文章编号:1000－2367(2017)03－0024－10　　**DOI**:10.16366/j.cnki.1000－2367.2017.03.003

流密码中的布尔函数设计研究进展

张卫国[1]，李路阳[2]

(1.西安电子科技大学 通信工程学院,西安 710071;2.保密通信重点实验室,成都 610041)

摘　要:密码函数,主要包括单输出布尔函数和多输出布尔函数,在流密码及分组密码系统中扮演着重要角色.在基于线性反馈移位寄存器的流密码系统中为了抵抗各种攻击,一个好的密码函数需要满足以下指标:较高的非线性度、平衡性、低阶相关免疫性、高的代数次数,高代数免疫阶等等.主要总结了近年来在高非线性度弹性密码函数,具有最优代数免疫度的函数和具有良好自相关性质的函数等研究方面的进展,并对其后续工作进行了展望.

关键词:流密码;布尔函数;非线性度;弹性;代数免疫;自相关性质

中图分类号:TN918.3　　**文献标志码**:A

流密码,又称之为序列密码,因其加解密原理简单,算法迅速快捷,在保密通信中扮演着不可替代的角色.在其加解密过程中,通过将明文或者密文与同一条密钥流序列(伪随机序列)进行叠加来实现明文加密或者密文恢复.

非线性滤波生成器和非线性组合生成器(图 1),是两种经典的基于线性反馈移位寄存器的伪随机序列生成器.它们的结构可分为驱动部分和非线性组合部分.而布尔函数作为非线性组合部分的重要部件,其密码学性质直接关系到整个流密码系统的安全性.这里的密码学性质,主要是通过布尔函数的各种密码学指标来衡量的,这些密码学指标与已知的各种针对流密码体制的攻击方式密切相关.譬如说为了抵抗线性攻击和最佳仿射逼近(BAA)攻击,需要布尔函数具有较高的非线性度;为了抵抗分别征服攻击,布尔函数要具有一定的相关免疫阶;为了抵抗高阶差分攻击,Berlekamp-Massey 算法攻击等,布尔函数需要具有较高的代数次数;为了抵抗代数攻击,函数需要有较好的代数免疫度和抵抗快速代数攻击的能力等等.

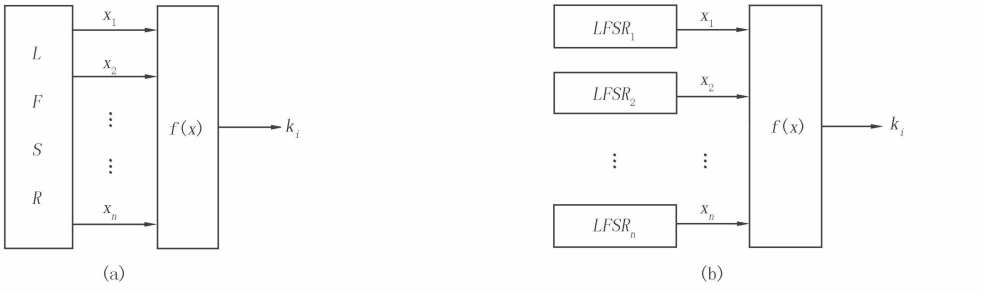

图1　非线性滤波生成器(a)和非线性组合生成器(b)

为了抵抗各种攻击,要求所使用的布尔函数的各种密码学性质都足够好.然而布尔函数的各项密码学指标之间存在一定的制约关系,密码函数的各种指标往往不能同时都达到最优,如何实现这些指标之间的最优折中是这一领域研究的重要难题.

为了实现布尔函数的非线性度、弹性、代数次数、代数免疫等指标在流密码系统中的优化折中,自从 20 世纪 90 年代以来,密码学家就该问题做了许多工作,得到了很多重要的成果.在本文中,将对近年来在高非线性度弹性布尔函数,高非线性度弹性多输出函数,具有最优代数免疫度和具有良好自相关性质的布尔函数

收稿日期:2017-03-09;**修回日期**:2017-04-17.

基金项目:国家自然科学基金(61672414)

作者简介(通信作者):张卫国(1977－),男,山东聊城人,西安电子科技大学教授,博士,博士生导师,研究方向为密码学,E-mail:wgzhang@foxmail.com.

等研究方面的一些比较重要的成果进行分析总结，并给出了一些尚未解决的公开问题.

下面是一些基本概念.

布尔函数　一个 n 元布尔函数 $f(x)$ 表示为某个 F_2^n 到 F_2 上的映射. 并且可以用如下代数正规型来表示

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

代数次数　代数正规型中出现的项中含有的最大的变元个数.

Walsh 谱　对于任意的 n 元布尔函数 $f(x)$，其在 $w\in F_2^n$ 点处的 Walsh 谱定义如下：

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

弹性　对于任意的 n 元布尔函数 $f(x)$，$w\in F_2^n$，$1\leq t\leq n$ 来说，$f(x)$ 是 t 阶弹性的当且仅当对于任意的 $0\leq wt(w)\leq t$，$W_f(w)=0$ 成立.

代数免疫度　对于任意的 n 元布尔函数 $f(x)$，定义满足 $fg=0$ 的 n 元函数 g 为 f 的零化子. 令 $A(f)$ 为函数 f 的零化子的集合，那么函数的代数免疫度 $A_I(f)$ 定义如下：

$$A_I(f)=\min\{\deg g\mid 0\neq g\in A(f)\cup A(1+f)\}.$$

严格雪崩性质　对于任意的 n 元布尔函数 $f(x)$ 和 $\alpha\in F_2^n$，定义函数 f 在 α 点处的自相关函数为：

$$C_f(\alpha)=\sum_{x\in F_2^n}(-1)^{f(x)+f(x+\alpha)}.$$

如果对于任意的 $wt(\alpha)=1$，都有 $C_f(\alpha)=0$，则函数 f 满足 SAC.

