ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.21, No.12, December 2010, pp.3165−3174
doi: 10.3724/SP.J.1001.2010.03671

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

几类旋转对称布尔函数的密码学性质*

孙光洪[1+], 武传坤[2]

[1](河海大学 理学院,江苏 南京 210098)

[2](中国科学院 软件研究所 信息安全国家重点实验室,北京 100190)

Cryptographic Properties of Several Classes of Rotation Symmetric Boolean Functions

SUN Guang-Hong[1+], WU Chuan-Kun[2]

[1](College of Sciences, Hohai University, Nanjing 210098, China)

[2](State Key Laboratory of Information Security, Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)

+ Corresponding author: E-mail: sgh1976@gmail.com

Sun GH, Wu CK. Cryptographic properties of several classes of rotation symmetric Boolean functions. *Journal of Software*, 2010,21(12):3165−3174. http://www.jos.org.cn/1000-9825/3671.htm

Abstract: Sumanta Sarkar, *et al*. give a class of rotation symmetric Boolean functions with maximum algebraic immunity, but only consider the nonlinearity of the functions and did not study other cryptographic properties. In this paper, other cryptographic properties of the class of Boolean functions are studied, such as, algebraic degree, linear structure, propagation, correlation immunity etc. The results, unfortunately, show that their other cryptographic properties are not good even though their algebraic immunity is optimum. Hence, the class of Boolean functions cannot be applied in cryptography.

Key words: Boolean function; symmetric Boolean function; rotation symmetric Boolean function; algebraic immunity; algebraic degree

摘 要: Sumanta Sarkar 等人给出了一类具有最大代数免疫阶的旋转对称布尔函数,但对给出的旋转对称布尔函数仅研究了该函数的非线性度而对其他密码学性质未加以研究.因此,研究了上面给出的旋转对称布尔函数的其他密码学性质:代数次数、线性结构、扩散性、相关免疫性等.研究结果显示,虽然这类布尔函数的代数免疫阶达到最大,但是其他的密码学性质并不好.因此,此类布尔函数并不能直接应用在密码系统中.

关键词: 布尔函数;对称布尔函数;旋转对称布尔函数;代数免疫阶;代数次数

中图法分类号: TN918 **文献标识码**: A

布尔函数在流密码的组合模型和滤波模型中有着重要的应用,但是这些函数必须满足一些条件才能用到实际的密码系统中,这些条件包括平衡性、高的代数次数、高的非线性度、相关免疫性、扩散性等.

近来,在对流密码和分组密码安全性分析方面,代数攻击受到很大的关注[1−11].它的本质是通过解超定的多

* Supported by the National Natural Science Foundation of China under Grant No.60673068 (国家自然科学基金); the Fundamental Research Funds for the Central Universities of China under Grant No.2009B27414 (中央高校基本科研业务费专项资金); the Natural Science Foundation of Hohai University of China under Grant No.2084/409270 (河海大学自然科学基金)

Received 2009-02-17; Revised 2009-04-27; Accepted 2009-07-07

元方程组来恢复秘密密钥,这种攻击方法近年来受到很多重视.对于n元布尔函数f,代数攻击的核心是发现f和$1+f$的次数最低的非零的零化子g,即使得$f\cdot g=0$和$(1+f)\cdot g=0$.为了实现代数攻击,我们需要有代数次数低的零化子.相反地,为了在密码系统中避免代数攻击,一个必要条件是必须要求构造的密码系统所对应的布尔函数(向量布尔函数)的代数免疫阶比较大,最好达到最大.但由文献[7,12]得知,n 元布尔函数的最大代数免疫阶为$\left\lceil \frac{n}{2} \right\rceil$.因此,如何构造布尔函数使其代数免疫阶达到最大是在代数攻击中的一个感兴趣的问题,吸引了众多研究者的注意[13−16].

但是到目前,对能够抗击代数攻击的布尔函数的研究并没有取得满意的结果.由于两个代数免疫阶相差为1的布尔函数在抗击代数攻击时的效果相差非常大,所以构造具有最大代数免疫阶的布尔函数就是一个重要的研究问题.目前,构造布尔函数使其达到最大代数免疫阶的文献并不多见,详细见文献[13–18].由于现在对密码系统的攻击除了代数攻击外还有很多其他的攻击方法,例如差分攻击、线性攻击、相关攻击等,因此构造的布尔函数除了要满足最大的代数免疫阶之外还必须满足其他密码学性质,例如低的差分均匀性、高的非线性度、具有相关免疫性等,只有满足了多个密码学性质的布尔函数才能应用到实际的密码系统中.

由于旋转对称布尔函数表示方法简单和具有一些有趣的密码学性质,因此受到很多研究者的关注[13,19−25].旋转对称布尔函数是否可以用到密码系统中,即它们的密码学性质如何,前面所述参考文献中对旋转对称布尔函数的一些密码学性质进行了研究,尤其是文献[13]构造了旋转对称布尔函数,使其代数免疫阶达到最大并且研究了这类旋转对称布尔函数抗击线性攻击的能力,即它们的非线性度.显然,在密码分析中除了代数攻击和线性攻击之外还存在很多的密码分析方法.因此,它们抗击其他密码攻击能力如何,即这类旋转对称布尔函数其他密码学性质是否也较好?这对密码学应用来说至关重要.因此,研究这类旋转对称布尔函数的其他密码学性质是一个非常有趣的问题.以此看出,是否可以在实际的密码系统中应用上面的旋转对称布尔函数,正是本文要研究的问题.

本文主要研究了文献[13]中所给的达到最大代数免疫阶的旋转对称布尔函数$R_n(X)$的代数次数、线性结构、扩散性、相关免疫性等,另外还研究了一类与文献[13]中的旋转对称布尔函数紧密相关的一类旋转对称布尔函数$R(X)$的密码学性质,包括代数免疫阶、代数次数、线性结构、扩散性、相关免疫阶等.我们的结果显示,虽然上面的旋转对称布尔函数$R_n(X)$有最优的代数免疫阶,但是其他密码学性质并不好;同样,虽然$R(X)$具有一阶相关免疫性,但是这类旋转对称布尔函数的代数免疫阶等密码学性质又不好.因此,它们都不能直接应用到密码系统中.

