doi:10.3969/j.issn.1000-436x.2013.08.011

平衡 *H* 布尔函数的相关免疫性研究

李卫卫
(上海政法学院 现代教育技术中心，上海 201701)

摘 要：引入布尔函数的 *E*-导数，并结合导数一起作为工具讨论关系密码系统安全性能的平衡 *H* 布尔函数的相关免疫性。通过 *E*-导数和导数深入揭示了平衡 *H* 布尔函数 0 和 1 值的分布结构，得出判定 *H* 布尔函数是否相关免疫的重要结果。并得以采用区分不同结构的计算方法来简化计算，解决了平衡 *H* 布尔函数相关免疫最高阶数这一问题。

关键词：*H* 布尔函数；*E*-导数；相关免疫性；信息安全；密码学
中图分类号：TP391 **文献标识码**：A **文章编号**：1000-436X(2013)08-0082-06

Correlation-immunity study of balanced *H*-Boolean functions

LI Wei-wei
(Modern Education Technology Center , Shanghai University of Political Science and Law, Shanghai 201701,China)

Abstract: As a novel definition, *E*-derivative was introduced to study problems that are extremely difficult to handle in the cryptographic system. By using the way of combining derivative with *E*-derivative and correlation-immunity of *H*-Boolean functions, the distribution structure of balanced *H*-Boolean functions were deeply analyzed, and some important results on how to determine whether or not a *H*-Boolean function has correlation-immunity with the relatively simplified method of distinguishing different structure were also obtained, which are going to play important roles in the field of cryptology and future worldwide applications. Beyond that, the problem of the most higher-order correlation-immunity of *H*-Boolean function which is also one of the most difficult unsolved problems in cryptology was solved successfully to improve the anti-attack ability of cryptosystem and ensured the secure transmission of secret information on the network effectively .

Key words: *H*-Boolean functions; *E*-derivative; correlation-immunity; information security; cryptology

1 引言

布尔函数是密码系统中一个重要的组成部分，其密码学性质直接关系到密码系统的安全性能。然而并非任意一个布尔函数都可以应用于密码体制中，为了确保密码系统具有较强的保密功能，要求所使用的布尔函数必须满足一定的性质，如平衡性、相关免疫性、有高的代数次数、高的非线性度、具有扩散性和严格雪崩特性等。但研究发现想要找到同时具备这些性质的优良布尔函数并不容易，因为这些性质之间往往存在着一定的制约关系，一种性能指标的实现或提高，可能必然要降低另外一些性能的指标。因此，研究分析密码学各性质之间的关系，并找到更多的具有优良密码学性质的布尔函数就成为密码学中的一个重要的研究课题。

本文所讨论的平衡 *H* 布尔函数是密码学中的一类重要函数，平衡 *H* 布尔函数既具有平衡性，又能够满足一次扩散准则，在密码系统中具有重要的应用价值，而且 Bent 函数又是 *H* 布尔函数的子类，所以国内外专家对它的研究也一直很活跃。也取得了一定成果，杨义先教授提出了构造四元 *H* 布尔函数的方法，并得出了一些重要定理。最后还对平衡 *H* 布尔函数、相关免疫 *H* 布尔函数的结构特点和性质进行了讨论。本文将在此基础之上，利用一种新的研究方

收稿日期：2012-11-07；**修回日期**：2013-02-08
基金项目：上海市优秀青年教师科研专项基金资助项目（shzf018）
Foundation Item: The Excellent Youth Scholars Foundation of Shanghai (shzf018)

法来研究分析平衡 H 布尔函数的相关免疫性问题，如果能够证明平衡 H 布尔函数具有至少一阶相关免疫性，将使它在密码系统的应用中能够进一步提高系统的抗 DC 攻击能力，这对密码学的发展有着重要意义。

2　预备知识

为了后面讨论相关免疫性的需要，先给出 E-导数的定义及几个 H 布尔函数、E-导数、导数及线性函数关系的一些相关引理。

定义 1[1]　布尔函数 $f(x)$ 的 E-导数为

$$ef(x)/ex_i = f(x_1,\cdots,x_{i-1},x_i,x_{i+1},\cdots,x_n)\cdot f(x_1,\cdots,x_{i-1},(x_i+1),x_{i+1},\cdots,x_n)$$

其中，$i=1,2,\cdots,n$。

引理 1[1]　布尔函数 $f(x)$ 的 E-导数有如下形式。

$$ef(x)/ex_i = f(x_1,\cdots,x_{i-1},1,x_{i+1},\cdots,x_n)\cdot f(x_1,\cdots,x_{i-1},0,x_{i+1},\cdots,x_n)$$

其中，$i=1,2,\cdots,n$。

引理 2[1]　对布尔函数 $f(x)$，有

$$\mathrm{d}f(x)/\mathrm{d}x_i \cdot ef(x)/ex_i = 0,(i=1,2,\cdots,n)$$

引理 3[2]　布尔函数 $f(x)$ 是平衡 H 布尔函数，当且仅当 $wt(\mathrm{d}f(x)/\mathrm{d}x_i)=2^{n-1}$，且

$$wt(ef(x)/ex_i)=2^{n-2},(i=1,2,\cdots,n)$$

引理 4[2]　对布尔函数 $f(x)$，有

$$f(x)=f(x)\mathrm{d}f(x)/\mathrm{d}x_i + ef(x)/ex_i \quad (i=1,2,\cdots,n)$$

$$wt(f(x))=wt(f(x)\mathrm{d}f(x)/\mathrm{d}x_i)+wt(ef(x)/ex_i) \quad (i=1,2,\cdots,n)$$

$$wt(f(x))=2^{-1}wt(\mathrm{d}f(x)/\mathrm{d}x_i)+wt(ef(x)/ex_i) \quad (i=1,2,\cdots,n)$$

