笛卡尔积与认证码

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：该文研究了笛卡尔积与认证码的关系，根据笛卡儿积的结构特点，提出了一种将认证符信息嵌入到编码规则的思想，从工程应用的角度实现了基于笛卡尔积的各阶欺骗概率相等的最优 Cartesian 认证码的构造，并给出了基于笛卡尔积和拉丁方的各阶欺骗概率相等的安全认证码的构造方案。以上两种构造方案均无需预先存储编码矩阵，既节约了大量的存储空间，又可以获得所需要的安全性。

关键词：笛卡尔积；最优认证码；拉丁方；安全认证码
中图分类号：TN918　　**文献标识码**：A　　**文章编号**：1009-5896(2008)06-1441-04

Cartesian Product and Authentication Codes

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

Abstract: The relation between the Cartesian product and authentication codes is studied in this paper. A new idea to use the private keys to carry the information of the authentication symbols is presented, which is based on the character of Cartesian product' structure. And the Cartesian product–based optimal authentication codes with equal cheating probabilities of all orders are constructed, which can be easily designed and can be applied well to engineering. In this paper, the secret authentication codes with equal cheating probabilities of all orders are also constructed which are founded on Cartesian product and Latin square. The two construction methods mentioned above need no pre-storing encoder matrix, so that a mass of storage is saved. At the same time, the two schemes can offer an enough security level expected.

Key words: Cartesian product; Optimal authentication codes; Latin square; Secret authentication codes

1　引言

消息认证是密码学的重要内容之一，它是检验收到的消息是否来源于真正的发信者，防止非法接收者接收消息以及检验收到的消息是否被篡改的一种重要的技术。1974 年，Gilbert，MacWilliams 和 Sloane[1]首次提出了消息认证的概念，并利用投影平面构造了认证码。1984，Simmons[2]等人发展了认证系统的信息理论。他将信息论用于研究认证系统的理论安全性和实际安全性，指出了认证系统的性能极限以及设计认证码所必须遵循的原则。此后，许多中外学者，如万哲先[3]、裴定一[4]、Stinson[5]等人，对认证码的组合特性和信息论界进行了深入的研究和探讨，并采用多种方法构造出多类性能优越的认证码，极大地丰富了认证码的研究成果。

在 Simmons 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。

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，并以 $\mathrm{AC}(k,v,b)$ 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。反之，如果对任意给定的消息 m，无法确定信源 s，则该认证码具有对信源的保密功能，称为保密认证码。

2　笛卡尔积与认证码

笛卡尔积属于集合论的范畴，其有如下定义和推论：

定义 1[6]　设 A,B 为二集合，称由 A 中元素为第一个元素，B 中元素为第二个元素的所有有序对组成的集合为 A 与 B 的笛卡尔积，记作 $A\times B$，即 $A\times B=\{<x,y>|\, x\in A\wedge y\in B\}$。

定义 2[6]　设 $A_1,A_2,\cdots,A_n$ 为 n 个集合 $(n\geq 2)$，称集合 $\{<x_1,x_2,\cdots,x_n>|\, x_1\in A_1\wedge x_2\in A_2\wedge\cdots\wedge x_n\in A_n\}$ 为 n 维笛卡尔积，记作 $A_1\times A_2\times\cdots\times A_n$，$A_1=A_2=\cdots=A_n=A$ 时，记 A 生成的 n 维笛卡尔积为 A^n。

2006-11-21 收到，2007-05-08 改回

推论 1[6] 设 $A_1, A_2, \cdots, A_n$ 均为有穷集合，并设 $|A| = n_i$，$i = 1,2,\cdots,n$，则 $|A_1 \times A_2 \times \cdots \times A_n| = n_1 \times n_2 \times \cdots \times n_n$。

对于消息认证系统而言，其安全性度量指标主要包括信源保密能力和对抗欺骗能力。

定义 3[7] 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 p_r 表示 r 阶欺骗攻击概率，即敌方在一次通信中观察到 r 个不同的消息后成功地发送一个自己的消息欺骗收方成功的最大概率，使得 $p_0, p_1, \cdots, p_{t-1}$ 和 v 都达到下界的认证码称为 t 阶最优认证码；若仅使得 $p_0, p_1, \cdots, p_{t-1}$ 达到它们各自下界的认证码称为 t 阶欺骗概率最优的认证码。

