利用 Cartesian 认证码构造安全认证码

刘金龙　　许宗泽
(南京航空航天大学信息科学与技术学院　南京　210016)

摘　要：该文提出了一种利用 Cartesian 认证码构造安全认证码的方法，该方法借助拉丁方，在保持编码规则不变的情况下，将最佳 Cartesian 认证码改造成完备安全的认证码。

关键词：Cartesian 认证码；正交排列；安全认证码；拉丁方
中图分类号：TN918　　**文献标识码**：A　　**文章编号**：1009-5896(2007)08-2026-03

Secret Authentication Codes from Cartesian Authentication Codes

Liu Jin-long　　Xu Zong-ze
(*College of Info. Sci. and Tech.*, *Nanjing Univ. of Aeronaut. and Astronaut.*, *Nanjing* 210016, *China*)

Abstract: A method to construct secret authentication codes by using Cartesian codes is presented in the paper. On the condition of not changing the quantity of encoding rules, the proposed method uses Latin square to reconstruct the optimum Cartesian authentication codes into perfect secret authentication codes.

Key words: Cartesian authentication codes; Orthogonal arrays; Secret authentication; Latin square

1　引言

在Simmons[1]消息认证模型中，一个没有仲裁的认证码由三方组成：发方、收方和敌方。发方和收方相互信任，共同约定编码规则，而敌方试图欺骗收方。发方将信源编码成消息经过信道传送给收方，收方收到消息后还要验证消息是否来自合法的发方。假定除发、收双方共同约定的编码规则保密外，整个认证码是公开的。敌方的攻击有两种：模仿攻击和替换攻击。在发方没有发送任何消息的情况下，敌方通过公开信道发送一个消息给收方，希望收方将其作为合法消息接收，称为模仿攻击；若敌方截获到一个发方发送给收方的消息，并用另一个代表不同信源的消息替换截获到的消息，希望收方将其作为合法消息接收，称为替换攻击。

通常，用 S 表示具有 k 个信源的集合，M 表示包含 v 个的消息集合，E 表示包含 b 个编码规则的集合，P_I 表示敌手模仿攻击成功的概率，P_S 表示敌手替换攻击成功的概率，并以 AC(k,v,b) 标记一个认证码。一个编码规则 $e\in E$，指 e 是一个从 S 到 M 的映射。认证码也可以用一个 $b\times k$ 阶编码矩阵表示，行标、列标分别由编码规则和信源所决定，其第 e 行 s 列的元素记为 $e(s)$。若一个认证码满足：给定任意消息 m，有唯一的信源 s，使得 $m=e(s)$，则称之为 Cartesian 认证码。

迄今为止，国内外的众多学者对 Cartesian 认证码的组合特性进行了详细分析，并采用多种方法构造出多类性能很好的Cartesian认证码，如文献[2–4]等，而有关利用Cartesian认证码构造安全认证码的文献很少。通常，将一个 Cartesian 认证码改造成一个安全认证码，其编码规则要增加。怎样在编码规则不增加的情况下，将 Cartesian 认证码改造成安全认证码是认证码研究的一个重要问题。本文给出了一种在保持编码规则不变的条件下，将最佳 Cartesian 认证码改造成完备安全认证码的方法。

2006-06-14 收到，2006-11-22 改回

2　Cartesian 认证码的相关知识

定义 1[5]　一个由 n 个符号构成的 $\lambda n^2\times k$ 排列，如满足在任意的两列，由 n 个元素构成的 n^2 个序对中的任一序对都出现在这两列的 λ 个行中，这个排列称作正交排列，记为 $\mathbf{OA}(n,k,\lambda)$。

定理 1[5]　若存在一个 OA$(n,k,1)$，则 $k\le n+1$。

定理 2[5]　对于一个Cartesian认证码，若编码规则均匀分布，且 $P_I=P_S=1/l$，则其认证码是一个正交排列 OA(n,k,λ)；反之，若存在一个正交排列 OA(n,k,λ)，则可以构造一个Cartesian认证码具有 k 个信源，λn^2 个编码规则，信源和编码规则分布等概，且 $P_I=P_S=1/l$。

