两类 Cartesian 认证码的构造

刘金龙，许宗泽

(南京航空航天大学 信息科学与技术学院，江苏 南京 210016)

摘要：利用循环排法构造了一类最优 Cartesian 认证码，避免了其他构造法所借助的群(或域)上的复杂运算. 对于任意两个相互无关的参数 k，n，采用迭代法构造了一类信源数为 k，且使敌方模仿攻击和替换攻击成功的概率均为 $1/n$ 的 Cartesian 认证码；在相同参数 k，n 的条件下，与已知的笛卡尔积构造法相比，利用迭代法所构造的 Cartesian 认证码的编码规则数目减少了.

关键词：Cartesian 认证码；最优 Cartesian 认证码；正交排列

中图分类号：TN918 **文献标识码**：A **文章编号**：1001-2400(2007)03-0505-04

Construction of two sorts of cartesian authentication codes

LIU Jin-long, *XU Zong-ze*

(Dept. of Info. Sci. and Tech., Nanjing Univ. of Aeronaut. and Astronaut, Nanjing 210016, China)

Abstract: A method to construct one sort of optimal Cartesian authentication codes by using the cyclic array is presented. The method is easy to realize and it needs no complicated calculation over group or finite fields. Another iterative means to construct one class of Cartesian authentication codes with the k sources and $1/n$ probabilities of successful impersonation and substitution attack is also proposed, where parameters k and n are two arbitrary positive integers. Compared with the Cartesian authentication codes constructed by Descartes product, the authentication codes produced by iterative means have far fewer encoding rules, when they contain the same parameters k and n.

Key Words: Cartesian authentication codes; the optimal Cartesian authentication codes; orthogonal arrays

在 Simmons[1] 消息认证模型中，一个没有仲裁的认证码由发方、收方和敌方组成. 收发双方相互信任，而敌方试图欺骗收方. 假定除发收双方共同约定的编码规则保密外，整个认证系统是公开的. 敌方的攻击有两种：模仿攻击和替换攻击. 若敌方发送一个假消息给收方，收方将其当作合法消息接收，则认为敌方攻击成功. 通常用 S 表示信源集合，M 表示消息集合，E 表示编码规则集合，P_I，P_S 分别表示敌方模仿和替换攻击成功的概率. 对于一个认证码，若敌方根据信道中截获的消息即可判断其对应的信源，则称之为 Cartesian 认证码.

一个由 n 个符号构成的 $\lambda n^2 \times k$ 排列，若任意两列中有 λ 个行对应着 n 个元素构成的 n^2 个序对中的任一对，则称该排列为正交排列，记为 $\mathrm{OA}(n,k,\lambda)$. 由文献[2] 可知，若存在一个 $\mathrm{OA}(n,k,\lambda)$，则可以构造一个参数为：$|S|=k$，$|E|=\lambda n^2$，$|M|=kn$ 的 Cartesian 认证码，当 S 和 E 分布等概时，有 $P_I=P_S=1/n$. 对于一个 Cartesian 认证码，若其参数为：$|S|=n+1$，$|E|=n^2$，$|M|=kn$ 且 $P_I=P_S=1/n$，则称之为最优 Cartesian 认证码[2].

1 Cartesian 认证码的构造

1.1 利用循环排列构造一类最优 Cartesian 认证码

Cartesian 认证码的构造问题就其本质来说是一个组合设计问题. 迄今为止，国内外众多学者对

收稿日期：2006-06-29

基金项目：国家部委预研基金资助(112031)

作者简介：刘金龙(1976-)，男，南京航空航天大学博士研究生.

Cartesian 认证码的组合特性进行了详细分析,并构造出多类性能良好的认证码[3~6]. 通常,Cartesian 认证码的构造都是基于群(或域),并借助较为复杂的运算来实现. 而笔者则提出了一种利用简单的循环排列来构造最优 Cartesian 认证码的方法.

