学 术 论 文

选择逻辑函数的密码学性质

梁 增，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] 通过计算选择逻辑函数的 Walsh 循环谱和自相关函数，系统分析了选择逻辑函数的密码学性质。所得结论表明选择逻辑函数在变元个数较大的情况下具有理想的稳定性，能够抵抗最佳仿射（BAA）攻击，但是其“扩散”特性不够理想，在一定意义下不能有效地抗击差分攻击。讨论了与选择逻辑函数线性等价意义下满足严格雪崩准则或具有相关免疫性的逻辑函数构造问题。

[关键词] 选择逻辑函数；Walsh 循环谱；自相关函数；严格雪崩准则；相关免疫；概率表示式
[中图分类号] TN918.1 [文献标识码] A [文章编号] 1009－1742（2005）07－0050－05

1 引言

逻辑函数在当今密码设计与分析中的重要性是众所周知的，因而 20 多年来关于逻辑函数的性质及具有特殊性质的逻辑函数的构造一直是密码学中最活跃的研究领域之一。文献[1]介绍了推广的 Geffe 发生器（见图 1），它是由 2^n+1 个线性移位寄存器（LFSR）和一个选择逻辑函数组成，其中 LFSR－2^n+1 比其他 2^n 个 LFSR 运行快 n 倍。当 $n=1$ 时，此发生器就是 Geffe 发生器[2]，不能抵抗相关攻击[3]。目前有关推广的 Geffe 发生器的复合器中使用选择逻辑函数的研究成果还不多见。

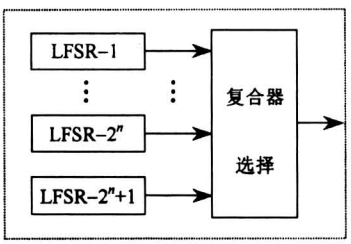

图 1 推广的 Geffe 发生器

Fig.1 Generalized Geffe generators

笔者分析了推广的 Geffe 发生器的复合器中使用的选择逻辑函数的 Walsh 循环谱和自相关函数，得到如下结论：$n+2^n$ 元选择逻辑函数 $f(\boldsymbol{x}, \boldsymbol{y})$ 的 Walsh 循环谱的取值为 0 或 $\pm 2^{-n}$，因而对于较小的 n，抵抗相关攻击的能力比较弱；对于较大的 n，$f(\boldsymbol{x}, \boldsymbol{y})$ 的稳定性比较理想，能够抵抗最佳仿射（BAA）攻击；尽管 $f(\boldsymbol{x}, \boldsymbol{y})$ 只有一个非零线性结构点，但是对于较大的 n 其自相关函数值接近于 1 或 －1 的点很多，特别有大部分汉明重量为 1，2 等的点的自相关函数值接近于 1 和大部分汉明重量为 2^n-1，2^n-2 等的点的自相关函数值接近于 －1，因而 $f(\boldsymbol{x}, \boldsymbol{y})$ 在一定意义下不能有效地抗击差分攻击。

为了进一步提高 $f(\boldsymbol{x}, \boldsymbol{y})$ 抵抗密码分析的能力，讨论了与 $f(\boldsymbol{x}, \boldsymbol{y})$ 线性等价意义下或满足严格雪崩准则[4]、或具有相关免疫[5]性、或同时具有这两种性质的逻辑函数构造问题。

2 基本概念

2.1 汉明重量的定义

设 $\boldsymbol{w}=(w_1, w_2, \cdots, w_n) \in \mathrm{GF}^n(2)$ 是 n 维布尔向量，称 $\boldsymbol{w}=(w_1, w_2, \cdots, w_n)$ 的不为零的分量的个数为其汉明重量，且记之为 $\boldsymbol{W}_{\mathrm{H}}(\boldsymbol{w})$。

[收稿日期] 2005－01－06；修回日期 2005－03－03
[作者简介] 梁 增（1973－），男，广东阳江市人，解放军信息工程大学信息工程学院硕士研究生

