doi:10.3969/j.issn.1000-436x.2014.z2.035

全局雪崩准则的刻画及函数构造

袁宏博，杨晓元，魏立线，刘龙飞
（武警工程大学 电子技术系网络与信息安全武警部队重点实验室，陕西 西安 710086）

摘 要：从研究全局雪崩准则的表达方式出发，提出了全局雪崩准则的矩阵刻画方法，为研究全局雪崩准则提供了新的工具。根据全局雪崩准则平方和指标的性质，提出了一种改造 M-M 型函数的奇数元几乎最优函数，其满足多个密码学性质，具有较小的平方和指标。构造全局雪崩准则性质优良的密码函数是当前研究的一个难点，利用构造新的映射的方法来改造 M-M 型函数是一种行之有效的办法。
关键词：布尔函数；全局雪崩准则；矩阵表示；函数构造；非线性度
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)Z2-0251-05

Description of global avalanche characteristics and constructions of Boolean functions

YUAN Hong-bo, YANG Xiao-yuan, WEI Li-xian, LIU Long-fei
（Key Laboratory of Network & Information Security of APF, Engineering University of APF, Xi'an, 710086 China）

Abstract: Global avalanche characteristics matrix representation method starting from the expression of global avalanche characteristics was proposed and a new tool for research global avalanche characteristics was provided. According to properties of sum-of-square indicator, an odd almost optimal Boolean functions which meet savariety of properties of cryptography was constructed and hold slower sum-of-square indicator via M-M Boolean functions. It is a problem that how to construct a kind of functions satisfying GAC. There is a effecint way that modifying M-M functions with designing new mapping.
Key words: Boolean functions; global avalanche characteristics; matrix; construction algorithm; nonlinearity

1 引言

密码函数在序列密码和分组密码的设计实现中起着举足轻重的作用。密码函数的构造、表示、计数及其密码学性质的分析是研究密码函数的研究热点与前沿。在序列密码中主要使用的是布尔函数，序列密码的安全性取决于密钥序列的安全性，因此产生密钥序列的布尔函数的密码学性质对一个序列密码体制的安全性起着决定性作用。

布尔函数的密码学性质主要有：平衡性、代数次数、非线性度、扩散性和相关免疫性、代数免疫性、正规性等。在构造一个密码学性能优良的布尔函数时，人们往往更加注重多个密码学性质的折中，以及相互制约关系。当前布尔函数的构造有了大量的研究和成果，但是部分构造方法只体现在某几个密码学性质，兼顾多种密码学性质的布尔函数构造仍然是布尔函数研究的热点问题。

全局雪崩准则是 Zhang 等[1]提出用来改进密码函数的全局性质。它拓展了严格雪崩准则（SAC）和扩散准则（PC）[2]。全局雪崩准则克服了严格雪崩准则和扩散准则在某些点的自相关值，使密码函数在整体上达到最优的一个衡量指标。

2010 年，周宇等提出了衡量 2 个不同函数互相关程度的“全局雪崩准则”概念[3]，受到一定关注和研究[4~8]。Shannon 提出了密码系统设计的 2 个原则：扩散和混淆。混淆表达了布尔函数之间的相关程度较小，也就是 2 个布尔函数距离较远；扩散则表示布尔函数自身具有一种均匀性。

收稿日期：2014-04-30
基金项目：国家自然科学基金资助项目（61272492）
Foundation Item: The National Natural Science Foundation of China (61272492)

当前，人们对一个布尔函数的全局雪崩准则的研究方法主要还停留在提出一个具体构造，而后进行全局雪崩准则的计算研究，缺少统一的研究工具和研究方法，因此，为研究全局雪崩准则提供新的研究工具，在衡量一个函数的全局雪崩准则时能有一个统一的方法和标准值的进一步研究和研讨。

从研究 GAC 准则的刻画方法出发，提出了全局雪崩准则的矩阵刻画方法。并在张卫国构造的奇数元几乎最优函数的工作基础上，构造了一种改进的平方和指标的奇数元几乎最优函数。

