doi:10.3969/j.issn.1000-436x.2013.04.012

一类密码函数的构造与分析

欧智慧[1]，赵亚群[1,2]，李旭[1]
(1. 信息工程大学 四院，河南 郑州 450002；2. 数学工程与先进计算国家重点实验室，河南 郑州 450002)

摘 要：利用 $t+1$ 个 n 元布尔函数(称为基函数)级联构造了一类 $n+t$ 元布尔函数 $G(x,y)$，并给出了 $G(x,y)$的 Walsh 循环谱和自相关系数。通过 Krawtchouk 多项式与 Krawtchouk 矩阵对 $G(x,y)$和基函数的关系进行了研究。分析了 $G(x,y)$的密码学性质：相关免疫性、扩散性和代数免疫性。特别地，当 $t=2$ 时，分析了 $G(x,y)$与基函数的具体关系。另外，一般化该构造方法构造了一类多输出布尔函数，给出了该类多输出布尔函数的广义 Walsh 循环谱，进而分析了该类多输出布尔函数的相关免疫性和代数免疫性。

关键词：密码函数；Plateaued 函数；Krawtchouk 矩阵；代数免疫性
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1000-436X(2013)04-0106-08

Construction and analysis of one class of cryptographic functions

OU Zhi-hui[1], ZHAO Ya-qun[1,2], LI Xu[1]
(1. The Fourth Institute, The Information Engineering University, Zhengzhou 450002, China;
2. State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450002, China)

Abstract: A novel class of $n+t$-variable Boolean functions $G(x,y)$ through adding t variables while concatenating $t+1$ Boolean functions (called basic function) was constructed and the Walsh spectrum and autocorrelation coefficient of $G(x,y)$ were given. The relationship between $G(x,y)$ and basic functions by Krawtchouk polynomial and Krawtchouk matrix was studied. Moreover, their cryptographic properties: correlation immunity, propagation and algebraic immunity were investigated. Specially, the detailed relationship between $G(x,y)$ and basic functions when $t=2$ was analyzed. In additional, a novel class of multioutput Boolean functions by generalizing the method was constructed and the general Walsh spectrum of the class of multioutput Boolean functions was proposed. Correlation immunity and algebraic immunity of the class of multioutput Boolean functions were analyzed.

Key words: cryptographic functions; Plateaued function; Krawtchouk matrix; algebraic immunity

1 引言

密码函数包括布尔函数和多输出布尔函数，它们是构成密码系统的重要组件。特别是在密码算法的非线性实现方面有着重要的应用，在序列密码中，密码函数多用于非线性反馈函数和非线性组合函数环节，在分组密码中多用于实现混乱作用的 S 盒。因此，对密码函数的研究是分析密码算法的基础性工作，具有十分重要的意义，国内外这方面的研究工作有许多[1~6]。因此，在密码函数的研究中，构造具有良好密码学性质的密码函数十分重要。由于密码函数的各个准则间具有一定的制约关系，构造具有良好密码学性质的密码函数并不容易。Bent 函数是一类具有最大非线性度的布尔函数，在抵抗线性攻击方面十分优越，但它有不平衡性、不具有相关免疫性等缺点。2001 年，Zheng 等[7]提出 Plateaued 函数的概念，它是一类比 Bent 函数更广的布尔函数，具有很好的非线性度，可以满足相关免疫性、平衡性，而且可以不具有非零的线性结构，近年来已成为密码工作者研究的热点之一[8~11]。密

收稿日期：2012-06-13；**修回日期**：2012-11-28
基金项目：国家自然科学基金资助项目（61072046）；国家高技术研究发展计划（“863”计划）基金资助项目（2012AA011603）
Foundation Items: The National Natural Science Foundation of China (61072046); The National High Technology Research and Development Program of China (863 Program) (2012AA011603)

码函数的各项刻画指标多是应对某种具体的密码攻击而提出的，例如，布尔函数的相关免疫性主要是针对相关攻击提出的，希望布尔函数具有较好的相关免疫性，布尔函数的代数免疫阶主要是针对代数攻击提出的，希望布尔函数具有较高的代数免疫阶。级联构造是一种常用的重要构造方法，形如 $h(x,x_{n+1})=f\|g=x_{n+1}f(x)+(1+x_{n+1})g(x)$ 的布尔函数，就是一种常见的级联构造。通过分析 $f(x)$ 和 $g(x)$ 的密码学性质，得到 $h(x,x_{n+1})$ 的性质。反之，通过分析 $h(x,x_{n+1})$ 的性质，也有利于掌握 $f(x)$ 和 $g(x)$ 的性质。

由于密码算法的设计中更多的是涉及多输出布尔函数，因此，在布尔函数研究相对成熟的基础上，各种研究向多输出布尔函数扩展。一方面，相关概念被推广到多输出布尔函数，如：相关函数、相关免疫性、扩散性、代数免疫性等，进而研究多输出布尔函数的此类性质及具有良好性质的多输出布尔函数的构造。另一方面，布尔函数与多输出布尔函数的关系也是研究的一个重要方面。由于多输出布尔函数的复杂性，关于它的研究，虽然国内外学者也做了不少工作[12~14]，总的来说相关研究并不像布尔函数那么成熟，因此还需做更深入的研究。

孙光洪等[11]通过级联构造了一类布尔函数 $f=f_1(x)\|f_3(x)\|f_3(x)\|f_2(x)$，详细讨论了此类函数的密码学性质，指出当 $f_1(x)$、$f_2(x)$、$f_3(x)$ 具有较好性质时，f 也具有较好的性质。受文献[11]工作的启发，通过级联 $t+1$ 个 n 元布尔函数，笔者构造了 $n+t$ 元布尔函数 $G(x,y)$，它是文献[11]工作的一般情况。以 Krawtchouk 多项式[15]和 Krawtchouk 矩阵[16]为工具，给出了基函数和 $G(x,y)$ 谱的确定关系，从而将对 $G(x,y)$ 的研究转化为对 Krawtchouk 多项式和 Krawtchouk 矩阵的研究。分析了 $G(x,y)$ 的相关免疫性、扩散性和代数免疫性，指出在基函数性质较好的情况下，$G(x,y)$ 也具有较好的密码学性质。在特殊情况下，作为 Plateaued 函数，分析了基函数与 $G(x,y)$ 的依赖关系。同时，更进一步将构造方法推广到多输出布尔函数，构造了一类多输出布尔函数 $H(x,y)$，分析了 $H(x,y)$ 的相关免疫性和代数免疫性。

