第 24 卷第 6 期　　四川理工学院学报(自然科学版)　　Vol. 24　No. 6
2011 年 12 月　　Journal of Sichuan University of Science & Engineering(Natural Science Edition)　　Dec. 2011
文章编号:1673-1549(2011)06-0726-03

S 盒布尔函数非线性度的分析

李小伟,王　娜,范安东

(成都理工大学管理科学学院,成都　610059)

摘　要:基于 S 盒构造准则,给出了构造较高非线性度,并具备良好密码学性质的布尔函数的理论依据;针对多输出布尔函数的非线性度和第二类非线性度,分析了两者之间的关系,并给出了有效抗击最佳多输出仿射逼近攻击的一个判断依据;最后利用 walsh 谱理论得出 walsh 循环谱与非线性度的关系,并对 Camellia 算法 S 盒中的布尔函数非线性度进行了刻画,从理论上揭示了此算法的安全性。

关键词:S 盒;布尔函数;非线性度;walsh 谱;Camellia 算法

中图分类号:TN918.1　　**文献标识码**:A

引　言

布尔函数的非线性度是密码体系中的一个重要的衡量指标,其非线性度的高低直接影响到密码的安全性能。流密码中的密钥流生成器、分组密码中的 S 盒、认证码等都需要使用布尔函数来构造[1-2],而 S 盒是分组密码算法中唯一的一个非线性部件,选用高非线性度的 S 盒可以有效的抵抗最佳仿射逼近法的攻击[3]。而 S 盒的设计准则一般包括非线性度、平衡性、差分均匀性、无偏性、代数次数和项数分布、正交性、雪崩效应和扩散特性[4]。如何提高 S 盒的各项指标使其达到最优是现在研究的重点,比如 cracraft 在文献[5]中构造的代数次数大于给定值的弹性 S 盒,dawson 和 tavares 在文献[6-7]中所做出的 S 盒构造准则研究,gupta 等在文献[8]中对提高 S 盒的非线性抵抗性提出的理论。Bent 函数由于其最高的非线性度特性而受到很大的重视[9],但是由于非线性度和其他的密码强度指标存在着制约关系,所以 Bent 函数虽然具有很高的非线性度,但是还存在一些缺陷,比如不平衡、不具有相关免疫性、代数次数不超过 N/2 等;相关学者对 Bent 函数提出了相应的改进[10-11]。利用 Walsh 谱理论,可以对布尔函数的非线性度进行很好的刻画,William Millan 曾给出一个能改善 S 盒非线性度的 Hill Climbing 算法,它通过交换 S 盒的两个输出向量来提高 S 盒的非线性度直到非线性度达到一个局部最优值。而对于多输出布尔函数的非线性度定义,相关学者也提出另外一种定义作为抵抗最佳多输出仿射逼近攻击的判断准则。2003 年提出的 Camellia 算法能很好的抵抗差分和线性密码分析这两种分组密码的主要攻击方式,本文最后对其非线性度进行探讨,从本质上解释了算法的安全性。

1　基本定义

定义 1　设 $f(x):F_2^n \to F_2$ 是 n 元布尔函数。称 $\hat{F}(w)$ 是 $f(x)$ 的 walsh - Hadamard 变换,是指:$\hat{F}(w) = \sum(-1)^{f(x)\oplus L_w(x)}$,其中 $L_w(x) = w_1x_1 \oplus w_2x_2 \oplus \cdots \oplus w_nx_n$,$w = (w_1, w_2, \cdots, w_n) \in F_2^n$。

定义 2　n 元布尔函数的非线性度 $N_f = \min_{l\in L_n} d_H(f, l)$,$l \in L_n$,其中 L_n 表示全体 n 元线性和仿射函数之集,$d_H(f,l)$ 表示 f 和 l 之间的汉明距离。

不妨用 $WH_{\max}$ 表示 $\hat{F}(w)$ 的最大绝对值,则 $N_f = \frac{1}{2}(2^n - WH_{\max})$,易知通过降低 $WH_{\max}$ 可以增加布尔函数的非线性度。