2.2 点积的定义[6]

设 $\boldsymbol{x}=(x_1, x_2, \cdots, x_n)\in \mathrm{GF}^n(2)$, $\boldsymbol{w}=(w_1, w_2, \cdots, w_n)\in \mathrm{GF}^n(2)$, $\boldsymbol{x}$ 和 $\boldsymbol{w}$ 的点积定义为

$$\boldsymbol{w}\cdot\boldsymbol{x}=w_1x_1+w_2x_2+\cdots+w_nx_n(\mathrm{mod}\ 2)。$$

2.3 选择逻辑函数的定义

根据推广的 Geffe 发生器中 LFSR－2^n+1 比其他 2^n 个 LFSR 运行快 n 倍，可以假定 LFSR－2^n+1 输出 $\boldsymbol{x}=(x_1, x_2, \cdots, x_n)$，LFSR－1 输出 y_1，LFSR－2 输出 y_2，…，LFSR－2^n 输出 y_{2^n} 由于 $y_1, y_2, \cdots, y_{2^n}$ 的取值互不相干，就可以如下定义选择逻辑函数：

若 $n+2^n$ 元布尔函数为

$$f(\boldsymbol{x}, \boldsymbol{y})=x_1x_2\cdots x_ny_{2^n}+(1+x_1)x_2\cdots x_ny_{2^n-1}+x_1(1+x_2)\cdots x_n y_{2^n-2}+\cdots+(1+x_1)(1+x_2)\cdots(1+x_n)y_1,$$

$$(\boldsymbol{x}, \boldsymbol{y})=(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_{2^n})\in \mathrm{GF}^{n+2^n}(2),$$

则称 $f(\boldsymbol{x}, \boldsymbol{y})$) 为选择逻辑函数。

由定义可知：当 $\boldsymbol{x}=(0, 0, \cdots, 0)$ 时，$f(\boldsymbol{x}, \boldsymbol{y})=y_1$；当 $\boldsymbol{x}=(1, 0, \cdots, 0)$ 时，$f(\boldsymbol{x}, \boldsymbol{y})=y_2$；……；当 $\boldsymbol{x}=(1, 1, \cdots, 1)$ 时，$f(\boldsymbol{x}, \boldsymbol{y})=y_{2^n}$。

2.4 Walsh 循环谱的定义[6]

n 元布尔函数 $f(\boldsymbol{x})$，$\boldsymbol{x}\in \mathrm{GF}^n(2)$ 的第二种 Walsh 变换定义为

$$S_{(f)}(\boldsymbol{w})=2^{-n}\sum_{x\in \mathrm{GF}^n(2)}(-1)^{f(\boldsymbol{x})+\boldsymbol{w}\cdot\boldsymbol{x}}, \boldsymbol{w}\in \mathrm{GF}^n(2),$$

称 $S_{(f)}(\boldsymbol{w})$，$\boldsymbol{w}\in \mathrm{GF}^n(2)$ 为 $f(\boldsymbol{x})$ 的 Walsh 循环谱。

2.5 自相关函数定义[7]

设 $f(\boldsymbol{x})$，$\boldsymbol{x}\in \mathrm{GF}^n(2)$ 是布尔函数，对

$$\boldsymbol{x}=(x_1, x_2, \cdots, x_n)\in \mathrm{GF}^n(2),$$

$$\boldsymbol{s}=(s_1, s_2, \cdots, s_n)\in \mathrm{GF}^n(2),$$

$$\boldsymbol{x}+\boldsymbol{s}=(x_1+s_1, x_2+s_2, \cdots, x_n+s_n),$$

称

$$r_f(\boldsymbol{s})=2^{-n}\sum_{x\in \mathrm{GF}^n(2)}(-1)^{f(\boldsymbol{x})+f(\boldsymbol{x}+\boldsymbol{s})}, \boldsymbol{s}\in \mathrm{GF}^n(2)$$

