doi: 103969/j. issn. 0490-6756. 2017. 01. 010

具有高非线性度和最优代数次数的弹性函数的构造

刘　倩[1]，王怀柱[2]，张丽娜[3]

(1. 西安电子科技大学 ISN 国家重点实验室，西安 710071；2. 宁夏大学数学计算机学院，银川 750021；
3. 西安科技大学计算机科学与技术学院，西安 710054)

摘　要：具有良好的非线性度和最优代数次数的弹性布尔函数在流密码和分组密码设计和分析中起着至关重要的作用. 本文通过修改 Maiorana-McFarland(M-M)类 Bent 函数，利用不同的低阶弹性函数，给出构造高非线性度弹性布尔函数的一种新方法，所构造的函数具有严格几乎最优的非线性度和最优的代数次数.

关键词：密码学；流密码；布尔函数；非线性度；弹性；代数次数

中图分类号：TN918.1；TP309　　**文献标识码**：A　　**文章编号**：0490-6756(2017)01-0061-04

Construction of resilient functions with high nonlinearity and optimal algebraic degree

LIU Qian[1], *WANG Huai-Zhu*[2], *ZHANG Li-Na*[3]

(1. State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China;
2. School of Mathematics and Computer Science, Ningxia University, Yinchuan 750021, China;
3. College of Computer Science and Technology, Xi'an University of Science and Technology, Xi'an 710054, China)

Abstract: Resilient Boolean functions with good nonlinearity and optimal algebraic degree play an important role in the design and analysis of stream cipher and block ciphers. In this paper, based on different lower resilient functions, a new construction method to obtain high nonlinearity resilient Boolean function is given via modifying Maiorana-McFarland (M-M) class bent functions. It is shown that the constructed functions have the strictly almost optimal nonlinearity and the optimal algebraic degree.

Keywords: Cryptography; Stream cipher; Boolean function; Nonlinearity; Resiliency; Algebraic degree

1　引　言

在流密码系统中，使用的密码函数常常需要满足高非线性度、高代数次数、高代数免疫度、适度弹性等性质. 在布尔函数所有的密码学指标中，非线性度是一个很重要的指标. 我们把非线性度达到最大值的函数称为 Bent[1] 函数. 这类密码函数能有效地抵抗线性攻击[2]和最佳仿射逼近攻击[3]. 然而 Bent 函数非线性度达到最高，但却不平衡且不具有弹性，代数次数不超过 $n/2$. 根据 Siegenthaler[4]不等式，弹性阶与代数次数有很强的相互制约性，而且对密码函数的非线性度也有一定的制约性. 因此，如何实现这几个安全性指标的折中，构造具有高非线性度的弹性函数，是一件具有挑战性的工作.

文献[5]通过修改 M-M[6]类函数，级联小的仿射函数来构造高非线性度弹性函数，但是其非线性度并未超过 $2^{n-1}-2^{\lfloor n/2\rfloor}$，而且代数次数也达不到最优. 2000 年，文献[7]指出可能存在非线性度超过 $2^{n-1}-2^{\lfloor n/2\rfloor}$ 的弹性函数. 2006 年 Maitra 和 Pasal-

收稿日期：2016-04-26
基金项目：国家自然科学基金(61562069)
作者简介：刘倩(1988－)，女，陕西西安人，博士生，研究方向为对称密码学中的布尔函数. E-mail:lqmova@foxmail.com

ic[8]提出了构造 m 阶弹性函数的一般方法. 文献[9]给出了一种构造代数次数最优 m 阶弹性函数的通用方法. 文献[10]利用级联不相交谱函数的方法,给出了偶变元高非线性度代数次数达到最优的弹性函数. 最近文献[11]在文献[10]的基础上,进一步提高了非线性度的上界. 本文基于级联不同的弹性函数,结合文献[8,11-12]的思想,利用不同的低阶弹性函数去构造更高阶的弹性函数,获得了一大类几乎最优的且代数次数最优的弹性函数.

