J. Appl. Math. & Informatics Vol. 27(2009), No. 5 - 6, pp. 1481 - 1488
Website: http://www.kcam.biz

CONSTRUCTION OF CARTESIAN AUTHENTICATION CODES OVER UNTITRAY GEOMETRY

WENYAN XU AND YOU GAO*

ABSTRACT. A construction of Cartesian authentication codes over unitary geometry is presented and its size parameters are computed. Assuming that the encoding rules are chosen according to a uniform probability distribution, the probabilities of success for different types of attacks are also computed.

AMS Mathematics Subject Classification : 94A60
Key words and phrases : Finite field; unitary geometry; Cartesian authentication code

1. Introduction

Let $\mathbb{S}, \mathbb{E}, \mathbb{M}$ be three non-empty finite sets and let $f : \mathbb{S} \times \mathbb{E} \to \mathbb{M}$ be a map. The four tuple $(\mathbb{S}, \mathbb{E}, \mathbb{M}, f)$ is called an authentication code[1], if

1) The map $f : \mathbb{S} \times \mathbb{E} \to \mathbb{M}$ is surjective and

2) Given any $m \in \mathbb{M}$ and $e \in \mathbb{E}$ such that there is an $s \in \mathbb{S}$ satisfying $f(s,e) = m$, then such an s is uniquely determined by the given m and e.

We call $\mathbb{S}, \mathbb{E}$ and $\mathbb{M}$ the set of source states, the set of encoding rules, and the set of messages respectively; f is called the encoding map. The cardinals $|\mathbb{S}|, |\mathbb{E}|$, and $|\mathbb{M}|$ are called the size parameters of the code. Moreover, if the authentication code satisfies the further requirement that given any message m there is a unique source state s such that $m = f(s,e)$ for any encoding rule contained in m, then the code is called a Cartesian authentication code.

The references [2,3] has used the similarly canonical forms of idempotent matrices and involutory matrices over finite fields to construct Cartesian authentication codes, [4-9] has used the symplectic geometry, the unitary geometry and the alternate matrices over finite fields to construct the codes. All above have got some beautiful results. In the present paper, a new construction of Cartesian authentication codes over unitary geometry is presented and its size

Received August 30, 2008. Revised May 11, 2009. Accepted May 28, 2009. *Corresponding author. This work is supported by the National Natural Science Foundation of China under Grant No. 60776810 and the Natural Science Foundation of Tianjin City under Grant No.08JCYBJC13900.

parameters are computed. Moreover, we assume that the encoding rules are chosen according to a uniform probability distribution, the P_I and P_S, which denote the largest the probabilities of a successful impersonation attack and of a successful substitution attack respectively, of these codes are computed.

Let $\mathbb{F}_{q^2}$ be a finite field with q^2 elements, where q is a power of a prime. $\mathbb{F}_{q^2}$ has an *involutive automorphism*:

$$a \mapsto \bar{a} = a^q$$

and the fixed field of this automorphism is $\mathbb{F}_q$. Let $n = 2\nu + \delta, \delta = 0$ or 1 and denote the $H_{2\nu+\delta}$

$$H_0 = \begin{pmatrix} 0 & I^{(\nu)} \\ I^{(\nu)} & 0 \end{pmatrix}$$

and

$$H_1 = \begin{pmatrix} 0 & I^{(\nu)} & \\ I^{(\nu)} & 0 & \\ & & 1 \end{pmatrix}.$$

We regard the unitary group as the *unitary group of degree n* with respect to H_n over the finite field $\mathbb{F}_{q^2}$ and denoted by $U_n(\mathbb{F}_{q^2})$, which is defined to be the set of matrices $U_n(\mathbb{F}_{q^2}) = \{T \in GL_n(\mathbb{F}_{q^2}) | TH_n{}^t\bar{T} = H_n\}$. Let $\mathbb{F}_{q^2}^{(n)}$ be the $n-$dimensional row vector space over $\mathbb{F}_{q^2}$. There is an action of $U_n(\mathbb{F}_{q^2})$ on $\mathbb{F}_{q^2}^{(n)}$ defined as follows:

$$\mathbb{F}_{q^2}^{(n)} \times U_n(\mathbb{F}_{q^2}) \longrightarrow \mathbb{F}_{q^2}^{(n)}.$$
$$((x_1, x_2, \cdots, x_n), T) \longmapsto (x_1, x_2, \cdots, x_n)T.$$

Then the vector space $\mathbb{F}_{q^2}^{(n)}$ with the above action of the group $U_n(\mathbb{F}_{q^2})$ is called the $n-$dimensional *unitary space* over $\mathbb{F}_{q^2}$.

