文章编号: 1001- 2486(2009) 02- 0086- 04

高非线性度弹性 S 盒的构造*

付绍静, 李 超, 董德帅
(国防科技大学 理学院, 湖南 长沙 410073)

摘 要: 弹性 S 盒可应用于容错分布计算, 量子密码密钥分配和流密码中伪随机序列产生。基于线性码和高非线性度的 S 盒, 给出了一种构造具有高非线性度, 且代数次数大于给定值的弹性 S 盒的方法。对于给定参数的线性码, 构造的弹性 S 盒的非线性度是可以计算的。结果表明所构造的函数的非线性度优于已有的结果。

关键词: 布尔函数; 弹性函数; 线性码; 非线性度
中图分类号: TP391 文献标识码: A

Constructions of High Degree Resilient S-boxes with High Nonlinearity

FU Shao-jing, LI Chao, DONG De-shuai
(College of Science, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: The resilient S-boxes have applications in fault tolerant distributed computing, quantum cryptographic key distribution and random sequence generation for stream ciphers. Based on the use of linear error correcting codes together with highly nonlinear S-Boxes, a new construction of highly nonlinear resilient S-boxes with given degree is provided. A contribution of the construction is that the nonlinearity of the resilient S-boxes can be calculated with the parameter of the linear code. As a result, the construction provides currently the best results in the aspect of nonlinearity.

Key words: boolean functions; resilient functions; linear codes; nonlinearity

弹性 S 盒的概念首先由 Chor 等提出[1], 这类函数可以广泛应用于容错分布计算, 量子密码的密钥分配, 以及流密码中的伪随机序列产生[2-3]。然而, 最初人们关于弹性 S 盒的研究, 主要是针对其非线性度, 没有考虑代数次数。在文献[4]中, Cheon 首次构造了代数次数大于给定值的弹性 S 盒, 即给定一个线性$[n-d-1, m, t+l]$码, 对任意的正整数 d, 可以构造出代数次数为 d 的(n, m, t)弹性S 盒, 其非线性度大于$2^{n-1}-2^{n-d-1}\lfloor\sqrt{2^n}\rfloor+2^{n-d-2}$。Gupta[5] 证明: 对于任意非负整数 d, 给定一个$[n-d-1, m, t+1]$线性码, 可以构造次数为 d 的(n, m, t)S 盒, 它非线性度为 $2^{n-1}-2^{n-\lceil\frac{d+1}{2}\rceil}-2^{n-d-1}(m+1)$。

本文通过级联满足一定条件的多输出函数, 得到了次数大于 d 的(n, m, t)弹性 S 盒, 并且该弹性函数具有较高非线性度。与已有的文献结果相比, 我们得到的弹性 S 盒的非线性度是最优的。

1 预备知识和主要引理

记 F_2^n 为 F_2 上的 n 维向量空间。对于一个 n 元布尔函数$f(x)$, 集合$\{x \mid f(x)=1\}$的元素个数称为$f(x)$的重量, 记为 $wt(f)$, 如果 $wt(f)=2^{n-1}$, 则称$f(x)$是平衡的。n 元布尔函数$f(x)$与所有 n 元仿射函数的最小汉明距离称为$f(x)$的非线性度 $nl(f)$。$f(x)$的walsh 变换定义为 $S_f(w)=\sum_{x\in F_2^n}(-1)^{f(x)\oplus x\cdot w}$, 这里 $w=(w_1\cdots w_r)$, $x=(x_1\cdots x_n)$, $x\cdot w=x_1w_1\oplus\cdots\oplus x_nw_n$。

定义 1 设$f(x_1\cdots x_n): F_2^n\to F_2$, 如果对于任意 $0\leqslant wt(w)\leqslant t$ 都有 $S_f(w)=0$, 则称$f(x)$是 t 阶弹性

* 收稿日期: 2008- 09- 31
基金项目: 国家自然科学基金资助项目(60573028); 国防科技大学基金资助项目(JC08- 02- 04)
作者简介: 付绍静(1984—), 男, 博士生。

