布尔函数扩散性的矩阵刻画

郭锦辉 李世取
(解放军信息工程大学信息研究系 郑州 450002)

摘 要 该文利用布尔函数的特征矩阵，给出了 $n(\geq 3)$ 元布尔函数在 $\boldsymbol{s}\in \mathrm{GF}^n(2)$ 满足扩散准则的充分必要条件，在此基础上得到了布尔函数满足严格雪崩准则(SAC)的一个充分必要条件和 n 元平衡布尔函数满足严格雪崩准则、代数次数达到最大且不含有非零线性结构的一个充分必要条件，最后提出了平衡且满足严格雪崩准则的布尔函数的两种特殊的“递补”构造法。

关键词 特征矩阵，扩散准则，严格雪崩准则(SAC)，非零线性结构，相关免疫
中图分类号: TN918.1 **文献标识码**: A **文章编号**：1009-5896(2006)04-0712-05

Matrix Description on Propagation Characteristic of Boolean Function

Guo Jin-hui Li Shi-qu
(*Dept of Information Research, PLA Information Engineering University, Zhengzhou* 450002, *China*)

Abstract With characteristic matrix of Boolean function, a necessary and sufficient condition is given on a Boolean function satisfying the propagation criterion on vector $\boldsymbol{s}\in \mathrm{GF}^n(2)$, which provides $n\geq 3$. On the basis of it, the necessary and sufficient conditions are given on a Boolean function satisfying Strict Avalanche Criterion (SAC) and on a balanced SAC function which achieves the maximum degree and no nonzero linear structure. Finally, two special “filling vacancies in the proper order ”methods of construction are presented.

Key words Characteristic matrix, Propagation criterion, Strict Avalanche Criterion(SAC), Nonzero linear structure, Correlation immune

1 引言

扩散准则是文献[1]中引入的“50%-依赖性”和“完全非线性”概念的推广，是密码设计的一个重要准则。它的含义是如果逻辑函数 $f(\boldsymbol{x})$ 在 $\boldsymbol{s}$ 满足扩散准则，则 $f(\boldsymbol{x})$ 与 $f(\boldsymbol{x}+\boldsymbol{s})$ 之间的互信息为零，即 $\boldsymbol{I}\left(f(\boldsymbol{x}),\ f(\boldsymbol{x}+\boldsymbol{s})\right)=0$，这正是密码设计者所期望的，因此密码学中研究逻辑函数的扩散特性有非常重要的意义。基于此，国内外学者对密码学中具有扩散性的逻辑函数特别是布尔函数进行了大量的研究，取得了丰富的成果。 国内单炜娟曾率先利用布尔函数的特征矩阵研究过布尔函数的相关免疫特性并取得了很好的效果[2]，随后杨义先教授利用特征矩阵就相关免疫布尔函数的计数开展过一系列研究工作[3]，王隽博士也曾利用特征矩阵研究过Bent函数的完全构造[4]。 但目前尚未发现直接利用特征矩阵来研究逻辑函数一般扩散特性和线性结构特性的研究工作。在本文中我们利用布尔函数的特征矩阵给出了 $n(\geq 3)$ 元布尔函数在 $\boldsymbol{s}\in \mathrm{GF}^n(2)$ 处满足扩散准则的充分必要条件。由此通过特征矩阵得到了布尔函数满足严格雪崩准则(SAC)的一个充分必要条件，从而在理论上或者说在原则上给出了满足严格雪崩准则的布尔函数的一种完全构造法。 由于密码学中使用的逻辑函数还常常要求具有平衡性、非退化性和高的代数次数，故本文还进一步通过特征矩阵给出了平衡布尔函数满足严格雪崩准则、代数次数达到最大且不含有“非零”线性结构(一定非退化)的一个充分必要条件。最后提出了平衡且满足严格雪崩准则的布尔函数的两种特殊的“递补”构造法。

2 基本概念

定义 1 称 $\mathrm{GF}^n(2)\to \mathrm{GF}(2)$ 的任一映射 f 为 n 个变元的($\mathrm{GF}^n(2)$ 上的)布尔函数，即若记 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in \mathrm{GF}^n(2)$，则有 $f(\boldsymbol{x})=f(x_1,x_2,\cdots,x_n)\in \mathrm{GF}(2)$。

定义 2 n 元布尔函数 $f(x_1,x_2,\cdots,x_n)$ 的汉明重量是指集合 $\left\{(x_1,x_2,\cdots,x_n):(x_1,x_2,\cdots,x_n)\in \mathrm{GF}^n(2),\ f(x_1,x_2,\cdots,x_n)=1\right\}$ 所含元素的个数。

定义 3 设 $w=(w_1,w_2,\cdots,w_n)\in \mathrm{GF}^n(2)$ 是 n 维布尔向量，称 $w=(w_1,w_2,\cdots,w_n)$ 的不为零的分量的个数为其汉明重量，且记之为 $W(\boldsymbol{w})$。

特别本文中 $\boldsymbol{e}_r$ 总表示 $\mathrm{GF}^n(2)$ 中满足 $W(\boldsymbol{e}_r)=1$ 且 $\boldsymbol{e}_r$ 的第 r 个分量为1的向量。

定义 4[5] 若 n 元布尔函数 $f(x_1,x_2,\cdots,x_n)$ 在 $(x_1,x_2,\cdots,x_n)=(c_{i1}+1,c_{i2}+1,\cdots,c_{in}+1)\in \mathrm{GF}^n(2),\ i=1,2,\cdots,k$ 时取值为1，否则取值为0，则汉明重量为 $k(\geq 1)$ 的 n 元布尔函数 $f(\boldsymbol{x})$ 的小项表示为