构造 1 设 q 为素数,$z_i(i=0,1,\cdots,q-1)$ 表示任意 q 个不同的元素,$\boldsymbol{a}=[z_0,z_1,\cdots,z_{q-1}]^{\mathrm{T}}$,$\boldsymbol{a}_i=[\underbrace{z_i,z_i,\cdots,z_i}_{q\text{个}z_i}]^{\mathrm{T}}$ $(i=0,1,\cdots,q-1)$;设 f 是一循环移位函数,定义 $f^{(j)}(\boldsymbol{a})=[z_{0+j},z_{1+j},\cdots,z_{q-1+j}]^{\mathrm{T}}$,$i+j$ $(i=0,1,\cdots,q-1)$ 表示模 q 加;构造如下矩阵

$$\boldsymbol{A}=\begin{bmatrix} f^{(0\times 0)}(\boldsymbol{a}) & f^{(0\times 1)}(\boldsymbol{a}) & \cdots & f^{(0\times(q-1))}(\boldsymbol{a}) & \boldsymbol{a}_0 \\ f^{(1\times 0)}(\boldsymbol{a}) & f^{(1\times 1)}(\boldsymbol{a}) & \cdots & f^{(1\times(q-1))}(\boldsymbol{a}) & \boldsymbol{a}_1 \\ \vdots & \vdots & & \vdots & \vdots \\ f^{((q-1)\times 0)}(\boldsymbol{a}) & f^{((q-1)\times 1)}(\boldsymbol{a}) & \cdots & f^{((q-1)\times(q-1))}(\boldsymbol{a}) & \boldsymbol{a}_{q-1} \end{bmatrix},$$

其中 $f^{(i\times j)}(\boldsymbol{a})(i,j=0,1,\cdots,q-1)$ 中的 $i\times j$ 表示模 q 乘.

设矩阵 $\boldsymbol{A}$ 的第 i 行,第 j 列的元素为 $a_{ij}(i=0,1,\cdots,q^2-1;j=0,1,\cdots,q)$,且有 $a_{ij}\in\{z_k:k=0,1,\cdots,q-1\}$. 设 s_j $(j=0,1,\cdots,q)$ 表示 $q+1$ 个信源,e_i $(i=0,1,\cdots,q^2-1)$ 表示 q^2 个编码规则,$e_i(s_j)\to(s_j,a_{ij})$ $(i=0,1,\cdots,q^2-1;j=0,1,\cdots,q)$ 表示信源 s_j 在编码规则 e_i 下映射成消息 (s_j,a_{ij}). 假定信源和编码规则分布等概,则可以得到一个 Cartesian 认证码.

引理 1 矩阵 $\boldsymbol{A}$ 的前 q 列构成一个 $\mathrm{OA}(q,q,1)$.

证明 假设矩阵 $\boldsymbol{A}$ 的前 q 列不是一个 $\mathrm{OA}(q,q,1)$,则必定存在某两行、两列相交处的元素 $a_{i_1q+j_1,k_1}$,$a_{i_2q+j_2,k_1}$,$a_{i_1q+j_1,k_2}$,$a_{i_2q+j_2,k_2}$ $(i_1,i_2,j_1,j_2,k_1,k_2\in\{0,1,\cdots,q-1\})$,满足以下方程

$$\begin{cases} a_{i_1q+j_1,k_1}=a_{i_2q+j_2,k_1}, \\ a_{i_1q+j_1,k_2}=a_{i_2q+j_2,k_2}. \end{cases} \tag{1}$$

且 $k_1\neq k_2$,$i_1q+j_1\neq i_2q+j_2$.

根据构造过程,可将式(1)写成如下形式

$$\begin{cases} z_{i_1k_1+j_1}=z_{i_2k_1+j_2}, \\ z_{i_1k_2+j_1}=z_{i_2k_2+j_2}. \end{cases} \tag{2}$$

若式(2)成立,则

$$\begin{cases} i_1k_1+j_1=i_2k_1+j_2 \pmod q, \\ i_1k_2+j_1=i_2k_2+j_2 \pmod q, \end{cases} \tag{3}$$

由式(3)可得

$$(i_1-i_2)(k_1-k_2)=0 \pmod q. \tag{4}$$

因为 $|i_1-i_2|<q$,$|k_1-k_2|<q$ 且 q 为素数,所以仅当 $i_1=i_2$ 或 $k_1=k_2$ 时,式(4)才成立. 于是解得 $k_1=k_2$ 或 $i_1q+j_1=i_2q+j_2$,这与假设相矛盾,于是可知 $\boldsymbol{A}$ 的前 q 列构成一个 $\mathrm{OA}(q,q,1)$.