2　预备知识

记二元域 $F_2=\{0,1\}$，n 是一正整数，以 F_2^n 表示 n 个 F_2 的笛卡尔积，称 F_2^n 到 F_2 的任一映射 $f(\cdot)$ 为 n 个变元的(F_2^n 上的)布尔函数，即：若记 $x\hat{=}(x_1,x_2,\cdots,x_n)\in F_2^n$，则 $f(x)\hat{=}f(x_1,x_2,\cdots,x_n)\in F_2$。记 x 的汉明重量为 $wt(x)=\#\{1\le i\le n\,|\,x_i=1\}$（其中，$\#S$ 表示集合 S 中元素的个数），下面先给出一些基本定义和引理。

定义 1[1]　设 $w,x\in F_2^n$，x 和 w 的点积定义为 $wx=w_1x_1\oplus w_2x_2\oplus\cdots\oplus w_nx_n$。设 $f(x)$ 为 F_2^n 上的布尔函数，$w\in F_2^n$，称 $S_{(f)}(w)=\frac{1}{2^n}\sum_{x\in F_2^n}(-1)^{f(x)+wx}$ 为 $f(x)$ 的 Walsh 循环谱。

定义 2[1]　设 $f(x)$ 是 F_2^n 上的布尔函数，如果对任意的 $w\in F_2^n$，$1\le wt(w)\le m$ ($0\le wt(w)\le m$)，$S_{(f)}(w)=0$，称 $f(x)$ 为 m 阶相关免疫的(m 阶弹性的)。

定义 3[1]　设 $f_1(x)$，$f_2(x)$ 是 F_2^n 上的布尔函数，$s\in F_2^n$，称 $r_{f_1f_2}(s)=\frac{1}{2^n}\sum_{x\in F_2^n}(-1)^{f_1(x)+f_2(x+s)}$ 为 $f_1(x)$ 和 $f_2(x)$ 在点 s 的互相关系数；称 $r_{f_1}(s)=\frac{1}{2^n}\sum_{x\in F_2^n}(-1)^{f_1(x)+f_1(x+s)}$ 为 $f_1(x)$ 在点 s 的自相关系数。

定义 4[1]　设 $f(x)$ 是 F_2^n 上的布尔函数，称 $f(x)$ 满足严格雪崩准则(m 阶扩散准则)，当且仅当 $r_f(s)=0$，$wt(s)=1$ ($1\le wt(s)\le m$)。

定义 5[17]　设 $f(x)$ 是 F_2^n 上的布尔函数，$0\le r\le n$，如果对任意的 $w\in F_2^n$，$S_{(f)}(w)=0$ 或 $\pm2^{-r/2}$，则称 $f(x)$ 为 r 阶 Plateaued 函数。

引理 1[18]　设 $f(x)$ 是 F_2^n 上的布尔函数，则

1) $\sum_{w\in F_2^n}[S_{(f)}(w)]^2=1$；

2) $(-1)^{f(x)}=\sum_{w\in F_2^n}S_{(f)}(w)\cdot(-1)^{wx}$。

对于组合数 $\binom{t}{k}$，若 $k<0$ 或 $k>t$，规定 $\binom{t}{k}=0$，$\binom{0}{0}=1$。对任意的 $a\in F_2^t$，并且 $wt(a)=k$，有 $\sum_{x\in F_2^t,wt(x)=i}(-1)^{ax}=\sum_{j=0}^{i}(-1)^j\binom{k}{j}\binom{t-k}{i-j}=K_i(k,t)$，$K_i(k,t)$ 称为 Krawtchouk 多项式[15]，$\boldsymbol{A}_t=(a_{t;i,j})_{(t+1)(t+1)}$ 称为 Krawtchouk 矩阵[16]，其中，$a_{t;i,j}=K_j(i,t)$。

引理 2[15,19]

1) $\binom{t}{k}K_i(k,t)=\binom{t}{i}K_k(i,t)$；

2) $K_i(k,t)=(-1)^k K_{t-i}(k,t)$；

3) 对任意的$0\le r\le t$且$t,k\ge 1$，有$\sum_{i=0}^{r}K_i(k,t)=K_r(k-1,t-1)$。

引理3[19] 对于$i\ge 0, j\ge 0, t\ge 0$，有$\sum_{s=0}^{k}\binom{t}{s}K_i(s,t)K_j(s,t)=d_{i,j}\binom{t}{i}\cdot 2^t$，其中，当$i=j$时，$d_{i,j}=1$；当$i\ne j$时，$d_{i,j}=0$，称为Krawtchouk多项式的正交性。

3 级联布尔函数$G(x,y)$的密码学性质

设$f_i(x)$，$0\le i\le t$(称为基函数)是$t+1$个F_2^n上的布尔函数，令$G(x,y)=\sum_{c=(c_1,\cdots,c_t)\in F_2^t}f_{wt(c)}(x_1,\cdots,x_n)\prod_{i=1}^{t}(y_i+c_i+1)$，它是$n+t$元布尔函数，其中，$x=(x_1,\cdots,x_n)$，$y=(y_1,\cdots,y_t)$。$G(x,y)$就是笔者给出的级联构造函数，下文重点讨论$G(x,y)$与基函数的关系以及$G(x,y)$的密码学性质。不加说明，$G(x,y)$与$f_i(x)$，$0\le i\le t$均指上述函数。

3.1 基函数与$G(x,y)$的Walsh循环谱关系

下面的引理4和引理6从正反2个方面反映了$G(x,y)$与其基函数的关系，是考察$G(x,y)$的密码性质与该性质与其基函数密码学性质关系的基础。

引理4 设$a\in F_2^n$，$ß\in F_2^t$，$s=(a,ß)$，则$S_{(G)}(s)=\frac{1}{2^t}\sum_{k=0}^{t}S_{(f_k)}(a)K_k(wt(ß),t)$。

证明 对$s=(a,ß)$，可得

$$S_{(g)}(s)=\frac{1}{2^{n+t}}\sum_{w\in F_2^{n+t}}(-1)^{G(w)+ws}$$

$$=\frac{1}{2^{n+t}}\sum_{y\in F_2^t}\sum_{x\in F_2^n}(-1)^{G(x,y)+ax+ßy}$$

$$=\frac{1}{2^{n+t}}\sum_{y\in F_2^t}(-1)^{ßy}\sum_{x\in F_2^n}(-1)^{ax}(-1)^{\sum_{k=0}^{t}f_k(x_1,\cdots,x_n)\sum_{wt(c)=k,c\in F_2^t}\prod_{i=1}^{t}(y_i+c_i+1)}$$

$$=\frac{1}{2^{n+t}}\sum_{y\in F_2^t}(-1)^{ßy}\sum_{x\in F_2^n}(-1)^{ax}(-1)^{f_{wt(y)}(x)}$$

$$=\frac{1}{2^t}\sum_{k=0}^{t}S_{(f_k)}(a)K_k(wt(ß),t)$$

推论1 设$a\in F_2^n, ß_1, ß_2\in F_2^t, wt(ß_1)=wt(ß_2)$，则$S_{(G)}(a,ß_1)=S_{(G)}(a,ß_2)$；$S_{(G)}(a,0)=\frac{1}{2^t}\sum_{k=0}^{t}\binom{t}{k}S_{(f_k)}(a)$。

