2-分解H布尔函数和高非线性度布尔函数

黄景廉 王 卓 李 娟
(西北民族大学电气工程学院 兰州 730030)

摘 要 以布尔函数的导数和自定义的e-导数为主要研究工具,研究满足一次扩散准则、可2-分解为两个子函数乘积的一类H布尔函数的非线性度、相关免疫性和代数免疫性等密码学性质。得到了这类H布尔函数的相关免疫阶与两个子函数的关系,以及这类H布尔函数的相关免疫阶可达到$\left\lceil \frac{n}{2} \right\rceil -1$的结论。还得到了利用两个子函数使布尔函数的非线性度易于求解的方法,以及这类H布尔函数的最低代数次数零化子与两个子函数的关系。进一步地,在这类H布尔函数上述特点的基础上,利用导数和e-导数构造出了非线性度提高到$2^{n-2}+2^{n-3}$、具有相关免疫性和2阶代数免疫性的一族H布尔函数。由此,解决了提高布尔函数的非线性度问题,以及同时具有较高非线性度、扩散性、相关免疫性和较高阶代数免疫性的布尔函数的存在性问题。

关键词 H布尔函数,2-分解,e-导数,非线性度,代数免疫性,相关免疫性
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.7.030

H Boolean Functions with Divided into Two Parts and High Nonlinearity Boolean Functions

HUANG Jing-lian WANG Zhuo LI Juan
(College of Electrical Engineering, Northwest University for Nationalities, Lanzhou 730030, China)

Abstract Using the derivative of the Boolean functions and the e-derivative defined by ourselves as research tools, we studied the cryptographic properties of a class of H Boolean function which satisfy one degree propagation and are divided into the product of two subfunctions, including nonlinearity, correlation immunity and algebraic immunity and so on. We achieved the relationship between the correlation immunity of this kind of H Boolean function and the two subfunctions, and also arrived at a conclusion on the correlation immunity of this kind of H Boolean function which can reach $\left\lceil \frac{n}{2} \right\rceil -1$. Moreover, we obtained the relationship between the lowest algebraic degree annihilator of this kind of an H Boolean function and the two subfunctions. Further, using e-derivative and derivative of a Boolean function, we constructed a cluster of H Boolean function which has the nonlinearity $2^{n-2}+2^{n-3}$, the correlation immunity and 2-order algebraic immunity from obtained H Boolean functions. In this way, we resolved the problem of improving the nonlinearity of a Boolean function, and the existence problem of a Boolean function having higher nonlinearity, propagation, correlation immunity and higher algebraic immunity.

Keywords H Boolean functions, 2-divide, e-derivative, Nonlinearity, Algebraic immunity, Correlation immunity

1 引言

布尔函数的高代数次数、非线性度、扩散性、相关免疫性、代数免疫性等性质,是为抵抗对密码体制的各种攻击技术而陆续研究出来的、布尔函数应具备的性质。布尔函数如能同时具有多种良好的密码学性质,便可使据此布尔函数设计的密码系统具有抵抗多种密码攻击的能力。而布尔函数密码学性质的好坏也直接关系到据此布尔函数设计的密码算法的安全性[1-5]。

布尔函数的代数免疫性反映了其抵抗代数攻击的能力,布尔函数的非线性度反映了其抵抗线性攻击或快速相关攻击的能力,相关免疫性反映了其抵抗相关攻击的能力[6]。近些年提出的抵抗代数攻击的代数免疫性[7],受到了人们极大的关注,涌现了许多方法和成果[8-15]。除此之外,其它密码学性质,如扩散性、相关免疫性和非线性度等,在构造布尔函数时也需要考虑。在对具有多种良好密码学性质的布尔函数的研究中,文献[16]给出了代数免疫度与非线性度的关系式;文献[17]给出了一类具有最优基本代数免疫度、最优代数次数的向量函数的构造,由此构造的向量函数同时具有较高的非线性度;文献[18]构造了一类具有高基本代数免疫度的向量Bent函数和一类同时具有高基本代数免疫度和高非线性度的平衡向量函数;文献[19]将文献[18]的构造推广,得到新构造的具有更高非线性度的函数;文献[20]利用群分解的方法,构造了一类具有最优基本代数免疫度且其他密码学性质良好

到稿日期:2015-06-22 返修日期:2015-09-14 本文受国家自然科学基金项目(61262085)资助。
黄景廉(1968-),女,教授,主要研究方向为计算机网络通信与信息安全、密码学,E-mail:huangjlstudy@163.com;王 卓(1944-),男,教授,主要研究方向为数学、布尔代数、分布式系统、计算机信息安全;李 娟(1984-),女,讲师,主要研究方向为密码学、计算机网络安全。

的向量函数。

H 布尔函数是具有 1 次扩散性的布尔函数。对于 H 布尔函数的非线性度 N_f，其大小范围为 $2^{n-2}\leqslant N_f\leqslant 2^{n-1}-2^{\frac{n}{2}-1}$。特殊的 H 布尔函数 Bent 函数($n$ 次扩散)的非线性度为$2^{n-1}-2^{\frac{n}{2}-1}$，这是所有布尔函数非线性度的最大值[21]，但 Bent 函数不是相关免疫函数。因此，需要研究并找到具有相关免疫性且非线性度大于 2^{n-2} 的 H 布尔函数。

高非线性度是布尔函数抵抗最佳仿射逼近攻击、线性攻击应具备的性质，求布尔函数的非线性度 N_f($N_f=\min\limits_{l(x)\in L_n[x]} w_t(f(x)+l(x))=w_t(f(x)+l_0(x))$)时，寻找 $l_0(x)$ 是较困难的工作[22-24]。导数和 e-导数具有将一些难以研究的复杂问题转化为较易讨论的较简单问题的特性。本文利用这一特性，以导数和 e-导数为主要研究工具，通过对 2-分解 H 布尔函数 $f(x)=R(y)S(z)$ 的相关免疫性、非线性度中的 $l_0(x)$ 与 $R(y)$ 和 $S(z)$ 的关系、代数免疫性中的最低代数次数零化子与 $R(y)$ 和 $S(z)$ 的关系等问题的研究，既可得出 $f(x)=R(y)S(z)$ 的相关免疫阶、非线性度求解方法，同时也找到一族相关免疫的、2 阶代数免疫的、非线性度为 $2^{n-2}+2^{n-3}$ 的 H 布尔函数。