引理 1[8] 设认证码的 S, E 等概分布，则该认证码是各阶欺骗概率为 $1/q$ 的 t 阶最优认证码当且仅当

(1) q 是大于 1 的正整数；

(2)认证码共有 q^t 个编码规则；

(3)对于任意 $1 \le r \le t$，任意 r 个消息要么在 0 个，要么在 q^{t-r} 个编码规则下有效。

定理 1 若有一个集合 A 生成的 k 维笛卡尔积 A^k，且 $|A| = n$，则可以构造一个参数为 $|S| = k$，$|E| = n^k$，$|M| = kn$，各阶欺骗概率均为 $1/n$ 的 k 阶最优 Cartesian 认证码。

证明 设集合 $A = \{z_i \mid i = 1,2,\cdots,n\}$，$A$ 的 k 维笛卡尔积为 $A^k = \{ < z_{i_1}, z_{i_2}, \cdots, z_{i_k} > \mid z_{i_1}, z_{i_2}, \cdots, z_{i_k} \in A\}$。首先将 A^k 中的所有有序组排列成一个 $n^k \times 1$ 的列向量，然后将每个有序组在不改变其 k 个元素顺序的条件下将其改写成 $1 \times k$ 的行向量，这样可以得到一个 $n^k \times k$ 阶矩阵 $\boldsymbol{C}$，$\boldsymbol{C}$ 中的每一元素 $c_{ij} \in A$，$i = 1,2,\cdots,n^k$，$j = 1,2\cdots,k$。若以 $\boldsymbol{C}$ 作为认证符编码矩阵[7]，则信源数目 $|S| = k$，密钥数目 $|E| = n^k$。当密钥 e_i 对信源 s_j 进行编码时，可得到消息 $m_{ij} = e_i(s_j) = (s_i, c_{ij})$；又因为 $c_{ij} \in A$，$|A| = n$，所以 (s_i, c_{ij}) 总共可以形成 kn 种不同的组合，即消息的数目 $|M| = kn$。

不失一般性，假定敌方截获到 r $(r \le k-1)$ 个不同的消息 $(s_1, z_{i_1}), (s_2, z_{i_2}), \cdots, (s_r, z_{i_r})$，$z_{i_j} \in A$，然后选择一个不同的信源 s_{i+1} 构造一个消息 $(s_{r+1}, z_{i_{r+1}})$ 进行欺骗。由笛卡尔积的性质可知，k 维笛卡尔积 A^k 中共有 n^{k-r} 个有序组使得 $z_{i_1}, z_{i_2}, \cdots, z_{i_r}$ 在有序组中的位置保持不变，即任意 r 个消息 $(s_1, z_{i_1}), (s_2, z_{i_2}), \cdots, (s_r, z_{i_r})$ 在 n^{k-r} 个编码规则下有效。又因为当 $r = k$ 时，任意消息 $(s_1, z_{i_1}), (s_2, z_{i_2}), \cdots, (s_r, z_{i_r})$ 只在一个编码规则下有效。

综上所述，根据引理 1 即知定理 1 成立。 证毕

将定理 1 的证明过程进行逆推，即可证明定理 2 成立。

定理 2 若存在一个参数为 $|S| = k$，$|E| = n^k$，$|M| = kn$ 且 S, E 等概分布时，各阶欺骗概率为 $1/n$ 的 k 阶最优 Cartesian 认证码，则其编码矩阵是一个由集合 $A_1, A_2, \cdots, A_k$ 生成的 k 维笛卡尔积，且 $|A_i| = n$，$i = 1,2,\cdots,k$。

下面，根据定理 1 来对文献[8]中的定理进行修正。

定理 3[8] 若 q 是素数方幂，则存在一个参数为 $k = t$，$b = q^t$，$v = qt$ 的各阶欺骗概率均为 $1/q$ 的 t 阶最优 Cartesian 认证码。