2004-07-19 收到，2005-02-08 改回

$$\begin{aligned} f(x_1,x_2,\cdots,x_n) &= (x_1+c_{11})(x_2+c_{12})\cdots(x_n+c_{1n}) \\ &\quad +(x_1+c_{21})(x_2+c_{22})\cdots(x_n+c_{2n})+\cdots \\ &\quad +(x_1+c_{k1})(x_2+c_{k2})\cdots(x_n+c_{kn}) \\ &\hat{=}(x+\boldsymbol{c}_1)+(x+\boldsymbol{c}_2)+\cdots+(x+\boldsymbol{c}_k) \end{aligned} \tag{1}$$

其中

$$c_i=(c_{i1},c_{i2},\cdots,c_{in}),\quad 1\le i\le k,$$

并且称

$$\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{k1} & c_{k2} & \cdots & c_{kn} \end{pmatrix} = \begin{pmatrix} \boldsymbol{c}_1 \\ \boldsymbol{c}_2 \\ \vdots \\ \boldsymbol{c}_k \end{pmatrix} \tag{2}$$

为 $f(\boldsymbol{x})$ 的特征矩阵。

定义 5[6]　称布尔函数 $f(\boldsymbol{x})$，$\boldsymbol{x}\in \mathrm{GF}^n(2)$ 关于 $\boldsymbol{s}\in \mathrm{GF}^n(2)$ 是满足扩散准则的，若其“差分函数”

$$f(\boldsymbol{x}+\boldsymbol{s})+f(\boldsymbol{x}),\quad \boldsymbol{x}\in \mathrm{GF}^n(2)$$

是平衡的，即

$$\begin{aligned} &\left|\{\boldsymbol{x}:\boldsymbol{x}\in \mathrm{GF}^n(2), f(\boldsymbol{x}+\boldsymbol{s})+f(\boldsymbol{x})=1\}\right| \\ &\quad =\left|\{\boldsymbol{x}:\boldsymbol{x}\in \mathrm{GF}^n(2), f(\boldsymbol{x}+\boldsymbol{s})+f(\boldsymbol{x})=0\}\right|=2^{n-1} \end{aligned}$$

定义 6[7]　称布尔函数 $f(\boldsymbol{x})$，$\boldsymbol{x}\in \mathrm{GF}^n(2)$ 是满足严格雪崩准则的，若对所有的 $\boldsymbol{e}_r$，$1\le r\le n$，其“差分函数” $f(\boldsymbol{x}+\boldsymbol{e}_r)+f(\boldsymbol{x})$，$\boldsymbol{x}\in \mathrm{GF}^n(2)$ 都是平衡的。

定义 7[6]　设 $f(\boldsymbol{x})$，$\boldsymbol{x}\in \mathrm{GF}^n(2)$ 是一布尔函数，$\boldsymbol{s}\in \mathrm{GF}^n(2)$，若对所有 $\boldsymbol{x}\in \mathrm{GF}^n(2)$ 都有 $f(\boldsymbol{x}+\boldsymbol{s})+f(\boldsymbol{x})=f(\boldsymbol{s})+f(0)$（=常数 0 或 1），则称 $\boldsymbol{s}$ 为 $f(\boldsymbol{x})$ 的一个线性结构。

令 $U_f^{(0)}=\{\boldsymbol{s}:\boldsymbol{s}\in \mathrm{GF}^n(2)$ 且对所有的 $\boldsymbol{x}\in \mathrm{GF}^n(2)$ 都有 $f(\boldsymbol{x}+\boldsymbol{s})+f(\boldsymbol{x})=0\}$，$U_f^{(1)}=\{\boldsymbol{s}:\boldsymbol{s}\in \mathrm{GF}^n(2)$ 且对所有的 $\boldsymbol{x}\in \mathrm{GF}^n(2)$ 都有 $f(\boldsymbol{x}+\boldsymbol{s})+f(\boldsymbol{x})=1\}$，则称 $U_f^{(0)}$ 中的元为 $f(\boldsymbol{x})$ 的“零类”线性结构，而称 $U_f^{(1)}$ 中的元为 $f(\boldsymbol{x})$ 的“1 类”线性结构。再记 $f(\boldsymbol{x})$ 的全体线性结构之集为 U_f，即 $U_f=U_f^{(0)}\cup U_f^{(1)}$。

3　本文主要结果

以下整数 $n\ge 3$，而整数 $k(\ge 1)$ 表示 $n(\ge 3)$ 元布尔函数 $f(\boldsymbol{x})$ 的汉明重量，$f(\boldsymbol{x})$ 的特征矩阵如式(2)，且对 $\boldsymbol{c}_i=(c_{i1},c_{i2},\cdots,c_{in})\in \mathrm{GF}^n(2)$，$1\le i\le k$，$\boldsymbol{s}=(s_1,s_2,\cdots,s_n)\in \mathrm{GF}^n(2)$，记 $\boldsymbol{c}_i+\boldsymbol{s}\hat{=}(c_{i1}+s_1,c_{i2}+s_2,\cdots,c_{in}+s_n)$，$1\le i\le k$。

引理 1　若 n 元布尔函数 $f(\boldsymbol{x})$ 的汉明重量为 $k(\ge 1)$，则对任意的 $0\ne\boldsymbol{s}\in \mathrm{GF}^n(2)$，都存在与 $\boldsymbol{s}$ 有关的整数 $0\le r\le k/2$，使其“差分函数” $f(\boldsymbol{x}+\boldsymbol{s})+f(\boldsymbol{x})$，$\boldsymbol{x}\in \mathrm{GF}^n(2)$ 的汉明重量为 $2k-4r$；而对整数 $0\le r\le k/2$，“差分函数” $f(\boldsymbol{x}+\boldsymbol{s})+f(\boldsymbol{x})$ 的汉明重量为 $2k-4r$ 的充分必要条件是 $f(\boldsymbol{x})$ 的特征矩阵式(2)中的行向量 $\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_k$ 满足：存在且仅存在 r 对(与 $\boldsymbol{s}$ 有关的) (i,j)，$1\le i\ne j\le k$，使得 $\boldsymbol{s}=\boldsymbol{c}_i+\boldsymbol{c}_j$，因而，$f(\boldsymbol{x}+\boldsymbol{s})+f(\boldsymbol{x})$ 的汉明重量取得最大值 $2k$ 的充分必要条件是其特征矩阵式(2)的行向量 $\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_k$ 中任意两个的和都不是 $\boldsymbol{s}$。