引理 5[2]　布尔函数 $f(x)$ 是 H 布尔函数，当且仅当 $wt(\mathrm{d}f(x)/\mathrm{d}x_i)=2^{n-1},(i=1,2,\cdots,n)$。

3　平衡 H 布尔函数的一阶相关免疫性

通过对平衡 H 布尔函数一阶相关免疫性的研究，可以简化检测平衡 H 布尔函数是否一阶相关免疫的计算[3,4]，从而能很容易地构造高维一阶相关免疫的平衡 H 布尔函数，得出许多重要的密码学性质和定理。

定理 1　设 $f(x)$ 是平衡 H 布尔函数，且 $f(x)=(1+x_1)f_{\mathrm{p}}(x)+x_1f_{\mathrm{q}}(x)$，其中，$f_{\mathrm{p}}(x)$，$f_{\mathrm{q}}(x)$，$(x=(x_2,\cdots,x_n))$均为 $n-1$ 维布尔函数，$wt(g(x))_r$ 表示当 $g(x)$ 是 r 维函数时的重量。

1) 若

$$\partial f(x)/\partial(x_1,x_2,\cdots,x_n)=0 \tag{1}$$

则 $f(x)$ 是一阶相关免疫函数，且 $f_{\mathrm{p}}(x)$、$f_{\mathrm{q}}(x)$ 均为 $n-1$ 维平衡 H 布尔函数。

2) 若

$$\partial f(x)/\partial(x_2,x_3,\cdots,x_n)=0 \tag{2}$$

则 $f(x)$ 是一阶相关免疫函数，且 $f_{\mathrm{p}}(x)$、$f_{\mathrm{q}}(x)$ 均为 $n-1$ 维一阶相关免疫的平衡布尔函数。

证明　1) 由式(1)求偏导数时函数值相加的特点，且 $f(x)$ 是平衡的，则对 $a_i\in \mathrm{GF}(2)$，显然有

$$wt(f(x)\,|\,x_i=a_i)=2^{-1}wt(f(x))=2^{n-2} \tag{1a}$$

故 $f(x)$ 是一阶相关免疫函数。

记 $h=(0,0,\cdots,0)$，$h\in \mathrm{GF}(2)^n$，则由于 $\partial f(x)/\partial(x_1,\cdots x_n)=f_{\mathrm{p}}(x)+f_{\mathrm{q}}(x^h)=0$，则必有

$$f_{\mathrm{p}}(x)=f_{\mathrm{q}}(x^h)$$

故

$$\begin{aligned} wt(f(x)) &= wt(f_{\mathrm{p}}(x))_{n-1}+wt(f_{\mathrm{q}}(x))_{n-1} \\ &= wt(f_{\mathrm{p}}(x))_{n-1}+wt(f_{\mathrm{q}}(x^h))_{n-1} \\ &= 2wt(f_{\mathrm{p}}(x))_{n-1}=2^{n-1} \end{aligned} \tag{1b}$$

所以

$$wt(f_{\mathrm{p}}(x))_{n-1}=wt(f_{\mathrm{q}}(x))_{n-1}=2^{-1}wt(f(x))=2^{n-2}$$

即 $f_{\mathrm{p}}(x)$、$f_{\mathrm{q}}(x)$ 均为 $n-1$ 维平衡布尔函数。

由于 $f_{\mathrm{p}}(x)=f_{\mathrm{q}}(x^h)$，显然有

$$\begin{aligned} ef_{\mathrm{q}}(x)/ex_i &= f(x_i=1)f(x_i=0) \\ &= f(x_i=0)f(x_i=1) \\ &= ef_{\mathrm{q}}(x^h)/ex_i,\ (i=2,3,\cdots,n) \end{aligned} \tag{1c}$$

故知

$$\begin{aligned} wt(ef_{\mathrm{p}}(x)/ex_i)_{n-1} &= wt(ef_{\mathrm{q}}(x)/ex_i)_{n-1} \\ &= 2^{-1}wt(ef(x)/ex_i) \\ &= 2^{n-3},(i=2,3,\cdots,n) \end{aligned} \tag{1d}$$

又由于

$$wt(f_{\mathrm{p}}(x))_{n-1}=2^{-1}wt(\mathrm{d}f_{\mathrm{p}}(x)/\mathrm{d}x_i)_{n-1}+$$

$$wt(ef_{\mathrm{p}}(x)/ex_i)_{n-1}=2^{n-2} \tag{1e}$$

故知 $wt(\mathrm{d}f_{\mathrm{p}}(x)/\mathrm{d}x_i)=2^{n-2},\ (i=2,3,\cdots,n)$ (1f)

同理，有

$$wt(\mathrm{d}f_{\mathrm{q}}(x)/\mathrm{d}x_i)=2^{n-2},\ (i=2,3,\cdots,n) \tag{1g}$$

故知 $f_{\mathrm{p}}(x)$、$f_{\mathrm{q}}(x)$ 均为 $n-1$ 维 H 布尔函数。

2) 由式(2)可知，对 $a_i\in \mathrm{GF}(2)$，有

$$\begin{aligned}&wt(f_{\mathrm{p}}(x)\,|\,x_i=a_i)_{n-1}=2^{-1}wt(f_{\mathrm{p}}(x))_{n-1}\\&wt(f_{\mathrm{q}}(x)\,|\,x_i=a_i)_{n-1}=2^{-1}wt(f_{\mathrm{q}}(x))_{n-1}\end{aligned} \tag{2a}$$