函数。

定义 2[6] 给定 m 个布尔函数$f_1(x), f_2(x), \cdots, f_m(x)$。则称 $F(x)=(f_1(x), f_2(x), \cdots, f_m(x))$ 为 $F_2^n \to F_2^m$ 的 S 盒, $F(x)$ 的非线性度定义为: $nl(F)=\min\limits_{\tau\in(F_2^m)^*} nl(g_\tau) \mid g_\tau=\oplus_{i=1}^m \tau_i f_i(x)$; F 的次数定义为: $\deg(F)=\min\limits_{\tau\in F_2^m} \deg(\oplus_{i=1}^m \tau_i f_i(x))$, 这里$(F_2^m)^* = F_2^m \setminus 0$, $\tau=(\tau_1 \cdots \tau_m)$。如果$f_1(x), f_2(x), \cdots, f_m(x)$的任意的非零线性组合都为 $F_2^n \to F_2$ 的 t 阶弹性函数, 则称 $F(x)$ 为 $F_2^n \to F_2^m$ 的 t 阶弹性 S 盒, 记为 (n, m, t) S 盒。

引理 1[6] 设$f(y): F_2^n \to F_2$, $g(x): F_2^u \to F_2$, 则 $h(y, x)=f(y)\oplus g(x)$ 非线性度为 $nl(h)=2^u nl(g)+2^u nl(f)-2nl(g)\,nl(h)$。

引理 2[7] 当 $n \geqslant 2m$ 且 n 是偶数时, 存在的(n, m) S 盒: $F=(f_1(x), \cdots, f_m(x))$ 非线性度为 $2^{n-1}-2^{\frac{n}{2}-1}$, 且所有$f_i(x)$次数不大于 $n/2$。

引理 3[8] 给定整数 m, 存在S 盒 $F: F_2^m \to F_2^m$ 满足 $nl(F) \geqslant 2^{m-1}-2^{\frac{1}{2}m}$。

引理 4[9] 如果存在一个(n, m, t) S 盒, 则可以构造一个次数不大于 $m-1$ (n, m, t) S 盒, 该 S 盒的非线性度大于或等于 $2^{n-1}-2^{n-\frac{m}{2}}$。

2 高次弹性 S 盒的构造

定理 1 对于给定的正整数 d, $m(d>m)$, 存在次数为 d 的$(d+1, m)$ S 盒 $H: F_2^{d+1} \to F_2^m$ 满足: (1) 当 $d \geqslant 2m-1$ 且 d 为奇数时, $nl(H) \geqslant 2^d-2^{\frac{d-1}{2}}-(m+1)$; (2) 当 $d \geqslant 2m-1$ 且 d 为偶数时, $nl(H) \geqslant 2^d-2^{\frac{d}{2}}-(m+1)$。

证明 首先定义 $g_i(x)=x_1x_2\cdots x_{i-1}x_{i+1}\cdots x_{d+1}$, $1 \leqslant i \leqslant m$, 则 $g_i(x)$ $(1 \leqslant i \leqslant m)$ 都是次数为 d 的函数, 并且 $g_i(x)$ $(1 \leqslant i \leqslant m)$ 的任意非零线性组合也是一个次数为 d 的函数。

(1) 当 $d \geqslant 2m-1$ 且 d 为奇数。此时 $d+1$ 为偶数, 由引理 2 可以构造一个次数不大于$(d+1)/2$ 的 $(d+1, m)$ S 盒: $F=(f_1(x), \cdots, f_m(x))$, 该S 盒的非线性度为 $nl(F) \geqslant 2^d-2^{\frac{d-1}{2}}$, 此时 $nl(f_i)=2^d-2^{\frac{d-1}{2}}$ 和 $\deg(f_i) \leqslant \frac{d+1}{2}$。

令 $h_i=f_i\oplus g_i$ $(1 \leqslant i \leqslant m)$, 则 $H=(h_1, \cdots, h_m)$ 也是$(d+1, m)$ S 盒。

$$\forall\, \tau=(\tau_1 \cdots \tau_m) \in (F_2^m)^*,\ \oplus_{i=1}^m \tau_i h_i=\oplus_{i=1}^m \tau_i(f_i+g_i)=(\oplus_{i=1}^m \tau_i f_i)+(\oplus_{i=1}^m \tau_i g_i)$$

$$\deg((\oplus_{i=1}^m \tau_i f_i) \leqslant \frac{d+1}{2} < \deg(\oplus_{i=1}^m \tau_i g_i) \equiv d,\ \text{可推得}\ \deg(H)=d$$