证明　由汉明重量为 k 的布尔函数 $f(\boldsymbol{x})$ 的小项表示式(1)知，对任意的 $0\ne\boldsymbol{s}\in \mathrm{GF}^n(2)$，都有

$$\begin{aligned} f(\boldsymbol{x}+\boldsymbol{s})+f(\boldsymbol{x}) &= \big[(\boldsymbol{x}+\boldsymbol{c}_1)+(\boldsymbol{x}+\boldsymbol{c}_2)+\cdots+(\boldsymbol{x}+\boldsymbol{c}_k) \\ &\quad +(\boldsymbol{x}+\boldsymbol{c}_1+\boldsymbol{s})+(\boldsymbol{x}+\boldsymbol{c}_2+\boldsymbol{s})+\cdots+(\boldsymbol{x}+\boldsymbol{c}_k+\boldsymbol{s})\big](\mathrm{mod}\,2) \end{aligned} \tag{3}$$

充分性　对 $0\ne\boldsymbol{s}\in \mathrm{GF}^n(2)$，若存在 1 对 (i,j)，$1\le i\ne j\le k$，使得 $\boldsymbol{s}=\boldsymbol{c}_i+\boldsymbol{c}_j$，就会同时成立

$$\boldsymbol{x}+\boldsymbol{c}_j+\boldsymbol{s}=\boldsymbol{x}+\boldsymbol{c}_i,\quad \boldsymbol{x}+\boldsymbol{c}_i+\boldsymbol{s}=\boldsymbol{x}+\boldsymbol{c}_j$$

式(3)中将有 4 项被“模”去，因此若同时有 r 对 (i,j)，$1\le i\ne j\le k$，使得 $\boldsymbol{s}=\boldsymbol{c}_i+\boldsymbol{c}_j$，而其余 $\boldsymbol{c}_i+\boldsymbol{c}_j$ 都不是 $\boldsymbol{s}$，则式(3)中将有 $4r$ 项被“模”去，而只余下互不相同的 $2k-4r$ 项，即“差分函数” $f(\boldsymbol{x}+\boldsymbol{s})+f(\boldsymbol{x})$ 的汉明重量为 $2k-4r$。

特别地，当 $\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_k$ 中的任意两个的和都不是 $\boldsymbol{s}$ 时，下述 $2k$ 个向量 $\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_k$，$\boldsymbol{c}_1+\boldsymbol{s},\boldsymbol{c}_2+\boldsymbol{s},\cdots,\boldsymbol{c}_k+\boldsymbol{s}$ 自然也就两两互不相同，“差分函数” $f(\boldsymbol{x}+\boldsymbol{s})+f(\boldsymbol{x})$ 的汉明重量即为 $2k$。

必要性　注意到 $0\ne\boldsymbol{s}\in \mathrm{GF}^n(2)$，而 $\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_k$ 两两互不相同，故 $\boldsymbol{c}_1+\boldsymbol{s},\boldsymbol{c}_2+\boldsymbol{s},\cdots,\boldsymbol{c}_k+\boldsymbol{s}$ 也两两互不相同以及式(3)即得证。　证毕

引理 2　若存在 $0\ne\boldsymbol{s}\in \mathrm{GF}^n(2)$，使得汉明重量为 k 的 n 元布尔函数 $f(\boldsymbol{x})$，$\boldsymbol{x}\in \mathrm{GF}^n(2)$ 关于 $\boldsymbol{s}$ 满足扩散准则，则存在整数 $0\le r\le k/2$，使得 $k=2^{n-2}+2r$，因而 $k\ge 2^{n-2}$ 且为偶数。

证明　若汉明重量为 k 的 n 元布尔函数 $f(\boldsymbol{x})$ 关于某 $0\ne\boldsymbol{s}\in \mathrm{GF}^n(2)$ 满足扩散准则，则由定义 5 知“差分函数” $f(\boldsymbol{x}+\boldsymbol{s})+f(\boldsymbol{x})$ 应为平衡函数，再由引理 1 知存在整数 $0\le r\le k/2$，使 $2k-4r=2^{n-1}$，即有 $k=2^{n-2}+2r$。　证毕

定理 1　汉明重量为 k 的 n 元布尔函数 $f(\boldsymbol{x})$，$\boldsymbol{x}\in \mathrm{GF}^n(2)$ 关于某 $0\ne\boldsymbol{s}\in \mathrm{GF}^n(2)$ 满足扩散准则的充分必要条件是其特征矩阵式(2)中的行向量 $\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_k$ 满足：存在且仅存在 $k/2-2^{n-3}$ 对(与 $\boldsymbol{s}$ 有关的) (i,j)，$1\le i\ne j\le k$，使得 $\boldsymbol{s}=\boldsymbol{c}_i+\boldsymbol{c}_j$。

证明　若汉明重量为 k 的 n 元布尔函数 $f(\boldsymbol{x})$ 关于 $0\ne\boldsymbol{s}\in \mathrm{GF}^n(2)$ 满足扩散准则，则由引理 2 知存在整数 $0\le r\le k/2$，使 $k=2^{n-2}+2r$，因而 $r=k/2-2^{n-3}$，根据引理 1 即知本定理的结论成立。

反之，若定理结论成立，则由引理 1 知“差分函数” $f(\boldsymbol{x}+\boldsymbol{s})+f(\boldsymbol{x})$ 的汉明重量即为

$$2k-4\times(k/2-2^{n-3})=2^{n-1}$$

因而 $f(\boldsymbol{x}+\boldsymbol{s})+f(\boldsymbol{x})$ 为平衡函数，故 $f(\boldsymbol{x})$ 关于 $\boldsymbol{s}$ 满足扩散准则。　证毕

