学术论文

密码函数的一类递归构造方法

滕吉红，张文英，刘文芬，李世取
（解放军信息工程大学信息工程学院信息研究系，郑州 450002）

[摘要] 首先利用递归的方法证明了结构形式更为一般的布尔函数的 Walsh 谱分解式，然后利用这类布尔函数 Walsh 谱分解式，给出了密码学和编码学中具有重要应用价值的一些布尔函数，如弹性函数、Bent 函数以及满足严格雪崩准则的布尔函数的构造方法。

[关键词] Walsh 谱；Walsh 谱分解式；Bent 函数；弹性函数；严格雪崩准则
[中图分类号] TN918.1 [文献标识码] A [文章编号] 1009－1742（2003）07－0047－06

1 引言

在密码体制中，密钥流生成器中非线性组合函数的设计对密码体制的安全起着关键的作用。根据相应需求，密码设计者设计了各类特殊的非线性组合函数，如为抵抗相关攻击，密码设计者给出了相关免疫函数[1]的概念和构造，而为抵抗差分攻击，Rothaus 又提出了 Bent 函数[2]的概念，后来不少专家又对 Bent 函数的性质和构造进行了深入研究。考虑到弹性函数（平衡的相关免疫函数）和 Bent 函数以及多输出 Bent 函数在密码设计中的重要应用，构造这两类函数一直是密码设计者所关注的重要问题。T. Siegenthaler 给出了一种构造平衡相关免疫布尔函数的方法[1]；而 P. Camion 等人利用编码理论来研究相关免疫布尔函数，给出了具有高阶相关免疫性的代数次数为 2 的布尔函数的递归构造方法[3]；张木想等人利用 Hadamard 矩阵理论提出了直接构造任意阶相关免疫函数的思想和方法[4]；在 Bent 函数的构造方面，典型的构造法有 Rothaus 构造法（但它并不能构造全部 Bent 函数）、Walsh－Hadamard 矩阵构造法、基于 Kronecker 代数和变元置换的构造等[5]，后来，王隽又在 Bent 矩阵原则上给出了 Bent 函数的一种完全构造法[6]；文献［7］给出了一类布尔函数的 Walsh 谱的分解式并且讨论了它在密码设计中的应用，如通过它可以递归构造弹性函数[8]以及一维 Bent 函数[6]。首先，笔者利用布尔随机变量联合分布的分解式[9]，用递归的方法证明了结构形式更为一般的一类布尔函数的 Walsh 谱分解式。由于密码学中逻辑函数的密码性质几乎完全可以由其 Walsh 谱来刻画，因此所给出的 Walsh 谱分解式在密码函数的构造中有重要应用。其次，讨论了这类 Walsh 谱分解式在密码设计中的应用，通过它给出了弹性函数和 Bent 函数的一种递归构造方法，而平衡且满足严格雪崩准则的函数有很大的应用价值，同时，满足严格雪崩的布尔函数和 H 布尔函数[10]又是等价的，而 H 布尔函数是阵列编码中一个重要的函数类，因此构造平衡且满足严格雪崩准则的布尔函数具有重要意义。

此外，多输出 Bent 函数在分组密码设计和通信中都有重要应用，但多输出 Bent 函数的构造和计数又是一个公开的同时也是困难的问题，其中密码学中常用的通过级联来递归构造新的逻辑函数的方法，在构造多输出 Bent 函数时是失效的。利用笔者所得到的一类布尔函数 Walsh 谱的分解式，就

[收稿日期] 2003－01－21；修回日期 2003－03－03
[作者简介] 滕吉红（1974－），女，山东烟台市人，解放军信息工程大学博士研究生

可以给出多输出 Bent 函数的一种递归构造法。

2 基本概念

定义 1[11] 设 $f(x), x \in GF^n(2)$ 为 n 元布尔函数，则称

$$S_{(f)}(w) = \frac{1}{2^n} \sum_{x \in GF^n(2)} (-1)^{f(x)+wx}, \quad w \in GF^n(2)$$

为 $f(x)$的 Walsh 循环谱。

定义 2[11] 设 $f(x), x \in GF^n(2)$ 为 n 元布尔函数，则 $f(x)$ 是 m 阶弹性函数当且仅当对任意的 $w \in GF^n(2)$，且 $W(w) \leqslant m, S_{(f)}(w) = 0$，其中 $W(w)$ 表示向量 w 中所含 1 的个数。