2 预备知识

布尔函数的导数是人们熟知的[21]，需要给出布尔函数 e-导数的概念。e-导数与导数的关系及 e-导数的性质，可参考文献[25-27]。

定义 1 n 元布尔函数 $f(x)=f(x_1,x_2,\cdots,x_n)\in GF(2)^{GF(2)^n}$ 对 r 个变元 $x_{i1},x_{i2},\cdots,x_{ir}$ 的导数(偏导数)表示和定义为：

$$\partial f(x)/\partial(x_{i1},x_{i2},\cdots,x_{ir})=f(x_1,x_2,\cdots,x_{i1},x_{i2},\cdots,x_{ir},\cdots,x_n)+f(x_1,x_2,\cdots,\overline{x_{i1}},\overline{x_{i2}},\cdots,\overline{x_{ir}},\cdots,x_n) \tag{1}$$

其中，$1\leqslant i\leqslant n,1\leqslant i_1\leqslant i_2\leqslant\cdots\leqslant i_r\leqslant n,1\leqslant r\leqslant n$。

当 $r=1$ 时，式(1)即为 $f(x)=f(x_1,x_2,\cdots,x_n)$ 对单个变元的导数，记为 $df(x)/dx_i(i=1,2,\cdots,n)$。经简单的计算化简，可得到如下便于使用的形式：

$$df(x)/dx_i=f(x_1,x_2,\cdots,x_{i-1},1,x_{i+1},\cdots,x_n)+f(x_1,x_2,\cdots,x_{i-1},0,x_{i+1},\cdots,x_n),i=1,2,\cdots,n$$

定义 2[25-27] n 元布尔函数 $f(x)=f(x_1,x_2,\cdots,x_n)\in GF(2)^{GF(2)^n}$ 对 r 个变元 $x_{i1},x_{i2},\cdots,x_{ir}$ 的 e-导数(e-偏导数)表示和定义为：

$$ef(x)/e(x_{i1},x_{i2},\cdots,x_{ir})=f(x_1,x_2,\cdots,x_{i1},x_{i2},\cdots,x_{ir},\cdots,x_n)\cdot f(x_1,x_2,\cdots,\overline{x_{i1}},\overline{x_{i2}},\cdots,\overline{x_{ir}},\cdots,x_n) \tag{2}$$

其中，$1\leqslant i\leqslant n,1\leqslant i_1\leqslant i_2\leqslant\cdots\leqslant i_r\leqslant n,1\leqslant r\leqslant n$。

当 $r=1$ 时，式(2)即为 $f(x)=f(x_1,x_2,\cdots,x_n)$ 对单个变元的 e-导数，记为 $ef(x)/ex_i(i=1,2,\cdots,n)$。经简单的计算化简，可得到如下便于使用的形式：

$$ef(x)/ex_i=f(x_1,x_2,\cdots,x_{i-1},1,x_{i+1},\cdots,x_n)\cdot f(x_1,x_2,\cdots,x_{i-1},0,x_{i+1},\cdots,x_n),i=1,2,\cdots,n$$

定义 3 若 $f(x)=f(x_1,x_2,\cdots,x_n)\in GF(2)^{GF(2)^n}$ 对任意 $\varepsilon_i=(0,0,\cdots,0,1,0,\cdots,0)$ $(1\leqslant i\leqslant n)$，有

$$w_t(f(x+\varepsilon_i)+f(x))=2^{n-1} \tag{3}$$

则称 $f(x)$ 为 H 布尔函数。其中，ε_i 表示第 i 个分量为 1、其余分量为 0 的 n 维布尔向量。

H 布尔函数就是具有 1 次扩散性的布尔函数。

定义 4 对 $f(x)=f(x_1,x_2,\cdots,x_n)\in GF(2)^{GF(2)^n}$，定义 $N_f=\min\limits_{l(x)\in L_n[x]} d(f(x),l(x))=\min\limits_{l(x)\in L_n[x]} w_t(f(x)+l(x))$ 为 $f(x)$ 的非线性度。其中，$L_n[x]$ 表示所有线性函数为元素的集合；$d(f(x),l(x))$(或记为 $d(f,l)$)表示 $f(x)$ 和 $l(x)$ 之间的 Hamming 距离，即

$$d(f(x),l(x))=|\{x\in GF(2)^n\mid f(x)\neq l(x)\}|$$

其中，$|\{\cdot\}|$ 表示集合 $\{\cdot\}$ 中元素的个数。

称 $C_f=\max\limits_{l(x)\in L_n[x]} d(f(x),l(x))$ 为 $f(x)$ 的线性度。

显然，对任意 n 元布尔函数 $f(x)$，有 $N_f+C_f=2^n$。

定义 5 两个 n 元布尔函数 $f_1(x')$ 与 $f_2(x')$($x'=(x_1x_2\cdots x_n)\in GF(2)^n$)的级联函数 $f(x)$($x=(x_0x_1x_2\cdots x_n)\in GF(2)^{n+1}$)是一个 $n+1$ 元布尔函数，有

$$f(x)=(1+x_0)f_1(x')+x_0f_2(x')=f_1(x')+x_0(f_1(x')+f_2(x'))$$

记为 $f(x)=f_1(x')\parallel f_2(x')$。

定义 6 对布尔函数 $f(x)=f(x_1,x_2,\cdots,x_n)\in GF(2)^{GF(2)^n}$，设 $\Gamma\cup\Lambda$ 是 $\{1,2,\cdots,n\}$ 的一个划分。如果存在 3 个布尔函数 $F(\varphi,\psi)\in GF(2)^{GF(2)^n}$，$\varphi(x_r\mid r\in\Gamma)\in GF(2)^{GF(2)^{|\Gamma|}}$(记为 $\varphi(x_r)$)和 $\psi(x_\lambda\mid\lambda\in\Lambda)\in GF(2)^{GF(2)^{|\Lambda|}}$(记为 $\psi(x_\lambda)$)，使得 $f(x_1,x_2,\cdots,x_n)=F(\varphi(x_r),\psi(x_\lambda))$，则称 $f(x_1,x_2,\cdots,x_n)$ 是关于 Γ 和 Λ 可以 2-分解的。