故

$$\begin{aligned}&wt(f(x)\,|\,x_i=a_i)=wt(f_{\mathrm{p}}(x)\,|\,x_i=a_i)_{n-1}+\\&wt(f_{\mathrm{q}}(x)\,|\,x_i=a_i)_{n-1}=2^{-1}wt(f_{\mathrm{p}}(x))_{n-1}+2^{-1}\cdot\\&wt(f_{\mathrm{q}}(x))_{n-1}=2^{-1}wt(f(x))_n=2^{n-2}\end{aligned} \tag{2b}$$

所以，$f(x)$ 是一阶相关免疫函数。

因此有

$$wt(f(x)+x_1)=wt(f(x))+wt(x_1)-2wt(x_1f_{\mathrm{q}}(x))=2^{n-1} \tag{2c}$$

故 $wt(f_{\mathrm{q}}(x))_{n-1}=2^{n-2}$，即 $f_{\mathrm{q}}(x)$ 为 $n-1$ 维平衡布尔函数。于是显然 $f_{\mathrm{p}}(x)$ 也必是 $n-1$ 维平衡布尔函数。

由于 $wt(f_{\mathrm{p}}(x))_{n-1}=2^{n-2}$，且

$$wt(\partial f_{\mathrm{p}}(x)/\partial(x_2,\cdots,x_n))=0$$

故知

$$\begin{aligned}wt(f_{\mathrm{p}}(x)\,|\,x_i=0)_{n-1}&=wt(f_{\mathrm{p}}(x)\,|\,x_i=1)_{n-1}\\&=2^{-1}wt(f_{\mathrm{p}}(x))_{n-1}\\&=2^{n-3}\end{aligned} \tag{2d}$$

所以，$f_{\mathrm{p}}(x)$ 为 $n-1$ 维一阶相关免疫函数。同理，$f_{\mathrm{q}}(x)$ 也是 $n-1$ 维一阶相关免疫函数。

推论 1 设 $f(x)$ 是平衡 H 布尔函数，以变换向量 $\boldsymbol{h}_1=(0,0,\cdots,0)$，$\boldsymbol{h}_2=(1,0,\cdots,0)$ 分别对 $f(x)$ 做变换。若

$$f(x^{\boldsymbol{h}_1})+f(x)=0 \tag{3}$$

或

$$f(x^{\boldsymbol{h}_2})+f(x)=0 \tag{4}$$

则 $f(x)$ 是一阶相关免疫的。

定理 2 对布尔函数 $f(x)$，有

1) 平衡布尔函数 $f(x)$ 是一阶相关免疫的，当且仅当

$$wt(x_if(x))=2^{n-2},\ (i=1,2,\cdots,n) \tag{5}$$

或

$$wt((1+x_i)f(x))=2^{n-2},(i=1,2,\cdots,n) \tag{6}$$

2) 若 $f(x)$ 是三维平衡 H 布尔函数，则必有

$$wt(f(x)\,|\,x_i=0)\neq wt(f(x)\,|\,x_i=1) \tag{7}$$

即三维平衡 H 布尔函数一定不是相关免疫的。

证明 1) 因为

$wt(f(x)+x_i)=wt(f(x))+wt(x_i)-2wt(x_if(x));$

$wt(f(x)+(1+x_i))=2^n-wt(f(x)+x_i)=wtf(x)+wt(1+x_i)-2wt((1+x_i)f(x)),(i=1,2,\cdots,n)$。因而可知结论成立。

2) $f(x)$ 是三维平衡 H 布尔函数，则必有 $wt(ef(x)/ex_n\,|\,x_i=a_i)=1$，$a_i\in\mathrm{GF}(2)$，又由于 $wt(\mathrm{d}f(x)/\mathrm{d}x_i)=4$，故知在求解导数时必定存在一对数字 1 在做异或运算后而被消除掉。故知式(7)成立。所以不存在相关免疫的三维平衡 H 布尔函数。

定理 2 虽然简单，但在后面的证明中要用到，而且式(5)和式(6)用起来很方便。

定理 3 平衡 H 布尔函数 $f(x)$ 是一阶相关免疫的，当且仅当

$$\begin{aligned}&wt(f(x)\mathrm{d}f(x)/\mathrm{d}x_{\mathrm{r}}\,|\,x_i=a_i)=wt(ef(x)/ex_{\mathrm{r}}\,|\\&\qquad x_i=a_i)=2^{n-3},a_i\in\mathrm{GF}(2)\end{aligned} \tag{8}$$

证明 由于 $f(x)$ 是平衡 H 布尔函数，且由 $ef(x)/ex_{\mathrm{r}}$ 的结构特点知必有

$$wt(ef(x)/ex_{\mathrm{r}}\,|\,x_i=a_i)=2^{n-3},a_i\in\mathrm{GF}(2) \tag{9}$$

若式(8)成立，则有

$$\begin{aligned}&wt(f(x)\,|\,x_i=a_i)=wt(f(x)\mathrm{d}f(x)/\mathrm{d}x_{\mathrm{r}}\,|\,x_i=a_i)+\\&\qquad wt(ef(x)/ex_{\mathrm{r}}\,|\,x_i=a_i)=2^{-1}wt(f(x))\end{aligned} \tag{10}$$