为 $f(\boldsymbol{x})$ 的自相关函数。

3 主要结果

以下假定

$$\boldsymbol{X}=(X_1, X_2, \cdots, X_n),$$

$$\boldsymbol{Y}=(Y_1, Y_2, \cdots, Y_{2^n}),$$

$$(\boldsymbol{X}, \boldsymbol{Y})=(X_1, X_2, \cdots, X_n, Y_1, Y_2, \cdots, Y_{2^n})$$

中的 $X_1, X_2, \cdots, X_n, Y_1, Y_2, \cdots, Y_{2^n}$ 是定义在同一概率空间相互独立，且具有均匀分布

$$P\{X_i=0\}=P\{X_i=1\}=P\{Y_j=0\}=P\{Y_j=1\}=2^{-1},$$

$$1\leqslant i\leqslant n, 1\leqslant j\leqslant 2^n$$

的布尔随机变量[7]。

选择逻辑函数 $f(\boldsymbol{x}, \boldsymbol{y})$ 可以写成如下形式

$$f(\boldsymbol{x}, \boldsymbol{y})=\sum_{(a_1,\cdots,a_n)\in \mathrm{GF}^n(2)}(x_1+1+a_1)\cdots(x_n+1+a_n)y_{\bar{a}+1},$$

$$(\boldsymbol{x}, \boldsymbol{y})=(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_{2^n})\in \mathrm{GF}^{n+2^n}(2),$$

其中非负整数 $\bar{a}$ 的二进制展式为

$$a_n+2a_{n-1}+\cdots+2^{n-2}a_2+2^{n-1}a_1。$$

根据

$$P\{f(\boldsymbol{X}, \boldsymbol{Y})=0\}=\sum_{a\in \mathrm{GF}^n(2)}P\{f(\boldsymbol{X}, \boldsymbol{Y})=0, \boldsymbol{X}=\boldsymbol{a}\}=\sum_{a\in \mathrm{GF}^n(2)}P\{Y_{\bar{a}+1}=0\}P\{\boldsymbol{X}=\boldsymbol{a}\}=2^{-1}\sum_{a\in \mathrm{GF}^n(2)}P\{\boldsymbol{X}=\boldsymbol{a}\}=2^{-1},$$

即知 $f(\boldsymbol{x}, \boldsymbol{y})$ 是平衡的。

3.1 选择逻辑函数 Walsh 循环谱

布尔函数的稳定性是判断其密码学性质的一个重要指标，而布尔函数的稳定性是通过其 Walsh 循环谱予以刻画的[6]，因而分析了选择逻辑函数的 Walsh 循环谱。

定理 1　若 $f(\boldsymbol{x}, \boldsymbol{y})$ 是 $n+2^n$ 元选择逻辑函数，对任意的 $\boldsymbol{w}\in \mathrm{GF}^n(2)$，$\boldsymbol{v}\in \mathrm{GF}^{2^n}(2)$：

1) 当 $\boldsymbol{W}_{\mathrm{H}}(\boldsymbol{v})=1$ 时，$|S_{(f)}(\boldsymbol{w}, \boldsymbol{v})|=2^{-n}$；

2) 当 $\boldsymbol{W}_{\mathrm{H}}(\boldsymbol{v})\neq 1$ 时，$S_{(f)}(\boldsymbol{w}, \boldsymbol{v})=0$。

证明：

1) 当 $\boldsymbol{W}_{\mathrm{H}}(\boldsymbol{v})=1$ 时，设 $\boldsymbol{v}$ 的第 $\bar{\boldsymbol{b}}+1$ 个分量为 1，

$$\boldsymbol{b}=(b_1, \cdots, b_n)\in \mathrm{GF}^n(2),$$

$$\bar{\boldsymbol{b}}=b_n+2b_{n-1}+\cdots+2^{n-2}b_2+2^{n-1}b_1,$$

由逻辑函数的 Walsh 循环谱的概率表示式[7]可知，

$$S_{(f)}(\boldsymbol{w}, \boldsymbol{v})=2P\{f(\boldsymbol{X}, \boldsymbol{Y})+(\boldsymbol{w}, \boldsymbol{v})\cdot(\boldsymbol{X}, \boldsymbol{Y})=0\}-1 \qquad (1)$$