根据定义 1－定义 3，可容易地得到引理 1－引理 3。

引理 1 布尔函数 $f(x)$ 是 r 次扩散函数当且仅当 $w_t(\partial f(x)/\partial(x_{i1},x_{i2},\cdots,x_{ir}))=2^{n-1}$，$1\leqslant i\leqslant n,1\leqslant r\leqslant n,1\leqslant i_1\leqslant i_2\leqslant\cdots\leqslant i_r\leqslant n$

引理 2 布尔函数 $f(x)$ 是 H 布尔函数当且仅当对一切 $x_i(i=1,2,\cdots,n)$，有

$$w_t(df(x)/dx_i)=2^{n-1},i=1,2,\cdots,n$$

引理 3 对任意布尔函数 $f(x)$，有

$$f(x)=f(x)df(x)/dx_i+ef(x)/ex_i,i=1,2,\cdots,n$$

和

$$w_t(f(x))=w_t(f(x)df(x)/dx_i)+w_t(ef(x)/ex_i)=2^{-1}w_t(df(x)/dx_i)+w_t(ef(x)/ex_i)\quad i=1,2,\cdots,n$$

引理 4 布尔函数 $f(x)$ 是平衡 H 布尔函数当且仅当

$$w_t(df(x)/dx_i)=2^{n-1}$$

且

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

引理 5 布尔函数 $f(x)\in GF(2)^{GF(2)^n}$ 是 $m(m\geqslant 1)$ 阶相关免疫的当且仅当对 $\omega x(1\leqslant w_t(\omega)\leqslant m)$，有

$$w_t(\omega xf(x))=2^{-1}w_t(f(x))$$

3 可 2-分解为 2 个函数乘积的 H 布尔函数的相关免疫性和代数免疫性

定理 1 先讨论 $f(x)$ 是 H 布尔函数，且 $f(x)$ 能 2-分解为 2 个函数的乘积，即 $f(x)=R(y)S(z)$ 时，$R(y)$ 和 $S(z)$ 的特性。

定理 1 设布尔函数 $f(x)$能 2-分解为 2 个函数的乘积，即 $f(x)=R(y)S(z)(\{y\}\cup\{z\}=\{x_1,x_2,\cdots,x_n\},\{y\}\cap\{z\}=\varnothing)$。则 $f(x)$是 H 布尔函数的充分必要条件是：$\deg R(y)=\deg S(z)=1$。

证明：(充分性)设 $f(x)=R(y)S(z)(\{y\}\cup\{z\}=\{x_1,x_2,\cdots,x_n\},\{y\}\cap\{z\}=\varnothing)$，并有 $\deg R(y)=\deg S(z)=1$。

因 $\deg R(y)=\deg S(z)=1$，故 $w_t(R(y))=w_t(S(z))=2^{n-1}$，$dR(y)/dy_i=1(y_i\in\{y\})$，$dS(z)/dz_i=1(z_i\in\{z\})$。所以有

$$w_t(df(x)/dy_i)=w_t(S(z)dR(y)/dy_i)=w_t(S(z))=2^{n-1}(y_i\in\{y\})$$

$$w_t(df(x)/dz_i)=w_t(R(y)dS(z)/dz_i)=w_t(R(y))=2^{n-1}(z_i\in\{z\})$$

即 $w_t(df(x)/dx_i)=2^{n-1}(i=1,2,\cdots,n)$。由引理 2 知，$f(x)$是 H 布尔函数。

(必要性)：用反证法。

1)先假设 $\deg R(y)=1,\deg S(z)>1$。

不失一般性，可设 $x_n\in\{z_i\},x_{n-2}\in\{z_i\}$。于是有

$$w_t(R(y))=2^{n-1} \tag{4}$$

且

$$dR(y)/dy_i=1(y_i\in\{y\})$$

由引理 2，有

$$w_t(df(x)/dy_i)=w_t(S(z)dR(y)/dy_i)=w_t(S(z))=2^{n-1} \tag{5}$$

和

$$w_t(df(x)/dz_i)=w_t(R(y)dS(z)/dz_i)=w_t(R(y))=2^{n-1} \tag{6}$$

比较式(4)和式(6)，便有

$dS(z)/dz_i=1$，或 $R(y)dS(z)/dz_i=R(y)(z_i\in\{z\})$。

若 $dS(z)/dz_i=1(z_i\in\{z\})$，则 $\deg S(z)=1$，与 $\deg S(z)>1$ 矛盾。

对 $R(y)dS(z)/dz_i=R(y)(z_i\in\{z\})$，即有

$$dS(z)/dz_i=R(y)+S_1(z),R(y)S_1(z)=0 \tag{7}$$

式(7)表示函数 $dS(z)/dz_i$ 是线性函数 $R(y)$与另一个函数 $S_1(z)$的和(函数 $dS(z)/dz_i$ 由$\{z\}$中变量构成，而 $R(y)$由$\{y\}$中变量构成)，且 $R(y)S_1(z)=0$。由于$\{y\}\cap\{z\}=\varnothing(\deg R(y)=1)$，因此式(7)不可能成立。故假设条件 $\deg S(z)>1$ 不成立，必有 $\deg S(z)=1$。

2)假设 $\deg R(y)>1,\deg S(z)>1$。必有 $R(y)dR(y)/dy_i\neq0$ 且$eR(y)/ey_i\neq0$，及 $S(z)dS(z)/dz_i\neq0$ 且 $eS(z)/ez_i\neq0$。