2 预备知识

一个 n 元布尔函数是一个从 F_2^n 到 F_2 的映射,我们用 B_n 来表示所有 n 元布尔函数的集合. 对于任意一个布尔函数 $f(x)\in B_n$,我们可以用它的代数正规型来表示:

$$f(x_1,x_2,\cdots,x_n)=\bigoplus_{u\in F_2^n}\lambda_u\left(\prod_{i=1}^{n}x_i^{u_i}\right),$$

其中,$\lambda_u\in F_2$,$u=(u_1,u_2,\cdots,u_n)\in F_2^n$. $f(x)$的代数次数是使得 $\lambda_u\neq 0$ 的 u 的最大汉明重量 $wt(u)$,用 $\deg(f)$表示. 若 $\deg(f)\leqslant 1$,则该函数为仿射函数,用 A_n 表示所有 n 元仿射函数的集合.

对于任意的 $x=(x_1,x_2,\cdots,x_n)$和 $\omega=(\omega_1,\omega_2,\cdots,\omega_n)\in F_2^n$,它们在 F_2^n 上的点积定义为

$$\omega\cdot x=\omega_1x_1\oplus\omega_2\omega_2\oplus\cdots\oplus\omega_nx_n.$$

定义 2.1 函数 $f(x)\in B_n$ 在 ω 点处的 Walsh-Hadamard[13]变换等于在 F_2^n 上的如下实值函数:

$$W_f(\omega)=\sum_{x\in F_2^n}(-1)^{f(x)\oplus\omega\cdot x}.$$

若它的真值表中输出列中 0 和 1 的个数相等,即 $W_f(0)=0$,称 $f(x)$是平衡的.

定义 2.2 函数 $f(x)\in B_n$ 和所有仿射函数 l 的最小汉明距离为它的非线性度,即

$$nl(f)=\min_{l\in A_n}d(f,l)=\min_{l\in A_n}wt(f\oplus l),$$

进一步可以计算得到

$$nl(f)=2^{n-1}-\frac{1}{2}\max_{\alpha\in F_2^n}|W_f(\alpha)|.$$

引理 2.3 设函数 $f(x)\in B_n$ 则

$$\sum_{\alpha\in F_2^n}W_f^2(\alpha)=2^{2n}$$

因此,$\forall f(x)\in B_n$,$\max_{\alpha\in F_2^n}|W_f(\alpha)|\geqslant 2^{n/2}$,即 $nl(f)\leqslant 2^{n-1}-2^{n/2-1}$,非线性度为 $2^{n-1}-2^{n/2-1}$的函数为 Bent 函数.

引理 2.4[14] 设任意 n 元布尔函数 $f(x)$,$\alpha\in F_2^n$,$1\leqslant t\leqslant n$,$f(x)$是 t 阶弹性函数当且仅当对任意满足 $0\leqslant wt(\alpha)\leqslant t$ 的 α,$W_f(\alpha)=0$.

引理 2.5[4] 如果 n 元函数 $f(x)$是 m 阶弹性函数,那么 $\deg(f)\leqslant n-m-1$;如果 $\deg(f)=n-m-1$,称 $f(x)$达到 Siegenthaler 限,即 $f(x)$具有最优的代数次数.

定义 2.6 严格几乎最优弹性布尔函数:令 $n\geqslant 4$ 是偶数,如果 $f\in B_n$ 的非线性度满足

$$2^{n-1}-2^{n/2}\leqslant nl(f)<2^{n-1}-2^{n/2-1},$$

我们就称 f 为严格几乎最优的[15].

定义 2.7 $f(x)$是一个 n 元布尔函数,若 $f(x)$是 m 阶弹性函数,其代数次数和非线性度分别为 d 和 l,则称它为(n,m,d,l)函数.

