计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190800124

基于布尔导数的布尔置换构造

吴万青[1]　周国龙[1]　马晓雪[2]
1 河北大学网络空间安全与计算机学院　河北 保定 071002
2 河北大学计算机教学部　河北 保定 071002
(wuwanqing8888@126.com)

摘　要　布尔函数导数的性质在密码构造中起着重要的作用。文中利用布尔函数导数的性质,构造了一个新的平衡布尔函数。然后基于平衡布尔函数与布尔置换的关系,构造出一种新的布尔置换。

关键词:布尔导数;布尔置换;平衡布尔函数
中图法分类号　TP309

Construction of Boolean Permutation Based on Derivative of Boolean Function

WU Wan-qing[1],ZHOU Guo-long[1] and MA Xiao-xue[2]
1 School of Cyber Security and Computer,Hebei University,Baoding,Hebei 071002,China
2 Department of Computer Teaching,Hebei University,Baoding,Hebei 071002,China

Abstract　The properties of Boolean functions derivative play a major role in the Cryptosystem structure. This paper proposes a new balanced Boolean function by using the properties of Boolean functions derivative. Then according to the relationship of balanced Boolean functions and Boolean permutation,this paper constructs a new Boolean permutation.

Keywords　Derivative of Boolean Function,Boolean Permutation,Balanced Boolean Function

密码学在保障信息安全问题中扮演着重要角色。布尔函数是设计密码体制的重要工具,在密码系统设计过程中也起到重要作用[1]。密码函数的密码学性质在很大程度上影响着一个密码系统抵御各种安全性攻击的能力。密码函数可分为两类:布尔函数和向量值函数。布尔置换是向量值函数的一种特殊形式[2]。布尔置换在对称加密体制的设计和分析中具有更广泛的应用,尤其在分组密码领域[3]。因此研究更好的布尔置换成为密码学领域的又一研究热点。

有关布尔置换的研究工作已取得了一些成果。早期的研究可追溯到1988年,文献[4]利用一类特殊的布尔函数的平衡性,提出了一种随机构造非线性置换的迭代算法,不过该算法形式单一、过程复杂,而且各分量函数具有子线性特性,影响了布尔置换的密码学性质,导致其在密码学中无法使用。文献[5]首先提出判断一组布尔函数构成置换的充要条件,基于此提出一种非线性置换的方案,与文献[4]相比其构造的置换形式更加多样化且无需迭代,而且非线性度相同。次年文献[6]中证明了文献[4]中的构造方法成功率很小,于是提出把布尔置换的判定转化为对布尔函数平衡性的判定,由此构造出一类特殊的布尔置换。邢育森等基于布尔函数级联运算的迭代构造方法,对计数下界方面做了改进[7]。陈鲁生等[8]提出了两种均可由简单的含较少变量的布尔置换的构造出形式复杂的含较多变量的布尔置换构造方案,方案得到的多变量布尔置换具有高非线性特点,具有较好的抵御线性逼近攻击的优势。金君娥等[9]在此基础上做了改进,提出一种由简单较少变量构造复杂较多变量的布尔函数的方法,理论上可以构造出任意高阶布尔置换。Zhang等[10]提出一种构造最优代数次数的方案,该方案构造出的布尔置换只有一个非线性项,能构造的布尔置换数量也较少。何良生[11]对布尔函数的统计独立的构造、判断及性质做出了研究,并利用汉明重量给出布尔函数之间相互统计独立的充要条件。文献[12-13]提出了在有限域上的一类最优代数次数的布尔置换,带来了不能轻易得到布尔置换的逆置换的问题。正形置换是布尔置换的一类特殊形式,郑浩然等提出一种可由 n-2 元正形置换迭代构造出 n 元正形置换的方法[14]。张凤荣提出一个在 F_2^n 上求逆布尔置换的方法,给出一类最优代数次数的布尔置换;结合文献[15]的构造方法,张凤荣给出一种正形置换构造方案,它是一种新的迭代级联构造方案[15]。Coulter等提出一种广义的满足某种性质的三元组布尔置换构造方案,并利用该方案构造出满足特定条件的三元组BENT函数[16]。刘师师在文献[16]的基础上,给出三元组置换成立的充分必要条件,提出一种等价的构造三元组布尔置换的方案,此方案可生成更多的三元组布尔置换[2]。