Let P be an $m-$dimensional subspace of $U_n(\mathbb{F}_{q^2})$. We use the same letter P to denote a matrix representation of P. For an $n \times n$ nonsingular Hermitian matrix H, it is clear that $PH_n{}^t\bar{P}$ is Hermitian. If the rank of $PH_n{}^t\bar{P}$ is r,then P is called a *subspace of type* (m, r). In particular, subspaces of type $(m, 0)$ are called $m-$dimensional *totally isotropic subspaces.*Denote by $P^\perp$ the *dual subspace of* P, i.e.,

$$P^\perp = \{y \in \mathbb{F}_{q^2}^{(n)} | yH^t\bar{x} = 0 \ for \ all \ x \in P\}$$

From the Lemma 5.7 of the reference [10], subspace of type (m, r) exists in the $n-$dimensional unitary space if and only if $2r \leq 2m \leq n + r$. And also from Lemma 5.8 of [10],we have

Lemma 1. *$U_n(\mathbb{F}_{q^2})$ acts transitively on each set of subspaces of the same type in $\mathbb{F}_{q^2}^{(n)}$.*

Notations. In this paper, let $\nu = [n/2]$ be the index of $n \times n$ Hermitian matrix of rank n; $N(m, r; n)$ denotes the number of subspaces of $\mathbb{F}_{q^2}^{(n)}$ of type (m, r); $N(m_1, r_1; m, r; n)$ denotes the number of subspaces of type (m_1, r_1) contained in a fixed subspace of type (m, r) in $\mathbb{F}_{q^2}^{(n)}$, denote by $N'(m_1, r_1; m, r; n)$ the number of subspaces of type (m, r) containing a fixed subspace of type (m_1, r_1) in $\mathbb{F}_{q^2}^{(n)}$.

Moreover, $|U_n(\mathbb{F}_{q^2})|$, $N(m, r; n)$, $N(m_1, r_1; m, r; n)$, $N'(m_1, r_1; m, r; n)$ are computed in [10].

2. Construction

Assuming that $q > 2$, $\nu \geq 2$, $1 \geq m \geq v$, denote

$$\begin{array}{rcl} \mathbb{S} & = & \{S \mid S =< e_1, e_2, \cdots, e_m >\}, \\ \mathbb{E} & = & U_n(\mathbb{F}_{q^2}), \\ \mathbb{M} & = & \{M \mid M \textit{ is a subspace of type } (m, 0)\}, \end{array}$$

Define
$$\begin{array}{rccc} f: & \mathbb{S} \times \mathbb{E}_T & \longrightarrow & \mathbb{M} \\ & (S\ ,\ T) & \longmapsto & ST \end{array}$$

For any message $M \in \mathbb{M}$, i.e., a subspace of type $(m, 0)$, let $S =< e_1, e_2, \cdots, e_m >$, hence a source state. By lemma 1 there is a $T \in U_n(\mathbb{F}_{q^2})$ such that $S = MT$, here M and S is matrix representations of the subspaces M and S, hence T is an encoding rule. So the map f is surjective. Moreover, the source state S is uniquely determined by the dimension of M. Therefore, the above construction results in a Cartesian authentication code.

Lemma 2.

$$\begin{array}{rcl} |\mathbb{S}| & = & v, \qquad |\mathbb{E}| = |U_n(\mathbb{F}_{q^2})|, \\ |\mathbb{M}| & = & \sum\limits_{m=1}^{[n/2]} N(m, 0; n), 0 < m \leq \nu, \end{array}$$

Proof. Since $2r \leq 2m \leq n + r, r = 0$ and $v = [n/2]$, hence by the definition,

$$\begin{array}{rcl} |\mathbb{S}| & = & \sum\limits_{i=1}^{v} 1, 0 < m \leq \nu, \\ |\mathbb{E}| & = & |U_n(\mathbb{F}_{q^2})| = q^{\frac{n(n-1)}{2}} \prod\limits_{i=1}^{n} (q^i - (-1)^i), \\ |\mathbb{M}| & = & \sum\limits_{m=1}^{[n/2]} N(m, 0; n), 0 < m \leq \nu, \end{array}$$

where $|U_n(\mathbb{F}_{q^2})|$ and $N(m, 0; n)$ is given in [10]. □

Lemma 3. *For any message $M \in \mathbb{M}$, i.e., a subspace of type $(m, 0)$, the number of encoding rules contained in M is*