2 基础知识

定义 1 n 元布尔函数 $f(x)$ 是指从 F_2^n 到 F_2 的一个映射，B_n 表示所有 n 元布尔函数的全体。

将 $f(x)\in B_n$ 的函数值按照 x 的字典顺序从小到大排成一个 2^n 维向量：$f(\alpha_0),f(\alpha_1),\cdots,f(\alpha_{2^n-1})$，其中 $\alpha_0=(00\cdots0)$，$\alpha_1=(00\cdots1)$，$\cdots$，$\alpha_{2^n-1}=(11\cdots1)$。将这个 2^n 维的向量 $(f(\alpha_1),f(\alpha_2),\cdots,f(\alpha_{2^n-1}))$ 称为 $f(x)$ 的真值表示。

定义 2 设 $f(x)\in B_n$，则 $f(x)$ 在 $\alpha=(\alpha_1,\alpha_2,\cdots,\alpha_n)\in F_2^n$ 处的 Walsh 谱值为

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

其中，$\phi_\alpha(x)=\alpha_1x_1+\alpha_2x_2+\cdots+\alpha_nx_n$，$\alpha=(\alpha_1,\alpha_2,\cdots,\alpha_n)\in F_2^n$，$x=(x_1,x_2,\cdots,x_n)\in F_2^n$

定义 3 设 $f(x)\in B_n$，则 $f(x)$ 的非线性度为

$$N_f=2^{n-1}-\frac{1}{2}\max_{\alpha\in F_2^n}|S_f(\alpha)|$$

当 $N_f=2^{n-1}-2^{\frac{n}{2}-1}$，即 $S_f(\omega)=\pm2^{\frac{n}{2}}$ 时，称 f 为 Bent 函数。

定义 4 设 $f(x),g(x)\in B_n$，则 $f(x)$ 的自相关函数为

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

$f(x)$ 和 $g(x)$ 的互相关函数为

$$\Delta_{f,g}(\alpha)=\sum_{x\in F_2^n}(-1)^{f(x)+g(x+\alpha)},\alpha\in F_2^n$$

定义 5 设 $f(x)\in B_n$，则 $f(x)$ 的平方和指标定义为

$$\sigma_f=\sum_{\alpha\in F_2^n}\Delta_f^2(\alpha)$$

$f(x)$ 的绝对值指标定义为

$$\Delta_f=\max_{\alpha\in F_2^n,wt(\alpha)\neq0}|\Delta_f(\alpha)|$$

定义 6 设 $f(x),g(x)\in B_n$，则 $f(x)$ 和 $g(x)$ 的互相关平方和指标定义为

$$\sigma_{f,g}=\sum_{\alpha\in F_2^n}\Delta_{f,g}^2(\alpha)$$

$f(x)$ 和 $g(x)$ 的互相关绝对值指标定义为

$$\Delta_{f,g}=\max_{\alpha\in F_2^n,wt(\alpha)\neq0}|\Delta_{f,g}(\alpha)|$$

引理 1[9] 设布尔函数 f 是 t 阶弹性函数当且仅当对任意的 $\omega\in F_2^n$，$0\leqslant W_H(\omega)\leqslant m$，都有

$$W_f(\omega)=0$$

成立。

引理 2 设 n 为偶数，$F_2^n=[(\boldsymbol{x},\boldsymbol{y})\,|\,\boldsymbol{x},\boldsymbol{y}\in F_2^{n/2}]$，$F_2^n$ 上的(M-M, maiorana-mcfarland)[10,11]型布尔函数，定义为

$$f(x,y)=x\pi(y)+g(y)$$

3 布尔函数的全局雪崩准则的矩阵表示

如下所示，构造矩阵[12,13] $\boldsymbol{H}_f$

$$\boldsymbol{H}_f=\begin{bmatrix}(-1)^{f(x_0+\alpha_0)} & (-1)^{f(x_0+\alpha_1)} & \cdots & (-1)^{f(x_0+\alpha_{2^n-1})}\\ (-1)^{f(x_1+\alpha_0)} & (-1)^{f(x_1+\alpha_1)} & \vdots & (-1)^{f(x_1+\alpha_{2^n-1})}\\ \vdots & \vdots & \vdots & \vdots\\ (-1)^{f(x_{2^n-1}+\alpha_0)} & (-1)^{f(x_{2^n-1}+\alpha_1)} & \cdots & (-1)^{f(x_{2^n-1}+\alpha_{2^n-1})}\end{bmatrix}$$