即 $f(x)$ 是一阶相关免疫的。

反之，若 $f(x)$ 是一阶相关免疫的，则式(10)成立，且又因式(9)成立，故式(8)成立。

这个定理使得可以简化检测平衡 H 布尔函数是否一阶相关免疫的计算。

为下面证明的需要，做如下设定：设 $f_{\mathrm{p}}(x)$ 和 $f_{\mathrm{q}}(x),x=(x_2,\cdots,x_n)$ 是 2 个 $n-1$ 维布尔函数，$f_{\mathrm{p}_1}(x)$，$f_{\mathrm{p}_2}(x)$，$f_{\mathrm{q}_1}(x)$，$f_{\mathrm{q}_2}(x),(x=(x_3,\cdots,x_n))$ 是 4 个 $n-2$ 维布尔函数，记

$$f(x)=(1+x_1)f_{\mathrm{p}}(x)+x_1f_{\mathrm{q}}(x) \tag{11}$$

$$f_{\mathrm{p}}(x)=(1+x_2)f_{\mathrm{p}_1}(x)+x_2f_{\mathrm{p}_2}(x)$$
$$f_{\mathrm{q}}(x)=(1+x_2)f_{\mathrm{q}_1}(x)+x_2f_{\mathrm{q}_2}(x) \quad (12)$$

记 $n-3$ 维布尔函数为

$f_{\mathrm{p}_{11}}(x)$, $f_{\mathrm{p}_{12}}(x)$, $f_{\mathrm{p}_{13}}(x)$, $f_{\mathrm{p}_{14}}(x)$, $f_{\mathrm{q}_{11}}(x)$, $f_{\mathrm{q}_{12}}(x)$, $f_{\mathrm{q}_{13}}(x)$, $f_{\mathrm{q}_{14}}(x)$, $x=(x_4,\cdots,x_n)$，并如式(11)和式(12)一样，对 $f_{\mathrm{p}_1}(x)$, $f_{\mathrm{p}_2}(x)$, $f_{\mathrm{q}_1}(x)$, $f_{\mathrm{q}_2}(x)$ 进行构造。如：

$$f_{\mathrm{p}_1}(x)=(1+x_3)f_{\mathrm{p}_{11}}(x)+x_3f_{\mathrm{p}_{12}}(x),\cdots$$

定理 4　设 $f(x)$ 为 n 元布尔函数，且 $f(x)=(1+x_1)f_{\mathrm{p}}(x)+x_1f_{\mathrm{q}}(x)$。

1) 若 $f(x)$ 是 n 维一阶相关免疫的平衡 H 布尔函数，且 $f_{\mathrm{p}}(x)$ 是 $n-1$ 维一阶相关免疫的 H 布尔函数，则 $f_{\mathrm{q}}(x)$ 是 $n-1$ 维一阶相关免疫的平衡 H 布尔函数。且有

$$wt(f_{\mathrm{p}}(x)f_{\mathrm{q}}(x))_n=2^{n-2} \quad (13)$$

2) 若 $f_{\mathrm{p}}(x)$, $f_{\mathrm{q}}(x)$ 均为 $n-1$ 维一阶相关免疫的平衡 H 布尔函数，且有式(13)所示的关系，则 $f(x)$ 必为一阶相关免疫的平衡 H 布尔函数。

证明　1) 当 $f(x)$ 为一阶相关免疫函数，则由式(5)和式(6)可知

$$wt(x_1f(x))_n=wt(f_{\mathrm{q}}(x))_{n-1}=2^{n-2} \quad (14)$$
$$wt((1+x_1)f(x))_n=wt(f_{\mathrm{p}}(x))_{n-1}=2^{n-2} \quad (15)$$

故 $f_{\mathrm{p}}(x)$、$f_{\mathrm{q}}(x)$ 均为 $n-1$ 维平衡布尔函数。

又由于

$$wt(\mathrm{d}f(x)/\mathrm{d}x_1)=wt(f_{\mathrm{p}}(x))_n+wt(f_{\mathrm{q}}(x))_n-2wt(f_{\mathrm{p}}(x)f_{\mathrm{q}}(x))_n=2^{n-1} \quad (16)$$

$$wt(\mathrm{d}f(x)/\mathrm{d}x_i)=wt((1+x_1)\mathrm{d}f_{\mathrm{p}}(x)/\mathrm{d}x_i)_{n-1}+wt(x_1\mathrm{d}f_{\mathrm{q}}(x)/\mathrm{d}x_i)_{n-1}=2^{n-1},$$

(x_1 为 n 维，且 $i=2,3,\cdots,n$) (17)

$$wt(f(x)\,|\,x_i=a_i)=wt(f_{\mathrm{p}}(x)\,|\,x_i=a_i)+wt(f_{\mathrm{q}}(x)\,|\,x_i=a_i)=2^{n-2},a_i\in\mathrm{GF}(2) \quad (18)$$

于是由式(16)、式(17)及式(18)可知，结论成立。

2) 由式(11)可知

$$wt(f(x))_n=wt(f_{\mathrm{p}}(x))_{n-1}+wt(f_{\mathrm{q}}(x))_{n-1} \quad (19)$$

则由式(16)~式(19)可知 $f(x)$ 是平衡 H 布尔函数。

又由 $f(x)=(1+x_1)f_{\mathrm{p}}(x)+x_1f_{\mathrm{q}}(x)$，$f(x)$ 是 n 维一阶相关免疫的平衡 H 布尔函数，且 $f_{\mathrm{p}}(x)$ 是 $n-1$ 维一阶相关免疫的平衡 H 布尔函数，可知，当 $i=2,3,\cdots,n$ 时，式(18)成立。于是 $f(x)$ 是一阶相关免疫的。