本文认为布尔函数统计独立的相关性质在构造新的布尔置换方案过程中具有重要作用。本文对文献[11]中的统计独立性质进一步扩展,结合布尔函数导数得到一种新的可获得平衡布尔函数的方法,进而在一定前提下,构造出了一种新的布尔置换。该布尔置换中的每一个子项都是平衡函数,这也是本方案的特点。虽然布尔函数统计独立性质早已被提出,但以此扩展的理论并不过时,新的布尔置换或可为公钥体制分析提供新思路。

基金项目:河北省自然科学基金重点项目(F2019201290)
This work was supported by the Key Projects of Hebei Natural Science Foundation (F2019201290).
通信作者:周国龙(glong_zhou@126.com)

1 基础知识

1.1 布尔导数及性质

n 元布尔函数定义为如下映射：

$f: GF^n(2) \to GF(2)$

记为 $f(x)$，其中 $x \in GF^n(2)$，$f(x) \in GF(2)$。

对任意 n 元布尔函数 $f(x_1, \cdots, x_n)$，称如下函数：

$$\frac{\partial f}{\partial(x_{i_1}, \cdots, x_{i_k})} = f(x_1, \cdots, x_{i_1}, \cdots, x_{i_k}, \cdots, x_n) \oplus f(x_1, \cdots, \overline{x_{i_1}}, \cdots, \overline{x_{i_k}}, \cdots, x_n)$$

为函数 f 关于变量集 $\{x_{i_1}, \cdots, x_{i_k}\}$ 的导数，其中 $1 \leqslant i_1, \cdots, i_k \leqslant n$，$\overline{x_i} = x_i + 1$[1]。下面介绍一些布尔函数导数的相关性质[17]，其中，$\oplus$ 表示模 2 加。

性质 1 $\dfrac{\partial^2 f}{\partial x_i \partial x_j} = \dfrac{\partial^2 f}{\partial x_j \partial x_i}$

性质 2 $\dfrac{\partial^2 f}{\partial x_i^2} = 0$

性质 3 $\dfrac{\partial}{\partial x_i}(f(x) \oplus g(x)) = \dfrac{\partial f(x)}{\partial x_i} \oplus \dfrac{\partial g(x)}{\partial x_i}$

性质 4 $\dfrac{\partial f(x)g(x)}{\partial(x_{i_1}, \cdots, x_{i_k})} = f(x)\dfrac{\partial g(x)}{\partial(x_{i_1}, \cdots, x_{i_k})} \oplus g(x)\dfrac{\partial f(x)}{\partial(x_{i_1}, \cdots, x_{i_k})} \oplus \dfrac{\partial f(x)}{\partial(x_{i_1}, \cdots, x_{i_k})}\dfrac{\partial g(x)}{\partial(x_{i_1}, \cdots, x_{i_k})}$

1.2 布尔置换

从向量空间 $GF^n(2)$ 到向量空间 $GF^m(2)$ 上的映射称为 (n, m) 函数。记 $F: GF(2)^n \to GF^m(2)$。函数 F 表示为：

$F(x) = (f_1(x), \cdots, f_m(x))$

其中，$f_1(x), \cdots, f_m(x) \in \mathscr{B}_n$，$\mathscr{B}_n$ 表示全体 n 元布尔函数的集合。当 $m = n$ 时，函数 F 为布尔置换[1]。记为：

$P(x) = [f_1(x), \cdots, f_n(x)]$。

能够构成布尔置换的一组布尔函数要满足一定的性质，下面给出引理。

引理 1[11] 一组 n 元布尔函数 $f_1(x), \cdots, f_n(x)$，满足 $P(x) = [f_1(x), \cdots, f_n(x)]$ 的充分必要条件是，对任意 $c = (c_1, \cdots, c_n) \in GF(2)^n$，$\oplus c_i f_i(x)$ 是平衡函数，其中 $\oplus$ 表示模 2 和。

1.3 一个特殊的实值函数

定义 1 设 4 个布尔值 $a, b, c, d \in \{0, 1\}$，在 $GF(2)$ 中定义 2 阶行列式的运算：

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad \oplus bc$$

其中，$\oplus$ 表示模 2 加。

定义 2 设 $\gamma(x)$ 是 $GF^n(2)$ 上的一个实值函数，则其表达形式为：

$$\gamma(x) = \sum_{x \in GF(2)^n} \begin{vmatrix} f(x) & g(x) \\ h(x) & \varphi(x) \end{vmatrix} = \sum_{x \in GF(2)^n} (f(x)\varphi(x) \oplus g(x)h(x))$$