在引理4中，令矩阵$\boldsymbol{C}_t=(c_{t;i,j})_{(t+1)\times 2^n}$，$\boldsymbol{B}_t=(b_{t;i,j})_{(t+1)\times 2^n}$，其中，$c_{t;i,j}=S_{(G)}(a_j,ß_i)$，$wt(ß_i)=i$，$b_{t;i,j}=S_{(f_i)}(a_j)$，$a_j\in F_2^n$，则$2^t\boldsymbol{C}_t=\boldsymbol{A}_t\boldsymbol{B}_t$。矩阵$\boldsymbol{A}_t$就是上面提到的Krawtchouk矩阵，它有很多性质。引理5在文献[16]中已经被给出，下面利用Krawtchouk多项式的正交性重新证明它。

引理5 矩阵$\boldsymbol{A}_t$可逆，且$\boldsymbol{A}_t^{-1}=\frac{1}{2^t}\boldsymbol{A}_t$。

证明 令矩阵$\boldsymbol{D}_t=(d_{t;i,j})=\boldsymbol{A}_t^2$，由于$\boldsymbol{A}_t=(K_j(i,t))$，则$d_{t;i,j}=\sum_{s=0}^{t}K_s(i,t)K_j(s,t)$，由引理2的1)可知：$d_{t;i,j}=\frac{\sum_{s=0}^{t}\binom{t}{s}}{\binom{t}{i}}K_i(s,t)K_j(s,t)$，再由引理3知$d_{t;i,j}=d_{i,j}2^t$，故$\boldsymbol{D}_t=(d_{t;i,j})=\boldsymbol{A}_t^2=2^t\boldsymbol{I}_t$，其中，$\boldsymbol{I}_t$为$t+1$阶单位阵，从而$\boldsymbol{A}_t$可逆且$\boldsymbol{A}_t^{-1}=\frac{1}{2^t}\boldsymbol{A}_t$。

由引理4及引理5，易得下面的引理6。它是引理4的反演公式。

引理6 设$a\in F_2^n$，$ß_i\in F_2^t$，$wt(ß_i)=i$，$0\le k\le t$，则$S_{(f_k)}(a)=\sum_{i=0}^{t}S_{(G)}(a,ß_i)K_i(k,t)$。

3.2 $G(x,y)$的相关免疫性

利用引理2的3)可得定理1和定理2。定理1是引理4的一个应用，这说明在一定条件下，基函数相关免疫性好时$G(x,y)$相关免疫性也较好，这为构造高阶相关免疫函数提供了可能。定理2是引理6的一个应用，说明$G(x,y)$相关免疫性较好时基函数相关免疫性也较好。

定理1 设$f_i(x), 0\le i\le t$均是m阶相关免疫函数，若对任意$0\le i\le t$，$S_{(f_i)}(0)=d$为定值，则$G(x,y)$也是m阶相关免疫函数；并且若对任意$a\in F_2^n$还有$S_{(f_i)}(a)+S_{(f_{t-i})}(a)=0$，则$G(x,y)$是$m+1$阶相关免疫函数。

证明 设$a\in F_2^n$，$ß\in F_2^t$，$s=(a,ß)$，$1\le wt(s)\le m$，则$0\le wt(a)\le m$。若$1\le wt(a)\le m$，

由引理 4 得 $S_{(G)}(s)=0$；若 $wt(a)=0$，则 $1\le wt(ß)\le m$。由引理 2 的 3)和引理 4 可得 $S_{(G)}(s)=\frac{1}{2^t}\sum_{k=0}^{t}S_{(f_k)}(0)K_k(wt(ß),t)=\frac{d}{2^t}\sum_{k=0}^{t}K_k(wt(ß),t)=\frac{d}{2^t}K_t(wt(ß)-1,t-1)=0$，因此定理的第一部分证毕。设 $1\le wt(s)\le m+1$，则 $0\le wt(a)\le m+1$。若 $0\le wt(a)\le m$，由第一部分的证明知 $S_{(G)}(s)=0$；若 $wt(a)=m+1$ 且 $wt(ß)=0$，则由引理 2 的 2)可得

$$S_{(G)}(s)=S_{(G)}(a,0)=\frac{1}{2^t}\sum_{k=0}^{t}S_{(f_k)}(a)K_k(0,t)$$
$$=\frac{1}{2^t}\sum_{k=0}^{t}\left(-S_{(f_{t-k})}(a)\right)\cdot(-1)^0K_{t-k}(0,t)$$
$$=-\frac{1}{2^t}\sum_{k=0}^{t}S_{(f_{t-k})}(a)K_{t-k}(0,t)=-S_{(G)}(a,0)$$

从而，$S_{(G)}(s)=0$，定理的第二部分得证。

推论 2　若对任意 $0\le i\le t$，$f_i(x)$ 均是 m 阶弹性函数，则 $G(x,y)$ 也是 m 阶弹性函数；并且若对任意 $a\in F_2^n$，$wt(a)=m+1$，且 $S_{(f_i)}(a)+S_{(f_{t-i})}(a)=0$，则 $G(x,y)$ 是 $m+1$ 阶相关免疫函数。

定理 2　若 $G(x,y)$ 是 $m+t$ 阶相关免疫函数，则 $f_k(x),0\le k\le t$ 均为 m 阶相关免疫函数；若对任意的 $0\le i\le t$，且 $S_{(G)}(a,ß_i)=S_{(G)}(a,ß_{t-i})$，则 $0\le k\le t$，k 为奇数，$f_k(x)$ 满足 n 阶相关免疫(即是常函数)；若对任意的 $0\le i\le t$，且 $S_{(G)}(a,ß_i)=-S_{(G)}(a,ß_{t-i})$，则 $0\le k\le t$，k 为偶数，$f_k(x)$ 满足 n 阶相关免疫(即是常函数)。其中，$a\in F_2^n,ß_i\in F_2^t,wt(ß_i)=i$。