故当 $f_{\mathrm{p}}(x)$ 和 $f_{\mathrm{q}}(x)$ 均为 $n-1$ 维一阶相关免疫的平衡 H 布尔函数，且 $wt(f_{\mathrm{p}}(x)f_{\mathrm{q}}(x))_n=2^{n-2}$ 时，$f(x)$ 是一阶相关免疫的平衡 H 布尔函数。

显然，定理中的条件都是可以实现的，因而可以按定理条件的要求，很容易地构造这一类型的高维一阶相关免疫的平衡 H 布尔函数[5~7]。

推论 2　若 $f(x)$ 是一阶相关免疫的，且 $f(x)=(1+x_1)f_{\mathrm{p}}(x)+x_1f_{\mathrm{q}}(x)$，$f_{\mathrm{p}}(x)$ 满足严格雪崩准则，则

$$wt(ef_{\mathrm{p}}(x)/ex_i)=wt(ef_{\mathrm{q}}(x)/ex_i)=2^{n-3},\quad i=2,3,\cdots,n \quad (20)$$

推论是显然成立的，不再证明。

定理 5　在 $f(x)=(1+x_1)f_{\mathrm{p}}(x)+x_1f_{\mathrm{q}}(x)$ 中，$f(x)$ 是平衡 H 布尔函数，

如果

1) $f_{\mathrm{p}}(x)$（或 $f_{\mathrm{q}}(x)$）是 $n-1$ 维平衡 H 布尔函数，且 $f_{\mathrm{p}}(x)$ 和 $f_{\mathrm{q}}(x)$ 满足式(13)，即

$$wt(f_{\mathrm{p}}(x)f_{\mathrm{q}}(x))_n=2^{n-2}$$

2) 对 $x_i(i=2,3,\cdots,n)$ 有

$$wt(x_i\mathrm{d}f_{\mathrm{p}}(x)/\mathrm{d}x_{\mathrm{r}})_{n-1}=wt(x_i\mathrm{d}f_{\mathrm{q}}(x)/\mathrm{d}x_{\mathrm{r}})_{n-1}=2^{n-3} \quad (21)$$

其中，$r\neq i$。

$$wt(x_ief_{\mathrm{p}}(x)/ex_{\mathrm{r}})_{n-1}=wt(x_ief_{\mathrm{q}}(x)/ex_{\mathrm{r}})_{n-1}=2^{n-4} \quad (22)$$

其中，$r\neq i$。

则平衡 H 布尔函数 $f(x)$ 是一阶相关免疫的。

证明　由定理 4 的式(16)~式(18)及定理 5 条件 1）可知，$f_{\mathrm{q}}(x)$ 是 $n-1$ 维平衡 H 布尔函数。又由于

$$wt(x_1f(x))=wt(x_1f_{\mathrm{q}}(x))=2^{n-2} \quad (23)$$

下面的证明中只对 $r\neq1$ 的 $f(x)$ 对 r 的导数和 E–导数来证。当 $r\neq i$ 时，

$$wt(x_if(x))=2^{-1}wt(x_i(1+x_1)\mathrm{d}f_{\mathrm{p}}(x)/\mathrm{d}x_{\mathrm{r}}+x_1\mathrm{d}f_{\mathrm{q}}(x)/\mathrm{d}x_{\mathrm{r}}))+wt(x_i(1+x_1)ef_{\mathrm{p}}(x)/ex_{\mathrm{r}}+x_1ef_{\mathrm{q}}(x)/ex_{\mathrm{r}}))=2^{-1}wt(x_i\mathrm{d}f_{\mathrm{p}}(x)/\mathrm{d}x_{\mathrm{r}})_{n-1}+wt(x_ief_{\mathrm{p}}(x)/ex_{\mathrm{r}})_{n-1}+2^{-1}wt(x_i\mathrm{d}f_{\mathrm{q}}(x)/\mathrm{d}x_{\mathrm{r}})_{n-1}+wt(x_ief_{\mathrm{q}}(x)/ex_{\mathrm{r}})=2^{n-2} \quad (24)$$

故由式(23)和式(24)且只对 $r=n-1$ 和 $r=n$ 可知，对一切 $i=1,2,3,\cdots,n$，均有

$$wt(x_if(x))=2^{n-2} \quad (25)$$

因此，由定理 2 的 1）可知，平衡 H 布尔函数 $f(x)$ 是一阶相关免疫函数。

此定理不仅把 $f(x)$ 分为 $f_{\mathrm{p}}(x)$ 和 $f_{\mathrm{q}}(x)$ 分别进行考察，做了判定的简化，而且更进一步由导数和 E−导数将 $f_{\mathrm{p}}(x)$ 和 $f_{\mathrm{q}}(x)$ 的各自不同性质的值分别进行考察，即进一步简化计算。

4 平衡 H 布尔函数的二阶相关免疫性

前面讨论了平衡 H 布尔函数是 CI 函数的情形。那么，对 $m\geqslant 2$，平衡 H 布尔函数还是 $CI(m)$ [8~10] 函数吗？下面讨论这一问题。

记 $f_{\mathrm{c}}(x)=\omega x$，$1\leqslant w(\omega)\leqslant m\leqslant n$，则

$$wt(f(x)+f_{\mathrm{c}}(x))=wt(f(x))+wt(f_{\mathrm{c}}(x))-2wt(f(x)f_{\mathrm{c}}(x)) \tag{26}$$

$$wt(f(x)+1+f_{\mathrm{c}}(x))=2^n-wt(f(x)+f_{\mathrm{c}}(x))=wt(f(x))+wt(1+f_{\mathrm{c}}(x))-2wt(f(x)(1+f_{\mathrm{c}}(x))) \tag{27}$$