$$\frac{|U_n(\mathbb{F}_{q^2})|}{N(m, 0; n)}.$$

Proof. Let M be any message, i.e., a subspace of type $(m, 0)$. Then there is an unique source state S contained in M. We may choose the matrix representation of S as

$$S = \begin{pmatrix} I^{(s)} & 0 & 0 & 0 \end{pmatrix}. \atop \qquad m \qquad \nu-m \qquad m \qquad \nu-m+\delta$$

where $\delta = 0$ or 1.By lemma 1, there is a $T \in U_n(\mathbb{F}_{q^2})$ and a matrix representation M of the subspace M such that $ST = M$. Then T has the form

$$T = \begin{pmatrix} M \\ T_1 \end{pmatrix} \begin{matrix} m \\ n-m \end{matrix} .$$

where T_1 is a $(n-m) \times n$ nonsingular matrix.

Note that if M and M' are two distinct subspaces of the same type $(m, 0)$, then

i) There is not T in $U_n(\mathbb{F}_{q^2})$, such that ST represents both M and M', i.e., two distinct subspaces of the same type can't contain an encoding rule in common;

ii) by lemma 1, there is a $Q \in U_n(\mathbb{F}_{q^2})$ and matrix representations M and M' of subspaces M and M' respectively, such that $M = M'Q$. Define map $\varphi : T \to TQ$, for $T \in \mathbb{E}$ and T is contained in M', then $TQ \in \mathbb{E}$ and TQ is contained in M. Clearly φ is a $1-1$ map. That is , the number of encoding rules contained in two distinct subspaces of the same type is equal.

For fixed s, the encoding rules contained in all the subspaces of the same type $(m, 0)$ form the group $U_n(\mathbb{F}_{q^2})$. It follows that the number of encoding rules contained in any subspace of type $(m, 0)$ is

$$\frac{|U_n(\mathbb{F}_{q^2})|}{N(m, 0; n)}.$$

□

Lemma 4. *Let M and M' be two distinct messages which contain an encoding rule in common and let S and S' be the unique source state contained in M and M' respectively. Then the number of encoding rules contained in both M and M' is*

$$n' = \begin{cases} 0, & \textit{if } m = m' \\ \dfrac{|U_n(\mathbb{F}_{q^2})|}{N(m, 0; n)N'(m, 0; m', 0; n)}, & \textit{if } m < m' \\ \dfrac{|U_n(\mathbb{F}_{q^2})|}{N(m', 0; n)N(m, 0; m', 0; n)}, & \textit{if } m > m' \end{cases} .$$

Proof. We choose M to be any subspace of type $(m, 0)$. Suppose M' is a distinct subspace of type $(m, 0)$. Let n' denote the number of encoding rules contained in both M and M'.

case i) $m = m'$. Then $n' = 0$ follows from the proof of lemma 3.

case ii) $m < m'$. By the proof of lemma 3, there is a $T \in \mathbb{E}$ such that $ST = M$, $S'T = M'$. Similar as the proof of Lemma 3, S has the form

$$S = \begin{pmatrix} I^{(m)} & 0 & 0 & 0 \end{pmatrix}. \atop \begin{matrix} m & \nu-m & m & \nu-m+\delta \end{matrix}$$

and S' has the form

$$S' = \begin{pmatrix} I^{(m)} & 0 & 0 \\ 0 & I^{(m'-m)} & 0 \end{pmatrix}. \atop \begin{matrix} m & m'-m & n-m' \end{matrix}$$

and T has the form as

$$T = \begin{pmatrix} M \\ M_{12} \\ T_1 \end{pmatrix} \begin{matrix} {\scriptstyle m} \\ {\scriptstyle m'-m} \\ {\scriptstyle n-m'} \end{matrix},$$

where M_{12} is $(m' - m) \times n$ nonsingular matrix. It is easy to check that M is the subspace of M'.Since M is fixed, then there are $N'(m, 0; m', 0; n)$ possible choices of M'.

By the proof of lemma 3, n' is equal to the number of encoding rules contained in M dividing the number of possible choices of M', i.e.,

$$n = \frac{|U_n(\mathbb{F}_{q^2})|}{N(m,0;n)N'(m,0;m',0;n)}.$$

case iii) $m > m''$. By the same discussion as in case ii), we get

$$n = \frac{|U_n(\mathbb{F}_{q^2})|}{N(m',0;n)N(m,0;m',0;n)}.$$

□

Lemma 5. *If the encoding rules are chosen according to a uniform probability distribution, then the probabilities of a success for different types of attacks are given by*

$$P_I = \frac{q^2-1}{(q^{n-1}-(-1)^{n-1})(q^n-(-1)^n)}, P_S = \frac{1}{q+1}$$

Proof. 1)Computation of P_I.