定义 3[2] 设 $f(x), x \in GF^n(2)$ 为 n 元布尔函数，则 $f(x)$ 是 Bent 函数的充分必要条件是对任意的 $w \in GF^n(2)$，都有 $S^2_{(f)}(w) = 1/2^n$；或等价的当且仅当对任意的 $s \in GF^n(2) \setminus \{0\}$，都有

$$r_f(s) = \frac{1}{2^n} \sum_{x \in GF^n(2)} (-1)^{f(x+s)-f(x)} = 0。$$

引理 1（布尔随机变量联合分布的分解式）[9] 设 (Ω, F, P) 是一概率空间，$\boldsymbol{Y} = (Y_1, Y_2, \cdots, Y_n)$ 是 (Ω, F, P) 上的任一 n 维布尔随机向量，$B \in F$ 是任一事件，则对任意的 $a = (a_1, a_2, \cdots, a_n) \in GF^n(2)$，都有

$$P\{B, Y_1 = a_1, Y_2 = a_2, \cdots, Y_n = a_n\} = \frac{1}{2^{n-1}} \sum_{0 \neq (\lambda_1, \cdots, \lambda_n) \in GF^n(2)} P\{B, \lambda_1 Y_1 + \cdots + \lambda_n Y_n = \lambda_1 a_1 + \cdots + \lambda_n a_n\} - \frac{2^{n-1}-1}{2^{n-1}} P(B)。$$

3 一类布尔函数 Walsh 谱的分解式

下面用概率的方法给出具有某种形式的一类布尔函数的 Walsh 谱分解式。

定理 1 设 $\phi(x, y), x \in GF^n(2), y \in GF^r(2)$ 为 $n + r$ 元布尔函数，$l_1(x)$ 是 n 元布尔函数，$l_1(y)$ 是 r 元布尔函数，则对任意的 $w \in GF^n(2)$，$v \in GF^r(2)$，有

$$S_{(\phi+l_1 l_2)}(w,v) = \frac{1}{2}[S_{(\phi)}(w,v) + S_{(\phi+l_1)}(w,v) + S_{(\phi+l_2)}(w,v) - S_{(\phi+l_1+l_2)}(w,v)]。 \quad (1)$$

证明 设 $X_1, X_2, \cdots, X_n, Y_1, Y_2, \cdots, Y_r$ 是定义在同一概率空间上相互独立且都具有均匀分布的布尔随机变量，对任意的 $w \in GF^n(2)$，$v \in GF^r(2)$，由全概率公式以及引理 1 有

$$P\{\phi(X,Y) + l_1(X)l_2(Y) = wX + vY\} = P\{\phi(X,Y) = wX + vY, l_1(X) = 0, l_2(Y) = 0\} + P\{\phi(X,Y) = wX + vY, l_1(X) = 0, l_2(Y) = 1\} + P\{\phi(X,Y) = wX + vY, l_1(X) = 1, l_2(Y) = 0\} + P\{\phi(X,Y) + 1 = wX + vY, l_1(X) = 1, l_2(Y) = 1\} = \frac{1}{4}[P\{\phi(X,Y) = wX + vY\} + P\{l_1(X) = 0\} + P\{l_2(Y) = 0\} + P\{\phi(X,Y) + l_1(X) = wX + vY\} + P\{\phi(X,Y) + l_2(Y) = wX + vY\} + P\{l_1(X) + l_2(Y) = 0\} + P\{\phi(X,Y) + l_1(X) + l_2(Y) = wX + vY\} - 3] + \frac{1}{4}[P\{\phi(X,Y) = wX + vY\} + P\{l_1(X) = 0\} + P\{l_2(Y) = 1\} + P\{\phi(X,Y) + l_1(X) = wX + vY\} + P\{\phi(X,Y) + l_2(Y) = wX + vY + 1\} + P\{l_1(X) + l_2(Y) = 1\} + P\{\phi(X,Y) + l_1(X) + l_2(Y) = wX + vY + 1\} - 3] + \frac{1}{4}[P\{\phi(X,Y) = wX + vY\} + P\{l_1(X) = 1\} + P\{l_2(Y) = 0\} + P\{\phi(X,Y) + l_1(X) = wX + vY + 1\} + P\{\phi(X,Y) + l_2(Y) = wX + vY\} + P\{l_1(X) + l_2(Y) = 1\} + P\{\phi(X,Y) + l_1(X) + l_2(Y) = wX + vY + 1\} - 3] + \frac{1}{4}[P\{\phi(X,Y) = wX + vY + 1\} + P\{l_1(X) = 1\}, P\{l_2(Y) = 1\} + P\{\phi(X,Y) + l_1(X) = wX + vY\} + P\{\phi(X,Y) + l_2(Y) = wX + vY\} + P\{l_1(X) + l_2(Y) = 0\} + P\{\phi(X,Y) + l_1(X) + l_2(Y) = wX + vY + 1\} - 3] = \frac{1}{2}[P\{\phi(X,Y) = wX + vY\} + P\{\phi(X,Y) + l_1(X) = wX + vY\} + P\{\phi(X,Y) + l_2(Y) = wX + vY\} + P\{\phi(X,Y) + l_1(X) + l_2(Y) = wX + vY + 1\}] - \frac{1}{2} = \frac{1}{4}[S(\phi)(w,v) + S_{(\phi+l_1)}(w,v) + S_{(\phi+l_2)}(w,v) - S_{(\phi+l_1+l_2)}(w,v)] + \frac{1}{2}。$$