那么，有 $\Delta_f(\alpha)=\sum_{x\in F_2^n}(-1)^{f(x)+f(x+\alpha)}=\overline{(-1)^{f(x)}}\,\boldsymbol{H}_f$，其中，$\overline{(-1)^{f(x)}}$ 为行向量 $\left[(-1)^{f(x_0)}\ \ (-1)^{f(x_1)}\ \cdots\ (-1)^{f(x_{2^n-1})}\right]$。可知，矩阵 $\boldsymbol{H}_f$ 是一个轴对称矩阵。例如，二元 Bent 序列 $f=[1,1,1,-1]$，那么

$$\boldsymbol{H}_f=\begin{bmatrix}1 & 1 & 1 & -1\\ 1 & 1 & -1 & 1\\ 1 & -1 & 1 & 1\\ -1 & 1 & 1 & 1\end{bmatrix}$$

$$\Delta_f(\alpha)=\sum_{x\in F_2^n}(-1)^{f(x)+f(x+\alpha)}=\overline{(-1)^{f(x)}}\boldsymbol{H}_f=[4,0,0,0]$$

可以求得 $\sigma_f=4^2=16=2^{2\times2}$，$\Delta_f=0$。与 Zhang 等的结论相符。

同理，有构造矩阵 $\boldsymbol{H}_g$

$$\boldsymbol{H}_g=\begin{bmatrix}(-1)^{g(x_0+\alpha_0)} & (-1)^{g(x_0+\alpha_1)} & \cdots & (-1)^{g(x_0+\alpha_{2^n-1})}\\ (-1)^{g(x_1+\alpha_0)} & (-1)^{g(x_1+\alpha_1)} & \vdots & (-1)^{g(x_1+\alpha_{2^n-1})}\\ \vdots & \vdots & \vdots & \vdots\\ (-1)^{g(x_{2^n-1}+\alpha_0)} & (-1)^{g(x_{2^n-1}+\alpha_1)} & \cdots & (-1)^{g(x_{2^n-1}+\alpha_{2^n-1})}\end{bmatrix}$$

则 $\Delta_{f,g}(\alpha)=\sum_{x\in F_2^n}(-1)^{f(x)+g(x+\alpha)}=\overline{(-1)^{f(x)}}\boldsymbol{H}_g$，其中，$\overline{(-1)^{f(x)}}$ 为行向量 $\left[(-1)^{f(x_0)}\quad(-1)^{f(x_1)}\quad\cdots\quad(-1)^{f(x_{2^n-1})}\right]$。类似于 Walsh 谱值的矩阵表示方法，构造了矩阵 $\boldsymbol{H}_f$ 来计算一个布尔函数的自相关函数和 2 个布尔函数的互相关函数。进一步，可以利用矩阵表示方法来研究布尔函数全局雪崩准则的平方和指标以及绝对值指标，不仅能从矩阵运算的角度证明前人得到的一些结论和定理，还能进一步提出一些全局雪崩准则的新性质。用矩阵的方法来表示全局雪崩准则，不仅是在表达形式上的研究，更是将雪崩准则研究方法拓展到程序实现的重要工具。

4　一种平方和指标优良的奇数元几乎最优函数的构造

4.1　一种序列构造的性质

k 为整数。$\forall\alpha\in F_2^k$，定义映射 $\pi_1(\alpha),\pi_2(\alpha)$ 满足以下条件：

1) $\pi_1(\alpha),\pi_2(\alpha)\in F_2^{k+1}$；

2) $wt(\pi_1(\alpha))\geqslant t,wt(\pi_2(\alpha))\geqslant t$；

3) $\pi_1(\alpha)\neq\pi_2(\alpha)$，且 $\pi_1(\alpha)\neq\pi_2'(\alpha),\pi_2'(\alpha)=\pi_2(\alpha)+(1,0,\cdots,0)$；

