具有最大代数免疫度的布尔函数的构造

熊晓雯[1] 屈龙江[1,2] 李 超[1]
(国防科技大学理学院数学与系统科学系 长沙 410073)[1]
(东南大学移动通信国家重点实验室 南京 210096)[2]

摘 要 系统地总结了现有的具有最大代数免疫度的布尔函数的构造方法,将现有各种构造方法按其构造思想的不同分为有代表性的几类,并分别介绍了基于这几类方法的一些结果和进展,其中包括作者自己在该方面的研究结果。

关键词 布尔函数,代数攻击,代数免疫度,最优性构造
中图法分类号 TP981 **文献标识码** A

Construction of Boolean Function with Maximum Algebraic Immunity

XIONG Xiao-wen[1] QU Liong-jiang[1,2] LI Chao[1]
(Department of Mathematics and System Science, College of Science, National University of Defence Technology, Changsha 410073, China)[1]
(State Key Laboratory of Mobile Communication, Southeast University, Nanjing 210096, China)[2]

Abstract In this survey paper, we reviewed the recent constructions of Boolean functions with maximum algebraic immunity(MAI), and classifeid those into several different classes by the construction idea. Further, we also presented some results and developments of these methods, including some results of the authors.

Keywords Boolean functions, Aalgebraic attacks, Algebraic immunity, Optimal construction

1 预备知识

布尔函数作为序列密码、分组密码和Hash函数中的重要组件,其密码学性质的好坏直接关系到密码算法的安全性。2003年以前,针对线性攻击、差分攻击、相关攻击等各种攻击方式,人们提出了多种布尔函数的密码学指标,如平衡性、非线性度、相关免疫度、弹性等等。2003年,Courtois, Armknecht等人提出和发展了一种新的攻击方式——代数攻击,它成功地攻击了许多流密码算法,受到了密码学界的高度关注[1-4]。代数攻击的提出与发展为布尔函数提供了一个新的密码学指标:代数免疫度(Algebraic Immunity, AI)[5]。为了抵抗代数攻击,密码算法中使用的布尔函数必须具有较大的代数免疫度。因此,具有较大代数免疫度,尤其是最大代数免疫度的布尔函数的构造就引起了人们的关注,得到众多研究[6-27]。

设F_2是二元域,F_2^n是F_2上的n维向量空间,一个n元布尔函数f是从F_2^n到F_2上的一个映射。n元布尔函数全体记作B_n。一个n元布尔函数f可以唯一地表示为

$$f(x_1,\cdots,x_n)=a_0+\sum_{i=1}^{n}a_ix_i+\sum_{1\leqslant i<j\leqslant n}a_{i,j}x_ix_j+\cdots+\sum_{1\leqslant i_1<\cdots<i_d\leqslant n}a_{i_1,\cdots,i_d}x_{i_1}\cdots x_{i_d}+\cdots+a_{1,\cdots,n}x_1x_2\cdots x_n$$

式中,$a_0,a_i,a_{i,j},\cdots,a_{1,\cdots,n}\in F_2$。$f$的这种表示形式称之为$f$的代数正规型,其系数非零项所含有的最多的变元个数称为代数次数,记为$\deg(f)$。代数次数小于等于1的布尔函数称为仿射函数。如果一个布尔函数的取值在输入变元置换下保持不变,则称之为对称布尔函数(Symmetric Boolean Function, SBF)。设$f\in B_n$,$x=(x_1,\cdots,x_n)\in F_2^n$,如果对$0\leqslant k\leqslant n-1$总有下式成立:$f(\rho_n^k(x_1,\cdots,x_n))=f(\rho_n^k(x_1),\cdots,\rho_n^k(x_n))=f(x_1,\cdots,x_n)$,其中

$$\rho_n^k(x_i)=\begin{cases}x_{i+k}, & i+k\leqslant n\\ x_{i+k-n}, & i+k>n\end{cases}$$

那么就称f为循环对称布尔函数(Rotation Symmetric Boolean Function, RSBF)。

n元布尔函数f的支撑集定义为$\mathrm{supp}(f)=\{x\in F_2^n\mid f(x)=1\}$。支撑集$\mathrm{supp}(f)$所含的元素个数称为$f$的Hamming重量,记为$wt(f)$。若$wt(f)=2^{n-1}$,则称$n$元布尔函数$f$是平衡的。两个$n$元布尔函数$f$和$g$的Hamming距离定义为$wt(f+g)$。

对给定的布尔函数$f(x)\in B_n$,$\alpha\in F_2^n$,令$W_f(\alpha)=\sum_{x\in F_2^n}(-1)^{f(x)\oplus x\cdot\alpha}$,则$W_f(\alpha)$称为函数$f(x)$在点$\alpha$的Walsh变换。布尔函数$f$的非线性度$NL(f)$是$f$和所有仿射函数的最小汉明距离,即有

$$NL(f)=\min_{g\in B_n,\deg g\leqslant 1}d(f,g)=2^{n-1}-\frac{1}{2}\max_{\alpha\in F_2^n}|W_f(\alpha)|$$

到稿日期:2010-03-05 返修日期:2010-05-18 本文受国家自然科学基金(60803156),东南大学移动通信国家重点实验室开放研究基金(W200807)资助。