因为

$$P\{f(\boldsymbol{X},\boldsymbol{Y})+(\boldsymbol{w},\boldsymbol{v})\cdot(\boldsymbol{X},\boldsymbol{Y})=0\}=$$
$$P\{f(\boldsymbol{X},\boldsymbol{Y})+\boldsymbol{w}\cdot\boldsymbol{X}+\boldsymbol{Y}_{\bar{b}+1}\}=0\}=$$
$$\sum_{a\in GF^n(2)} P\{f(\boldsymbol{X},\boldsymbol{Y})+\boldsymbol{w}\cdot\boldsymbol{X}+\boldsymbol{Y}_{\bar{b}+1}=0,\ \boldsymbol{X}=\boldsymbol{a}\}=$$
$$\sum_{a\in GF^n(2),a\neq b} P\{f(\boldsymbol{X},\boldsymbol{Y})+\boldsymbol{w}\cdot\boldsymbol{X}+\boldsymbol{Y}_{\bar{b}+1}=0,\ \boldsymbol{X}=\boldsymbol{a}\}+P\{\boldsymbol{w}\cdot\boldsymbol{b}=0,\ \boldsymbol{X}=\boldsymbol{b}\} \quad (2)$$

根据随机变量 $X_1, X_2, \cdots, X_n, Y_1, Y_2, \cdots, Y_{2^n}$ 之间的相互独立性可知

$$\sum_{a\in GF^n(2),a\neq b} P\{f(\boldsymbol{X},\boldsymbol{Y})+\boldsymbol{w}\cdot\boldsymbol{X}+\boldsymbol{Y}_{\bar{b}+1}=0,\ \boldsymbol{X}=\boldsymbol{a}\}=$$
$$2^{-1}\sum_{a\in GF^n(2),a\neq b} P\{\boldsymbol{X}=\boldsymbol{a}\}=2^{-n-1}(2^n-1), \quad (3)$$

由式 (1) 至式 (3) 即得:

当 $\boldsymbol{w}\cdot\boldsymbol{b}=0$ 时,

$S_{(f)}(\boldsymbol{w},\boldsymbol{v})=2[2^{-n}+2^{-n-1}(2^n-1)]-1=2^{-n}$;

当 $\boldsymbol{w}\cdot\boldsymbol{b}\neq 0$ 时,

$S_{(f)}(\boldsymbol{w},\boldsymbol{v})=2\times 2^{-n-1}(2^n-1)-1=-2^{-n}$。

所以,

$$|S_{(f)}(\boldsymbol{w},\boldsymbol{v})|=2^{-n}。$$

2) 因为

$$\sum_{w\in GF^n,v\in GF^{2^n}(2),W_H(v)=1}[S_{(f)}(\boldsymbol{w},\boldsymbol{v})]^2=\sum_{w\in GF^n,v\in GF^{2^n}(2),W_H(v)=1}2^{-2n}=1,$$

再由能量守恒定理[6] (Parseval 定理) 知, 任给 $\boldsymbol{w}\in GF^n(2)$, $\boldsymbol{v}\in GF^n(2)$, 当 $\boldsymbol{W}_H(\boldsymbol{v})\neq 1$ 时,

$$S_{(f)}(\boldsymbol{w},\boldsymbol{v})=0。$$

综上所述, $n+2^n$ 元选择逻辑函数 $f(\boldsymbol{x},\boldsymbol{y})$ 的 Walsh 循环谱的取值为 0 或 $\pm 2^{-n}$。由于当 $\boldsymbol{W}_H(\boldsymbol{v})=1$ 时, $|S_{(f)}(\boldsymbol{w},\boldsymbol{v})|=2^{-n}$, 因而对于较小的 n, 抵抗相关攻击的能力比较弱; 对于较大的 n, $f(\boldsymbol{x},\boldsymbol{y})$ 的稳定性比较理想, 能够抵抗最佳仿射 (BAA) 攻击。