Suppose that the opponent simply sends a message M, M is accepted as authentic if and only if M contains the receiver's encoding rule. So

$$P_I = \max_{M \in \mathbb{M}} \frac{|\{e \in \mathbb{E} | e \in M\}|}{|\mathbb{E}|} = \max_{1 \le m \le \nu} \frac{1}{N(m,0;n)}.$$

From reference [10],

$$P_I = \max_{1 \le m \le \nu} \frac{1}{N(m,0;n)} = \max_{1 \le m \le \nu} \frac{\prod_{i=1}^{m}(q^{2i}-1)}{\prod_{i=n-2m+1}^{n}(q^i-(-1)^i)}.$$

Let

$$\begin{aligned} I(m) &= \frac{1}{N(m,0;n)} \\ &= \frac{(q^2-1)(q^4-1)}{(q^{n-1}-(-1)^{n-1})(q^n-(-1)^n)(q^{n-3}-(-1)^{n-3})(q^{n-2}-(-1)^{n-2})\cdots} \\ &\quad \cdot \frac{\cdots(q^{2m}-1)}{\cdots(q^{n-2m+1}-(-1)^{n-2m+1})(q^{n-2m+2}-(-1)^{n-2m+2})}. \end{aligned}$$

and

$$I(1) = \frac{q^2-1}{(q^{n-1}-(-1)^{n-1})(q^n-(-1)^n)},$$

When $m \leq n-2m+1$,i.e.,$m \leq [\frac{n+1}{3}]$, $I(m)$ decrease monotonously;

when $m \geq n-2m+2$,i.e.,$m \geq [\frac{n+2}{3}]$, $I(m)$ increase monotonously.

The case of n is even,

$$\frac{I(n/2)}{I(1)} = \frac{(q^n-1)}{(q^2-1)(q^{n-3}+1)\cdots(q^3+1)(q+1)} \leq 1,$$

The case of n is odd,

$$\frac{I((n-1)/2)}{I(1)} = \frac{(q^{n-1}-1)}{(q^{n-2}-1)(q^{n-4}-1)\cdots(q^3-1)(q^2-1)} \leq 1,$$

Therefore

$$P_I = \max_{1 \leq m \leq \nu}\{I(m)\} = I(1) = \frac{q^2-1}{(q^{n-1}-(-1)^{n-1})(q^n-(-1)^n)}$$

2)Computation of P_S.

Suppose that the opponent has observed a message M, and now he replaces this with another message M'. The source state S corresponding to M and the source state S' corresponding to M' must be distinct,i.e., $m \neq m'$. Because the encoding rule $T \in M$, the opponent should chose M' so that $T \in M'$, therefore the number of T contained in both M and M' is

$$\frac{|U_n(\mathbb{F}_{q^2})|}{N(m,0;n)N'(m,0;m',0;n)}, (m < m')$$

or

$$\frac{|U_n(\mathbb{F}_{q^2})|}{N(m,0;n)N(m',0;m,0;n)}, (m > m')$$

For the number of T contained in M is $\frac{|U_n(\mathbb{F}_{q^2})|}{N(m,0;n)}$, so

$$\begin{aligned} P_S &= \max_{M,M' \in \mathbb{M}, M \neq M'} \frac{|\{e \in \mathbb{E} | e \in M, and\ e \in M'\}|}{|\{e \in \mathbb{E} | e \in M\}|} \\ &= \max\{\max_{1 \leq m < m' \leq \nu}\{\frac{1}{N'(m,0;m',0;n)}\}, \max_{1 \leq m < m' \leq \nu}\{\frac{1}{N(m',0;m,0;n)}\}\} \end{aligned}$$

let $S_1(m,m') = \frac{1}{N'(m,0;m',0;n)} = \frac{\prod_{i=1}^{m'-m}(q^{2i}-1)}{\prod_{i=n-2m'+1}^{m-2m}(q^i-(-1)^i)}, (1 \leq m < m' \leq \nu)$