上述定理未能完全刻画出这类 Cartesian 认证码的数学结构，因为由定理 1 可知，当 q 为任意正整数时，定理 3 的结论依然成立。现将定理 3 修正如下：

定理 4 当 q 是为任意正整数时，均存在一个参数为 $k = t$，$b = q^t$，$v = qt$ 的各阶欺骗概率均为 $1/q$ 的 t 阶最优 Cartesian 认证码。

3 基于笛卡尔积的各阶欺骗概率为 $1/n$ 的 k 阶最优 Cartesian 认证码的实现

设 A 是包含 n 个元素的集合，A^k 是由 A 生成的 k 维笛卡尔积，由定理 1 的证明过程可知，由 A^k 构造的 $\boldsymbol{C}$ 是一个 $n^k \times k$ 阶的认证符编码矩阵。为了获得较高的安全性和编码效率，n, k 应该越大越好，然而编码矩阵 $\boldsymbol{C}$ 的存贮空间却随着 k 的增加呈指数增长，随着 n 的增加呈 k 次方增长。原始的编码方法(先存储 $\boldsymbol{C}$，后编码的方法)由于需要巨大的存储开销而变得不再实用。经过深入的研究，作者发现认证符的信息可以嵌入到密钥中，收方可以根据收到的密钥临时建立一个该密钥控制下的 $1 \times k$ 阶编码矩阵对收到的消息进行验证；当该密钥失效时，即可丢弃所建立的编码矩阵，再根据新的密钥重新建立编码矩阵。这样，就可以不用预先存储编码矩阵，既节省大量的存储空间，又可以获得所需要的安全性。

3.1 基于笛卡尔积的各阶欺骗概率为 $1/n$ 的 k 阶最优 Cartesian 认证码的构造

构造 1：

(1)发方随机的选择一个非负整数 x $(x < n^k)$ 通过密钥通道发送给收方；

(2)收、发双方利用除法将 x 转化为 n 进制的数，并以如下形式表示

$$x = \lambda_{k-1} n^{k-1} + \lambda_{k-2} n^{k-2} + \cdots + \lambda_1 x + \lambda_0 \tag{1}$$

$\lambda_i \in \{0,1,\cdots,n-1\}$，$i = 0,1,\cdots,k-1$；

(3)双方临时建立一个 $1 \times k$ 阶认证符编码矩阵 $[\lambda_0, \lambda_1, \cdots, \lambda_{k-1}]$，并共同约定编码规则 $e_x : s_i \to (s_i, \lambda_i)$，$i = 0,1,\cdots, k-1$，$s_0, s_1, \cdots, s_{k-1}$ 为 k 个不同的信源；

(4)发方按照既约的编码规则对任一信源 s 编码成消息 (s, λ)，并通过公共信道发送给收方；收方接收到消息 (s', λ') 后，用认证符编码矩阵把 s' 编码成消息 (s', λ^*)，若 $(s', \lambda') = (s', \lambda^*)$，则将 (s', λ') 作为合法的消息接受；否则，拒绝接受。

注 以上构造步骤中的 n 取 $n \ge 2$。

定理 5 假定 x 被等概选取时，以上方法构造的是一个参数为 $|S| = k$，$|E| = n^k$，$|M| = kn$，各阶欺骗概率均为 $1/n$ 的 k 阶最优 Cartesian 认证码。

证明　因为 $0 \le x < n^k$，当 x 作为密钥被等概选取时，编码矩阵 $[\lambda_0,\lambda_1,\cdots,\lambda_{k-1}]$ 总共有 n^k 种不同的形式，在不改变每个编码矩阵 $[\lambda_0,\lambda_1,\cdots,\lambda_{k-1}]$ 中元素顺序的条件下，将其改写成有序组 $<\lambda_0,\lambda_1,\cdots,\lambda_{k-1}>$，所有的有序组便构成了一个 k 维笛卡尔积 A^k，$|A|=n$，由定理 1 可知，定理 5 成立。