全局雪崩特性　布尔函数 f 的全局雪崩特性崩主要由以下两个指标体现：

(1)绝对值指标

$$\Delta_f=\max_{\alpha\neq 0}\mid C_f(\alpha)\mid;$$

(2)平方和指标

$$\sigma_f=\sum_{a\in F_2^n}C_f^2(\alpha).$$

1　具有高非线性度弹性密码函数的研究

非线性度是最重要的密码学指标之一，非线性度低的布尔函数无论用于流密码还是分组密码都是有缺陷的. 在构造密码函数的时候，首先要保证它具有较高的非线性度. 但是由于人们对非线性的理论知之甚少，要构造更多类型的高非线性度布尔函数并不是一件容易的事情.

Siegenthaler 提出的相关免疫函数是为防止攻击者对流密码系统进行分别征服攻击[1]. 最初相关免疫的概念是通过概率的形式刻画的，后来肖国镇教授与 Massey 一起提出了相关免疫函数的频谱特征化定理[2](国际上称为 Xiao-Massey 定理)，从此人们对弹性函数(平衡的相关免疫函数)的认识愈加清晰. 弹性与很多密码学指标都相互制约. 例如 n 元布尔函数的代数次数 d 和弹性 t 之间存在关系 $d\leq n-t-1$(这个界叫 Siegenthaler 界)；另外，弹性阶和非线性度之间也存在很强的制约关系，关于弹性函数的非线性度的紧上界也是由来已久的问题[3].

1.1　高非线性度弹性布尔函数的构造

对于一个 n 元布尔函数来说，其最大非线性度不会超过 $2^{n-1}-2^{n/2-1}$. 当 n 为偶数的时候，非线性度为 $2^{n-1}-2^{n/2-1}$ 的布尔函数被称为 Bent 函数[4]. Bent 函数在所有点处的谱值绝对值都相同，具有最大的非线性度，能很好抵抗线性攻击和最佳仿射逼近攻击. Bent 函数不具有平衡性，也不是弹性函数，在实用中受到了很大限制.

Maiorana-Mcfarland(M-M)[5]构造法和 Partial Spread(PS)[6]构造法是两类构造 Bent 函数的方法. Bent 函数具有最高的非线性度，可以通过修改 M-M 类或者 PS 类 Bent 函数，牺牲掉其一部分非线性度来获得一定的弹性阶. 这一问题的难点在于如何让修改后的函数在保证一定弹性阶的同时具有更高的非线性度. 这里将非线性度达到 $2^{n-1}-2^{\lfloor n/2\rfloor}$ 的布尔函数称为几乎最优函数，严格大于此值的布尔函数称为严格几乎最

优函数.关于具有高非线性度的弹性布尔函数的构造,一些比较重要的成果介绍如下.

1)在文献[5]中,Camion 等人首次将 M-M 构造技术进行改进,用于弹性函数的构造.通过级联若干弹性仿射函数来构造具有弹性的非线性函数.该类构造得到的 M-M 类弹性函数的非线性度都没有超过 $2^{n-1}-2^{\lfloor n/2\rfloor}$,而且受限于 M-M 构造的特点,这些函数的代数次数一般情况下不能达到最优.

2)在文献[7]中,Pasalic 给出了一种提高 M-M 类函数代数次数的方法,该方法可以在非线性度不变的前提下,使得到的函数代数次数达到最优.虽然这类函数的非线性度仍然无法超过 $2^{n-1}-2^{\lfloor n/2\rfloor}$,但是这种不损害非线性度的优化代数次数的方法却非常有用.

3)Carlet 在文献[8]给出了一种对 M-M 类构造技术的推广方法,该方法的主要原理是将原 M-M 构造中级联的仿射函数替换为二次函数.遗憾的是,这类函数也不是代数次数最优的,非线性度和弹性阶之间也没能更好地实现折中.

4)Sarkar 和 Maitra 在文献[9]中给出,对于任意的整数 $n\geq 12$,n 为偶数,一定存在一个非线性度严格大于 $2^{n-1}-2^{n/2}$,而且次数为 $n-t-1$ 的 t 阶弹性 n 元函数.他们还给出了构造 n 元 1 阶弹性,代数次数为 $n-2$,非线性度达到 $2^{n-1}-2^{n/2-1}-2^{n/2-2}-2^{n/4-2}-4$ 布尔函数的方法.随后在文献[10]中,Maitra 和 Pasalic 给出了进一步的改进方法,在 $n\geq 10$ 的时候,将上述代数次数最优的 1 阶弹性,布尔函数的非线性度提高至 $2^{n-1}-2^{n/2-1}-2^{n/4-2}-4$.

5)Seberry 等在文献[11]中使用迭代的方法,通过对 M-M 类 Bent 函数进行修改,得到一类高非线性度平衡布尔函数.在他们的构造方法中,为了得到 n 元高非线性度布尔函数,需要级联 $2^{n/2}-1$ 个 $n/2$ 元线性函数和一个 $n/2$ 元高非线性度平衡函数,而这个高非线性度平衡函数也是由同样的方法递归得来.Dobbertin 在文献[12]中也独立地提出一种通过对 PS 类 Bent 函数进行迭代修改构造高非线性度平衡布尔函数的方法,两者思路类似,得到的结果也是相同的.截止到目前,关于平衡布尔函数的最大非线性度的下界,该结果仍然是最好的.

6)$n\geq 12$,且 n 为偶数时,Maitra 和 Pasalic 在文献[13]中给出一种新的构造方法,该方法将 $2^{n-1}-2^k$ 个谱值不相交的 t 阶弹性仿射函数和一个 $n/2+k$ 元 t 阶弹性且非线性度很高的函数进行级联,得到了一类非线性度大于 $2^{n-1}-2^{n/2-1}-2^{n/2-2}$ 的 n 元 t 阶弹性布尔函数.更进一步,当 $n\geq 8m+6$,还给出了一种构造非线性度为 $2^{n-1}-2^{n/2-1}-2^{n/2-4}$ 的 t 阶弹性布尔函数的方法.