由 Walsh 谱的概率表示式[6]知

$$S_{(\phi+l_1l_2)}(w,v)=\frac{1}{2}$$
$$[S_{(\phi)}(w,v)+S_{(\phi+l_1)}(w,v)+$$
$$S_{(\phi+l_2)}(w,v)-S_{(\phi+l_1+l_2)}(w,v)]。$$

下面利用定理 1，用递归方法给出一类布尔函数 Walsh 谱的分解式的证明。

定理 2　设 $n+r$ 元布尔函数

$$\psi_k(x,y)=f(x)+g(y)+\sum_{i=1}^{k}h_{1i}(x)\cdot h_{2i}(y),$$
$$x\in GF^n(2),y\in GF^r(2),$$

其中 $h_{1i}(x),x\in GF^n(2),1\leqslant i\leqslant k$ 都是 n 元布尔函数，$h_{2i}(y),y\in GF^r(2),1\leqslant i\leqslant k$ 都是 r 元布尔函数，记

$$h_1^{(k)}(x)=(h_{11}(x),h_{12}(x),\cdots,h_{1k}(x)),$$
$$h_2^{(k)}(y)=(h_{21}(x),h_{22}(y),\cdots,h_{2k}(y)),$$

则对任意的 $w\in GF^n(2),v\in GF^r(2)$，有

$$S_{(\psi_k)}(w,v)=\frac{1}{2^k}\sum_{a\in GF^k(2)}S_{(g+ah_2^{(k)})}(v)\cdot$$
$$\sum_{\beta\in GF^k(2)}(-1)^{a\beta}S_{(f+\beta h_1^{(k)})}(w);\qquad(2)$$

$$S_{(\psi_k)}(w,v)=\frac{1}{2^k}\sum_{\beta\in GF^k(2)}S_{(f+\beta h_1^{(k)})}(w)\cdot$$
$$\sum_{a\in GF^k(2)}(-1)^{a\beta}S_{(g+ah_2^{(k)})}(v)\qquad(3)$$

证明（归纳法）　当 $k=1$ 时，在定理 1 中，取

$$\phi(x,y)=f(x)+g(x),l_1(x)=h_{11}(x),$$
$$l_2(y)=h_{21}(y),$$

可得

$$S_{(f+g+h_{11}h_{21})}(w,v)=\frac{1}{2}[S_{(f)}(w)S_{(g)}(v)+$$
$$S_{(f+h_{11})}(w)S_{(g)}(v)+S_{(f)}(w)S_{(g+h_{21})}(v)-$$
$$S_{(f+h_{11})}(w)S_{(g+h_{21})}(v)]=$$
$$\frac{1}{2}S_{(g)}(v)[S_{(f)}(w)+S_{(f+h_{11})}(w)]+$$
$$\frac{1}{2}S_{(g+h_{21})}(v)[S_{(f)}(w)-S_{(f+h_{11})}(w)],$$

这正是文献 [7] 所给出的布尔函数的 Walsh 谱分解式。假设结论对 k 成立，即

$$S_{(\psi_k)}(w,v)=\frac{1}{2^k}\sum_{a\in GF^k(2)}S_{(g+ah_2^{(k)})}(v)\cdot$$
$$\sum_{\beta\in GF^k(2)}(-1)^{a\beta}S_{(f+\beta h_1^{(k)})}(w)。\qquad(4)$$