3 严格几乎最优的高非线性弹性布尔函数的构造

引理 3.1[8] 令 $1\leqslant m\leqslant n/2-2$,$1\leqslant k\leqslant n/2-1$. 假设存在一个$(n/2+k,m,d,\tau)$布尔函数 h,并且 $d>k+1$. 同样,对于一个固定的 $\delta\in F_2^{n/2-k}$,假设存在一个单射 $\phi:F_2^k\times(F_2^{n/2-k}\backslash\{\delta\})\longrightarrow F_2^n$,并且 $\forall Y\in F_2^{n/2}$ 都有 $wt(\phi(Y))>m$. 那么 $\forall X,Y\in F_2^{n/2}$,$Y=(Y',Y'')\in F_2^k\times F_2^{n/2-k}$,可以构造一个函数

$$f(X,Y)=\begin{cases}\phi(Y)\cdot X\oplus g(Y), & Y''\neq\delta\\ h(X,Y'), & Y''=\delta\end{cases}$$

其中,$g(Y)$为 $n/2$ 元的布尔函数,那么函数 f 是一个代数次数为 $n/2-k+d$,非线性度为 $nl(f)\geqslant 2^{n-1}-2^{n/2-1}-2^{n/2+k-1}+\tau$ 的 m 阶弹性函数.

根据引理 3.1 提出的构造方法,结合文献[11,12]的思想,我们提出了一种利用低阶弹性函数去构造更高阶的弹性函数,得到了几乎最优并且代数次数好的弹性布尔函数.

构造 3.2 令 n 为偶数,$1\leqslant m\leqslant n/2-2$,$1\leqslant k\leqslant n/2-1$. 假设存在一个代数次数最优的$(n/2+k,m-1,n/2+k-m,\tau)$布尔函数 h. 令 $X=(X_1,\cdots,X_{n/2})\in F_2^{n/2}$,$Y=(Y_1,\cdots,Y_k,Y_{k+1},\cdots,Y_{n/2})=(Y',Y'')\in F_2^k\times F_2^{n/2-k}$. 令 $S=\{Y/Y'\in F_2^k,Y''\in F_2^{n/2-k}\backslash\{\mathbf{0},\mathbf{1}\}\}$,$T=\{X/X\in F_2^{n/2}\}$,这里,$\mathbf{0}=(0,\cdots,0)\in F_2^{n/2-k}$,$\mathbf{1}=(1,\cdots,1)\in F_2^{n/2-k}$. 而且 $\forall Y\in S$,存在一个从 S 到 T 的双射 $\phi(Y)$,使得 $wt(\phi(Y))>m$.

因此,我们可以构造如下结构的密码函数$f\in B_n$:

$$f(X,Y)=\begin{cases}\phi(Y)\cdot X\oplus g(Y),Y''\in F_2^{n/2-k}\backslash\{\mathbf{0},\mathbf{1}\}\\ h(X,Y'),Y''=\mathbf{0}\\ h(X+\mathbf{1},Y'+\mathbf{1})\oplus a_0,Y''=\mathbf{1},a_0\in F_2\end{cases}$$

其中，$g(Y)$为 $n/2$ 元布尔函数.

定理 3.3　通过构造 3.2 得到的布尔函数 $f\in B_n$，满足以下性质：

(1) f 是 m 阶弹性函数；

(2) $nl(f)=2^{n-1}-2^{n/2-1}-2^{n/2+k}+2\tau$；

(3) $\deg(f)=n-m-1$.

证明　令 $(\alpha,\beta)\in F_2^{n/2}\times F_2^{n/2}$，$\beta=(\beta',\beta'')\in F_2^k\times F_2^{n/2-k}$. 通过前面的定义，我们有