熊晓雯(1985-),女,硕士,主要研究方向为编码密码理论及其应用,E-mail:winnie101206@126.com;屈龙江(1980-),男,博士,讲师,主要研究方向为编码密码理论及其应用;李 超(1966-),男,博士,教授,主要研究方向为编码密码理论及其应用。

对 $f\in B_n$，f 的零化子为集合：

$$\mathrm{Ann}(f)=\{g\in B_n \mid f\cdot g=0\}$$

那么 f 的代数免疫度定义为：

$$AI(f)=\min\{\deg(g)\mid 0\neq g\in \mathrm{Ann}(f)\cup \mathrm{Ann}(1+f)\}$$

由 $f(1+f)=f+f^2=0$ 知，对每个 $0\neq f\in B_n$，$AI(f)\leqslant \deg(f)$。另一方面，可以证明：如果 f 是一个 n 元布尔函数，那么 $AI(f)\leqslant\left\lceil\frac{n}{2}\right\rceil$[2,5]。构造代数免疫度较大的布尔函数，特别是构造达到上界 $AI(f)=\left\lceil\frac{n}{2}\right\rceil$ 的 n 元布尔函数就成为了研究布尔函数代数免疫性的重点问题之一。在过去的几年里，人们已经提出了一些关于构造具有最大代数免疫度(Maximum Algebraic Immunity，MAI)的布尔函数的方法。本文系统地总结了现有的具有最大代数免疫度的布尔函数的构造方法，将现有各种构造方法按其构造思想的不同分为有代表性的几类，并分别介绍了基于这几类方法的一些结果和进展。

2 MAI 函数的构造方法

2.1 基于支撑包含关系的构造方法

Dalai 于 2005 年提出了一种基于支撑包含关系的 MAI 函数的构造方法[6]，其主要思想来自以下引理：

引理 1[6] 设 $f,f_1,f_2\in B_n$ 满足如下条件：

(1) f_1,f_2 没有次数低于 $\left\lceil\frac{n}{2}\right\rceil$ 的非零零化子；

(2) $\mathrm{supp}(f)\supseteq\mathrm{supp}(f_2)$，$\mathrm{supp}(f+1)\supseteq\mathrm{supp}(f_1)$，则有 $AI(f)=\left\lceil\frac{n}{2}\right\rceil$。

由代数免疫度的定义，易知引理 1 成立。下面是基于该思想构造的函数：

构造算法 1[6] 设 $f\in B_n$，当 n 为奇数时，令

$$f(x)=\begin{cases}0, & wt(x)<\left\lceil\frac{n}{2}\right\rceil\\ 1, & wt(x)\geqslant\left\lceil\frac{n}{2}\right\rceil\end{cases}$$

当 n 为偶数时，令

$$f(x)=\begin{cases}0, & wt(x)<\left\lceil\frac{n}{2}\right\rceil\\ 1, & wt(x)>\left\lceil\frac{n}{2}\right\rceil\\ b\in\{0,1\}, & wt(x)=\left\lceil\frac{n}{2}\right\rceil\end{cases}$$

定理 1[6] 构造算法 1 中给出的两类布尔函数均为 MAI 函数。

在构造算法 1 中，对任意正整数 n，考虑 $g(x)=\begin{cases}0, & wt(x)<\left\lceil\frac{n}{2}\right\rceil\\ 1, & wt(x)\geqslant\left\lceil\frac{n}{2}\right\rceil\end{cases}$，由于 $g(x)=1$ 当且仅当其输入变元中至少有一半取值为 1，因此 $g(x)$ 也被称为择多逻辑函数(Majority Function)。由定理 1 可知，择多逻辑函数 $g(x)$ 是 MAI 函数。

具有 MAI 的对称布尔函数得到了较多研究[7-11]。研究具有 MAI 的对称布尔函数(SBF)的一种主要方法就是考查其“重量支撑”。当 n 为奇数时，屈龙江等证明了：具有 MAI 的 n 元 SBF 有且仅有择多逻辑函数 $g(x)$ 和 $g(x)+1$[7]；当 n 为偶数时，具有 MAI 的 n 元 SBF 有很多，An. Braekn 和屈龙江等在文献[8,9]中分别给出了一些构造。当 $n=2^m$ 时，屈龙江等给出了 n 元 SBF 具有 MAI 的一系列必要条件，并猜测该系列必要条件事实上已构成充分条件[10]。屈龙江和 Braeken 等的工作的一个重要思想是：若 f 为具有 MAI 的 n 元 SBF，

$$S_n=\{hp\mid h\in SB_m,p(x)=(x_{m+1}+x_{m+2})\cdots(x_{n-1}+x_n),$$
$$1\leqslant m\leqslant n,1\leqslant\deg h\leqslant\left\lfloor\frac{n}{2}\right\rfloor-\frac{n-m}{2}\}$$

则 f 不能被 S_n 中的函数零化[7,8,10]。刘峰等进一步指出，f 不能被 S_n 中函数零化，事实上已经是 $AI(f)=\left\lceil\frac{n}{2}\right\rceil$ 的充要条件，由此证实了文献[10]中的猜想[11]。

2.2 基于平面理论的构造方法

Carlet 在 2006 年提出了一种基于平面理论的 MAI 函数的构造方法[12]。使用该方法，他给出了构造平衡 MAI 布尔函数的两个新算法。其主要思想来自于以下命题：