本文首先给出布尔函数、对称布尔函数和旋转对称布尔函数的一些基础知识,同时也给出对称布尔函数、旋转对称布尔函数的一些性质.第 2 节处理本文需要解决的问题,研究两类旋转对称布尔函数的密码学性质:代数次数、代数免疫阶、相关免疫性等.第 3 节是结束语.

1 预备知识

设F_2是一个二元域,F_2^n为F_2上的n维向量空间,从F_2^n到F_2上的函数称为布尔函数,B_n表示从F_2^n到F_2上的全体布尔函数集.布尔函数$f(x_1,x_2,\ldots,x_n)$最基本的表示方法是通过长为2^n的真值表表示:

$$f=[f(0,0,\ldots,0),f(1,0,\ldots,0),f(0,1,\ldots,0),f(1,1,\ldots,0),f(1,1,\ldots,1)].$$

在长为 2^n的二元串中,1 的个数称为布尔函数f的重量,记为$wt(f)$.集合 $\sup p(f)=\{x\in F_2^n \mid f(x)=1\}$ 称为布尔函数f的支撑集.两个n元布尔函数f,g的距离为布尔函数$f+g$真值表中 1 的个数,即是布尔函数$f+g$的重量,其中,+是F_2上的加.如果n元布尔函数f的重量为2^{n-1},称函数f是平衡的.

由于布尔函数的真值表表示方法不能很好地研究布尔函数的代数性质,所以我们需要布尔函数的其他表示方法.布尔函数f的另一种表示方法是多元多项式表示,即:每一个n元布尔函数f都可以唯一地表示为F_2上的多元多项式,即

$$f(x_1,x_2,...,x_n)=a_0+\sum_{1\leqslant i\leqslant n}a_ix_i+\sum_{1\leqslant i<j\leqslant n}a_{ij}x_ix_j+...+a_{12...n}x_1x_2...x_n,$$

其中,系数$a_0,a_i,a_{ij},\ldots,a_{12\ldots n}\in\{0,1\}$,+为$F_2$上的加法,称为布尔函数$f$的代数正规型.函数$f$的代数次数$\deg(f)$为系数不等于 0 时最大的变量个数.在代数正规型中,当$\deg(f)\leqslant 1$ 时称为仿射布尔函数;全体仿射布尔函数用A_n表示.在仿射布尔函数中,当常数项为 0 时,称为线性布尔函数.

设n元布尔函数f在$(x_1,x_2,\ldots,x_n)=(c_{i1},c_{i2},...,c_{in})\in F_2^n, i=1,2,...,k$ 时取值为 1,否则取值为 0,则函数f可以写为

$$f(x_1,x_2,\ldots,x_n)=(x_1+c_{11}+1)(x_2+c_{12}+1)\ldots(x_n+c_{1n}+1)+(x_1+c_{21}+1)(x_2+c_{22}+1)\ldots(x_n+c_{2n}+1)+\ldots+$$
$$(x_1+c_{k1}+1)(x_2+c_{k2}+1)\ldots(x_n+c_{kn}+1),$$

即

$$f(x_1,x_2,...,x_n)=\sum_{(c_1,c_2,...,c_n)\in F_2^n}f(c_1,c_2,...,c_n)x_1^{c_1}x_2^{c_2}...x_n^{c_n},$$

其中,$x_i^1=x_i,x_i^0=x_i+1$,称为布尔函数 f 的小项表示.在研究布尔函数 f 的代数次数时,有时利用它的小项表示比较简单.

给定一个布尔函数 $f:F_2^n\to F_2$,函数

$$a\to W_f(a)=\sum_{x\in F_2^n}(-1)^{f(x)+a\cdot x},a\in F_2^n$$

称为布尔函数f的Walsh变换,其中,$a\cdot x=a_1x_1+a_2x_2+\ldots+a_nx_n,a=(a_1,a_2,\ldots,a_n),x=(x_1,x_2,\ldots,x_n)$.函数值$w_f(a)$称为函数$f$的Walsh系数,也称为函数$f$的Walsh谱.

n 元布尔函数的非线性度为 f 到所有仿射布尔函数的最小距离,即 $nl(f)=\min_{g\in A_n}(d(f,g))$.

容易验证,Walsh 谱和非线性度之间有关系 $nl(f)=2^{n-1}-\frac{1}{2}\max_{a\in F_2^n}|W_f(a)|$.由 Parseval 等式 $\sum_{a\in F_2^n}W_f^2(a)=2^{2n}$,我们能够得到 $nl(f)\leqslant 2^{n-1}-2^{\frac{n}{2}-1}$.使得等式成立的布尔函数称为 bent 函数.可以容易地看出,bent 函数只可能在 n 是偶数时存在,并且,bent 函数是取得最大非线性度的函数.

如果对任意满足 $1\leqslant wt(a)\leqslant k$的$a$都有$w_f(a)=0$,称布尔函数$f$满足$k$阶相关免疫性.平衡的$k$阶相关免疫布尔函数称为$k$阶弹性函数.

称 $\Delta_f(w)=\sum_{x\in F_2^n}(-1)^{f(x)+f(x+w)}$ 为布尔函数 f 的自相关函数,$\{\Delta_f(w)\mid w\in F_2^n\}$为布尔函数 f 的自相关谱.如果对于任意满足 $1\leqslant wt(w)\leqslant k$的$w$都有$\Delta_f(w)=0$,则称布尔函数$f$满足$k$次扩散性准则.如果$k=1$,则称布尔函数$f$满足严格雪崩准则.

设 f 是 F_2^n 上的布尔函数,如果对任意的 $x\in F_2^n$ 都有 $f(x)+f(x+a)$是常数,称 $a\in F_2^n$ 是布尔函数 f 的线性结构.在构造密码函数时,线性结构是密码性质的一个弱性质[26,27],因此要求应用在密码系统中的布尔函数不具有线性结构.

对于布尔函数f,如果存在非零的$g\in B_n$使得$f\cdot g=0$,称g为布尔函数f的零化子,称$AN(f)=\{g\in B_n\mid f\cdot g=0,g\neq 0\}$为$f$的零化子集.称$f$和$f+1$ 的零化子的最小代数次数为f的代数免疫阶或者代数免疫度,记为$AI_n(f)$.避免代数攻击的一个必要条件是要求所给的布尔函数的代数免疫阶越高越好,但由文献[7,12]我们知道,对任意布尔函数$f\in B_n$有 $AI_n(f)\leqslant\left\lceil\frac{n}{2}\right\rceil$,$\lceil x\rceil$表示不小于$x$的最小整数.

