

具有K阶代数免疫的布尔函数

张毛优, 常祖领

(郑州大学 数学系, 河南 郑州 450001)

摘要:代数免疫度是衡量布尔函数抵抗代数攻击的重要性能指标, 具有低代数免疫度的布尔函数是不能抵抗代数攻击的。根据1型线性结构布尔函数的代数免疫阶完全取决于其零化子代数次数的结论, 文中从线性结构的角度构造了具有K代数免疫阶的布尔函数, 并且给出了此类函数循环谱特征、自相关特征及非线性度值。一系列的结论揭示了布尔函数的线性结构对其代数免疫阶的制约作用。并且通过特殊“分配”A和SVA中点的取值可重新调整循环谱值及自相关值。

关键词:代数免疫度; 循环谱; 非线性度

中图分类号: O153.2

文献标识码: A

文章编号: 1673-629X(2011)03-0158-03

Boolean Functions with K Algebraic Immune Degree

ZHANG Mao-you, CHANG Zu-ling

(College of Mathematics, Zhengzhou University, Zhengzhou 450001, China)

Abstract: Algebraic immunity is an important index to measure the ability to resist algebraic attack. If a Boolean function has a low algebraic immunity, it cannot resist the algebraic attack. According to the algebraic immune degree of a Boolean function with 1-form linear structure is completely determined by the lowest degree of the annihilator for f . From the perspective of linear structure, this paper is given Boolean functions with K algebraic immunity and the characters of walsh transform and the nonlinearity of the functions. A series of conclusions reveals a linear structure of Boolean function restricts algebraic immunity. Meanwhile, special allocation of points of Sand SVA which can be re-adjusted value of cyclic spectrum and autocorrelation values.

Key words: algebraic immunity; walsh transform; nonlinearity

0 引言

代数攻击首次应用于序列密码是在 Courtois 对 Toyocryp 的分析中。它的提出对流密码中所使用的布尔函数提出了更高的要求。为了衡量布尔函数抵抗代数攻击的能力, Meier 等提出了代数免疫阶 (Algebraic Immunity, 简记 AI) 的概念。并且 Courtois 和 Meier 等证明了一个 n 元布尔函数的代数免疫不大于 $\lfloor n/2 \rfloor$, 称达到这一上界的布尔函数为具有最优代数免疫阶^[1,2]的布尔函数。

1 相关概念

定义1 若 f 为 $F_2^n \rightarrow F_2$ 的映射, 那么称 f 为 n 元布尔函数。

定义2 若 $x \in F_2^n$, x 中 1 的个数称为 x 的重量, 记为 $w(x)$ 。

定义3^[3] 若 f 为 n 元布尔函数, x_1, x_2, \dots, x_i 是它的

某个单项式, 那么称它的次数为 d , f 的次数是它所有单项式中次数最大的。

定义4^[4,5] 若 $f \in B_n$ 是一个布尔函数, 称非 0 布尔函数 $g \in B_n$ 是 f 的一零化函数, 若有 $fg \equiv 0$ 成立。记 $An(f) = \{g \in B_n \mid fg \equiv 0\}$ 为 f 的所有零化函数组成的集合。

定义5^[6,7] 若 $f \in B_n$, f 的代数免疫度记作 $AI(f)$, 它是 f 的零化函数和 $f+1$ 的零化函数中代数次数最低的零化函数的次数, 即

$$AI(f) = \min \{ \deg(g) \mid g \in An(f) \text{ 或 } g \in An(f+1) \}。$$

定义6 若 $f \in B_n$, 称 $\text{mind}(f, l)$ 为 f 的非线性度, 记为 $nl(f)$, 其中 l 为所有的线性函数。

定义7^[8] 若 x 与 w 点积 $x \cdot w = \sum_{i=1}^n x_i w_i$, 其中 $x = (x_1, x_2, \dots, x_n)$, $w = (w_1, w_2, \dots, w_n)$, 则函数 f 在 u 处的 walsh 循环谱定义为: $S_{(f)}(w) = 2^{-n} \sum_{x \in F_2^n} (-1)^{f(x) + w \cdot x}$ 。

定义8^[9] 若对所有 $x \in F_2^n$ 都有 $f(x+s) + f(x) = 1$, 其中 $f(x)$, $x \in F_2^n$ 是一布尔函数, 则称 s 为 $f(x)$ 的 1 型线性结构。