证明　设 $0\le k\le t$，因为对任意 $a\in F_2^n$，$ß\in F_2^t$，$1\le wt(a)\le m$，故 $1\le wt(a,ß)\le m+t$，从而 $S_{(f_k)}(a)=\sum_{i=0}^{t}S_{(G)}(a,ß_i)K_i(k,t)=0$，定理的第一部分证毕。对于定理的第二部分，设 $1\le wt(a)\le n$，则一方面，$S_{(f_k)}(a)=\sum_{i=0}^{t}S_{(G)}(a,ß_i)K_i(k,t)=\sum_{i=0}^{t}S_{(G)}(a,ß_{t-i})K_{t-i}(k,t)$，另一方面，因为 $S_{(G)}(a,ß_i)=S_{(G)}(a,ß_{t-i})$，又由引理 6 和引理 2 的 3)可得 $S_{(f_k)}(a)=\sum_{i=0}^{t}S_{(G)}(a,ß_i)K_i(k,t)=\sum_{i=0}^{t}S_{(G)}(a,ß_{t-i})\cdot(-1)^kK_{t-i}(k,t)$，故当 k 为奇数时，$S_{(f_k)}(a)=-S_{(f_k)}(a)$，这表明 $S_{(f_k)}(a)=0$，第二部分证毕。定理第三部分的证明同第二部分的证明。

3.3　$G(x,y)$的扩散性

下面的引理 7 是分析 $G(x,y)$的扩散性的基础，为方便，记 $(-1)^A=?(A)$。

引理 7　设 $a\in F_2^n,ß=(b_1,b_2,\cdots,b_t)\in F_2^t$，$wt(ß)=l,s=(a,ß)$，则

$$r_G(s)=\frac{1}{2^t}\sum_{j=0}^{t}\sum_{k=0}^{j}\binom{t-l}{k}\binom{l}{i-k}r_{f_jf_{l+2k-j}}(a)$$
$$=\frac{1}{2^t}\sum_{j=0}^{t}\sum_{k=0}^{l}\binom{t-l}{j-k}\binom{l}{k}r_{f_jf_{l+j-2k}}(a)$$

证明　$r_G(s)=\frac{1}{2^t}\sum_{x\in F_2^n}\sum_{y\in F_2^t}(-1)^{G(x,y)+G(x+a,y+ß)}$

$$=\frac{1}{2^t}\sum_{x\in F_2^n}\sum_{y\in F_2^t}?\left(\sum_{c\in F_2^t}f_{wt(c)}(x)\prod_{i=1}^{t}(y_i+c_i+1)+\sum_{c\in F_2^t}f_{wt(c)}(x+a)\prod_{i=1}^{t}(y_i+c_i+b_i+1)\right)$$
$$=\frac{1}{2^t}\sum_{x\in F_2^n}\sum_{j=0}^{t}\sum_{y\in F_2^t,wt(y)=j}?\left(\sum_{c\in F_2^t}f_{wt(c)}(x)\prod_{i=1}^{t}(y_i+c_i+1)+\sum_{c\in F_2^t}f_{wt(c)}(x+a)\prod_{i=1}^{t}(y_i+c_i+b_i+1)\right)$$
$$=\frac{1}{2^t}\sum_{x\in F_2^n}\sum_{j=0}^{t}\sum_{y\in F_2^t,wt(y)=j}?\left(f_j(x)+f_{l+j-2wt(yß)}(x+a)\right)$$
$$=\frac{1}{2^t}\sum_{x\in F_2^n}\sum_{j=0}^{t}\sum_{k=0}^{j}\binom{t-l}{k}\binom{l}{j-k}?\left(f_j(x)+f_{l+2k-j}(x+a)\right)$$
$$=\frac{1}{2^t}\sum_{j=0}^{t}\sum_{k=0}^{j}\binom{t-l}{k}\binom{l}{j-k}r_{f_jf_{l+2k-j}}(a)$$

注意到上述倒数第 3 个等式也等于 $\frac{1}{2^t}\sum_{x\in F_2^n}\sum_{j=0}^{t}\sum_{k=0}^{l}\binom{t-l}{j-k}\binom{l}{k}?\left(f_j(x)+f_{l+j-2k}(x+a)\right)$

$=\frac{1}{2^t}\sum_{j=0}^{t}\sum_{k=0}^{l}\binom{t-l}{j-k}\binom{l}{k}r_{f_jf_{l+j-2k}}(a)$。证毕。

推论 3　设 $a\in F_2^n,ß_1\in F_2^t,ß_2\in F_2^t$，$s_1=(a,ß_1)$，$s_2=(a,ß_2)$，如果 $wt(ß_1)=wt(ß_2)$，则 $r_G(s_1)=r_G(s_2)$。

推论 4　设 $a\in F_2^n$，$s=(a,0)\in F_2^{n+t}$，则 $r_G(s)=\frac{1}{2^t}\sum_{j=0}^{t}\binom{t}{j}r_{f_j}(a)$。

由引理 7 及推论 4 可得下面的定理 3，它表明在一定条件下 $G(x,y)$ 满足严格雪崩准则。

定理3 设 $f_i(x),0\le i\le t$ 均满足严格雪崩准则，对任意 $0\le i<j\le t$，$f_i(x)+f_j(x)$ 是平衡函数(即 $r_{f_if_j}(0)=0$)，则 $G(x,y)$ 满足严格雪崩准则。

证明 $a\in F_2^n,ß\in F_2^t,s=(a,ß),w(s)=1$，当 $wt(a)=1$ 且 $wt(ß)=0$ 时，因为 $f_i(x),0\le i\le t$ 均满足严格雪崩准则，由推论4可得 $r_G(s)=\frac{1}{2^t}\sum_{j=0}^{t}\binom{t}{j}r_{f_j}(a)=0$。当 $wt(ß)=1$ 且 $wt(a)=0$ 时，由于对任意 j，$j\ne 1+2k-j$，以及当 $i\ne j$ 时，$r_{f_if_j}(0)=0$，可得 $r_G(s)=\frac{1}{2^t}\sum_{j=0}^{t}\sum_{k=0}^{j}\binom{t-1}{k}\binom{1}{j-k}r_{f_jf_{1+2k-j}}(0)=0$。证毕。

3.4 $G(x,y)$的代数免疫阶

对于 n 元布尔函数 $f(x)$，如果存在布尔函数 $g(x)$ 使得 $f(x)g(x)=0$，称 $g(x)$ 为 $f(x)$ 的零化子。称 $f(x)$ 和 $f(x)+1$ 的非零零化子的最小代数次数为 $f(x)$ 的代数免疫阶，记为 $AI(f)$。