对 $k+1$，由归纳假设知

$$S_{(\psi_k+1)}(w,v)=\frac{1}{2}[S_{(\psi_k)}(w,v)+$$
$$S_{(\psi_k+h_{1k+1})}(w,v)+S_{(\psi_k+h_{2k+1})}(w,v)-$$
$$S_{(\psi_k+h_{1k+1}+h_{2k+1})}(w,v)]。\qquad(5)$$

在式(4)中，取 $f(x)$ 为 $f(x)+h_{1k+1}(x)$，则

$$S_{(\psi_k+h_{1k+1})}(w,v)=\frac{1}{2^k}\sum_{a\in GF^k(2)}S_{(g+ah_2^{(k)})}(v)\cdot$$
$$\sum_{\beta\in GF^k(2)}(-1)^{a\beta}S_{(f+h_{1k+1}+\beta h_1^{(k)})}(w)。$$

同理，在式（4）中，取 $g(y)$ 为 $g(y)+h_{2k+1}(y)$，则

$$S_{(\psi_k+h_{2k+1})}(w,v)=\frac{1}{2^k}\sum_{a\in GF^k(2)}S_{(g+h_{2k+1}+ah_2^{(k)})}(v)\cdot$$
$$\sum_{\beta\in GF^k(2)}(-1)^{a\beta}S_{(f+\beta h_1^{(k)})}(w)。$$

在式(4)中，取 $g(y)$ 为 $g(y)+h_{2k+1}(y)$，取 $f(x)$ 为 $f(x)+h_{1k+1}(x)$，则

$$S_{(\psi_k+h_{1k+1}h_{2k+1})}(w,v)=$$
$$\frac{1}{2^k}\sum_{a\in GF^k(2)}S_{(g+h_{2k+1}+ah_2^{(k)})}(v)\cdot$$
$$\sum_{\beta\in GF^k(2)}(-1)^{a\beta}S_{(f+h_{1k+1}\beta h_1^{(k)})}(w)。$$

由式(5)得

$$S_{(\psi_k+1)}(w,v)=\frac{1}{2^{k+1}}\sum_{a\in GF^k(2)}S_{(g+ah_2^{(k)})}(v)\cdot$$
$$\Big[\sum_{\beta\in GF^k(2)}(-1)^{a\beta}S_{(f+\beta h_1^{(k)})}(w)+$$
$$\sum_{\beta\in GF^k(2)}(-1)^{a\beta}S_{(f+h_{1k+1}+\beta h_1^{(k)})}(w)\Big]+$$
$$\frac{1}{2^{k+1}}\sum_{a\in GF^k(2)}S_{(g+h_{2k+1}+ah_2^{(k)})}(v)\cdot$$
$$\Big[\sum_{\beta\in GF^k(2)}(-1)^{a\beta}S_{(f+\beta h_1^{(k)})}(w)-$$
$$\sum_{\beta\in GF^k(2)}(-1)^{a\beta}S_{(f+h_{1k+1}+\beta h_1^{(k)})}(w)\Big]=$$
$$\frac{1}{2^{k+1}}\sum_{a\in GF^{k+1}(2)}S_{(g+ah_2^{(k+1)})}(v)\cdot$$
$$\sum_{\beta\in GF^{k+1}(2)}(-1)^{a\beta}S_{(f+\beta h_1^{(k+1)})}(w)。$$

所得结论对 $k+1$ 也成立，因而式(2)得证。

同样的方法，由 $f(x)$ 和 $g(y)$ 的对称性可得式(3)。

4　一类 Walsh 谱分解式在密码函数的构造中的应用

文献 [8] 指出了研究弹性函数——平衡的相

关免疫函数的意义，并给出了弹性函数的一些构造方法。下面的定理表明，利用上面的Walsh谱的分解式也可以递归构造弹性函数。

定理3 设 $\psi_k(x,y)=f(x)+g(y)+\sum_{i=1}^{k}h_{1i}(x)h_{2i}(y)$，$h_1^{(k)}(x)$和$h_2^{(k)}(y)$如定理2中所定义，若对任意的$\alpha,\beta\in GF^k(2)$，$f(x)+\beta h_1^{(k)}(x)$都是$m_1$阶弹性函数，$g(y)+\alpha h_2^{(k)}(y)$都是$m_2$阶弹性函数，则$\psi_k(x,y)$是$n+r$元$m_1+m_2+1$阶弹性函数。