收稿日期: 2010-06-25; 修回日期: 2010-09-18

作者简介: 张毛优 (1985-), 女, 硕士研究生, 研究方向为布尔函数、密码学; 常祖领, 博士后, 副教授, 硕士生导师, 研究方向为密码学、信息安全。

2 具有K阶代数免疫的平衡布尔函数

引理1^[10] 设 $f(x)$ 是 n 元布尔函数,如果有1型线性结构,则 $f(x)$ 零化子代数次数的最小值等于 $f(x)+1$ 零化子代数次数的最小值。于是 $f(x)$ 的代数免疫阶就等于 $f(x)$ 的所有零化子代数次数的最小值。

若 $f(x)$ 有1型线性结构,那么在求 $f(x)$ 的代数免疫阶时只须求得 $f(x)$ 零化子代数次数的最小值即可。无须再研究 $f(x)+1$ 的零化子的代数次数,由此可见,从抗代数攻击的角度而言,有线性结构也是密码函数的一个弱点。

定理1 令 $w(x)$ 表示二元向量表示中1的个数,则如下定义的 n 元布尔函数是代数次数不小于 k ,代数免疫阶等于 k 的平衡函数。

定义函数

$$f(x) = \begin{cases} 0 & w(x) < k \text{ 或 } x \in A \\ 1 & w(x) > n-k \text{ 或 } x \in S \setminus A \end{cases} \quad (1)$$

此处 $S = \{x; k \leq w(x) \leq n-k\}$, A 是 S 的子集,使得 $|A| = 1/2(C_n^k + C_n^{k+1} + \dots + C_n^{n-k})$ 且 $S \setminus A = \{1+a, a \in A\}$,其中 A 中每个向量前 k 分量中至多 $k-1$ 个0, $|A|$ 表示集合 A 中的元素个数, $1 = (1, 1, \dots, 1) \in F_2^n$ 。

证明:由组合知识得, $\sum_{i=0}^{k-1} C_n^i = \sum_{i=n-k+1}^n C_n^i$,并且有假设知道, $|A| = |S \setminus A|$,所以式(1)中的函数是平衡函数。

设 $a = (a_1, a_2, \dots, a_n)$,以下以 a_i^c 记 $a_i + 1$

$$f(x) = \sum_{w(a) > n-k} (x_1 + a_1)^c \dots (x_n + a_n)^c + \sum_{\substack{k \leq w(a) \leq n-k \\ f(a)=1}} (x_1 + a_1)^c \dots (x_n + a_n)^c$$

我们知道若 $a_i = 1$,则 $x_i + a_i + 1 = x_i$,并且在和式的前一项中等于1的 $a_i = 1$ 的个数都大于 $n-k$,所以其展开式中单项式的次数都大于 k ,后一项展开式中单项式的次数都不小于 k ,所以 $f(x)$ 的ANF中各单项式的代数次数都不小于 k 。

先来说明 $f+1$ 的零化子的代数次数不小于 k 。假设 $f+1$ 的次数至多为 $k-1$ 的零化子为

$$g = a_0 + \sum_{i=1}^n a_i x_i + \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j + \dots + \sum_{1 \leq i_1 < \dots < i_{k-1} \leq n} a_{i_1 i_2 \dots i_{k-1}} x_{i_1} \dots x_{i_{k-1}},$$

而对 $w(x) < k$,由于 $f+1=1$,因此 $g(x)=0$ 。

当 $w(x)=0$,即 $x=(0,0,\dots,0)$,有 $g(0,0,\dots,0)=0$,则 $a_0=0$;

当 $w(x)=1$,有 $g(1,0,\dots,0)=g(0,1,\dots,0)=g(0,0,\dots,1)=0$ 则 $a_i=0$;同理有 $a_{ij}=0, \dots, a_{i_1 \dots i_{k-1}}=0$,则 $g=0$ 。

故 $An(f+1)$ 的次数不小于 k 。对于任意自然数 $n, 1$ 都是 $f(x)$ 的1型线性结构,利用引理1得 $An(f+1)$ 的代数次数的最小值等于 $An(f)$ 的代数次数的最

小值。所以 $f(x)$ 的代数免疫阶等于 $f(x)+1$ 所有零化子的代数次数的最小值。因此, $AI(f) \geq k$ 。而可以验证 $g = (x_1+1)(x_2+1)\dots(x_k+1)$ 是 f 的零化子。这样 $AI(f)=k$ 。

证毕。

例1 设 $n=4, k=2, S = \{x \in F_2^4 \mid w(x)=2\}$, A 满足定理1要求 $|A|=1/2 C_4^2, A = \{(1,0,1,0), (1,1,0,0), (1,0,0,1)\}$

$$\text{令 } f(x) = \begin{cases} 0 & w(x) < 2 \text{ 或 } x \in S \setminus A \\ 1 & w(x) > 2 \text{ 或 } x \in A \end{cases}$$

