmatrix} = \begin{pmatrix} Q_1 & Q_2 \end{pmatrix} \begin{pmatrix} A & \alpha & I_{2(v-m_0)} & 0 \\ C & \beta & 0 & I_{m_0} \end{pmatrix} =$$

$$\begin{pmatrix} Q_1A + Q_2C & Q_1\alpha + Q_2\beta & Q_1 & Q_2 \end{pmatrix}$$

So $Q_1 = Y, Q_2 = 0$, and $\begin{pmatrix} Y_1 & Y_2 & Y & 0 \end{pmatrix} = \begin{pmatrix} YA & Y\alpha & Y & 0 \end{pmatrix}$. On the other hand $\eta \subseteq s$, by lemma 2.1 there is a matrix $\begin{pmatrix} D_1 & D_2 & D_3 \end{pmatrix}$ such that

$$\begin{pmatrix} YA & Y\alpha & Y & 0 \end{pmatrix} = \begin{pmatrix} D_1 & D_2 & D_3 \end{pmatrix} \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & X & 0 \end{pmatrix}.$$

So $D_1 = YA, D_2 = Y\alpha$ and $D_3X = Y$. Since X and Y are full rank in rows , D$_3$ is invertible. Thus $\begin{pmatrix} Y_1 & Y_2 & Y & 0 \end{pmatrix} =$ $\begin{pmatrix} YA & Y\alpha & Y & 0 \end{pmatrix} = \begin{pmatrix} D_3XA & D_3X\alpha & D_3X & 0 \end{pmatrix} =$ $D_3\begin{pmatrix} XA & X\alpha & X & 0 \end{pmatrix}$

Since D$_3$ is invertible, the message η has a matrix representation $\begin{pmatrix} YA & Y\alpha & Y & 0 \end{pmatrix}$. The proof of (2) is similar so that of (1)

Lemma 3.3.4 Given an encoding rule e_T of transmitter, the number of encoding rules e_R of receiver contained in e_T is $q^{(m_0-1)(m_0+1)}$, and given an encoding rule e_R of the receiver, the number of the related encoding rules e_T of the transmitter is $q^{2(v-m_0)+m_0^2}$.

Proof That e_T and e_R are relative means that any message gotten from a source state s encoding by e_T can pass through the authentication e_R. That is so to say, any message $\eta = \begin{pmatrix} XA & X\alpha & X & 0 \end{pmatrix}$ obtained by e_T encoding s = $\begin{pmatrix} I & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & X & 0 \end{pmatrix}$ (where $\begin{pmatrix} 0 & 0 & X & 0 \end{pmatrix}$ is a subspace of type $\begin{pmatrix} m - m_0 & 0 \end{pmatrix}$ in W) is contained in a subspace $\begin{pmatrix} \delta & 1 & 0 & 0 \\ XB & 0 & X & 0 \end{pmatrix}$. By lemma 2.1 there is a matrix $\begin{pmatrix} Q_1 & Q_2 \end{pmatrix}$ such that $\begin{pmatrix} XA & X\alpha & X & 0 \end{pmatrix} = \begin{pmatrix} Q_1 & Q_2 \end{pmatrix}$ $\begin{pmatrix} \delta & 1 & 0 & 0 \\ XB & 0 & X & 0 \end{pmatrix} = \begin{pmatrix} Q_1\delta + Q_2XB & Q_1 & Q_2X & 0 \end{pmatrix}$. So $Q_1 = X\alpha$ and $Q_2X = X$. Further, we have $XA = X(B + \alpha\delta)$ (note that α is $2(v - m_0) \times 1$ matrix and δ is a $1 \times (m_0 - 1)$ matrix). Since the block X in the matrix $\begin{pmatrix} I & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & X & 0 \end{pmatrix}$ may take the form $X_i = \begin{pmatrix} o \cdots 1 o \cdots o \\ o \end{pmatrix}_{(m-m_0)\times 2(v-m_0)}$ where 1 runs over every column on the first row (note that $\begin{pmatrix} 0 & 0 & X_i & 0 \end{pmatrix}$ is a totally isotropic subspace in W), we have that the $i - th$ row of $B + \alpha\delta$ is equal to A's , i.e., $A = B + \alpha\delta$. When e_T fixed, from the equality $A = B + \alpha\delta$, we know that only δ and D in e_R can be chosen freely; and when e_R fixed (i.e., B and δ are fixed with it), from the equality $A = B + \alpha\delta$ we know C, α, β in e_T can be chosen freely. Then it is easy to get the results

Proposition 3.3. 5 The probability of a successful impersonation attack by the transmitter is $P_T = \frac{1}{q^{m_0-1}}$.

Proof Given an encoding rule e_T of the transmitter, its matrix representation is $\begin{pmatrix} A & \alpha & I_{2(v-m_0)} & 0 \\ C & \beta & 0 & I_{m_0} \end{pmatrix}$.

By lemma3.3.4 the number of encoding rules e_R of the receiver , which is related to e_T is $q^{(m_0-1)(m_0+1)}$. Choose a message η which can't be obtained by e_T encoding some source state and suppose its matrix representation is $\begin{pmatrix} X_1 & X_2 & X & 0 \end{pmatrix}$. We know that the representation of the correspondent source state is $\begin{pmatrix} I & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & X & 0 \end{pmatrix}$.