其中 $\pi_1(\alpha),=(\pi_1'(\alpha),\pi_1^{k+1}(\alpha)),\pi_2(\alpha)=(\pi_2'(\alpha),\pi_2^{k+1}(\alpha))$，$\pi_1'(\alpha),\pi_2'(\alpha)\in F_2^k$，$\pi_1^{k+1}(\alpha),\pi_2^{k+1}(\alpha)\in F_2^1$。$X_{k+1}'=(x_0,x_1,\cdots,x_k)$，$X_k=(x_0,x_1,\cdots,x_{k-1})$。

定义函数 $\varphi(X_{k+1})$

$$\varphi(X_{k+1})=x_k\pi_1(\alpha)X_{k+1}'+(x_k+1)\pi_2(\alpha)X_{k+1}'$$

那么函数 $\varphi(X_{k+1})$ 具有以下性质：

1) $N_\varphi=2^{n-1}-2^{n-2}$；

2) $\varphi(X_{k+1})$ 是平衡的；

3) $\varphi(X_{k+1})$ 是 m 阶弹性的。

证明

$$\begin{aligned}W_\varphi(\omega)|(x_k=0\,\&\,\omega=(\pi_2'(\alpha),\pi_2^{k+1}(\alpha)))&=\sum_{\omega\in F_2^{k+1}}(-1)^{\pi_2(\alpha)X_{k+1}'+\omega x}\\&=\sum_{\omega\in F_2^{k+1}}(-1)^{(\pi_2'(\alpha),\pi_2^{k+1}(\alpha))(X_k,0)+\omega(X_k,0)}\\&=\sum_{\omega=(\pi_2'(\alpha),\pi_2^{k+1}(\alpha))}(-1)^{\pi_2'(\alpha)X_k+\pi_2'(\alpha)X_k}=\pm2^k\end{aligned}$$

同理，

$$W_\varphi(\omega)|(x_k=0\,\&\,\omega=(\pi_2'(\alpha),\pi_2^{k+1}(\alpha)+1))=\pm2^k$$

$$W_\varphi(\omega)|(x_k=1\,\&\,\omega=(\pi_1'(\alpha),\pi_1^{k+1}(\alpha)))=\pm2^k$$

$$W_\varphi(\omega)|(x_k=1\,\&\,\omega=(\pi_1'(\alpha),\pi_1^{k+1}(\alpha)+1))=\pm2^k$$

其余 $W_\varphi(\omega)=0$。

那么 $N_\varphi=2^k-1/2\max|W_\varphi|=2^k-2^{k-1}$。容易得到，$W_\varphi(0)=0$，可证 $\varphi(X_{k+1})$ 是平衡函数。

因为 $wt(\pi_1(\alpha))\geqslant t,wt(\pi_2(\alpha))\geqslant t$，根据上面的推导，当 $1\leqslant wt(\omega)\leqslant t-1$ 时，有 $S_\varphi(\omega)=0$。由引理 1 可知，$\varphi(X_n)$ 是一个 t–1 阶相关免疫函数。

4.2　构造满足多个密码学准则的奇数元几乎最优函数

下面利用函数 $\varphi(X_{k+1})$ 来构造一种满足多个密码学准则的奇数元几乎最优函数。

$n=2k+1$，其中 k 是一个整数。构造函数 $f(x)$ 是一个改造的 $F_2^k\times F_2^{k+1}$ 上的 M-M 型函数。在 F_2^{k+1} 中选择一个集合 T 满足以下 3 个条件：

1) $|T|=2^k+3m$，其中 m 是正整数；

2) $\forall\gamma\in T,l\leqslant wt(\gamma)\leqslant k-l+1$，其中

$$l=\min\left\{j\,|\sum_{i=0}^{j}C_{k+1}^i\geqslant2^{k-1}+3m\right\}$$

3) $\forall\gamma\in T,\overline{\gamma}\in T,\overline{\gamma}=\gamma+(1,1,\cdots,1)$。