因 $f(x)$是 H 布尔函数，所以有

$$w_t(df(x)/dz_i)=w_t(R(y)dS(z)/dz_i)=2^{n-1}(z_i\in\{z\}) \tag{8}$$

和

$$w_t(df(x)/dy_i)=w_t(S(z)dR(y)/dy_i)=2^{n-1}(y_i\in\{y\}) \tag{9}$$

故必有 $w_t(R(y))\geqslant2^{n-1}$，$w_t(dS(z)/dz_i)\geqslant2^{n-1}$，$w_t(S(z))\geqslant2^{n-1}$和 $w_t(dR(y)/dy_i)\geqslant2^{n-1}(y_i\in\{y\},z_i\in\{z\})$。记 $R(y)$ $dS(z)/dz_i=R_1(y)$，即 $R(y)=R_1(y)+R_2(y)$且

$$w_t(R_1(y))=2^{n-1},R_1(y)R_2(y)=0 \tag{10}$$

和

$$dS(z)/dz_i=R_1(y)+S_1(z),R_1(y)S_1(z)=0 \tag{11}$$

但由于$\{y\}\cap\{z\}=\varnothing$，因此式(11)不成立。从而式(10)也不成立。因此，$\deg R(y)>1$ 和 $\deg S(z)>1$ 不成立。故必有 $\deg R(y)=\deg S(z)=1$。定理 1 成立。证毕。

定理 2 讨论可 2-分解为 $f(x)=R(y)S(z)$形式的 H 布尔函数的相关免疫性。记能 2-分解为 2 个函数乘积的所有 n 元 H 布尔函数 $f(x)=R(y)S(z)$构成的集合为 $F[y,z]$。

定理 2 对 $f(x)=R(y)S(z)\in F[y,z]$，有 $\max\limits_{f(x)\in F[y,z]}CI(f(x))=\left\lceil\frac{n}{2}\right\rceil-1$。

证明：对线性函数 ωx，有

$$w_t(f(x)+\omega x)=w_t(R(y)S(z))+w_t(\omega x)-2w_t(\omega xR(y)S(z)) \tag{12}$$

由定理 1 知，$\deg R(y)=\deg S(z)=1$。故当 $\omega x=R(y)$或 $\omega x=S(z)$时，$w_t(f(x)+\omega x)=w_t(\omega x)-w_t(R(y)S(z))=2^{n-2}$。这时 $f(x)$不是 $w_t(\omega)$阶相关免疫函数。

当 $w_t(\omega)\leqslant\min(|\{y\}|,|\{z\}|)-1$ 时，$w_t(f(x)+\omega x)=2^{n-2}+2^{n-1}-2\cdot2^{n-3}=2^{n-1}$。$f(x)$为 $\min(|\{y\}|,|\{z\}|)-1$ 阶相关免疫函数。

而 $\max\min(|\{y\}|,|\{z\}|)=\left\lceil\frac{n}{2}\right\rceil$。故 $\max\limits_{f(x)\in F[y,z]}CI(f(x))=\left\lceil\frac{n}{2}\right\rceil-1$。证毕。

推论 1 对 $f(x)=R(y)S(z)\in F[y,z]$，当 $\omega x\neq R(y)$且 $\omega x\neq S(z)$时，必有 $w_t(f(x)+\omega x)=2^{n-1}$。

推论 1 由定理 2 的证明即可看出，不再证明。

由定理 2 可知，H 布尔函数 $f(x)=R(y)S(z)$的相关免疫阶可以达到$\left\lceil\frac{n}{2}\right\rceil-1$，但 $f(x)$的代数免疫阶却不高。有下面的定理 3。

定理 3 有 H 布尔函数 $f(x)=R(y)S(z)\in F[y,z]$，则 $1+R(y)$和 $1+S(z)$是 $f(x)$的 2 个最低代数次数零化子，且 $AI(f(x))=1$。

证明：对 $f(x)=R(y)S(z)$，有$(1+R(y))f(x)=0$，$(1+S(z))f(x)=0$，且 $\deg(1+R(y))=\deg(1+S(z))=1$。故 $1+R(y)$和 $1+S(z)$是 $f(x)$的 2 个最低代数次数零化子，且 $AI(f(x))=1$。证毕。

从定理 2 对 $f(x)=R(y)S(z)$的相关免疫性的讨论中可以看到，$f(x)$和线性函数 ωx 的关系很奇特：除了 $\omega x=R(y)$和 $\omega x=S(z)$之外的任意 $\omega x\in L_n[x]$，都有 $w_t(f(x)+\omega x)=2^{n-1}$。由此可知，只要选取 $l_0(x)=R(y)$和 $l_0(x)=S(z)$，则有

$$\min_{l(x)\in L_n[x]}w_t(f(x)+l(x))=w_t(f(x)+l_0(x))=2^{n-2}$$

所以有下面的定理 4。

定理 4 对 H 布尔函数 $f(x)=R(y)S(z)\in F[y,z]$，有

$$N_f=\min_{l(x)\in L_n[x]}w_t(f(x)+l(x))=w_t(f(x)+l_{0i}(x))=2^{n-2},i=1,2$$

且 $l_{01}(x)=R(y),l_{02}(x)=S(z)$。

定理 4 不再详证。

从定理 2－定理 4 可以看到，$f(x)=R(y)S(z)\in F[y,z]$这一类型的 H 布尔函数，可以由不同元数的线性函数生成。因而 $f(x)$的非线性度只由生成它的线性函数 $R(y)$和 $S(z)$确定。$f(x)$的最低代数次数零化子也由 $R(y)$和 $S(z)$确定。同时，$f(x)$还可以具有从 1 阶直到$\left\lceil\frac{n}{2}\right\rceil-1$ 阶的相关免疫性，