引理 2 矩阵 $\boldsymbol{A}$ 是一个 $\mathrm{OA}(q,(q+1),1)$.

证明 由构造过程易知,$\boldsymbol{A}$ 的第 $q+1$ 列与其他任意一列均构成 $\mathrm{OA}(q,2,1)$,结合引理 1 即知 $\boldsymbol{A}$ 是一个 $\mathrm{OA}(q,(q+1),1)$.

定理 1 由构造 1 所得到的认证码是最优 Cartesian 认证码,其参数为:$|S|=q+1$,$|E|=q^2$,$|M|=q(q+1)$;当 S 和 E 分布等概率时,敌方模仿攻击和替换攻击成功的概率均为 $1/q$.

证明 由引理 2 知,$\boldsymbol{A}$ 是一个 $\mathrm{OA}(q,(q+1),1)$,$\boldsymbol{A}$ 的 $q+1$ 列对应着 $q+1$ 个信源,$\boldsymbol{A}$ 的 q^2 行对应着 q^2 个编码规则,$q+1$ 个信源与 q 个 z_i $(i=0,1,\cdots,q-1)$ 可以组合成 $q(q+1)$ 个消息.

设 $(s_i,z_j)(i=0,1,\cdots,q;j=0,1,\cdots q-1)$ 为敌方模仿攻击采用的任一消息,因为 $\boldsymbol{A}$ 是 $\mathrm{OA}(q,(q+1),1)$,所以 $|\{e:e(s_i)\to(s_i,z_j)\}|=q$. 又因为 $|E|=q^2$,所以,当 S,E 分布等概时,敌方模仿攻击成功的概率 $P_I=1/q$.

设 (s_{i_1},z_{j_1}) 表示敌方在信道中获得的一个消息,$(s_{i_2},z_{j_2})(i_1,i_2=0,1,\cdots,q;i_1\neq i_2)$ 为敌方替换攻击采用的另一不同的消息. 因为 $\boldsymbol{A}$ 为 $\mathrm{OA}(q,(q+1),1)$,于是有

$$|\{e:e(s_{i_1})\to(s_{i_1},z_{j_1})\}|=q,\quad |\{e:e(s_{i_1})\to(s_{i_1},z_{j_1}),e(s_{i_2})\to(s_{i_2},z_{j_2})\}|=1.$$

所以,敌方替换攻击成功的概率 $P_S=1/n$.

1.2　利用迭代法构造 $|S|=k, P_I=P_S=1/n$ 的 Cartesian 认证码

对于任意两个相互无关的参数 n,k,构造信源数目为 k,敌方模仿攻击和替换攻击成功的概率均为 $1/n$ 的认证码是认证理论研究的一个重要问题. 迄今为止,相关的构造方法很少,文献[2]给出了一种满足上述要求的笛卡尔积构造法,其缺点是编码规则数目太大. 针对其不足,这里提出了一种迭代构造法.

1.2.1　构造及证明

构造 2　设 $k>1, n>1, q$ 为 n 的最小素因数,令 $k=q^t+r(0\leqslant r<q^{t+1}-q^t)$;设 $\{z_i; i=0,1,\cdots,n-1\}$ 表示 n 个不同的元素的集合;设 $\boldsymbol{A}$ 为一矩阵且满足条件:$\boldsymbol{A}$ 中的任意元素 $a_{ij}\in\{z_i: i=0,1,\cdots,n-1\}$ 且 $a_{ij}=z_u$,定义函数 $f^{(l)}(\boldsymbol{A}): f^{(l)}(\boldsymbol{A})(a_{ij})\to z_{u+l}$,$u+l$ 表示模 n 加;设 $\boldsymbol{a}=[z_0,z_1,\cdots,z_{n-1}]^{\mathrm{T}}$,利用 $\boldsymbol{a}$ 构造 $\boldsymbol{A}_0$ 如下

$$\boldsymbol{A}_0=\begin{bmatrix} f^{(0\times 0)}(\boldsymbol{a}) & f^{(0\times 1)}(\boldsymbol{a}) & \cdots & f^{(0\times(q-1))}(\boldsymbol{a}) \\ f^{(1\times 0)}(\boldsymbol{a}) & f^{(1\times 1)}(\boldsymbol{a}) & \cdots & f^{(1\times(q-1))}(\boldsymbol{a}) \\ \vdots & \vdots & & \vdots \\ f^{((n-1)\times 0)}(\boldsymbol{a}) & f^{((n-1)\times 1)}(\boldsymbol{a}) & \cdots & f^{((n-1)\times(q-1))}(\boldsymbol{a}) \end{bmatrix}.$$