7)张卫国和肖国镇在文献[14]中给出了不相交谱函数的定义,并给出一类特殊的不相交谱函数:部分线性函数.利用部分线性函数,张卫国和肖国镇得到了一大类变元个数为偶数、非线性度严格大于 $2^{n-1}-2^{n/2}$ 的弹性布尔函数.他们还给出了一种优化方法,使构造出的函数的次数也能达到 Siegenthaler 界.相比文献[13]来说,该方法进一步提高了弹性函数的非线性度上界.

8)张卫国和 Pasalic 于 2014 年在文献[15]中提出了 GMM 类密码函数的构造方案,通过级联若干组定义在不同的仿射函数,得到了非线性度严格几乎最优的弹性布尔函数.实际上,M-M 类布尔函数也可以看作是 GMM 类布尔函数的一种特殊形式.计算机仿真表明该类函数在保证高非线性度和适当弹性的前提下,还可以同时具有最优代数免疫阶和抵抗快速代数攻击的能力.他们还给出了构造具有严格几乎最优非线性度的奇数元弹性布尔函数的方法.

9)张卫国和 Pasalic 在文献[16]中给出了一种提高一阶弹性布尔函数最大非线性度下界的方法,得到了一大类具有目前最高非线性度的 1 阶弹性函数,在 n 为不小于 8 的偶数时,非线性度是 $2^{n-1}-2^{n/2-1}-2^{\lceil n/4\rceil}$.同时通过简单的修改,这些函数还可以具有较好的代数免疫度和抵抗快速代数攻击的能力.

除了上面的构造方法,还有一系列其他构造具有高非线性度,高代数次数的平衡及弹性布尔函数的方法,可以参考文献[17-28]等.特别值得指出的是,利用计算机搜索,在文献[29-38]中,得到了一些无法直接构造出来的函数,比如 10 元 2 阶弹性非线性度为 488 的函数,9 元 3 阶弹性非线性度为 240 的函数.采用计算机搜索技术,在变元个数较小时,可以实现较多密码学指标的优化折中.具有以下参数的密码函数是前人未曾得到过的[39]:(9,1,7,236,4,8);(10,1,8,484,5,9);(11,1,9,984,5,10);(12,1,10,1988,6,11);(13,1,11,4012,6,12);(14,1,12,8072,7,13).上述函数的 7 个指标分别是,变元个数,弹性阶,代数次数,非线性度,代数免疫阶,抵抗快速代数攻击的能力.

在高非线性度弹性布尔函数的构造方面，仍然有很多重要问题没有解决.

问题 1　当 $n\geq 8$，且 n 为偶数时，对于一个 n 元平衡布尔函数 f 来说，其最大非线性度是多少？能否达到 $2^{n-1}-2^{n/2-1}-2$？目前已知在 $n\leq 6$ 时都可以达到这个界.

问题 2　当 $t\leq n/2-2$ 时，对于一个 n 元 t 阶弹性布尔函数 f 来说，其非线性度最高为多少？能否达到 $2^{n-1}-2^{n/2-1}-2^{t+1}$？目前 8 元 1 阶非线性度为 116，10 元 1 阶和 2 阶非线性度分别为 492 和 448 的函数都已经证明存在，这些函数的非线性度值均达到该上界.

问题 3　文献[31]指出，当 $n\geq 9$ 且 n 为奇数时，对于 f 来说，其非线性度最大值可以严格大于 $2^{n-1}-2^{(n-1)/2}$. 两类比较经典的函数分别是非线性度达到 242 的 9 元 Kavut-Yücel 函数[40]，和非线性度达到16 276 的 15 元 Patterson-Wiedemann 函数[41]. 如何寻找其他奇数元具有严格几乎最优非线性度的布尔函数仍然是一个公开难题.

如果将平衡函数看作是 0 阶弹性的，这些问题便可以归结为一个问题：一个 n 元布尔函数在弹性阶为 t 时，其非线性度最高能达到多少？这也是目前最难的公开问题之一[3].

猜想　设 f 为 n 元 t 阶弹性布尔函数，其中 n 为不小于 8 的偶数. 则 f 的非线性度

$$N_f\leq 2^{n-1}-2^{n/2}-2^{\lfloor n/4\rfloor+m-1}.$$

1.2　高非线性度弹性多输出布尔函数的构造

在图 1 所示的密钥流生成器中，如果使用多输出的布尔函数，可以提高密钥流的生成效率. 和单输出函数类似，多输出布尔函数也需要具有较高的非线性度，较低的弹性阶和高的代数次数等等.

多输出布尔函数 F 是一个从 F_2^n 到 F_2^m 的映射（n 输入 m 输出），可以看作 m 个 n 元布尔函数的组合，也就是 $F=(f_1,\cdots,f_m)$. 多输出布尔函数用于流密码系统时也需要具有和布尔函数类似的各种指标：高非线性度，适当的弹性阶，高的代数次数等等. F 是 t 阶弹性的当且仅当它的分量函数的任意非零线性组合都是 t 阶弹性的. 当然函数 F 的非线性度也需要考虑所有分量函数的非零线性组合. 因此，多输出函数的研究更加复杂. 在这里主要就流密码中高非线性度多输出弹性函数的构造做一个简单的总结. 为简便起见，用 t 阶 (n,m) 函数来指代 n 输入 m 输出且弹性阶为 t 的多输出布尔函数.

1）Zhang 和 Zheng 在文献[42]中给出了一种办法可以把一个线性的 t 阶 (n,m) 函数 F 转变为一个非线性 t 阶 (n,m) 函数 $F'=G(F)$，这里 G 是 F_2^m 上的一个置换. 如果用 N_G 表示 G 的非线性度，可以证明 $N_{F'}$ 和 N_G 两者之间满足 $N_{F'}=2^{m-n}N_G$，注意到作为一个置换，$N_G\leq 2^{m-1}-2^{(m-1)/2}$[43]，于是总有 $N_{F'}\leq 2^{n-1}-2^{n-(m+1)/2}$. 明显地，该函数的非线性度并不高.