且具有扩散性。利用 $f(x)$的这些特点，可以构造出具有较高非线性度并同时具有扩散性、代数免疫性和相关免疫性的布尔函数。

4 高非线性度 H 布尔函数的构造

高非线性度是提高密码系统抵抗线性攻击能力的布尔函数的重要性质。定理 5 讨论利用可 2-分解为 2 个函数乘积的 H 布尔函数，构造出具有较高非线性度的相关免疫 H 布尔函数的问题。

定理 5 对可 2-分解 H 布尔函数 $f_i(x)=R(y)S(z)=\sum_{r=1}^{n-i}x_r\sum_{k=n}^{n-i+1}x_k(i=2,3,\cdots,n-2)$，取

$$f_1(x)=(x_n+x_{n-3})+(x_n+x_{n-1})\sum_{k=n-2}^{n-i+1}x_k+\sum_{k=n-2}^{n-i+1}x_k\sum_{j=1}^{n-i}x_j+f_i(x),i=2,3,\cdots,n-2$$

则

1) $f_1(x)$是 1 阶相关免疫平衡 H 布尔函数。

2)有 $l_{01}(x)=x_n+x_{n-3}$，$l_{02}(x)=x_{n-1}+x_{n-3}$，使

$$\begin{aligned}N_{f_1}&=\min_{l(x)\in L_n[x]}w_t(f_1(x)+l(x))\\&=w_t(f_1(x)+l_{01}(x))=w_t(f_1(x)+l_{02}(x))\\&=2^{n-2}\end{aligned}$$

3)令 $N=n+1$，级联函数 $f(x)=(1+x_0)f_1(x)+x_0f_i(x)$是 N 维相关免疫的、2 阶代数免疫的 H 布尔函数。

当 $l_{01}(x)\neq S(z)$且 $l_{01}(x)=R(y)$，及 $l_{02}(x)\neq S(z)$且 $l_{02}(x)\neq R(y)$时，有

$$N_f=\min_{l(x)\in L_{n+1}[x]}w_t(f(x)+l(x))=2^{N-2}+2^{N-3}$$

证明：

1)由于 $\deg f_1(x)=2$，且 $f_1(x)$的 2 次项中含有 x_1，$x_2,\cdots,x_n$ 中所有任意 2 个元，因此对一切 $i=1,2,\cdots,n$，有 $\deg(df_1(x)/dx_i)=1$。故

$$w_t(df_1(x)/dx_i)=2^{n-1},i=1,2,\cdots,n$$

即 $f_1(x)$是 H 布尔函数。

经计算，有

$$\begin{aligned}w_t(ef_1(x)/ex_n)&=w_t((x_{n-3}+x_{n-1})(\sum_{k=n-2}^{n-i+1}x_k+\sum_{k=1}^{n-i}x_k))\\&=2^{n-2}\end{aligned}$$

由引理 4 知，

$$\begin{aligned}w_t(f_1(x))&=2^{-1}w_t(df_1(x)/dx_n)+w_t(ef_1(x)/ex_n)\\&=2^{-1}\cdot 2^{n-1}+2^{n-2}\\&=2^{n-1}\end{aligned}$$

故 $f_1(x)$是平衡布尔函数，有

$$w_t(d(f_1(x)+x_i)/dx_i)=2^n-w_t(df_1(x)/dx_i)=2^{n-1}$$

$$w_t(e(f_1(x)+x_n)/ex_n)=w_t(x_{n-3}+x_{n-1}\sum_{k=1}^{n-2}x_k)=2^{n-2}$$

$$w_t(e(f_1(x)+x_{n-1})/ex_{n-1})=w_t(x_{n-3}\sum_{k=1}^{n-2}x_k)=2^{n-2}$$

和

$$\begin{aligned}w_t(e(f_1(x)+x_i)/ex_i)&=w_t((x_n+x_{n-1})(x_n+x_{n-3}+x_1+\cdots+x_{i-1}+x_{i+1}+\cdots+x_{n-2}))\\&=2^{n-2}\end{aligned}$$

$i=n-2,n-4,\cdots,1$

由引理 5 知

$$\begin{aligned}w_t(f_1(x)+x_i)&=2^{-1}w_t(d(f_1(x)+x_i)/dx_i)+w_t(e(f_1(x)+x_i)/ex_i)\\&=2^{n-1}\end{aligned}$$

故 $f_1(x)$是相关免疫函数。

因此 $f_1(x)$是 1 阶相关免疫平衡 H 布尔函数。

2)直接计算，即可得

$$w_t(f_1(x)+l_{01}(x))=w_t(f_1(x)+l_{02}(x))=2^{n-2}$$

而由文献[9]知，H 布尔函数的非线性度有

$$2^{n-2}\leqslant N_f\leqslant 2^{n-1}-2^{\frac{n}{2}-1}$$

所以 $N_{f_1}=2^{n-2}$。

3)由于

$$\begin{aligned}w_t(f(x)+x_r)=w_t((1+x_0)(f_1(x)+x_r))+w_t(x_0(f_i(x)+x_r))-w_t(x_r)\end{aligned}\tag{13}$$

且 $f_1(x)$和 $f_i(x)$都是相关免疫函数，有 $w_t(f_1(x)+x_r)=2^{n-1}$和 $w_t(f_i(x)+x_r)=2^{n-1}$。故由式(13)知，$f(x)$是相关免疫函数。

由于

$$w_t(d(f_1(x)+f_i(x))/dx_n)=w_t(1+\sum_{k=n-2}^{n-i+1}x_k)=2^{n-1}$$

和

$$\begin{aligned}&w_t(e(f_1(x)+f_i(x))/ex_n)\\&=w_t((1+x_{n-3}+\sum_{k=n-2}^{n-i+1}x_k+x_{n-1}\sum_{k=n-2}^{n-i+1}x_k+\sum_{k=n-2}^{n-i+1}x_k\sum_{j=1}^{n-i}x_j)\\&\quad(x_{n-3}+x_{n-1}\sum_{k=n-2}^{n-i+1}x_k+\sum_{k=n-2}^{n-i+1}x_k\sum_{j=1}^{n-i}x_j))\\&=w_t((x_{n-3}+x_{n-1}+\sum_{j=1}^{n-i}x_j)\sum_{k=n-2}^{n-i+1}x_k)\\&=2^{n-2}\end{aligned}$$