经过 t 次迭代后,可得

$$\boldsymbol{A}_t=\begin{bmatrix} f^{(0\times 0)}(\boldsymbol{A}_{t-1}) & f^{(0\times 1)}(\boldsymbol{A}_{t-1}) & \cdots & f^{(0\times(q-1))}(\boldsymbol{A}_{t-1}) \\ f^{(1\times 0)}(\boldsymbol{A}_{t-1}) & f^{(1\times 1)}(\boldsymbol{A}_{t-1}) & \cdots & f^{(1\times(q-1))}(\boldsymbol{A}_{t-1}) \\ \vdots & \vdots & & \vdots \\ f^{((n-1)\times 0)}(\boldsymbol{A}_{t-1}) & f^{((n-1)\times 1)}(\boldsymbol{A}_{t-1}) & \cdots & f^{((n-1)\times(q-1))}(\boldsymbol{A}_{t-1}) \end{bmatrix}.$$

若 $t=0$,则从 $\boldsymbol{A}_0$ 中任意选取 k 列作为编码矩阵 $\boldsymbol{A}$. 若 $t>0$,则分两种情况选取编码矩阵:① 当 $r=0$ 时,则以 $\boldsymbol{A}_t$ 作为编码矩阵 $\boldsymbol{A}$;② 当 $0<r<q^{t+1}-q^t$ 时,则从 $\boldsymbol{A}_{t+1}$ 中取出任意 k 列作为编码矩阵 $\boldsymbol{A}$. 设编码矩阵 $\boldsymbol{A}$ 的第 i 行、第 j 列的元素为 a_{ij},且有 $a_{ij}\in\{z_k: k=0,1,\cdots,n-1\}$. 并以 $e_i(s_j)\to(s_j,a_{ij})$ 表示信源 s_j 在编码规则 e_i 下映射成消息 (s_j,a_{ij}). 假定信源和编码规则分布等概,则可以得到一个 Cartesian 认证码.

注　当 $k=1$ 时,用 n 个不同元素构作一个 $n\times 1$ 阶的矩阵作为消息编码矩阵,即可构造满足条件的 Cartesian 认证码;当 $n=1$ 时,用 k 个不同元素构作一个 $1\times k$ 阶的矩阵作为消息编码矩阵,也可构造满足条件的 Cartesian 认证码.

引理 3　若 $\boldsymbol{X}$ 是一个 $\mathrm{OA}(n,2,\lambda)$,函数 f 的定义同构造 2,则

$$\boldsymbol{Y}=\left[f^{(l_0)}(\boldsymbol{X}^{\mathrm{T}})\quad f^{(l_1)}(\boldsymbol{X}^{\mathrm{T}})\quad\cdots\quad f^{(l_{n-1})}(\boldsymbol{X}^{\mathrm{T}})\right]^{\mathrm{T}}$$

构成一个 $\mathrm{OA}(n,2,n\lambda)$.

证明　设 $x_i(i=0,1,\cdots,n-1)$ 是 $\boldsymbol{X}$ 中的 n 个不同符号,(x_i,x_j) 为 $\boldsymbol{X}$ 的任一有序对. 于是有 $f^{(l_k)}(x_i,x_j)\to(x_{i+l_k},x_{j+l_k})$,其中 $i+l_k, j+l_k$ 均为模 n 加. 因为有序对 (x_i,x_j) 在 $\boldsymbol{X}$ 中出现的次数为 λ,所以有序对 (x_{i+l_k},x_{j+l_k}) 出现的次数也是 λ. 因为 $i+l_k, j+l_k\in\{0,1,\cdots,n-1\}$,所以 $f^{(l_k)}(\boldsymbol{X})$ 仍是一个 $\mathrm{OA}(n,2,\lambda)$. 又因为 $k=0,1,\cdots,n-1$,所以 $\boldsymbol{Y}$ 构成一个 $\mathrm{OA}(n,2,n\lambda)$.