定理4 设 $0\le i\le t,0\le j<\binom{t}{i}$，$g_{i,j}(x)$ 为 $f_i(x)$(或 $f_i(x)+1$)的任意 $\binom{t}{i}$ 个零化子，若所有 $g_{i,j}(x)$ 和的代数次数等于它们中代数次数的最大值，则 $AI(G(x,y))=\min\{AI(f_0(x)),\cdots,AI(f_t(x))\}+t$。

证明 可令 $G(x,y)=f_0(x)g_0(y)+\cdots+f(x)_tg_t(y)$，其中，$g_i(y)=\sum_{c\in F_2^t,wt(c)=i}\prod_{j=1}^{t}(y_j+c_j+1)$。一方面，设 $h_i(x),0\le i\le t$ 分别为达到 $f_i(x)$ 代数免疫阶的布尔函数，取 $p_i(y)=\sum_{c\in F_2^t,wt(c)=i}\prod_{j=1}^{t}(y_j+c_j+1)$，如果 $f_i(x)h_i(x)=0$，则 $G(x,y)h_i(x)p_i(y)=\sum_{0\le j\le t,j\ne i}f_j(x)\cdot h_i(x)p_i(y)g_j(y)=0$；如果 $(1+f_i(x))h_i(x)=0$，则 $(G(x,y)+1)h_i(x)p_i(y)=\sum_{0\le j\le t,j\ne i}f_j(x)h_i(x)p_i(y)g_j(y)+(f_i(x)g_i(y)+1)h_i(x)p_i(y)=(f_i(x)+1)h_i(x)p_i(y)=0$。故 $AI(G(x,y))\le\min\{AI(f_0(x)),\cdots,AI(f_t(x))\}+t$。

另一方面，设 $h(x,y)$ 为达到 $G(x,y)$ 代数免疫阶的布尔函数，则 $h(x,y)$ 可表示成如下形式：$h(x,y)=q_0(x)h_0(y)+\cdots+q_{2^t-1}(x)h_{2^t-1}(y)$，其中，$0\le i\le 2^t-1$，$h_i(y)=\prod_{j=1}^{t}(y_j+i_j+1)$，$(i_1,i_2,\cdots,i_t)$ 为 i 的二进制表示。如果 $G(x,y)h(x,y)=0$，则 $(f_0g_0+\cdots+f_tg_t)\cdot(q_0(x)h_0(y)+\cdots+q_{2^t-1}(x)h_{2^t-1}(y))=0$，即 $\sum_{0\le k\le t,0\le i\le 2^t-1}f_kg_kq_i(x)h_i(y)=0$，取 $y=(i_1,i_2,\cdots,i_t)\in F_2^t$ 代入上述等式可得 $f_{wt(i)}q_i(x)=0$，其中，i 的二进制表示为 $(i_1,i_2,\cdots,i_t)$；如果 $(G(x,y)+1)h(x,y)=0$，同样取 $y=(i_1,i_2,\cdots,i_t)\in F_2^t$，则 $(f_{wt(i)}+1)q_i(x)=0$，其中，i 的二进制表示为 $(i_1,i_2,\cdots,i_t)$。由题设条件知

$$\deg(\sum_{j=0}^{2^t-1}q_j(x))=\max\{\{\deg(q_j(x))\mid 0\le j\le 2^t-1\}\}\ge\max\{AI(f_0(x)),\cdots,AI(f_t(x))\}$$

。又由 $h(x,y)=q_0(x)h_0(y)+\cdots+q_{2^t-1}(x)h_{2^t-1}(y)=y_0y_1\cdots y_t\cdot\sum_{j=0}^{2^t-1}q_j(x)+w(x,y)$，其中，$w(x,y)$ 中不含 y 的 t 次项，以及 $q_j(x),0\le j\le 2^t-1$ 不全为0，可得 $AI(G(x,y))=\deg(h)=\deg(\sum_{i=0}^{2^t-1}q_i(x))+t\ge\max\{AI(f_0(x)),\cdots,AI(f_t(x))\}+t\ge\min\{AI(f_0(x)),\cdots,AI(f_t(x))\}+t$。综上有 $AI(G(x,y))=\min\{AI(f_0(x)),\cdots,AI(f_t(x))\}+t$。证毕。

3.5 t=2 时 $G(x,y)$的性质

特殊地，针对 t=2 的情况，$G(x,y_1,y_2)=(y_1+1)(y_2+1)f_0(x)+(y_1+y_2)f_1(x)+y_1y_2f_2(x)$，文献[11]给出了其为 Bent 函数的充要条件。当 $G(x,y)$ 或基函数为 Plateaued 函数时，分析 $G(x,y)$ 与其基函数的依赖关系。对于其他特殊类型的布尔函数，可以类似地进行分析。

对任意 $u\in F_2^n$，a、$ß\in F_2$，$s=(u,a,ß)$，由引理4和引理6可得

$$\begin{cases}S_{(G)}(u,0,0)=\frac{1}{4}S_{(f_0)}(u)+\frac{1}{2}S_{(f_1)}(u)+\frac{1}{4}S_{(f_2)}(u)\\ S_{(G)}(u,0,1)=S_{(G)}(u,1,0)=\frac{1}{4}S_{(f_0)}(u)-\frac{1}{4}S_{(f_2)}(u)\\ S_{(G)}(u,1,1)=\frac{1}{4}S_{(f_0)}(u)-\frac{1}{2}S_{(f_1)}(u)+\frac{1}{4}S_{(f_2)}(u)\end{cases}\quad(1)$$

$$\begin{cases}S_{(f_0)}(u)=S_{(G)}(u,0,0)+2S_{(G)}(u,0,1)+S_{(G)}(u,1,1)\\ S_{(f_1)}(u)=S_{(G)}(u,0,0)-S_{(G)}(u,1,1)\\ S_{(f_2)}(u)=S_{(G)}(u,0,0)-2S_{(G)}(u,0,1)+S_{(G)}(u,1,1)\end{cases}\quad(2)$$

定理5 设 $G(x,y_1,y_2)=(y_1+1)(y_2+1)f_0(x)+(y_1+y_2)f_1(x)+y_1y_2f_2(x)$，其中，$y_1$、$y_2\in F_2$，$f_0(x)$、

$f_1(x)$ 和 $f_2(x)$ 是 F_2^n 上的布尔函数，则下面结论成立。

1) 若 G 是 r 阶 Plateaued 函数，$f_0(x)$、$f_1(x)$、$f_2(x)$ 都是 Plateaued 函数，则 $f_0(x)$、$f_1(x)$、$f_2(x)$ 阶数相同，若令此阶数为 k，必有 $k=r-2$ 或 r，当 $k=r$ 时，还有 $f_0(x)=f_2(x)$。