一个布尔函数f称为对称布尔函数,如果当输入$(x_1,x_2,\ldots,x_n)$的重量相同时,布尔函数f的输出$f(x_1,x_2,\ldots,x_n)$的取值也相同.从而可以将n变量的布尔函数f简化为$n+1$ 比特串re_f的形式,即当$wt(x_1,x_2,\ldots,x_n)=i$时,$ra_f(i)=f(x_1,x_2,\ldots,x_n)$.明显地,在布尔函数的代数正规型中,对称布尔函数或者含所有相同次数的单项式或者都不含,从而又可以将n元对称布尔函数的代数正规型简化为$n+1$ 比特串ra_f的形式,即当所有次数为i的单项式都出现时,$ra_f(i)=1$,否则,$ra_f(i)=0$.故对称布尔函数f的re_f,ra_f都是$\{0,1,\ldots,n\}$到$\{0,1\}$的映射.对称布尔函数比较早的研究见

文献[28−30].

在文献[15]中,Dalai 等人引入了奇数个变元 n 的对称布尔函数:

$$G_n(x_1,x_2,...,x_n)=\begin{cases}1, & wt(x_1,x_2,...,x_n)\leqslant\dfrac{n-1}{2}\\ 0, & wt(x_1,x_2,...,x_n)\geqslant\dfrac{n+1}{2}\end{cases},$$

并且研究了这类对称布尔函数的代数免疫阶达到最大为 $\frac{n+1}{2}$,非线性度为 $2^{n-1}-\binom{n-1}{\frac{n-1}{2}}$,代数次数为 $2^{\lfloor\log_2 n\rfloor}$.

设 $x_i\in F_2$,$1\leqslant i\leqslant n$.对 $1\leqslant k\leqslant n$,定义

$$\rho_n^k(x_1,x_2,...,x_{n-1},x_n)=(x_{1+k},x_{2+k},...,x_{n-1+k},x_{n+k}),$$

其中,$k+i(1\leqslant i\leqslant n)$取 mod n,只有当 $k+i\equiv 0 \bmod n$ 时取 n.如果对每一个 $(x_1,x_2,...,x_{n-1},x_n)\in F_2^n$,$1\leqslant k\leqslant n$,都有

$$f(\rho_n^k(x_1,x_2,...,x_{n-1},x_n))=f(x_1,x_2,...,x_{n-1},x_n),$$

则称布尔函数 f 为旋转对称布尔函数[13,19,20,23,24].设 $x=(x_1,x_2,\ldots,x_n)$,记 $O_x=\{\rho_n^i(x_1,x_2,...,x_n)\,|\,1\leqslant i\leqslant n\}$,称为含元 $x=(x_1,x_2,\ldots,x_n)$ 的轨道.旋转对称布尔函数的其他性质见文献[19,20].

在文献[13],Sarkar 等人构造了旋转对称布尔函数:

(1) 取大于等于 5 的奇数 n;

(2) 在 F_2^n 中取重量为 $\frac{n-1}{2}$ 的元 x,由 x 生成轨道 O_x;

(3) 在 F_2^n 中取重量为 $\frac{n+1}{2}$ 的元 y,并由 y 生成轨道 O_y,使得对任意的 $x'\in O_x$ 存在唯一的 $y'\in O_y$,有 $WS(x')\subset WS(y')$,其中,$WS((x_1,x_2,\ldots,x_n))=\{i\,|\,x_i=1,1\leqslant i\leqslant n\}$;

(4) 构造旋转对称布尔函数

$$R_n(X)=\begin{cases}G_n(X)+1, & X\in O_x\cup O_y\\ G_n(X), & \text{否则}\end{cases},$$

并且研究了旋转对称布尔函数 $R_n(X)$ 的代数免疫阶达到最大为 $\frac{n+1}{2}$,非线性度为 $2^{n-1}-\binom{n-1}{\frac{n-1}{2}}+2$.但是文中并没有研究此函数的其他密码学性质,因此研究旋转对称布尔函数 $R_n(X)$ 的其他密码学性质是一个感兴趣的问题.

注 1:上面限制 $n\geqslant 5$ 的主要原因是当 $n\leqslant 3$ 时所有的旋转对称布尔函数都是对称布尔函数.

利用上面的 O_x,O_y,我们构造下面的旋转对称布尔函数:

$$R(X)=\begin{cases}1, & X\in O_x\cup O_y\\ 0, & \text{否则}\end{cases}.$$

容易看出,$R_n(X)=G_n(X)+R(X)$,因此它们之间的密码学性质应该存在某种联系.我们知道,旋转对称布尔函数 $R_n(X)$ 和对称布尔函数 $G_n(X)$ 的代数免疫阶都达到最大.那么旋转对称布尔函数 $R(X)$ 的代数免疫阶是否也达到最大;以及 $R(X)$ 和 $R_n(X)$ 的其他密码学性质如何是下一节我们要讨论的问题.

若无特别说明,O_x,O_y 都是Sarkar等人构造的旋转对称布尔函数中的 O_x 和 O_y.

2 两类旋转对称布尔函数的密码学性质

本节主要讨论上面两类旋转对称布尔函数的密码学性质,包括代数次数、相关免疫性、平衡性等.如无特别说明,我们总是假设 n 是奇数.

为了后面应用方便,我们先给出下面两个引理:

引理 1[13]. 设n是奇数,O_u是由$u=(u_1,u_2,\ldots,u_n)$生成的轨道,如果 $wt(u)=\frac{n-1}{2}$,则$|O_u|=n$;如果 $wt(u)=\frac{n+1}{2}$,则$|O_u|=n$.

引理 2[31]. 设f是 F_2^n 上代数次数为k的布尔函数,且相关免疫阶为m,则k,m,n三者之间有关系:$k+m\leqslant n$.