由 $g_i(x)$ 的构造可知 $wt(\oplus_{i=1}^m \tau_i g_i) \leqslant m+1$, 可推得

$$\begin{aligned} nl(H) &= \min_\tau nl(\oplus_{i=1}^m \tau_i h_i)=\min_\tau nl((\oplus_{i=1}^m \tau_i f_i)\oplus(\oplus_{i=1}^m \tau_i g_i)) \\ &= \min_{\tau,\, a(x)\in A_f} wt((\oplus_{i=1}^m \tau_i f_i(x))\oplus(\oplus_{i=1}^m \tau_i g_i(x))\oplus a(x)) \\ &\geqslant \min_{\tau,\, a(x)\in A_f} wt((\oplus_{i=1}^m \tau_i f_i(x))\oplus a(x))-(m+1)=nl(F)-(m+1) \end{aligned}$$

所以 $nl(H) \geqslant 2^d-2^{\frac{d-1}{2}}-(m+1)$ 且 $\deg(H)=d$。

(2) 当 $d \geqslant 2m-1$, d 为偶数。此时 $d+1$ 为奇数, 由引理 2 可以构造一个次数不大于$\frac{d}{2}$的(d, m) S 盒: $F=(f_1, \cdots, f_m)$, 该 S 盒的非线性度为 $nl(F)=2^d-2^{\frac{d-2}{2}}$, 此时 $nl(f_i) \geqslant 2^d-2^{\frac{d-1}{2}}$ 和 $\deg(f_i) \leqslant \frac{d}{2}$。

令 $h_i=f_i\oplus g_i$ $(1 \leqslant i \leqslant m)$, 则 $H=(h_1, \cdots, h_m)$ 是$(d+1, m)$ S 盒。 $\forall\, \tau=(\tau_1 \cdots \tau_m) \in (F_2^m)^*$

$\deg(\oplus_{i=1}^{m}\tau_i f_i) \leqslant d/2 < \deg(\oplus_{i=1}^{m}\tau_i g_i) \equiv d$，可推得 $\deg(H) = d$。

$$\begin{aligned} nl(H) &= \min_{\tau} nl(\oplus_{i=1}^{m}\tau_i h_i) = \min_{\tau} nl((\oplus_{i=1}^{m}\tau_i f_i) + (\oplus_{i=1}^{m}\tau_i g_i)) \\ &= \min_{\tau,\, a(x)\in A_f} wt((\oplus_{i=1}^{m}\tau_i f_i(x)) \oplus (\oplus_{i=1}^{m}\tau_i g_i(x)) \oplus a(x)) \\ &\geqslant \min_{\tau,\, a(x)\in A_f} wt((\oplus_{i=1}^{m}\tau_i f_i(x)) \oplus a(x)) - (m+1) = 2^d - 2^{\frac{d}{2}} - (m+1) \end{aligned}$$ □

定理2 给定一个$[n-d-1, m, t+1]$线性码及正整数 $d > m$，则可以构造出次数为 d 的(n, m, t) S盒 W，它非线性度满足：(1)当 $d \geqslant 2m-1$ 且 d 为奇数时，$nl(W) \geqslant 2^{n-1} - 2^{n-\frac{m}{2}-d-1}\cdot(2^{\frac{d-1}{2}} + m + 1)$；(2)当 $d \geqslant 2m-1$ 且 d 为偶数时，$nl(W) \geqslant 2^{n-1} - 2^{n-\frac{m}{2}-d-1}(2^{\frac{d}{2}} + m + 1)$；(3)当 $d < 2m-1$ 时，$nl(W) \geqslant 2^{n-1} - 2^{n-\frac{m}{2}-\frac{d+1}{2}}$。

证明 由定理1可构造次数 $d > m$ 的$(d+1, m)$ S盒 $H = (h_1(x), \cdots, h_m(x)): F_2^{d+1} \to F_2^m$，它的非线性度

$$nl(H): \begin{cases} \geqslant 2^d - 2^{\frac{d-1}{2}} - (m+1), d \geqslant 2m-1, d \text{ 为奇数} \\ \geqslant 2^d - 2^{\frac{d}{2}} - (m+1), d \geqslant 2m-1, d \text{ 为偶数} \end{cases} \quad (\text{Ⅰ})$$

如果存在$[n-d-1, m, t+1]$线性码，则可以构造出一个$(n-d-1, m, t)$ S盒，再由引理4可以构造出非线性度大于 $2^{n-d-2} - 2^{n-d-1-\frac{1}{2}m}$ 的$(n-d-1, m, t)$ S盒 $F = (f_1(y), \cdots, f_m(y))$，且该S盒的次数不大于 $m-1$。