由引理知，$w_t(f_1(x)+f_i(x))=2^{n-1}$。

令 $N=n+1$。由于 $f_1(x)$和 $f_i(x)$均为 H 布尔函数，因此对一切 $r=1,2,\cdots,n$，有

$$\begin{aligned}w_t(df(x)/dx_r)&=w_t((1+x_0)df_1(x)/dx_r+x_0df_i(x))/dx_r)\\&=2^{N-1}\end{aligned}$$

由于已证明有 $w_t(f_1(x)+f_i(x))=2^{n-1}$，因此

$$w_t(df(x)/dx_0)=2w_t(f_1(x)+f_i(x))=2^{N-1}$$

由引理 2 知，$f(x)$是 H 布尔函数。

由于 $f_1(x)$是平衡 H 布尔函数，因此有

$$w_t(f_1(x)df_1(x)/dx_n)=2^{n-2}$$

且 $w_t(ef_1(x)/ex_n)=2^{n-2}$。所以 $f_1(x)$只能有 2 次以上零化子。

又 $f_i(x)$有 1 次零化子 $1+S(z)$和 $1+R(y)$，所以 $f(x)$有 2 次零化子$(1+x_0)\cdot 0+x_0(1+S(z))$和$(1+x_0)\cdot 0+x_0(1+R(y))$。故 $AI(f(x))=2$，$f(x)$是 2 阶代数免疫函数。

由定理 5 的 2)可知：对 $f_1(x)$，有且仅有 $l_{01}(x)=x_n+x_{n-3}$和 $l_{02}(x)=x_{n-1}+x_{n-3}$，使 $w_t(f_1(x)+l_{0i}(x))=\min_{l(x)\in L_n[x]}w_t(f_1(x)+l(x))$。

但对 $f_i(x)=R(y)S(z)$，当 $l_{01}(x)\neq S(z)$且 $l_{01}(x)\neq R(y)$，及 $l_{02}(x)\neq S(z)$且 $l_{02}(x)\neq R(y)$时，为方便计算且不失一般性，假设 $S(z)$中含 x_{n-3}，记 $S(z)=S_1(z)+x_{n-3}$。于是有

$$\begin{aligned}&w_t(d(R(y)S(z)+l_{0r}(x))/dx_{n-3})\\&=w_t(R(y)+x_k)=2^{n-1},k=n\text{ 或 }n-1\\&w_t(e(R(y)S(z)+l_{0r}(x))/ex_{n-3})\\&=w_t(R(y)(S_1(z)+x_k))=2^{n-2},k=n\text{ 或 }n-1\end{aligned}$$

所以由引理有

$$w_t(f_i(x)+l_{0r}(x))=2^{n-1},r=1,2$$

同样，可计算出

$w_t(f_1(x)+R(y))=w_t(f_1(x)+S(z))=2^{n-1}$

记 $l'_{01}(x)=x_{n-3}+x_n$ 和 $l'_{02}(x)=x_{n-3}+x_{n-1}$ 为 $n+1$ 维函数。当 $l_{01}(x)\neq S(z)$ 且 $l_{01}(x)\neq R(y)$，及 $l_{02}(x)\neq S(z)$ 且 $l_{02}(x)\neq R(y)$ 时，有

$$\begin{aligned}N_f&=\min_{l(x)\in L_{n+1}[r]} w_t(f(x)+l(x))\\&=w_t(f(x)+l'_{0r}(x))\\&=w_t(f(x)+(1+x_0)\cdot 0+x_0R(y))\\&=w_t(f(x)+(1+x_0)\cdot 0+x_0S(z))\\&=2^{N-2}+2^{N-3},N=n+1\end{aligned}$$

证毕。

定理 5 得到了一族具有相关免疫性、2 阶代数免疫性、扩散性和较高非线性度(达到 $2^{n-2}+2^{n-3}$)的布尔函数。由于我们只知道 H 布尔函数的非线性度取值范围为 $2^{n-2}\leqslant N_f\leqslant 2^{n-1}-2^{\frac{n}{2}-1}$，及布尔函数最大非线性度为 Bent 函数(0 阶相关免疫)的非线性度为 $2^{n-1}-2^{\frac{n}{2}-1}$，而非线性度大于 2^{n-2} 的 H 布尔函数还未见到，因此定理 5 得出的非线性度达到 $2^{n-2}+2^{n-3}$ 的一族 H 布尔函数的结果是一个很好的新结果。

例　取 $f_3(x)=(x_1+x_2+x_3)(x_4+x_5+x_6)$，则 $f_1(x)=(x_6+x_3)+(x_6+x_5)(x_1+x_2+x_3+x_4)$。有

$w_t(df_1(x)/dx_i)=2^{n-1}=2^5,i=6,5,4,3,2,1$

$w_t(ef_1(x)/ex_6)=2^{n-2}=2^{6-2}=2^4$

故有

$$\begin{aligned}w_t(f_1(x))&=2^{-1}w_t(df_1(x)/dx_6)+w_t(ef_1(x)/ex_6)\\&=2^{n-1}=2^5\end{aligned}$$

所以 $f_1(x)$ 是平衡 H 布尔函数。

同样可求得：

$$\begin{cases}w_t(d(f_1(x)+x_i)/dx_i)=2^n-w_t(df_1(x)/dx_i)=2^{n-1}\\w_t(e(f_1(x)+x_i)/ex_i)=2^{n-2}\end{cases}$$

所以有

$$\begin{aligned}w_t(f_1(x)+x_i)&=2^{-1}w_t(d(f_1(x)+x_i)/dx_i)+w_t(ef_1(x)/ex_i)\\&=2^{n-1},i=1,2,3,4,5,6\end{aligned}$$