证毕

3.2　性能分析

(1)与目前已知的一些各阶欺骗概率相等的最优认证码构造方法[8]相比，本文提出的基于笛卡尔积的构造法，其参数 n,k 的选择具有更大的灵活性：(a) n 可以取大于等于 2 的任意整数；(b) n,k 可以相互无关，无需限制 $k \le n$。

(2)本文给出的构造方法，只需进行 k 次简单的除法运算，便可以得到一个密钥控制下的 k 个认证符，与文献[8,9]中采用的基于有限域的运算相比，本文构造法的计算量更少。

(3)本文提出的基于笛卡尔积的各阶欺骗概率相等的最优 Cartesian 认证码构造方法，只需存储 k 个信源状态和临时存储 k 个认证符，大大地节省了存储空间。

(4)对于认证码来说，敌方是不能获得密钥的，根据本文方法具有较小的计算量和较少的存储空间的特点，可以构造出任意小欺骗概率的高安全性的认证码。

(5)在 n,k 确定的条件下，可以将密钥推广到更大的空间，即 x 为任意的非负整数，只需将 x 写成

$$x=\lambda_{k-1}n^{k-1}+\lambda_{k-2}n^{k-2}+\cdots+\lambda_1 x+\lambda_0,\ \mathrm{mod}\, n^k \qquad (2)$$

3.1 节所述的构造方法仍然适用。

4　利用笛卡尔积和拉丁方构造各阶欺骗概率相等的安全认证码

3.1 节构造的各阶欺骗概率为 $1/n$ 的 k 阶最优 Cartesian 认证码具有很好的抗欺骗能力，但是没有信源保密能力。下面，利用拉丁方将 3.1 节构造的 Cartesian 认证码改造成各阶欺骗概率相等的安全认证码。

定义 5[10]　设 N 是一个 k 元集，若有元素全在 N 上的一个 $k\times k$ 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 k 阶拉丁方。

构造 2：

(1)收、法双方约定一个 k 阶拉丁方

$$\boldsymbol{L}=\begin{bmatrix} L_{00} & L_{01} & \cdots & L_{0,k-1} \\ L_{10} & L_{11} & \cdots & L_{1,k-1} \\ \vdots & \vdots & \ddots & \vdots \\ L_{k-1,0} & L_{k-1,1} & \cdots & L_{k-1,k-1} \end{bmatrix} \qquad (3)$$

$L_{ij}\in\{0,1,\cdots,k-1\}$，$i,j=0,1,\cdots,k-1$。

(2)发方随机的选择一对整数数 (x,y) $(0\le x<n^k;0\le y\le k-1)$ 通过密钥通道发送给收方；

(3)收、发双方利用除法将 x 转化为 n 进制的数，并以如下形式表示

$$x=\lambda_{k-1}n^{k-1}+\lambda_{k-2}n^{k-2}+\cdots+\lambda_1 x+\lambda_0$$

$$\lambda_i\in\{0,1,\cdots,n-1\}\, i=0,1,\cdots,k-1$$

(4)双方临时建立一个 $1\times k$ 阶认证符编码矩阵 $[\lambda_0,\lambda_1,\cdots,\lambda_{k-1}]$，并共同约定编码规则 $e_{x,y}:s_i\to(s_{L_{yi}},\lambda_i)$，$i=0,1,\cdots,k-1$，$s_0,s_1,\cdots,s_{k-1}$ 为 k 个不同的信源；

(5)发方按照约定的编码规则，利用密钥 (x,y) 将任一信源 s 编码成消息 (s_{i_1},λ_{j_1})，并通过公共信道发送给收方；收方接收到消息 (s_{i_2},λ_{j_2}) 后，用密钥 y 找到 s_{i_2} 在拉丁方第 y 行中的位置 i_3，再选取认证符 λ_{i_3} 与 λ_{j_2} 比较，若 $\lambda_{i_3}=\lambda_{j_2}$，则 (s_{i_2},λ_{j_2}) 将作为合法的消息接受；否则，拒绝接受。

定理 6　假定 x,y 均等概分布时，以上方法构造的是一个参数为 $|S|=k$，$|E|=kn^k$，$|M|=kn$，各阶欺骗概率均为 $1/n$ 的安全认证码。