利用定理 1 的结论不难给出 n 元布尔函数满足严格雪崩准则的如下特征矩阵刻画。

定理 2　n 元布尔函数 $f(\boldsymbol{x})$ 满足严格雪崩准则的充分必要条件是其汉明重量 $k\ge 2^{n-2}$ 为偶数，并且 $f(\boldsymbol{x})$ 的特征矩阵式(2)中的行向量 $\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_k$ 还满足：对任意的 $\boldsymbol{e}_r$，$1\le r\le n$，都存在且仅存在 $k/2-2^{n-3}$ 对(与 $\boldsymbol{e}_r$ 有关的) (i,j)，

$1\le i\ne j\le k$, 使得 $\boldsymbol{e}_r=\boldsymbol{c}_i+\boldsymbol{c}_j$。

特别地, 平衡的 n 元布尔函数 $f(\boldsymbol{x})$ 满足严格雪崩准则的充分必要条件为其特征矩阵式(2)中的行向量 $\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_{2^{n-1}}$ 满足: 对所有的 $\boldsymbol{e}_r$, $1\le r\le n$, 都存在且仅存在 2^{n-3} 对(与 $\boldsymbol{e}_r$ 有关的) (i,j), $1\le i\ne j\le k$, 使得 $\boldsymbol{e}_r=\boldsymbol{c}_i+\boldsymbol{c}_j$。

注 1 定理 2 揭示了平衡且满足严格雪崩准则的 n 元布尔函数的特征矩阵的共有性质, 即对任意的 $\boldsymbol{e}_r$, 其 2^{n-1} 个行向量中都有且仅有 2^{n-3} 对, 使它们对应分量"模 2 加"后所得正好是 $\boldsymbol{e}_r$, 因而如同单炜娟通过特征矩阵来刻画布尔函数的相关免疫性所取得的效果一样, 这里我们也不仅在理论上提供了平衡且满足严格雪崩准则的布尔函数的一种完全构造法, 同时还提供了平衡且满足严格雪崩准则的布尔函数的一个计数模型。

接下来我们将利用定理 2 的结果来构造平衡、代数次数达到最大、满足严格雪崩准则且非退化的布尔函数, 为此再做如下准备。

引理 3 n 元平衡布尔函数 $f(\boldsymbol{x})$ 的代数次数为 $\deg(f)=n-1$ 的充分必要条件是 $f(\boldsymbol{x})$ 的特征矩阵中至少存在一列, 这一列里 1 的个数为奇数。

对 $m\ge 2$, n 元平衡布尔函数 $f(\boldsymbol{x})$ 的代数次数 $\deg(f)=n-m$ 的充分必要条件是 $f(\boldsymbol{x})$ 的特征矩阵中至少存在 m 列, 这 m 列组成的矩阵中行向量为 $(\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_m)=(1,1,\cdots,1)$ 的个数为奇数, 且 $f(\boldsymbol{x})$ 的特征矩阵中任意 j ($1\le j\le m-1$) 列组成的矩阵中行向量为 $(\boldsymbol{a}_1,\cdots,\boldsymbol{a}_j)=(1,\cdots,1)$ 的个数为偶数。

证明 为记号简单, 这里只对 $m=1$ 时给出主要结论的证明。

周知, $n\ge 3$ 时 n 元平衡布尔函数的多项式表示式里不含 n 次项, 又若 $f(\boldsymbol{x})$ 的特征矩阵中至少有一列里 1 的个数为奇数, 不妨是第 1 列里 1 的个数为奇数, 则不难知直接展开 $f(\boldsymbol{x})$ 的小项表示式(1)后所得"和式"里单项式 $x_2x_3\cdots x_n$ 将出现奇数次, "模 2 加"后这一项必定仍在 $f(\boldsymbol{x})$ 的多项式表示式——代数标准形里, 因此 $\deg(f)=n-1$。

又若 n 元布尔函数 $f(\boldsymbol{x})$ 的特征矩阵的每一列里 1 的个数都为偶数或 0, 则同理可知 $f(\boldsymbol{x})$ 的代数标准形里不含所有的 $n-1$ 次项 $x_2x_3\cdots x_n$, $x_1x_3x_4\cdots x_n$, $\cdots$, $x_1x_2\cdots x_{n-2}x_n$, 因而若 n 元布尔函数 $f(\boldsymbol{x})$ 平衡且代数次数 $\deg(f)=n-1$, 则其特征矩阵中至少有一列里 1 的个数为奇数。 证毕

引理 4 设 n 元布尔函数 $f(\boldsymbol{x})$ 的汉明重量为 k (≥ 1), 则存在 $0\ne\boldsymbol{s}\in U_f^{(0)}$ 的充分必要条件是 k 为偶数, 并且 $f(\boldsymbol{x})$ 的特征矩阵式(2)中的行向量 $\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_k$ 满足: 存在且仅存在 $k/2$ 对(与 $\boldsymbol{s}$ 有关的) (i,j), $1\le i\ne j\le k$, 使得 $\boldsymbol{s}=\boldsymbol{c}_i+\boldsymbol{c}_j$。

证明 注意到 $0\ne\boldsymbol{s}\in U_f^{(0)}$ 的充分必要条件是 $f(\boldsymbol{x}+\boldsymbol{s})+f(\boldsymbol{x})\equiv 0$, $\boldsymbol{x}\in\mathrm{GF}^n(2)$, 因而引理 1 中的 $2k-4r=0$, 由此据引理 1 立即可得所欲证。 证毕