3.2 选择逻辑函数的自相关特征

逻辑函数的自相关函数能刻画逻辑函数的扩散特征和线性结构特征, 在逻辑函数的性质研究中发挥了重要作用[7]。

引理 1[8] 设 $f(\boldsymbol{x}),\boldsymbol{x}\in GF^n(2)$ 是布尔函数, 其自相关函数和 Walsh 谱分别为 $r_f(\boldsymbol{s}),\boldsymbol{s}\in GF^n(2)$ 和 $S_{(f)}(\boldsymbol{w}),\boldsymbol{w}\in GF^n(2)$, 则

$$\sum_{w\in GF^n(2)} S^2_{(f)}(\boldsymbol{w})(-1)^{\boldsymbol{w}\cdot\boldsymbol{s}}=r_f(\boldsymbol{s}),\boldsymbol{s}\in GF^n(2)。$$

定理 2 若 $f(\boldsymbol{x},\boldsymbol{y})$ 是 $n+2^n$ 元选择逻辑函数, 对任意的 $\boldsymbol{s}\in GF^n(2)$, $\boldsymbol{t}\in GF^{2^n}(2)$:

1) 当 $\boldsymbol{s}\neq(0,0,\cdots,0)$ 时, $r_f(\boldsymbol{s},\boldsymbol{t})=0$;

2) 记 $0=(0,0,\cdots,0)\in GF^n(2)$, 则

$$r_f(0,\boldsymbol{t})=1-2^{1-n}\boldsymbol{W}_H(\boldsymbol{t})。$$

证明

1) 由引理 1 和定理 1 可知,

$$r_f(\boldsymbol{s},\boldsymbol{t})=\sum_{w\in GF^n(2),v\in GF^{2^n}(2)} S^2_{(f)}(\boldsymbol{w},\boldsymbol{v})(-1)^{\boldsymbol{w}\cdot\boldsymbol{s}+\boldsymbol{v}\cdot\boldsymbol{t}}=$$
$$\sum_{w\in GF^n(2),v\in GF^{2^n}(2),W_H(v)=1} S^2_{(f)}(\boldsymbol{w},\boldsymbol{v})(-1)^{\boldsymbol{w}\cdot\boldsymbol{s}+\boldsymbol{v}\cdot\boldsymbol{t}}=$$
$$2^{-2n}\sum_{v\in GF^{2^n}(2),W_H(v)=1}(-1)^{\boldsymbol{v}\cdot\boldsymbol{t}}\sum_{w\in GF^n(2)}(-1)^{\boldsymbol{w}\cdot\boldsymbol{s}} \quad (4)$$

当 $\boldsymbol{s}\neq(0,0,\cdots,0)$ 时,

$$\sum_{w\in GF^n(2)}(-1)^{\boldsymbol{w}\cdot\boldsymbol{s}}=0,$$

因而可得

$$r_f(\boldsymbol{s},\boldsymbol{t})=0。$$

2) 由式 (4) 可知,

$$r_f(0,\boldsymbol{t})=2^{-n}\sum_{v\in GF^{2^n}(2),W_H(v)=1}(-1)^{\boldsymbol{v}\cdot\boldsymbol{t}}=$$
$$2^{-n}(2^n-2\boldsymbol{W}_H(\boldsymbol{t}))=1-2^{1-n}\boldsymbol{W}_H(\boldsymbol{t})。$$