定理 3[5]　若一个Cartesian认证码有 k 个信源，kn 个消息，$P_I=P_S=1/n$，则 $b\ge k(n-1)+1$，当且仅当编码矩阵是一个正交排列 OA(n,k,λ) 时，等式成立，其中 $\lambda=(k(n-1))/n^2$，且编码规则分布等概。

定义 2[5]　对一个 Cartesian 认证码，若 $\log_2 P_I=\log_2 P_S=-I(M;E)$，则称为完备Cartesian认证码。

由以上的定义和定理可知，若 $P_I=P_S=1/n$，最佳 Cartesian 认证码具有如下参数：$|S|=n+1$，$|E|=n^2$，$|M|=n(n+1)$。即最佳 Cartesian 认证码是编码规则最少，信源数目最多，且使敌方模仿和替换攻击成功的概率都达到最小的认证码。

目前，有关最佳 Cartesian 认证码的构造方法有很多，如文献[6]提出的投影平面构造法，文献[7]采用的有限域和初等代数方法等。

3　利用最佳 Cartesian 认证码构造完备安全认证码

3.1 安全认证码和拉丁方的基本概念

定义 3[5]　对于一个认证码，若对手在信道获得一个消息 m，对于任意信源 s，有 $P(s\mid m)=P(s)$，称该认证码为安全认证码。

定义 4[8]　设 N 是一个 n 元集，若有元素全在 N 上的一个 $n\times n$ 阶阵列 $\boldsymbol{L}$，其每一行与每一列都是集合 N 的一个全排列，则称 $\boldsymbol{L}$ 是 N 上的一个 n 阶拉丁方。

有关拉丁方的设计方法很多，参考文献[9]。下面，本文给出拉丁方的平凡构造方法。

拉丁方的构造　设 $N=\{a_i:i=1,2,\cdots,n\}$，依次构造 n 阶置换矩阵 $\boldsymbol{P}_1,\boldsymbol{P}_2,\cdots,\boldsymbol{P}_n$，并满足 $\sum_{i=1}^{n}\boldsymbol{P}_i=\boldsymbol{J}$，$\boldsymbol{J}$ 为 n 阶全一矩阵；再用 a_i 替换 $\boldsymbol{P}_i$ 中的非零元素得到 $\boldsymbol{P}_i'$，$i=1,2,\cdots,n$；于是可得拉丁方 $\boldsymbol{L}=\sum_{i=1}^{n}\boldsymbol{P}_i'$。

证明　由以上的构造过程可知，集合 N 中任意元素 a_i，在每行、每列均出现一次，由 a_i 的任意性可得，矩阵 $\sum_{i=1}^{n}\boldsymbol{P}_i'$ 每一行、每一列均包含了 N 中的 n 个不同元素，所以 $\sum_{i=1}^{n}\boldsymbol{P}_i'$ 为 n 阶拉丁方。

通过改变置换矩阵 $\boldsymbol{P}_1,\boldsymbol{P}_2,\cdots,\boldsymbol{P}_n$，共计可以得到 $\prod_{k=1}^{n}k!$ 个不同的拉丁方。