By lemma3.3.3 we may get a message $\begin{pmatrix} XA & X\alpha & X & 0 \end{pmatrix}$ by e_T encoding the source state . Since η can not be obtained by e_T encoding some source state, then $\begin{pmatrix} X_1 & X_2 & X & 0 \end{pmatrix}$ and $\begin{pmatrix} XA & X\alpha & X & 0 \end{pmatrix}$ represent different subspace , so $X_1 - XA$ and $X_2 - X\alpha$ can not equal simultaneously. To pass through e_R 's authentication, η has to $(\eta + P_0) \cap e_R \supset \eta$. This just requires $e_R \supseteq \eta$. Then there is a matrix $\begin{pmatrix} Q_1 & Q_2 & Q_3 \end{pmatrix}$ such that $\begin{pmatrix} X_1 & X_2 & X & 0 \end{pmatrix}$ = $\begin{pmatrix} Q_1 & Q_2 & Q_3 \end{pmatrix} \begin{pmatrix} \delta & 1 & 0 & 0 \\ B & 0 & I_{2(v-m_0)} & 0 \\ D & 0 & 0 & I_{m_0} \end{pmatrix}$

= $\begin{pmatrix} Q_1\delta + Q_2B + Q_3D & Q_1 & Q_2 & Q_3 \end{pmatrix}$ So $Q_3 = 0$; $Q_2 = X$; $Q_1 = X_2$ and furthermore $XB + X_2\delta = X_1$. Since e_R and e_T are related, we have $B = A - \alpha\delta$ by lemma 3.3.4. Then $X(A - \alpha\delta) + X_2\delta = X_1$, this implies $(X_2 - X\alpha)\delta = X_1 - XA$. Now we claim that there is a unique δ satisfying the equation.

Otherwise, if $\delta_1 \neq \delta_2$ both satisfy $(X_2 - X\alpha)\delta_i = X_1 - XA$ (i = 1,2), then $(X_2 - X\alpha)(\delta_1 - \delta_2) = 0$. Note that $X_2 - X\alpha$ is an $(m - m_0) \times 1$ matrix and $\delta_1 \neq \delta_2$ is a matrix $1 \times (m_0 - 1)$ matrix. This means

$X_2 - X\alpha$ =0. Simultaneously we have $X_1 - XA = 0$. Hence, when δ is chosen $B = A - \alpha\delta$ is uniquely determined. Above all, there are at most $q^{m_0(m_0-1)}$ (i.e., the number of D) encoding rules of the receiver contained in η and related to e_T. Thus we have

$$P_T = \max_{e_T}\left\{ \frac{\max_{\eta \not\subset e_T} \{the\ number\ of\ e_R\ in\ \eta\ related\ to\ e_T\}}{the\ number\ of\ e_R\ related\ to\ e_T} \right\}$$

$$= \frac{q^{m_0(m_0-1)}}{q^{(m_0+1)(m_0-1)}}$$

$= \frac{1}{q^{m_0-1}}$. (Here $\eta \not\subset e_T$ means that η can not obtained by e_T encoding some source state)

Proposition 3.3.6 The probability of successful impersonation attack by the receiver is $P_{R_0} = \frac{1}{q^{m-m_0}}$

Proof By lemma 3.3.4 the number of encoding rules e_T of the transmitter which are related to a given encoding rule e_R of the receiver is $q^{2(v-m_0)+m_0^2}$. By similar argument as in Lemma3.3.3 and 3.3.5. we may get the number of encoding rules e_T contained in a given message η and related to a given encoding rules e_R is $q^{2v-m-m_0+m_0^2}$. Thus we have

$$P_{R_0} = \max_{e_R}\left\{ \frac{\max_{\eta} \{the\ number\ of\ e_T\ in\ \eta\ related\ to\ e_R\}}{the\ number\ of\ e_T\ related\ to\ e_R} \right\}$$

$$= \frac{q^{2v-m-m_0+m_0^2}}{q^{2(v-m_0)+m_0^2}} = \frac{1}{q^{m-m_0}}.$$

Proposition 3.3.7 The probability of a successful attack by the receiver is $P_{R_1} = \frac{1}{q}$

Proof Choose an encoding rule e_R of the receiver and take two messages $\eta = \begin{pmatrix} X_1 & X_2 & X & 0 \end{pmatrix}$ and $\eta_1 = \begin{pmatrix} X_1' & X_2' & X' & 0 \end{pmatrix}$ which correspond different source states s and s' respectively. It is clear that the representation of s and s' are $\begin{pmatrix} I & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & X & 0 \end{pmatrix}$ and $\begin{pmatrix} I & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & X' & 0 \end{pmatrix}$ respectively. Note that $\begin{pmatrix} 0 & 0 & X & 0 \end{pmatrix}$ and