由定理 2 可知, 只有当 $\boldsymbol{W}_H(\boldsymbol{t})=2^n$ 即 $\boldsymbol{t}=(1,1,\cdots,1)$ 时, $r_f(0,\boldsymbol{t})=-1$, 因而 $f(\boldsymbol{x},\boldsymbol{y})$ 只有一个非零线性结构点。

对取定的任一正整数 k, 当 $\boldsymbol{t}\in GF^{2^n}(2)$ 且 $\boldsymbol{W}_H(\boldsymbol{t})=k$ 时, 有

$$r_f(0,\boldsymbol{t})=1-\frac{k}{2^{n-1}}\xrightarrow[n\to\infty]{}1;$$

当 $\boldsymbol{t}\in GF^{2^n}(2)$ 且 $\boldsymbol{W}_H(\boldsymbol{t})=2^n-k$ 时, 有

$$r_f(0,\boldsymbol{t})=-1+\frac{k}{2^{n-1}}\xrightarrow[n\to\infty]{}-1,$$

因而当 n 较大时, $GF^{n+2^n}(2)$ 中大部分汉明重量为 1,2 等点的自相关函数接近于 1, 且大部分汉明重量为 $2^n-1, 2^n-2$ 等点的自相关函数接近于 -1, 故选择逻辑函数抵抗差分密码分析的能力比较弱, 在一定意义下不能有效地抗击差分攻击。

3.3 线性等价意义下满足严格雪崩准则或具有相

关免疫性的逻辑函数构造

令 $\boldsymbol{x} \in \mathrm{GF}^{n+2^n}(2)$，对 $n+2^n$ 元选择逻辑函数 $f(\boldsymbol{x})$，记

$$\boldsymbol{S}_{f0} = \{\boldsymbol{w} : \boldsymbol{w} \in \mathrm{GF}^{n+2^n}(2), S_{(f)}(\boldsymbol{w}) = 0\},$$

$$\boldsymbol{R}_{f0} = \{\boldsymbol{s} : \boldsymbol{s} \in \mathrm{GF}^{n+2^n}(2), r_f(\boldsymbol{s}) = 0\},$$

由定理 1 和定理 2 中的结论可知，$\boldsymbol{S}_{f0}$ 所含元素个数是 $|\boldsymbol{S}_{f0}| = 2^n(2^{2^n} - 2^n)$，而 $\boldsymbol{R}_{f0}$ 所含元素个数是 $|\boldsymbol{R}_{f0}| = 2^{2^n}(2^n - 1) + C_{2^n}^{2^{n-1}}(2^{2^n} - 2^n)$。

设 $f(\boldsymbol{x})$ 是 $n+2^n$ 元选择逻辑函数，定义 $n+2^n$ 元布尔函数

$$g(\boldsymbol{x}) = f(\boldsymbol{x}\boldsymbol{A} + \boldsymbol{a}) + \boldsymbol{b} \cdot \boldsymbol{x} + c,\ \boldsymbol{x} \in \mathrm{GF}^{n+2^n}(2),$$

其中 $\boldsymbol{a}, \boldsymbol{b} \in \mathrm{GF}^{n+2^n}(2), c \in \mathrm{GF}(2)$，$\boldsymbol{A}$ 是 $(n+2^n) \times (n+2^n)$ 可逆矩阵，因为[9]

$$r_g(\boldsymbol{s}) = (-1)^{\boldsymbol{b}\cdot\boldsymbol{s}} r_f(\boldsymbol{s}\boldsymbol{A}), \boldsymbol{s} \in \mathrm{GF}^{n+2^n}(2),$$

$$S_{(g)}(\boldsymbol{w}) = (-1)^{c+\boldsymbol{a}\boldsymbol{A}^{-1}(\boldsymbol{w}+\boldsymbol{b})^{\mathrm{T}}} \cdot$$

$$S_{(f)}((\boldsymbol{w}+\boldsymbol{b})(\boldsymbol{A}^{-1})^{\mathrm{T}}), \boldsymbol{w} \in \mathrm{GF}^{n+2^n}(2),$$