定义 3　函数 $S(x) = (f_1(x), \cdots f_m(x))$ 是一个多输出函数,称 $N_s = \min d_H(u \cdot s(x), l(x))$ 为 $S(x)$ 的非线性度,其中,$l \in L_n$,$0 \neq u \in F_2^m$ 它等于 S 盒各输出位的任意非零线性组合所形成的布尔函数与 l 之间的最小汉明距离。

收稿日期:2011-10-17

作者简介:李小伟(1984-),男,河南新乡人,硕士生,主要从事信息安全方面的研究,(E-mail)twinslixiaowei@163.com

不妨对每个非零线性组合都进行 WHT 变换形成 WHT 矩阵,矩阵元素可表示为:

$B_\theta(\tilde{w}) = \sum_x L_\theta(y) \cdot L_{\tilde{w}}(x)$,用 $WH_{\max}$ 表示 $B_\theta(\tilde{w})$ 的最大绝对值,因此可以得到如下结论: $N_s = \frac{1}{2}(2^n - WH_{\max})$。显然,降低 $WH_{\max}$ 同样可以提高 S 盒的非线性度。

定义 4　设 F 是 V_n 到 V_m 的多输出布尔函数,称 $N_f = \min_{\Phi \in AF_{n,m}} d(F,\Phi)$ 为 F 的第二类非线性度,其中 $AF_{n,m}$ 表示所有从 V_n 到 V_m 的仿射函数的集合, $d(F,\Phi) = |\{x \in V_n: F(x) \neq \Phi(x)\}|$。

定义 5　设 F_2^n 上 $x = (x_1,x_2,\cdots,x_n)$, $w = (w_1,w_2,\cdots,w_n)$, x 和 w 点积定义为: $w \cdot x = w_1x_1 + w_2x_2 + \cdots + w_nx_n$, n 个变元的布尔函数 $f(x)$ 的 Walsh 谱定义为: $S_{(f)}(w) = \frac{1}{2^n}\sum_{x \in F_2^n} (-1)^{f(x)+w\cdot x}$。

2　定理与分析

定理 1　对任意的 $1 \leqslant i \neq j \leqslant n$, 函数 $f_{ij}(x) = x_ix_j + g_{ij}(x)$ 的非线性度至少为 2^{n-2}, 即 $N_{f_{ij}} \geqslant 2^{n-2}$。

证明　设 $g_{ij}(x)$ 是这样的 n 元函数: x_i, x_j 不同时出现在其任何一项之中, f 为 V_n 上的函数, U 为 V_n 的 s 维子空间。则有: $V_n = \Pi_0 \cup \Pi_1 \cup \cdots \cup \Pi_{2^{n-s}-1}$, 并且可得:

$\Pi_0 = U$, 对于任意 $\alpha,\beta \in V_n$, α,β 属于同一个子集 Π_j, 当且仅当 $\alpha \oplus \beta \in \Pi_0 = U$; 因此,对于 $i \neq j$, $\Pi_i \cap \Pi_j = \phi$。再令

$N_j = |\{\alpha | \alpha \in \Pi_j, f(\alpha) = 1\}|$

$j = 0,1,\cdots,2^{s-1}$。因为 $\Pi_0 = U$, N_0 是奇数,注意到 $\Pi_0 \cup \Pi_j$ 为 V_n 的一个 $s+1$ 维子空间, $j = 1,\cdots,2^{n-s}-1$。

因为 $\Pi_0 = U$ 是 f 的一个最大奇权重子空间, f 上的 $\Pi_0 \cup \Pi_j$ 的汉明距离为偶数,也就是说 $N_0 + N_j$ 为偶数,这就证明了对于 $j = 1,\cdots,2^{n-s}-1$, N_j 是奇数的。因此: $N_0 + N_1 + \cdots + N_{2^{n-s}-1} \geqslant 2^{n-s}$, 也就是说汉明距离最少为 2^{n-s}。$s = 2$ 即为此定理。