2）当 n 为奇数时，Kurosawa 等人在文献[44]介绍了一个简单的办法来构造新的 t 阶 (n,m) 函数. 令 $\phi(X_{n-l})$ 是非线性度为 N_ϕ 的 t 阶 $(n-l,m)$ 函数，$\varphi(Y_l)$ 是一个 (l,m) 完全非线性函数. 将这两个函数直接进行直和便可以得到一个 t 阶 (n,m) 函数 $F(X_{n-l},Y_l)=\phi(X_{n-l})\oplus\varphi(Y_l)$. 可以证明该函数的非线性度为 $N_F=2^{n-1}-2^{n-l/2-1}+2^{l/2}N_\phi$. F 具有严格几乎最优的非线性度当且仅当 $\varphi(Y_l)$ 非线性度是严格几乎最优的.

3）Chen 和 Fu 在文献[45]中也提出了一个具有一般形式的线性构造方法用来构造奇数元 t 阶 (n,m) 函数. 其方法仍然是采用直和的方式：如果 F 和 G 分别是 t_1 阶 (n_1,m) 函数和 t_2 阶 (n_2,m) 函数，那么直和后的函数 $F\oplus G$ 是一个 t_1+t_2+1 阶 (n_1+n_2,m) 函数.

4）如果 $[n-d-1,m,t+1]$ 线性码存在，可以借助 Cheon 在文献[46]中给出的方法来构造 t 阶 (n,m) 函数. 此方法得到的函数的代数次数是 d，非线性度是 $2^{n-1}-2^{n-d-1}\cdot\lfloor 2^{n/2}\rfloor+2^{n-d-2}$. 可以看出，这种方法得到的函数具有比较高的代数次数，但是非线性度不高.

5）Johansson 和 Pasalic 在文献[47]中证明了利用足够多的 $[n-d,m,t+1]$ 不相交线性码集合可以构造非线性度为 $2^{n-1}-2^{n-d-1}$ 的 t 阶 (n,m) 函数. 然而如何去寻找足够多的不相交线性码集合却成为一个瓶颈的难题，这种构造方法也引出了文献[48－49]中涉及的构造不相交线性码集合的问题.

6）在文献[50]中，通过用单一的线性码来替代不相交线性码，Pasalic 和 Maitra 给出了一种构造高非线性 t 阶 (n,m) 函数的方法. 给定一个 $[u,m,t+1]$ 线性码，他们证明了当 $n\geq u$ 时，便可以构造高非线性 t 阶 (n,m) 函数.

7）李路阳和张卫国在文献[51]中通过修改 PS 类 Bent 函数，得到了两类具有较高代数次数和非线性度

严格几乎最优的多输出布尔函数.这两类函数分别满足平衡性和一阶相关免疫性.其非线性度均为 $2^{n-1}-2^{n/2-1}-2^{\lceil n/4\rceil}$.对于一阶相关免疫多输出布尔函数来说,这个非线性度是目前最好的.遗憾的是这种构造方法得到的弹性函数不能同时兼顾平衡性和相关免疫性.

8)在文献[52]中,张卫国和 Pasalic 给出了一种生成 $[u,m]$ 不相交线性码集合的新思路.并且利用一些长度不等的不相交码,他们构造出一类非线性度严格大于 $2^{n-1}-2^{n/2}$ 的 t 阶 (n,m) 函数,这里 n 是偶数且 $1<m\leq_{\mathrm{L}} n/4\rfloor$.这是第一次构造出非线性度超过 $2^{n-1}-2^{n/2}$ 且同时具有弹性的多输出布尔函数.

9)张卫国和 Pasalic 在文献[53]中还给出了一种利用 m 序列构造平衡 (n,m) 函数的方法,所构造出的平衡 (n,m) 函数不仅输出维数可以达到输入的一半,而且其非线性度也可以达到严格几乎最优.计算机仿真表明其差分性质也很优良.

10)张卫国和李路阳等提出一种 GMM 类多输出布尔函数的构造方法[54].构造的多输出弹性布尔函数同时具有严格几乎最优的非线性度和目前已知最高的输出维数.对于一个 n 输入 m 输出的函数来说,首次在 $\lfloor_{\mathrm{L}} n/4\rfloor\leq m<n/2$ 时构造出非线性度严格大于 $2^{n-1}-2^{n/2}$ 的多输出函数.并且在 $m<_{\mathrm{L}} n/4\rfloor$ 时,该构造方法也能得到一大批目前已知非线性度最高的多输出弹性函数.

除了以上列出的文献外,在构造高非线性度多输出弹性布尔函数方面,还有很多工作.然而前文中也提到,对多输出布尔函数的指标进行研究时,不仅需要考虑全体分量函数,还要考虑它们所有的线性组合,这无疑极大地增加了研究的难度.我们亟须找到构造多输出弹性函数新的思路和方法.以下是尚未解决的难题.

问题 4 当 $m\leq n/2$ 时,t 阶弹性 (n,m) 函数的非线性度上界是多少?如何构造出非线性度比文献[52,54]更好的函数?

问题 5 当 $n/2<m\leq n$ 时,目前已知 (n,m) 函数的非线性度能达到 $2^{n-1}-2^{n/2}$,那么其非线性度能否超过这个界?此时是否存在具有严格几乎最优非线性度的 t 阶 (n,m) 函数?如果存在如何构造?如果不存在,其非线性度最高为多少?

问题 6 当 n 为奇数时,如何构造非线性度大于 $2^{n-1}-2^{(n-1)/2}$ 的多输出布尔函数?