其中，$f(x), g(x), h(x), \varphi(x)$ 是 4 个 n 元布尔函数。

2 布尔置换的构造

定义 3 设 $f(x), g(x)$ 是两个 n 元布尔函数，若对任意 $a, b \in \{0, 1\}$，都有：

$Prob(f(x) = a \mid g(x) = b) = Prob(f(x) = a)$

称 $f(x), g(x)$ 统计独立。其中 $Prob(A \mid B)$ 表示在事件 B 发生的条件下，事件 A 发生的条件概率。$Prob(A)$ 表示事件 A 发生的概率。

性质 5[11] n 元布尔函数 $f(x), g(x)$ 统计独立的充分必要条件是：

$\omega t(f)\omega t(g) = 2^n \omega t(fg)$

其中，$\omega t(f)$ 表示函数 $f(x)$ 的汉明重量。

推论 1 当 $f(x), g(x)$ 为平衡函数，且 $f(x), g(x)$ 统计独立时，有：

$$Prob(f(x) = 0, g(x) = 0) = \frac{1}{4}$$

$$Prob(f(x) = 0, g(x) = 1) = \frac{1}{4}$$

$$Prob(f(x) = 1, g(x) = 0) = \frac{1}{4}$$

$$Prob(f(x) = 1, g(x) = 1) = \frac{1}{4}$$

证明：因为 $f(x), g(x)$ 相互独立，当 $f(x) = 1, g(x) = 1$ 时，由性质 5 得：

$$Prob(f(x) = 1, g(x) = 1) = \frac{\omega t(fg)}{2^n} = \frac{\omega t(f)}{2^n}\frac{\omega t(g)}{2^n}$$

又 $f(x), g(x)$ 都为平衡函数，有：

$\omega t(f) = 2^{n-1}$

$\omega t(g) = 2^{n-1}$

得：

$$Prob(f(x) = 1) = \frac{\omega t(f)}{2^n} = \frac{2^{n-1}}{2^n} = \frac{1}{2} \tag{1}$$

$$Prob(g(x) = 1) = \frac{\omega t(g)}{2^n} = \frac{2^{n-1}}{2^n} = \frac{1}{2} \tag{2}$$

所以：

$$Prob(f(x) = 1, g(x) = 1) = \frac{1}{4}$$

当 $f(x) = 0, g(x) = 0$ 时，

$$Prob(f(x) = 0) = \frac{2^n - \omega t(f)}{2^n} \tag{3}$$

$$Prob(g(x) = 0) = \frac{2^n - \omega t(g)}{2^n} \tag{4}$$

由条件概率公式得：

$$Prob(f(x) = 0 \mid g(x) = 0) = \frac{Prob(f(x) = 0, g(x) = 0)}{Prob(g(x) = 0)}$$

化简得：

$Prob(f(x) = 0, g(x) = 0) = Prob(f(x) = 0 \mid g(x) = 0)\ Prob(g(x) = 0)$

由定义 3 得：

$Prob(f(x) = 0, g(x) = 0) = Prob(f(x) = 0)Prob(g(x) = 0)$

将式(3)、式(4)代入上式得：

$$Prob(f(x) = 0, g(x) = 0) = \frac{2^n - \omega t(f)}{2^n}\frac{2^n - \omega t(g)}{2^n} = (1 - \frac{2^{n-1}}{2^n})(1 - \frac{2^{n-1}}{2^n}) = (1 - \frac{1}{2})(1 - \frac{1}{2}) = \frac{1}{4}$$

同理，当 $f(x) = 1, g(x) = 0$ 时，由定义 3 得：

$Prob(f(x) = 1, g(x) = 0) = Prob(f(x) = 1 \mid g(x) = 0)Prob(g(x) = 0) = Prob(f(x) = 1)Prob(g(x) = 0)$

将式(1)、式(4)代入上式得：

$$Prob(f(x)=1,g(x)=0)=\frac{1}{2}(\frac{2^n-\omega t(g)}{2^n})$$
$$=\frac{1}{2}(1-\frac{1}{2})=\frac{1}{4}$$

当 $f(x)=0,g(x)=1$ 时，由定义 3 得：

$$Prob(f(x)=0,g(x)=1)$$
$$=Prob(f(x)=0|g(x)=1)Prob(g(x)=1)$$
$$=Prob(f(x)=0)Prob(g(x)=1)$$

将式(2)、式(3)代入上式得：

$$Prob(f(x)=0,g(x)=1)=(\frac{2^n-\omega t(f)}{2^n})\frac{1}{2}=$$
$$(1-\frac{1}{2})\frac{1}{2}=\frac{1}{4}$$