故知平衡 H 布尔函数 $f(x)$ 为 $CI(m)$ 函数，当且仅当

$$wt(f_{\mathrm{c}}(x)f(x))=2^{n-2} \tag{28}$$

但是，需要分别取 $m=2,3,\cdots,n$，才能具体判定 m 实际为何数。

所以，取 $f_{\mathrm{c}}(x)=\omega x$，$w(\omega)=n$，则对平衡 H 布尔函数确有式(28)成立，但不能由此断言存在 n 阶免疫的平衡 H 布尔函数，因为它首先必须一阶和二阶免疫。如：平衡 H 布尔函数 $f(x)=1+x_3+x_4+x_1x_2+x_1x_3+x_2x_4+x_3x_4$ 是一阶相关免疫的。当 $wt(\omega)=3$ 或 4 时，式(28)也成立。但当 $wt(\omega)=2$ 时，式(28)并不全部成立。对此，定理 6 给出了一个明确的结论，从而消除了以往在这一问题上的模糊性。

定理 6 不存在二阶相关免疫的平衡 H 布尔函数。

证明 将 $f(x)$ 分为如式(11)和式(12)形式的组成。由于存在一阶相关免疫的平衡 H 布尔函数，只需要讨论 $f(x)$ 为 CI 函数时 $m\geqslant 2$ 的情形。故设 $f(x)$ 是一阶相关免疫的平衡 H 布尔函数。于是由定理 2 可知，式(5)和式(6)成立。于是由 $wt(x_1f(x))=2^{n-2}$ 可得

$$wt(f_{\mathrm{p}_{11}}(x))_{n-3}+wt(f_{\mathrm{p}_{12}}(x))_{n-3}+wt(f_{\mathrm{p}_{13}}(x))_{n-3}+wt(f_{\mathrm{p}_{14}}(x))_{n-3}=wt(f_{\mathrm{q}_{11}}(x))_{n-3}+wt(f_{\mathrm{q}_{12}}(x))_{n-3}+wt(f_{\mathrm{q}_{13}}(x))_{n-3}+wt(f_{\mathrm{q}_{14}}(x))_{n-3}=2^{n-2}$$

由 $wt(x_2f(x))=2^{n-2}$ 可得

$$wt(f_{\mathrm{p}_{11}}(x))_{n-3}+wt(f_{\mathrm{p}_{12}}(x))_{n-3}+wt(f_{\mathrm{q}_{11}}(x))_{n-3}+wt(f_{\mathrm{q}_{12}}(x))_{n-3}=wt(f_{\mathrm{p}_{13}}(x))_{n-3}+wt(f_{\mathrm{p}_{14}}(x))_{n-3}+wt(f_{\mathrm{q}_{13}}(x))_{n-3}+wt(f_{\mathrm{q}_{14}}(x))_{n-3}=2^{n-2} \tag{29}$$

现在假设 $f(x)$ 为 $CI(2)$ 函数，用反证法来证明定理的结论。

于是 $wt((x_1+x_2)f(x))=2^{n-2}$，故有

$$wt(f_{\mathrm{p}_{11}}(x))_{n-3}+wt(f_{\mathrm{p}_{12}}(x))_{n-3}+wt(f_{\mathrm{q}_{13}}(x))_{n-3}+wt(f_{\mathrm{q}_{14}}(x))_{n-3}=wt(f_{\mathrm{p}_{13}}(x))_{n-3}+wt(f_{\mathrm{p}_{14}}(x))_{n-3}+wt(f_{\mathrm{q}_{11}}(x))_{n-3}+wt(f_{\mathrm{q}_{12}}(x))_{n-3}=2^{n-2} \tag{30}$$

由式(28)和式(29)可得

$$\begin{aligned}&wt(f_{\mathrm{p}_{13}}(x))_{n-3}+wt(f_{\mathrm{p}_{14}}(x))_{n-3}\\&=wt(f_{\mathrm{q}_{11}}(x))_{n-3}+wt(f_{\mathrm{q}_{12}}(x))_{n-3}\\&wt(f_{\mathrm{p}_{11}}(x))_{n-3}+wt(f_{\mathrm{p}_{12}}(x))_{n-3}\\&=wt(f_{\mathrm{q}_{13}}(x))_{n-3}+wt(f_{\mathrm{q}_{14}}(x))_{n-3}\end{aligned} \tag{a1}$$

由式(28)和式(30)可得

$$\begin{aligned}&wt(f_{\mathrm{p}_{11}}(x))_{n-3}+wt(f_{\mathrm{p}_{12}}(x))_{n-3}\\&=wt(f_{\mathrm{q}_{11}}(x))_{n-3}+wt(f_{\mathrm{q}_{12}}(x))_{n-3}\\&wt(f_{\mathrm{p}_{13}}(x))_{n-3}+wt(f_{\mathrm{p}_{14}}(x))_{n-3}\\&=wt(f_{\mathrm{q}_{13}}(x))_{n-3}+wt(f_{\mathrm{q}_{14}}(x))_{n-3}\end{aligned} \tag{a2}$$

由式(29)和式(30)可得

$$\begin{aligned}&wt(f_{\mathrm{p}_{11}}(x))_{n-3}+wt(f_{\mathrm{p}_{12}}(x))_{n-3}\\&=wt(f_{\mathrm{p}_{13}}(x))_{n-3}+wt(f_{\mathrm{p}_{14}}(x))_{n-3}\\&wt(f_{\mathrm{q}_{11}}(x))_{n-3}+wt(f_{\mathrm{q}_{12}}(x))_{n-3}\\&=wt(f_{\mathrm{q}_{13}}(x))_{n-3}+wt(f_{\mathrm{q}_{14}}(x))_{n-3}\end{aligned} \tag{a3}$$