3.2 利用最佳 Cartesian 认证码构造完备安全认证码

构造　设 $\boldsymbol{A}$ 是任意最佳 Cartesian 认证码 $\mathrm{AC}((n+1),n(n+1),n^2)$ 的编码矩阵；$M^i\ (i=1,2,\cdots,n+1)$ 表示信源 s_i 所对应的消息集合，$M_j^i\ (j=1,2,\cdots,n)$ 表示集合 M^i 中的第 j 个消息；根据前面的介绍，不妨将 $\boldsymbol{A}$ 写成如下的形式：

$$\boldsymbol{A}=\begin{bmatrix} M_1^1 & M_1^2 & \cdots & M_1^n & M_1^{n+1}\\ M_2^1 & M_2^2 & \cdots & M_2^n & M_1^{n+1}\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ M_n^1 & M_n^2 & \cdots & M_1^n & M_1^{n+1}\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ M_1^1 & M_n^2 & \cdots & M_2^n & M_n^{n+1}\\ M_2^1 & M_1^2 & \cdots & M_3^n & M_n^{n+1}\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ M_n^1 & M_{n-1}^2 & \cdots & M_1^n & M_n^{n+1} \end{bmatrix} \tag{1}$$

第 $(n+1)$ 列为 $\left[\underbrace{M_1^{n+1},M_1^{n+1},\cdots,M_1^{n+1}}_{n\text{个}},\underbrace{M_2^{n+1},M_2^{n+1},\cdots,M_2^{n+1}}_{n\text{个}},\cdots,\underbrace{M_n^{n+1},M_n^{n+1},\cdots,M_n^{n+1}}_{n\text{个}}\right]$ 去除编码矩阵 $\boldsymbol{A}$ 的第 $(n+1)$ 列，使之变为 $\boldsymbol{A}'$，并将 $\boldsymbol{A}'$ 写成如下形式：

$$\boldsymbol{A}'=\begin{bmatrix} \boldsymbol{A}_1^1 & \boldsymbol{A}_1^2 & \cdots & \boldsymbol{A}_1^n\\ \boldsymbol{A}_2^1 & \boldsymbol{A}_2^2 & \cdots & \boldsymbol{A}_2^n\\ \vdots & \vdots & \ddots & \vdots\\ \boldsymbol{A}_n^1 & \boldsymbol{A}_n^2 & \cdots & \boldsymbol{A}_n^n \end{bmatrix} \tag{2}$$

上式中的 $\boldsymbol{A}_j^i\ (i,j=1,2,\cdots,n)$ 表示编码矩阵 $\boldsymbol{A}$ 的第 i 列，从第 $n(j-1)+1$ 行到 nj 行的 n 个消息构成的列向量。设 $\boldsymbol{L}$ 是任意一个 n 阶拉丁方，$\boldsymbol{L}$ 中的元素集合 $N=\{1,2,\cdots,n\}$，并以 $\boldsymbol{A}_j^i\ (i,j=1,2,\cdots,n)$ 取代 $\boldsymbol{L}$ 中的第 j 行的元素 i，则可以得到一个 $n^2\times n$ 阶的认证码编码矩阵 $\boldsymbol{A}^*$。假定信源和编码规则分布等概，则有如下结论：

定理 4　由以上方法构造的认证码是一个完备安全认证码，且具有参数：$|S|=n$，$|M|=n^2$，$|E|=n^2$，$P_I=P_S=1/n$。

证明　由构造过程可知，每个 $\boldsymbol{A}_j^i\ (i,j=1,2,\cdots,n)$ 包含集合 M^i 中全部 n 个消息，每个 j 对应着这 n 个消息的一种全排列。由矩阵 $\boldsymbol{A}'$ 结合拉丁方 $\boldsymbol{L}$ 构造出的编码矩阵 $\boldsymbol{A}^*$，其每一列均由一个 $\boldsymbol{A}_{j_1}^1,\boldsymbol{A}_{j_2}^2,\cdots,\boldsymbol{A}_{j_n}^n$ 组成，即 $\boldsymbol{A}^*$ 的每一列都包含有消息集合 M 中的全部消息，且每个消息仅出现一次。即任意信源 s 在 n^2 个不同的编码规则下，可以映射成 n^2 个不同的消息，所以 $P(s\mid m)=P(s)$，即 $\boldsymbol{A}^*$ 为安全认证码编码矩阵。