命题 1[12] 设 $f\in B_n$，$k\leqslant\left\lceil\frac{n}{2}\right\rceil$，如果存在一系列维数至少为 k 的平面 $A_i(1\leqslant i\leqslant r)$(也就是 F_2^n 的仿射子空间)，使得下列条件成立：

(1) $\forall i\leqslant r,|A_i\backslash(\mathrm{supp}(f)\cup\bigcup_{j<i}A_j)|\leqslant 1$，

(2) $(F_2^n\backslash\mathrm{supp}(f))\subseteq\bigcup_{i\leqslant i}A_i$，

那么 f 不存在次数小于 k 的非零零化子。

命题 1 的成立是基于这样一个事实：设 $g\in B_n$，$degg\leqslant k$，若 g 在一个维数至少为 k 的平面上除去一点外的其余点取值均为零，则 g 在该平面上恒为零。

由命题 1，根据 n 的奇偶性不同，可以得到以下的两个推论以及分别的构造方法。

推论 1[12] 设 n 为奇数，对任意整数 $1\leqslant i\leqslant 2^{n-1}$，令 A_i 为 F_2^n 的维数至少为 $\frac{n+1}{2}$ 的仿射子空间，且满足 $A_i\backslash\bigcup_{t<i}A_t$ 非空，任取元素 $b_i\in A_i\backslash\bigcup_{t<i}A_t$，构造布尔函数 f，使得 $\mathrm{supp}(f)=\{b_i\mid 1\leqslant i\leqslant 2^{n-1}\}$(或者为其支撑集的补集)，则 f 为平衡 MAI 函数。

构造算法 2[12](n 为奇数)

Step1 记 $a_1,a_2,\cdots,a_{2^{n-1}}$ 为 F_2^n 中所有重量大于 $\frac{n}{2}$ 的点，且按重量升序排列，相同重量时可以随意排列；

Step2 从 $i=1$ 到 2^{n-1} 选取点 b_i，使得 $\mathrm{supp}(b_i)\subseteq\mathrm{supp}(a_i)$，且对任意的 $j<i$，$\mathrm{supp}(b_i)\nsubseteq\mathrm{supp}(a_j)$；

Step3 输出 n 元布尔函数 f，使得 $\mathrm{supp}(f)=\{b_i\mid 1\leqslant i\leqslant 2^{n-1}\}$，则 $\mathrm{AI}(f)=\frac{n+1}{2}$。

构造算法 2 中的集合 $\{b_i\}$ 是存在的，特别可以取 $b_i=a_i$。实际上，当 a_i 的重量超过 $\frac{n+1}{2}$ 时，必有 $b_i=a_i$，否则，必存在某个 $j<i$，使得 $\mathrm{supp}(b_i)\subseteq\mathrm{supp}(a_j)$。由推论 1 可知构造算法 2 中的布尔函数显然为 MAI 函数。而且所构造布尔函数的支撑集实际上就是由所有重量不低于 $\frac{n+3}{2}$ 的点以及 $C_n^{\frac{n+1}{2}}$ 个重量不超过 $\frac{n+1}{2}$ 的点组成的。

推论 2[12] 设 n 为偶数，令 $A=\{a_1,a_2,\cdots,a_{C_n^{\frac{n}{2}}}\}$ 为 F_2^n 上所有重量为 $\frac{n}{2}$ 的点的一个有序集合，对任意的 $1\leqslant i\leqslant C_n^{\frac{n}{2}}$，定义平面 $A_i=\{x\in F_2^n\mid \mathrm{supp}(a_i)\subseteq\mathrm{supp}(x)\}$，$B_i=\{x\in F_2^n\mid \mathrm{supp}(x)\subseteq\mathrm{supp}(a_i)\}$，设 I,J,K 为 A 的 3 个互不相交的子集，并且满足：对任意 $i\in I$，存在某个点 $b_i\neq a_i$ 且 $b_i\in(A_i\setminus\bigcup_{t\in I,t<i}A_t)$；对任意 $i\in J$，存在某个点 $c_i\neq a$ 且 $c_i\in(B_i\setminus\bigcup_{t\in J,t<i}B_t)$，则支撑集为 $\{x\in F_2^n\mid wt(x)>\frac{n}{2}\}\cup\{c_i,i\in J\}\cup\{a_i,i\in I\cup K\}\setminus\{b_i,i\in I\}$ 的布尔函数 f 的代数免疫度为 $\frac{n}{2}$。

构造算法 3[12]（n 为偶数）

Step1 选择两个正整数 $k\leqslant l\leqslant C_n^{\frac{n}{2}}$；

Step2 对 i 从 1 到 k，选取 $a_i\in F_2^n$，使得其重量为 $\frac{n}{2}$，且与 $a_1,\cdots,a_{i-1}$ 不同，选取向量 b_i，使得 $\mathrm{supp}(a_i)\subseteq\mathrm{supp}(b_i)$，且对任意的 $j<i$，$\mathrm{supp}(a_j)\not\subseteq\mathrm{supp}(b_i)$；

Step3 对 i 从 $k+1$ 到 l，选取 $a_i\in F_2^n$，使得其重量为 $\frac{n}{2}$，且与 $a_1,\cdots,a_{i-1}$ 不同，选取向量 c_i，使得 $\mathrm{supp}(c_i)\subseteq\mathrm{supp}(a_i)$，且对任意的 $k+1\leqslant j<i$，$\mathrm{supp}(c_i)\not\subseteq\mathrm{supp}(a_j)$；