令 $w_i(x, y) = f_i(y) \oplus h_i(x)$ $(1 \leqslant i \leqslant m)$，令 $W = (w_1, \cdots, w_m)$，则 W 是(n, m) S盒，由于 $F = (f_1(y), \cdots, f_m(y))$ t 阶弹性S盒，所以

$$S_{(\odot_{i=1}^{m}\tau_{i\,i}^{w})}(u_1, u_2) = S_{(\odot_{i=1}^{m}\tau_{i\,i}^{f}) + (\odot_{i=1}^{m}\tau_{i\,i}^{h})}(u) = S_{(\odot_{i=1}^{m}\tau_{i\,i}^{f})}(u_1) \cdot S_{(\odot_{i=1}^{m}\tau_{i\,i}^{h})}(u_2) = 0$$

从而 W 是 t 阶弹性S盒。

$$\deg(W) = \min_{\tau=(\tau_1,\cdots\tau_m)} \deg((\oplus_{i=1}^{m}\tau_i f_i) + (\oplus_{i=1}^{m}\tau_i h_i)) = d$$

再利用引理1，得

$$\begin{aligned} nl(\oplus_{i=1}^{m}\tau_i w_i) &= 2^{n-d-1} nl(\oplus_{i=1}^{m}\tau_i h_i) + 2^{d+1} nl(\oplus_{i=1}^{m}\tau_i f_i) - 2nl(\oplus_{i=1}^{m}\tau_i h_i)\, nl(\oplus_{i=1}^{m}\tau_i f_i) \\ &= 2^{n-d-1} nl(\oplus_{i=1}^{m}\tau_i h_i) + [2^{d+1} - 2nl(\oplus_{i=1}^{m}\tau_i h_i)]\, nl(\oplus_{i=1}^{m}\tau_i f_i) \\ &\geqslant 2^{n-d-1} nl(\oplus_{i=1}^{m}\tau_i h_i) + [2^{d+1} - 2nl(\oplus_{i=1}^{m}\tau_i h_i)](2^{n-d-2} - 2^{n-d-1-\frac{1}{2}m}) \\ nl(W) &= \min_{\tau} nl(\oplus_{i=1}^{m}\tau_i w_i) \\ &\geqslant \min_{\tau}\{2^{n-d-1} nl(\oplus_{i=1}^{m}\tau_i h_i) + [2^{d+1} - 2nl(\oplus_{i=1}^{m}\tau_i h_i)](2^{n-d-2} - 2^{n-d-1-\frac{1}{2}m})\} \\ &= 2^{n-d-1} nl(H) + [2^{d+1} - 2nl(H)](2^{n-d-2} - 2^{n-d-1-\frac{1}{2}m}) \end{aligned} \quad (\text{Ⅱ})$$ □

把(Ⅰ)的结果代入(Ⅱ)即得结论。

3 结果比较

在文献[5]中，Gupta得到下面结论。

引理5[5] 对于任意非负整数 d，如果存在$[n-d-1, m, t+1]$二元线性码，则可以构造次数为 d 的(n, m, t) S盒，它非线性度为 $2^{n-1} - 2^{n-\lceil\frac{d+1}{2}\rceil} - 2^{n-d-1}(m+1)$。

Gupta比较发现他构造的S盒非线性度优于与Cheon[4]的结果。下面这个定理表明本文构造的S盒非线性度是最高的。

定理3 本文构造的次数为 d 的(n, m, t) S盒的非线性度优于文献[5]。

证明　本文构造的 S 盒非线性度满足

$$nl(H) \geqslant \min\{2^{n-1} - 2^{n-\frac{m}{2}-d-1}(2^{\frac{d-1}{2}} + m + 1), 2^{n-1} - 2^{n-\frac{m}{2}-d-1}(2^{\frac{d}{2}} + m + 1), 2^{n-1} - 2^{n-\frac{m}{2}-\frac{d+1}{2}}\}$$
$$\geqslant 2^{n-1} - 2^{n-\frac{m}{2}-\frac{d+1}{2}}$$