故式(a1)、式(a2)、式(a3)中任一等式两端中任一端与另一等式两端中任一端也彼此相等，且均等于 2^{n-3}。于是可得出结论：由于 $f(x)$ 是 CI 函数，则由 x_1 在 $x_1f(x)$ 分成的两部分 $f_{\mathrm{p}}(x)$ 和 $f_{\mathrm{q}}(x)$ 重量相等。由于 $f(x)$ 还是 $CI(2)$ 函数，则进一步由 x_2 在 $x_2f(x)$ 分成的各部分 $f_{\mathrm{p}_1}(x)$、$f_{\mathrm{p}_2}(x)$、$f_{\mathrm{q}_1}(x)$、$f_{\mathrm{q}_2}(x)$ 重量均等于 2^{n-3}。

又由 $wt(x_3f(x))=2^{n-2}$，有

$$wt(f_{\mathrm{p}_{11}}(x))_{n-3}+wt(f_{\mathrm{p}_{13}}(x))_{n-3}+wt(f_{\mathrm{q}_{11}}(x))_{n-3}+wt(f_{\mathrm{q}_{13}}(x))_{n-3}=wt(f_{\mathrm{p}_{12}}(x))_{n-3}+wt(f_{\mathrm{p}_{14}}(x))_{n-3}+wt(f_{\mathrm{q}_{12}}(x))_{n-3}+wt(f_{\mathrm{q}_{14}}(x))_{n-3}=2^{n-2} \tag{31}$$

由 $wt((x_1+x_3)f(x))=2^{n-2}$，有

$$wt(f_{p_{12}}(x))_{n-3}+wt(f_{p_{14}}(x))_{n-3}+wt(f_{q_{11}}(x))_{n-3}+$$
$$wt(f_{q_{13}}(x))_{n-3}=wt(f_{p_{11}}(x))_{n-3}+wt(f_{p_{13}}(x))_{n-3}+$$
$$wt(f_{q_{12}}(x))_{n-3}+wt(f_{q_{14}}(x))_{n-3}=2^{n-2} \quad (32)$$

由 $wt((x_2+x_3)f(x))=2^{n-2}$，有

$$wt(f_{p_{12}}(x))_{n-3}+wt(f_{p_{13}}(x))_{n-3}+wt(f_{q_{11}}(x))_{n-3}+$$
$$wt(f_{q_{13}}(x))_{n-3}=wt(f_{p_{11}}(x))_{n-3}+wt(f_{p_{14}}(x))_{n-3}+$$
$$wt(f_{q_{12}}(x))_{n-3}+wt(f_{q_{14}}(x))_{n-3}=2^{n-2} \quad (33)$$

由式(31)和式(32)可得

$$wt(f_{q_{11}}(x))_{n-3}+wt(f_{q_{13}}(x))_{n-3}=wt(f_{q_{12}}(x))_{n-3}+$$
$$wt(f_{q_{14}}(x))_{n-3}wt(f_{p_{11}}(x))_{n-3}+wt(f_{p_{13}}(x))_{n-3}$$
$$=wt(f_{p_{12}}(x))_{n-3}+wt(f_{p_{14}}(x))_{n-3} \quad (b1)$$

由式(31)和式(33)可得

$$wt(f_{p_{11}}(x))_{n-3}+wt(f_{q_{11}}(x))_{n-3}=wt(f_{p_{12}}(x))_{n-3}+$$
$$wt(f_{q_{12}}(x))_{n-3}wt(f_{p_{13}}(x))_{n-3}+wt(f_{q_{13}}(x))_{n-3}$$
$$=wt(f_{p_{14}}(x))_{n-3}+wt(f_{q_{14}}(x))_{n-3} \quad (b2)$$

由式(28)和式(31)可得

$$wt(f_{p_{11}}(x))_{n-3}+wt(f_{p_{13}}(x))_{n-3}=wt(f_{q_{12}}(x))_{n-3}+$$
$$wt(f_{q_{14}}(x))_{n-3}wt(f_{p_{12}}(x))_{n-3}+wt(f_{p_{14}}(x))_{n-3}$$
$$=wt(f_{q_{11}}(x))_{n-3}+wt(f_{q_{13}}(x))_{n-3} \quad (b3)$$

由式(29)和式(31)，有

$$wt(f_{p_{12}}(x))_{n-3}+wt(f_{q_{12}}(x))_{n-3}=wt(f_{p_{13}}(x))_{n-3}+$$
$$wt(f_{q_{13}}(x))_{n-3}wt(f_{p_{11}}(x))_{n-3}+wt(f_{q_{11}}(x))_{n-3}$$
$$=wt(f_{p_{14}}(x))_{n-3}+wt(f_{q_{14}}(x))_{n-3} \quad (b4)$$

于是由式(b1)和式(b3)联立，式(a3)和式(b1)联立，式(a2)和式(b2)联立，并再经式(a2)、式(b4)及式(b2)的关系，可得

$$wt(f_{p_{11}}(x))_{n-3}=wt(f_{p_{14}}(x))_{n-3}$$
$$=wt(f_{q_{12}}(x))_{n-3}=wt(f_{q_{13}}(x))_{n-3};$$
$$wt(f_{p_{12}}(x))_{n-3}=wt(f_{p_{13}}(x))_{n-3}$$
$$=wt(f_{q_{11}}(x))_{n-3}=wt(f_{q_{14}}(x))_{n-3} \quad (34)$$

