Journal of Mathematical Research & Exposition
Vol. 18, No. 3, 341 - 346, August 1998

Using Normal Form of Matrices over Finite Fields to Construct Cartesian Authentication Codes *

You Hong
(Dept. of Math. Harbin Institute of Technology, Harbin 150001)

Nan Jizhu
(Dept. of Math. Veterinary University, Changchun 130062)

Abstract In this paper, one construction of Cartesian authentication codes from the normal form of matrices over finite fields are presented and its size parameters are computed. Moreover, assume that the encoding rules are chosen according to a uniform probability distribution, the P_I and P_S, which denote the largest probabilities of a successful impersonation attack and of a successful substitution attack respectively, of these codes are also computed.

Keywords cartesian authentication codes, finite field, normal form of matrices.

Classification AMS(1991) 94A60/CCL O157.4

1. Introduction

Let S, E and M be three non - empty finite sets and let $f: S \times E \rightarrow M$ be a map. The four tuple $(S, E, M; f)$ is called an authentication code [2,3], if

(1) the map $f: S \times E \rightarrow M$ is surjective and

(2) for any $m \in M$ and $e \in E$ there is an $s \in S$ such that $f(s, e) = m$,

then such an s is uniquely determined by the given m and e. Suppose that $(S, E. M; f)$ is an authentication code, we call S, E, and M the set of source states, the set of encoding rules, and the set of messages respectively, and call f he encoding map. The cardinals $|S|$, $|E|$, $|M|$ are called the size parameters of the code. Let $s \in S$, $e \in E$, and $m \in M$ be such that $m = f(s, e)$. Then we say that the message m contains the encoding rule e. 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 every encoding rule e contained in m, then the code is called a Cartesian authentication code.

Some authentication codes based on projective geometry over finite fields were constructed in [1]. Projective geometry, according to Klein's Erlangen Program, is the geometry of the projective general linear group. Wan[3,4,5] used symplectic and unitary groups over finite fields to construct Cartesian

* Received October 4, 1995. This preject is supported by Heilongjiang Natural Science Foundation.

authentication codes. In the present paper, one construction of Cartesian authentication code from the normal form of matrices over finite fields are presented and its size parameters are computed. Moreover, assume that the encoding rules are chosen according to a uniform probability distribution, the P_I and P_S, which denote the largest probabilities of a successful impersonation attack and of a successful substitution attack respectively (see [3]), of these codes are also computed. Comparing with the geometry method of constructions of Cartesian authentication codes, we see that the matrix method is simpler and better in some way. Before this paper, we have not seen using matrix method to construct Cartesian authentication codes.

Let F_q be a finite field containing $q > 2$ elements. Denote by $M^*_{n,t}(F_q)$ the set of all nonzero n by t $(2 \leq n \leq t)$ matrices over the field F_q, and denote by $GL_n(F_q)$ the general linear group consisting of all n by n invertible matrices over F_q.

Set

$$N = \left\{ \begin{pmatrix} I_i & 0 \\ 0 & 0 \end{pmatrix}_{n \times t} : i = 1, 2, \cdots, n \right\},$$

$$G = (GL_n(F_q), GL_t(F_q)) = GL_n(F_q) \times GL_t(F_q).$$

2. Construction of cartesian authentication codes

Define the source state S to be the set N, the message M to be the set $M^*_{n,t}(F_q)$, and the encoding rules E to be the set G.

Define

$$f : S \times E \to M,$$

$$s \times (g_1, g_2) \to g_1 s g_2,$$

where $g_1 \in GL_n(F_q)$, $g_2 \in GL_t(F_q)$.

Since every n by t matrix over a field is equivalent to a "diagonal" form, i.e., a normal form, the map f is surjective. It is easy to show that the map f satisfies the second condition of the definition of authentication code. By the invariance of the rank of matrices under the "equivalent actions", we can show that given any message m there is a unique source state s such that $m = f(s, e)$ for every encoding rule e contained in m. Hence, the above construction yields a Cartesian authentication code.