引理 4　若 $\boldsymbol{X}$ 是一个 $\mathrm{OA}(n,2,\lambda)$,$\boldsymbol{X}_1,\boldsymbol{X}_2$ 分别为 $\boldsymbol{X}$ 的两个列向量,函数 f 的定义同构造 2,则

$$\boldsymbol{Y}=\begin{bmatrix} f^{(l_0)}(\boldsymbol{X}_1^{\mathrm{T}}) & f^{(l_1)}(\boldsymbol{X}_1^{\mathrm{T}})\cdots & f^{(l_{n-1})}(\boldsymbol{X}_1^{\mathrm{T}}) \\ f^{(d_0)}(\boldsymbol{X}_2^{\mathrm{T}}) & f^{(d_1)}(\boldsymbol{X}_2^{\mathrm{T}})\cdots & f^{(d_{n-1})}(\boldsymbol{X}_2^{\mathrm{T}}) \end{bmatrix}^{\mathrm{T}}$$

构成一个 $\mathrm{OA}(n,2,n\lambda)$.

证明　设 $x_i(i=0,1,\cdots,n-1)$ 是 $\boldsymbol{X}$ 中的 n 个不同符号,(x_i,x_j) 为 $\boldsymbol{X}$ 的任一有序对,x_i,x_j 分别是 $\boldsymbol{X}_1$,$\boldsymbol{X}_2$ 中的元素. 于是有 $[f^{(l_k)}(x_i),f^{(d_k)}(x_j)]\to(x_{i+l_k},x_{j+d_k})$,其中 $i+l_k, j+d_k$ 均为模 n 加. 因为有序对 (x_i,x_j) 在 $\boldsymbol{X}$ 中出现的次数为 λ,所以有序对 (x_{i+l_k},x_{j+d_k}) 出现的次数也是 λ. 因为 $i+l_k, j+d_k\in\{0,1,\cdots,n-1\}$,所以 $[f^{(l_k)}(\boldsymbol{X}_1),f^{(d_k)}(\boldsymbol{X}_2)]$ 仍是一个 $\mathrm{OA}(n,2,\lambda)$. 又因为 $k=0,1,\cdots,n-1$,所以 $\boldsymbol{Y}$ 构成一个 $\mathrm{OA}(n,2,n\lambda)$.

引理 5　设矩阵 $\boldsymbol{X}$ 是一个 $\mathrm{OA}(n,2,\lambda)$,$\boldsymbol{X}_1$ 为 $\boldsymbol{X}$ 的任一列向量,函数 f 的定义同构造 2,若 $j,k\in\{0,1,\cdots,n-1\}$,且当 $j\neq k$ 时,有 $l_j-d_j\neq l_k-d_k \bmod n$ 成立,则

$$\boldsymbol{Y}=\begin{bmatrix} f^{(l_0)}(\boldsymbol{X}_1^{\mathrm{T}}) & f^{(l_1)}(\boldsymbol{X}_1^{\mathrm{T}})\cdots & f^{(l_{n-1})}(\boldsymbol{X}_1^{\mathrm{T}}) \\ f^{(d_0)}(\boldsymbol{X}_1^{\mathrm{T}}) & f^{(d_1)}(\boldsymbol{X}_1^{\mathrm{T}})\cdots & f^{(d_{n-1})}(\boldsymbol{X}_1^{\mathrm{T}}) \end{bmatrix}^{\mathrm{T}}$$

构成一个 $\mathrm{OA}(n,2,n\lambda)$.

证明 根据条件可将 Y 写成另一种等效形式的矩阵 Y'

$$Y'=\begin{bmatrix} X_1 & X_1 & \cdots & X_1 \\ f^{(0)}(X_1) & f^{(1)}(X_1) & \cdots & f^{(n-1)}(X_1) \end{bmatrix}.$$

设 $x_i(i=0,1,\cdots,n-1)$ 是 X 中的 n 个不同符号,在任意一对$[X_1, f^{(k)}(X_1)]$构成的矩阵中,有序对(x_i, x_{i+k})出现 $n\lambda$ 次,因为 i,k 是任意选取的,所以 Y' 构成一个 $\mathrm{OA}(n,2,n\lambda)$. 又因为 Y' 可以经过基本的行列置换得到 Y,且其正交性不变,所以 Y 也是一个 $\mathrm{OA}(n,2,n\lambda)$.