T 的一个真子集 U 满足以下 2 个条件：

1) $|U|=4m$；

2) $\forall\gamma\in U,\gamma'\in U,\gamma'=\gamma+(1,0,\cdots,0)$。

构造集合 N，M。令集合 $N\cup M=F_2^k,N\cap M=\phi,|N|=m$。对于任意 $\alpha_i,\alpha_j\in N$，其中 $\pi_k(\alpha_i)\neq\pi_1(\alpha_j)\neq\pi_1'(\alpha_j)\neq\pi_2(\alpha_j)\neq\pi_2'(\alpha_j)$，$k=1,2$。

那么令 P 是从 N 到 U 的映射 π_1,π_2。Q 是从 M 到 $T-U$ 的单射，$W=T-U$。那么构造函数 $f(x)$

$$f(x)=\begin{cases}x_k\pi_1(X_k)X_{k+1}'+(x_k+1)\pi_2(X_k)X_{k+1}', X_k\in N\\ Q(X_k)X_{k+1}', X_k\in M\end{cases}$$

那么有以下结论成立：

1) $f(x)$ 是一个奇数元几乎最优函数；

2) $f(x)$ 是平衡的；

3) $f(x)$ 是 $(t-1)$ 阶相关免疫函数；

4) $\sigma_f = 2^{2n+1} - 3m2^{3n+1/2}$ 。

证明 $n = 2k+1$ ，设 $\eta \in F_2^n$ ， $\eta = (\beta, \gamma)$ ， $\beta \in F_2^k$ ， $\gamma \in F_2^{k+1}$ 。

当 $y \in M$ 时

$$\begin{aligned} W_f(\omega) &= \sum_{x \in F_2^n} (-1)^{f(x)+\omega x} \\ &= \sum_{y \in M, z \in F_2^{k+1}} (-1)^{Q(y)z+\beta y+\gamma z} \\ &= \sum_{y \in M} (-1)^{\beta y} \sum_{z \in F_2^{k+1}} (-1)^{(Q(y)+\gamma)z} \end{aligned}$$

若 $Q^{-1}(\gamma)$ 存在，即 $\gamma \in W$ ，那么有

$$W_f(\omega) = 2^{k+1}(-1)^{\beta \bullet Q^{-1}(\gamma)} = \pm 2^{k+1}$$

$\gamma \notin W$,那么

$$W_f(\omega) = 0$$

当 $y \in N$ 时，因为对于任意 $\alpha_i, \alpha_j \in N$ ，有 $\pi_k(\alpha_i) \neq \pi_1(\alpha_j) \neq \pi_1'(\alpha_j) \neq \pi_2(\alpha_j) \neq \pi_2'(\alpha_j)$， $k = 1, 2$ 。由 4.1 节中构造的证明，有

$$W_f(\omega) \in [0, \pm 2^k]$$

由 U 选取的条件 2)和 4.1 节中的构造的证明，得

$$W_f(\omega) \in [0, \pm 2^k, \pm 2^{k+1}]$$

那么函数 $f(x)$ 的非线性度为

$$N_f = 2^{n-1} - 2^{n-1/2}$$

因此，函数 $f(x)$ 是一个奇数元的几乎最优函数。

因为零向量不属于集合 T，所以 $W_f(0) = 0$ ，函数 $f(x)$ 是平衡的。

当 $y \in M$ 时，由文献[14]中的证明可知，当 $1 \leqslant wt(\omega) \leqslant t-1$ 时， $W_f(\omega) = 0$ 。

当 $y \in N$ 时，由 4.1 节的证明可知，当 $1 \leqslant wt(\omega) \leqslant t-1$ 时， $W_f(\omega) = 0$ 。

因此， $f(x)$ 是一个 $t-1$ 阶相关免疫函数。

最后，讨论 $f(x)$ 的全局雪崩准则。

由之前 Walsh 谱的推导可知

$$\{|\eta \| W_f(\eta)| = 2^{k+1}, \eta \in F_2^n |\} = 2^{n-1} - m2^{(n-1)/2}$$

$$\{|\eta \| S_f(\eta)| = 2^k, \eta \in F_2^n |\} = 4m2^{(n-1)/2}$$

由公式

$$\sigma_f = 2^{-n} \sum_{\eta \notin F_2^n} (W_f(\eta))^4$$

可得

$$\sigma_f = 2^{-n} \sum_{\eta \notin F_2^n} (W_f(\eta))^4$$

$$\begin{aligned} &= 2^{-n}[(2^{n-1} - m2^{(n-1)/2})(2^{(n+1)/2})^4 + \\ &\quad 4m2^{(n-1)/2}(2^{(n-1)/2})^4] \\ &= 2^{2n+1} - 3m2^{3n+1/2} \end{aligned}$$