2 具有最优代数免疫度函数的研究

代数攻击的思想主要是基于代数学上求解方程组的过程.该攻击方法十分有效并且已经成功对部分流密码算法比如 Toyocrypt 和 LILI-128 等等进行了攻破.代数攻击的提出为密码函数的分析和设计提出了新的难题.

随着代数攻击的提出与深入研究,在使用图 1 所示的密钥流生成器的时候必须保证非线性组合部分的布尔函数要有抵抗代数攻击的能力.为了刻画函数抵抗代数攻击的能力,Meier 等人提出了代数免疫的概念[55].对于一个 n 元布尔函数来说,其代数免疫度最高为 $\lceil n/2\rceil$.由于代数攻击的提出,在构造布尔函数时,除了之前要求的具有高非线性度、弹性等条件外,还要具有最优的代数免疫度.代数免疫度不高的函数,容易遭受代数攻击.在这种情况下,代数免疫最优函数的构造引起了人们的极大关注.目前关于此类函数的构造方法已经有很多结果,比如基于支撑集包含关系的构造,基于平面理论的构造,基于有限域的构造等等.比较有代表性的结论有以下几种.

1)Dalai 于 2005 年在文献[56]中提出了一种基于支撑包含关系构造 MAI 函数的方法,分别给出了在奇数情况和偶数情况下具有最优代数免疫度的函数.这些函数其实是一种特殊的布尔函数,称之为择多逻辑函数.但是这种函数的非线性度很差.

2)屈龙江,李娜等分别在文献[57-58]中研究了对称布尔函数的代数免疫,证明了奇数元具有最优代数免疫度的函数只有一类.

3)Carlet 等人在文献[59]中给出了代数免疫最优的函数与 Reed-Muller 码之间的关系,还给出了基于 Reed-Muller 码的生成矩阵来构造最优代数免疫函数的充分必要条件,这个条件为以后使用线性码的生成矩阵来研究函数的代数免疫度奠定了良好的基础.

4)Carlet 和冯克勤于 2008 年在文献[60]中构造出了一类支撑集定义在 $GF(2)$ 上的平衡布尔函数.这种

构造方法非常简单，用这种方法得到的函数其代数次数是最大的，但是其非线性度仍然不够好.

5）涂自然和邓映蒲于 2010 年提出了一个猜想[61]，在它成立的前提下，利用 BCH 界可以证明一类 PS 类 Bent 函数具有最优的代数免疫度，并且在不改变代数免疫度的前提下可以将该函数修改为具有最大代数次数的高非线性度平衡函数. 随后涂自然和邓映蒲在文献[62]中还给出了一类具有高非线性度和最优代数免疫 1 阶弹性布尔函数的构造方法. 这类函数抵抗快速代数攻击的能力也比较弱.

6）在文献[63]中唐灯和 Carlet 等给出了一类函数，这类函数具有最优的代数免疫度，可以是平衡的，并且其非线性度还很高. 计算机仿真表明该函数可以具有优良的抵抗快速代数攻击的能力.

7）张卫国和 Pasalic 在文献[16]中给出一种方案，通过修改 PS 型 Bent 函数真值表的特殊位置，可以实现非线性度、平衡性、代数次数、代数免疫、抵抗快速代数攻击等多种密码学性质的折中。遗憾的是，这类函数不能保证具有弹性.

除了以上提到的函数类，国内学者在这一研究课题上还有很多结果，限于篇幅不再一一列举. 然而，大多数结果都主要是从代数免疫的角度来进行考虑，因此所构造函数的非线性度大都是进行估算得到的，相比之前提及的弹性高非线性度函数来说，这些代数性质较好的函数其非线性度都不够高. 特别是弹性阶大于 1 的时候，还没有找到一般性的方法来构造代数免疫度最优，非线性度较好的函数. 总之，具有最优代数免疫性质的函数虽已经有了很好的发展，但是仍然存在着问题，可用于密码体制中的各方面性质好的密码函数还是比较少，所以仍有待于更进一步的研究和分析.

问题 7　如何构造非线性度严格几乎最优并且具有最优代数免疫度的弹性函数？

3　具有好的自相关性质的布尔函数的研究

在 1985 年，Webster 和 Tavares 提出了严格雪崩（SAC）的概念[64]. SAC 刻画了一个非常重要的性质：当布尔函数有一个输入比特发生变化，其结果有一半产生变化. 很快 SAC 被广泛接受成为布尔函数设计的一个指标. 在 1995 年，Zhang 和 Zheng 指出 SAC 作为衡量雪崩特性的指标还有一些不足. 于是他们提出了全局雪崩特性（GAC）[65]，该性质包含两个指标：绝对值指标和平方和指标，这两个指标可以用来衡量一个函数的整体雪崩特性.

在前文曾指出，Bent 函数具有最高的非线性度，实际上它也有最好的自相关性质. 但 Bent 函数不是平衡函数，更不是弹性函数. 构造具有 SAC 性质的弹性布尔函数并且具有高的非线性度，好的 GAC 性质（低的绝对值指标和低的平方和指标）是很必要的. 为了构造这样类型的函数，一些密码学家也做出值得借鉴的工作.

1）在文献[66－68]中，Canteaut 和 Stanica 等人分别独立地得到了一类非线性度为 $2^{n-1}-2^{n/2}$，平方和与绝对值指标分别为 2^n 和 2^{2n+2} 的平衡函数. 虽然这些函数满足严格雪崩准则，但是比较遗憾的是这些函数非线性度并不太高，全局雪崩性质也不太好.

2）在文献[69]中，得到了非线性度为 $2^{n-2}-2^{n/2-1}-2^{n/2-2}$ 的布尔函数，这是首次构造出非线性度严格几乎最优并且满足严格雪崩准则的平衡布尔函数，并且相比文献[66－68]中的结果，平方和指标和绝对值指标的值都得到了一定程度的降低.