证毕。

性质 6[11] 若函数 $f(x),g(x)$ 统计独立，则 $f(x)\oplus g(x)$ 为平衡函数。

证：由推论 1 可得。

定理 1 n 元布尔函数 $f(x)=f(x_1,\cdots,x_n),g(x)=g(x_1,\cdots,x_n)$ 均为平衡函数且它们之间统计独立，若 $\frac{\partial f(x)}{\partial x_i}=1$ 且 $\frac{\partial g(x)}{\partial x_i}$ 为平衡函数，其中 $1\leqslant x_i\leqslant n$，则 $f(x)\frac{\partial g(x)}{\partial x_i}\oplus g(x)$ 为平衡函数。

证：已知 $\frac{\partial f(x)}{\partial x_i}=1$，那么：

$$f(x)\frac{\partial g(x)}{\partial x_i}\oplus g(x)$$
$$=f(x)\frac{\partial g(x)}{\partial x_i}\oplus\frac{\partial f(x)}{\partial x_i}g(x)$$
$$=f(x)(g(x)g\oplus(x\oplus\alpha))\oplus(f(x)\oplus f(x\oplus\alpha))g(x)$$
$$=f(x)g(x)\oplus f(x)g(x\oplus\alpha)\oplus f(x\oplus\alpha)g(x)\oplus f(x)g(x)$$
$$=f(x)g(x\oplus\alpha)\oplus f(x\oplus\alpha)g(x)$$

其中，$\alpha=(0_1,\cdots,1_i,\cdots,0_n)\in GF^n(2)$，$x\oplus\alpha=(x_1,\cdots,1+x_i,\cdots,x_n)$。

由已知可得 $\frac{\partial f(x)}{\partial x_i}=1$，即 $f(x)\oplus f(x\oplus\alpha)=1$。由于 $f(x)$ 是平衡函数，得：

$$|\{f(x)=1,f(x\oplus\alpha)=0\}|$$
$$=|\{f(x)=0,f(x\oplus\alpha)=1\}|$$
$$=2^{n-1}$$

已知 $\frac{\partial g(x)}{\partial x_i}$ 是平衡函数，由导数定义得：

$$|\{g(x)\oplus g(x\oplus\alpha)=0\}|$$
$$=|\{g(x)\oplus g(x\oplus\alpha)=1\}|$$
$$=2^{n-1}$$

已知 $g(x)$ 是平衡函数，那么：

$$|\{g(x)=0,g(x\oplus\alpha)=0\}|$$
$$=|\{g(x)=0,g(x\oplus\alpha)=1\}|$$
$$=|\{g(x)=1,g(x\oplus\alpha)=0\}|$$
$$=|\{g(x)=1,g(x\oplus\alpha)=1\}|$$
$$=2^{n-2}$$

函数 $f(x),g(x)$ 为平衡函数且统计独立，由推论 1 得：

$$|\{f(x)=0,g(x)=0\}|=|\{f(x)=0,g(x)=1\}|$$
$$=|\{f(x)=1,g(x)=0\}|$$
$$=|\{f(x)=1,g(x)=1\}|$$
$$=2^{n-2}$$

由以上结果可直接得：

$$|\{f(x)=0,g(x)=0,f(x\oplus\alpha)=1,g(x\oplus\alpha)=1\}|$$
$$=|\{f(x)=0,g(x)=1,f(x\oplus\alpha)=1,g(x\oplus\alpha)=0\}|$$
$$=|\{f(x)=1,g(x)=0,f(x\oplus\alpha)=0,g(x\oplus\alpha)=0\}|$$
$$=|\{f(x)=1,g(x)=1,f(x\oplus\alpha)=0,g(x\oplus\alpha)=1\}|$$
$$=2^{n-2}$$

根据定义 2 和 $\frac{\partial f(x)}{\partial x_i}=1$ 得：

$$\omega t(f\frac{\partial g(x)}{\partial x_i}\oplus g)=\omega t(f\frac{\partial g(x)}{\partial x_i}\oplus\frac{\partial f(x)}{\partial x_i}g)$$
$$=\sum_{x\in GF^n(2)}\begin{vmatrix}f(x)&g(x)\\f(x\oplus\alpha)&g(x\oplus\alpha)\end{vmatrix}$$
$$=2^{n-2}\begin{vmatrix}0&0\\1&1\end{vmatrix}+2^{n-2}\begin{vmatrix}0&1\\1&0\end{vmatrix}+$$
$$2^{n-2}\begin{vmatrix}1&0\\0&0\end{vmatrix}+2^{n-2}\begin{vmatrix}1&1\\0&1\end{vmatrix}$$
$$=2^{n-1}$$