Step4 输出布尔函数 f，其支撑集恰为 $\{x\in F_2^n\mid wt(x)>\frac{n}{2}\}\cup\{c_i,i=k+1,\cdots,l\}\cup\{a_i,i=1,\cdots,k\}\setminus\{b_i,i=1,\cdots,k\}$，则 $AI(f)=\frac{n}{2}$。

构造算法 3 相当于在推论 2 中取 $I=\{1,2,\cdots,k\}$，$J=\{k+1,k+2,\cdots,l\}$，K 为空集。由推论 2，显然构造出的布尔函数 f 的代数免疫度为 $\frac{n}{2}$，而且 f 的重量为

$$2^{n-1}-\frac{1}{2}C_n^{\frac{n}{2}}+l-k+|\{b_i\mid wt(b_i)=\frac{n}{2},i=1,2,\cdots,k\}|$$

通过选取合适的参数，可以使得构造的函数 f 为平衡的。

使用基于平面理论的构造方法，Carlet、曾祥勇等进一步构造了几类新的具有 MAI 的平衡函数，并且构造函数的非线性度远高于其它已有构造[13]。通过选取适当的 I,J,K，当 $n\geqslant 8$ 为偶数时，构造函数的非线性度为 $2^{n-1}-C_{n-1}^{\frac{n}{2}-1}+2C_{n-2}^{\frac{n}{2}-2}/(n-2)$；当 n 为奇数时，构造函数的非线性度为 $C_{n-1}^{\frac{n-1}{2}}+\delta(n)$，其中 $\delta(n)$ 为随 n 取值增加而迅速增长的函数[13]。王永娟等推广了推论 1，当 n 为奇数时，构造了一类具有 MAI 的 n 元布尔函数。另外，当 n 为偶数时，构造了一类平衡的 n 元 MAI 布尔函数，并且给出了此时的一个计数下界 $M\geqslant 2(\prod_{k=1}^{n/2}(2^k-1)^{l_k})^2$[14]。付绍静等基于平面理论的构造方法研究了偶数元循环对称布尔函数，构造了一类具有最大代数免疫度的 RSBF 函数，并且证明了所构造的这类 RSBF 函数具有更高的非线性度：$NL(f)\geqslant 2^{n-1}-\frac{1}{2}C_n^{n/2}$[15]。

2.3 基于交换基技术的构造方法

为了介绍这种构造方法，首先引入几个记号和一个引理。

给定一个 $f\in B_n$ 和一个正整数 $d\leqslant n$，设 $\mathrm{supp}(f)=\{X_1,\cdots,X_{wt(f)}\}$，$F_2^n\setminus\mathrm{supp}(f)=\{X_{wt(f)+1},\cdots,X_{2^n}\}$。对 $X=(x_1,\cdots,x_n)\in F_2^n$，令 $v_d(X)=(1,x_1,\cdots,x_n,x_1x_2,\cdots,x_{n-1}x_n,\cdots,x_1\cdots x_d,\cdots,x_{n-d+1}\cdots x_n)$。记向量组 $\{v_d(X_1),\cdots,v_d(X_{wt(f)})\}$ 为 $S_{1,d}(f)$，$\{v_d(X_{wt(f)+1}),\cdots,v_d(X_{2^n})\}$ 为 $S_{0,d}(f)$。

设 $g\in B_n$，$\deg g\leqslant d$ 为 f 的一个零化子，其代数正规型为

$$g(x_1,\cdots,x_n)=g_0+\sum_{i=1}^{n}g_ix_i+\sum_{1\leqslant i<j\leqslant n}g_{i,j}x_ix_j+\cdots+\sum_{1\leqslant i_1<\cdots<i_d\leqslant n}g_{i_1,\cdots,i_d}x_{i_1}\cdots x_{i_d}$$

由于 $fg=0$，从而若 $f(x)=1$，则有 $g(x)=0$。由此可以得到关于 g 的代数正规型系数的方程 $g(x)=0$，建立一个有 $\sum_{i=0}^{d}\binom{n}{i}$ 个变元和 $wt(f)$ 个方程的线性方程组。则容易看出方程组系数矩阵的行向量组即为 $S_{1,d}(f)$，于是 f 没有代数次数小于等于 d 次的非零零化子等价于该方程组只有零解，该方程组只有零解又等价于 $S_{1,d}(f)$ 为 $\sum_{i=0}^{d}\binom{n}{i}$ 维向量空间 $F_2^{\sum_{i=0}^{d}\binom{n}{i}}$ 的生成集。考虑到 $1+f$，则有类似的结论，只是 $S_{1,d}(f)$ 应该换成 $S_{0,d}(f)$。当 $d=\left\lceil\frac{n}{2}\right\rceil-1$ 时，记 $S_1(f)=S_{1,\lceil\frac{n}{2}\rceil-1}(f)$，$S_0(f)=S_{0,\lceil\frac{n}{2}\rceil-1}(f)$，于是有：