3）Stanica 和 Sung 在文献[70]中提出了一种具有 5 个可控密码学性质的布尔函数的构造方法，他们构造出一类平方和指标为 $2^{2n}+3\cdot 2^{3n/2+1}$ 的满足严格雪崩准则的平衡布尔函数，然而这类函数非线性度不是严格几乎最优的.

4）李路阳等在文献[71]中介绍了一种构造方法，在偶数变元的情况下，给出了构造满足严格雪崩准则并且具有较好的全局雪崩特性的平衡布尔函数的方法，这些函数的非线性度可以达到严格几乎最优，并且全局雪崩特性中绝对值指标和平方和指标也都给出了精确的结果.

5）唐灯和张卫国等在文献[72]中通过对 M-M 类函数的修改，得到了一类具有平衡性并且满足严格雪崩准则的布尔函数，和之前的方法相比，他们得到的函数非线性度达到严格几乎最优，并且全局雪崩性质也是目前最好的.

6)张卫国和蒋福强等通过改进文献[73]中的构造,将其推广为弹性,构造出了同时满足弹性和严格雪崩准则的函数,这类布尔函数的非线性度仍然是严格几乎最优的.

上面这些构造分别解决了具有良好自相关性质的高非线性度平衡布尔函数的构造和满足严格雪崩的高非线性度弹性函数的构造问题. 如果考虑函数更高阶的扩散性质时,如何构造此类函数仍然比较困难,值得进一步研究. 前文介绍过平衡布尔函数的最大非线性度界,由于该界比上述一系列文献得到的非线性度值都要大,于是我们有以下公开问题:

问题 8 如何构造非线性度比文献[72－73]中结果更高的具有好的自相关性质的平衡(弹性)布尔函数?

4 结 论

本文对高非线性度弹性密码函数、具有最优代数免疫度的函数及具有良好自相关性质的函数的发展现状进行了综述,对已有的重要结果进行了总结和分析,并给出了一些尚未解决的公开难题. 目前关于满足多种密码学指标折中的密码函数的构造问题虽然已经取得了一系列重要进展,但是还有很多基本问题并没有实质性的突破. 本文给出的问题值得进一步深入研究.

参 考 文 献

[1] Siegenthaler T. Correalation immunity of nonlinear combining functions for cryptographic applications[J]. IEEE Transactions on Information Theory,1984,30(5):776-780.

[2] Xiao G Z and Massey J L. A spectral characterization of correlation-immune combining func- tions[J]. IEEE Transactions on Information Theory,1988,34(3):569-571.

[3] 张卫国,肖国镇. 弹性布尔函数的非线性度的紧上界[M]. 北京:科学出版社,2011:403-405.

[4] Rothaus O S. On bent functions[J]. Journal of Combinatorial Theory,Series A,1976,20:300-305.

[5] Camion P,Carlet C,Charpin P,et al. On correlation-immune functions[C]// Advances in Cryptology-EUROCRYPT 1991. Lecture Notes in Computer Science. Berlin:Springer,1991:86-100.

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

[7] Pasalic E. Maiorana-McFarland class:degree optimization and algebraic properties[J]. IEEE Transactions on Information Theory,2006,52:4581-4594.

[8] Carlet C. A larger class of cryptographic Boolean functions via a study of the Maiorana- McFarland construction[C]// Advances in Cryptology-CRYPTO 2002. Lecture Notes in Computer Science. Berlin:Springer,2002:549-564.

[9] Sarkar P,Maitra S. Construction of nonlinear Boolean functions with important cryptographic properties[C]// Advances in Cryptology-EUROCRYPT 2000,Lecture Notes in Computer Science. Berlin:Springer,2000:485-506.

[10] Maitra S,Pasalic E. Further construction of resilient Boolean functions with very high nonlinea- rity[J]. IEEE Transactions on Information Theory,2006,52:2269-2270.

[11] Seberry J,Zhang X M,Zheng Y L. Nonlinearly balanced Boolean functions and their propagation characteristics[C]// Advances in Cryptology-CRYPTO 1993. Lecture Notes in Computer Science. Berlin:Springer,1993:49-60.

[12] Dobbertin H. Construction of bent functions and balanced boolean functions with high nonlinearity[C]// In Fast Software Encryption. Lecture Notes in Computer Science. Berlin:Springer,1994:61-74.

[13] Maitra S,Pasalic E. A Maiorana-McFarland type construction for resilient Boolean functions on n variables (n even) with nonlinearity$>2^{n-1}-2^{n/2}+2^{n/2-2}$[J]. Discrete Applied Mathematics,2006,154:357-369.

[14] Zhang W G,Xiao G Z. Constructions of almost optimal resilient Boolean functions on large even number of variables[J]. IEEE Transactions on Information Theory,2009,55:5822-5831.

[15] Zhang W G,Pasalic E. Generalized Maiorana-McFarland construction of resilient Boolean func- tions with high nonlinearity and good algebraic properties[J]. IEEE Transactions on Information Theory,2014,60:6681-6695.

[16] Zhang W G,Pasalic E. Improving the lower bound on the maximum nonlinearity of 1-resilient Boolean functions and designing functions satisfying all cryptographic criteria[J]. Information Sciences,2016,376:21-30.

[17] Carlet C. On the coset weight divisibility and nonlinearity of resilient and correlation-Immune functions[J]. Sequences and their Applications,2002. DOI:10.1007/978-1-4471-0673-9_9.

[18] Carlet C,Sarkar P. Spectral domain analysis of correlation immune and resilient Boolean functions[J]. Finite Fields and Their Applications,2002,8(1):120-130.

[19] Chee S C, Lee S L, Kim K K, et al. Correlation immune functions with controllable nonlinearity[J]. Etri Journal, 1997, 19(4): 389-401.

[20] Chee S C, Lee S L, Lee D, et al. On the correlation immune functions and their nonlinearity[C]// Advances in Cryptology-ASIACRYPT '96. Lecture Notes in Computer Science. Berlin: Springer, 1996: 232-243.