故 $\omega t(f\frac{\partial g(x)}{\partial x_i}\oplus g)=2^{n-1}$，所以函数 $f\frac{\partial g(x)}{\partial x_i}\oplus g$ 是平衡函数。证毕。

下面举例说明性质 6 与定理 1 构造的布尔函数不一样。

例 1 设 4 元函数 $f(x)=x_1+x_2x_3+x_2x_4+x_3x_4$，$g(x)=x_1+x_2+x_4+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4+x_1x_2x_4+x_2x_3x_4+x_1x_2x_3x_4$。

令 $D=\frac{\partial}{\partial x_1}$，那么 $f(x),g(x),f(x\oplus\alpha),g(x\oplus\alpha),f(x)Dg(x)\oplus g(x),f(x)\oplus g(x)$ 的真值表如表 1 所列，其中 $\alpha=(1,0,0,0)$。

表 1 各函数值真值表

Table 1 Truth table of individual functions

x	$f(x)$	$g(x)$	$f(x\oplus\alpha)$	$g(x\oplus\alpha)$	$f(x)Dg(x)\oplus g(x)$	$f(x)\oplus g(x)$
0000	0	0	1	1	0	0
0001	0	1	1	1	1	1
0010	0	0	1	0	0	0
0011	1	0	0	1	1	1
0100	0	1	1	0	1	1
0101	1	1	0	0	0	0
0110	1	0	0	0	0	1
0111	1	1	0	1	1	0
1000	1	1	0	0	0	0
1001	1	1	0	1	1	0
1010	1	0	0	0	0	1
1011	0	1	1	0	1	1
1100	1	0	0	1	1	1
1101	0	0	1	1	0	0
1110	0	0	1	0	0	0
1111	0	1	1	1	1	1

可以看出 $f(x)Dg(x)\oplus g(x)\neq f(x)\oplus g(x)$，故性质 6 与定理 1 构造的布尔函数不一样。

由以上结论可以得到一个新的布尔置换。

定理 2 设 $[g_1(x),\cdots,g_n(x)]$ 是一个布尔置换，$\frac{\partial g_i(x)}{\partial x_j}$ 是平衡函数，$f_i(x)$ 与 $g_i(x)$ 统计独立且 $\frac{\partial f_i(x)}{\partial x_j}=1$，其中 $i=1,\cdots,n,1\leqslant j\leqslant n$，若对于任意的 $c=(c_1,\cdots,c_n)\in GF^n(2)$，使得 $\bigoplus_{i=1}^{n}c_if_i\frac{\partial g_i(x)}{\partial x_j}$ 与 $\bigoplus_{i=1}^{n}c_ig_i$ 统计独立，则：

$$[f_1\frac{\partial g_1(x)}{\partial x_j}\oplus g_1,\cdots,f_n\frac{\partial g_n(x)}{\partial x_j}\oplus g_n]$$

是一个布尔置换。

（下转第 359 页）

复杂度是下一阶段需要研究的难点。

致谢 在此感谢华东政法大学陈德强老师对算法改进提出的建议,感谢华东政法大学刘洋老师对于数据处理与交叉验证的协助。

参 考 文 献

[1] 陈波,于泠,肖军模. 计算机系统安全原理与技术[M]. 北京:机械工业出版社,2009.

[2] SUI M. Network security situation assessment model based on information fusion [J]. Digital Communication World,2019(8):153.

[3] WANG X P. Computer network security analysis modeling based on deep learning algorithm [J]. Electronic Technology and Software Engineering,2019(16):195-196.

[4] LI X,DUAN Y C. Network security situation assessment method based on Improved Hidden Markov model [J]. Computer Science,2020,47(5):1-5.

[5] YE M X. Design and research of SQL injection vulnerability scanning system based on Web [J]. Electronic Design Engineering,2019,27(16):20-23,28.

[6] TIAN Y J,ZHAO Z M,WANG L J,et al. Research on the double layer defense model of SQL injection attack based on classification [J]. Information Network Security,2015(6):1-6.

[7] LU J Y,XIONG Y S,CHEN W,et al. Cyber security defense model based on spark [J]. Electronic Technology and Software Engineering,2019(17):184-185.

[8] HOU P. SQL injection attack model based on SGM model [J]. Journal of Anyang Normal University,2019(2):38-43.