引理 5 设 n 元布尔函数 $f(\boldsymbol{x})$ 的汉明重量为 k (≥ 1), 则存在 $0\ne\boldsymbol{s}\in U_f^{(1)}$ 的充分必要条件是 $k\ge 2^{n-1}$ 为偶数, 并且当 $k>2^{n-1}$ 时为 $f(\boldsymbol{x})$ 的特征矩阵式(2)中的行向量 $\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_k$ 满足: 存在且仅存在 $k/2-2^{n-2}$ 对(与 $\boldsymbol{s}$ 有关的) (i,j), $1\le i\ne j\le k$, 使得 $\boldsymbol{s}=\boldsymbol{c}_i+\boldsymbol{c}_j$。而当 $k=2^{n-1}$ 时即为 $f(\boldsymbol{x})$ 的特征矩阵式(2)中的行向量 $\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_k$ 还满足:

$$\boldsymbol{c}_i+\boldsymbol{c}_j\ne\boldsymbol{s},\quad 1\le i\ne j\le 2^{n-1}$$

证明 注意到 $0\ne\boldsymbol{s}\in U_f^{(1)}$ 的充分必要条件是 $f(\boldsymbol{x}+\boldsymbol{s})+f(\boldsymbol{x})\equiv 1$, $\boldsymbol{x}\in\mathrm{GF}^n(2)$, 因而引理 1 中的 $2k-4r=2^n$, 由此据引理 1 立即可得所欲证。 证毕

注 2 引理 4 告知, 汉明重量为奇数的布尔函数没有"非零"的零类线性结构, 只有汉明重量为偶数的布尔函数才可能有"非零"的零类线性结构。由此联系定理 2 便知, 即使布尔函数满足严格雪崩准则, 它也可能有不少"非零"的零类线性结构, 因而这样的函数必定"退化"[5], 将之用于密码设计中就存在"安全隐患", 而密码学中还常常要求好的布尔函数有高的代数次数[5]。针对这些需求, 我们下面的定理 3 通过特征矩阵给出了平衡、满足严格雪崩准则、代数次数达到最大且 $U_f=\{\boldsymbol{0}\}$ 的布尔函数(一定非退化)的一种完全构造法。

定理 3 n 元平衡布尔函数 $f(\boldsymbol{x})$ 满足严格雪崩准则、代数次数达到最大且 $U_f=\{\boldsymbol{0}\}$ 的充分必要条件是 $f(\boldsymbol{x})$ 的特征矩阵式(2)中的行向量 $\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_{2^{n-1}}$ 满足:

(1) 对任意的 $\boldsymbol{e}_r$, $1\le r\le n$ 存在且仅存在 2^{n-3} 对(与 $\boldsymbol{e}_r$ 有关的) (i,j), $1\le i\ne j\le k$, 使得 $\boldsymbol{e}_r=\boldsymbol{c}_i+\boldsymbol{c}_j$。

(2) 对任意的 $\boldsymbol{s}\in\mathrm{GF}^n(2)$, $W(\boldsymbol{s})\ge 2$, 存在且仅存在(与 $\boldsymbol{s}$ 有关的)整数 $1\le r<2^{n-2}$ 和 r 对(与 $\boldsymbol{s}$ 有关的) (i,j), $1\le i\ne j\le k$, 使得 $s=c_i+c_j$; 并且

(3) $f(\boldsymbol{x})$ 的特征矩阵中至少存在一列, 这一列里 1 的个数为奇数。

证明 根据定理 2, 引理 4, 引理 5 及引理 3 即得证。 证毕

例如, 对任一 $\boldsymbol{c}=(\boldsymbol{c}_1,\boldsymbol{c}_2,\boldsymbol{c}_3,\boldsymbol{c}_4)\in\mathrm{GF}^4(2)$ 和 $\mathrm{GF}^4(2)$ 中的向量 $\boldsymbol{e}_1=(1,0,0,0)$, $\boldsymbol{e}_2=(0,1,0,0)$, $\boldsymbol{e}_3=(0,0,1,0)$, $\boldsymbol{e}_4=(0,0,0,1)$, 矩阵:

$$\begin{pmatrix}\boldsymbol{c}\\ \boldsymbol{e}_2+\boldsymbol{c}\\ \boldsymbol{e}_3+\boldsymbol{c}\\ \boldsymbol{e}_4+\boldsymbol{c}\\ \boldsymbol{e}_1+\boldsymbol{e}_3+\boldsymbol{c}\\ \boldsymbol{e}_2+\boldsymbol{e}_3+\boldsymbol{c}\\ \boldsymbol{e}_2+\boldsymbol{e}_3+\boldsymbol{e}_4+\boldsymbol{c}\\ \boldsymbol{e}_1+\boldsymbol{e}_2+\boldsymbol{e}_3+\boldsymbol{e}_4+\boldsymbol{c}\end{pmatrix}=\begin{pmatrix}\boldsymbol{c}_1 & \boldsymbol{c}_2 & \boldsymbol{c}_3 & \boldsymbol{c}_4\\ \boldsymbol{c}_1 & 1+\boldsymbol{c}_2 & \boldsymbol{c}_3 & \boldsymbol{c}_4\\ \boldsymbol{c}_1 & \boldsymbol{c}_2 & 1+\boldsymbol{c}_3 & \boldsymbol{c}_4\\ \boldsymbol{c}_1 & \boldsymbol{c}_2 & \boldsymbol{c}_3 & 1+\boldsymbol{c}_4\\ 1+\boldsymbol{c}_1 & \boldsymbol{c}_2 & 1+\boldsymbol{c}_3 & \boldsymbol{c}_4\\ \boldsymbol{c}_1 & 1+\boldsymbol{c}_2 & 1+\boldsymbol{c}_3 & \boldsymbol{c}_4\\ \boldsymbol{c}_1 & 1+\boldsymbol{c}_2 & 1+\boldsymbol{c}_3 & 1+\boldsymbol{c}_4\\ 1+\boldsymbol{c}_1 & 1+\boldsymbol{c}_2 & 1+\boldsymbol{c}_3 & 1+\boldsymbol{c}_4\end{pmatrix}\tag{4}$$

所对应的 4 元布尔函数是平衡、满足严格雪崩准则、代数次数达到最大且没有非零线性结构(一定非退化)的。特别, 取 $\boldsymbol{c}=(0,0,0,0)$, 特征矩阵式(4)所对应的布尔函数的小项表示