[21] Cusick T W. On constructing balanced correlation immune functions[J]. Sequences and their Applications, 1999, 94: 184-190.

[22] Filiol E, Fontaine C. Highly nonlinear balanced Boolean functions with a good correlation- immunity[J]. Lecture Notes in Computer Science, 1998, 1403: 475-488.

[23] Khoo K, Gong G. New constructions for resilient and highly nonlinear Boolean functions[J]. Australasian Conference on Information Security and Privacy, 2003, 2727: 498-509.

[24] Maitra S, Sarkar P. Highly nonlinear resilient functions optimizing Siegenthaler's inequality[C]// Advances in Cryptology-CRYPTO 1999. Lecture Notes in Computer Science. Berlin: Springer, 1999: 198-215.

[25] Pasalic E, Johansson T. Further results on the relation between nonlinearity and resiliency for Boolean functions[M]. Berlin: Springer, 1999: 35-44.

[26] Pasalic E, Maitra S, Johansson T, et al. New constructions of resilient and correlation immune Boolean functions achieving upper bound on nonlinearity[J]. Electronic Notes in Discrete Mathematics, 2001, 6(4): 158-167.

[27] Pasalic E. Degree optimized resilient Boolean functions from Maiorana-McFarland class. Cryptography and Coding[M]. Berlin: Springer, 2003: 93-114.

[28] Sarkar P, Maitra S. Nonlinearity bounds and constructions of resilient Boolean functions[C]// Advances in Cryptology-CRYPTO 2000. Lecture Notes in Computer Science. Berlin: Springer, 2000: 515-532.

[29] Clark J, Jacob J, Stepney S, et al. Evolving Boolean functions satisfying multiple criteria[C]// Progress in INDOCRYPT 2002, Lecture Notes in Computer Science. Berlin: Springer, 2002: 246-259.

[30] Fedorova M, Tarannikov Y V. On the constructing of highly nonlinear resilient Boolean functions by means of special matrices[C]// Progress in Cryptology-INDOCRYPT 2001. Lecture Notes in Computer Science. Berlin: Springer, 2001: 254-266.

[31] Kavut S, Maitra S, Yücel M D. Search for Boolean functions with excellent profiles in the rotation symmetric class[J]. IEEE Transations on Information Theory, 2007, 53(5): 1743-1751.

[32] Millan W, Clark A, Dawson E. An effective genetic algorithm for finding highly nonlinear Boolean functions[C]// In Proceedings of the First International Conference on Information and Communication Security. Lecture Notes in Computer Science. Berlin: Springer, 1997: 149-158.

[33] Millan W, Clark A, Dawson E. Heuristic design of cryptographically strong balanced Boolean functions[C]// Advances in Cryptology-EUROCRYPT'98. Lecture Notes in Computer Scie- nce. Berlin: Springer, 1998: 489-499.

[34] Millan W, Clark A, Dawson E. Boolean function design using hill climbing methods[C]// In Proceedings of the 4th Australasian Conference on Information Security and Privacy. Lecture Notes in Computer Science. Berlin : Springer, 1999: 1-11.

[35] Saber Z, Uddin M F, Youssef A. On the existence of (9, 3, 5, 240) resilient functions[J]. IEEE Transations on Information Theory, 2002, 48(7): 1825-1834.

[36] Sarkar P, Maitra S. Efficient implementation of cryptographically useful large Boolean functions[J]. IEEE Transactions on Computers, 2003, 52(4): 410-417.

[37] Tarannikov Y V. On resilient Boolean functions with maximum possible nonlinearity[C]// In Progress in Cryptology-INDOCRYPT 2000. Lecture Notes in Computer Science. Berlin: Springer, 2001: 19-30.

[38] Tarannikov Y V. New constructions of resilient Boolean functions with maximal nonlinearity[C]// In Workshop on Fast Software Encryption (FSE 2001). Lecture Notes in Computer Science. Berlin: Springer, 2001: 66-77.

[39] Yang J P, Zhang W G, Generating highly nonlinear resilient Boolean functions resistance against algebraic and fast algebraic attacks[J]. Security and Communication Networks, 2015, 8: 1256-1264.

[40] Kavut S, Yücel M D. Generalized rotation symmetric and dihedral symmetric Boolean functions-9 variable Boolean functions with nonlinearity 242[C]//Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, International Symposium, Aaecc-17. Berlin: Springer, 2007: 321-329.

[41] Patterson N J, Wiedemann D H. The covering radius of the $(2^{15}, 6)$ Reed-Muller code is at least 16 276[J]. IEEE Transactions on Information Theory, 1990, 36: 43-43.

[42] Zhang X M, Zheng, Y L. Cryptographically resilient functions[J]. IEEE Transactions on Information Theory, 1997, 43: 1740-1747.

[43] Chabaud F, Vaudenay S. Links between differential and linear cryptanalysis[C]// Advances in Cryptology-EUROCRYPTO 1995. Lecture Notes in Computer Science. Berlin: Springer, 1995: 356-365.

[44] Kurosawa K, Satoh T, Yamamoto K. Highly nonlinear t-resilient functions[J]. Journal of Universal Computer Science, 1997, 3(6): 721-729.

[45] Chen L, Fu F W. On the construction of new resilient functions from old ones[J]. IEEE Transactions on Information Theory, 1999, 45

(6):2077-2082.

[46] Cheon J H. Nonlinear vector resilient functions[C]// In Advances in Cryptology-CRYPTO 2001. Lecture Notes in Computer Science. Berlin:Springer,2001:485-469.

[47] Johansson T,Pasalic E. A construction of resilient functions with high nonlinearity[J]. IEEE Transactions on Information Theory,2003,49:494-501.

[48] Charpin P,Pasalic E. Highly nonlinear resilient functions through disjoint codes in projective spaces[J]. Designs Codes and Cryptography,2005,37(2):319-346.