2) G 是 r 阶 Plateaued 函数，对任意 $u\in F_2^n$，$S_{(G)}(u,0,1)=S_{(G)}(u,1,1)=0$ 或 $S_{(G)}(u,0,0)=S_{(G)}(u,0,1)=0$，则 $f_0(x)$、$f_1(x)$、$f_2(x)$ 都是 r 阶 Plateaued 函数。

3) G 是 $r+2$ 阶 Plateaued 函数，对任意 $u\in F_2^n$，$S_{(G)}(u,0,0)=-S_{(G)}(u,1,1)$ 或 $S_{(G)}(u,0,0)=S_{(G)}(u,1,1)$，$S_{(G)}(u,0,1)=0$，则 $f_0(x)$、$f_1(x)$、$f_2(x)$ 都是 r 阶 Plateaued 函数。

4) $f_0(x)$、$f_1(x)$、$f_2(x)$ 是 r 阶 Plateaued 函数，对任意 $u\in F_2^n$，$S_{(f_0)}(u)=-S_{(f_2)}(u)$ 或 $S_{(f_0)}(u)=S_{(f_2)}(u)$，$S_{(f_1)}(u)=0$，则 G 是 $r+2$ 阶 Plateaued 函数。

证明　1) 由条件知，对任意 $u\in F_2^n$，$S_{(G)}(u,0,0)$、$S_{(G)}(u,0,1)$、$S_{(G)}(u,1,0)$ 及 $S_{(G)}(u,1,1)$ 均属于集合 $\{\pm 2^{\frac{-r}{2}},0\}$，又 $f_0(x)$、$f_1(x)$、$f_2(x)$ 是 Plateaued 函数，代入式(2)可得它们具有相同的阶，阶数 $k=r-4$，$r-2$ 或 r，若 $k=r-4$，可得对任意的 $u\in F_2^n, S_{(f_1)}(u)=0$，这与引理 1 的 1)矛盾，故 $k=r-2$ 或 r，当 $k=r$ 时，对任意的 $u\in F_2^n$ 有 $S_{(f_0)}(u)=S_{(f_2)}(u)$，从而由引理 1 的 2)知 $f_0(x)=f_2(x)$。

2) 若 $S_{(G)}(u,0,1)=S_{(G)}(u,1,1)=0$，代入式(2)得 $S_{(f_0)}(u)=S_{(f_1)}(u)=S_{(f_2)}(u)=S_{(g)}(u,0,0)$；若 $S_{(G)}(u,0,0)=S_{(G)}(u,1,0)=0$，同样代入式(2)得 $S_{(f_0)}(u)=-S_{(f_1)}(u)=S_{(f_2)}(u)=S_{(G)}(u,1,1)$。又由于 G 是 r 阶 Plateaued 函数，故 $f_0(x)$、$f_1(x)$、$f_2(x)$ 是 r 阶 Plateaued 函数。

3) 若 $S_{(G)}(u,0,0)=-S_{(G)}(u,1,1)$，代入式(2)得 $S_{(f_0)}(u)=-S_{(f_2)}(u)=2S_{(G)}(u,0,1)$ 且 $S_{(f_1)}(u)=2S_{(G)}(u,0,0)$；若 $S_{(G)}(u,0,0)=S_{(G)}(u,1,1)$，$S_{(G)}(u,0,1)=0$ 同样代入式(2)得 $S_{(f_0)}(u)=S_{(f_2)}(u)=2S_{(G)}(u,0,0)$，$S_{(f_1)}(u)=0$，又因为 G 是 $r+2$ 阶 Plateaued 函数，故 $f_0(x)$、$f_1(x)$、$f_2(x)$ 是 r 阶 Plateaued 函数。

4) 对任意 $u\in F_2^n$，若 $S_{(f_0)}(u)=-S_{(f_2)}(u)$，代入式(1)得 $S_{(G)}(u,0,0)=-S_{(G)}(u,1,1)=\frac{1}{2}S_{(f_1)}(u)$，$S_{(G)}(u,0,1)=\frac{1}{2}S_{(f_0)}(u)$；若 $S_{(f_0)}(u)=S_{(f_2)}(u)$，$S_{(f_1)}(u)=0$，代入式(1)得 $S_{(G)}(u,0,0)=S_{(G)}(u,1,1)=\frac{1}{2}S_{(f_0)}(u)$ 且 $S_{(G)}(u,0,1)=S_{(G)}(u,1,0)=0$，又由于 $f_0(x)$、$f_1(x)$、$f_2(x)$ 是 r 阶 Plateaued 函数，故 G 是 $r+2$ 阶 Plateaued 函数。

设 $f_i(x),0\le i\le t$ 是 $t+1$ 个 F_2^n 上的布尔函数，$x=(x_1,\perp,x_n)\in F_2^n$，$y=(y_1,\perp,y_t)\in F_2^t$，若构造 $G(x,y)=\sum_{c=(c_1,\perp,c_t)\in F_2^t} f_{wt(c)}(x_1,\perp,x_n)\prod_{i=1}^{t}(y_i+c_i)$，则完全可得到与第 3 节相似的结果。此时只需注意此时的 $f_i(x_1,\perp,x_n)$ 相当于原来的 $f_{t-i}(x_1,\perp,x_n)$，$0\le i\le t$ 即可。

4　基函数与构造的多输出布尔函数的关系

本节将上述构造推广到多输出布尔函数上，先引入一些基本的定义与结论。

设 m，n 为正整数且 $m\le n$，称 F_2^n 到 F_2^m 的任一映射 $F(x)=(f_1(x),\perp,f_m(x))$ 为 (n,m)多输出布尔函数，其中，$f_i(x)$，$1\le i\le m$ 是 F_2^n 上的布尔函数。

定义 6[1]　设 $F(x)$为(n,m)多输出布尔函数，$v\in F_2^n$，$u\in F_2^m$，称 $S_{(F)}(u,v)=\frac{1}{2^n}\sum_{x\in F_2^n}(-1)^{uF(x)+vx}$ 为 $F(x)$的广义 Walsh 循环谱。

定义 7[1]　设 $F(x)$为(n,m)多输出布尔函数，$1\le k\le m$，随机向量 $\boldsymbol{z}=F(x)=(f_1(x),\perp,f_m(x))$。如果对任意的 $1\le i_1<i_2<\perp<i_j\le n$ 及 $u\in F_2^m$，$1\le wt(u)\le k$，有 uz 与 $(x_{i_1},x_{i_2},\perp,x_{i_j})$ 统计独立，则称多输出函数 $F(x)$ 是 k 级 j 阶相关免疫的。