和代数标准形是

$$\begin{aligned}&x_1x_2x_3x_4+x_1(x_2+1)x_3x_4+x_1x_2(x_3+1)x_4+x_1x_2x_3(x_4+1)\\&\quad+(x_1+1)x_2(x_3+1)x_4+x_1(x_2+1)(x_3+1)x_4\\&\quad+x_1(x_2+1)(x_3+1)(x_4+1)+(x_1+1)(x_2+1)(x_3+1)(x_4+1)\\&=1+x_2+x_3+x_4+x_1x_4+x_2x_3+x_3x_4+x_1x_2x_3+x_1x_2x_4,\\&\qquad(x_1,x_2,x_3,x_4)\in \mathrm{GF}^4(2)\end{aligned}$$

不难直接验证此布尔函数确实平衡、满足严格雪崩准则、代数次数达到最大且没有非零线性结构(一定非退化)。

注 3　联系单炜娟在文献[2]中的工作又知，若在上述定理 2 中添加特征矩阵“列平衡”的条件，则得到布尔函数既相关免疫也满足严格雪崩准则的矩阵刻画。

根据满足一阶相关免疫的 n 元平衡布尔函数的代数次数不超过 $n-2$[8] 和引理 3，我们还可得到 n 元平衡布尔函数 $f(\boldsymbol{x})$ 满足严格雪崩准则、一阶相关免疫且代数次数达到最大的充分必要条件是其特征矩阵满足:

(1) 对任意的 $\boldsymbol{e}_r$, $1\le r\le n$, $f(\boldsymbol{x})$ 的特征矩阵式(2)中的行向量 $\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_{2^{n-1}}$ 存在且仅存在 2^{n-3} 对(与 $\boldsymbol{e}_r$ 有关的) (i,j), $1\le i\ne j\le k$, 使得 $\boldsymbol{e}_r=\boldsymbol{c}_i+\boldsymbol{c}_j$;

(2) “列平衡”且至少存在两列，这两列组成的矩阵中行向量为 (1,1) 的个数为奇数。

4　平衡且满足严格雪崩准则的布尔函数的两种特殊的“递补”构造法

根据前述定理 2，在变元个数 n 较少时，我们通过直接分析(必要时再通过微机搜索)可以构造出所有平衡且满足严格雪崩准则的 n 元布尔函数，例如通过直接分析不难知在所谓“等价”的意义下平衡且满足严格雪崩准则的 3 元布尔函数的特征矩阵必为如下形式之一:

$$\begin{pmatrix}\boldsymbol{c}\\ \boldsymbol{e}_1+\boldsymbol{c}\\ \boldsymbol{e}_2+\boldsymbol{c}\\ \boldsymbol{e}_3+\boldsymbol{c}\end{pmatrix},\begin{pmatrix}\boldsymbol{c}\\ \boldsymbol{e}_1+\boldsymbol{c}\\ \boldsymbol{e}_2+\boldsymbol{c}\\ \boldsymbol{e}_1+\boldsymbol{e}_3+\boldsymbol{c}\end{pmatrix},\begin{pmatrix}\boldsymbol{c}\\ \boldsymbol{e}_1+\boldsymbol{c}\\ \boldsymbol{e}_1+\boldsymbol{e}_2+\boldsymbol{c}\\ \boldsymbol{e}_1+\boldsymbol{e}_2+\boldsymbol{e}_3+\boldsymbol{c}\end{pmatrix},\begin{pmatrix}\boldsymbol{c}\\ \boldsymbol{e}_1+\boldsymbol{c}\\ \boldsymbol{e}_1+\boldsymbol{e}_2+\boldsymbol{c}\\ \boldsymbol{e}_1+\boldsymbol{e}_3+\boldsymbol{c}\end{pmatrix}$$

其中 $\boldsymbol{c}=(\boldsymbol{c}_1,\boldsymbol{c}_2,\boldsymbol{c}_3)\in \mathrm{GF}^3(2)$ 任意选定，而 $\boldsymbol{e}_1=(1,0,0)$, $\boldsymbol{e}_2=(0,1,0),\boldsymbol{e}_3=(0,0,1)$, 由此容易得到三元平衡且满足严格雪崩准则的布尔函数共 32 个; 同理，经直接分析并再通过微机搜索我们还找到了所有 1368 个四元平衡且满足严格雪崩准则的布尔函数。

无庸讳言，随着变元个数 n 的增大，用上述方法构造全部平衡且满足严格雪崩准则的 n 元布尔函数的难度将异乎寻常地增大，但我们总可依据定理 2 采用很普通的“递补法”——在待定的 2^{n-1} 个特征向量中逐次选定若干个，以最终确保所有的 $\boldsymbol{e}_i$, $1\le i\le n$ 都能且仅能被选到的 2^{n-1} 个向量中的某 2^{n-3} 对的和表出——构造“许许多多”的平衡且满足严格雪崩准则的 n 元布尔函数。

(1) 例如，对 $n\ge 5$, 选定任一 $\boldsymbol{c}\in \mathrm{GF}^n(2)$, 在待定的 2^{n-1} 个特征向量中先选定:

$$\begin{aligned}&\boldsymbol{c},\boldsymbol{e}_i+\boldsymbol{c},1\le i\le n-2,\boldsymbol{e}_i+\boldsymbol{e}_j+\boldsymbol{c},1\le i<j\le n-2,\cdots,\\&\boldsymbol{e}_{i_1}+\cdots+\boldsymbol{e}_{i_p}+\boldsymbol{c},\ 1\le i_1<\cdots<i_p\le n-2,3\le p\le n-3,\cdots,\\&\boldsymbol{e}_1+\boldsymbol{e}_2+\cdots+\boldsymbol{e}_{n-2}+\boldsymbol{c}\end{aligned}$$