证明　当 y 固定，x 等概选取时，由定理 5 可知，所有的认证符编码矩阵构成的有序组 $<\lambda_0,\lambda_1,\cdots,\lambda_{k-1}>$ 组成一个 k 维笛卡尔积 A^k，$|A|=n$，所以该认证码是各阶欺骗概率均为 $1/n$ 的 Cartesian 认证码；又因为 y 有 k 种取值，所以 $|E|=kn^k$。

对每个密钥 x 控制下的消息编码矩阵为 $[(s_0,\lambda_0),(s_1,\lambda_1),\cdots,(s_{k-1},\lambda_{k-1})]$，当 x 固定，y 等概选取时，编码矩阵变为

$$\boldsymbol{C}_y=\begin{bmatrix} (s_{L_{00}},\lambda_0) & (s_{L_{01}},\lambda_1) & \cdots & (s_{L_{0,k-1}},\lambda_{k-1}) \\ (s_{L_{10}},\lambda_0) & (s_{L_{11}},\lambda_1) & \cdots & (s_{L_{1,k-1}},\lambda_{k-1}) \\ \vdots & \vdots & \ddots & \vdots \\ (s_{L_{k-1,0}},\lambda_0) & (s_{L_{k-1,1}},\lambda_1) & \cdots & (s_{L_{k-1,k-1}},\lambda_{k-1}) \end{bmatrix} \qquad (4)$$

因为 $L_{ij}\in\{0,1,\cdots,k-1\}$，所以 $s_{L_{ij}}\in\{s_0,s_1,\cdots,s_{k-1}\}$，即 $\boldsymbol{C}_y$ 的每一列都包含了 k 个信源开头的消息；在 $\boldsymbol{C}_y$ 的基础上，x 等概选取时，λ_i，$i=0,1,\cdots,k-1$ 可以等概取遍集合 $\{0,1,\cdots,n-1\}$ 中的所有值，所以，认证码的编码矩阵 $\boldsymbol{C}_{y,x}$ 每一列均包含有全部的 kn 个消息，即 $P(s\mid m)=P(s)$ 成立，所以该认证码是安全的。

综上所述，定理 6 成立。　　证毕

5　结束语

本文对笛卡尔积与各阶欺骗概率相等的认证码之间的关系进行了研究，给出了两者关系定理；为了有效地减少编码矩阵的存储空间，使得基于笛卡尔积上的各阶欺骗概率相等认证码具有适用价值，本文利用密钥本身携载认证符信息的特点，给出了实现该认证码的工程应用算法；本文利用拉丁方的性质，并结合笛卡尔积构造了各阶欺骗概率相等的安全认证码，构造算法简单，存储量小，并且可以获得很好的安全性能。

参 考 文 献

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

[2] Simmons G J. Authentication theory/coding theory,

Advances in Cryptology. In: Proc. Crypto'84. Berlin: Springer-Verlag, 1984: 411–431.

[3] Wan Zhexian. Further constructions of Cartesian authentication codes from symplectic geometry. *Northeaster Mathematical Journal*, 1992, 8(1): 4–20.

[4] Pei Dingyi. A problem of combinatorial designs related to authentication codes. *Journal of Combinatorial Designs*, 1998, 6(6): 417–429.

[5] Stinson D R. Combinatorial characterizations of authentication codes. *Designs, Codes and Cryptography*, 1992, 2(2): 175–187.

[6] 耿素云. 集合论与图论. 北京: 北京大学出版社, 1998: 30–34.
Geng Su-yun. Set Theory and Graph Theory. Beijing: Peking University Press, 1998: 30–34.

[7] 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.

[8] 胡磊, 裴定一. 各阶欺骗概率相等的最优认证码. 应用数学学报, 2002, 25(1): 43–48.
Hu Lei and Pei Ding-yi. Optimal authentication codes with equal cheationg probabilities of all orders. *Acta Mathematicae Applicatae Sinica*, 2002, 25(1): 43–48.

[9] Pei Dingyi. A problem of combinatorial designs related to authentication codes. *Journal of Combinatorial Design*, 1998, 6: 417–429.

[10] 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.

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.