证毕。

以上定理给出构造高非线性度布尔函数的一个方法,事实上,设 $f_1(x)$, $f_2(x)$ 是两个 m 元布尔函数,若

$f(x) = x_{m+1}f_1(x) + (x_{m+1}+1)f_2(x)$

则可证明其非线性度 $N_f \geqslant 2^m - 2^{m/2}$。反复递归构造这样的函数,可得到一个 $m+k$ 元布尔函数,使其非线性度大于 2^{n-2}。只要布尔函数在某个子空间上的常值,就可以根据它来构造出高非线性度的平衡函数。

定理 2　对任意 V_n 到 V_m 的函数 $F = (f_1,f_2,\ldots,f_m)$, $N_2(F) \geqslant N_1(F)$。

证明　令 $\Phi = (\phi_1,\phi_2,\ldots,\phi_m)$ 为 V_n 到 V_m 的仿射函数, $f(x) = \bigoplus_{i=1}^m c_if_i(x)$ 是的分量函数的任意非零线性组合,则

$\phi(x) = \bigoplus_{i=1}^m c_i\phi_i(x)$

是 Φ 的分量函数的一个非零线性组合,则

$N_2(F) = d(F,\Phi) =$

$|\{x \in V_n: F(x) \oplus \Phi(x) \neq (0,0,\ldots,0)\}| \geqslant$

$2^n - |\{x \in V_n: f(x) \oplus \phi(x) = 0\}| =$

$d(f,\phi) \geqslant N_f$

另外,设 $N_{f_i} = d(f_i,\theta_i)$, 其中 θ_i 是 V_n 上的仿射函数,令 $\Theta = (\theta_1,\theta_2,\ldots,\theta_m)$, 则

$N_2(F) \leqslant d(F,\Theta) =$

$|\{x \in V_n: F(x) \neq \Theta(x)\}| \leqslant \sum_{i=1}^m N_{f_i}$

根据定义 1.4,即得 $N_2(F) \geqslant N_1(F)$。

证毕。

由以上定理可知,两类非线性度比较高的布尔函数对其分量函数的任意非零线性组合进行的最佳仿射逼近攻击,也可抵抗最佳多输出仿射逼近的攻击。

引理　设 $f_1(x)$, $f_2(x)$ 是两个 n 元布尔函数。如果 $f(x) =: x_{n+1}f_1(x) + (1+x_{n+1})f_2(x)$, 那么有:

$N_f \geqslant N_{f_1} + N_{f_2}$

推论　设 $f_1(x) =: f_1(x_1,x_2,\ldots,x_m)$ 和 $f_1(x) = f_1(x_1,x_2,\ldots,x_m)$ 是两个 m 元 Bent 函数,若

$f(x) =: x_{m+1}f_1(x) + (1+x_{m+1})f_2(x)$

则其线性度满足

$N_f \geqslant 2^m - 2^{m/2}$

通过以上推论,在构造布尔函数的时候,可以递归地构造出 m + k 元的布尔函数,其非线性度比 2^{n-2} 大得多,并且代数次数也有相应的提高。此类函数是基于 Bent 函数构造的,虽不满足雷崩准则,但仍具有较好的扩散性。

3　Walsh 谱与非线性度的关系

根据定义 5, Walsh 循环谱表征的是 $f(x)$ 与线性函数 $x \cdot w$ 相符合的程度。据此可以求出 $f(x)$ 的最佳线性逼近,事实上,

$P(f(x) = w \cdot x) = (1 + W_{(f)}(w))/2$ $P(f(x) = w \cdot x + 1) = (1 - W_{(f)}(w))/2$

若 $W_{(f)}(w) > 0$, 则 $w \cdot x$ 是 $f(x)$ 的最佳线性逼近; 若 $W_{(f)}(w) < 0$, 则 $w \cdot x + 1$ 是 $f(x)$ 的最佳线性逼近。Walsh 循环谱与非线性度的关系如下:

定理 3　对 n 元布尔函数 $f(x)$, $N_{(f)} = 2^{n-1}(1 -$

$\max_w |W_{(f)}(w)|$。

Camellia 算法由有限域 $GF(2^8)$ 上的乘法逆和仿射变换组成,算法包含 4 个 S 盒(S_1,S_2,S_3,S_4),后三个为第一个的循环移位,S_1 的变换为 $y_{(8)} = s_1(x_{(8)})$,如下:

$h(g(f(0xC5 \oplus x_{(8)}))) \oplus 0x6E$

其中 h,g,f 为变换函数。根据定理及 Walsh 循环谱,可以得到 8 个布尔函数的最佳线性逼近函数如下(不唯一):

$x_5 + x_4 + x_2 + x_1 + x_0, x_2 + x_1$

$x_4 + x_3 + x_0, x_2 + x_1, x_4 + x_3$

$x_5 + x_4 + x_3 + x_0, x_4 + x_1 + 1$

$x_5 + x_4 + x_3 + x_0 + 1$

8 个布尔函数都不存在非零线性结构,8 个布尔函数的非线性度均为 112。

4 结 论

布尔函数的非线性度是密码性质的重要指标,本文给出构造高非线性度且具有其他良好密码性质的布尔函数的若干理论,并论证了使用第二类线性度作为布尔函数抵抗最佳逼近攻击的合理性,然后给出利用 Walsh 循环谱来衡量布尔函数非线性度的方法,实际中的 Camellia 算法具有很高的非线性度,其构造方法值得借鉴,但对若干指标的追求下,可能会削弱另外的指标,如何来对这些指标进行折衷量化是有待继续深入研究的。

参 考 文 献:

[1] 斯延森 D R 著. 张文政译. 密码学-理论与实践 [M]. 国防科学技术保密通讯实验室,1997.

[2] 卓先德. 非对称加密技术研究 [J]. 四川理工学院学报:自然科学版,2010,23(5):562-565.

[3] Matsui M. Linear Cryptanalysis Method for DES Cipher [C]. Advances in Cryptology-EUROCRYPT'93, Berlin: Spring-Verlag, 386-397.

[4] 冯登国. 频谱理论及其在通信保密技术中的应用 [D]. 西安电子科技大学,1995.

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

[6] Dawson M H, Tavares S E. An Expanded Set of Design Criteria for Substitution Box and Their Use in Strengthening DES-like [C]. Cryptosystems IEEE Pacific Rim Conference on Communications, victoria, Bl, Canada: Computer and Sigual Processing, 1991: 191-195.

[7] Dawson M H, Tavares S E. An Expanded Set of Design Criteria Based on Information Theory and its Relation to Differen-tial-Like Attacks [C]. Advances in Cryptology EUROCRYPT'91 Processing, Berlin: Springer-Verlag, 1991: 352-367.

[8] Gupta K C, arkar P S. Improved construction of nonlinear resilient S-boxes [J]. IEEE Transactions on Information Theory, 2005, 51(1): 339-348.

[9] Dobbertin. Construction of bent function and balanced Boolean functions with high nonlinearity [A]. Proceedings of the 1994 Leuven Workshop on Cryptographic Algorithms [C]. Berlin: Spring-Verlag, 1995: 61-74.

[10] Canteaut A, Daum M, Dobbertin H, et al. Normal and nonnormal bent functions [A]. in Proc. Workshop on Coding and Cryptography (WCC 2003) [C]. Versailles, France, 2003: 91-100.

[11] Carlet C, Dobbertin H, Leander G. Normal extension of bent functions [J]. IEEE Transacions on Information Theory, 2004, 50(11): 2880-2885.

Analysis of Boolean Function with High Nonlinearity in S-Box

LI Xiao-wei, WANG Na, FAN An-dong

(College of Management Science, Chendu University of Technology, Chengdu 610059, China)

Abstract: Based on the criterion of constructing S-Box, the theoretical basis of constructing a high nonlinearity Boolean function, also with some good cryptographic properties is provided. For the nonlinearity and a new kind of nonlinerity of muti output Boolean function, the relation between them is analyzed, and then an effective estimation method to resist best affine approximation attack is provided. Furthermore, using the theory of Walsh spectrum, the relation between Walsh spectrum and nonlinearity is given, and then the nonlinearity of S-Box in Camellia algorithm is analyzed, the security of the algorithm is revealed theoretically.

Key words: S-Box; Boolean function; nonlinearity; Walsh spectrum; Camellia algorithm