则 $f(x)$ 的代数标准型为 $f(x) = x_1 x_3 + x_1 x_2 + x_1 x_4 + \sigma_{4,3}$,其中 $\sigma_{4,3}$ 表示所有4元3次单项式的和。

例2 设 $n=5, k=2, S = \{x \in F_2^5; 2 \leq w(x) \leq 3\}$, A 仍满足定理1,所以 $|A|=1/2(C_5^2 + C_5^3), A = \{(11000), (10100), (10010), (10001), (11100), (10101), (10110), (10011), (11001), (11010)\}$, 令

$$f(x) = \begin{cases} 0 & w(x) < 2 \text{ 或 } x \in S \setminus A \\ 1 & w(x) > 3 \text{ 或 } x \in A \end{cases}$$

则 $f(x)$ 的代数标准型为 $f(x) = x_1 x_2 + x_1 x_3 + x_1 x_4 + x_1 x_5 + x_1 x_2 x_3 + x_1 x_3 x_5 + x_1 x_3 x_4 + x_1 x_4 x_5 + x_1 x_2 x_5 + x_1 x_2 x_4 + \sigma_{5,4}$,其中 $\sigma_{5,4}$ 表示所有5元4次单项式的和。

循环谱和自相关是刻画函数密码学性质的两个重要指标,下面来研究定理1中的函数的循环谱和自相关函数的取值特点。

定理2 对任意的 $x \in F_2^n$,定理1中所构造 $f(x)$ 的循环谱都满足

$$S_{(f)}(w) = 1/2^{n-1} \begin{cases} 0 & E \\ \sum_{x \in A \text{ 或 } w(x) < k} (-1)^{w \cdot x} & O \end{cases}$$

其中 O 表示事件“ w 的Hamming重量是奇数”, E 表示事件“ w 的Hamming重量是偶数”。

对于任意 $x \in F_2^n$,定理1中所构造的自相关函数都满足 $r_f(1+s) = r_f(s)$

证明:由定理1中所定义的函数都满足 $f(x+1) = f(x)+1$ 及式(1)得

$$\begin{aligned} S_{(f)}(w) &= 1/2^n \sum_{x \in F_2^n} (-1)^{f(x)+w \cdot x} = 1/2^n \left[\sum_{w(x) < k} (-1)^{w \cdot x} + \sum_{x \in A} (-1)^{w \cdot x} - \sum_{w(x) > n-k} (-1)^{w \cdot x} - \sum_{x \in S \setminus A} (-1)^{w \cdot x} \right] \\ &= 1/2^n \left[\sum_{x \in A} (-1)^{w \cdot x} - \sum_{x \in A} (-1)^{w \cdot (x+1)} + \sum_{w(x) < k} (-1)^{w \cdot x} - \sum_{w(x) < k} (-1)^{w \cdot (x+1)} \right] \\ &= 1/2^n \left[\sum_{x \in A} (-1)^{w \cdot x} - \sum_{x \in A} (-1)^{w \cdot x + w} + \sum_{w(x) < k} (-1)^{w \cdot x} - \sum_{w(x) < k} (-1)^{w \cdot x + w} \right] \end{aligned}$$

$$\text{故, } S_{(f)}(w) = 1/2^{n-1} \begin{cases} 0 & E \\ \sum_{x \in A \text{ 或 } w(x) < k} (-1)^{w \cdot x} & O \end{cases}$$

下面来考察定理1中所构造 $f(x)$ 的自相关特点:

$$\begin{aligned}
 r_f(1+s) &= 1/2^n \sum_{x \in F_2^n} (-1)^{f(x)+f(x+1+s)} \\
 &= 1/2^n \sum_{x \in F_2^n} (-1)^{f(x)+f(x+s)+1} \\
 &= -r_f(s)
 \end{aligned}$$

要抵抗代数攻击,布尔函数的代数免疫度就必须高,但是代数免疫度高了,其非线性度会不会减少。如果减少了,就会遭受到线性攻击。所以研究非线性度和代数免疫度之间的关系是一个十分重要的任务。

引理 2^[11,12] 若 f 为 F_2^n 上的布尔函数,其代数免疫度 $AI(f) = k$ 则 $nl(f) \geq 2 \sum_{i=0}^{k-2} \binom{n-1}{i}$ 。且这个下界为紧的。

函数的非线性度和循环谱之间有关系:

$$nl(f) = 2^{n-1} (1 - \max_u |S_{\cap}(u)|) \quad (2)$$

下面具体讨论定理 1 中所构造平衡函数的非线性度的取值特点:

推论:对任意 $x \in F_2^n$, 定理 1 中所构造 $f(x)$ 的非线性度为:

$$nl(f) = 2^{n-1} - \max_u \left| \sum_{x \in A \text{ 或 } w(x) < k} (-1)^{u \cdot x} \right|, \text{ 其中 } u \text{ 的重量为奇数。}$$

3 结束语

研究了一类具有 k 阶代数免疫的平衡函数,给出了此类函数循环谱特征、自相关特征及非线性度特征。并且根据其特点,可以通过特殊“分配” A 和 $S \setminus A$ 中点的取值来调整循环谱,自相关的值,使得密码函数的性能得到最大的发挥。

参考文献:

- [1] Carlet C. A method of construction of balanced functions with

optimum algebraic immunity [EB/OL]. 2006. <http://eprint.iacr.org/2006/149>.