Lemma 1 $|S| = n$, $|m| = q^{nt} - 1$, $|E| = q^{\frac{n(n-1)+t(t-1)}{2}} \prod_{i=1}^{n}(q^i - 1) \cdot \prod_{j=1}^{t}(q^j - 1)$.

Proof It is obvious that $|S| = n$, $|M| = q^{nt} - 1$. The cardinal $|E|$ follows from that

$$|GL_n(F_q)| = q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n}(q^i - 1) \quad \text{(see [6])}. \qquad \square$$

Lemma 2 *The number of encoding rules contained in a message is* $|GL_r(F_q)| \cdot |GL_{n-r}(F_q)| \cdot |GL_{t-r}(F_q)| \cdot q^{r(n+t-2r)}$, *where* $r = rank(M)$, *M is the given message.*

Proof Let M be a message, i. e., $M \in M^{*}_{n,t}(F_q)$. Assume rank$(M) = r$. Let $P = \begin{pmatrix} I_r & O \\ 0 & 0 \end{pmatrix}$ be a source state corresponding to M. The number of encoding rules contained in the message M is equal to the number of the solution of the pairs (U, V) which satisfy the equation $UPV = M$, where $U \in GL_n(F_q)$, $V \in GL_t(F_q)$. We know that there is at least a pair $(X, Y) \in GL_n(F_q) \times GL_t(F_q)$ such that

$$XPY = M. \tag{1}$$

So

$$X^{-1} UPV Y^{-1} = P. \tag{2}$$

Set

$$A = \{(U, V) \in GL_n(F_q) \times GL_t(F_q) : UPV = M\},$$
$$B = \{(X, Y) \in GL_n(F_q) \times GL_t(F_q) : XPY = P\}.$$

Define

$$\varnothing : A \to B,$$
$$(U, V) \to (X^{-1}U, VY^{-1}),$$

where (X, Y) is a fixed solution of the equation (1). It is not difficult to show that the map $\varnothing$ is injective. So the number of encoding rules contained in a message M is equal to the cardinal $|B|$. Then we shall compute the number $|B|$, i.e., the number of the solutions of the pairs $(X, Y) \in GL_n(F_q) \times GL_t(F_q)$ which satisfy the equation

$$XPY = P. \tag{3}$$

In fact we only need to compute the number of the pairs $(X, Y) \in GL_n(F_q) \times GL_t(F_q)$ which satisfy the equation

$$XP = PY. \tag{4}$$

Let

$$X = \begin{array}{c} \begin{array}{cc} r & n-r \end{array} \\ \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \end{array} \begin{array}{l} r \\ n-r \end{array}, \quad Y = \begin{array}{c} \begin{array}{cc} r & t-r \end{array} \\ \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix} \end{array} \begin{array}{l} r \\ t-r \end{array}$$

By the equation (4) we have

$$\begin{pmatrix} x_{11} & 0 \\ x_{21} & 0 \end{pmatrix} = \begin{pmatrix} y_{11} & y_{12} \\ 0 & 0 \end{pmatrix}. \tag{5}$$

This means that $x_{11} = y_{11}$, $x_{21} = 0$, $y_{12} = 0$. Hence

$$X = \begin{pmatrix} x_{11} & x_{12} \\ 0 & x_{22} \end{pmatrix}, \quad Y = \begin{pmatrix} y_{11} & 0 \\ y_{21} & y_{22} \end{pmatrix} \tag{6}$$

where $x_{11} = y_{11} \in GL_r(F_q)$, $x_{22} \in GL_{n-r}(F_q)$, and $y_{22} \in GL_{t-r}(F_q)$. Conversely, if X and Y have the form (6), then (X, Y) is a pair which satisfies the equation (4). Thus the number for choosing the pairs (X, Y) which have the form (6), i.e., the number of encoding rules contained in a message M is equal to