引理 2[16] 设 $f\in B_n$，则 $AI(f)>d$ 当且仅当 $S_{1,d}(f)$ 和 $S_{0,d}(f)$ 均为 $\sum_{i=0}^{d}\binom{n}{i}$ 维向量空间 $F_2^{\sum_{i=0}^{d}\binom{n}{i}}$ 的生成集。特别地，f 为 MAI 函数当且仅当 $S_1(f)$ 和 $S_0(f)$ 均为 $\sum_{i=0}^{\lceil\frac{n}{2}\rceil-1}\binom{n}{i}$ 维向量空间 $F_2^{\sum_{i=0}^{\lceil\frac{n}{2}\rceil-1}\binom{n}{i}}$ 的生成集。

基于交换基技术的构造方法的主要思想是[8]：取一个 n 元 MAI 函数 f，则由引理 2 知 $S_1(f)$ 和 $S_0(f)$ 均为向量空间 $F_2^{\sum_{i=0}^{\lceil\frac{n}{2}\rceil-1}\binom{n}{i}}$ 的生成集。交换 $S_1(f)$ 和 $S_0(f)$ 之间的部分元素就会得到两个新集合，这两个新集合可以看成某个新函数 g 的 $S_1(g)$ 和 $S_0(g)$。从而如果两个新集合仍是向量空间 $F_2^{\sum_{i=0}^{\lceil\frac{n}{2}\rceil-1}\binom{n}{i}}$ 的两个生成集，则新函数 g 也具有最大代数免疫度。

下面关于向量空间的两个结论是基于交换基技术的构造方法的理论基础：

引理 3[16] 设 U 为一个 m 维向量空间，$\alpha_1,\alpha_2,\cdots,\alpha_m$ 和 $\beta_1,\beta_2,\cdots,\beta_m$ 为 U 的两组基，则对于任意整数 $1\leqslant k\leqslant m$，任取 k 个整数 $1\leqslant i_1<i_2<\cdots<i_k\leqslant m$，总存在 k 个整数 $1\leqslant j_1<j_2<\cdots<j_k\leqslant m$，使得 $\{\alpha_1,\alpha_2,\cdots,\alpha_m\}\cup\{\beta_{j_1},\cdots,\beta_{j_k}\}\setminus\{\alpha_{i_1},\cdots,\alpha_{i_k}\}$ 和 $\{\beta_1,\beta_2,\cdots,\beta_m\}\cup\{\alpha_{i_1},\cdots,\alpha_{i_k}\}\setminus\{\beta_{j_1},\cdots,\beta_{j_k}\}$ 仍为 U 的两组基。

进一步，可以得到一个广义的结论：

引理 4[16] 设 U 为一个 m 维向量空间，整数 $m\leqslant s\leqslant t$，$A=\{\alpha_1,\cdots,\alpha_s\}$ 和 $B=\{\beta_1,\cdots,\beta_t\}$ 为 U 的两个生成集。设 $\{\alpha_{i_1},\cdots,\alpha_{i_k}\}(1\leqslant i_1<\cdots<i_k\leqslant s)$ 为 A 的任一子集，r 为 $\{\alpha_{i_1},\cdots,\alpha_{i_k}\}$ 的秩，则对任意整数 $l(r\leqslant l\leqslant t+r-m)$，总存在 B 中的 l 个元素 $\beta_{j_1},\cdots,\beta_{j_l}(1\leqslant j_1<\cdots<j_l\leqslant t)$，使得 $A\cup\{\beta_{j_1},\cdots,\beta_{j_l}\}\setminus\{\alpha_{i_1},\cdots,\alpha_{i_k}\}$ 和 $B\cup\{\alpha_{i_1},\cdots,\alpha_{i_k}\}\setminus\{\beta_{j_1},\cdots,\beta_{j_l}\}$ 仍为 U 的两个生成集。

由引理 3 和引理 4，依据输入变元个数为奇数或偶数，可以分别给出构造 MAI 函数的一个有效方法。

构造算法 4[16] 设 $n=2t+1$，$f\in B_n$，$AI(f)=t+1$，且

$\mathrm{supp}(f)=\{X_1,\cdots,X_{wt(f)}\}$，$F_2^n\backslash\mathrm{supp}(f)=\{X_{wt(f)+1},\backslash ldots,X_{2^n}\}$，记 $S_1(f)$ 为 $2^{n-1}\times 2^{n-1}$ 的矩阵，其行向量为 $v(X_1),\cdots,v(X_{2^{n-1}})$；记 $S_0(f)$ 为 $2^{n-1}\times 2^{n-1}$ 的矩阵，其行向量为 $v(Y_1),\cdots,v(Y_{2^{n-1}})$。

Step1　随机选择一个整数 $1\leqslant k\leqslant 2^{n-1}$ 和 k 个整数 $1\leqslant i_1<\cdots<i_k\leqslant 2^{n-1}$；

Step2　对矩阵 $P=S_1(f)S_0(f)^{-1}$ 的第 $i_1,\cdots,i_k$ 行构成的 $k\times 2^{n-1}$ 矩阵的列向量做高斯约化，找到一组整数 $1\leqslant j_1<\cdots<j_k\leqslant 2^{n-1}$ 使得 $k\times k$ 矩阵 $D_P\begin{pmatrix}i_1,\cdots,i_k\\ j_1,\cdots,j_k\end{pmatrix}$ 可逆。那么可以如下构造函数：

$$f_{(i_1,\cdots,i_k;j_1,\cdots,j_k)}(X)=\begin{cases}f(X)\oplus 1, & \text{若 } X\in\{X_{i_1},\cdots,X_{i_k},Y_{j_1},\cdots,Y_{j_k}\}\\ f(X), & \text{其它情形}\end{cases}$$