证明 对任意的$w\in GF^n(2)$，$v\in GF^r(2)$，若$W(w,v)\leqslant m_1+m_2+1$，则有下列两种情况：

1) $w=0$或$v=0$，设$w=0$，则由式(2)知

$$S_{(\psi_k)}(0,v)=\frac{1}{2^k}\sum_{\alpha\in GF^k(2)}S_{(g+\alpha h_2^{(k)})}(v)\cdot\sum_{\beta\in GF^k(2)}(-1)^{\alpha\beta}S_{(f+\beta h_1^{(k)})}(0),$$

由$f(x)+\beta h_1^{(k)}(x)$是平衡函数知

$S_{(f+\beta h_1^{(k)})}(0)=0$，所以$S_{(\psi_k)}(0,v)=0$。

当$v=0$时，同样的方法，由式(3)知$S_{(\psi_k)}(w,0)=0$。

2) $w\neq 0$且$v\neq 0$，则此时或者$W(w)\leqslant m_1$，或者$W(v)\leqslant m_2$，不妨设$W(w)\leqslant m_1$，则由于对任意的$\beta\in GF^k(2)$，$f(x)+\beta h_1^{(k)}(x)$是m_1阶弹性函数，即$S_{(f+\beta h_1^{(k)})}(w)=0$，由式(2)知

$$S_{(\psi_k)}(w,v)=\frac{1}{2^k}\sum_{\alpha\in GF^k(2)}S_{(g+\alpha h_2^{(k)})}(v)\cdot\sum_{\beta\in GF^k(2)}(-1)^{\alpha\beta}S_{(f+\beta h_2^{(k)})}(w)=0。$$

若$W(v)\leqslant m_2$，同样的方法，由式(3)知$S_{(\psi_k)}(w,v)=0$。

所以由定义2知$\psi_k(x,y)$是$n+r$元m_1+m_2+1阶弹性函数。

推论1 设 $\psi_k(x,y)=f(x)+g(y)+\sum_{i=1}^{k}h_{1i}(x)h_{2i}(y)$，$h_1^{(k)}(x)$和$h_2^{(k)}(y)$如定理2中所定义，若对任意的$\alpha,\beta\in GF^k(2)$，$f(x)+\beta h_1^{(k)}(x)$是$m_1$阶弹性函数，$g(y)+\alpha h_2^{(k)}(y)$是任意$r$元平衡的布尔函数，则$\psi_k(x,y)$是$n+r$元$m_1+1$阶弹性函数。

注：在定理3中，特别地取$k=2$，即得文献[8]的结论。

Bent函数的构造也是密码设计者关心的问题，利用上面的Walsh谱的分解式同样可以由变元个数少的Bent函数构造变元个数多的Bent函数。

定理4 设 $\psi_k(x,y)=f(x)+g(y)+\sum_{i=1}^{k}h_{1i}(x)h_{2i}(y)$，$h_1^{(k)}(x)$和$h_2^{(k)}(y)$如定理2中所定义，若对任意的$\alpha,\beta\in GF^k(2)$，$f(x)+\beta h_1^{(k)}(x)$和$g(y)+\alpha h_2^{(k)}(y)$都是Bent函数，且下列条件之一成立：

1) 对任意给定的$w\in GF^n(2)$，存在$\alpha_w\in GF^k(2)$，$b_w\in GF(2)$(只与w有关)，使得对任意的$\beta\in GF^k(2)$，都有

$$S_{(f+\beta h_1^{(k)})}(w)=2^{-n/2}(-1)^{\alpha_w\beta+b_w};$$

2) 对任意给定的$v\in GF^r(2)$，存在$\beta_v\in GF^k(2)$，$b_v\in GF(2)$(只与v有关)，使得对任意的$\alpha\in GF^k(2)$，都有

$$S_{(g+\alpha h_1^{(k)})}(v)=2^{-r/2}(-1)^{\beta_v\alpha+b_v};$$

则$\psi_k(x,y)$是$n+r$元Bent函数。

证明 1)若对任意给定的$w\in GF^n(2)$，存在$\alpha_w\in GF^k(2)$，$b_w\in GF(2)$，使得对任意的$\beta\in GF^k(2)$，都有