$$|GL_r(F_q)| \cdot |GL_{n-r}(F_q)| \cdot |GL_{t-r}(F_q)| \cdot q^{r(n-r)} \cdot q^{r(t-r)},$$

where r is the rank of M. $\square$

Lemma 3 *Let M_1 and M_2 be two distinct message which contain an encoding rule in common. Then the number of encoding rules contained in both M_1 and M_2 is equal to $|GL_{r_2}(F_q)| \cdot |GL_{r_1-r_2}(F_q)| \cdot |GL_{n-r_1}(F_q)| \cdot |GL_{t-r_1}(F_q)| \cdot q^{r_1(n+t-2r_1)}$*, where $\operatorname{rank}(M_1) = r_1$, $\operatorname{rank}(M_2) = r_2$, and $r_1 \geq r_2$.

Proof Let M_1 and M_2 be two distinct messages, $\operatorname{rank}(M_1) = r_1$ and $\operatorname{rank}(M_2) = r_2$ (without los of generality, assume $r_1 \geq r_2$).

Let $P_1 = \begin{pmatrix} I_{r1} & O \\ 0 & 0 \end{pmatrix}$ wh at be a source state, corresponding to M_1 and $P_2 = \begin{pmatrix} I_{r2} & O \\ 0 & 0 \end{pmatrix}$ be a source state corresponding to M_2. The number of encoding rules contained in both M_1 and M_2 is equal to the number of solutions of the pairs (X, Y) which satisfy the following equation

12

$$\begin{cases} XP_1 Y = M_1 \\ XP_2 Y = M_2 \end{cases} \tag{8}$$

where $M_2' = UM_2 V$ for some $U \in GL_n(F_q)$, $V \in GL_t(F_q)$.

By Lemma 2 we can assume that X, Y have the form

e f 6)

$$X = \begin{array}{c} \begin{array}{cc} r_1 & n-r_1 \end{array} \\ \begin{pmatrix} x_{11} & x_{12} \\ 0 & x_{12} \end{pmatrix} \end{array} \begin{array}{c} r_1 \\ n-r_1 \end{array}, \quad Y = \begin{array}{c} \begin{array}{cc} r_1 & t-r_1 \end{array} \\ \begin{pmatrix} x_{11} & 0 \\ y_{21} & y_{22} \end{pmatrix} \end{array} \begin{array}{c} r_1 \\ t-r_1 \end{array}, \tag{9}$$

where x_{11}, x_{22}, y_{22} are invertible.

Let

L 2

$$P_2 = \begin{pmatrix} I_{r2} & & O \\ & 0 & \\ & & 0 \end{pmatrix}.$$

By the second equation in (8) we have

$$x_{11} \begin{pmatrix} I_{r2} & 0 \\ 0 & 0 \end{pmatrix} x_{11}^{-1} = m_{11}, \tag{10}$$

where $M_2' = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$.

Note that the rank of m_{11} is r_2 and $m_{22} = 0$, $m_{12} = 0$, $m_{21} = 0$. Using the above line of argument in Lemma 2, we obtain that the number of x_{11} which satisfies (10) is equal to the number of the matrices having the form $\begin{pmatrix} \omega_1 & \\ & \omega_2 \end{pmatrix}$ where $\omega_1 \in GL_{r2}(F_q)$, $\omega_2 \in GL_{r1-r2}(F_q)$, so is equal to $|GL_{r2}(F_q)| \cdot |GL_{r1-r2}(F_q)|$. Observing (9) and using the above result, we obtain the number of encoding rules contained in both M_1 and M_2 is

$$|GL_{r2}(F_q)| \cdot |GL_{r1-r2}(F_q)| \cdot |GL_{n-r1}(F_q)| \cdot |GL_{t-r1}(F_q)| \cdot q^{r_1(n+t-2r_1)},$$

where $r_1 = \text{rank}(M_1)$, $r_2 = \text{rank}(M_2)$, and $r_2 \leq r_1$. $\square$