由于对称布尔函数$G_n(X)$是平衡的,而由引理 1 知,在$R_n(X)$构造中的O_x,O_y有$|O_x|=|O_y|=n$,故旋转对称布尔函数$R_n(X)$是平衡的.但对于旋转对称布尔函数$R(X)$,显然$|\mathrm{supp}(R)|=2n$,因此要使$R(X)$平衡的充要条件是 $2n=2^{n-1}$.但是当$n\geqslant 5$ 时上面等式不可能成立,因此$R(X)$不平衡.

2.1 代数次数

由于$R_n(X)=G_n(X)+R(X)$,而我们已经知道$G_n(X)$的代数次数为 $2^{\lfloor \log_2 n\rfloor}$,因此要讨论$R_n(X)$的代数次数,只要讨论$R(X)$的代数次数并与$G_n(X)$的代数次数比较,就可以得到$R_n(X)$的代数次数.

定理 1. 旋转对称布尔函数 $R(X)$的代数次数为 $n-1$.

证明:利用布尔函数的小项表示来验证旋转对称布尔函数 $R(X)$的代数次数为 $n-1$.

由于在旋转对称布尔函数$R(X)$的小项表示中,每个项的展开式中都含$x_1x_2\ldots x_n$,又由于$|O_x|=|O_y|=n$且$R(X)=1$的充要条件是$X\in O_x\cup O_y$,故在小项表示中共有 $2n$个项,因此在$R(X)$的代数正规型中不含$x_1x_2\ldots x_n$.因此,如果我们可以验证$x_1x_2\ldots x_{n-2}x_{n-1}$在旋转对称布尔函数$R(X)$的代数正规型中必出现,则我们可得函数$R(X)$的代数次数为$n-1$.

事实上,在布尔函数小项表示的单个项的展开式中要出现$x_1x_2\ldots x_{n-2}x_{n-1}$的充要条件是:$R(X)$只能在形如$(x_1,x_2,\ldots,x_{n-1},x_n)=(x_1,x_2,\ldots,x_{n-1},0)$的元上取值为 1.由于在$O_x$中有$n$个元,而在$O_x$中$x_n$为 0 的元的个数为 $n-\frac{n-1}{2}=\frac{n+1}{2}$.同样地,在$O_y$中有$n$个元,而在$O_y$中$x_n$为 0 的元的个数为 $n-\frac{n+1}{2}=\frac{n-1}{2}$.故$x_1x_2\ldots x_{n-2}x_{n-1}$在函数$R(X)$的小项展开式中出现 $\frac{n+1}{2}+\frac{n-1}{2}=n$ 次.由于n是奇数,因此在旋转对称布尔函数$R(X)$的代数正规型中$x_1x_2\ldots x_{n-2}x_{n-1}$必出现,即$R(X)$的代数次数为$n-1$.定理得证. □

注 2:利用上面证明$x_1x_2\ldots x_{n-2}x_{n-1}$必出现的方法,实际上可以证明所有的$n-1$ 次单项式在旋转对称布尔函数$R(X)$的代数正规型中都出现.

定理 2. 旋转对称布尔函数$R_n(X)$的代数次数为:

(1) 当$n=2^{k-1}+1$ 时,$\deg(R_n(X))\leqslant n-2$;

(2) 当 $2^{k-1}+2\leqslant n<2^k-1$ 且n为奇数时,$\deg(R_n(X))=n-1$.

证明:由文献[15]可知, $\deg(G_n(X))=2^{\lfloor \log_2 n\rfloor}$,因此:

(1) 当$n=2^{k-1}+1$ 时,$\deg(G_n(X))=2^{k-1}=n-1$,而$\deg(R(X))=n-1$.由注 2 得知,在旋转对称布尔函数$R(X)$的代数正规型中,所有的$n-1$ 次单项式都出现,而由于$G_n(X)$是对称布尔函数,故在$G_n(X)$的代数正规型中所有的$n-1$ 次单项式也都出现,从而$\deg(R_n(X))=\deg(G_n(X)+R(X))\leqslant n-2$;

(2) 当 $2^{k-1}+2\leqslant n<2^k-1$ 且n为奇数时,$\deg(G_n(X))=2^{k-1}$,而$\deg(R(X))=n-1>2^{k-1}$,故

$$\deg(R_n(X))=\deg(G_n(X)+R(X))=\deg(R(X))=n-1.$$

故定理得证. □

2.2 线性结构

定理 3. 旋转对称布尔函数 $R(X)$无非零的线性结构.

证明:首先证明对任意非零 $a=(a_1,a_2,\ldots,a_n)\in F_2^n$,如果 $a\neq 1$,则 a 不是 $R(X)$的线性结构.事实上,在 $R(X)$的代数正规型表示中,次数为 $n-1$ 的所有单项式都出现,因此我们可以设 $R(X)$的代数正规型为

$$R(X)=\sum_{1\leqslant i_1<i_2<\ldots<i_{n-1}\leqslant n} X_{i_1}X_{i_2}\ldots X_{i_{n-1}}+H(X),$$

其中,$H(X)$是代数次数小于 $n-1$ 的函数.所以我们有

$$R(X)+R(X+a)=\sum_{1\leqslant i_1<i_2<\ldots<i_{n-1}\leqslant n}X_{i_1}X_{i_2}\ldots X_{i_{n-1}}+H(X)+\sum_{1\leqslant i_1<i_2<\ldots<i_{n-1}\leqslant n}(X_{i_1}+a_{i_1})(X_{i_2}+a_{i_2})\ldots(X_{i_{n-1}}+a_{i_{n-1}})+H(X+a)$$

$$=\sum_{1\leqslant i_1<i_2<\ldots<i_{n-1}\leqslant n}\sum_{j=1}^{n-1}X_{i_1}X_{i_2}\ldots X_{i_{j-1}}a_{i_j}X_{i_{j+1}}\ldots X_{i_{n-1}}+H'(X)$$

$$=\sum_{1\leqslant i_1<i_2<\ldots<i_{n-1}\leqslant n}(a_{i_1}+a_{i_2})X_{i_3}\ldots X_{i_{n-1}}+H''(X),$$

其中,$H'(X)$是代数次数小于 $n-2$ 的函数,$H''(X)$是代数次数小于 $n-3$ 的函数.因此,要使得 $R(X)+R(X+a)$为常数,首先必须要求

$$\sum_{1\leqslant i_1<i_2<\ldots<i_{n-1}\leqslant n}(a_{i_1}+a_{i_2})X_{i_3}\ldots X_{i_{n-1}}\equiv 0.$$

因此,对任意$i,j\in\{1,2,\ldots,n\}$都有$a_i=a_j$.由于$a\neq 0$,故$a=1$.因此,上面的断言得证.此断言说明,如果旋转对称布尔函数存在非零线性结构,则非零线性结构只可能为 1.下面我们证明 1 不是函数$R(X)$的线性结构.为此,只需要计算 $R(X)+R(X+1)$是否对任意 $X\in F_2^n$ 都是常数.分下面两种情形考虑:

情形 1. 如果$X\in O_x\cup O_y$,由O_x,O_y的定义,显然$X+1\notin O_x\cup O_y$,因此$R(X)+R(X+1)=1+0=1$.