构造算法 5[16]　设 $n=2t$，$f\in B_n$，$AI(f)=t$，且 $\mathrm{supp}(f)=\{X_1,\cdots,X_{wt(f)}\}$，$F_2^n\backslash\mathrm{supp}(f)=\{X_{wt(f)+1},\cdots,X_{2^n}\}$，其中 $\sum_{i=0}^{t-1}\binom{n}{i}\leqslant s\leqslant t$，且 $s+t=2^n$。记 E 为 $\sum_{i=0}^{t-1}\binom{n}{i}$。

Step1　随机选择一个整数 $k(0<k\leqslant s)$ 和 k 个向量 $v(X_{i_1}),v(X_{i_2}),\cdots,v(X_{i_k})(1\leqslant i_1<i_2<\cdots<i_k\leqslant s)$。

Step2　对向量组 $\{v(X_{i_1}),v(X_{i_2}),\cdots,v(X_{i_k})\}$ 找到一个极大线性无关组，然后把它扩充到一个集合 $A=\{v(X_{i_{l_1}}),v(X_{i_{l_2}}),\cdots,v(X_{i_{l_r}}),v(X_{i_{k+1}}),v(X_{i_{k+2}}),\cdots,v(X_{i_{E+k-r}})\}$，使得 A 为 $\mathbb{F}_2^E$ 的一个生成集。

Step3　对向量组 $\{v(Y_1),v(Y_2),\cdots,v(Y_t)\}$ 做高斯约化，找到 $\mathbb{F}_2^E$ 的一个生成集 $B=\{v(Y_{j_1}),v(Y_{j_2}),\cdots,v(Y_{j_E})\}$。

Step4　仍用 A 表示用它们中向量作行向量所得的矩阵，设 $P=AB^{-1}$，找到整数 $1\leqslant m_1<m_2<\cdots<m_r\leqslant E$，使得 $\det(D_P\begin{pmatrix}1,\cdots,r\\ m_1,\cdots,m_r\end{pmatrix})\neq 0$ 且 $\det(M_P\begin{pmatrix}1,\cdots,r\\ m_1,\cdots,m_r\end{pmatrix})\neq 0$。

Step5　对任意的 $w(0\leqslant w\leqslant t-E)$，随机选择 w 个整数的集合 $\{j_{E+1},\cdots,j_{E+w}\}\subseteq\{1,2,\cdots,t\}\backslash\{j_1,\cdots,j_E\}$，则可以如下构造函数 $g=f_{(i_1,\cdots,i_k;j_{m_1},\cdots,j_{m_r},j_{E+1},\cdots,j_{E+w})}$：

$$g(X)=\begin{cases}f(X)\oplus 1, & \text{若 } X\in\{Y_{j_{m_1}},\cdots,Y_{j_{m_r}},Y_{j_{E+1}},\cdots,Y_{j_{E+w}},X_{i_1},\cdots,X_{i_k}\}\\ f(X), & \text{其它情形}\end{cases}$$

定理 2[16]　构造算法 4 和算法 5 中的函数均有最大代数免疫度。进一步，当 n 为奇数时，任意一个 n 元具有 MAI 的布尔函数均可以通过构造算法 4 构造出。

另外，文献[16]中还讨论了上述构造函数的密码学性质，包括平衡性、代数次数等性质；最后给出了该类函数的一个计数下界，它不同于以往关于该值的概率性结果，这是目前关于该值的第一个确定性理论结果。

定理 3[16]　设 $S_n=\{f\in B_n\mid AI(f)=\lceil\frac{n}{2}\rceil\}$，$T_n=\{f\in B_n\mid AI(f)=\lceil\frac{n}{2}\rceil$，$f$ 是平衡函数$\}$，

(1)若 n 为奇数时，则 $|S_n|=|T_n|\geqslant 2^{2^{n-1}}$；

(2)若 n 为偶数时，则 $|S_n|\geqslant 2^{2^{n-1}+\frac{1}{2}C_n^{\frac{n}{2}}}$，$|T_n|\geqslant C_{C_n^{\frac{n}{2}}}^{\frac{1}{2}C_n^{\frac{n}{2}}}2^{2^{n-1}-\frac{1}{2}C_n^{\frac{n}{2}}}$。

许多学者对基于交换基技术的 MAI 函数构造方法进行了进一步的研究。李娜等研究了 n 为奇数时矩阵 $P=S_1(f)S_0(f)^{-1}$ 的性质，构造了几类奇数元高非线性度的一阶弹性 MAI 函数[17]。Sarkar 等[18]和李春雷等[19]利用该方法研究了奇数元 RSBF，构造了几类非线性度更高的具有最大代数免疫度的 RSBF 函数。刘美成等构造了 n 为偶数时的一个矩阵 M，通过研究 M 的性质提出了一个判定 MAI 函数的充要条件，并给出了几类构造[20]。