在编码矩阵 $\boldsymbol{A}^*$ 中，每个编码规则 e 对应 n 个不同的消息，又因为消息数目 $|M|=n^2$，所以，在该编码规则下，敌方模仿攻击成功的概率 $P_I=1/n$。

因为 $\boldsymbol{A}$ 是最佳 Cartesian 认证码 $\mathrm{AC}((n+1),n(n+1),n^2)$ 的编码矩阵，根据定理 2，定理 3 可得：$\left|\left\{e:e(s_i)=M_j^i\right\}\right|=n$，$\left|\left\{e:e(s_i)=M_j^i,e(s_k)=M_l^k,i\neq k\right\}\right|=1$。由构造的过程可知，$\boldsymbol{A}'$ 与 $\boldsymbol{A}^*$ 中相同的行所包含的消息集合相同，只是该集合中的消息的排列顺序或发生变化或保持不变，但无论顺序改变或不变，均不改变 $\boldsymbol{A}'$ 中消息的正交性，所以敌方替换攻击成功的概率 $P_S=1/n$。

当信源、编码规则分布等概时，对于认证码 $\boldsymbol{A}^*$ 有

$$\begin{aligned} I(M;E)&=H(E)-H(E\mid M)\\ &=\sum_e p(e)\log_2\frac{1}{p(e)}-\sum_{m,e}p(m,e)\log_2\frac{1}{p(e\mid m)}\\ &=\log_2 n \end{aligned} \tag{3}$$

即 $\log_2 P_I=\log_2 P_S=-I(M;E)$，所以 $\boldsymbol{A}^*$ 是完备认证码。

综上所述，$\boldsymbol{A}^*$ 为完备安全认证码。　　证毕

例 1　将最佳 Cartesian 认证码 $\mathrm{AC}(4,12,9)$ 改造成完备安全认证码。不妨将 $\mathrm{AC}(4,12,9)$ 的编码矩阵写成如下形式

$$\boldsymbol{A}=\begin{bmatrix} m_1 & m_4 & m_7 & m_{10} \\ m_2 & m_5 & m_8 & m_{10} \\ m_3 & m_6 & m_9 & m_{10} \\ m_1 & m_5 & m_9 & m_{11} \\ m_2 & m_6 & m_7 & m_{11} \\ m_3 & m_4 & m_8 & m_{11} \\ m_1 & m_6 & m_8 & m_{12} \\ m_2 & m_4 & m_9 & m_{12} \\ m_3 & m_5 & m_7 & m_{12} \end{bmatrix} \tag{4}$$

令 $\boldsymbol{A}_1^1=[m_1 \quad m_2 \quad m_3]^{\mathrm{T}}$，$\boldsymbol{A}_1^2=[m_4 \quad m_5 \quad m_6]^{\mathrm{T}}$，$\boldsymbol{A}_1^3=[m_7 \quad m_8 \quad m_9]^{\mathrm{T}}$，$\boldsymbol{A}_2^1=[m_1 \quad m_2 \quad m_3]^{\mathrm{T}}$，$\boldsymbol{A}_2^2=[m_5 \quad m_6 \quad m_4]^{\mathrm{T}}$，$\boldsymbol{A}_2^3=[m_9 \quad m_7 \quad m_8]^{\mathrm{T}}$，$\boldsymbol{A}_3^1=[m_1 \quad m_2 \quad m_3]^{\mathrm{T}}$，$\boldsymbol{A}_3^2=[m_6 \quad m_4 \quad m_5]^{\mathrm{T}}$，$\boldsymbol{A}_3^3=[m_8 \quad m_9 \quad m_7]^{\mathrm{T}}$；设 $\boldsymbol{L}$ 为一 3 阶标准拉丁方

$$\boldsymbol{L}=\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \tag{5}$$

由 $\boldsymbol{A}_j^i\ (i,j=1,2,3)$ 与 $\boldsymbol{L}$ 中元素 i 的对应关系有

$$\boldsymbol{A}^*=\begin{bmatrix} \boldsymbol{A}_1^1 & \boldsymbol{A}_1^2 & \boldsymbol{A}_1^3 \\ \boldsymbol{A}_2^2 & \boldsymbol{A}_2^3 & \boldsymbol{A}_2^1 \\ \boldsymbol{A}_3^3 & \boldsymbol{A}_3^1 & \boldsymbol{A}_3^2 \end{bmatrix} \tag{6}$$