情形 2. 如果$X\notin O_x\cup O_y$,则显然存在 $X\in F_2^n$ 使得$X+1\notin O_x\cup O_y$(如取X重量为 1),因此$R(X)+R(X+1)=0+0=0$.

由情形 1 和情形 2 可得,1 不是旋转对称布尔函数 $R(X)$的线性结构,因此结论得证. □

利用定理 3 相同的证明方法,得到下面定理:

定理 4. 旋转对称布尔函数$R_n(X)$无非零的线性结构,其中,$2^{k-1}+2\leqslant n<2^k-1$ 且n为奇数.

2.3 扩散性

定理 5. 旋转对称布尔函数$R(X)$和$R_n(X)$在$n\geqslant 7$ 时都不满足扩散性.

证明:事实上,如果我们可以证明存在重量为 1 的元 $w\in F_2^n$ 使得$\Delta_f(w)\neq 0$($f=R$或者$f=R_n$),则由扩散性定义可得结论成立.下面我们只证明旋转对称布尔函数$R(X)$在$n\geqslant 7$ 时不满足扩散性,而函数$R_n(X)$的证明类似得到.

取 $w=(1,0,\ldots,0)\in F_2^n$,则由于$|O_x|=|O_y|=n$,因此,显然有 $2n$个 $X\in F_2^n$ 使得$X+w\in O_x\cup O_y$.由O_x,O_y的定义,当$X\in O_x$时,设有n_1个 $X\in F_2^n$ 使得$X+w\in O_x\cup O_y$;当$X\in O_y$时,设有n_2个 $X\in F_2^n$ 使得$X+w\in O_x\cup O_y$.因此当$X\notin O_x\cup O_y$时,则只有$2n-n_1-n_2$个 $X\in F_2^n$ 使得$X+w\in O_x\cup O_y$.故下面等式成立:

$$\Delta_R(w)=\sum_{X\in F_2^n}(-1)^{R(X)+R(X+w)}$$

$$=\sum_{X\in O_x}(-1)^{1+R(X+w)}+\sum_{X\in O_y}(-1)^{1+R(X+w)}+\sum_{X\notin O_x\cup O_y}(-1)^{R(X+w)}$$

$$=n_1-(n-n_1)+n_2-(n-n_2)-(2n-n_1-n_2)+(2^n-2n-(2n-n_1-n_2))$$

$$=2^n-8n+4n_1+4n_2$$

$$\geqslant 2^n-8n.$$

显然当在$n\geqslant 7$ 时,$2^n-8n>0$.因此,旋转对称布尔函数$R(X)$在$n\geqslant 7$ 时不满足扩散性.定理得证. □

因此由定理 5,要研究布尔函数$R(X)$和$R_n(X)$在$n\geqslant 5$ 时的扩散性,只需要讨论$n=5$ 时的扩散性.在$n=5$ 时,通过搜索满足构造条件的O_x,O_y只有下面两类:

(1) $O_x=\{(1,0,1,0,0),(0,1,0,1,0),(0,0,1,0,1),(1,0,0,1,0),(0,1,0,0,1)\}$,对应的$O_y$只能为

$O_y=\{(1,1,1,0,0,),(0,1,1,1,0),(0,0,1,1,1),(1,0,0,1,1),(1,1,0,0,1)\}$.

(2) $O_x=\{(1,1,0,0,0),(0,1,1,0,0),(0,0,1,1,0),(0,0,0,1,1),(1,0,0,0,1)\}$,对应的$O_y$只能为

$O_y=\{(1,0,1,0,1),(1,1,0,1,0),(0,1,1,0,1),(1,0,1,1,0),(0,1,0,1,1)\}$.

通过计算发现,旋转对称布尔函数$R(X)$和$R_n(X)$只满足 1 次扩散准则($\Delta_f(w)\neq 0,w=(1,1,0,0,0)$, $f=R$或者$f=R_n$),即满足严格雪崩准则,而不满足其他的扩散准则.

2.4 相关免疫性

定理 6. 旋转对称布尔函数$R_n(X)$不具有相关免疫性,旋转对称布尔函数$R(X)$只具有一阶相关免疫性.

证明:由相关免疫性的定义,我们需要计算函数$R_n(X)$和$R(X)$的Walsh谱:

$$\begin{aligned}W_{R_n}(z)&=\sum_{X\in F_2^n}(-1)^{R_n(X)+X\cdot z}=\sum_{X\in O_x\cup O_y}(-1)^{G_n(X)+X\cdot z+1}+\sum_{X\in F_2^n-(O_x\cup O_y)}(-1)^{G_n(X)+X\cdot z}\\&=\sum_{X\in F_2^n-(O_x\cup O_y)}(-1)^{G_n(X)+X\cdot z}-\sum_{X\in O_x}(-1)^{G_n(X)+X\cdot z}-\sum_{X\in O_y}(-1)^{G_n(X)+X\cdot z}\\&=\sum_{X\in F_2^n}(-1)^{G_n(X)+X\cdot z}-2\sum_{X\in O_x}(-1)^{X\cdot z+1}-2\sum_{X\in O_y}(-1)^{X\cdot z}\\&=W_{G_n}(z)+2\sum_{X\in O_x}(-1)^{X\cdot z}-2\sum_{X\in O_y}(-1)^{X\cdot z}.\end{aligned}$$

当 $wt(z)=1$ 时,由文献[15]可知,$W_{G_n}(z)=-2\binom{n-1}{\frac{n-1}{2}}$,

又由于当 $wt(z)=1, wt(x)=\frac{n-1}{2}, wt(y)=\frac{n+1}{2}$ 时有 $\sum_{X\in O_x}(-1)^{X\cdot z}=1, \sum_{X\in O_y}(-1)^{X\cdot z}=-1$,

故$wt(z)=1$ 时,$W_{R_n}(z)=-2\binom{n-1}{\frac{n-1}{2}}+4$.因此,$R_n(X)$是一阶相关免疫函数的充要条件是 $-2\binom{n-1}{\frac{n-1}{2}}+4=0$.但是我们知道$\binom{n-1}{1}\leqslant\binom{n-1}{\frac{n-1}{2}}=2$,因此$n-1\leqslant 2$,从而得到$n\leqslant 3$.但是由假设$n\geqslant 5$,因此,$-2\binom{n-1}{\frac{n-1}{2}}+4\neq 0$,故$R_n(X)$不具有相关免疫性.