$\begin{pmatrix} 0 & 0 & X' & 0 \end{pmatrix}$ are different subspaces of type $(m-m_0, 0)$ in W. So rank$\begin{pmatrix} X \\ X' \end{pmatrix} \geq m-m_0+1$. The subspace representing e_T which is related to e_R should contain that of η and η_1 (note that $A = B + \alpha\delta$, see lemma 3.3.4). So the messages obtained from e_T encoding s and s' should equal to η and η_1 respectively and we have that $\begin{pmatrix} X_1 & X_2 & X & 0 \end{pmatrix} = \begin{pmatrix} XA & X\alpha & X & 0 \end{pmatrix}$ and $\begin{pmatrix} X_1' & X_2' & X' & 0 \end{pmatrix} = \begin{pmatrix} X'A & X'\alpha & X' & 0 \end{pmatrix}$. Thus $XA = X_1, X'A = X_1', X\alpha = X_2, X'\alpha = X_2$.

On the other hand , the two messages should pass through the authentication e_R. By the proof of proposition3.3.5 we have that $XB + X_2\delta = X_1$; $X'B + X_2'\delta = X_1'$. Under the conditions : $A = B + \alpha\delta$ and $XB + X_2\delta = X_1$, if $X\alpha = X_2$ we must have $XA = X_1$. So we only need to consider the conditions $X\alpha = X_2$ and $X'\alpha = X_2'$. Combining the two equations, we have $\begin{pmatrix} X \\ X' \end{pmatrix}\alpha = \begin{pmatrix} X_2 \\ X_2' \end{pmatrix}$. Since rank$\begin{pmatrix} X \\ X' \end{pmatrix} \geq m-m_0+1$, the dimension of the solution space of $\begin{pmatrix} X \\ X' \end{pmatrix}\gamma^t = 0$ is at most $2(v-m_0)-(m-m_0+1)$. Moreover the number (denote it by $N(e_T, e_R, \eta, \eta')$) of e_T contained in the two messages obtained from different source state and related to a given encoding rule e_R is at most $q^{2v-m-m_0-1}.q^{m_0^2}$. Thus we have

$$P_{R_1} = \max_{e_R}\left\{\frac{\max\limits_{\eta',\eta}\ \{N(e_T, e_R, \eta, \eta'\}}{the\ \ number\ \ of\ \ e_T\ \ in\ \ \eta\ \ related\ \ to\ \ e_R}\right\}$$

$$= \frac{q^{2v-m-m_0-1}.q^{m_0^2}}{q^{2v-m-m_0}.q^{m_0^2}} = \frac{1}{q}.$$

Conclusion

This paper investigated a new construction of authentication codes with arbitration based on symplectic geometry. Thus we have proved that this new construction provided us an A^2-model, moreover several counting theorems and lemma have been proved. We also described the subspaces's geometrical characteristics with matrices and use this method to deal with the counting problems in the computation of the parameters and probabilities. Authentication code with arbitration is more complicated than other code. Since its parameters and probabilities are difficult to be computed. So there is no much in this erea. Then in this paper we have done a new construction of authentication code with arbitration using a symplectic geometry, and we obtained some new results which have led to the contribution for the research on the code.

REFERENCES

Boubacar Abba, You Hong . Lower bounds on the sizes of keys of authentication codes with arbitration. The proceedings of the 9th Inter. Conf on applied Mathematics, Istanbul Turkey, May 27-29, 2006, 546-549

Boubacar Abba, You Hong. Some new bounds on A^2-Model. WSEAS Trans. On Communication Vol. 5, N^{0}6, pp 1008-1014 , June 2006

BoubacarAbba, You Hong. Using Pseudo-symplectic Spaces to construct authentication codes with arbitration. *J. of Heilongjiang Science Nat.*, Vol.23, N^{0}5, pp 681-689, Oct 2006.

Cunsheng Ding, XiaojianTian, Three Constructions of Authentication codes with perfect secrecy, Designs, Codes and Cryptography, 33 (2004), 227-239.

Hu L. On construction of optimal A^2-model [J]. *Northeast Math J*, 2001, 17; 27-33.

Kurosowa K. and S. Obana Combinatorial classification of optimal authentication codes with arbitration, *Designs and Cryptography*, 20(2000), 281-305.

Kurosowa K., and S. Obana Combinatorial Bounds on authentication codes with arbitration, Designs, Codes and Cryptography, 22(2001), 265-281

Li R., L. Guo, X. Li. Construction of Cartesianauthentication codes with arbiter from error2 correcting codes (in Chinese), 29(4)(2002), 530-533.

Li R., Z Li, X. Li, Further Construction of authentication code with arbitration from unitary geometry. *J. of Electronics and Information Technology* (in Chinese), 24(3)(2002), 418-421.

Luo J Z. Construction of Authentication code with arbitration [D] Harbin : Harbin Institute of Technology , 2001.

Luo J.Z., Construction of authentication codes with arbitration, Thesis for master degree, harbinInstitute of Technology 2001, 1-55.

Yu J., Z. Li, Construction of authentication codes with arbitration from Pseudo-symplectic geometry (in Chinese), *J. of Northeast University* (Natural Science Edition), 35 (1) (2005), 7-10.

****