- [2] Dalai D K, Maitra S, Sarkar S. Basic theory in construction of Boolean functions with maximum possible annihilator immunity [C]//In: Des Codes Crypt (2006). [s. l.]: [s. n.], 2006:41-58.
- [3] Mac Williams F J, Sloane N J A. The Theory of Error-Correcting Codes [M]. North-Holland; Elsevier, 1977.
- [4] 徐春霞, 陈卫红. 求布尔函数零化子的一种算法及一类代数攻击不变量 [J]. 电子与信息学报, 2007, 29(4): 66-73.
- [5] 杨 洋. 广义布尔函数的代数免疫与零化子 [J]. 湖北大学学报, 2008, 30(4): 329-332.
- [6] Meier W, Pasalic E, Carlet C. Algebraic Attacks and Decomposition of Boolean Functions [C]//Proc. of EUROCRYPT'04. Interlaken, Switzerland; Springer, 2004: 474-491.
- [7] 王永娟, 范淑琴, 冀慧芳, 等. 正规性和代数免疫 [J]. 解放军理工大学学报, 2009, 10(4): 329-333.
- [8] 冯登国. 密码学分析 [M]. 北京: 清华大学出版社, 2000.
- [9] 温巧燕, 钮心忻, 杨义先. 密码学中的布尔函数 [M]. 北京: 科学出版社, 2000.
- [10] Dalai D K, Gupta K C, Maitra S. Results on Algebraic Immunity for Cryptographically Significant Boolean Functions [C]//Proc. of INDOCRYPT'04. Chennai, India; Springer, 2004: 92-106.
- [11] Dalai D K, Gupta K C, Maitra S. Cryptographically significant Boolean functions: construction and analysis in terms of algebraic immunity [C]//In: Fast Software Encryption, FSE 2005: number 3557, Lecture Notes in Computer Science. [s. l.]: Springer-Verlag, 2005: 98-111.
- [12] Courtois N, Meier W. Algebraic attacks on stream ciphers with linear feedback [C]//In Advances in Cryptology-EUROCRYPT 2003, number 2656 in Lecture Notes in Computer Science. [s. l.]: Springer-Verlag, 2003: 345-359.

(上接第 157 页)

参考文献:

- [1] 成际镇, 林晓勇. 计算机电信集成技术及应用 [M]. 北京: 人民邮电出版社, 2008: 17-20.
- [2] ITU-T. Recommendation H. 323, Packet-based multimedia communication system [S]. Switzerland: [s. n.], 1998.
- [3] Handley M, Schulzrinne H, Schooler E, et al. SIP: session initiation protocol [S]. RFC2543. IETF, 1999.
- [4] Handley M, Jacobson V. SDP: session description protocol [S]. RFC2327. IETF, 1998.
- [5] 张永强, 张捍东, 赵金宝. SIP 协议栈研究 [J]. 计算机技术与发展, 2007, 17(11): 49-50.
- [6] Rosenberg J. SIP: Session Initiation Protocol [S]. RFC3261. IETF, 2002.
- [7] 信息产业部电信研究院. YD/T 1046/2000. H. 323 和 SIP 的互通技术规范 [S]. 2000.
- [8] Singh K, Schulzrinne H. Interworking between SIP/SDP and H. 323 [S]. IETF, 2000.
- [9] IETF. Draft-agrawal-SIP-H. 323-interworking-01. txt [EB/OL]. 2001-07. <http://www.ietf.com>.
- [10] IETF. Draft-agrawal-SIP-H. 323-interworking-reqs-06. txt [EB/OL]. 2004-02. <http://www.ietf.com>.
- [11] Wang Ligang, Agarwal, Anjali, et al. Modelling and verification of interworking between SIP and H. 323 [J]. Computer Networks, 2004, 45(2): 363-369.
- [12] 张越峰, 唐学文, 张志军. IPv4 与 IPv6 混合网络中的 SIP 电话通信的研究 [J]. 计算机技术与发展, 2007, 17(5): 83-86.