[9] KUGU Z Z. Public management paradigm of Japanese super intelligent society [J]. Shanghai Quality,2019(7):25-26.

[10] SUN T T. Characteristics and challenges of intelligent society [D]. Shanghai:Shanghai Academy of Social Sciences,2018.

[11] ZHANG Q Q,YOU J S,GAO Y F. Overview of big data forensics technology [J]. Information Security Research,2017,3(9):795-802.

ZHU Jun-wen, born in 1999, undergraduate. His main research includes network and information security, electronic data forensics technology and norms.

(上接第 351 页)

证明:对于任意的 $c=(c_1,\cdots,c_n)\in GF^n(2)$有:

$$\bigoplus_{i=1}^{n}(c_i f_i\frac{\partial g_i(x)}{\partial x_j}\oplus c_i g_i)=\bigoplus_{i=1}^{n}c_i f_i\frac{\partial g_i(x)}{\partial x_j}\oplus\bigoplus_{i=1}^{n}c_i g_i$$

已知条件$\bigoplus_{i=1}^{n}c_i f_i\frac{\partial g_i(x)}{\partial x_j}$与$\bigoplus_{i=1}^{n}c_i g_i$统计独立且$\bigoplus_{i=1}^{n}c_i g_i$是平衡函数,由性质 6 可知:$\bigoplus_{i=1}^{n}(c_i f_i\frac{\partial g_i(x)}{\partial x_j}\oplus c_i g_i)$是平衡函数。证毕。

结束语 布尔置换在众多密码体制中发挥着重要作用,相关工作在近二十多年间也有了重要的进展。本文在已有结论的基础上,根据布尔导数性质和平衡函数性质,结合定义运算给出了一种布尔置换构造方法。

参 考 文 献

[1] 温巧燕. 现代密码学中的布尔函数[M]. 北京:科学出版社,2000.

[2] 刘师师. 基于 Rothaus 构造的 Bent 函数构造方法研究[D]. 徐州:中国矿业大学,2019.

[3] CADET C. Vectorial Boolean functions for cryptography,Chapter of the monography Boolean Models and Methods in Mathematics, Computer Science, and Engineering [D]. Cambridge:Cambridge University Press. 2010:98-469.

[4] PIEPRZYK J,FINKELSTEIN G. Towards effective nonlinear cryptosystem design [J]. IEEE Proceedings of Computers & Digital Techniques,1988,135(6):325-335.

[5] 武传坤. 非线性置换的构造[J]. 科学通报,1992,37(12):1147-1147.

[6] 武传坤. 密码学中的布尔函数[D]. 西安:西安电子科技大学,1993.

[7] 邢育森,杨义先. 密码体制中的布尔置换的构造与计数[J]. 通信学报,1998(3):74-76.

[8] 陈鲁生,符方伟,沈世镒. 关于密码体制中布尔置换的构造[J]. 工程数学学报,2016,19(2):23-30.

[9] 金君娥,朱华安,谢端强. 密码体制中布尔置换的构造[J]. 国防科技大学学报,2003,25(5):90-93.

[10] ZHANG W,WU C K,LI S. Construction of Cryptographically Important Boolean Permutations[J]. Applicable Algebra in Engineering Communication & Computing, 2004, 15(3/4):173-177.

[11] 何良生. 布尔函数的统计独立性[J]. 计算机科学,2008,35(1):83-86.

[12] CARLET C,FENG K. An infinite class of balanced vectorial Boolean functions with optimum algebraic immunity and good nonlinearity[C]// IWCC 2009. 2009:1-11.

[13] FENG K,LIAO Q,YANG J. Maximal values of generalized algebraic immunity[J]. Designs,Codes and Cryptography,2009,50(2):243-252.

[14] 郑浩然,张海模,樊东. 对一个正形置换构造方法的修正及其计数结果的改进[J]. 通信学报,2009(12):51-55,63.

[15] 张凤荣. 密码学中布尔函数及多输出布尔函数的构造[D]. 西安:西安电子科技大学,2012.

[16] COULTER R S,MESNAGER S. Bent functions from involutions over F2n[J]. IEEE Transactions on Information Theory,2017,PP(99):1-1.

[17] 张志杰,王卓,李卫卫. E-导数在 Bent 函数研究中的应用[C]// 中国通信学会第五届学术年会论文集. 2008.

WU Wan-qing, born in 1981, Ph.D, lecturer. His main research interests include information security and quantum-resistant cryptography.

ZHOU Guo-long, born in 1996, postgraduate. His main research interests include information security and so on.