[49] Niederreiter H,Xing C. Disjoint linear codes from algebraic function fields[J]. IEEE Transactions on Information Theory,2004,50(9):2174-2177.

[50] Pasalic E,Maitra S. Linear codes in generalized construction of resilient functions with very high nonlinearity[J]. IEEE Transactions on Information Theory,2002,48(8):2182-2191.

[51] Li L Y,Zhang W G. Constructions of vectorial Boolean functions with good cryptographic properties[J]. Science China Information Sciences,2016,59(11):119103:1-119103:2.

[52] Zhang W G,Pasalic E. Constructions of resilient S-boxes with strictly almost optimal nonlinearity through disjoint linear codes[J]. IEEE Transactions on Information Theory,2014,60:1638-1651.

[53] Zhang W G,Pasalic E. Highly nonlinear balanced S-boxes with good differential properties[J]. IEEE Transactions on Information Theory,2014,60:7970-7979.

[54] Zhang W G,Li L Y ,Enes P. Construction of resilient S-boxes with higher-dimensional vectorial outputs and strictly almost optimal nonlinearity[J]. IET Information Security. DOI:10.1049/iet-ifs.2016.0168.

[55] Meier W,Pasalic E,Carlet C. Algebraic Attacks and Decomposition of Boolean Functions[C]//In Advances in Cryptology-EUROCRYPT 2004. Lecture Notes in Computer Science,Berlin:Springer,2004:474-491.

[56] Dalai D,Maitra S,Sarkar S. Basic theory in construction of Boolean functions with maximum possible annihilator immunity[J]. Designs Codes and Cryptographic,2006,40(1):41-58.

[57] Qu L J,Feng K Q,Liu F,et al. Constructing Symmetric Boolean Functions With Maximum Algebraic Immunity[J]. IEEE Transactions on Information Theory,2009,55(5):2406-2412.

[58] Li Na,Qi Wen Feng. Symmetric Boolean functions depending on an odd number of variables with maximum algebraic immunity[J]. Information Theory IEEE Transactions on,2006,52(5):2271 -2273.

[59] Carlet C,Gablrit P. On the construction of balanced Boolean functions with a good algebraic immunity[C]// Information Theory(ISIT) 2005. Adelaide:IEEE,2005:1101-1105.

[60] Carlet C,Feng K Q. An infinite class of balanced functions with optimal algebraic immunity,good immunity to fast algebraic attacks and good nonlinearity[C]// Advances in Cryptology-ASIACRYPT 2008,Lecture Notes in Computer Science. Berlin:Springer,2008:425-440.

[61] Tu Z R,Deng Y P. A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity[J]. Designs Codes and Cryptographic,2011,60(1):1-14.

[62] Tu Z R,Deng Y P. Boolean functions optimizing most of the cryptographic criteria[J]. Discrete Applied Mathematics,2012,160:427-435.

[63] Tang D,Carlet C,Tang X. Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks[J]. IEEE Transactions on Information Theory,2012,59(1):653-664.

[64] Webster A F,Tavares S E. On the design of S-boxes[C]// Advance in Cryptology - CRYPTO'85 Lecture Notes in Computer Science. Berlin:Springer,1986:523-534.

[65] Zhang X M,Zheng Y L. GAC-The Criterion for Global Avalanche Characteristics of Cryptogra- phic Functions[J]. Journal for Universal Computer Science,1995,1(5):315-333.

[66] Canteaut A,Carlet C,Charpin P,et al. Propagation characteristics and correlation immunity of highly nonlineaar Boolean functions[C]// Advances in Cryptology-EUROCRYPT 2000. Lecture Notes in Computer Science. Berlin:Springer,2000:507-522.

[67] Stanica P. Nonlinearity,local and global avalanche characteristics of balanced Boolean functions[J]. Discrete Mathematics,2002,248:181-193.

[68] Stanica P,Sung S H. Improving the nonlinearity of certain balanced Boolean functions with good local and global avalanche characteristics [J]. Inform. Process Lett,2001,79,167-172.

[69] Maitra S. Highly nonlinear balanced Boolean functions with good local and global avalanche characteristics[J]. Information Process Letter,2002,83:281-286.

[70] Stanica P,Sung S H. Boolean functions with five controllable cryptographic properties[J]. Designs Codes Cryptographic,2004,31,147-157.

[71] Li L Y,Sun Y J,Zhang W G. Construction of balanced Boolean functions with high nonlinearity,good local and global avalanche characteristics[J]. Frontiers of Mathematics in China,2016,11(2):339-352.

[72] Tang D, Zhang W, Tang X H. Construction of balanced Boolean functions with high nonlinearity and good autocorrelation properties[J]. Designs Codes and Cryptographic, 2013, 67(1): 77-91.

[73] Zhang W G, Jiang F Q, Tang D. Construction of highly nonlinear resilient Boolean functions satisfying strict avalanche criterion[J]. Science China Information Sciences, 2014, 57(4): 1-6.

Constructions of Cryptographic Boolean Functions in Stream Ciphers

Zhang Weiguo[1], Li Luyang[2]

(1. State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China;
2. Key Laboratory of Security Communications, Chengdu 610041, China)

Abstract: Cryptographic functions, including Boolean functions and multiple output Boolean functions, play an important role in block ciphers schemes and certain stream ciphers schemes. Generally, the Boolean functions used in stream ciphers should satisfy several criteria. The widely accepted criteria are high nonlinearity, balancedness, correlation immunity, high algebraic degree, good algebraic immunity and so on. In this paper, we present a survey on the recent progress on constructing resilient functions with high nonlinearity. Boolean functions with optimal algebraic immunity or good autocorrelation properties are also discussed. In addition, some open problems are presented in this paper.

Keywords: stream cipher; Boolean functions; nonlinearity; resiliency; algebraic immunity; autocorrelation property

[责任编辑　陈留院]