$$S_{(f+\beta h_1^{(k)})}(w)=2^{-n/2}(-1)^{\alpha_w\beta+b_w},$$

则由式(2)知

$$S_{(\psi_k)}(w,v)=\frac{1}{2^k}\sum_{\alpha\in GF^k(2)}S_{(g+\alpha h_2^{(k)})}(v)\cdot\sum_{\beta\in GF^k(2)}(-1)^{\alpha\beta}S_{(f+\beta h_1^{(k)})}(w)=2^{-k-n/2}\sum_{\alpha\in GF^k(2)}S_{(g+\alpha h_2^{(k)})}(v)\cdot\sum_{\beta\in GF^k(2)}(-1)^{\alpha\beta+\alpha_w\beta+b_w}\overset{\text{正交性}}{=}2^{-n/2}(-1)^{b_w}S_{(g+\alpha_w h_2^{(k)})}(v)$$

所以$\psi_k(x,y)$是$n+r$元Bent函数。

用同样的方法，由式(3)可以证明，当条件2成立时$\psi_k(x,y)$是$n+r$元Bent函数。

注：在上面的定理中，当$k=1$时，则对任意的$w\in GF^n(2)$，$S_{(f)}(w)$和$S_{(f+h_{11})}(w)$自然满足条件1；当$k=2$时，若对任意的$w\in GF^n(2)$，$S_{(f)}(w)$，$S_{(f+h_{11})}(w)$，$S_{(f+h_{12})}(w)$，$S_{(f+h_{11}+h_{12})}(w)$同号，或两个为正值、两个为负值时，则满足定理的条件1。

下面给出一类满足定理4条件的函数的构造：

定理5 设$f(x)=\pi(x^{(2)})x^{(1)}$，$x=(x^{(1)},$

$x^{(2)}) \in GF^{2n}(2)$，其中 π 为 $GF^n(2)$ 到 $GF^n(2)$ 的置换，又设 $h_{1i}(x^{(1)}, x^{(2)}) = l_i(x^{(2)})(1 \leqslant i \leqslant k)$，$g(y), h_{2i}(y)(1 \leqslant i \leqslant k), y \in GF^r(2)$ 满足：对任意的 $a \in GF^k(2)$，$g(y) + ah_2^{(k)}(y)$ 都是 Bent 函数，则

$$\psi_k(x,y) = f(x) + g(y) + \sum_{i=1}^{k} l_i(x^{(2)}) h_{2i}(y)$$

是 $2n + r$ 元 Bent 函数。

证明　记 $l^{(k)}(x^{(2)}) = (l_1(x^{(2)}), \cdots, l_k(x^{(2)}))$，则对任意的 $w^{(1)}, w^{(2)} \in GF^n(2)$，及任意的 $\beta \in GF^k(2)$，有

$$S_{(f+\beta h_1^{(k)})}(w^{(1)}, w^{(2)}) = 2^{-2n} \sum_{x^{(1)} \in GF^n(2), x^{(2)} \in GF^n(2)} (-1)^{\pi(x^{(2)})x^{(1)} + \beta l^{(k)}(x^{(2)}) + w^{(1)}x^{(1)} + w^{(2)}x^{(2)}} =$$

$$2^{-2n} \sum_{x^{(2)} \in GF^n(2)} (-1)^{\beta l^{(k)}(x^{(2)}) + w^{(2)}x^{(2)}} \sum_{x^{(1)} \in GF^n(2)} (-1)^{(\pi(x^{(2)}) + w^{(1)})x^{(1)}} = 2^{-2n}(-1)^{\beta l^{(k)}(x^{(2)}_{w^{(1)}}) + w^{(2)}x^{(2)}_{w^{(1)}}},$$

则 $a_{(w^{(1)}, w^{(2)})} = l^{(k)}(x^{(2)}_{w^{(1)}}) = (l_1(x^{(2)}_{w^{(1)}}), l_2(x^{(2)}_{w^{(1)}}), \cdots, l_k(x^{(2)}_{w^{(1)}}))$，而 $b_{(w^{(1)}, w^{(2)})} = w^{(2)}x^{(2)}_{w^{(1)}}$，其中 $\pi(x^{(2)}_{w^{(1)}}) = w^{(1)}$，所以对任意的 $\beta \in GF^k(2)$，$S_{(f+\beta h_1^{(k)})}(w^{(1)}, w^{(2)})$ 满足定理 4 的条件 1，因此 $\psi_k(x,y)$ 是 $2n + r$ 元 Bent 函数。