2.4　基于有限域表示的构造方法

2008 年 Carlet C. 和冯克勤提出了一种新的具有 MAI 的布尔函数的构造方法[21]。他们的构造方法使用了有限域 F_{2^n} 上的乘法群表示，我们称之为“基于有限域表示的构造方法”。该方法简洁优美，构造的函数性质优良。

首先回顾一下有限域的乘法群表示：有限域 F_q 的乘法群为循环群，即存在一个元素 α，称为 F_q 的一个本原元，使得 $F_q=\{0\}\cup\{\alpha^i;i=0,1,\cdots,q-2\}$。

定理 4[21]　设 $n\geqslant 2$ 为一整数，α 为 F_{2^n} 上的一个本原元，f 为 F_{2^n} 上支撑为 $\{0\}\cup\{\alpha^i;i=0,1,\cdots,2^{n-1}-2\}$ 的布尔函数，则 f 具有最大代数免疫度 $\lceil\frac{n}{2}\rceil$。

上述定理事实上证明了：若一个非零布尔函数的单变量表示中含有至多 2^{n-1} 个非零系数，则它不可能为 f 的零化子。

文献[21]中证明了定理 4 中所构造函数的代数次数为 $n-1$，其达到了平衡函数的最大代数次数，它的非线性度 $NL(f)\geqslant 2^{n-1}+\frac{2^{\frac{n}{2}+1}}{\pi}\ln(\frac{\pi}{4(2^n-1)})-1\approx 2^{n-1}-\frac{2\ln 2}{\pi}n2^{\frac{n}{2}}$，优于已知的其它具有 MAI 的布尔函数。尽管通过证明得到的下界并不能充分说明该类函数具有很好的非线性度，但通过具体计算的例子，可以发现它们的非线性度是相当好的。另外，文献[21]中指出在特定条件下，该类函数对快速代数攻击具有相当好的免疫性。特别地，当 $n=9$ 时的情形是最优的，这是第一次发现对快速代数攻击具有 MAI 的布尔函数。

利用有限域表示的构造方法，涂自然给出了当 n 为偶数时，构造具有 MAI 的平衡布尔函数的一种方法[22]：他提出了一个组合猜想，在基于该猜想成立的前提下，找到了一个 Partial-Spread 函数类的子类，其代数免疫度和非线性度都达到最高，并把它修改成了平衡函数，这种函数同时具有最大的代数免疫度、最高的代数次数 $n-1$ 和到目前为止所有已知偶数变元的布尔函数中最高的非线性度 $NL(f)\geqslant 2^{n-1}-2^{\frac{n}{2}-1}+2^{\frac{k}{2}}k\cdot\ln 2-1$。

2.5　其它构造

除了上述 4 种典型的构造方法外，构造 MAI 布尔函数还有以下的两类方法：递归构造法和区间差值法。

Dalai 等在文献[23,24]中给出了首个具有 MAI 的函数构造，这是一种复杂的二阶迭代构造法，基本思想是从一个 $AI=1$ 的 $n-2d$ 元布尔函数出发，不断扩充变元数，最后得到一个 n 元函数，其 $AI\geqslant d+1$，由此构造具有 MAI 的布尔函数。遗憾的是，该构造函数并不平衡，且非线性度很弱。付绍静等利用该思想，推广了文献[23,24]中的构造方法，给出了一类 MAI 布尔函数[25]。另外，文献[25]中还给出了奇数元情形时的一种新的二阶递归构造方法，构造了一类奇数元 MAI 布尔函数。陈银东等提出了一阶递归构造 MAI 布尔函

数的方法，这是MAI布尔函数的首个一阶递归构造法，表现了不同奇偶性变元数量的MAI布尔函数之间的关系[26]。另外，由一阶递归构造法可以递推出任意阶的递归构造法，因而该方法在递归构造法中具有特殊意义。

董德帅等利用区间插值的思想，给出了构造达到最大代数免疫度布尔函数的两个算法[27]。其中算法1构造出的布尔函数在偶数情形下是不平衡的。而算法2改进了偶数时的构造，使得此时构造出的布尔函数也是平衡的。其次，作者讨论了所构造的布尔函数的计数问题，给出了算法1的具体的计数结果，而对算法2，给出了其计数问题的上下界。最后，作者给出了布尔函数代数次数达到 $n-1$ 的一个简单充要条件，利用该条件，可使得所构造的布尔函数代数次数达到最优。

结束语 代数免疫度的概念提出后，构造具有最大代数免疫度的布尔函数就受到了许多学者的关注。虽然关于具有最大代数免疫度的构造研究已经取得了不少进展，但是仍然有很多需要进一步研究的地方，例如：关于MAI布尔函数的计数问题，以及布尔函数的弹性性质方面的结果并不是很丰富；现有的构造方法虽然很多，但是如何提高已有方法的构造效率也是一个问题；在构造具有最大代数免疫度的布尔函数的同时，也需要兼顾其它密码学性质，比如说如何使所构造出的布尔函数同时具有更高的非线性度等等。另外，我们也可以考虑具有次优代数免疫度的布尔函数的构造。若次优代数免疫度的函数能够避免太特殊的结构，则在密码学上它可能比具有最优代数免疫度的布尔函数更有价值。

参 考 文 献

[1] Armknecht F. Improving fast algebraic attacks: FSE 2004[C]// LNCS 3017. Springer Verlag, 2004: 65-82