由文献[9]中的结论可知：

a. 若取 A 是 R_{f0} 中任意 $n+2^n$ 个线性无关的向量为行所构成的矩阵，则对任意 $\boldsymbol{b} \in \mathrm{GF}^{n+2^n}(2)$，$g(\boldsymbol{x})$ 不仅保持了选择逻辑函数 $f(\boldsymbol{x})$ 的稳定性，而且满足严格雪崩准则。

根据定理 2 可知 $\boldsymbol{R}_{f0}$ 中存在线性空间 $\mathrm{GF}^{n+2^n}(2)$ 中的多组基：任选 $\mathrm{GF}^n(2)$ 的一组基 $\alpha_1, \cdots, \alpha_n$，再任选 $\mathrm{GF}^{2^n}(2)$ 的一组基 $\beta_1, \cdots, \beta_{2^n}$，则 $(\alpha_1, 0), \cdots, (\alpha_n, 0), 0 = (0, 0, \cdots, 0) \in \mathrm{GF}^{2^n}(2)$ 和 $(\gamma_1, \beta_1), \cdots, (\gamma_{2^n}, \beta_{2^n}), 0 \neq \gamma_i \in \mathrm{GF}^n(2), 1 \leqslant i \leqslant 2^n$ 都是 $f(\boldsymbol{x})$ 的扩散点，且它们显然是 $\mathrm{GF}^{n+2^n}(2)$ 中的一组基，这样可以得到 $\mathrm{GF}^{n+2^n}(2)$ 中的

$$(2^n - 2^0)(2^n - 2^1)\cdots(2^n - 2^{n-1}) \times$$

$$(2^{2^n} - 2^0)(2^{2^n} - 2^1)\cdots(2^{2^n} - 2^{2^n-1})(2^n - 1)^{2^n}$$

组基（有序）。因而可以由 $f(\boldsymbol{x})$ 线性等价地变换出大量满足严格雪崩准则且具有相同稳定性的逻辑函数。

b. 若取 B 是 R_{f0} 中任意 $n+2^n$ 个线性无关的向量为行所构成的矩阵，令 $\boldsymbol{B} = (\boldsymbol{A}^{-1})^{\mathrm{T}}$，再取 $\boldsymbol{b} = (0, 0, \cdots, 0) \in \mathrm{GF}^{n+2^n}(2)$，则由选择逻辑函数 $f(\boldsymbol{x})$ 线性等价地变换出的 $g(\boldsymbol{x})$ 是平衡的，且至少是 1 阶相关免疫的。

由 $|\boldsymbol{S}_{f0}| = 2^n(2^{2^n} - 2^n)$ 至少可以得到

$$(2^{n+2^n} - 2^{2n} - 2^0)(2^{n+2^n} - 2^{2n} - 2^1)\cdots \cdot$$

$$(2^{n+2^n} - 2^{2n} - 2^{n+2^n-1})$$

个矩阵 $\boldsymbol{B}$，可以由 $f(\boldsymbol{x})$ 线性等价地变换出大量平衡且具有相关免疫性的逻辑函数。

c. 由选择逻辑函数 $f(\boldsymbol{x})$ 线性等价地变换出既满足严格雪崩准则，又具有相关免疫性的逻辑函数。例如，当 $n = 2$ 时，可取

$$\boldsymbol{A} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix} \Rightarrow$$

$$\boldsymbol{B} = (\boldsymbol{A}^{-1})^{\mathrm{T}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}。$$