下面考察了在一定的限制条件下，$\psi_k(x,y)$ 的自相关特征：

定理 6　设 $\psi_k(x,y) = f(x) + g(y) + \sum_{i=1}^{k} h_{1i}(x)h_{2i}(y)$，$h_1^{(k)}(x)$ 和 $h_2^{(k)}(y)$ 如定理 2 中所定义，若对任意的 $\alpha, \beta \in GF^k(2)$，$f(x) + \beta h_1^{(k)}(x)$ 都是满足 l_1 次扩散准则的 n 元布尔函数，$g(y) + ah_2^{(k)}(y)$ 都是满足 l_2 次扩散准则的 r 元布尔函数，则对任意的 $s_1 \in GF^n(2), s_2 \in GF^r(2)$，且 $W(s_1) \leqslant l_1, W(s_2) \leqslant l_2$，$\psi_k(x,y)$ 的自相关函数满足：

1) $r_{\psi_k}(s_1, 0) = 0$；

2) $r_{\psi_k}(0, s_2) = 0$；

证明　对任意的 $s_1 \in GF^n(2), W(s_1) \leqslant l_1$，由 X 和 Y 的相互独立性知

$$P\{\psi_k(X + s, Y) + \psi_k(X, Y) = 0\} =$$

$$P\{f(X + s_1) + \sum_{i=1}^{k} h_{1i}(X + s_1)h_{2i}(Y) + f(x) + \sum_{i=1}^{k} h_{1i}(X)h_{2i}(Y) = 0\} =$$

$$\sum_{\beta \in GF^k(2)} P\{h_2^{(k)}(Y) = \beta, f(X + s_1) + f(x) + \beta(h_1^{(k)}(X + s_1) + h_1^{(k)}(X)) = 0\} =$$

$$\sum_{\beta \in GF^k(2)} P\{h_2^{(k)}(Y) = \beta\} P\{f(X + s_1) + \beta h_1^{(k)}(X + s_1) + f(X) + \beta h_1^{(k)}(X) = 0\},$$

由于对 $\beta \in GF^k(2)$，$f(x) + \beta h_1^{(k)}(x)$ 都是满足 l_1 次扩散准则，即

$$P\{f(X + s_1) + \beta h_1^{(k)}(X + s_1) + f(X) + \beta h_1^{(k)}(X) = 0\} = 1/2,$$

所以

$$P\{\psi_k(X + s, Y) + \psi_k(X, Y) = 0\} = \frac{1}{2} \sum_{\beta \in GF^k(2)} P\{h_2^{(k)}(Y) = \beta\} = \frac{1}{2},$$

即 $r_{\psi_k}(s_1, 0) = 0$。对任意的 $s_2 \in GF^r(2)$，由对称性同样可证 $r_{\psi_k}(0, s_2) = 0$。

在实际应用中，平衡且满足严格雪崩准则的函数有很大的应用价值，同时满足严格雪崩的布尔函数和 H 函数是等价的，它是阵列编码中的一个重要的函数类。因此，构造平衡且满足严格雪崩准则的布尔函数具有重要意义，而下面的定理表明利用上面的谱分解式可以递归构造平衡的满足严格雪崩的布尔函数。

定理 7　设 $\psi_k(x,y) = f(x) + g(y) + \sum_{i=1}^{k} h_{1i}(x)h_{2i}(y)$，$h_1^{(k)}(x)$ 和 $h_2^{(k)}(y)$ 如定理 2 中所定义，若对任意的 $\alpha, \beta \in GF^k(2)$，$f(x) + \beta h_1^{(k)}(x)$ 都是平衡且满足严格雪崩准则的 n 元布尔函数，$g(y) + ah_2^{(k)}(y)$ 都是满足严格雪崩准则的 r 元布尔布尔函数，则 $\psi_k(x,y)$ 是 $n + r$ 元平衡且满足严格雪崩准则的布尔函数。