所以 $f_1(x)$ 是相关免疫函数。

因此 $f_1(x)$ 是相关免疫的平衡 H 布尔函数。

对于定理 5 的结论 2)和 3)，要对 $f_1(x)$、$i=3$ 的 $f_i(x)$ 以及 $f(x)=(1+x_0)f_1(x)+x_0f_i(x)$ 进行验证，只需同验证 $f_1(x)$ 是相关免疫的平衡 H 布尔函数一样，按定理 5 证明中的方法进行计算即可。限于篇幅，不再赘述。

结束语　本文得到了一些很有意义的新结果，如使 H 布尔函数非线性度大于 2^{n-2}，达到 $2^{n-2}+2^{n-3}$；同时得出具有较高非线性度、相关免疫性、2 阶代数免疫性和扩散性等多种密码安全性质的一族布尔函数等。

本文以导数和 e-导数为主要研究工具进行研究。文中有多处必须使用导数和 e-导数才能够较易证明的地方。如：定理 5 中，证明 $f_1(x)$ 和级联函数 $f(x)$ 是 H 布尔函数时，直接求较复杂函数表示式的重量很困难，利用导数和 e-导数，将求较复杂函数表示式的重量转化为求线性函数和 2 个线性函数乘积的重量，即可以直接得出结果，并具有很强的推理性(因若 $\deg h_1(x)=1$ 时，有 $w_t(dh_1(x)/dx_i)=2^n$，$w_t(eh_1(x)/ex_i)=0$($h_1(x)$ 含变元 x_i)，所以 $w_t(h_1(x))=2^{n-1}$。又还有 $\deg h_2(x)=1$ 且 $h_1(x)\neq h_2(x)$ 时，由 $w_t(h_1(x)+h_2(x))=w_t(h_1(x))+w_t(h_2(x))-2w_t(h_1(x)h_2(x))$，可直接得到 $w_t(h_1(x)h_2(x))=2^{n-2}$)。因此，以导数和 e-导数来证明问题，是布尔函数密码学性质研究中有时不可缺少的研究方法。

本文利用 2-分解函数得到 H 布尔函数较高非线性度的结果也引出一些需进一步研究的问题，如利用 2-分解 H 布尔函数，研究在提高非线性度的基础上提高 H 布尔函数相关免疫阶、代数免疫阶，并赋予 H 布尔函数平衡性的问题；利用任意 2-分解布尔函数进一步提高布尔函数的非线性度问题，构造高代数次数布尔函数的问题，以及构造高维最优代数免疫函数等问题。今后将对这些问题逐步展开研究。

参 考 文 献

[1] Carlet C. Boolean Functions for Cryptography and Error Correcting Codes[M]. Cambridge University Press, 2010

[2] Carlet C. Vectorial Boolean functions for cryptography[M]// Crama E Y, Hammer P, eds. Boolean Models and Methods Cambridge University Press, 2006

[3] Xiong F, Qiao D, Wang H X, et al. A Novel Network Reliability Evaluating Algorithm with Ordered Binary Decision Diagram Based on Boolean Function[J]. Journal of Electronics & Information Technology, 2014, 36(11): 2786-2790(in Chinese)
熊飞，乔迪，王宏祥，等. 一种基于有序二元决策图和布尔函数性质计算网络可靠性的算法[J]. 电子与信息学报，2014，36(11)：2786-2790

[4] Cusick T W, Stanica P. Cryptographic Boolean Functions and Applications[M]. Academic Press, 2009

[5] Gao G P, Liu W F. The Notes on the Linear Structures of Rotation Symmetric Boolean Functions[J]. Journal of Electronics & Information Technology, 2012, 34(9): 2273-2276(in Chinese)
高光普，刘文芬. 关于旋转对称布尔函数线性结构的几点注记[J]. 电子与信息学报，2012，34(9)：2273-2276

[6] Qu L J, Fu S J, Li C. Recent Progress in Properties of Cryptographic Functions[J]. Journal of Cryptologic Research, 2014, 1(6): 578-588(in Chinese)
屈龙江，付绍静，李超. 密码函数安全性指标的研究进展[J]. 密码学报，2014，1(6)：578-588

[7] Courtois N, Meier W. Algebraic attacks on stream ciphers with linear feedback[M]// Advances in Cryptology—EUROCRYPT 2003. Warsaw, Poland, 2003: 345-359

[8] Carlet C, Zeng X Y. Further properties of several classes of Boolean functions with optimum algebraic immunity[J]. Designs, Codes and Cryptography, 2009, 52(3): 303-338

[9] Xiong X W, Wei A G, Zhang Z J. Construction of Rotation Symmetric Boolean Functions with Good Cryptographic Properties [J]. Journal of Electronics & Information Technology, 2012, 34(10): 2358-2362(in Chinese)
熊晓雯，魏爱国，张智军. 构造具有良好密码学性质的旋转对称布尔函数[J]. 电子与信息学报，2012，34(10)：2358-2362

[10] Chen Y D, Zhang Y N, Tian W. Construction of Even-variable Rotation Symmetric Boolean Functions with Optimal Algebraic Immunity[J]. Journal of Cryptologic Research, 2014, 1(5): 437-448(in Chinese)
陈银冬，张亚楠，田威. 具有最优代数免疫度的偶数元旋转对称布尔函数的构造[J]. 密码学报，2014，1(5)：437-448

(下转第 202 页)

少数据的合并时间，减少合并过程对系统性能的影响。测试结果表明，通过以上策略可以明显减少数据的合并时间，提高Cassandra服务器的读取响应性能。

参考文献

[1] Ferdman M, Adileh A, Kocberber O, et al. Clearing the clouds: a study of emerging scale-out workloads on modern hardware[J]. ACM SIGARCH Computer Architecture News, 2012, 40(1): 37-48

[2] Lotfi-Kamran P, Grot B, Ferdman M, et al. Scale-out processors [J]. IEEE Computer Society ACM SIGARCH Computer Architecture News, 2012, 40(3): 500-511