由上面的推导可以看出，结论是成立的。在此不再用归纳法详证。

对 x_{n-1}，由 $x_{n-1}f(x)$ 分出的一维的所有 2^{n-1} 个小块，或者重量都相等，均为 $wt(f_i(x))_1=wt(f_{i+1}(x))_1=2^{n-(n-1)-1}=1$，于是有 $wt(\mathrm{d}f(x)/\mathrm{d}x_n)=2^n$ 和 $wt(ef(x)/ex_n)=0$；或者相邻块的重量为 $wt(f_i(x))_1=0$（或 $wt(f_i(x))_1=2$），而 $wt(f_{i+1}(x))_1=2$（或 $wt(f_{i+1}(x))_1=0$），于是有 $wt(\mathrm{d}f(x)/\mathrm{d}x_n)=0$，$wt(ef(x)/ex_n)=2^{n-1}$。2 种情况均与 $f(x)$ 是平衡 H 布尔函数矛盾。故知平衡 H 布尔函数一定不是 $CI(2)$ 函数。

5　结束语

从本文的讨论可知，以导数和 E−导数为工具来讨论平衡 H 布尔函数的相关免疫性时，可以深入到布尔函数的内部结构中，可以得出一些有用的且能揭示满足相关免疫性的平衡布尔函数结构特点的性质[11,12]，进一步揭示了布尔函数优良的密码学性质，为更好地研究布尔函数的密码学性质，保证密码系统的安全性和抗攻击性打下了基础。

参考文献：

[1] LI W W, WANG Z. The E-derivative of Boolean functions and its application in the fault detection and cryptographic system[J]. Kybernetes(SCI), 2011, 40(5-6):905-911.

[2] 温巧燕, 钮心忻, 杨义先. 现代密码学中的布尔函数[M]. 北京: 科学出版社, 2000. 31-33.
WEN Q Y, NIU X X, YANG Y X. Boolean Function in Modern Cryptoloy[M]. Beijing: Science Publishing House, 2000. 31-33.

[3] 杨义先. 布尔函数的相关免疫性[J]. 北京邮电学院学报, 1990, 13(3):27-35.
YANG Y X. Correlation-immunity of Boolean functions[J]. Journal of Beijing University of Posts and Telecommunications, 1990, 13(3): 27-35.

[4] GUO Y F, LAN L Y. Balanced correlation-immune functions[J]. China Science and Technology Information, 2006, (20):22-25.

[5] XIAO G Z, MASSEY J L. A spectral characterization of correlation-immune combining functions[J]. IEEE Trans on Inform Theory, 1988, 34(3):725-728.

[6] 李卫卫. 布尔函数相关免疫性与平衡性关系的研究[J]. 通信学报, 2011, 31(5):93-97.
LI W W. Study of relationships between correlation-immunity and balanceness based on Boolean functions[J]. Journal on Communications, 2011, 31(5):93-97.

[7] 张串绒, 肖国镇. 一类布尔函数的性质和应用[J]. 通信技术, 2001, 16(2):11-14.
ZHANG C R. XIAO G Z. Properties and applications of a class of Boolean functions[J]. Communications Technology, 2001, 16(2): 11-14.

[8] SIEGENTHALER T. Correlation-immunity of nonlinear combining functions for cryptographic applications[J]. IEEE Trans, 1984, 30(5): 776-778.

[9] ZHANG W G, XIAO G Z. A characterization of algebraic immune Boolean functions[J]. Journal of Beijing University of Posts and Telecommunications, 2007, 30(5):56-57.

[10] LUO W H, LI C. Algebraic immunity study of Boolean functions[J]. Computer Engineering and Applications, 2007, 43(8):59-60.

（下转第 94 页）

pollution-level estimation in P2P file-sharing systems[A]. Technologies for Advanced Heterogeneous Networks[C]. Springer Berlin Heidelberg, 2005. 1-21.
[18] Ed2k URI scheme [EB/OL]. https://en.wikipedia.org/wiki/Ed2k_URI_scheme.
[19] BitTorrent tracker [EB/OL]. https://en.wikipedia.org/wiki/ BitTorrent_tracker.
[20] OMNeT++ [EB/OL]. http://omnetpp.org/.

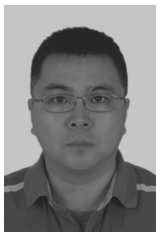
作者简介：

姚汝颢（1989-），男，宁夏银川人，北京大学硕士生，主要研究方向为 P2P 网络安全。

刘丙双（1985-），男，河北唐山人，北京大学博士生，主要研究方向为 P2P 网络安全。

曲德帅（1975-），男，辽宁大连人，国家计算机网络应急技术处理协调中心工程师，主要研究方向为信息安全与网络攻防。

周渊（1972-），男，江苏无锡人，国家计算机网络应急技术处理协调中心高级工程师，主要研究方向为互联网安全。



韩心慧[通信作者]（1969-），男，河南开封人，博士，北京大学高级工程师，主要研究方向为网络与信息安全。

（上接第 87 页）

[11] XIAO G Z, MASSEY J L. Aspectral charact erizat ion of correlation-immune comb ining functions[J]. IEEE Trans IT , 1988, 34(3):569-571.
[12] 冯登国, 肖国镇. 有限域上的函数的相关免疫性和线性结构的谱特征[J]. 通信学报,1997, 18(1):40-45.
FENG D G, XIAO G Z. Spectral characterization of correlation-immune and linear structures of functions over finite field[J]. Journal on Communications, 1997, 18(1):40-45.

作者简介：

李卫卫（1980-），女，上海人，硕士，上海政法学院讲师，主要研究方向为计算机取证与现代密码学。