Obviously, $m'-m$ is smaller as $S_1(m,m')$ is larger, and

$$S_1(m,m+1) = \frac{q^2-1}{(q^{n-2m-1}-(-1)^{n-2m-1})(q^{n-2m}-(-1)^{n-2m})}$$

so

$$\max_{1 \leq m < m' \leq \nu}\{S_1(m,m')\} = S_1(\nu-1,\nu) = \frac{1}{q+1}$$

let $S_2(m,m') = \frac{1}{N(m',0;m,0;n)} = \frac{\prod_{i=1}^{m'}(q^{2i}-1)}{\prod_{i=m-m'+1}^{m}(q^{2i}-1)}, (1 \le m' < m \le \nu)$

Obviously, m is smaller as $S_2(m,m')$ is larger, and

$$S_2(m'+1,m') = \frac{q^2-1}{(q^{2(m'+1)}-1)}$$

so

$$\max_{1\le m'<m\le\nu}\{S_2(m,m')\} = S_2(2,1) = \frac{1}{q^2+1}$$

Therefore

$$P_S = \max\{\max_{1\le m<m'\le\nu}\{S_1(m,m')\}, \max_{1\le m'<m\le\nu}\{S_2(m,m')\}\} = \frac{1}{q+1}$$

□

Theorem. *The above construction yields a Cartesian code with size parameters*

$$\begin{aligned}\mathbb{S} &= \{S \mid S =< e_1, e_2, \cdots, e_m >\},\\ \mathbb{E} &= U_n(\mathbb{F}_{q^2}),\\ \mathbb{M} &= \{M \mid M \textit{ is a subspace of type } (m,0)\},\end{aligned}$$

where $N(m,0;n)$ is given in [10]. Moreover, assume that the encoding rules are chosen according to a uniform probability distribution, and denote the largest probabilities of a successful impersonation attack and of a successful substitution attack by P_I and P_S, respectively. Then

$$P_I = \frac{q^2-1}{(q^{n-1}-(-1)^{n-1})(q^n-(-1)^n)}, P_S = \frac{1}{q+1}$$

REFERENCES

1. G.J.Simmons, *Authentication theory/Coding theory[A],* Advances in Cryptology, Proceedings of Crypto 84, Lecture Notes in Computer Science, 196 Springer (1985), 411-431.
2. Wan ZheXian, *Construction of Cartesian authentication codes from unitary geometry[J], Designs, codes and cryptography,* **2**(1992), 333-356.
3. Li Li, *Using non Trivial Idempotent Matrices over Finite Fields to Construct Cartesian Authentication Codes[J],* Journal of Mathematics, **17(4)**(1997), 487-490.
4. Zheng Baodong, *Construction of Authentication Codes from Involutory Matrix Over Finite Fields[J],* Journal of Mathematics, **19(3)**(1999),263-269(In Chinese)
5. YOU Hong and GAO You, *Some new constructions of Cartesian authentication codes from symplectic geometry[J],* Systems Science and Mathematical Sciences, **7(4)**(1994), 317-327.
6. TAO Yayuan, *Construction of Cartesian Authentication Codes from Symplectic Geometry[J],* Journal of Hebei Polytechnic University (Natual Science Edition), **30(1)**(2008), 49-53(In Chinese)
7. Gao Suogang, *Two Constructions of Cartesian Authentication Codes from Unitary Geometry[J],* Applied Mathematics A Journal of Chinese University[A], **11(3)**(1996), 343-353(In Chinese)

8. GAO You and TAO Yayuan, *Construction of Cartesian Authentication Codes from Alternate Matrices over finite fields[J],* Applied Mathematics A Journal of Chinese Universities, **22(4)**(2007), 385-390(In Chinese)
9. Gao Suogang and Li Zengti, *A construction of Cartesian authentication code from symplectic geometry[J],* Journal of Northeast normal university, **34(4)**(2002), 20-25(In Chinese)
10. Wan ZheXian, *Geometry of Classical Groups over Finite Fields (Second Edition)[M],* Beijing/New York:Science Press, 2002.

Wenyan Xu is a associate professor in Inner Mongolia WuLaqub Occupational College,Her research interests focus on Algebra, Coding and Cryptography.

Inner Mongolia WuLaqub Occupational College,Inner Mongolia Jining 01200, P.R. China
E-mail: xwy8831099@163.com

You Gao received his Ph.D in Basic mathematics from Harbin Institute of Technology and now is a professor in Civil Aviation University of China. His research interests focus on Algebra, Coding and Cryptography.

College of Science, Civil Aviation University of China, Tianjin 300300, P.R. China.
e-mail: gao_you@263.net