$$W_f(\alpha,\beta)=\sum_X\sum_Y(-1)^{f(X,Y)\oplus(X,Y)\cdot(\alpha,\beta)}=$$
$$\sum_{Y''}(-1)^{Y''\cdot\beta''}\sum_{Y'}\sum_X(-1)^{f(X,Y)\oplus X\cdot\alpha\oplus Y'\cdot\beta'}=$$
$$\sum_{Y',X|Y''=0}(-1)^{h(X,Y')\oplus X\cdot\alpha\oplus Y'\cdot\beta'}+$$
$$(-1)^{\mathbf{1}\cdot\beta''}\sum_{Y',X|Y''=\mathbf{1}}(-1)^{h(X+\mathbf{1},Y'+\mathbf{1})\oplus\alpha_0\oplus X\cdot\alpha\oplus Y'\cdot\beta'}+$$
$$\sum_{Y|Y''\neq\{\mathbf{0},\mathbf{1}\}}(-1)^{g(Y)\oplus Y\cdot\beta}\sum_X(-1)^{(\phi(Y)\oplus\alpha)\cdot X}=$$
$$W_h(\alpha,\beta')+(-1)^{\mathbf{1}\cdot\beta''\oplus\alpha_0}$$
$$\sum_{Y',X|Y''=\mathbf{1}}(-1)^{h(X+1,Y'+1)\oplus X\cdot\alpha\oplus Y'\cdot\beta'}+$$
$$\sum_{Y'|Y''\neq\{\mathbf{0},\mathbf{1}\}}(-1)^{g(Y)\oplus Y\cdot\beta}\sum_X(-1)^{(\phi(Y)\oplus\alpha)\cdot X}=$$
$$W_h(\alpha,\beta')+$$
$$(-1)^{1\cdot\beta''\oplus\alpha_0}\sum_{Y',X|Y''=\mathbf{1}}(-1)^{h(X+\mathbf{1},Y'+\mathbf{1})\oplus(X+\mathbf{1})\cdot\alpha\oplus(Y'+\mathbf{1})\cdot\beta'\oplus\mathbf{1}\cdot\alpha\oplus\mathbf{1}\cdot\beta}+$$
$$\sum_{Y|Y''\neq\{\mathbf{0},\mathbf{1}\}}(-1)^{g(Y)\oplus Y\cdot\beta}\sum_X(-1)^{(\phi(Y)\oplus\alpha)\cdot X}=$$
$$W_h(\alpha,\beta')+(-1)^{1\cdot\beta''\oplus\mathbf{1}\cdot\alpha\oplus\mathbf{1}\cdot\beta''\oplus\alpha_0}W_h(\alpha,\beta')+$$
$$\sum_{Y|Y''\neq\{\mathbf{0},\mathbf{1}\}}(-1)^{g(Y)\oplus Y\cdot\beta}\sum_X(-1)^{(\phi(Y)\oplus\alpha)\cdot X}=$$
$$W_h(\alpha,\beta')+(-1)^{wt(\alpha,\beta)\oplus\alpha_0}W_h(\alpha,\beta')+$$
$$\sum_{Y|Y''\neq\{\mathbf{0},\mathbf{1}\}}(-1)^{g(Y)\oplus Y\cdot\beta}\sum_X(-1)^{(\phi(Y)\oplus\alpha)\cdot X}$$

当 $0\leqslant wt(\alpha,\beta)\leqslant m$ 时，显然 $0\leqslant wt(\alpha,\beta')\leqslant m$，$0\leqslant wt(\alpha)\leqslant m$. 又 $wt(\phi(Y))>m$，故 $\phi(Y)\oplus\alpha\neq 0$，从而 $\sum_{Y|Y''\neq\{\mathbf{0},\mathbf{1}\}}(-1)^{g(Y)\oplus Y\cdot\beta}\sum_X(-1)^{(\phi(Y)\oplus\alpha)\cdot X}=0$. 因此，$W_f(\alpha,\beta)=W_h(\alpha,\beta')+(-1)^{wt(\alpha,\beta)\oplus\alpha_0}W_h(\alpha,\beta')$.

当 $wt(\alpha,\beta')=m$ 时，

$$W_f(\alpha,\beta)=W_h(\alpha,\beta')+(-1)^{m\oplus\alpha_0}W_h(\alpha,\beta')=$$
$$W_h(\alpha,\beta')(1+(-1)^{m\oplus\alpha_0}).$$

由此可见，若 m 为偶数，选取时 $a_0=1$，$W_f(\alpha,\beta)=0$；若 m 为奇数，选取 $a_0=0$ 时，$W_f(\alpha,\beta)=0$. 又函数 h 为 $m-1$ 阶弹性函数，故当 $0\leqslant wt(\alpha,\beta')\leqslant m-1$ 时，$W_h(\alpha,\beta')=0$，即 $W_f(\alpha,\beta)=0$.

因此，$0\leqslant wt(\alpha,\beta)\leqslant m$ 时，$W_f(\alpha,\beta)=0$，即 f 是 m 阶弹性函数.