[3] First the tick, now the tock: Next generation Intel microarchitecture (Nehalem) [OL]. http://www.bitpipe.com/detail/RES/123871608_708.html

[4] Rabl T, Sadoghi M, Jacobsen H A, et al. Solving Big Data Challenges for Enterprise Application Performance Management[J]. PVLDB, 2012, 5(12): 1724-1735

[5] DeCandia G, Hastorun D, Jampani M, et al. Dynamo: Amazon's Highly Available Key-Value Store[J]. ACM Sigops Oper. Syst. rev, 2007, 41(6): 205-220

[6] Cartell R. Scalable SQL and NoSQL data stores[J]. ACM Sigmod Record, 2010, 39(4): 12-27

[7] Nguyen T T, Nguyen M H. Zing Database: high-performance key-value store for large-scale storage service[J]. Vietnam Journal of Computer Science, 2015, 2(1): 13-23

[8] The Apache Cassandra Project[OL]. http://cassandra.apache.org

[9] Chen C, Hsiao M. Bigtable: A distributed storage system for structured data[J]. Proceedings of Osdi, 2006, 26(2): 205-218

[10] Cooper B F, Silberstein A, Tam E, et al. Benchmarking cloud serving systems with YCSB[C]// SoCC. 2010: 143-154

[11] Bridges J T, Dieffenderfer J N, Sartorius T, et al. Caching memory attribute indicators with cached memory data field[P]. US, US20070094475 A1, 2005

[12] Spillane R P, Shetty P J, Zadok E, et al. An efficient multi-tier tablet server storage architecture [C] // Acm Symposium on Cloud Computing Acm. 2011: 1-14

(上接第 170 页)

[11] Li Y, Yang M, Kan H B. Constructing and counting Boolean functions on even variables with maximum algebraic immunity [J]. IEICE Transactions on Fundamentals, 2010, 93-A(3): 640-643

[12] Rizomiliotis P. On the resistance of Boolean functions against algebraic attacks using univariate polynomial representation[J]. IEEE Transactions on Information Theory, 2010, 56(8): 4014-4024

[13] Wu B F, Lin D D. Constructing Boolean Functions with Good Cryptographic Properties by Concatenation[J]. Journal of Cryptologic Research, 2014, 1(1): 64-71(in Chinese)
吴保峰，林东岱. 具有良好密码学性质的布尔函数的级联构造[J]. 密码学报，2014，1(1)：64-71

[14] Wang Q, Peng J, Kan H, et al. Constructions of cryptographically significant Boolean functions using primitive polynomials[J]. IEEE Transactions on Information Theory, 2010, 56(6): 3048-3053

[15] Zhou Q F, Li X X, Qian H F. Construction of almost perfect algebraic immune resilient functions on even variables[J]. Computer Engineering, 2014, 40(12): 74-77(in Chinese)
周祁丰，李祥学，钱海峰. 具有几乎完美代数免疫的偶数元弹性函数构造[J]. 计算机工程，2014，40(12)：74-77

[16] Carlet C. On the higher order nonlinearities of algebraic immune functions[M] // Advances in Cryptology — CRYPTO 2006. Springer Berlin Heidelberg, 2006: 584-601

[17] Carlet C, Feng K. An infinite class of balanced vectorial Boolean functions with optimum algebraic immunity and good nonlinearity[M] // Coding and Cryptology. Springer Berlin Heidelberg, 2009: 1-11

[18] Feng K, Yang J. Vectorial Boolean functions with good cryptographic properties[J]. International Journal of Foundations of Computer Science, 2011, 22(6): 1271-1282

[19] Dong D, Qu L, Fu S, et al. New constructions of vectorial Boolean functions with good cryptographic properties[J]. International Journal of Foundations of Computer Science, 2012, 23(3): 749-760

[20] Lou Y, Han H, Tang C, et al. Constructing vectorial Boolean functions with high algebraic immunity based on group decomposition[J]. International Journal of Computer Mathematics, 2014, 92(3): 451-462

[21] 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

[22] Li C L, Zhang H G, Zeng X Y, et al. The lower bound on the second-order nonlinearity for a class of Bent functions[J]. Chinese Journal of Computers, 2012, 35(8): 1588-1593(in Chinese)
李春雷，张焕国，曾祥勇，等. 一类 Bent 函数的二阶非线性度下界[J]. 计算机学报，2012，35(8)：1588-1593

[23] Sun G H, Wu C K. On the nonlinearity, algebraic degree and algebraic immunity of some symmetric Boolean functions[J]. Chinese Journal of Computers, 2014, 37(11): 2247-2255(in Chinese)
孙光洪，武传坤. 几类对称布尔函数的非线性度、代数次数和代数免疫阶[J]. 计算机学报，2014，37(11)：2247-2255

[24] Zhou Y. Characterization of a Balanced Boolean Function with the Minimum of the Sum-of-squares Indicator[J]. Journal of Cryptologic Research, 2015, 2(1): 17-26(in Chinese)
周宇. 具有最小平方和指标的平衡布尔函数性质刻画[J]. 密码学报，2015，2(1)：17-26

[25] Li W, Wang Z, Huang J. The e-derivative of boolean functions and its application in the fault detection and cryptographic system[J]. Kybernetes, 2011, 40(5/6): 905-911

[26] Huang J L, Wang Z. The relationship between correlation immune and weight of H Boolean function[J]. Journal on Communications, 2012, 33(2): 110-118(in Chinese)
黄景廉，王卓. H 布尔函数的相关免疫性与重量的关系[J]. 通信学报，2012，33(2)：110-118

[27] Zhao M L. Method of detecting special logic function based on Boolean e-derivative[J]. Journal of Zhejiang University (Science Edition), 2014, 41(4): 424-426(in Chinese)
赵美玲. 基于布尔 e 导数的特殊逻辑函数检测方法[J]. 浙江大学学报(理学版)，2014，41(4)：424-426