定义 8[20]　设 $F(x)$为(n,m)多输出布尔函数，给定输出 $y\in F_2^m$，若存在 n 元布尔函数 $F_y(x)$ 使得任意 $x\in F^{-1}(y)$ 都有 $F_y(x)=0$，则称 $F_y(x)$ 为输出 y 的状态函数。记 $AI_y(F)$ 为输出非零状态函数的代数次数的最小值，当输出 y 遍历时，称 $AI_y(F)$ 的最小值为多输出布尔函数 $F(x)$的代数免疫阶，记为 $AI(F)$。

引理 8[1]　设 $F(x)$为(n,m)多输出布尔函数，则 $F(x)$是 k 级 j 阶相关免疫的充要条件是对任意的 $v\in F_2^n$，$1\le wt(v)\le j$ 及 $u\in F_2^m$，$1\le wt(u)\le k$，有 $S_{(F)}(u,v)=0$。

设 $g_{i,j}(x), 0 \le i \le s, 0 \le j \le t$ 为 n 元布尔函数，$F_j(x) = (g_{0,j}(x), g_{1,j}(x), \cdots, g_{s,j}(x))$ 为$(n, s+1)$多输出布尔函数(称为基函数)，$0 \le j \le t$。令 $f_i(x,y) = \sum_{c=(c_1,\cdots,c_t)\in F_2^t} g_{i,wt(c)}(x)\prod_{j=1}^{t}(y_j + c_j + 1)$，$0 \le i \le s$。构造$(n+t, s+1)$多输出布尔函数 $H(x,y) = (f_0(x,y), f_1(x,y), \cdots, f_s(x,y))$。不加说明，下面的 $H(x,y)$即为按上述方法构造的。

类似于引理 4 和引理 6，可以得到下面的引理 9 和引理 10，它们是互为反演的。

引理9 设 $v = (v_1, v_2), u \in F_2^{s+1}$，$v_1 \in F_2^n, v_2 \in F_2^t$，则 $S_{(H)}(u,v) = \frac{1}{2^t}\sum_{i=0}^{t} K_i(wt(v_2), t) S_{(F_i)}(u, v_1)$。

引理 10 设 $u \in F_2^{s+1}, v_1 \in F_2^n, v_{2,k} \in F_2^t$，$wt(v_{2,k}) = k$，$0 \le k \le t$，则 $S_{(F_i)}(u, v_1) = \sum_{k=0}^{t} S_{(H)}(u, v_1, v_{2,k}) K_k(i,t)$。

利用上面的 2 个引理可以方便地讨论基函数与 $H(x,y)$的相互关系，从而构造密码学性质好的多输出布尔函数。作为应用，给出下面的定理 6 和定理 7。

定理 6 若任意 $F_i(x)$ 是 k 级 j 阶相关免疫的，$0 \le i \le t$，对于 $u \in F_2^{s+1}$ 及任意的 $0 \le i, j \le t$，有 $S_{(F_i)}(u,0) = S_{(F_j)}(u,0) = d_u$，则 $H(x,y)$是 k 级 j 阶相关免疫的。

证明 设 $v=(v_1,v_2)$，$u \in F_2^{s+1}$，$v_1 \in F_2^n$，$v_2 \in F_2^t$，$1 \le wt(u) \le k$，$1 \le wt(v) \le j$，则必有 $0 \le wt(v_1) \le j$。若 $1 \le wt(v_1) \le j$，由 $F_i(x)$，$0 \le i \le t$ 是 k 级 j 阶相关免疫及引理 8 得 $S_{(F_i)}(u, v_1) = 0$，故 $S_{(H)}(u,v) = \frac{1}{2^t}\sum_{i=0}^{t} K_i(wt(v_2), t) S_{(F_i)}(u, v_1) = 0$；若 $wt(v_1) = 0$，则 $1 \le wt(v_2) \le j$，由引理 2 的 3)可得 $S_{(H)}(u,v) = \frac{d_u}{2^t}\sum_{i=0}^{t} K_i(wt(v_2), t) = \frac{d_u}{2^t} K_t(wt(v_2) - 1, t-1) = 0$。综上，由引理 8 可知 $H(x,y)$是 k 级 j 阶相关免疫的。

定理 7 $AI(H(x,y)) \le \min\{AI(F_0), \cdots, AI(F_t)\} + t$。

证明 设 $0 \le i \le s$，$f_i(x,y) = g_{i,0}(x)h_0(y) + \cdots + g_{i,t}(x)h_t(y)$，其中，$h_i(y) = \sum_{c\in F_2^t, wt(c)=i}\prod_{j=1}^{t}(y_j + c_j + 1)$。由文献[13]的推理 1 可知，多输出布尔函数的代数免疫阶等于其分量函数的非零非线性组合的代数免疫阶的最小值。因此，可设 $0 \le j \le t$，$m_{0,j}(x)g_{0,j}(x) + m_{1,j}(x)g_{1,j}(x) + \cdots + m_{s,j}(x)g_{s,j}(x)$ 的代数免疫阶分别等于 $AI(F_j)$，设 $N_j(x)$ 为达到 $m_{0,j}(x)g_{0,j}(x) + m_{1,j}(x)g_{1,j}(x) + \cdots + m_{s,j}(x)g_{s,j}(x)$ 的代数免疫阶的布尔函数。取 $P_j(x,y) = N_j(x) \cdot \sum_{c\in F_2^t, wt(c)=j}\prod_{i=1}^{t}(y_i + c_i + 1)$，如果 $(m_{0,j}(x)g_{0,j}(x) + m_{1,j}(x)g_{1,j}(x) + \cdots + m_{s,j}(x)g_{s,j}(x))N_j(x) = 0$，则

$$\begin{aligned} & P_j(x,y)(m_{0,j}(x) f_0(x,y) + m_{1,j}(x) f_1(x,y) + \cdots + m_{s,j}(x) f_s(x,y)) \\ &= P_j(x,y) \cdot \sum_{i=0}^{s} m_{i,j}(x)(g_{i,0}(x)h_0(y) + g_{i,1}(x)h_1(y) + \cdots + g_{i,t}(x)h_t(y)) \\ &= P_j(x,y) \cdot \sum_{k=0}^{t}\sum_{i=0}^{s} h_k(y)\left(m_{i,j}(x)g_{i,k}(x)\right) \\ &= N_j(x) \cdot \sum_{i=0}^{s}\left(m_{i,j}(x)g_{i,j}(x)\right) = 0 \end{aligned}$$