将 $\boldsymbol{A}_j^i\ (i,j=1,2,3)$ 的向量表达式代入，即得

$$\boldsymbol{A}^*=\begin{bmatrix} m_1 & m_4 & m_7 \\ m_2 & m_5 & m_8 \\ m_3 & m_6 & m_9 \\ m_5 & m_9 & m_1 \\ m_6 & m_7 & m_2 \\ m_4 & m_8 & m_3 \\ m_8 & m_1 & m_6 \\ m_9 & m_2 & m_4 \\ m_7 & m_3 & m_5 \end{bmatrix} \tag{7}$$

这样，就得到一个具有 3 个信源，9 个编码规则，9 个消息的认证码编码矩阵 $\boldsymbol{A}^*$。当信源和编码规则等概分布时，该认证码为完备安全的认证码，敌方模仿攻击和替换攻击成功的概率均为 1/3。

4 结束语

本文利用拉丁方将最佳 Cartesian 认证码 $\mathrm{AC}((n+1),n(n+1),n^2)$ 改造成完备安全的认证码 $\mathrm{AC}(n,n^2,n^2)$，编码规则在改造前后保持不变。本文提出的利用最佳 Cartesian 认证码构造完备安全认证码的方法仅以减少一个信源的代价换得了认证码的更高的安全性能，同时消息的数量减少了 n 个。

参 考 文 献

[1] Simmons G J. Authentication theory/coding theory, Advances in Cryptology. In: Proc. Crypto'84. Berlin: Springer-Verlag, 1984: 411–431.

[2] Stinson D R. Construction for authentication/secrecy codes from certain combinatorial designs. *Journal of Cryptology*, 1988, 1(2): 119–127.

[3] Stinson D R. The combinatorics of authentication and secrecy codes. *Journal of Cryptology*, 1990, 2(1): 23–49.

[4] Jimbo M and Fuji-Hara R. Optimal authentication systems and combinatorial designs. *IEEE Trans. on Info. Theory*, 1990, 36(1): 54–62.

[5] 王新梅, 马文平, 武传坤. 纠错密码理论. 北京: 人民邮电出版社, 2001: 246–258.
Wang Xin-mei, Ma Wen-ping, and Wu Chuan-kun. Theory of Cryptology Based on Error-Correcting codes. Beijing: Posts & Telecom Press, 2001: 246–258.

[6] Gilbert E N, MacWilliams F J, and Stoane N J A. Codes which detect deception. *The Bell System Technical.*, 1974, 53(3): 405–424.

[7] 马文平, 王新梅. 关于 CARTESIAN 认证码的构造. 电子学报, 1999, 27(5): 33–35.
Ma Wen-ping and Wang Xin-mei. On the construction of CARTESIAN authentication codes. *Acta Electronica Sinica*, 1999, 27(5): 33–35.

[8] 邵嘉裕. 组合数学. 上海: 同济大学出版社, 1991: 39–49.
Shao Jia-yu. Combinatorial Mathematics. Shanghai: Tongji University Press, 1991: 39–49.

[9] 杨德. 试验设计与分析. 北京: 中国农业出版社, 2002: 83–88.
Yang De. Experimental Design and Analysis. Beijing: China Agriculture Press, 2002: 83–88.

刘金龙： 男，1976年生，博士生，研究方向为信息安全理论与技术.

许宗泽： 男，1940年生，教授，博士生导师，研究方向为数字通信、编码理论与应用.