当 $wt(\alpha,\beta)>m$ 时，

$$\sum_{Y|Y''\neq\{\mathbf{0},\mathbf{1}\}}(-1)^{g(Y)\oplus Y\cdot\beta}\sum_X(-1)^{(\phi(Y)\oplus\alpha)\cdot X}=0$$ 或 $\pm 2^{n/2}$. 故 $\max_{\alpha,\beta}|W_f(\alpha,\beta)|\leqslant 2\max_{\alpha,\beta'}|W_h(\alpha,\beta')|+2^{n/2}$，又 $\max_{\alpha,\beta'}|W_h(\alpha,\beta')|=2^{n/2+k}-2\tau$，则 $\max_{\alpha,\beta}|W_f(\alpha,\beta)|=2^{n/2+k+1}+2^{n/2}-4\tau$，因此，

$$nl(f)=2^{n-1}-1/2\max_{\alpha,\beta}|W_f(\alpha,\beta)|=$$
$$2^{n-1}+2^{n/2-1}-2^{n/2+k}+2\tau.$$

注意到函数 f 的代数正规型可表示为

$$f(X,Y)=\bigoplus_{\substack{C_i'\in F_2^k\\ C_j''\in F_2^{n/2-k}\setminus\{\mathbf{0},\mathbf{1}\}}}\Big(\prod_{i=1}^{k}C_i'\oplus Y_i'\oplus 1\Big)$$
$$\Big(\prod_{j=1}^{n/2-k}C_j''\oplus Y_j''\oplus 1\Big)(\phi(C_i',C_j'')\cdot X)\oplus$$
$$\prod_{j=1}^{n/2-k}(Y_j''\oplus 1)h(X,Y')\oplus\prod_{j=1}^{n/2-k}(Y_j'')(h(X+\mathbf{1},$$
$$Y'+\mathbf{1})\oplus\alpha_0)=$$
$$S(X,Y)\oplus T(X,Y)$$

$$S(X,Y)=\prod_{j=1}^{n/2-k}(Y_j''\oplus 1)h(X,Y')\oplus$$
$$\prod_{j=1}^{n/2-k}(Y_j'')(h(X+\mathbf{1},Y'+\mathbf{1})\oplus\alpha_0)$$

$$T(X,Y)=\bigoplus_{\substack{C_i'\in F_2^k\\ C_j''\in F_2^{n/2-k}\{\mathbf{0},\mathbf{1}\}}}\Big(\prod_{i=1}^{k}C_i'\oplus Y_i'\oplus$$
$$1\Big)\Big(\prod_{j=1}^{n/2-k}C_j''\oplus Y_j''\oplus 1\Big)(\phi(C_i',C_j'')\cdot X)$$

在 $S(X,Y)$ 中，$\prod_{j=1}^{n/2-k}(Y_j''\oplus 1)h(X,Y')$ 单项中包含了 $\prod_{j=1}^{n/2-k}(Y_j'')h(X+\mathbf{1},Y'+\mathbf{1})$ 项，故单项 $\prod_{j=1}^{n/2-k}(Y_j'')h(X+\mathbf{1},Y'+\mathbf{1})$ 会被抵消掉，即 $\prod_{j=1}^{n/2-k-1}(Y_j''\oplus 1)h(X,Y')$ 单项拥有最大的代数次数，为 $n/2-k-1+\deg(h)=n-m-1$. 在 $T(X,Y)$ 中，很明显可以看到，$\deg(\prod_{i=1}^{k}(C_i'\oplus Y_i'\oplus 1))=k$，$\deg(\prod_{j=1}^{n/2-k}(C_j''\oplus Y_j''\oplus 1))=n/2-k$，$\deg(\phi(C_i',C_j'')\cdot X)=1$. 故 $\deg(T(X,Y))\leqslant n/2+1$. 由于 $1\leqslant m\leqslant n/2-2$，故 $\deg(f)=n-m-1$.