下面研究旋转对称布尔函数 $R(X)$的相关免疫性.由定理 1 得知,旋转对称布尔函数 $R(X)$的代数次数为 $n-1$.因此由引理 2,如果函数 $R(X)$具有相关免疫性,则相关免疫阶只能是 1.

下面证明旋转对称布尔函数 $R(X)$的相关免疫阶确实是 1.

由于

$$\begin{aligned}W_R(z)&=\sum_{X\in F_2^n}(-1)^{R(X)+X\cdot z}=\sum_{X\in F_2^n-(O_x\cup O_y)}(-1)^{X\cdot z}+\sum_{X\in O_x\cup O_y}(-1)^{1+X\cdot z}\\&=\sum_{X\in F_2^n}(-1)^{X\cdot z}-2\sum_{X\in O_x}(-1)^{X\cdot z}-2\sum_{X\in O_y}(-1)^{X\cdot z}.\end{aligned}$$

因此,

(1) 当$wt(z)=0$ 时,$W_R(z)=2^n-4n$;

(2) 当 $wt(z)=1$ 时,由于

$$\sum_{X\in F_2^n}(-1)^{X\cdot z}=0,\ \sum_{X\in O_x}(-1)^{X\cdot z}=1,\ \sum_{X\in O_y}(-1)^{X\cdot z}=-1,$$

故$W_R(z)=0$.由一阶相关免疫定义得知,旋转对称布尔函数$R(X)$是一阶相关免疫的.定理得证. □

2.5 非线性度

由文献[13]可知,旋转对称布尔函数$R_n(X)$的非线性度为 $2^{n-1}-\binom{n-1}{\frac{n-1}{2}}+2$,因此我们只需要讨论旋转对称布尔函数$R(X)$的非线性度.

定理 7. 旋转对称布尔函数 $R(X)$的非线性度为 $2n$.

证明:由定理 6 可知,

$$W_R(z)=\sum_{X\in F_2^n}(-1)^{X\cdot z}-2\sum_{X\in O_x}(-1)^{X\cdot z}-2\sum_{X\in O_y}(-1)^{X\cdot z}.$$

因此,

(1) 当$wt(z)=0$时,$W_R(z)=2^n-4n$;

(2) 当 $wt(z)\neq 0$时,

$$W_R(z)=-2\sum_{X\in O_x}(-1)^{X\cdot z}-2\sum_{X\in O_y}(-1)^{X\cdot z}.$$

由引理 1 可知,当 $wt(x)=\frac{n-1}{2}$时,$|O_x|=n$;当 $wt(y)=\frac{n+1}{2}$时,$|O_y|=n$.故

$$|W_R(z)|=|-2\sum_{X\in O_x}(-1)^{X\cdot z}-2\sum_{X\in O_y}(-1)^{X\cdot z}|\leqslant 4n.$$

显然,当$n\geqslant 7$时,$2^n\geqslant 8n$.故当$n\geqslant 7$时,$\max_{z\in F_2^n}|W_R(z)|=W_R(0)=2^n-4n$.因此,当$n\geqslant 7$时,$R(X)$的非线性度为

$$nl(R)=2^{n-1}-\frac{1}{2}\max_{z\in F_2^n}|W_R(z)|=2^{n-1}-\frac{1}{2}(2^n-4n)=2n.$$

因此,要讨论函数 $R(X)$的非线性度,还需要讨论当 n=5 时的非线性度.

当n=5 时,通过搜索满足上面构造条件的O_x,O_y只有下面两类:

(1) O_x={(1,0,1,0,0),(0,1,0,1,0),(0,0,1,0,1),(1,0,0,1,0),(0,1,0,0,1)},对应的O_y只能为

O_y={(1,1,1,0,0,),(0,1,1,1,0),(0,0,1,1,1),(1,0,0,1,1),(1,1,0,0,1)}.

(2) O_x={(1,1,0,0,0),(0,1,1,0,0),(0,0,1,1,0),(0,0,0,1,1),(1,0,0,0,1)},对应的O_y只能为

O_y={(1,0,1,0,1),(1,1,0,1,0),(0,1,1,0,1),(1,0,1,1,0),(0,1,0,1,1)}.

对上面两种情形,经过计算得到

$$\max_{z\in F_2^n}|W_R(z)|=|W_R(0,0,0,0,0)|=12.$$

因此,当 n=5 时,旋转对称布尔函数 $R(X)$也有 $\max_{z\in F_2^n}|W_R(z)|=2^n-4n=12$.因此,旋转对称布尔函数 $R(X)$的非线性度为 $nl(R)=2n$.定理得证. □

2.6 代数免疫阶

由文献[13]可知,旋转对称布尔函数$R_n(X)$的代数免疫阶达到最大为$\frac{n+1}{2}$.因此,我们只需要讨论旋转对称布尔函数 $R(X)$的代数免疫阶.

定理 8. 旋转对称布尔函数 $R(X)$的代数免疫阶是 2.