不难知 $\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_{n-2}$ 中的每一个都能且仅能被选到的这 2^{n-2} 个中的某 2^{n-3} 对的和表出，由于 $n\ge 5$ 时，成立

$$C_{n-2}^2+\cdots+C_{n-2}^{n-3}=2^{n-2}-n>2^{n-3}-2$$

故我们可以在

$$\boldsymbol{e}_i+\boldsymbol{e}_j,1\le i<j\le n-2,\cdots,\boldsymbol{e}_{i_1}+\cdots+\boldsymbol{e}_{i_{n-3}},\ 1\le i_1<\cdots<i_{n-3}\le n-2$$

这 $L=2^{n-2}-n$ 个向量中任意选取出 $l=2^{n-3}-2$ 个，记为 $\boldsymbol{a}_i$, $1\le i\le l$, 再在待定的特征向量中补进

$$\begin{aligned}&\boldsymbol{e}_{n-1}+\boldsymbol{c},\boldsymbol{e}_n+\boldsymbol{c},\boldsymbol{e}_{n-1}+\boldsymbol{e}_n+\boldsymbol{c},\boldsymbol{a}_i+\boldsymbol{e}_{n-1}+\boldsymbol{c},\ 1\le i\le l,\ \boldsymbol{a}_i+\boldsymbol{e}_n+\boldsymbol{c},\\&\qquad 1\le i\le l,\boldsymbol{e}_1+\boldsymbol{e}_2+\cdots+\boldsymbol{e}_{n-2}+\boldsymbol{e}_{n-1}+\boldsymbol{e}_n+\boldsymbol{c}\end{aligned}$$

这 $3+2l+1=3+2(2^{n-3}-2)+1=2^{n-2}$ 个，易知 $\boldsymbol{e}_{n-1},\boldsymbol{e}_n$ 都能且仅能被选到的这 2^{n-2} 个向量中的某 2^{n-3} 对的和表出，即以这些向量为特征向量的 n 元布尔函数是平衡且满足严格雪崩准则的。不难知，用这种方法我们至少可以得到 $C_{2^{n-2}-n}^{2^{n-3}-2}$ 个满足要求的函数。以下就是 $n=5$ 时用上述方法得到的一例:

$$\begin{aligned}&x_1x_2x_3x_4+x_1x_2x_3x_5+x_1x_2x_4x_5+x_1x_3x_4x_5+x_2x_3x_4x_5+x_1x_4x_5\\&+x_2x_4x_5+x_3x_4x_5+x_2x_3x_4+x_2x_3x_5+x_1x_2+x_1x_3+x_1x_4+x_1x_5\\&+x_2x_3+x_1+x_2+x_3+x_4+x_5+1,\ (x_1,x_2,x_3,x_4,x_5)\in \mathrm{GF}^5(2)\end{aligned}$$

(2) 又如，根据任一 n 元布尔函数 $f(x_1,\cdots,x_{n-1},x_n)$ 都能分解为

$$\begin{aligned}&f(x_1,\cdots,x_{n-1},x_n)=f_1(x_1,\cdots,x_{n-1})x_n+f_2(x_1,\cdots,x_{n-1}),\\&\qquad(x_1,\cdots,x_{n-1})\in \mathrm{GF}^{n-1}(2),\ x_n\in \mathrm{GF}(2)\end{aligned}\tag{5}$$

设 $n-1$ 元布尔函数 $f_1(x_1,\cdots,x_{n-1})$ 是平衡的，其特征向量构成的集合为

$$\boldsymbol{A}_1=\{\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_k\},\quad \boldsymbol{a}_i\in \mathrm{GF}^{n-1}(2),\quad 1\le i\le k=2^{n-2}$$

为记号简略，$f_1(x_1,\cdots,x_{n-1})$ 的特征矩阵仍记为 $\boldsymbol{A}_1$，又设 $n-1$ 元布尔函数 $f_2(x_1,\cdots,x_{n-1})$ 的汉明重量是 2^{n-3}，其特征向量构成的集合为

$$\boldsymbol{A}_2=\{\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_r\},\quad \boldsymbol{b}_j\in \mathrm{GF}^{n-1}(2),\quad 1\le j\le r=2^{n-3}$$

同样为记号简略，$f_2(x_1,\cdots,x_{n-1})$ 的特征矩阵也记为 $\boldsymbol{A}_2$; 且设 $\boldsymbol{A}_1\cap\boldsymbol{A}_2=\phi$，这时根据式 (5) 易知 n 元布尔函数 $f(x_1,\cdots,x_{n-1},x_n)$ 的特征矩阵为

$$\boldsymbol{B}=\begin{pmatrix}\boldsymbol{A}_1 & 0\\ \boldsymbol{A}_2 & 0\\ \boldsymbol{A}_3 & 0\end{pmatrix}$$

显然函数 $f(x_1,\cdots,x_{n-1},x_n)$ 是平衡的，且根据 $(\boldsymbol{b}_j,0)+(\boldsymbol{b}_j,1)=(0,\cdots,0,1)$, $1\le j\le 2^{n-3}$ 等知 $\boldsymbol{e}_n=(0,\cdots,0,1)\in \mathrm{GF}^n(2)$ 能且仅能被 $\boldsymbol{B}$ 中 2^{n-3} 对向量的和表出，由此不难知在上述条件下布尔函数 $f(x_1,\cdots,x_{n-1},x_n)$ 满足严格雪崩准则当且仅当对任意的 $1\le j\le r=2^{n-3}$，都有

$$\begin{aligned}&(\boldsymbol{A}_1,0)+(\boldsymbol{b}_j,0)\hat{=}\{(\boldsymbol{a}_1,0)+(\boldsymbol{b}_j,0),(\boldsymbol{a}_2,0)+(\boldsymbol{b}_j,0),\cdots,\\&\qquad(\boldsymbol{a}_k,0)+(\boldsymbol{b}_j,0)\}\supset\{\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_{n-1}\}\end{aligned}$$