根据定理 1 和定理 2 可知，矩阵 $\boldsymbol{A}$ 满足 a 节中的条件，$\boldsymbol{B}$ 满足 a 节和 b 节中的条件，这时取 $\boldsymbol{b} = (0, 0, \cdots, 0) \in \mathrm{GF}^6(2)$，如此得到的 $g(\boldsymbol{x})$ 既满足严格雪崩准则又具有相关免疫性的逻辑函数。事实上容易证明，对选定的满足 a 节中条件的 $\boldsymbol{A}$，若存在 $\boldsymbol{S}_{f0}$ 中 $n+2^n$ 个向量（不一定线性无关）为行所构成的矩阵，记为 $\boldsymbol{C}$，使得

$$\boldsymbol{C}\boldsymbol{A}^{\mathrm{T}} + \boldsymbol{E} = (\boldsymbol{b}, \boldsymbol{b}, \cdots, \boldsymbol{b})^{\mathrm{T}},$$

其中 $\boldsymbol{E}$ 是单位阵，$\boldsymbol{b} \in \mathrm{GF}^{n+2^n}(2)$，则对任意的 $\boldsymbol{a} \in \mathrm{GF}^{n+2^n}(2)$ 和 $\boldsymbol{C} \in \mathrm{GF}(2)$，所得的 $g(\boldsymbol{x})$ 既满足严格雪崩准则又具有相关免疫性的逻辑函数。前述 $n = 2$ 的例子正好是 $\boldsymbol{C} = (\boldsymbol{A}^{-1})^{\mathrm{T}}$ 的特殊情况。

4　结语

通过全面分析选择逻辑函数的 Walsh 循环谱和自相关函数，说明选择逻辑函数当变元个数 n 不大时，其密码学性质不好，在 n 较大的情况下能够抵抗最佳仿射（BAA）攻击，但是在一定意义上不

能有效地抗击差分攻击。这些结果无疑对密码设计者和攻击者均有参考价值。此外，笔者充分利用概率论的思想和方法，对得出主要结论起了很好的作用。

参考文献

[1] Bruce Schneier. 应用密码学协议算法与C源程序 [M]. 吴世忠，祝世雄，张文政译. 北京：机械工业出版社，2000. 271～272

[2] Geffe P R. How to protect data with ciphers that are really hard to break [J]. Electronics, 1973, 46 (1): 99～101

[3] Amenisch J L C, Piveteau J M, Stadler M A. An efficient electronic payment system protecting privacy [A]. Computer Security-ESORICS94 [C]. Springer-Verlag, 1994. 207～215

[4] Webster A F and Tavares S E. On the design of S-boxes [A], Advances in CryptologyCrypt'85 [C], Springer-Verlag, 1986, 523～534

[5] Siegenthaler T. Correlation immunity of nonlinear combining functions for cryptographic applications [J]. IEEE Transactions on Information Theory, 1984, IT-30 (9): 776～780

[6] 丁存生，肖国镇. 流密码学及其应用 [M]. 北京：国防工业出版社，1994

[7] 李世取，曾本胜，廉玉忠，刘文芬，王 隽，赵雅群，黄晓英. 密码学中的逻辑函数 [M]. 北京：中软电子出版社，2003

[8] Carlet C. Partially-bent functions [A]. Advances in Cryptology-CRYPTO'92 [C]. Springer- Verlag, 1993. 280～291

[9] 杨 锐. 密码学中逻辑函数的有关性质研究 [D]. 郑州：解放军信息工程大学，2005. 25～26

The Cryptographic Properties of Select Logic Functions

Liang Zeng, Li Shiqu

(*Department of Information Research, PLA Information Engineering College, Information Engineering Institute, Zhengzhou* 450002, *China*)

[**Abstract**] In this paper, the main results are concerned with the Walsh transform and the autocorrelation function of select logic functions. Select logic functions with large number of variables have perfect stability and can resist towards cryptanalysis of best affine approximation, but they can't resist towards differential cryptanalysis efficiently because of weak propagation property. By a linear transformation of coordinates, an explicit construction for functions satisfying the strict avalanche criterion or being correlation immune is provided.

[**Key words**] select logic function; Walsh transform; autocorrelation function; strict avalanche criterion; correlation immune; probability expressions