证明:设 $g(x_1,x_2,...,x_n)=a_0+\sum_{i=1}^{n}a_ix_i+\sum_{1\leqslant i<j\leqslant n}a_{ij}x_ix_j$,下面我们证明存在非零的、代数次数为 2 的布尔函数 $g(x_1,x_2,\ldots,x_n)$,使得$g(x_1,x_2,\ldots,x_n)R(x_1,x_2,\ldots,x_n)=0$.即存在不全为 0 的$a_i$,$0\leqslant i\leqslant n$和$a_{ij}$,$1\leqslant i<j\leqslant n$,使得

$$g(x_1,x_2,\ldots,x_n)R(x_1,x_2,\ldots,x_n)=0.$$

事实上,由于$R(x_1,x_2,\ldots,x_n)=1\Leftrightarrow(x_1,x_2,\ldots,x_n)\in O_x\cup O_y$,因此要使$g(x_1,x_2,\ldots,x_n)R(x_1,x_2,\ldots,x_n)=0$,只需要当$(x_1,x_2,\ldots,x_n)\in O_x\cup O_y$时$g(x_1,x_2,\ldots,x_n)=0$.由于$|O_x\cup O_y|=2n$,$g(x_1,x_2,\ldots,x_n)=0$ 中有$1+n+\frac{n(n-1)}{2}$个变量$a_i(0\leqslant i\leqslant n)$和$a_{ij}(1\leqslant i<j\leqslant n)$,因此我们可以得到一个由 $2n$个方程、$1+n+\frac{n(n-1)}{2}$个变量组成的齐次线性方程组.由于当$n\geqslant 5$时$1+n+\frac{n(n-1)}{2}>2n$,故上面的齐次线性方程组总存在非零的解$a_i(0\leqslant i\leqslant n)$和$a_{ij}(1\leqslant i<j\leqslant n)$,即总存在非零的代数次数为 2 的函数$g(x_1,x_2,\ldots,x_n)$使得$g(x_1,x_2,\ldots,x_n)R(x_1,x_2,\ldots,x_n)=0$.因此,我们得到函数$R(X)$的代数免疫阶小于等于 2.如果存在代数次数为 1 的函数$h(x_1,x_2,\ldots,x_n)=a_0+a_1x_1+a_2x_2+\ldots+a_nx_n$使得$h(x_1,x_2,\ldots,x_n)R(x_1,x_2,\ldots,x_n)=0$.则当$(x_1,x_2,\ldots,x_n)\in O_x\cup O_y$时有$h(x_1,x_2,\ldots,x_n)=0$,从而构成一个由 $2n$个方程、n+1 个变量$a_i(0\leqslant i\leqslant n)$组成的齐次线性

方程组.由于对任意的$x'\in O_x$存在唯一的$y'\in O_y$有$WS(x')\subset WS(y')$且$wt(x)=\frac{n-1}{2}, wt(y)=\frac{n+1}{2}$,因此由$x'$所对应的方程和$y'$所对应的方程之和为$a_i=0,1\leqslant i\leqslant n$.再将$a_i=0(1\leqslant i\leqslant n)$带入原方程组的任意一个方程得$a_0=0$.因此我们得到$h(x_1,x_2,\ldots,x_n)\equiv 0$,即旋转对称布尔函数$R(x_1,x_2,\ldots,x_n)$不存在代数次数为 1 的零化子.

由于当$wt(X)\leqslant\frac{n-3}{2}$时$R(X)+1=1$,如果存在代数次数为 1 的函数$h(x_1,x_2,\ldots,x_n)=a_0+a_1x_1+a_2x_2+\ldots+a_nx_n$使得$h(x_1,x_2,\ldots,x_n)(R(x_1,x_2,\ldots,x_n)+1)=0$,则当$wt(X)\leqslant\frac{n-3}{2}$时$h(x_1,x_2,\ldots,x_n)=0$,因此取$X(0,0,\ldots,0)$则有$h(0,0,\ldots,0)=0$,从而可得$a_0=0$.由于$n\geqslant 5$,同理取$X(0,0,\ldots,0,1,0,\ldots,0)$,即$X$的第$i$个位置为 1,其余位置为 0,代入$h(x_1,x_2,\ldots,x_n)$得$h(0,0,\ldots,0,1,0,\ldots,0)=0$,因此得到$a_i=0,1\leqslant i\leqslant n$,故$h(x_1,x_2,\ldots,x_n)\equiv 0$.即是说,$R(X)+1$ 不存在代数次数为 1 的零化子.

综上,我们可以得到旋转对称布尔函数 $R(X)$的代数免疫阶是 2.定理得证. □

3 结束语

本文主要研究了一类奇数个变元的具有最大代数免疫阶的旋转对称布尔函数及其与其相关的一类旋转对称布尔函数的密码学性质:代数免疫阶、非线性度、代数次数、相关免疫性、线性结构、扩散性、平衡性.通过研究发现,虽然文献[13]中构造的旋转对称布尔函数的代数免疫阶达到最大,代数次数也很高并且没有非零的线性结构,同时还具有平衡性,但是它却不具有相关免疫性,因此不能直接应用到实际的密码系统中.与其相关的一类旋转对称布尔函数的代数次数也很高,同时还具有一阶相关免疫性,但是却不具有平衡性,并且代数免疫阶也很低,为 2,因此同样不能用在实际的密码系统中.对上面的旋转对称布尔函数,我们没有研究的密码学性质是互相关性.同时,如何改造上面的旋转对称布尔函数使得改造后的布尔函数的密码学性质较好是一个非常感兴趣的研究问题,这将是我们下一步的研究工作.

致谢 衷心感谢审稿人的审理意见.

References:

[1] Armknecht F. Improving fast algebraic attacks. In: Roy B, Meier W, eds. Proc. of the Fast Software Encryption (FSE 2004). LNCS 3017, Berlin: Springer-Verlag, 2004. 65−82.

[2] Batten LM. Algebraic attacks over $GF(q)$. In: Canteaut A, Viswanathan K, eds. Proc. of the Progress in Cryptology-Indocrypt 2004. LNCS 3348, Berlin: Springer- Verlag, 2004. 84−91.

[3] Braeken A, Praneel B. Probabilistic algebraic attacks. In: Smart NP, ed. Proc. of the 10th IMA Int'l Conf. on Cryptography and Coding. LNCS 3796, Berlin: Springer-Verlag, 2005. 290−303.

[4] Cheon J, Lee D. Resistance of S-boxes against algebraic attacks. In: Roy B, Meier W, eds. Proc. of the Fast Software Encryption (FSE 2004). LNCS 3017, Berlin: Springer-Verlag, 2004. 83−94.