这个数值是较小的。

例如，令 n=9，按照如图 1 所示的映射来构造函数。

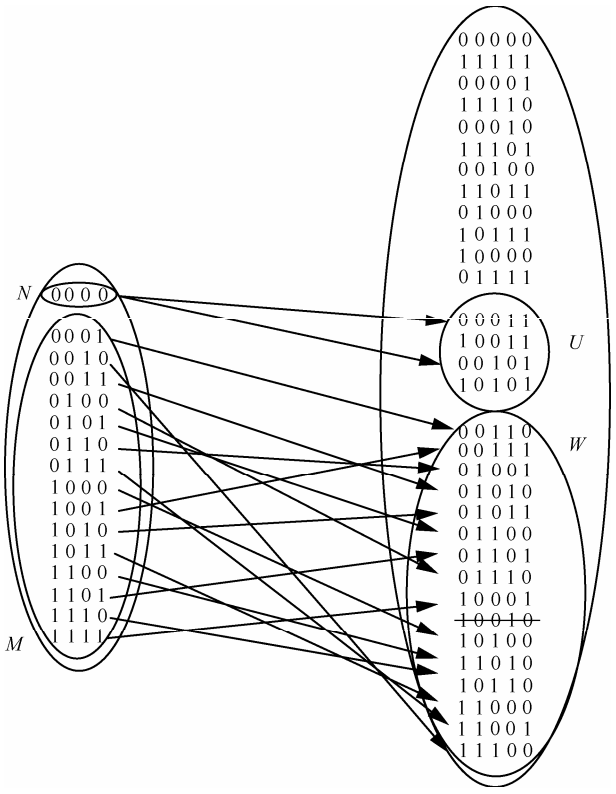

图 1 9 元函数的映射方法

这样构造得到的一阶弹性九元布尔函数，非线性度为 240， $S_f(\eta) \in [0, \pm 16, \pm 32]$，其全局雪崩准则平方和指标为： $2^{19} - 2^{15} + 2^{13}$ 。

表 1 是根据本方法进行构造得到的奇数元几乎

最优函数的全局雪崩准则平方和指标。

表 1　奇数元几乎最优函数的平方和指标

n	弹性阶	m	平方和指标
9	1	1	$2^{19}-3\times1\times2^{13}$
11	1	6	$2^{21}-3\times6\times2^{17}$
13	1	17	$2^{25}-3\times17\times2^{20}$
13	2	2	$2^{25}-3\times2\times2^{20}$
15	1	32	$2^{29}-3\times32\times2^{23}$
15	2	13	$2^{29}-3\times13\times2^{23}$

5　结束语

全局雪崩准则在近年来受到国内外学者的广泛关注和研究[15~19]。本文提出了全局雪崩准则的矩阵刻画方法，为进一步构造全局雪崩准则性质好的布尔函数提供了一个研究的工具。并根据全局雪崩准则的性质来构造一种平方和指标优良的奇数元几乎最优函数，为进一步研究如何得到平方和指标更小的布尔函数提供了一种方法。但是对一些问题的研究仍不足，例如构造多个密码学性质达到折中的函数构造研究，是否有达到最小平方和指标的平衡布尔函数等问题仍然有待研究。

参考文献：

[1] ZHANG X M, ZHENG Y L. GAC—the criterion for global avalanche characteristics of cryptographic functions[J]. Journal for Universal Computer Science, 1995, 1(5):316-333.

[2] ADAMS C M, TAVARES S E. Generating and counting binary bent sequences[J]. IEEE Transactions on Information Theory, 1995, 36(5): 1170-1173.