For convenient sake, let

$$\begin{aligned} f(r) &= |GL_r(F_q)||GL_{n-r}(F_q)||GL_{t-r}(F_q)| \cdot q^{r(n+t-2r)} \\ &= \prod_{i=1}^{r}(q^i - 1)\prod_{j=1}^{n-r}(q^j - 1)\prod_{k=1}^{t-r}(q^k - 1) \cdot q^{\frac{n(n-1)+t(t-1)+r(r-1)}{2}}, \end{aligned}$$

where r is the rank of a message M (see Lemma 2).

We have

$$\frac{f(r+1)}{f(r)} = \frac{q - \frac{1}{q^r}}{(q^{n-r} - 1)(q^{t-r} - 1)}. \tag{11}$$

Since $q \geq 3$, $2 \leq n \leq t$ and $r \geq 1$, $q - \frac{1}{q^r} < (q^{n-r} - 1)(q^{t-r} - 1)$ for all $1 \leq r \leq n - 1$. Then $\frac{f(r+1)}{f(r)} < 1$, so

$$f(n) < f(n-1) < \cdots < f(1). \tag{12}$$

Now assuming that the encoding rules are chosen according to a uniform probability distribution, we compute the probabilities of a successful impersonation attack P_I and of a successful substitution attack P_S. It follows from Lemma 1 and 2 and the result (12) that

$$P_I = \frac{q-1}{(q^n - 1)(q^t - 1)},$$

and follows from Lemma 2 and 3 and the result (12) that

$$\begin{aligned} &P_S(P_2 \mid P_1) \\ &= \max_{1 \leq r_2 < r_1 \leq n}\left\{\frac{|GL_{r_2}(F_q)||GL_{r_1-r_2}(F_q)||GL_{n-r_1}(F_q)||GL_{t-r_1}(F_q)|\, q^{r_1(n+t-2r_1)}}{f(r_1)}\right\} \\ &= [q(q+1)]^{-1}. \end{aligned}$$

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

$$|S| = n,$$
$$|M| = q^{nt} - 1,$$
$$|E| = \prod_{i=1}^{n}(q^i - 1)\prod_{j=1}^{t}(q^j - 1)\, q^{\frac{n(n-1)+t(t-1)}{2}}.$$

Assume that the encoding rules are chosen according to a uniform probability distribution, the probabilities of a successful impersonation attack P_I and of a successful substitution attack P_S are given by

$$P_I = \frac{q-1}{(q^n-1)(q^t-1)}$$

and

$$P_S = \frac{1}{q(q+1)}$$

respectively.

References

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

[2] G. Simmons, *Authentication theory/ secrecy theory*, *Advances in Cryptography*, Proc. of Crypto 84, Lecture Notes in Computer Science, No. 196, Springer, 1985, 411 - 431.

[3] Z. Wan, *Construction of Cartesian authentication codes from unitary geometry*, Designs, Codes and Cryptography, **2** (1992), 335 - 356.

[4] Z. Wan, *Further constructions of Cartesian authentication codes from symplectic geometry*, Northeastern Mathematical Journal, **8** (1992), 4 - 20.

[5] Z. Wan, B. Smeets and P. Vanroose, *On the construction of authentication codes over symplectic space*, Preprint.

[6] Z. Wan, *Geometry of classical groups over finite fields*, Student litteratur, Chart Well Bratt, Lund, Sweden, 1993.

利用有限域上矩阵的标准型构作卡氏认证码

游　宏

(**哈尔滨工业大学数学系**, 150001)

南 基 洙

(**解放军农牧大学基础部**, **长春** 130062)

摘　要

本文利用有限域上长方矩阵的等价标准型构作了一个笛卡尔认证码并计算出该码的所有参数. 进而,假定编码规则按照统一的概率分布所选取,该码的成功伪造与成功替换的最大概率 P_I 与 P_S 亦被计算出来.