[2] Courtois N, Meier W. Algebraic attacks on stream ciphers with linear feedback: Cryptology-EUROCRYPT 2003[C]// LNCS 2656. Springer Verlag, 2003: 345-359

[3] Courtois N. Fast algebraic attacks on stream ciphers with linear feedback: Cryptology-CRYPTO 2003[C]//LNCS 2729. Springer Verlag, 2003: 176-194

[4] Batten L M. Algebraic attacks over GF(q): Cryptology-INDOCRYPT 2004[C]//LNCS 3348. Springer Verlag, 2004: 84-91

[5] Meier W, Pasalic E, Carlet C. Algebraic attacks and decomposition of Boolean functions: Cryptology-EUROCRYPT 2004[C]// LNCS 3027. Springer Verlag, 2004: 474-491

[6] Dalai D K. Basic theory in construction of Boolean functions with maximum possible annihilator immunity[J]. Desings, Codes and Cryptography, 2006, 40(1): 41-58

[7] Qu Long-jiang, Li Chao, Feng Ke-qin. A Note on Symmetric Boolean Functions with Maximum Algebraic Immunity in Odd Number of Variables[J]. IEEE Transactions on Information Theory, 2007, 53(8): 2908-2910

[8] Bracken A, Preneel B. On the algebraic immunity of symmetric Boolean functions: INDOCRYPT 2005[C] // LNCS 3797. Springer-Verlag, 2005: 35-48

[9] Qu Long-jiang, Feng Ke-qin, Liu Feng. Construction Symmetric Boolean Functions with Maximum Algebraic Immunity[J]. IEEE Transactions on Information Theory, 2009, 55(5): 2406-2412

[10] Qu Long-jiang, Li Chao. On the 2^m-variable symmetric Boolean functions with maximum algebraic immunity[J]. Science in China Series F-Information Sciences, 2008, 51(2): 120-127

[11] Liu Feng, Feng Ke-qin. On the 2^m-variable symmetric Boolean functions with maximum algebraic immunity 2^{m-1}[C]// WCC 2007. 2007: 225-232

[12] Carlet C. A method of construction of balanced functions with optimal algebraic immunity[EB/OL]. http://eprint.iacr.org/2006/149.pdf

[13] Carlet C, Zeng Xiang-yong. Further properties of several classes of Boolean functions with optimum AI[J]. Design, Codes, Cryptography, 2009, 52(3): 303-338

[14] Wang Y J, Fan S Q. New construction of Boolean function with optimum Algebraic Immunity[OL]. http://eprint.iacr.org/2008/176.pdf

[15] Fu Shao-jing, Li Chao, Qu Long-jiang. Construction of Rotation Symmetric Boolean Functions with Maximum Algebraic Immunity: CANS 2009[C]// LNCS 5888. Springer Verlag, 2007: 402-412

[16] Li Na, Qu Long-jiang. On the Construction of Boolean Functions with Optimal Algebraic Immunity[J]. IEEE Transactions on Information Theory, 2008, 53(3): 1330-1334

[17] Li Na, Qi Wen-feng. Construction and Analysis of Boolean Functions of $2t+1$ Variables with Maximum Algebraic Immunity: ASIACRYPT 2006[C]// LNCS 4284. Springer Verlag, 2006: 82-98

[18] Sarkar S, Maitra S. Construction of Rotation Symmetric Boolean Functions on Odd Number of Variables with Maximum Algebraic Immunity: Algebra, Algebraic Algorithms and Error-Correcting Codes, 2007[C]// LNCS 4851. Springer Verlag, 2007: 271-280

[19] Li Chun-lei, Zeng Xiang-yong. A class of rotation symmetric Boolean functions with optimum Algebraic Immunity[J]. Wuhan University Journal of Natural Sciences, 2008, 13(6): 702-706

[20] Liu Mein-cheng, Pei Ding-yi. Identification and construction of Boolean functions with Maximum Algebraic Immunity[J]. Science in China, 2009

[21] Carlet C, Feng Ke-qin. An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity: ASIACRYPT 2008[C]// LNCS 5350. Springer Verlag, 2008: 425-440

[22] Tu Zi-ran, Deng Ying-pu. A conjecture on binary string and its applications on constructing Boolean functions of optimum AI[OL]. http://eprint.iacr.org/2009/272

[23] Dalai D K. Cryptographically significant Boolean functions: construction and analysis in terms of algebraic immunity: FSE 2005[C]// LNCS 3557. Springer Verlag, 2005: 98-111

[24] Carlet C, Dalai D K, Gupta K C. Algebraic Immunity for Cryptographically Significant Boolean Functions: Analysis and Construction[J]. IEEE Transactions on Information Theory, 2006, 52(7): 3105-3121

[25] Fu Shao-jing, Qu Long-jiang, Li Chao. Construction of odd-variable Boolean Functions with Maximum Algebraic Immunity: WISA 2009[C]// LNCS 5932. Springer Verlag, 2009: 109-117

[26] Chen Yin-dong. A First Order Recursive Construction of Boolean Function with Optimum Algebraic Immunity[EB/OL]. http://eprint.iacr.org/2009/134.pdf

[27] Dong De-shuai, Fu Shao-jing, Qu Long-jiang. A new construction of Boolean functions with Maximum Algebraic Immunity: ISC 2009[C]// LNCS 5735. Springer Verlag, 2009: 177-185