容易知道 n 充分大后，满足上述条件的$\boldsymbol{A}_1$是大量存在的，且由此可知作为充分条件就有

(1) 若$\boldsymbol{A}_1$中向量的汉明重量全为偶数(包含 0)或者 (2) 若$\boldsymbol{A}_1$中向量的汉明重量全为奇数，则 $f(x_1,\cdots,x_{n-1},x_n)$ 在所有汉明重量为奇数的$\boldsymbol{s}$处满足扩散准则，自然就满足严格雪崩准则。

事实上，若$\boldsymbol{A}_1$中向量的汉明重量全为偶数(包含 0)，则因为$\boldsymbol{A}_2$中 $\boldsymbol{b}_j$，$1\le j\le r=2^{n-3}$ 的汉明重量都为奇数，故易知

$$\begin{aligned}\boldsymbol{A}_1+\boldsymbol{b}_j &\hat{=}\left\{\boldsymbol{a}_1+\boldsymbol{b}_j,\boldsymbol{a}_2+\boldsymbol{b}_j,\cdots,\boldsymbol{a}_k+\boldsymbol{b}_j\right\}\\ &=\mathrm{GF}^{n-1}(2)\setminus\boldsymbol{A}_1,\quad 1\le j\le r=2^{n-3}\end{aligned}$$

即对 $\mathrm{GF}^n(2)$ 中汉明重量为奇数的每一 $\boldsymbol{s}$，都存在 $\boldsymbol{a}_{j_s}\in\boldsymbol{A}_1$, $1\le j\le 2^{n-3}$，使得

$$\boldsymbol{s}=(\boldsymbol{a}_{1_s},0)+(\boldsymbol{b}_1,0)=(\boldsymbol{a}_{2_s},0)+(\boldsymbol{b}_2,0)=\cdots=(\boldsymbol{a}_{r_s},0)+(\boldsymbol{b}_r,0)$$

即每一汉明重量为奇数的$\boldsymbol{s}$都能被$\boldsymbol{B}$中 2^{n-3} 对向量的和表出。且易知 $\boldsymbol{B}$ 中其它任意一对向量的和都不能表示出这样的$\boldsymbol{s}$。若 $\boldsymbol{A}_1$ 中向量的汉明重量全为奇数，则因为 $\boldsymbol{A}_2$ 中 $\boldsymbol{b}_j$，$1\le j\le r=2^{n-3}$ 的汉明重量全为偶数(包含 0)，故易知

$$\boldsymbol{A}_1+\boldsymbol{b}_j\hat{=}\left\{\boldsymbol{a}_1+\boldsymbol{b}_j,\boldsymbol{a}_2+\boldsymbol{b}_j,\cdots,\boldsymbol{a}_k+\boldsymbol{b}_j\right\}=\boldsymbol{A}_1,\ 1\le j\le r=2^{n-3}$$

由此同样可知每一汉明重量为奇数的 $\boldsymbol{s}$ 都能且仅被 $\boldsymbol{B}$ 中 2^{n-3} 对向量的和表出。又不难知用这种方法构造出的平衡且满足严格雪崩准则的 n 元布尔函数至少有 $C_{2^{n-3}}^{2^{n-3}}$ 个。

而满足上述条件(1)或(2)的函数恰为

$$\begin{aligned}&(x_1+\cdots+x_{n-1}+a)x_n+f_2(x_1,\cdots,x_{n-1}),(x_1,\cdots,x_{n-1})\\ &\qquad\in\mathrm{GF}^{n-1}(2),\quad x_n\in\mathrm{GF}(2)\end{aligned}$$

其中 $a=0$ 或 1，它正以人们已知的某些满足严格雪崩准则的函数为其特例[9]。

应用本文的基本结论来进一步探讨构造具有扩散特性等的布尔函数的方法，我们还做了不少工作，限于篇幅，恕不能在此一一列出。

5 结束语

同行们和本文的工作都表明通过布尔函数的特征矩阵来刻画其相关免疫性、扩散性等重要密码学性质并构造具有这些性质的某类函数常常是直接了当的(如依据条件逐次递补出符合要求的特征向量等)，可以说思想简单、构造易行(特别是在变元个数较少的情况下)。而且联系单炜娟在文献[2]中的工作易知，若在本文定理 2 等中再添加特征矩阵“列平衡”的条件，则得到布尔函数既相关免疫也满足有关特殊扩散特性的矩阵刻画；我们进一步的研究结果还表明，通过特征矩阵刻画布尔函数的高阶扩散特性并给出相应的构造方法等也是可行的。因此，在研究密码学中逻辑函数的有关特殊性质时直接借助其特征矩阵的思想方法值得一试。

参 考 文 献

[1] Forre R. The strict avalanche criterion: Properties of Boolean functions and extended definition. Advances in Crytology -Crypt’88, Springer-Verlag, 1990: 450−468.

[2] 单炜娟. 相关免疫函数的结构和构造. 应用数学学报, 1991,(3): 331−336.

[3] 杨义先. 相关免疫布尔函数的计数. 电子科学学刊, 1993, 15(2): 140−146.

[4] 王隽, 李世取. Bent 函数的一般构造法. 高校应用数学学报, 1999, (4): 473−479.

[5] 温巧燕, 钮心忻, 杨义先. 现代密码学中的布尔函数. 北京: 科学出版社, 2000: 5−6.

[6] 冯登国, 裴定一. 密码学导引. 北京: 科学出版社, 1999: 81.

[7] Webster A F, Tavares S E. On the Design of S-Boxes. Advances in Cryptology-Crypt’85, Springer-Verlag, 1986: 523−534.

[8] 王育民, 何大可. 保密学—基础与应用. 西安: 西安电子科技大学出版社, 1990: 154.

[9] 杨义先, 林须端. 编码密码学, 北京: 人民邮电出版社, 1992: 81−82.

郭锦辉： 女， 1979 年生，硕士生，研究方向为逻辑函数在密码学中的应用.

李世取： 男， 1945 年生，教授，博士生导师，研究领域包括密码学与信息安全.