[5] Cho J, Pieprzyk J. Algebraic attacks on SOBER-t32 and SOBER-128. In: Roy B, Meier W, eds. Proc. of the Fast Software Encryption (FSE 2004). LNCS 3017, Berlin: Springer-Verlag, 2004. 49−64.

[6] Courtois N, Pieprzyk J. Cryptanalysis of block ciphers with overdefined systems of equations. In: Advances in Cryptology-Asiacrypt 2002. LNCS 2501, Berlin: Springer-Verlag, 2002. 267−287. http://eprint.iacr.org/2002/044/

[7] Courtois N, Meier W. Algebraic attacks on stream ciphers with linear feedback. In: Advances in Cryptology-Eurocrypt 2003. LNCS 2656, Berlin: Springer-Verlag, 2003. 345−359.

[8] Courtois N. Fast algebraic attacks on stream ciphers with linear feedback. In: Advances in Cryptology-Crypto 2003. LNCS 2729, Berlin: Springer-Verlag, 2003. 176−194.

[9] Lee D, Kim J, Hong J, Han J, Moon D. Algebraic attacks on summation generators. In: Roy B, Meier W, eds. Proc. of the Fast Software Encryption (FSE 2004). LNCS 3017, Berlin: Springer-Verlag, 2004. 34−48.

[10] Didier F, Tillich J. Computing the algebraic immunity efficiently. http://www.iacr.org/archive/fse2006/40470362/40470362.pdf

[11] Courtois N, Debraize B, Garrido E. On exact algebraic [non-]immunity of S-boxes based on power functions. In: Proc. of the Australasian Conf. on Information Security and Privacy (ACISP 2006). LNCS 4058, Berlin: Springer-Verlag, 2006. 76−86. http://eprint.iacr.org/2005/203

[12] Meier W, Pasalic E, Carlet C. Algebraic attacks and decomposition of Boolean functions. In: Advances in Cryptology-Eurocrypt 2004. LNCS 3027, Berlin: Springer-Verlag, 2004. 474−491. http://www.iacr.org/archive/eurocrypt2004/30270469/finaleurocr.pdf

[13] Sarkar S, Maitra S. Construction of rotation symmetric Boolean functions with maximum algebraic immunity on odd number of variables. In: Proc. of the Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC 2007). LNCS 4851, Berlin: Spring-Berlin 2007. 271−280. http://eprint.iacr.org/2007/290.pdf

[14] Dalai D, Gupta K, Maitra S. Cryptographically significant Boolean functions: Construction and analysis in terms of algebraic immunity. In: Proc. of the Fast Software Encryption (FSE 2005). LNCS 3557, Berlin: Springer-Verlag, 2005. 98−111.

[15] Dalai D, Maitra S, Sarkar S. Basic theory in construction of Boolean functions with maximum possible annihilator immunity. Design, Codes and Cryptography, 2006,40(1):41−58. http://eprint.iacr.org/2005/229

[16] Carlet C. A method of construction of balanced functions with optimum algebraic immunity. In: Proc. of the Wuyi Workshop on Coding and Cryptology, Published by World Scientific Publishing Co. in its Series of Coding and Cryptology. 2006. http://eprint.iacr.org/2006/149

[17] Carlet C, Feng K. An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity. In: Advances in Cryptology-ASIACRYPT 2008. LNCS 5350, Berlin: Springer-Verlag, 2008. 425−440.

[18] Zhang WY, Wu CK, Liu XZ. Construction and enumeration of Boolean functions with maximum algebraic immunity. Science in China Series F: Information Sciences, 2009,52(1):32−40.

[19] Stănică P, Maitra S. Rotation symmetric Boolean functions-count and cryptographic properties. Discrete Applied Mathematics, 2008,156(10):1567−1580.

[20] Stănică P, Maitra S, Clark J. Results on rotation symmetric bent and correlation immune Boolean functions. In: Roy B, Meier W, eds. Proc. of the Fast Software Encryption (FSE 2004). LNCS 3017, Berlin: Springer-Verlag, 2004. 161−177.

[21] Dalai D, Maitra S, Stănică P. Results on rotation symmetric bent functions. Discrete Mathematics, 2009,309:2398−2409. http://iacr.org/2005/118.ps.gz

[22] Kavut S, Maitra S, Sarkar S, Yuecel M. Enumeration of 9-variable rotation symmetric Boolean functions having nonlinearity>240. In: Barua R, Lange T, eds. Proc. of the Int'l Conf. on Cryptology in India (INDOCRYPT 2006). LNCS 4329, Berlin: Springer-Verlag, 2006. 266−279.

[23] Stănică P, Maitra S. A constructive count of rotation symmetric functions. Information Processing Letters, 2003,88:299−304.

[24] Stănică P, Maitra S. Rotation symmetric Boolean functions-count and cryptographic properties. Discrete Applied Mathematics, 2008,156(10):1567−1580.

[25] Pieprzyk J, Qu C. Fast hashing and rotation-symmetric functions. Journal of Universal Computer Science, 1999,5(1):20−31.

[26] Evertse J. Linear structures in block ciphers. In: Advances in Cryptology-EUROCRYPT'87. LNCS 304, Berlin: Springer-Verlag, 1988. 249−266.

[27] Chaum D, Evertse J. Cryptanalysis of DES with a reduced number of rounds sequences of linear factors in block cipher. In: Advances in Cryptology-CRYPTO'85. LNCS 218, Berlin: Springer-Verlag, 1986. 192−211.

[28] Dunne P, Leng P, Nwana G. On the complexity of Boolean functions computed by lazy oracles. IEEE Trans. on Computers, 1995, 44(4):495−502.

[29] Schnorr G. The network complexity and the turing machine complexity of finite functions. Acta Informatica, 1976,7:95−107.

[30] Stockmeyer L. On the combinational complexity of certain symmetric Boolean functions. Mathematical Systems Theory, 1977,10: 323−336.

[31] Siegenthaler T. Correlation-Immunity of nonlinear combining functions for cryptographic applications. IEEE Trans. on Information Theory, 1984,30(5):776−780.

孙光洪(1976－),男,重庆人,博士,讲师,主要研究领域为密码学.

武传坤(1964－),男,博士,研究员,博士生导师,主要研究领域为密码学,网络安全.