[3] 周宇.布尔函数的密码学性质研究[D]. 西安电子科技大学, 2009.
ZHOU Y. Research on Cryptographic Properties of Boolean Functions[D]. Xi'an University of Electronic Science and Technology, 2009.

[4] CARLET C. Generalized partial spreads[J]. IEEE Trasactions on Informatiom Theory,1995,41(5):1482-1487.

[5] BIHAM E, SHAMIR A. Differential cryptanalysis of DES-like cryptosystems[J]. Journal of Cryptology,1991,4(1):3-72.

[6] ZHOU J, CHEN W, GAO F. Best linear approximation and correlation immunity of functions over Z_m[J]. IEEE Transaction on Information Theory,1999,45(1):303-308.

[7] ZENG X, CARLET C, SHAN J, *et al*. More balanced Boolean functions with optimal algebraic immunity and good nonlinearity and resistance to fast algebraic attacks[J]. IEEE Transactions on Information Theory, 2011.6310-6320.

[8] ROTHAUS O S. On `bent' functions[J]. J Combin Theory A, 1976, 20: 300-305.

[9] XIAO G Z, MASSEY J L.A Spectral characterization of correlation-immune combining functions[J]. IEEE Transaction on Information Theory, 1988,34(3):569-571.

[10] 张薇, 杨晓元, 韩益亮.密码基础理论与协议[M]. 北京: 清华大学出版社, 2012, 23-27.
ZHANG W, YANG X Y, HAN Y L. Cryptography Based Theory and Agreement[M]. Beijing: Tsinghua University Press,2012,23-27.

[11] ZHENG Y, ZHANG X M. Plateaued functions[A]. advances in cryptology-ICIC'99, lecture notes in computer science[C]. Heidelberg, Ed, Springer-verlag, 1999, 1726:284-300.

[12] 常志文, 张杰, 李红霞. 由已知 Bent 序列构造新的 Bent 序列[J].哈尔滨理工大学学报, 2010, 15:78-81.
CHANG Z W, ZHANG J, LI H X. Constructing Bent sequence form given bent sequence[J]. Journal of Harbin University of Science and Technology, 2010, 15:78-81.

[13] 张恭庆. 高维哈达玛矩阵理论与应用[M]. 北京: 科学出版社, 2010. 66-92
ZHANG G Q. High-dimensional Hadamard Matrix Theory and Application[C]. Beijing: Science Press, 2010.66-92.

[14] 张卫国.密码函数及其构造[D]. 西安电子科技大学, 2006.
ZHANG W G. Research on Boolean Function and Construction[D]. Xi'an University of Electronic Science and Technology, 2006.

[15] MAITRA S. Highly nonlinear balanced Boolean functions with good local and global avalanche characteristics[J]. Inform Process Lett, 2002, 83: 281-286.

[16] LI N, QU L, QI W, *et al*. On the construction of Boolean functionswith optimal algebraic immunity[J]. IEEE Transaction on Informations Theory, 2008, 54: 1330-1334.

[17] CARLET C, DALAI D K, GUPTA K C, *et al*. Algebraic immunity for cryptographically significant Boolean functions: analysis and construction[J]. IEEE Transactions on Information Theory, 2006, 52: 3105-3121.

[18] DILLON J F. Elementary hardamard difference sets[A]. Proceeding of 6th S E Conference of Combinatorics, Graph Theory, and Computing[C]. Utility Mathematics,Winnipeg, 1975. 237-249.

[19] MAITRA S, SARKAR P. Modifications of pattterson-wiedemann functions for cryptographic applications[J]. IEEE Transactions on Information Theory, 2002,48(1):278-284.

作者简介：

袁宏博（1989-），男，吉林白山人，武警工程大学硕士生，主要研究方向为序列密码、密码函数。

杨晓元（1959-），男，湖南湘潭人，武警工程大学教授、博士生导师，主要研究方向为密码学、信息安全。

魏立线（1966-），男，陕西户县人，武警工程大学教授，主要研究方向为密码学、信息安全。

刘龙飞（1990-），男，河南沈丘人，武警工程大学讲师，主要研究方向为序列密码、割圆序列。