文献[11]主要利用 $2^{n/2}-\sum_{i=1}^{s}2^{k_i}$ 个不同的 $n/2$ 元 m 阶弹性线性函数和 s 个 $n/2+k_i$ 元高非线性 m 阶弹性函数进行级联，而文献[12]构造的函数在全 0 和全 1 点处用两个特殊的平衡函数代替，在其他点处则是线性函数的级联组成的. 而我们给出的构造 3.2，充分结合了前两者的思想，得到的函

数 f 可以看作是 $2^k(2^{n/2-k}-2)$个不同的 $n/2$ 元 m 阶弹性仿射函数,1 个在部分 0 点处的 $n/2+k$ 元代数次数最优的 $m-1$ 阶弹性函数 $h(X,Y')$和 1 个在部分 1 点处的 $n/2+k$ 元代数次数最优的 $m-1$ 阶弹性函数 $h(X+\mathbf{1},Y'+\mathbf{1})\oplus a_0$ 的级联. 此处,$(n/2+k,m-1,n/2+k-m,\tau)$布尔函数 h 可根据文献[7,16]构造得到. 我们充分利用了弹性仿射函数和低阶弹性函数来构造更高阶代数次数最优的弹性函数.

4 结 论

布尔函数作为设计序列密码和分组密码的重要部件,其密码学性质的好坏直接影响到密码系统的安全性. 为了使构造的密码体制能抵抗线性攻击,具有较高的非线性度,密码学界一直在努力地构造和寻找具有优良性质的密码函数. 本文提出了一种构造弹性布尔函数的方法,得到了一大类具有几乎最优的非线性度和最优的代数次数的函数. 当然,在向量空间上很容易计算函数的谱值,进而得到其非线性度,但是很难估算出代数免疫度. 因此,如何提高这类函数的代数免疫度将是未来的一个研究方向.

参考文献:

[1] Rothaus O S. On "Bent" functions[J]. J Combin Theory, 1976, 20(3): 300.

[2] Matsui M. Linear cryptanalysis method for DES cipher [C]//Proceedings of Eurocrypt. Berlin: Springer, 1994.

[3] 胡云山,申意,曾光,等. 针对减宽 SHA-1 算法的模差分攻击分析[J]. 四川大学学报:自然科学版, 2016, 53(5): 1041.

[4] Siegenthaler T. Correlation-immunity of nonlinear combining function for cryptographic application[J]. IEEE Trans Inform Theory, 1984, 30(5): 776.

[5] Camion P, Carlet C, Charpin P, *et al*. On correlation-immune functions[C] //Proceedings of Eurocrypt. Berlin: Springer, 1991.

[6] Dillon J F. Elementary Hadamard difference sets[D]. Maryland: University of Maryland, 1974.

[7] Sarkar P, Maitra S. Construction of nonlinear Boolean functions with important cryptographic properties[C]//Proceedings of Eurocrypt. Berlin: Springer, 2000.

[8] Maitra S, Pasalic E. A Maiorana-McFarland type construction for resilient Boolean functions on n variables (n even) with nonlinearity [J]. Discrete Appl Math, 2006, 154(2): 357.

[9] Pasalic E. Maiorana-McFarland class: degree optimization and algebraic properties[J]. IEEE Trans Inform Theory, 2006, 52(10): 4581.

[10] Zhang W G, Xiao G Z. Constructions of almost optimal resilient Boolean functions on large even number of variables[J]. IEEE Trans Inform Theory, 2009, 55(12): 5822.

[11] Li L Y, Zhang W G. Construction of resilient Boolean functions with high nonlinearity and good algebraic degree[J]. Secur and Commun Netw, 2015, 8(16): 2909.

[12] Tang D, Zhang W G, Tang X H. Construction of balanced Boolean functions with high nonlinearity and good autocorrelation properties[J]. Des Codes Cryptogr, 2013, 67(1): 77.

[13] 秦小二,胡双年,姜灏,等. 用 Hadamard 矩阵构造线性码[J]. 四川大学学报:自然科学版, 2015, 52(6): 1221.

[14] Xiao G Z, Massey J L. A spectral characterization of correlation-immune combining functions [J]. IEEE Trans Inform Theory, 1988, 34(3): 569.

[15] Zhang W G, Pasalic E. Constructions of resilient S-boxes with strictly almost optimal nonlinearity through disjoint linear codes[J]. IEEE Trans Inform Theory, 2014, 60(3): 1638.

[16] Maitra S, Pasalic E. Further construction of resilient Boolean functions with very high nonlinearity[J]. IEEE Trans Inform Theory, 2002, 48(7): 1825.