需要证明 $2^{n-1} - 2^{n-\lceil\frac{d+1}{2}\rceil} - 2^{n-d-1}(m+1) \leqslant 2^{n-1} - 2^{n-\frac{m}{2}-\frac{d+1}{2}}$

$$[2^{n-1} - 2^{n-\lceil\frac{d+1}{2}\rceil} - 2^{n-d-1}(m+1)] - (2^{n-1} - 2^{n-\frac{m}{2}-\frac{d+1}{2}})$$
$$= -2^{n-\lceil\frac{d+1}{2}\rceil} - 2^{n-d-1}(m+1) + 2^{n-\frac{m}{2}-\frac{d+1}{2}}$$

□

容易验证上式结果小于 0, 即得结论。

参 考 文 献:

[1] Chor B, Goldreich O, Hastad J, et al. The bit extraction problem or t-resilient functions[C]//26th IEEE Symposium on Foundations of Computer Science, 1985: 396-407.

[2] Maity S, Maitra S. Minimum Distance Between Bent and 1-resilient Boolean Functions[C]//FSE 2004, Lecture Notes in Computer Science, 3017, Springer, Berlin, 2004: 143-160.

[3] Rurppet R. Analysis and Design of Stream Ciphers[J]. Berlin Germany: Spring-verlag, 1996.

[4] Cheon J H. Nonlinear Vector Resilient Functions[J]. Cryptology CRYPTO 2001, Lecture Notes in Computer Science. Springer Verlag, 2001.

[5] Gupta K C, Sarkar P. Construction of High Degree Resilient S-boxes with Improve Nonlinearity[J]. 2005 Elsevier B. V Information Processing Letters 95: 413-417.

[6] Carlet C. Boolean Functions for Cryptography and Error Correcting Codes[M]. London: Cambridge University, 2007.

[7] Neberg K. Constructions of bent Functions and difference sets[C]//Cryptology-EUROCRYPT' 90, Berlin: Springer-verlag, 1991, 373: 155-160.

[8] Nyberg K. Differentially Uniform Mappings for Cryptography[C]//Cryptology-eUROCRYPT' 93, Berlin: Springer-verlag, 1994, 765: 55-64.

[9] Zhang X M, Zheng Y. Cryptographically Resilient functions[J]. IEEE Transactions on Information Theory, 43(5): 1740-1747, 1997.

(上接第 58 页)

4 结 论

本文将任意布局传输线进行离散, 引入理想节点的概念, 应用 BLT 方程, 对共地任意布局传输线间的串扰进行了分析, 突破了传统串扰分析方法只适用于平行线的限制。数值算例表明本文方法的正确性和有效性。研究表明, 相对于平行线, 非平行线受扰线远端受串扰的影响随线间角度的增大而减小; 两线距离越大, 串扰越小。对于交叉线情况, 交叉角度越大, 受扰线受串扰的影响越小。

虽然只对非平行线和交叉线两种特例进行了分析, 但本文方法适合于任意布局电缆间的串扰分析。本文方法可应用在系统级和板级的电磁兼容分析中。

参 考 文 献:

[1] Baum C E, Liu T K, Tesche F M. On the Analysis of General Multiconductor Transmission Line Networks[J]. Interaction Note 350, Kirtland AFB, NM, 1978.

[2] Baum C E. The Theory of Electromagnetic Interference Control[J]. Interaction Notes, Note 478, 1989.

[3] Haase H, Steinmetz T, Nitsch J. New Propagation Models for Electromagnetic Waves along Uniform and Nonuniform Cables[J]. IEEE Transactions on Electromagnetic Compatibility, 2004, 46(3).

[4] Cracraft M A. Crosstalk Analysis for Nonparallel Transmission Lines Using PEEC with a Dynamic Green's Function Formulation[C]//International Symposium on EMC, 2006: 29-33.

[5] Khalaj-amirhosseini M. Analysis of Coupled or Single Nonuniform Transmission Lines Using Taylor's Series Expansion[J]. Progress in Electromagnetics Research, PIER 60, 2006: 107-117.

[6] Besnier P. Electromagnetic Topology: Investigations of Nonuniform Transmission Line Networks[J]. IEEE Trans. on EMC, 1995, 37(2).

[7] Parmantier J P. An Efficient Technique to Calculate Ideal Junction Scattering Parameters in Multiconductor Transmission Line Networks[J]. Interaction Notes, Note 536, 1998.

[8] Brandao Faria J A. Nonuniform Transmission-line Structures Internal and External Propagation Parameters[J]. Electrical Engineering, 2005, 87: 19-22.