证明　平衡性由式 (2) 可证，而满足严格雪崩准则由定理 6 可知。

注：在上面的定理中，并不要求 $g(y) + ah_2^{(k)}(y)$ 是平衡的布尔函数。

例 1　设 $f(x) = x_0(x_1x_2 + x_3) + x_1x_4 + x_2x_5 + (x_0 + x_1 + x_2 + 1)x_6, x \in GF^7(2)$；

$h_{11}(x) = (x_0 + x_1)x_3 + x_0(x_1 + x_1x_2 + x_4) +$

$$(x_1+1)x_5+x_2x_6+x_2, x\in GF^7(2);$$

$$h_{12}(x)=(x_0+x_1+x_2)x_3+(1+x_0+x_2)x_4+x_0x_5+x_1x_6, x\in GF^7(2);$$

$$g(y)=y_0(y_1y_2+y_3)+y_1y_4+y_2y_5+(y_0+y_1+y_2+1)y_6, y\in GF^7(2);$$

$$h_{21}(y)=(y_0+y_1)y_3+y_0(y_1+y_1y_2+y_4)+(y_1+1)y_5+y_2y_6+y_2, y\in GF^7(2);$$

$$h_{22}(y)=(y_0+y_1+y_2)y_3+(1+y_0+y_2)y_4+y_0y_5+y_1y_6, y\in GF^7(2)。$$

则可以验证 $f(x), h_{11}(x), h_{12}(x), g(y), h_{21}(y), h_{22}(y)$ 满足定理 7 的条件，所以函数 $\psi_2(x,y)=f(x)+g(y)+h_{11}(x)h_{21}(y)+h_{12}(x)$ 是平衡的满足严格雪崩准则的 14 元布尔函数。

5 结语

给出了结构形式更为一般的一类布尔函数 Walsh 谱的分解式，并利用这种谱分解式给出了在密码设计中有重要应用的弹性函数和 Bent 函数的一些新的递归构造方法，还利用这种谱分解式和概率的方法考察了一类特殊布尔函数的自相关特征等，构造了平衡且满足严格雪崩准则的一类布尔函数。而且利用所提的方法也可以给出多输出 Bent 函数[11]的递归构造等。

参考文献

[1] Siegenthaler T. Correlation—immunity of the combining functions for cryptographic applications [J]. IEEE Trans, on Inform. Theory, 1984, IT-30(5): 776~780

[2] Rothaus O S. On Bent functions [J]. J Combinatorial Theory (Ser A), 1976, 20: 300~305

[3] Camion P, Canleaut A. Construction of t-resilient functions over a finite alphabet [M]. Advances in Cryptology, Eurocrypt'96, Springer Verlag, 1996. 283~293

[4] Zhang X M, Zheng Y. On nonlinear resilient functions [M]. Advances in Cryptology, Eurocrypt'95, Springer Verlag, 1995. 274~288

[5] Yarlagadda R, Hershey J E. Analysis and synthesis of Bent sequences [A]. IEEE Proceeding (Part E) [C], 1989, 136: 112~123

[6] 李世取，曾本胜，廉玉忠，等. 密码学中的逻辑函数 [M]. 北京：北京中软出版公司，2003

[7] 曾本胜，李世取，李 坤. 一类布尔函数 Walsh 谱的分解式及其应用 [A]. 密码学进展—CHINACRYPT'98 [M]. 北京：科学出版社，1998. 217~220

[8] 刘文芬. 关于具有相关免疫性的多值逻辑函数的性质和构造研究 [D]. 郑州：解放军信息工程学院，1999

[9] 李世取，曾本胜，廉玉忠. 布尔随机向量联合分布的分解式及其应用 [J]. 通信学报，1998，(11)：61~64

[10] 杨义先，林须端. 编码密码学 [M]. 北京：人民邮电出版社，1992

[11] 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

The Constructions of Cryptographic Functions

Teng Jihong, Zhang Wenying, Liu Wenfen, Li Shiqu

(*Department of Information Research, Information Engineering University, Zhengzhou* 450002, *China*)

[**Abstract**] This paper investigates a decomposition formula of Walsh spectrum for a class of Boolean functions. On the basis of this formula, the constructions of some cryptographic functions, such as resilient functions, Bent functions and H-Boolean function are studied H-Boolean function is a class of Boolean functions of much importance to the applications of coding theory and satisfying the strict Avalanche criterion.

[**Key words**] Walsh spectrum; decomposition formula of Walsh spectrum; Bent function; resilient function; strict avalanche criterion