如果 $(m_{0,j}(x)g_{0,j}(x) + m_{1,j}(x)g_{1,j}(x) + \cdots + m_{s,j}(x)g_{s,j}(x) + 1)N_j(x) = 0$，相似地，可得 $P_j(x,y)(m_{0,j}(x) f_0(x,y) + m_{1,j}(x) f_1(x,y) + \cdots + m_{s,j}(x) f_s(x,y) + 1) = 0$，故由文献[13]的推理 1 可知 $AI(H(x,y)) \le \deg(P_j(x,y)) = \deg(N_j(x)) + t = AI(F_j) + t$，因此，$AI(H(x,y)) \le \min\{AI(F_0), \cdots, AI(F_t)\} + t$。证毕。

5 结束语

通过级联 $t+1$ 个 n 元布尔函数构造了 $n+t$ 元布尔函数 $G(x,y)$，将对 $G(x,y)$与基函数的关系研究转化为对 Krawtchouk 多项式和 Krawtchouk 矩阵的研究，得到了彼此间循环谱的相互表达式。分析了 $G(x,y)$的相关免疫性、扩散性和代数免疫性。当 $t=2$ 时，分析了该类函数与基函数作为 Plateaued 函数的依赖关系。同时将上述构造方法推广到多输出布尔函数，通过级联 $t+1$ 个$(n, s+1)$多输出布尔函数的分量函数，构造了一类$(n+t, s+1)$多输出布尔函数 $H(x,y)$。同样利用 Krawtchouk 矩阵给出了该类函数的广义 Walsh 循环谱与基函数的广义 Walsh 循环谱之间的相互表达式。分析了 $H(x,y)$的相关免疫性和代数免疫性。对 Krawtchouk 多项式和 Krawtchouk 矩阵的深入研究是进一步分析 $G(x,y)$和 $H(x,y)$密码学性质的基础。

参考文献：

[1] 冯登国.频谱理论及其在密码学中的应用[M]. 北京: 科学出版社, 2000.
FENG D G. Sectrum Theory and the Application in Cryptography[M].Beijing: Publishing Company of Science, 2000.

[2] 何业锋, 马文平. 3 类 semi-Bent 函数的构造[J]. 电子学报, 2011, 39(1):233-236.
HE Y F, MA W P. Constructions of three classes of semi-Bent functions[J]. Chinese Journal of Electronics, 2011, 39(1):233-236.

[3] 谢佳, 王天择. 寻找布尔函数的零化子[J].电子学报, 2010, 38(11): 2686-2690.
XIE J, WANG T Z. Finding the annihilators of a Boolean function[J]. Chinese Journal of Electronics, 2010, 38(11):2686-2690.

[4] HU B, JIN C H, SHAO Z Y. Relationship among three kinds of cryptographic Boolean functions with special Walsh spectru [J]. Journal on Communications, 2010, 31(7):104-109.

[5] MEIER W, PASALIC E, CARLET C. Algebraic attacks and decomposition of Boolean functions[A]. Advances in Cryptology-Eurocrypt 2004[C]. Berlin, Germany, 2004. 474-491.

[6] CLAUDE C. Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions[J]. Des Codes Cryptogr, 2011, 59(1-3):89-109.

[7] ZHENG Y, ZHANG X M. On Plateaued functions[J]. IEEE Transactions on Information Theory, 2001, 47(3):1215-1223.

[8] 胡斌, 金晨辉, 冯春海. Plateaued 函数的密码学性质[J]. 电子与信息学报, 2008, 30(3): 660-664.
HU B, JING C H, FENG C M. Cryptographic properties of Plateaued functions[J]. Journal of Electronics & Information Tec nology, 2008, 30(3):660-664.

[9] 王维琼, 周宇, 肖国镇. Plateaued 函数的正规性[J]. 电子与信息学报, 2008, 30(9): 2283-2286.
WANG W Q , ZHOU Y, XIAO G Z. Normality of Plateaued functions[J]. Journal of Electronics & Information Technology, 2008, 30(9):2283-2286.

[10] CARLET C, PROUF E. On Plateaued functions and their constructions[A]. Fast Software Encryption 2003[C]. Lund, Sweden, 2887. 54-73.

[11] 孙光洪, 武传坤. 级联函数的密码学性质[J]. 电子学报, 2009, 37(4): 884-888.
SUN G H, WU C K. Some cryptographic properties of Boolean functions by concatenation[J]. Chinese Journal of Electron : 884-888.

[12] YING D H, ZHAO Y Q, FENG D G. Correlation functions of mulioutput m-valued logical functions and relation between correlat n functions and spectra[J]. Zhengzhou Univ NatSci.Ed, 2007,39(2):21-24.

[13] 王秋艳, 金晨辉. 多输出布尔函数与布尔函数代数免疫阶之间的关系[J]. 电子学报, 2011, 39(1):124-127.
WANG Q Y, JIN C H. Relationship between the algebraic immunity of multi-output Boolean functions and Boolean functions[J]. Chinese Journal of Electronics, 2011, 39(1):124-127.

[14] 胡斌, 金晨辉, 史建红. 多输出 Plateaued 函数的密码学性质[J]. 电子与信息学报, 2009, 31(6):1433-1437.
HU B, JIN C H, SHI J H. Cryptographic properties of mu ti-output Plateaued functions[J]. Journal of Electronics & Inform ion Technology, 2009, 31(6):1433-1437.

[15] MACWILLIAMS F J, SLOANE N J. The Theory of Error-Correcting Codes[M]. North Holland: Elsevier, 1977.

[16] FEINSILVER P, KOCIK J. Krawtchouk matrices from classical and quantum random walks[J]. Contemporary Mathematics, 2007, 287(2001): 83-96.

[17] CARLET C. Partially-bent functions[J]. Des Codes Cryptogr, 1993, 3(2):135-145.

[18] 丁存生, 肖国镇. 流密码学及其应用[M]. 国防工业出版社, 1994.
DING C S, XIAO G Z. Stream Cipher and Its Applications[M]. National Defence Industry Press, 1994.

[19] KRASIKOV I, LITSYN S. On integral zeros of krawtchouk polynomials[J]. Journal of Combinatorial Theory, 1996, 74(1):71-99.

[20] FISCHER S, MEIER W. Algebraic immunity of S-boxes and augmented functions[A]. Advances in FSE 2007[C]. Berlin, many, 2007. 366-381.

作者简介：

欧智慧（1985-），男，河南周口人，信息工程大学硕士生，主要研究方向为密码基础理论及概率统计应用。

赵亚群（1961-），女，江苏淮安人，博士，信息工程大学教授、硕士生导师，主要研究方向为密码基础理论及概率统计应用。

李旭（1986-），男，河北定州人，信息工程大学硕士生，主要研究方向为密码基础理论及概率统计应用。