定理 2 由构造 2 得到的 Cartesian 认证码具有参数:$|S|=k$, $|M|=kn$, $|E|$ 分两种情况讨论:

① 当 $k\leqslant q$(q 是 n 的最小素因数)时,编码规则数目 $|E|=n^2$;

② 当 $k>q$ 时,编码规则数目 $|E|=n^{\lceil \log_q k \rceil+1}$($\lceil x \rceil$为向上取整符号).

当 S,E 分布等概时,敌方模仿攻击和替换攻击成功的概率均为$1/n$.

证明 类似引理 1 的证明方法可以证明 A_0 是一个 $\mathrm{OA}(n,q,1)$. 当$k\leqslant q$时,编码矩阵 A 是一个 $\mathrm{OA}(n,k,1)$;当$k>q$时,利用数学归纳法结合引理 $2\sim$ 引理 4,易证:A_t 是一个 $\mathrm{OA}(n,q^t,n^{t-1})$,所以编码矩阵 A 是一个 $\mathrm{OA}(n,k,n^{\lceil \log_q k \rceil-1})$. 所以当 S 和 E 分布等概时,有 $P_I=P_S=1/n$.

1.2.2 **性能分析**

(1) 当 $k>1, n>1$ 且 $k\leqslant q+1$(q 为 n 的最小素因数)时,迭代法所需要的编码规则数目 $|E|=n^2$,而笛卡尔积法所需要的编码规则数为 $|E'|=n^k$, $|E'|\geqslant|E|$.

(2) 当 $k>1, n>1$ 且 $k>q+1$(q 为 n 的最小素因数)时,迭代法所需要的编码规则数目 $|E|=n^{\lceil \log_q k \rceil+1}$,而笛卡尔积法所需要的编码规则数 $|E'|=n^k$, $|E'|>|E|$. 若 n 为素数时,随着 k 的增加,用迭代法构造的 Cartesian 认证码的编码规则数目 $|E|$ 近似呈线性增长;而用笛卡尔积法构造的 Cartesian 认证码的编码规则数目 $|E'|$ 则呈指数级增长.

2 结 束 语

迄今为止,多数 Cartesian 认证码的构造是通过群(或域)上的运算来实现的. 笔者利用循环排列法得到了一类最优 Cartesian 认证码,且有效地避免了较为复杂的运算,该方法简单易行,易于软硬件实现.

当 n,k 为两个相互无关的参数时,文中利用迭代法构造出了信源数目为 k,敌方模仿攻击和替换攻击成功的概率均为$1/n$ 的 Cartesian 认证码. 在相同 n,k 的条件下,与笛卡尔积构造法相比,迭代法构造的 Cartesian 认证码的编码规则数目大为减少.

参考文献:

[1] Simmons G J. Authentication Theory/Coding Theory[C]//Advances in Cryptology-CRYPTO'85. Berlin: Springer-Verlag, 1984: 411-431.

[2] Wang Xinmei, Ma Wenping, Wu Chuankun. Theory of Cryptology Based on Error-correcting Codes[M]. Beijing: Posts & Telecom Press, 2001.

[3] Li Dinglong, Zhai Hongchun. A Simple Construction of Cartesian Authentication Codes[J]. Journal of Southern Yangtze University, 2004, 3(5): 541-543.

[4] Zhou Qi, Wang Dengyin. Using Normal Form of Anti-symmetric Matrices over Finite Fields to Construct Cartesian Authentication Codes[J]. Journal of Mathematical Study, 2004, 37(1): 42-47.

[5] Li Zengti, Yin Chengli. A Construction of Cartesian Authentication Code from Orthogonal Geometry of Finite Fields of Odd Characteristic[J]. Journal of Hebei University (Natural Science Edition), 2006, 26(2):142-147.

[6] Gilberto B. A-codes from Rational Functions over Galois Rings[J]. Designs, Codes and Cryptography, 2006, 39(2): 207-214.

(编辑:齐淑娟)